# Solving Elliptic Diophantine Equations by estimating Linear Forms in Elliptic Logarithms. The case of Quartic Equations

N. Tzanakis *

Department of Mathematics, University of Crete, Iraklion, Greece

## 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 over $\mathbb{Q}$ an elliptic curve. A little later, J.Gebel,A.Pethö 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"; see an interesting application in [Str],where fifty elliptic equations are solved. On the other hand,the (theoretically) ineffective part of the method (i.e. the computation of a Mordell-Weil basis), which may be very easy but also very difficult or,in exceptional cases,even impossible,is well separated from the rest steps of the method,so that,if necessary,one can turn for it to the specialists,without asking from them that they be involved in anything else related to the specific equation he wants to solve,but the computation of the Mordell-Weil basis.

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. For such equations one can find in the litterature only sporadic results; see Chapter XXII of [Di] and sections D24 of [V] and [G]. Very few of them are of a general character and these deal with special types of quartic elliptic equations (like,for example,$x^4 - Dy^2 = 1$). Most of the results consist in solving completely specific numerical examples by clever but often very laborious ad hoc arguments; typical examples are the papers [L1],[L2] and [L3] by W.Ljunggren or [B] by R.Bumby. It is worthnoticing that the solution of these equations,as well as of some other difficult ones found in the litterature,turned out to be *very easy* applications of the method of the present paper; see Section 6. It is a remarkable fact

*e-mail: tzanakis@math.uch.gr

that these "historic" examples are associated with elliptic curves of rank 1 or 2 with an easily found Mordell-Weil basis. On the other hand,it is not the purpose of this paper to check the limits of the method presented in it,but rather to expose a method of a general character,which works smoothly in "reasonable" examples. The best choice for such examples,we think,are equations already well known for the difficulty and complexity of their solution. Such equations are found in examples 2 to 7 of Section 6; example 1 has been chosen by the author to illustrate in more detail the method. In the near future we plan to solve equations associated with elliptic curves of higher rank. Such quartic equations have been already constructed by J.Top [T2]; we have good reasons to believe that apart from the much heavier computations that will be involved in these examples,our method will be proven effective for these examples too.

## 2 Preliminaries

The basic aim of this section is the proof of Proposition 2.4, which is fundamental for the purpose of this paper. At the beginning we introduce the necessary concepts and set up the relevant notation.

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,which implies that we may assume the constant term of $Q$ to be a perfect square. Thus,we have to solve in integers an equation of the form

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

This equation defines an elliptic curve $E/\mathbb{Q}$ and the following birational transformation (see [Cn])

$$U = \frac{4e^2X + 4e^2c - d^2}{2eY} \tag{2}$$

$$\begin{aligned} V &= \frac{16e^4X^3 + (32e^4c - 8d^2e^2)X^2 + (d^2 - 4e^2c)^2X - 8e^4Y^2 - 8de^3XY + (2d^3e - 8cde^3)Y}{8e^3Y^2} \\ &= \frac{X}{2e}U^2 - \frac{d}{2e}U - e \end{aligned} \tag{3}$$

transforms (1) to the Weierstrass equation

$$Y^2 + \frac{d}{e}XY + 2ebY = X^3 + \frac{4e^2c - d^2}{4e^2}X^2 - 4e^2aX + ad^2 - 4e^2ac \ , \tag{4}$$

the inverse transformation being

$$X = \frac{2eV + dU + 2e^2}{U^2} \ , \ Y = \frac{8e^3V + 8e^4 + 4e^2dU + (4e^2c - d^2)U^2}{2eU^3} \ ; \tag{5}$$

these transformations are automatically performed by running on a PC Ian Connell's **Apecs**,based on **MapleV** [1] . Finally,the transformation

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

[1]Remark useful for my UBASIC program `comb[No]q.ub`: From these relations we see that,for finite values $U, V$,we have $Y = 0$ only if $V = \frac{(d^2-4e^2c)U^2-4e^2dU-8e^4}{8e^3}$. Replacing in (1) gives $U = 0$, $\frac{32e^4cd-64e^6b-8d^3e^2}{64e^6a-16e^4c^2-d^4+8d^2e^2c}$.

transforms (4) to

$$y^2 = x^3 + Ax + B \ , \tag{7}$$

$$A = -\frac{1}{3}c^2 + bd - 4e^2a \ , \ B = \frac{2}{27}c^3 - \frac{1}{3}bcd - \frac{8}{3}e^2ac + e^2b^2 + ad^2 \ .$$

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

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

depending on which model of $E$ among (1),(4) or (7) we refer to. We also denote the roots of the polynomial $x^3 + Ax + B$ by $e1, e2, e3$, where $e1$ denotes the real root of this cubic polynomial,if it has only one ; in case of three real roots we assume $e1 > e2 > e3$.

As usually,the coefficients of the Weierstrass equation (4) will be denoted by $a1, a3, a2, a4, a6$ and on putting

$$Y = \frac{1}{2}(Y_1 - a_1X - a_3) \tag{8}$$

we transform (4) into

$$Y_1^2 = 4X^3 + b_2X^2 + 2b_4X + b_6 \ , \tag{9}$$

$$b_2 = 4c \, , \ 2b_4 = 4bd - 16e^2a \, , \ b_6 = 4e^2b^2 - 16e^2ac + 4ad^2 \ .$$

We define the following functions :

$$\begin{aligned} \mathcal{U}(x,y) &= \frac{4e^2x + 4e^2c - d^2}{2ey} \ , \\ \mathcal{U}_1(x,y) &= \mathcal{U}(x - \frac{c}{3}, \sigma y - \frac{1}{2}a_1x + \frac{1}{6}a_1c - \frac{1}{2}a_3) \ , \\ f(x) &= \mathcal{U}_1(x, \sqrt{x^3 + Ax + B}) \ . \end{aligned}$$

Observe that,in view of (2) and (6),

$$U(P) = f(x(P)) \ \ \textit{if} \ \ P \in E \ .$$

We also define

$$\begin{aligned} \mathcal{F}(X) &= \mathcal{U}(X, -\frac{a_1}{2}X - \frac{a_3}{2} + \frac{\sigma}{2}\sqrt{4X^3 + b_2X^2 + 2b_4X + b_6}) \\ &= \frac{4e^2X + 4e^2c - d^2}{-dX - 2e^2b + \sigma e\sqrt{4X^3 + b_2X^2 + 2b_4X + b_6}} \end{aligned}$$

and we observe that,if $x - c/3$ is not a zero of the denominator,

$$\mathcal{F}(x - \frac{c}{3}) = f(x) \ . \tag{10}$$

Finally,we put

$$\begin{aligned} \mathcal{F}^*(u) &= \frac{2e\sqrt{Q(u)} + du + 2e^2}{u^2} \ , \\ \mathcal{R}(u) &= beu^3 + 2ceu^2 + 3deu + 4e^3 + (4e^2 + du)\sqrt{Q(u)} \end{aligned}$$

and we easily check that

$$\mathcal{F}^{*\prime}(u) = \frac{-\mathcal{R}(u)}{u^3\sqrt{Q(u)}} \; , \tag{11}$$

where the dash denotes derivative.

**Lemma 2.1.** *i) At least one of the two quantities*

$$d\sqrt{a} + eb \; , \; 8e^3\sqrt{a} + 4e^2c - d^2$$

*is non-zero.*
*ii) Put* $\sigma = sgn(d\sqrt{a} + eb)$ *if* $d\sqrt{a} + eb \neq 0$ *and* $\sigma = sgn(8e^3\sqrt{a} + 4e^2c - d^2)$ *if* $d\sqrt{a} + eb = 0$*. If* $u$ *is sufficiently large,then* $Q(u) > 0$ *and* $sgn(\mathcal{R}(u)) = \sigma$*.*

Proof. (i) From $d\sqrt{a} + eb = 0$ and $8e^3\sqrt{a} + 4e^2c - d^2 = 0$ it follows that $b = -d\sqrt{a}/e$ and $c = -2e\sqrt{a}+d^2/(4e^2)$. Then, $Q(u) = (\sqrt{a}u^2 - (d/2e)u - e)^2$ ,which contradicts the hypothesis $discr(Q) \neq 0$.
(ii) Suppose first that $d\sqrt{a} + be \neq 0$. Then $\lim_{u\to\infty} \mathcal{R}(u)/u^3 = d\sqrt{a} + be$ ,which proves our claim in this case. Next,let $d\sqrt{a} + be = 0$. Then

$$\frac{\mathcal{R}(u)}{u^2} = (be + d\sqrt{a + \frac{b}{u} + \ldots})u + (2ce + 4e^2\sqrt{a + \frac{b}{u} + \ldots}) + \frac{3de}{u} + \frac{4e^3}{u^2} \; .$$

As $u$ tends to infinity the right-hand side tends to $bd/(2\sqrt{a}) + (2ce + 4e^2\sqrt{a}) + 0 + 0$,which,in view of $d\sqrt{a} + be = 0$, is equal to $(8e^3\sqrt{a} + 4e^2c - d^2)/(2e)$ , hence of the same sign as $\sigma$. □

**Lemma 2.2.** *Suppose that* $u$ *is so large that the conclusion of Lemma 2.1 (ii) is satisfied. Then* $\mathcal{F}(\mathcal{F}^*(u)) = u$*.*

Proof. For arbitrary $u, v$ we have the formal identity (cf. (2) and (5))

$$\frac{4e^2\dfrac{2ev + du + 2e^2}{u^2} + 4e^2c - d^2}{\dfrac{8e^3v + 8e^4 + 4e^2du + (4e^2c - d^2)u^2}{u^3}} = u \; . \tag{12}$$

