Computing all integer solutions of a genus 1 equation

R.J. Stroeker* N. Tzanakis†

Abstract

The Elliptic Logarithm Method has been applied with great success to the problem of computing all integer solutions of equations of degree 3 and 4 defining elliptic curves. We extend this method to include any equation $f(u, v) = 0$, where $f \in \mathbb{Z}[u, v]$ is irreducible over $\overline{\mathbb{Q}}$, defines a curve of genus 1, but is otherwise of arbitrary shape and degree. We give a detailed description of the general features of our approach, and conclude with two rather unusual examples corresponding to equations of degree 5 and degree 9.

1991 *Mathematics subject classification:* 11D41, 11G05
Key words and phrases: diophantine equation, elliptic curve, elliptic logarithm

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

†Department of Mathematics, University of Crete, Iraklion, Greece; e-mail: tzanakis@math.uch.gr; homepage: http://www.math.uoc.gr/~tzanakis

1 Introduction

In this paper we discuss a general method for solving equations defining plane curves of genus 1 in rational integers. This method generalizes the so-called Elliptic Logarithm Method—$\mathfrak{Ellog}$ for short—which, as a practical routine ('getting one's hands dirty', so to speak) for solving Weierstrass equations, was first described and applied by Stroeker and Tzanakis [16] and, independently, by Gebel, Pethő and Zimmer [8]. Since then, it has been applied by a number of authors to a variety of elliptic equations of degree 3 or 4; see [15], [21], [3], [9], [19], [20], [17]. In particular, a general treatment of the cubic elliptic equation can be found in [20].

Now that many elliptic equations of standard types have been successfully solved by application of $\mathfrak{Ellog}$, it seems natural to ask whether we can extend this method to arbitrary equations defining a genus 1 plane curve. To be more precise, the problem we wish to deal with in this paper is to develop a general practical method for solving explicitly the diophantine equation in rational integers u, v

$$f(u, v) = 0,$$

where $f \in \mathbb{Z}[u, v]$ is irreducible over $\overline{\mathbb{Q}}$ and $f = 0$ defines a curve $\mathcal{C}$ of genus 1.
This equation has at most finitely many solutions in integers, which can be effectively computed; see for instance [1] and [13]. However, the explicit computation of all such is quite a different matter and to this we shall direct our efforts. What is new in this paper is a general procedure, in the framework of $\mathfrak{Ellog}$, for obtaining, starting from an elliptic equation of arbitrary shape, an explicit linear form in elliptic logarithms and an upper bound for it. This is a non-standard task because it depends non-trivially on the particular shape of the initial equation $f(u, v) = 0$. After this stage the process of obtaining explicitly all integer solutions may be considered standard at the present state of affairs.

In Section 2 we give a full description of this generalization of $\mathfrak{Ellog}$, and in Section 3 we present two rather unusual curves of total degree 5 and 9 respectively. They serve the purpose of illustrating essential points in the description of our method.

In **Notes**, right at the end of this paper, we have collected some relevant facts that are considered standard but may be difficult to locate in the literature.

A preliminary, incomplete version of this paper found its way into the Proceedings of Ants-iv [18].

2 Description of $\mathfrak{Ellog}$

In this section we shall give a detailed description of $\mathfrak{Ellog}$ in its most general form. We shall reserve the letter n for $\deg_v f$. If $\mathcal{C}(\mathbb{R})$ is a bounded subset of $\mathbb{R}^2$, then, solving this equation in integers should be a trivial task. We therefore consider only such polynomials f for which $\mathcal{C}(\mathbb{R})$ is unbounded. Then, without loss of generality, we may assume that there are real solutions (u, v) with $|u|$ arbitrary large.