Now take $u$ as large as in the announcement and $v = \sqrt{Q(u)}$, so that (12) becomes

$$u = \frac{4e^2\mathcal{F}^*(u) + 4e^2c - d^2}{\dfrac{8e^3\sqrt{Q(u)} + 8e^4 + 4e^2du + (4e^2c - d^2)u^2}{u^3}} \; . \tag{13}$$

On the other hand,by the definition of F,

$$\mathcal{F}(\mathcal{F}^*(u)) = \frac{4e^2\mathcal{F}^*(u) + 4e^2c - d^2}{-d\mathcal{F}^*(u) - 2e^2b + \sigma e\sqrt{4\mathcal{F}^*(u)^3 + b_2\mathcal{F}^*(u)^2 + 2b_4\mathcal{F}^*(u) + b_6}} \; . \tag{14}$$

It remains to show that the denominators in the right-hand sides of (13) and (14) are equal. We already know that if $u, v$ satisfy $v^2 = Q(u)$,then,in view of (5),(8) and (9),the $X$ and $Y_1$ given by

$$\begin{aligned} X &= \frac{2ev + du + 2e^2}{u^2} \\ Y_1 &= \frac{8e^3v + 8e^4 + 4e^2du + (4e^2c - d^2)u^2}{eu^3} + \frac{d}{e}X + 2eb \end{aligned} \tag{15}$$

satisfy

$$Y_1^2 = 4X^3 + b_2X^2 + 2b_4X + b_6 \; . \tag{16}$$

Taking $u, v$ as above,we get from (16)

$$X = \mathcal{F}^*(u) \; , \; Y_1 = \frac{D}{e} + \frac{d}{e}\mathcal{F}^*(u) + 2eb \; , \tag{17}$$

where $D$ denotes the denominator in the right-hand side of (13). Therefore,in view of (16) and (17),

$$4\mathcal{F}^*(u)^3 + b_2\mathcal{F}^*(u)^2 + 2b_4\mathcal{F}^*(u) + b_6 = (\frac{D}{e} + \frac{d}{e}\mathcal{F}^*(u) + 2eb)^2 = (\frac{2}{u^3}\mathcal{R}(u))^2$$

and,since $sgn(\mathcal{R}(u)) = \sigma$,the denominator in the right-hand side of (14) becomes

$$-d\mathcal{F}^*(u) - 2e^2b + \frac{2e}{u^3}\mathcal{R}(u) = \frac{2e\mathcal{R}(u) - du^3\mathcal{F}^*(u) - 2e^2bu^3}{u^3} \; ,$$

which,as easily checked,is equal to the denominator in the right-hand side of (13). □

Now we observe that,in view of (11) and Lemma 2.1(ii),on the set

$$\{u : u \text{ is as large as in Lemma 2.1}\}$$

$\mathcal{F}^*$ is strictly monotonous ; moreover, $\lim_{u\to\infty}\mathcal{F}^*(u) = 2e\sqrt{a}$ . Note that $2e\sqrt{a}$ is a root of the denominator of F,the other *possible* roots being $-2e\sqrt{a}$ and $(d^2 - 4e^2c)/(4e^2)$ ; in view of the strict monotony of $\mathcal{F}^*$, if $u$ is sufficiently large,the denominator of $\mathcal{F}$ does not vanish in the open interval with endpoints $\mathcal{F}^*(u)$ and $2e\sqrt{a}$ ;hence,in this interval F is defined and Lemma 2.2 holds. From now on the parameter $u_0 > 0$ will be such that *if* $u > u_0$ *then,the conclusion of Lemma 2.1(ii) is satisfied and the interval with endpoints* $\mathcal{F}^*(u)$ *and* $2e\sqrt{a}$ *does not contain neither of the two numbers* $-2e\sqrt{a}$ *and* $(d^2 - 4e^2c)/(4e^2)$. This situation is described in the figure below.


For every specific numerical example,one can esily determine by "experiments" an appropriate value for $u_0$ ; nevertheless,in Appendix 2 we compute an explicit value for this parameter (Proposition 8.4); one can write a simple program based on **MapleV**,so that the computation of $u_0$ can be performed automatically by a PC,given $a, b, c, d, e$ as input data.

In the sequel,the following notation will be used : For any distinct real numbers $a, b$,we denote by $I(a, b)$ the open interval with endpoints $a$ and $b$.

**Lemma 2.3.** *i) The functions* $\mathcal{F}^* \,|\, (u_0, +\infty)$ *and* $\mathcal{F} \,|\, I(\mathcal{F}^*(u_0), 2e\sqrt{a})$ *are inverse to each other.*
*ii) For* $u > u_0$ *we put*

$$f^*(u) = \mathcal{F}^*(u) + \frac{c}{3}\ .$$

*We also define*

$$x_0 = 2e\sqrt{a} + \frac{c}{3}\ .$$

*Then the functions* $f^* \,|\, (u_0, +\infty)$ *and* $f \,|\, I(f^*(u_0), x_0)$ *are inverse to each other.*

Proof. (i) In view of the previous discussion,the function $\mathcal{F}^*\ :\ (u_0, +\infty) \longrightarrow I(\mathcal{F}^*(u_0), 2e\sqrt{a})$ is a bijection. Let $\mathcal{G}$ be the inverse function. For any $X \in I(\mathcal{F}^*(u_0), 2e\sqrt{a})$ there exists an $u > u_0$ such that $\mathcal{F}^*(u) = X$. Then $\mathcal{G}(X) = \mathcal{G}(\mathcal{F}^*(u)) = u$. On the other hand,by Lemma 2.2, $u = \mathcal{F}(\mathcal{F}^*(u))$,hence $u = \mathcal{F}(X)$ , $\mathcal{F}(X) = \mathcal{G}(X)$ and thus F is the inverse of $\mathcal{F}^*$.
(ii) Let $X \in I(f^*(u_0), x_0)$. Then, $X - c/3 \in I(\mathcal{F}^*(u_0), 2e\sqrt{a})$,hence,in view of (i) and (10), $X - c/3 = \mathcal{F}^*(\mathcal{F}(X - c/3)) = \mathcal{F}^*(f(x))$,therefore,by the definition of $f^*$, $f^*(f(X)) = X$. □

Now we prove the main result of this section.

**Proposition 2.4.** *Let* $U > u_0$. *Then*

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

Proof. To the right-hand side integral we make the change of variable $x = f^*(u)$ , $u \in (u_0, +\infty)$. Then,taking also (11) into account,

$$\frac{dx}{\sqrt{x^3+Ax+B}} = \frac{f^{*\prime}(u)\,du}{\sqrt{f^*(u)^3+Af^*(u)+B}} = -\frac{\mathcal{R}(u)\,du}{u^3\sqrt{Q(u)}\sqrt{f^*(u)^3+Af^*(u)+B}} \ . \tag{18}$$

By the definition of $f^*$ and $\mathcal{F}^*$ and in view of (5)-(7),we have $f^*(u)^3 + Af^*(u) + B = y^2$ , where

$$\begin{aligned} \sigma y &= \frac{8e^3\sqrt{Q(u)} + 8e^4 + 4e^2du + (4e^2c - d^2)u^2}{2eu^3} + \\ &\quad \frac{d}{2e}\left(\frac{c}{3} + \frac{2e\sqrt{Q(u)} + du + 2e^2}{u^2}\right) - \frac{cd}{6e} + eb \\ &= \frac{\mathcal{R}(u)}{u^3} \ , \end{aligned}$$

hence,by (18) and Lemma 2.1(ii),

$$\frac{dx}{\sqrt{x^3+Ax+B}} = -\frac{\mathcal{R}(u)\,du}{\sqrt{Q(u)}u^3\left|\frac{\mathcal{R}(u)}{u^3}\right|} = \frac{-\sigma\,du}{\sqrt{Q(u)}} \ .$$

Now the proof follows from Lemma 2.3 (ii). □

# 3 The elliptic integral as a linear form in elliptic logarithms

Let $U$ be any real number $> u_0$. Here $u_0$ is as in Proposition 2.4; an explicit value for this parameter is given in Proposition 8.4 of Appendix 2. In this section we express the integral

$$\int_U^{+\infty} \frac{du}{\sqrt{Q(u)}} \ , \ U > u_0 \tag{19}$$

as linear form in the $\phi-$values of certain fixed points on $E$. Here $\phi$ denotes the group isomorphism

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

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]. Put

$$q(x) = x^3 + Ax + B$$

and denote by $\omega$ the fundamental real period of the Weierstrass $\wp$ function associated with $y^2 = q(x)$ (for the practical computation of $\omega$ see Section 7). For any point $P \in E_0(\mathbb{R})$ we have by [Z],

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

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

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

Note that if both $U$ and $\sqrt{Q(U)}$ are rationals,then,by (1)-(6),$P$ is a rational point. If $P$ is on $E_0(\mathbb{R})$ (equivalently,if $x(P) \geq e_1$) 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 8.4 the integral in (19),which corresponds to the particular value $U$ we consider,is,up to sign,equal to the right-hand side of the last relation,hence equal,up to sign,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 not such a direct relation between the integrals in (19) and $\phi(P)$. At this point,an important role is played by the position of $x_0$ relatively to the roots $e_1, e_2, e_3$ of $q(x)$. We remind that $x_0 = 2e\sqrt{a} + c/3$ ;also, $e_1$ is real and $e_1 > e_2 > e_3$ in case that all three $e_i$'s are real.

**Proposition 3.1.** *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.*

Proof. We have $q(x_0) = (d\sqrt{a} + eb)^2$. Therefore,in case that $d\sqrt{a} + eb \neq 0$ our claim is clear. In the opposite case, $x_0$ is a root of $q(x)$,the other two roots being those of the quadratic polynomial $q(x)/(x - x_0) = x^2 + x_0x + A + x_0^2 =: h(x)$. If $e_2, e_3 \notin \mathbb{R}$,then $x_0$ must coincide with the only real root of $q(x)$,which is $e_1$. Next,suppose that $e_2, e_3 \in \mathbb{R}$ and observe that $h(x_0) = 3x_0^2 + A = 8e^2a + 4ce\sqrt{a} + bd$. On replacing $b$ by $-d\sqrt{a}/e$,we get $h(x_0) = \sqrt{a}(8e^3\sqrt{a} + 4e^2c - d^2)/e$,hence $h(x_0)$ has the sign of $\sigma$. In case that $\sigma = +1$,this implies that $x_0$ is outside the interval having as endpoints the roots of $h(x)$,hence $x_0$ coincides with either $e_1$ or with $e_3$. The second alternative must be excluded,however,for, in that case,the parabola $y = h(x)$,would cut the $x-$axis on $e_2$ and $e_1$ and,since $x_0 = e_3 < e_2 < e_1$,we would have $h'(x_0) < 0$ (the dash denoting derivative) i.e. $3x_0 < 0$. Then,by the definition of $x_0$ , $c < -6e\sqrt{a}$ and $8e^3\sqrt{a} + 4e^2c - d^2 < -16e^3\sqrt{a} - d^2 < 0$,which contradicts the fact that $\sigma = +1$. We conclude therefore that,if $\sigma = +1$ the $x_0 = e_1$. In the case that $\sigma = -1$,we have $h(x_0) < 0$,which implies that $x_0$ is between the roots of $h(x)$ and this happens only if $x_0 = e_2$. □

**Lemma 3.2.** *Let $x_0 \geq e_1$. Put $e_1' = e_1$ if $e_1 - c/3$ is not a root of the denominator of F(see the remark below) and $e_1' = e_1 + \epsilon$, where the "small"positive number $\epsilon$ 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 $x(P) > e_1$.*

Proof. Note first that $f^*(U)$ is defined,since $U > u_0$ (cf. Lemma 2.3). By the definition of $P$ we have $x(P) = f^*(U) = \mathcal{F}^*(U) + c/3$,so that the condition $x(P) > e_1$ is equivalent to $\mathcal{F}^*(U) > e_1 - c/3$. Let first $\sigma = +1$. Then,the function $\mathcal{F}^*$ is strictly decreasing for $U > u_0$, with limiting value $2e\sqrt{a}$,as $U \to +\infty$ (cf. the figure in Section 2),hence $\mathcal{F}^*(U) > 2e\sqrt{a} = x_0 - c/3 \geq e_1 - c/3$. Next,let $\sigma = -1$. Then,the function $\mathcal{F}^*$ is strictly increasing,hence our assumption $U > \mathcal{F}(e_1' - c/3)$ and Lemma 2.3 imply $\mathcal{F}^*(U) > e_1' - c/3 \geq e_1 - c/3$. □

**Remark** It is easy to see that,for any $i = 1,2,3$ ,$e_i - c/3$ is a root of the denominator of F iff $de_i = cd/3 - 2e^2b$.

**Lemma 3.3.** *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 Fand $e_2' = e_2 - \epsilon_2$, where $\epsilon_2$ 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 Fand $e_3' = e_3 + \epsilon_3$, where $\epsilon_3$ is a 'small"positive number, otherwise. The $\epsilon$'s can be chosen arbitrarily,but in such a way that $e_3 \leq e_3' < e_2' \leq e_2$. Let*

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

*Then,for the point $P \in E$,which,according to the beginning of this section, corresponds to $U$,we have $x(P) \in (e_3, e_2)$.*

Proof. Note first that $f^*(U)$ is defined,since $U > u_0$ (cf. Lemma 2.3). By the definition of $P$ we have $x(P) = f^*(U) = \mathcal{F}^*(U) + c/3$,so that the condition $x(P) \in (e_3, e_2)$ is equivalent to $e_3 - c/3 < \mathcal{F}^*(U) < e_2 - c/3$. If $\sigma = +1$, then $\mathcal{F}^*$ is,as already noted in the proof of the previous lemma,strictly decreasing for $U > u_0$, with limiting value $2e\sqrt{a}$,as $U \to +\infty$. It follows that,on the one hand $\mathcal{F}^*(U) + c/3 > 2e\sqrt{a} = x_0 - c/3 \geq e_3 - c/3$ and,on the other hand,in view also of the assumption $U > \mathcal{F}(e_2' - c/3)$, that $\mathcal{F}^*(U) < e_2' - c/3 \leq e_2 - c/3$. If $\sigma = -1$,the proof is completely analogous. □

**Lemma 3.4.** *Let $e_1 > e_2 > e_3$. For every $X \in \mathbb{R}$, $X \neq e_2$ put*

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

*If $X \in (e_3, e_2)$,then $X' > e_1$ and*

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

Proof. Make the change of variable $X \to X'$ in the left-hand side integral and then some routine calculations. □

Let now $U > U_0$ and denote by $P$ the point on $E$ which, acording to the beginning of this section,corresponds to $U$.

First,suppose that $eb + d\sqrt{a} \neq 0$. According to Proposition 3.1, either $x_0 > e_1$ or $e_2, e_3 \in \mathbb{R}\,\&\, x_0 \in (e_3, e_2)$. In the first case we have,in view of Lemma 3.2,$x(P) > e_1$,so that we can write

$$\int_{x_0}^{x(P)} \frac{dx}{\sqrt{q(x)}} = \int_{x_0}^{+\infty} \frac{dx}{\sqrt{q(x)}} - \int_{x(P)}^{+\infty} \frac{dx}{\sqrt{q(x)}} \tag{20}$$

and in the second case we have,in view of Lemma 3.3, $x(P) \in (e_3, e_2)$,so that,on applying Lemma 3.4,we can write

$$\begin{align} \int_{x_0}^{x(P)} \frac{dx}{\sqrt{q(x)}} &= \int_{x_0}^{e_2} \frac{dx}{\sqrt{q(x)}} - \int_{x(P)}^{e_2} \frac{dx}{\sqrt{q(x)}} \tag{21} \\ &= \int_{x_0'}^{+\infty} \frac{dx}{\sqrt{q(x)}} - \int_{x(P)'}^{+\infty} \frac{dx}{\sqrt{q(x)}}\ . \tag{22} \end{align}$$

Next,suppose that $be + d\sqrt{a} = 0$. By Proposition 3.1,either $\sigma = +1 \,\&\, x_0 = e_1$ or $e_2, e_3 \in \mathbb{R} \,\&\, \sigma = -1 \,\&\, x_0 = e_2$. In the first case we have,by Lemma 3.2,$x(P) > e_1$,so that we can write

$$\int_{x_0}^{x(P)} \frac{dx}{\sqrt{q(x)}} = \int_{e_1}^{+\infty} \frac{dx}{\sqrt{q(x)}} - \int_{x(P)}^{+\infty} \frac{dx}{\sqrt{q(x)}} \; ; \tag{23}$$

in the second case,by Lemma 3.3,$x(P) \in (e_3, e_2)$ and,on applying Lemma 3.4,we can write

$$\int_{x_0}^{x(P)} \frac{dx}{\sqrt{q(x)}} = \int_{e_2}^{x(P)} \frac{dx}{\sqrt{q(x)}} = -\int_{x(P)'}^{+\infty} \frac{dx}{\sqrt{q(x)}} \; . \tag{24}$$

Now we express the integrals in the left-hand sides of (20)-(24) in terms of $\phi$-values and $\omega$. In case that $e_2, e_3 \in \mathbb{R}$,we denote by $Q_2$ the point with $x(Q_2) = e_2$ , $y(Q_2) = 0$ and we put for any point $\Pi \in E$

$$\Pi' = \Pi + Q_2 \; .$$

Observe that

$$y(\Pi') \geq 0 \Longleftrightarrow y(\Pi) \geq 0$$

and that

$$x(\Pi') = x(\Pi)' \; .$$

The last relation permits to replace the lower limits $x(P)'$ of the integrals in (22) and (24) 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 $x(P_0) = x_0, y(P_0) = \sigma(be + d\sqrt{a})$.

Having in mind the definition of the function $\phi$ as defined by Zagier in page 429 of [Z] (see also the Introduction of [ST]) and also that,by the definition of $P$ , $y(P) \geq 0$,we can write (20)-(24),respectively,as follows.