2.1 The birational transformation

The curve $\mathcal{C}$ is birationally equivalent over a number field $\mathbb{K}$ to

$$\mathcal{E} : y^2 = q(x) = x^3 + Ax + B, \tag{1}$$

where the degree of $\mathbb{K}$ is at most $\min\{\deg_u f, \deg_v f = n\}$. A proof can be found in [13, Proposition 1]. Moreover, for our method to work we need $\mathbb{K}$ to be real. Fortunately this can always be guaranteed as we shall see shortly. Because $\mathcal{C}(\mathbb{R})$ is non-empty, an assumption we made above, we can choose a non-singular point $(u_0, v_0) \in \mathcal{C}(\mathbb{R} \cap \overline{\mathbb{Q}})$ and put $\mathbb{K} = \mathbb{Q}(u_0, v_0)$. The function field $\mathbb{K}(\mathcal{C})$ is of genus 1 and admits a place of degree 1, namely, the one corresponding to the point (u_0, v_0). By [4, Chapter II, § 3] this function field is generated over $\mathbb{K}$ by two functions $\mathbf{x}, \mathbf{y} \in \mathbb{K}(\mathcal{C})$ related by a Weierstrass equation (1), where $\mathbf{x}$ takes the place of x and $\mathbf{y}$ that of y. This shows that $\mathbb{K}(\mathcal{C})$ can be both expressed as the quotient field $\mathbb{K}[u, v]/\langle f \rangle$ and as the quotient field $\mathbb{K}[x, y]/\langle q \rangle$, which is precisely what we require. Note that this argument also shows that $[\mathbb{K} : \mathbb{Q}] \leq \min\{\deg_u f, \deg_v f = n\}$.

Alternatively, by [13, § 6], a field $\mathbb{K}$ as above can be obtained by adjoining to $\mathbb{Q}$ the coefficients of any Puiseux series at infinity of the algebraic function implicitly defined by $f(u, v) = 0$. Given the existence of points $(u, v) \in \mathcal{C}(\mathbb{R})$ with $|u|$ arbitrarily large, Lemma 2.2.1 below implies the existence of such Puiseux series and ensures that $\mathbb{K}$ is real. A practical algorithm for computing the Weierstrass model (1) and the birational transformation between $\mathcal{C}$ and $\mathcal{E}$ is described in [12]; an implementation of this algorithm is included in the package `algcurves` of recent releases of the computer algebra system Maple. It is worth noticing that this algorithm, when given a non-singular point $(u_0, v_0) \in \mathcal{C}(\overline{\mathbb{Q}})$ and the coefficients of f as input, produces an output (that is to say the coefficients A, B of (1) and the coefficients of the isomorphism $\mathcal{C} \to \mathcal{E}$ and its inverse) belonging to $\mathbb{Q}(u_0, v_0)$. Although this is not very explicit in [12], it can be verified by careful scrutiny of [10, §§ 1 and 2.1] and [11, §§ 1-3.1] on which the algorithm of [12] is based.

The inclusion $A, B \in \mathbb{K}$ can be further improved to $A, B \in \mathbb{Q}$: by an argument found on pages 93–95 of [6], a simple transformation $(x, y) \mapsto (t^2 x, t^3 y)$ for a conveniently chosen $t \in \overline{\mathbb{Q}}$ maps equation (1) to an equivalent Weierstrass equation with coefficients in $\mathbb{Q}$. Therefore, we have established the following

Fact 1. *The curve $\mathcal{C}$ is birationally equivalent over $\overline{\mathbb{Q}}$ to a Weierstrass equation* (1) *with $A, B \in \mathbb{Q}$ by means of a birational transformation*

$$\begin{aligned} u &= \mathcal{U}(x, y), \quad & v &= \mathcal{V}(x, y) \\ x &= \mathcal{X}(u, v), \quad & y &= \mathcal{Y}(u, v) \end{aligned} \tag{2}$$

whose coefficients are real algebraic numbers of degree at most $\min\{\deg_u f, \deg_v f = n\}$. *These coefficients, as well as A and B, can be explicitly computed.*

Throughout this paper we shall adopt the following convention and notation. In our terminology, 'a point P of the curve' is a point with coordinates $(u(P), v(P))$ on $\mathcal{C}$

satisfying $f(u(P), v(P)) = 0$, or, as the case may be, a point with coordinates $(x(P), y(P))$ on $\mathcal{E}$ satisfying (1). Then, according to Fact 1,

$$u(P) = \mathcal{U}(x(P), y(P)), \quad v(P) = \mathcal{V}(x(P), y(P))$$
$$x(P) = \mathcal{X}(u(P), v(P)), \quad y(P) = \mathcal{Y}(u(P), v(P)).$$