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

$$\int_{x_0}^{x(P)} \frac{dx}{\sqrt{q(x)}} = \omega\phi(P_0) - \omega\phi(P) \; . \tag{25}$$

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

$$\int_{x_0}^{x(P)} \frac{dx}{\sqrt{q(x)}} = \omega\phi(P_0') - \omega\phi(P') \; . \tag{26}$$

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

$$\int_{x_0}^{x(P)} \frac{dx}{\sqrt{q(x)}} = \frac{\omega}{2} - \omega\phi(P) \; . \tag{27}$$

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

$$\int_{x_0}^{x(P)} \frac{dx}{\sqrt{q(x)}} = -\omega\phi(P') \; . \tag{28}$$

Now we apply Proposition 2.4. In view of (25)-(28) we have :

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

$$\frac{1}{\omega}\int_U^{+\infty}\frac{du}{\sqrt{Q(u)}} = \sigma(\phi(P_0) - \phi(P)) \tag{29}$$

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

$$\frac{1}{\omega}\int_U^{+\infty}\frac{du}{\sqrt{Q(u)}} = \sigma(\phi(P_0') - \phi(P')) \tag{30}$$

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

$$\frac{1}{\omega}\int_U^{+\infty}\frac{du}{\sqrt{Q(u)}} = \frac{1}{2} - \phi(P) \tag{31}$$

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

$$\frac{1}{\omega}\int_U^{+\infty}\frac{du}{\sqrt{Q(u)}} = \phi(P') \tag{32}$$

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

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

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 (with $U_0$ as in Lemma 3.3),we may assume that $U > U_0$ . We write

$$P = m_1 P_1 + \ldots + m_r P_r + T , \tag{33}$$

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

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

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

$$V^2 = aU^4 - bU^3 + cU^2 - dU + e^2 , \; U > 0 \tag{34}$$

On replacing the coefficients $a, b, c, d, e$ by $a, -b, c, -d, e$,respectively, there will be,probably,a change in the parameters $u_1, u_2, u_3, u_4, u_0$ and $U_0$ (see Proposition 8.4 and Lemmas 3.2,3.3), so we assume that our solution $U$ exceeds the larger of the two values $U_0$. Another change is,in generally,caused by the above change of the coefficients $a,\ldots,e$ to the parameters $c_{10}$ and $c_9$ (for their definition see at the beginning of the next section) but,again,we simply take the larger of the two values for each of these parameters. Apart from this,the solution of both (34) and (1) with $U>0$, by means of the procedure that we propose in this paper,leads to the same upper bound for $M$. Indeed,equation (34) defines the same elliptic curve $E$ as (1) and,on the other hand,as it will be clear below, all constants or parameters that will finally lead to the bound of $M$ are not affected if we replace the coefficients $a,b,c,d,e$ by $a,-b,c,-d,e$, respectively, except,possibly,for $\sigma$ (and $U_0, c_9$ and $c_{10}$,as already noted). This,in turn,would only change the sign of the right-hand sides of the relations (37)-(40) below,i.e. it would cause a change of sign to the linear form $\Phi(U)$, which we will consider in the following section. Since, however,the bound that we will get in the next section depends on the *absolute value* of $\Phi(U)$, our claim follows.

In view of the definition of the $R_i$'s and the relation $2\cdot Q_2=\mathcal{O}$,we can write (33) as

$$P=m_1R_1+\ldots+m_rR_r+T_0\ , \tag{35}$$

where $T_0=T$ or $T'(=T+Q_2)$ and,of course,$T_0$ is a torsion point of $E$. If $P\in E_0(\mathbb{R})$,then $T_0\in E_0(\mathbb{R})$. If $P\notin E_0(\mathbb{R})$,then, we add to both sides of (35) the point $Q_2$ and we replace $T_0+Q_2$ by $T_0$,so that we obtain the relation

$$P'=m_1R_1+\ldots+m_rR_r+T_0\ . \tag{36}$$

According to our previous discussion,which concluded to relations (29)-(32),it is in case of the relations (29) and (31) that (35) holds,while (36) holds in case of the relations (30) and (32). In both cases,all the points $P$ (resp.$P'$),$R_1,\ldots,R_r,T_0$ belong to $E_0(\mathbb{R})$,so that their $\phi-$values are defined. Then,in view of (35) (resp. (36)) we have

$$\phi(P)(\text{resp. }\phi(P'))=m_1\phi(R_1)+\ldots+m_r\phi(P_r)+\phi(T_0)+m_0\ ,$$

for some $m_0\in\mathbb{Z}$,which,in absolute value,does not exceed $rM+1$, in view of the fact that the $\phi$-values belong to the interval $[0,1)$. Note that we can write

$$\phi(T_0)=\frac{s}{t}\ ,\ s,t\in\mathbb{Z}\ ,\ 0\le s<t\ ,$$

where $t$ does not exceed the maximal order of the points of $E_{tors}(\mathbb{Q})$, hence,in any case, $t\le 12$ by Mazur's Theorem. Now we go back to (29)-(32). By replacing,if necessary,the $m_i$'s by $-m_i$'s for $i=0,1,\ldots,r$ we are led to the following relations :

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

$$\frac{\sigma}{\omega}\int_U^{+\infty}\frac{du}{\sqrt{Q(u)}}=(m_0-\frac{s}{t})+\phi(P_0)+m_1\phi(R_1)+\ldots+m_r\phi(R_r) \tag{37}$$

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

$$\frac{\sigma}{\omega}\int_U^{+\infty}\frac{du}{\sqrt{Q(u)}}=(m_0-\frac{s}{t})+\phi(P_0')+m_1\phi(R_1)+\ldots+m_r\phi(R_r) \tag{38}$$

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

$$\frac{1}{\omega}\int_U^{+\infty} \frac{du}{\sqrt{Q(u)}} = (m_0 - \frac{s}{t} + \frac{1}{2}) + m_1\phi(R_1) + \ldots + m_r\phi(R_r) \tag{39}$$

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

$$\frac{1}{\omega}\int_U^{+\infty} \frac{du}{\sqrt{Q(u)}} = (m_0 + \frac{s}{t}) + m_1\phi(R_1) + \ldots + m_r\phi(R_r) \tag{40}$$

Let $\wp$ denote the Weierstrass function associated with the equation $y^2 = q(x)$. By the definition of the function $\phi$,we have,for any point $\Pi$ on $E_0(\mathbb{R})$ , $\wp(\omega\phi(\Pi)) = x(\Pi)$,hence $\omega\phi(\Pi)$ is the *elliptic logarithm* of either $\Pi$ or of $-\Pi$; also,$\omega$ is the elliptic logarithm of the point $\mathcal{O}$ . It follows that,on multiplying by $\omega$ the relations (37)-(40),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 (37) (respectively,(38)),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.in Section 6 the examples 1,2,3 and 4 ),the term $\phi(P_0)$ (respectively $\phi(P_0'))$ can be removed,at the cost of a slight change of the $m_i$'s (for $i = 1,\ldots,r$ and,probably,the appearance in some of the modified $m_i$'s of small (known) denominators. The important fact,however,is that,in such a case,we can find an upper bound for the (unknown) nominators of the modified $m_i$'s $i = 1,\ldots,r$,which is of the form $c_{12}'M + c_{13}'$ and $c_{12}', c_{13}'$ is trivial to compute explicitly.

# 4 An upper bound of $M$

In this section we assume that $U$ is an integer $> U_0$ (with $U_0$ as in lemma 3.2 or 3.3) such that $\sqrt{Q(U)} \in \mathbb{Z}$ and that $P$ is the point on $E$ that corresponds to $U$,as explained at the begining of Section 3,therefore one out of the four relations (37)-(40) holds. In any of these relations,we denote the linear form in 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 in the left-hand side is positive and we can find for it an upper bound of the form $c_9 \cdot U^{-1}$,hence

$$0 < \Phi(U) < \frac{c_9}{\omega} \cdot |U|^{-1} \ . \tag{41}$$

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 $\alpha$ and $\beta$ and since we have,by the definition of $P$,

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

it follows that a non-negative constant $c_{10}$ can be explicitly calculated [2], such that,

$$h(X_1(P)) \le c_{10} + 2\log U \quad \text{if } U \text{ is not “very small”} \ . \tag{42}$$

[2]We remind 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 (34).

Here $h(\cdot)$ denotes the Weil height (if $m/n$ is a rational number in lowest terms,then $h(m/n) = \log\max(|m|,|n|)$) [3] . On the other hand,if we denote by $\hat{h}(\cdot)$ the Néron-Tate hate, then,by applying Theorem 1.1 of J.Silverman [S3],we can easily calculate an explicit positive constant $c_{11}$,such that

$$\hat{h}(P) - \frac{1}{2}h(X_1(P)) \leq c_{11} \ . \tag{43}$$

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 what one does,when he has to solve a particular numerical example,is to choose an equation which implies the smallest possible value for $c_{11}$. In the examples that we solve in Section 6,we choose the *minimal Weierstrass equation*,computed by Apecs (Laska's algorithm); sometimes,it turns out that this equation is (7). By Inequality 1,Section 3 of [ST],we have $\hat{h}(P) \geq c_1 M^2$ 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 at the end of Section 2 of [ST]),therefore,by (43),

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

and now by (42) and (41)

$$|\omega \cdot \Phi(U)| \leq c_9 \exp(c_{11} + \frac{1}{2}c_{10}) \cdot \exp(-c_1 M^2) \ . \tag{44}$$

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,

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

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 are differing from them "very little",if any at all. We define now

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

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

$$N \leq c_{12}M + c_{13} \ . \tag{45}$$

By David's theorem (see Theorem 7.1),we have

$$|\omega\Phi(U)| \geq \exp\left(-c_4(\log N + c_5)(\log\log N + c_6)^{\nu+2}\right) \tag{46}$$

(the computation of the constants $c_4, c_5, c_6$ is discussed in detail in Section 7). The combination of (44) and (46) gives

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

[3] Here we use the fact that $U$ is an integer; otherwise,in (42) we should have $h(U)$ in place of $\log U$.