Remark. A rational integer solution of $f(u, v) = 0$ corresponds to a point P with $u(P), v(P) \in \mathbb{Z}$. Although $\mathcal{E}$ is defined over $\mathbb{Q}$ by (1), the field $\mathbb{K}$ not necessarily coincides with $\mathbb{Q}$. Now $x(P), y(P) \in \mathbb{K}$, and so we need to consider $\mathcal{E}$ over $\mathbb{K}$. According to Section 2.5 it will be necessary to compute a Mordell-Weil basis for $\mathcal{E}(\mathbb{K})$, which may turn out to be tricky in case $\mathbb{K} \neq \mathbb{Q}$. Such complications can be avoided if we happen to know a non-singular point in $\mathcal{C}(\mathbb{Q})$.

2.2 Puiseux series

The complex solutions (u, v), implicitly given by $f(u, v) = 0$, can be made explicit 'near infinity' by means of Puiseux series. We gather the details in the following

Fact 2. (a) *There is a finite Galois extension $\mathbb{L}/\mathbb{Q}$, which we view as a subfield of $\mathbb{C}$, and n distinct formal power series* (Puiseux expansions at infinity)

$$v_i(u) = \sum_{k=\mu_i}^{\infty} \alpha_{k,i} u^{-k/\nu_i}, \quad \text{with } \alpha_{\mu_i,i} \neq 0 \ (i = 1, \ldots, n), \tag{3}$$

where for each i, $\nu_i, \mu_i \in \mathbb{Z}$, $\nu_i \geq 1$, all $\alpha_{k,i}$'s belong to $\mathbb{L}$, the formal identity $f(u, v_i(u)) = 0$ holds, and ν_i is minimal subject to the restriction that no proper divisor of ν_i divides all $k \geq \mu_i$ with $\alpha_{k,i} \neq 0$.

(b) *Any formal power series $v(u)$ satisfying the formal identity $f(u, v(u)) = 0$ and having properties analogous to those of the series* (3)*, even without the requirement that the coefficients of $v(u)$ be algebraic, necessarily coincides with one of the above n series.*

(c) *The formal identity*

$$f(u, v) = p_0(u) \prod_{i=1}^{n} (v - v_i(u))$$

holds, where $p_0(u)$ is the coefficient of v^n in $f(u, v)$.

(d) *Each series* (3) *converges for u in the range $|u| > M$, where M is the maximum modulus of the roots of the polynomial* $\mathrm{res}_v(f, \frac{\partial f}{\partial v}) \in \mathbb{Z}[u]$.

(e) *For each i the function $t \mapsto v_i(t^{-\nu_i}) = \sum_{k=\mu_i}^{\infty} \alpha_{k,i} t^k$ is analytic and one-to-one in the punctured disk with center at the origin and radius M^{-1/ν_i}.*

Most of these facts are considered standard, but detailed references are not always easy to find. In the **Notes**[1] section at the end of this paper we have collected as much information as we have been able to trace. The reader may find it useful; we certainly did.

In **Notes**[2] an algorithm is presented that determines the finite extension of $\mathbb{Q}$ generated by the infinitely many $\alpha_{k,i}$'s, once the integers ν_i and μ_i have been computed (e.g. by the first few steps in the construction of a Newton polygon).

The following lemma shows how to obtain points (u, v) belonging to $\mathcal{C}(\mathbb{R})$ with arbitrary large u.

Lemma 2.2.1. *Let $f(u_0, v_0) = 0$ with $u_0, v_0 \in \mathbb{R}$ and $u_0 > M$. There is exactly one series $v_i(u)$ of (3) with all its coefficients $\alpha_{k,i}$ $(k = \mu_i, \mu_{i+1}, \ldots)$ in $\mathbb{R}$ such that, if we give u^{-1/ν_i} its usual interpretation of the real ν_i-th root of $1/u$, then $v_0 = v_i(u_0)$.*