In view of (45) and the fact that we may assume $M \geq 16$ this implies

$$M^2 \leq c_1^{-1} \left( \log c_9 + \frac{1}{2} c_{10} + c_{11} \right) + c_1^{-1} c_4 (\log M + c_7)(\log \log M + c_8)^{\nu+2} \ , \tag{47}$$

where

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

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

# 5 Reduction of the upper bound

In view of inequality (44) and the upper bound obtained from (47) we can write

$$|\Phi| < K_1 \exp(-K_2 M^2) \ , \ M < K_3 \ , \tag{48}$$

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

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

and $K_3$ is "very large". We put

$$\frac{s'}{t'} = \begin{cases} -\dfrac{s}{t} & \text{in case of (37), (38)} \\ -\dfrac{s}{t} + \dfrac{1}{2} & \text{in case of (39)} \\ \dfrac{s}{t} & \text{in case of (40)} \end{cases} \quad , \ t' > 0 \ , \ \gcd(s', t') = 1 \ .$$

We also put for simplicity in the notation

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

and in case of (37) and (38) only,

$$\rho_0 = \begin{cases} \phi(P_0) & \text{in case of (37)} \\ \phi(P_0') & \text{in case of (38)} \end{cases}$$

We distinguish three cases :

- *Case 1*: One of the relations (39) or (40) holds In this case our linear form is

$$\Phi = m_1 \rho_1 + \ldots + m_r \rho_r + (m_0 + \frac{s'}{t'}) \ .$$

- *Case 2*: One of the relations (37) or (38) holds and $\rho_0$ is *linearly independent* over $\mathbb{Q}$ from $\rho_1, \ldots, \rho_r$. In this case our linear form is

$$\Phi = \rho_0 + m_1 \rho_1 + \ldots + m_r \rho_r + (m_0 + \frac{s'}{t'}) \ . \tag{49}$$

- *Case 3*: One of the relations (37) or (38) holds and $\rho_0$ is *linearly dependent* on $\rho_1, \ldots, \rho_r$ over $\mathbb{Q}$ . In this case our linear form is

$$\Phi = \frac{n_0}{d_0} + \frac{n_1}{d_1}\rho_1 + \ldots + \frac{n_r}{d_r}\rho_r \ ;$$

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

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

$$\mathcal{A} = \begin{pmatrix} 1 & \cdots & 0 & 0 \\ 0 & \cdots & 0 & 0 \\ \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 1 & 0 \\ [K_0\rho_1] & \cdots & [K_0\rho_r] & K_0 \end{pmatrix}$$

($[\cdot]$ means rounding towards zero,i.e. $[\alpha] = \lfloor \alpha \rfloor$ if $\alpha \geq 0$ 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 $t_0 \leq 12$ 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 5.1.** *If* $|\mathbf{b}_1| > 2^{r/2}t'K_3\sqrt{r^2+r}$, *then*

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

In Case 3,we apply the folowing result,the proof of which is essentially identical to that of Proposition 5.1.

**Proposition 5.2.** *Let*

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

*(note that* $c'_{12} \leq c_{12}$ *and* $c'_{13} \leq c_{13}$ *; cf. (45)) and*

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

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

$$M^2 \leq K_2^{-1}\left(\log(dK_0K_1) - \log(\sqrt{2^{-r}|\mathbf{b}_1|^2 - rK_4^2} - rK_4)\right) \ .$$

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

$$\mathbf{x} = \begin{pmatrix} 0 \\ \vdots \\ 0 \\ -t'[K_0\rho_0] \end{pmatrix} ,$$

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

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

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,

$$\begin{pmatrix} x_1 \\ \vdots \\ x_{r+1} \end{pmatrix} = \mathcal{V}\mathcal{A}^{-1}\mathbf{x} = -\frac{t'[K_0\rho_0]}{K_0} \cdot \begin{pmatrix} v_{1,r+1} \\ \vdots \\ v_{r+1,r+1} \end{pmatrix} .$$

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 $\Gamma$ : By Lemma 3.5 of [dW] we have

$$d(\mathbf{x}, \Gamma) \geq 2^{r/2} \|x_{i_0}\| |\mathbf{b}_1| , \tag{50}$$

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 $\lambda_0 = t'm_1[K_0\rho_1] + \ldots + t'm_r[K_0\rho_r] + (t'm_0 + s')K_0$. In view of (50) 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 $\lambda = t'[K_0\rho_0] + \lambda_0$,hence,as it is easily seen,

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

In view of this and (50) 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 (48) 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 in both sides and obtain thus the following result,which we apply in case that $\Phi$ is given by (49):

**Proposition 5.3.** *If* $\|x_{i_0}\||\mathbf{b}_1| > 2^{r/2}t'\sqrt{(r^2+r)K_3^2 + 2rK_3 + 1}$ *,then*

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

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 $\Pi$, are always $(x(\Pi), y(\Pi))$,i.e. they refer to the model $y^2 = x^3 + Ax + B$, in the notation of Section 2. Also,we do not make any special mentioning to the values of the parameters $u_0$ and $U_0$; these can be easily calculated and never,in these examples, exceed 12.

## 6.1 Example 1

Consider the equation

$$V^2 = Q(U) := U^4 - 8U^2 + 8U + 1 \tag{51}$$

and denote by $E$ the elliptic curve defined by means of (51). Here,

$$a = 1\,,\, b = 0\,,\, c = -8\,,\, d = 8\,,\, e = 1\ ;\ A = \frac{-76}{3}\,,\, B = \frac{1280}{27}\,,\, \sigma = +1\ ,$$

$$a_1 = 8\ ,\ a_2 = -24\ ,\ a_3 = 0\ ,\ a_4 = -4\ ,\ a_6 = 96\ ,\ \Delta_E = 2^{12}\cdot 17 = -5296\ ,\ j_E = \frac{438976}{17}\ ,$$

$$e_3 = -\frac{5}{3} - \sqrt{17} < x_0 = -\frac{2}{3} < -\frac{5}{3} + \sqrt{17} = e_2 < e_1 = \frac{10}{3}\ ,$$

$$\omega_1 = \frac{2\pi i}{M(\sqrt{e_1-e_3}, \sqrt{e_2-e_3})} = 2.133100331\ldots\cdot i\ ,\omega_2 = -\frac{2\pi}{M(\sqrt{e_1-e_3}, \sqrt{e_1-e_2})} = 3.438877420\ldots\ ,$$

$$\tau = 1.612149869\ldots i\ ,\ \omega = -\omega_2\ .$$

We apply Silverman's Theorem 1.1 [S3] 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. (43) $c_{11} = 3.19241$. 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

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

provided that $|U| \geq 4$. But we have also 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 (34)). Again, $X_1(P) = X(P) - 3$ and the above inequality becomes

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

provided that $U > 10$. Also,if $U \geq 15$ 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*) with is given by

$$P_1 = (-\frac{2}{3}, -8)\ ,\ P_2 = (\frac{22}{3}, 16)\ ,\ T = (\frac{10}{3}, 0)\ ,$$

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 [S2], $\hat{h}(P_1) = 0.317137308\ldots\ ,\ \hat{h}(P_2) = 0.480233071\ldots$ 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

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

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

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

Since $x_0 \in (e_3, e_2)$,we need also the point $P_0'$ (cf.(38)); we have

$$P_0 = (-\frac{2}{3}, 8) = -P_1\ ,\ \ P_0' = P_0 + Q_2 = -P_1 - Q_2 = -R_1\ ,$$

which immediately implies that

$$\phi(P_0') = \phi(-R_1) = 1 - \phi(R_1)$$

and the right-hand side of (38),which we denoted by $\Phi(U)$ in section 4,becomes

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

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

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

and,since $|m_0| \leq 2M + 1$ (see just before (45)),

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

For the application of David's theorem we calcule:

$$h\left(\frac{A}{4},\frac{B}{16}\right)=h\left(\frac{-19}{3},\frac{80}{27}\right)=\log(9\cdot 19)\ ,\ h(j_E)=h\left(\frac{438976}{17}\right)=\log 438976\ ,\ h_E=\log 438976\ .$$

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

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

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

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

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

$$c_4=2.9\cdot 10^{24}\cdot 4^{18}\cdot 2^8\cdot 4^{57.3}\cdot 1.26829^{-7}\cdot 2193.0479=6.6723\times 10^{74}\ ,$$

$$c_5=\log(D\mathcal{E})=1.96144\ ,\ c_6=\log(D\mathcal{E})+h_E=14.953641\ ,\ c_7=3.42586\ ,\ c_8=15.482\ .$$

Now (47) implies $M<2.15\times 10^{41}$ and by the definition of $K_1,\ldots,K_4$ we have

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

The hypothesis of Proposition 5.2 requires that $|\mathbf{b}_1|>2\sqrt{6}K_4$, and this is satisfied if we choose $K_0=10^{128}$.Then,Proposition 5.2 gives the new bound $M\le 29$. 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 $M\le 8$. This bound cannot be essentially improved further,therefore we give all points

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

in the range $|m_1|,|m_2|\le 8$, as an input to a simple program based on Ubasic,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 $(U,V)=(-6,\pm 31),(0,\pm 1),(2,\pm 1)$. For the computation of $c_9$ and $c_{10}$,we have assumed that $|U|\ge 15$,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 (51) are* $(U,V)=(-6,\pm 31),(0,\pm 1),(2,\pm 1)$.

### 6.2 Example 2

Consider Fermat's equation

$$V^2=Q(U):=U^4+4U^3+10U^2+20U+1 \tag{52}$$

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

$$a=1\,,\,b=4\,,\,c=10\,,\,d=20\,,\,e=1\ ;\ A=\frac{128}{3}\,,\,B=\frac{5312}{27}\,,\,\sigma=+1\ ,$$

$$a_1 = 20 \ , \ a_2 = -90 \ , \ a_3 = 8 \ , \ a_4 = -4 \ , \ a_6 = 360 \ , \ \Delta_E = -2^4 \cdot 331 = -5296 \ , \ j_E = \frac{131072}{331} \ ,$$

$$e_1 = -3.556644723\ldots < x_0 = \frac{16}{3} \ , \ e_2, e_3 \not\in \mathbb{R} \ ,$$

$$\omega_1 = \Omega_1 - \Omega_2 \ , \ \omega_2 = \Omega_1 + \Omega_2 \ , \ \Omega_1 = 1.502217471\ldots \ , \ \Omega_2 = 1.108711951\ldots \cdot i$$

$$\tau = 0.294734582\ldots + 0.955579157\ldots \cdot i \ , \ \omega = 2\Omega_1 \ .$$

The minimal Weierstrass model for the elliptic curve $E$ is

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

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

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

and

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

respectively,provided that $U \geq 20$. 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 a better for the reduction process (i.e. greater) $K_2 = c_1$. Thus,we take as a basis

$$R_1 = (-\frac{8}{3}, 8) \ , \ R_2 = (\frac{16}{3}, 24) \ ;$$

$$\hat{h}(R_1) = 0.176622454\ldots \ , \ \hat{h}(R_2) = 0.317960695\ldots \ , \ c_1 = 0.173655878\ldots \ .$$

$$\phi(R_1) = 0.428683280\ldots \ , \ \phi(R_2) = 0.251223446\ldots \ .$$

In this example,it is relation (37) that holds,hence we need the point $P_0$,which,it is straightforward to see,is equal to $R_2$ and the right-hand side of (37) 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,

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

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

Now (47) implies $M < 3.5 \times 10^{40}$ ; also

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

The hypothesis of Proposition 5.2 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 $M \leq 33$ and by repeating the process with $K_3 = 33$ and $K_0 = 10^9$ we get the bound $M \leq 9$. Then,a direct search in the computer,as in Example 1, shows that
*The only integers satisfying (52) 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).

### 6.3 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

$$V^2 = Q(U) := 6U^4 - 6U^2 + 9 \tag{53}$$

and we denote by $E$ the corresponding elliptic curve. Here

$$a = 6\,,\, b = 0\,,\, c = -6\,,\, d = 0\,,\, e = 3\,;\; A = -228\,,\, B = 848\,,\, \sigma = +1\,,\, be + d\sqrt{a} = 0\,,$$

$$a_1 = 0\ ,\ a_2 = -6\ ,\ a_3 = 0\ ,\ a_4 = -216\ ,\ a_6 = 1296\ ,\ \Delta_E = 2^{13} \cdot 3^7 \cdot 5^2 = -5296\ ,\ j_E = \frac{219488}{75}\ ,$$

$$e_3 = -6\sqrt{6} - 2 < e_2 = 4 < e_1 = 6\sqrt{6} - 2 = x_0\ ,$$

$$\omega_1 = 1.262713190\ldots \cdot i\ ,\ \omega_2 = -1.535696208\ldots\ ,\ \tau = 1.216187666\ldots \cdot i\ ,\ \omega = -\omega_2\ .$$

The minimal Weierstrass model for the elliptic curve $E$ is

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

from this we find,as in the previous examples, $c_{11} = 3.39514$ , $c_{10} = 2.54766$ , $c_9 = 0.41$ , provided that $|U| \geq 15$. 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

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

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

$$\hat{h}(R_1) = 0.45320430\ldots,\ \hat{h}(R_2) = 0.21172057\ldots;\ \phi(R_1) = 0.36241206\ldots,\ \phi(R_2) = 0.22774550\ldots\ .$$

In this example,it is relation (39) that holds,which is

$$\Phi(U) = (m_0 + \frac{s}{2}) + m_1\phi(R_1) + m_2\phi(R_2)$$

We see then that $c_{12} = 4$ , $c_{13} = 5$ .
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 $A_0 = A_1 = A_2 = h_E$ , $\mathcal{E} = 1.0358\, e$ .
Finally,

$$c_4 = 2.9 \cdot 10^{24} \cdot 4^{18} \cdot 4^{57.3} \cdot 1.035174^{-7} \cdot 1860.4372 = 9.163 \times 10^{72} ,$$

$$c_5 = \log \mathcal{E} \ , \ c_6 = \log \mathcal{E} + h_E \ , \ c_7 = 2.49962 \ , \ c_8 = 13.862405 .$$

Now (47) implies $M < 2.35 \times 10^{40}$ ; also

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

The hypothesis of Proposition 5.1 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 $M \leq 32$ and by repeating the process with $K_3 = 32$ and $K_0 = 10^9$ we get the bound $M \leq 10$. Then,a direct search in the computer,as in Example 1,shows that
*The only integers satisfying (53) are given by*

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

### 6.4 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

$$V^2 = Q(U) := 6U^4 + 24U^3 + 36U^2 + 24U + 4 \tag{54}$$

and we denote by $E$ the corresponding elliptic curve. Here

$$a = 6\,,\ b = 24\,,\ c = 36\,,\ d = 24\,,\ e = 2\,;\ A = 48\,,\ B = 0\,,\ \sigma = +1 ,$$

$$a_1 = 12 \ , \ a_2 = 0 \ , \ a_3 = 96 \ , \ a_4 = -96 \ , \ a_6 = 0 \ , \ \Delta_E = -1728 \ , \ j_E = 1728 ,$$

$$e_1 = 0 < x_0 = 4\sqrt{6} + 12 \ , \ e_2, e_3 \notin \mathbb{R} ,$$

$$\Omega_1 = 1.408792103\ldots \ , \ \Omega_2 = \Omega_1 \cdot i \ , \ \omega_1 = \Omega_1 - \Omega_2 \ , \ \omega_2 = \Omega_1 + \Omega_2 \ , \ \tau = i \ , \ \omega = 2\Omega_1 .$$

The minimal Weierstrass model for the elliptic curve $E$ is

$$Y_1^2 = X_1^3 + 3X_1 \ , \ \left(X_1(P) = \frac{1}{4}X(P) + 3\right) .$$

Then, $c_{11} = 1.69123$ , and for $|U| \geq 20$, $c_{10} = 1.7927$ , $c_9 = 0.4566$ .
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,$c_1 = \hat{h}(P_1) = 0.250591196\ldots$ and

$\phi(R_1) = 0.301121610\ldots$ In this example,it is relation (37) 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 (37) in our case becomes

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

Then $c_{12} = 2$ , $c_{13} = 5$ , $c'_{12} = 2$ , $c'_{13} = 1$ . For the application of David's theorem we calculate

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

Finally,

$$c_4 = 2.9\cdot 10^{18}\cdot 4^8\cdot 3^{38.3}\cdot 140.52 = 5.01603\times 10^{43}\ ,$$

$$c_5 = 1\ ,\ c_6 = 1 + h_E\ ,\ c_7 = 1.8493972\ ,\ c_8 = 8.761075225$$

and now (47) implies $M < 5\times 10^{24}$ ; also

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

The hypothesis of Proposition 5.2 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 $M \leq 15$ and by repeating the process with $K_3 = 15$ and $K_0 = 10^5$ we get the bound $M \leq 5$. Then,a direct search in the computer,as in Example 1,shows that *The only integers satisfying (54) are* $(U,V) = (-4,\pm 22), (-2,\pm 2), (0,\pm 2), (2,\pm 22)$ .

## 6.5 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

$$V^2 = Q(U) := 3U^4 + 12U^3 + 12U^2 + 9 \tag{55}$$

and we denote by $E$ the corresponding elliptic curve. Here

$$a = 3\,,\, b = 12\,,\, c = 12\,,\, d = 0\,,\, e = 3\ ;\ A = -156\,,\, B = 560\,,\, \sigma = +1\ ,$$

$$a1 = 0\ ,\ a_2 = 12\ ,\ a_3 = 72\ ,\ a_4 = -108\ ,\ a_6 = -1296\ ,\ \Delta_E = 2^{14}3^8\ ,\ j_E = \frac{35152}{9}\ ,$$

$$e_3 = -14 < e_2 = 4 < e_1 = 10 < x_0 = 6\sqrt{3} + 4\ ,$$

$$\omega_1 = -1.376409401\ldots\cdot i\ ,\ \omega_2 = 1.760787652\ldots\ ,\ \tau = 1.279261571\ldots\cdot i\ ,\ \omega = \omega_2\ .$$

The minimal Weierstrass model for the elliptic curve $E$ is

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

Then,$c_{11} = 4.34$ , and for $|U| \geq 20$ ,$c_{10} = 2.7394$ , $c_9 = 0.6455$. 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,

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

Torsion group is $\{\mathcal{O},(10,0),(4,0),(-14,0)\}$. In this example,it is relation (37) 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 (37) in our case becomes

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

Then,$c_{12}=4\ ,\ c_{13}=11\ ,\ c'_{12}=2\ ,\ c'_{13}=1$ .
For the application of David's theorem we calculate

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

Finally,

$$c_4=2.9\cdot 10^{18}\cdot 4^8\cdot 3^{38.3}\cdot 126.2033344=4.505\times 10^{43}\ ,$$

$$c_5=1\ ,\ c_6=1+h_E\ ,\ c_7=2.55817\ ,\ c_8=12.02943$$

and now (47) implies $M<4.54\times 10^{24}$ ; also

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

The hypothesis of Proposition 5.2 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 $M\le 11$ and one more reduction step with $K_3=11$ and $K_0=10^5$ implies $M\le 4$. Then, a direct search in the computer shows that
*The only integers satisfying (55) are* $(U,V)=(-14,\pm 291),(-3,\pm 6),(-2,\pm 3),(0,\pm 3),(1,\pm 6),(12,\pm 291)$ .