Proof. By statement (c) of Fact 2, $0 = f(u_0, v_0) = p_0(u_0) \prod_{s=1}^{n}(v_0 - v_s(u_0))$. Further, by remark (iii) of **Notes**[1], $p_0(u_0) \neq 0$, hence $v_i(u_0) = v_0$ for some series $v_i(u)$. This series has only real coefficients $\alpha_{k,i}$ $(k = \mu_i, \mu_{i+1}, \ldots)$. Indeed, assume the contrary and denote by σ_0 the element of $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ obtained by restricting the complex conjugation automorphism of $\mathbb{C}$ to $\mathbb{L}$. Then, by remark (v) of **Notes**[1], $v_i(u, 0, \sigma_0)$ coincides with a series $v_j(u)$, the coefficients of which are the complex conjugates of the corresponding coefficients of $v_i(u)$, and hence $v_j(u)$ is distinct from $v_i(u)$. Then, $v_j(u_0) = \overline{v_i(u_0)} = \overline{v_0} = v_0$, so that $f(u_0, v) = p_0(u_0) \prod_{s=1}^{n}(v - v_s(u_0)) \in \mathbb{Z}[v]$ is a non-zero polynomial divisible by $(v - v_i(u_0))(v - v_j(u_0)) = (v - v_0)^2$, which is impossible by remark (iii) of **Notes**[1]. This shows that all coefficients of $v_i(u)$ are real.
Finally, if $v_l(u_0) = v_0$ were true for some l distinct from i, an argument analogous to that just given would show the polynomial $f(u_0, v) \in \mathbb{Z}[v]$ to be divisible by $(v - v_0)^2$, which again is impossible. □

2.3 A limiting value for $\mathcal{X}$

Our intention of giving a full description of the $\mathfrak{Ellog}$ way of solving $f(u, v) = 0$ in integers u and v is clearly not hampered by the restriction $u > 0$. As the computation of all such solutions (or 'integral points' of $\mathcal{C}$) with $0 \leq u \leq M$ is rather straightforward, it suffices to consider only those points $P \in \mathcal{C}(\mathbb{R})$ with $u(P) > M$. By Lemma 2.2.1, for any such point P, there is a subscript $i \in \{1, \ldots, n\}$, such that the series $v_i(u)$ of (3) has only real coefficients and $v(P) = v_i(u(P))$. Therefore, the problem we need to solve is essentially this:

> For any (fixed) series $v_i(u)$ of (3) having all its coefficients in $\mathbb{R}$, find all points $P \in \mathcal{C}(\mathbb{R})$ such that $u(P)$ is a rational integer $> M$ and $v_i(u(P))$ is a rational integer too.

In view of this, from now on and until the end of the paper the following will always be tacitly understood:

- The subscript i belongs to $\{1, \ldots, n\}$ and $v_i(u)$ is as in (3) with all its coefficients belonging to $\mathbb{R}$.
- For the generic point P under consideration, $(u(P), v(P)) \in \mathcal{C}(\mathbb{R})$, $u(P) > M$ and $v(P) = v_i(u(P))$.
- The meaning of u^{-k/ν_i} is the usual one (see Lemma 2.2.1).

Proposition 2.3.1. *The expression $\mathcal{X}(u, v_i(u))$ always has a limiting value for $u \to \infty$, including $\pm\infty$. Notation: $x_{0i} = \lim_{u\to\infty} \mathcal{X}(u, v_i(u))$. If finite, x_{0i} is a real algebraic number that can be explicitly computed.*

Proof. First note that $f(u, v)$ cannot be a factor of either the numerator or the denominator of the rational function $\mathcal{X}(u, v)$. For, otherwise, the curve $\mathcal{C}$ could be injectively mapped into a straight line, which is impossible for a curve of genus 1.
Next, put $u = t^{-\nu_i}$ with $t \in \mathbb{R}$ and $0 < t < M^{-1/\nu_i}$. In view of Facts 1 and 2, it is easy to see that $\mathcal{X}(u, v_i(u))$ takes the form

$$\frac{\beta t^{\lambda} + \beta' t^{\lambda'} + \beta'' t^{\lambda''} + \ldots}{\gamma t^{\rho} + \gamma' t^{\rho'} + \gamma'' t^{\rho''} + \ldots},$$

for certain non-zero real algebraic numbers $\beta, \beta', \beta'', \ldots, \gamma, \gamma', \gamma'', \ldots$ and rational integers $\lambda < \lambda' < \lambda'' < \ldots$ and $\rho < \rho' < \rho'' < \ldots$. This shows that

$$x_{0i} = \lim_{u\to\infty} \mathcal{X}(u, v_i(u)) = \begin{cases} \beta/\gamma & \text{if } \lambda = \rho, \\ 0 & \text{if } \lambda > \rho, \\ \operatorname{sgn}(\beta/\gamma)\infty & \text{if } \lambda < \rho. \end{cases}$$

By Facts 1 and 2, β and γ can be explicitly computed, hence the same is true for x_{0i}.

□

Definition 2.3.2. *In case x_{0i} is finite we denote by $Q_{0i} \in \mathcal{E}(\overline{\mathbb{Q}} \cap \mathbb{R})$ the point with x-coordinate x_{0i} and non-negative y-coordinate. In case $x_{0i} = \pm\infty$ we set $Q_{0i} = \mathcal{O}$, the group identity of $\mathcal{E}(\overline{\mathbb{Q}})$.*

2.4 The elliptic integrals

In this section we are concerned with the precise connection between the elliptic integrals corresponding to the two models of our curve of genus 1, that is to say, the original $f(u, v) = 0$ on the one hand, and the Weierstrass equation (1) on the other. It is not difficult to see that

$$\frac{\mathrm{d}x}{y} = G(u, v) \frac{\mathrm{d}u}{f_v(u, v)}\ , \tag{4}$$

where

$$G(u, v) = 2\ \frac{\mathcal{Y}_u(u, v) \cdot f_v(u, v) - \mathcal{Y}_v(u, v) \cdot f_u(u, v)}{3\mathcal{X}^2(u, v) + A}\ .$$

In case $f(u,v) = 0$ is a Weierstrass equation, a quartic equation of type $v^2 = Q(u)$ for some quartic polynomial Q, or a general cubic elliptic equation, $G(u,v)$ is constant with value 2; see [16], [21] and [20].
Now put

$$g_i(u) = G(u, v_i(u)), \quad x_i(u) = \mathcal{X}(u, v_i(u)), \quad y_i(u) = \mathcal{Y}(u, v_i(u)). \tag{5}$$

Obviously, $x_i(u)$ and $y_i(u)$ are continuous real functions of the real argument $u > M$, and satisfy $y_i(u)^2 = x_i(u)^3 + Ax_i(u) + B$. Hence

$$y_i(u) = \varepsilon\sqrt{q(x_i(u))}, \text{ with } \varepsilon \in \{-1, 1\},$$

and consequently

$$\frac{\mathrm{d}x}{y} = \frac{\mathrm{d}x}{\varepsilon\sqrt{q(x)}}\,. \tag{6}$$

Then, by relations (4) and (6), we get

$$\int_{u(P)}^{\infty} \frac{g_i(u)\,\mathrm{d}u}{f_v(u, v_i(u))} = \int_{x(P)}^{x_{0i}} \frac{\mathrm{d}x}{\varepsilon\sqrt{q(x)}}\,, \tag{7}$$

under the assumption that $u(P) \geq M$ is sufficiently large[4]. Indeed, recall the assumption $v(P) = v_i(u(P))$, which we made at the beginning of Section 2.3. By the relations given at the end of Section 2.1 and (5), $x(P) = \mathcal{X}(u(P), v(P)) = \mathcal{X}(u(P), v_i(u(P))) = x_i(u(P))$. Now (7) follows by Proposition 2.3.1, and relations (4) and (6). Observe that for $u(P)$ large enough (see **Notes**[3] at the end of the paper), the open integration intervals of both integrals are in one-to-one correspondence for the birational map (see Fact 1).

We shall now estimate the integrand in the left-hand side of (7). For $\mathfrak{Ellog}$ to work, it is essential that the corresponding integral tends to zero as $u(P)$ tends to ∞.

Proposition 2.4.1.

$$\frac{g_i(u)}{f_v(u, v_i(u))} = O(u^{-1-\delta}) \quad (u \to \infty), \tag{8}$$

where $\delta \geq \nu_i^{-1}$.