### 6.6 Example 6

Next,we consider the rather well knowm 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

$$V^2=Q(U):=2U^4+8U^3+12U^2+8U+1 \qquad (56)$$

and we denote by $E$ the corresponding elliptic curve. In this example

$$a=2\,,\,b=8\,,\,c=12\,,\,d=8\,,\,e=1\ ;\ A=8\,,\,B=0\,,\,\sigma=+1$$

$$a_1=8\ ,\ a_2=-4\ ,\ a_3=16\ ,\ a_4=-8\ ,\ a_6=32\ ,\ \Delta_E=-2^{15}\ ,\ j_E=1728$$

$$e_1=0<x_0=2\sqrt{2}+4\ ,\ e_2,e_3\not\in\mathbb{R}$$

$$\Omega_1=2.204878798\ldots\ ,\ \Omega_2=\Omega_1 i\ ,\ \omega_1=\Omega_1-\Omega_2\ ,\ \omega_2=\Omega_1+\Omega_2\ ,\ \tau=i\ ,\ \omega=2\Omega_1\ .$$

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

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

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

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

Generator of the torsion group : $T = (0,0)$, of order 2. We are in case (37) :

$$P_0 = (2\sqrt{2}+4\, ,\, 8\sqrt{2}+8)\ ,\ 2P_0 = P_1\ .$$

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

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

For the application of David's theorem we calculate

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

$$c_4 = 2.9\cdot 10^{18}\cdot 4^8\cdot 3^{38.3}\cdot 140.518161 = 5.016\times 10^{43}\ ,$$

$$c_5 = 1\ ,\ c_6 = 1+h_E\ ,\ c_7 = 1.8493972\ ,\ c_8 = 8.76108\ .$$

Relation (47) implies $M < 3.5\times 10^{24}$

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

First reduction $M \le 10$,second reduction $M \le 4$.
*The only integers satisfying (56) are* $(U,V) = (-14,\pm 239), (-2,\pm 1), (0,\pm 1), (12,\pm 239)$ .

### 6.7 Example 7

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

$$V^2 = Q(U) := 2U^4+8U^3+16U^2+16U+4 \tag{57}$$

and we denote by $E$ the corresponding elliptic curve. In this example

$$a=2\, ,\, b=8\, ,\, c=16\, ,\, d=16\, ,\, e=2\ ;\ A = \frac{32}{3}\, ,\, B = \frac{1280}{27}\, ,\, \sigma = +1\ ,$$

$$a_1 = 8\ ,\ a_2 = 0\ ,\ a_3 = 32\ ,\ a_4 = -32\ ,\ a_6 = 0\ ,\ \Delta_E = -2^8\ ,\ j_E = 2^7\ ,$$

$$e_1 = -\frac{8}{3} < x_0 = 4\sqrt{2}+\frac{16}{3}\ ,\ e_2, e_3 \notin \mathbb{R}$$

$$\Omega_1 = 2.018230827\ldots\ ,\ \Omega_2 = 1.37367687\ldots\cdot i\ ,\ \omega_1 = \Omega_1-\Omega_2\ ,\ \omega_2 = \Omega_1+\Omega_2\ ,\ |\tau| = 1\ ,\ \omega = 2\Omega_1\ .$$

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

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

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

$$R_1 = (\frac{4}{3},8)\ ,\ c_1 = \hat{h}(R_1) = 0.2161655\ldots\ ,\ \phi(R_1) = 0.295679873\ldots\ .$$

Generator of the torsion group : $T = (-8/3, 0)$, of order 2. We are in case (37) :

$$P_0 = (4\sqrt{2} + \frac{16}{3} \, , \, 16\sqrt{2} + 16) \ , \ 2P_0 = P_1 \ .$$

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

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

For the application of David's theorem we calculate

$$h_E = h(j_E) = \log 128 \ , \ \frac{3\pi\omega^2}{D|\omega_1|^2\Im\tau} = 6\pi\frac{\Omega_1}{|\Omega_2|} = A_0 \ , \ A_1 = h_E \ , \ \mathcal{E} = e$$

$$c_4 = 2.9 \cdot 10^{18} \cdot 4^8 \cdot 3^{38.3} \cdot 134.37266 = 4.7966 \times 10^{43} \ ,$$

$$c_5 = 1 \ , \ c_6 = 1 + h_E \ , \ c_7 = 1.8494 \ , \ c_8 = 6.252312 \ .$$

Relation (47) implies $M < 3.8 \times 10^{24}$

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

First reduction $M \leq 17$,second reduction $M \leq 6$.
*The only integers satisfying (57) 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 $\omega$ is the fundamental real period of the Weierstrass $\wp$ function associated with the eliptic curve

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

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 $\Pi_i$'s are the basic points $R_1, \ldots, R_r$ and,probably $P_0$ 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 $\omega_1, \omega_2$ 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,then we can take

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

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

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

where

$$\Omega_1 = \frac{\pi}{M\left(\sqrt[4]{3e_1^2+A}, \frac{1}{2}\sqrt{3e_1+2\sqrt{3e_1^2+A}}\right)}\ ,$$

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

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

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

From $\omega_1,\omega_2$ we can also easily find the least real period $\omega$.

We define now the *height* of a rational $n$-tuple. Let,in general, $(a_1/b_1,\ldots,a_n/b_n)$ , $n\geq 1$ 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

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

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

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

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

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

$$A_0\geq\max\left\{h_E\ ,\ \frac{3\pi|\omega|^2}{D|\omega_1|^2\Im\tau}\right\}\ ,\ A_i\geq\max\left\{h_E\ ,\ \frac{3\pi|\omega|^2\phi(\Pi_i)^2}{D|\omega_1|^2\Im\tau}\ ,\ \hat{h}(\Pi_i)\right\}\ i=1,\ldots,k$$

and

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

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

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

*or*

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

*where*

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

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

# 8 Appendix 2

In this Appendix we compute explicit values of the parameter $u_0$, which appear in Proposition 2.4. Recall that $u_0$ is a positive number such that,for $u > u_0$,we have $Q(u) > 0$ , $sgn(\mathcal{R}(u)) = \sigma$ , and the open interval with endpoints $\mathcal{F}^*(u)$ and $2e\sqrt{a}$ does not contain neither of the two numbers $-2e\sqrt{a}$ and $(d^2 - 4e^2c)/(4e^2)$. We compute first such a number $u_0$.

**Lemma 8.1.** *Let $u_1$ be the greatest positive root of the polynomial $Q$ (if such a root exists; otherwise, $u_1 = 0$ ). If $d\sqrt{a} = be$,then $\mathcal{F}^*(u) > -2e\sqrt{a}$ for every $u > u_1$. If $d\sqrt{a} \neq be$,then $\mathcal{F}^*(u) > -2e\sqrt{a}$ for every $u > \max(u_1,(d^2 + 8e^3\sqrt{a} - 4e^2c)/(4be^2 - 4de\sqrt{a}))$.*

Proof. Consider the function $\mathcal{H}(u) = \mathcal{F}^*(u) + 2e\sqrt{a}$ defined in the interval $(u_1, +\infty)$. The fact that $\lim_{u\to+\infty}\mathcal{H}(u) = 4e\sqrt{a} > 0$ implies that,if in the interval $(u_1, +\infty)$ this function does not have a root,then,in this interval it assumes only positive values,while,if it has roots,then $\mathcal{H}(u) > 0$ for every $u$ exceeding the largest of them. On the other hand,any root $u$ of H must,in view of the definition of H and $\mathcal{F}^*$, satisfy

$$4e^2Q(u) = (2e\sqrt{a}u^2 + du + 2e^2)^2\ ,$$

from which

$$4e(d\sqrt{a} - be)u + d^2 + 8e^3\sqrt{a} - 4e^2c = 0\ .$$

If $d\sqrt{a} = be$,then $d^2 + 8e^3\sqrt{a} - 4e^2c \neq 0$ (the proof is completely analogous to that of Lemma 2.1(i)),hence H has no root in $(u_1, +\infty)$. If $d\sqrt{a} \neq be$,then the only possible root of H is $(d^2 + 8e^3\sqrt{a} - 4e^2c)/(4be^2 - 4de\sqrt{a})$. □

**Lemma 8.2.** *Let $u_1$ be as in Lemma 8.1 and let $u_2$ be equal to the largest real root of the polynomial*

$$(ad^2 - b^2e^2)t^3 + (bd^2 + 8e^2ad - 4e^2bc)t^2 + (cd^2 + 2e^2bd + 16e^4a - 4c^2e^2)t + (d^3 + 8e^4b - 4e^2cd)\ ,$$

*(if such a root exists;otherwise $u_2 = 0$).Then,$sgn(\mathcal{R}(U)) = \sigma$ for every $U > \max(u_1, u_2)$.*

Proof. For $u > u_1$ ,$\mathcal{R}(u)$ is a real-valued function and for all sufficiently large $u$, $\sigma\mathcal{R}(u) > 0$ (by Lemma 2.1(ii)). This means that,if R does not vanish in the interval $(u_1, +\infty)$ then,in this interval,$\sigma\mathcal{R}$ assumes only positive values ; if,on the other hand, R has zeros in $(u_1, +\infty)$, then $\sigma\mathcal{R}(u) > 0$ for every $u$ greater than the largest of these zeros. Now,by the definition of R we easily deduce that $\mathcal{R}(u) = 0$ implies $(4e^2 + du)^2Q(u) = (beu^3 + 2ceu^2 + 3deu + 4e^3)^2$ and after some easy calculations, we see that $u$ must be a root of the cubic polynomial appearing in the announcement. □

**Lemma 8.3.** *Let $u_1$ be as in Lemma 8.1. i) If $(d^2-4e^2c)/(4e^2) > 2e\sqrt{a}$,then $64e^6a-(4e^2c-d^2)^2 \neq 0$ and*

$$\mathcal{F}^*(u) < \frac{d^2-4e^2c}{4e^2} \qquad \forall u > \max\left(\frac{8e^2(4e^2cd-d^3-8e^4b)}{64e^6a-(4e^2c-d^2)^2}\,,\,u_1\right)\,.$$

*ii) Let $(d^2-4e^2c)/(4e^2) < 2e\sqrt{a}$. If $64e^6a-(4e^2c-d^2)^2 \neq 0$, then*

$$\mathcal{F}^*(u) > \frac{d^2-4e^2c}{4e^2} \qquad \forall u > \max\left(\frac{8e^2(4e^2cd-d^3-8e^4b)}{64e^6a-(4e^2c-d^2)^2}\,,\,u_1\right)\,,$$

*while,if $64e^6a-(4e^2c-d^2)^2=0$,then $\mathcal{F}^*(u) > (d^2-4e^2c)/(4e^2)\ \ \forall u > u_1$.*

Proof. (i) Let $(d^2-4e^2c)/(4e^2) > 2e\sqrt{a}$ ,so that

$$8e^3\sqrt{a}+4e^2c-d^2 < 0\,. \tag{58}$$

If $64e^6a-(4e^2c-d^2)^2=0$,then,in view of (58), $8e^3\sqrt{a}-4e^2c+d^2=0$ ; if we add this to relation (58) we get $16e^3\sqrt{a}<0$ ,a contradiction. Now we consider the function $\mathcal{H}(u)=\mathcal{F}^*(u)-(d^2-4e^2c)/(4e^2)$ , $u\in(u_1,+\infty)$. We observe that $\lim_{u\to+\infty}\mathcal{H}(u)=2e\sqrt{a}+(4e^2c-d^2)/(4e^2)<0$, in view of (58); therefore,if in the interval $(u_1,+\infty)$ the function H has no zero,then,in this interval it assumes only negative values, while if it has zeros,then,for every $u>u_1$,greater than the largest of these roots, $\mathcal{H}(u)<0$. On the other hand,if $u$ is a zero of H,then

$$(8e^3\sqrt{Q(u)})^2 = ((4e^2c-d^2)u^2+4e^2du+8e^4)^2\,,$$

which,after some easy computations becomes

$$\left(64e^6a-(4e^2c-d^2)^2\right)\,u = 8e^2(4e^2cd-d^3-8e^4b)\,, \tag{59}$$

and now our assertion is clear.

(ii) Let now $(d^2-4e^2c)/(4e^2) < 2e\sqrt{a}$,so that

$$8e^3\sqrt{a}+4e^2c-d^2 > 0\,. \tag{60}$$

We consider the same function H defined as in (i),for which we have now $\lim_{u\to+\infty}\mathcal{H}(u)>0$. As in (i),either H has no zero in the interval $(u_1,+\infty)$,in which case H assumes only positive values, or it has,in which case $\mathcal{H}(u)>0$,for every $u>u_1$,greater than the largest of these zeros. Searching for the possible zeros $u$ of the function H,we are led,as in case (i),to (59) and if the coefficient of $u$ is non-zero our assertion is clear;if it is zero,then,in view of (60),we conclude that $8e^3\sqrt{a}-4e^2c+d^2=0$ and also that the right-hand side of (59) is non-zero (otherwise $b=(4e^2cd-d^3)/(8e^4)=d\sqrt{a}/e$ and $c=(8e^3\sqrt{a}+d^2)/(4e^2)$ so that $Q$ would be a square),which means that, in such a case,H has no root at all. □

Now we prove the main result of this Appendix.

**Proposition 8.4.** *Let $u_1,u_2$ be as in Lemma 8.2 and define*

$$u_3 = \begin{cases} \max\left(\dfrac{d^2+8e^3\sqrt{a}-4e^2c}{4e(be-d\sqrt{a})}\,,\,u_1\right) & \text{if } be\neq d\sqrt{a} \\ u_1 & \text{otherwise} \end{cases}$$

$$u_4 = \begin{cases} \max\left(\dfrac{8e^2(4e^2cd - d^3 - 8e^4b)}{64e^6a - (4e^2c - d^2)^2}\,,\, u_1\right) & \textit{if } 64e^6a - (4e^2c-d^2)^2 \neq 0 \\ u_1 & \textit{otherwise} \end{cases}$$

*Finally,choose a positive number*

$$u_0 \geq \begin{cases} \max(u_2,u_4) & if \;\; \sigma = 1 \\ \max(u_2,u_3,u_4) & if \;\; \sigma = -1 \end{cases} .$$

*Then,for every $U > u_0$,we have $Q(U) > 0$, $sgn(\mathcal{R}(U)) = \sigma$ and the interval $I(\mathcal{F}^*(u), 2e\sqrt{a})$ does not contain any of the two numbers $-2e\sqrt{a}$ and $(d^2 - 4e^2c)/(4e^2)$; hence,the parameter $u_0$ appearing in Proposition 2.4 can be taken as above.*

Proof. Let $\sigma = +1$. By $U > u_1, u_2$ and the definition of $u_1$ and $u_2$ it follows that $Q(U) > 0$ and,in view of Lemma 8.2, $sgn(\mathcal{R}(U)) = \sigma$. Then,in view of (11),in the interval $(\max(u_1,u_2), +\infty)$, $\mathcal{F}^*$ is strictly decreasing with $\lim_{u\to+\infty}\mathcal{F}^*(u) = 2e\sqrt{a}$ (cf.the comment and the figure following Lemma 2.2). It follows that $\mathcal{F}^*(U) > 2e\sqrt{a}$ and $I(\mathcal{F}^*(U), 2e\sqrt{a})$ is the interval $(2e\sqrt{a}, \mathcal{F}^*(U))$, which,of course,does not include $-2e\sqrt{a}$. Next we check $(d^2 - 4e^2c)/(4e^2)$. If it is $\leq 2e\sqrt{a}$ then,of course,it does not belong to the above interval. If it is greater than $2e\sqrt{a}$ then,by Lemma 8.3(i) and the assumption $U > u_4$, $\mathcal{F}^*(U) < (d^2 - 4e^2c)/(4e^2)$; hence in any case, $(d^2 - 4e^2c)/(4e^2) \notin I(\mathcal{F}^*(U), 2e\sqrt{a})$.

Let $\sigma = -1$. From $U > u_1, u_2$ and Lemma 8.2,it follows that $Q(U) > 0$ and $\mathcal{R}(U) < 0$. Now,in view of (11), $\mathcal{F}^*$ is stictly increasing in the interval $(\max(u_1,u_2), +\infty)$ with $\lim_{u\to+\infty}\mathcal{F}^*(u) = 2e\sqrt{a}$. We conclude that $\mathcal{F}^*(U) < 2e\sqrt{a}$,so that $I(\mathcal{F}^*(U), 2e\sqrt{a})$, is the interval $(\mathcal{F}^*(U), 2e\sqrt{a})$. On the other hand,in view of $U > u_3$ and Lemma 8.1, $-2e\sqrt{a} < \mathcal{F}^*(U)$; hence $-2e\sqrt{a} \notin (\mathcal{F}^*(U), 2e\sqrt{a})$. Finally,we check $(d^2 - 4e^2c)/(4e^2)$. If it is $\geq 2e\sqrt{a}$ then,trivially,it does not belong to the above interval. If it is less than $2e\sqrt{a}$,then,since $U > u_4$ and Lemma 8.3(ii),it must be less than $\mathcal{F}^*(U)$ and thus,in any case, $(d^2 - 4e^2c)/(4e^2) \notin I(\mathcal{F}^*(U), 2e\sqrt{a})$. □

# 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, *Soc.Math.France, Mémoire 62 (Suppl. Bull. S.M.F.)*, **123** (1995), fasc.3, 143 pp.

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

[G] R.K. Guy,"Reviews in Number Theory 1973-83", Vol. 2A, *American Math. Soc.*, Providence - Rhode Island,1984.

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

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

[L1] W. Ljunggren, Einige Sätze über unberstimmte Gleichungen von der Form $Ax^4+Bx^2+C=Dy^2$, *Vid.-Akad. Skrifter I* No **9**,53 p.p. (1942).

[L2] ———, Zur Theorie der Gleichung $X^2+1=DY^4$, *Avh. Norske, Vid. Akad. Oslo 1* No **5**, 27 p.p. (1942).

[L3] ———, Proof of a theorem of de Jonquieres (Norwegian), *Norsk. mat. tidsskrift* **26** (1944),3-8.

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

[S2] J.H. Silverman, Computing Heights on Elliptic Curves,*Math. Computation* **51** (1988), 339-358

[S3] J.H. Silverman, The difference between the Weil height and the canonical height on elliptic curves, *Math. Computation* **55** (1990), 723-743.

[Str] R.J. Stroeker, On the sum of consecutive cubes being a perfect square, *Report 9457/B*, Erasmus Univ. Rotterdam, 1994.

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

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

[SW] R.J. Stroeker and B.M.M. de Weger, On a quartic Diophantine equation, *Report 9371/B*, Erasmus Univ. Rotterdam, 1993.

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

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

[V] W.J. LeVeque,"Reviews in Number Theory 1940-72", Vol. 2, *American Math. Soc.*, Providence - Rhode Island,1974.

[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. Computation* **48** (1987), 425-436.