Proof. By a classical result the integral associated with the differential in the left-hand side of (4) is an elliptic integral of the first kind, and by implication, so is the corresponding integral of the right-hand side of (4). This means[5] that for any parametrization $(u, v) = (u(t), v(t))$ of $f(u, v) = 0$, the t-expansion of $\dfrac{G(u(t), v(t))}{f_v(u(t), v(t))} \cdot \dfrac{\mathrm{d}u}{\mathrm{d}t}$ contains no negative t-powers. Using this fact in the parametrization

$$u(t) = t^{-\nu_i}, \quad v(t) = v_i(t^{-\nu_i}) = \sum_{k=\mu_i}^{\infty} \alpha_{k,i} t^k,$$

[4]This can be made explicit; see **Notes**[3]
[5]See for example [2, § 24].

and taking into account that $\mathrm{d}u/\mathrm{d}t = -\nu_i t^{-\nu_i - 1}$, leads to the inequality

$$\mathrm{ord}_t \frac{G(t^{-\nu_i}, v_i(t^{-\nu_i}))}{f_v(t^{-\nu_i}, v_i(t^{-\nu_i}))} \geq \nu_i + 1.$$

Now on putting $t^{-\nu_i} = u$ in the relation above we conclude that

$$\mathrm{ord}_u \frac{g_i(u)}{f_v(u, v_i(u))} \leq -1 - \frac{1}{\nu_i}.$$

□

For example, if $f(u, v) = 0$ happens to be a Weierstrass equation to start with, no birational transformation is needed, and $\delta = \frac{1}{2}$, while in case of either a non-Weierstrass cubic equation or of a quartic equation of type $v^2 = Q(u)$ with quartic polynomial Q, it is easily shown that $\delta = 1$ (see [20] and [21], respectively). In both examples studied in Section 3 of this paper, $\delta = 1/\nu_i$.

2.5 Linear forms in elliptic logarithms

In this section we shall show that the integral in the right-hand side of (7) can be expressed as a linear form in elliptic logarithms of points in $\mathcal{E}(\overline{\mathbb{Q}})$, so that estimates for the integral automatically provide estimates for this linear form.

The group $\mathcal{E}(\mathbb{R})$, defined by $y^2 = q(x)$, has the identity component $\mathcal{E}_0(\mathbb{R})$ and in the real case—we remind the reader of the fact that in this case $q(x) = 0$ has three real roots $e_1 > e_2 > e_3$—also the bounded component $\mathcal{E}_1(\mathbb{R})$. Let $Q_j = (e_j, 0) \in \mathcal{E}(\overline{\mathbb{Q}})$ for $j = 1, 2, 3$. For any $R \in \mathcal{E}_1(\mathbb{R})$ we put $R' = R + Q_2 \in \mathcal{E}_0(\mathbb{R})$. We have the usual isomorphism

$$\phi : \mathcal{E}_0(\mathbb{R}) \longrightarrow [0, 1) = \mathbb{R}/\mathbb{Z}$$

(see [16]). In the complex case—that is when $q(x) = 0$ has a single real root—$\mathcal{E}_0(\mathbb{R}) = \mathcal{E}(\mathbb{R})$ and ϕ is defined on the whole of $\mathcal{E}(\mathbb{R})$. In the real case ϕ is extended to a two-to-one epimorphism $\tilde{\phi}$, defined by

$$\tilde{\phi}(R) = \begin{cases} \phi(R), & \text{if } R \in \mathcal{E}_0(\mathbb{R}) \\ \phi(R'), & \text{if } R \in \mathcal{E}_1(\mathbb{R}) \end{cases}.$$

Let $\omega = 2\displaystyle\int_{e_1}^{\infty} \frac{\mathrm{d}t}{\sqrt{q(t)}}$, the fundamental real period. A bit of thought suffices to convince one that

$$\omega \cdot \tilde{\phi}(R) = \begin{cases} \text{elliptic log of } R, & \text{if } R \in \mathcal{E}_0(\mathbb{R}) \\ \text{elliptic log of } R', & \text{if } R \in \mathcal{E}_1(\mathbb{R}) \end{cases} \tag{9}$$

We write

$$P = n_1 P_1 + \cdots + n_r P_r + T,$$

where $P_1, \ldots, P_r$ form a Mordell-Weil basis of $\mathcal{E}(\mathbb{K})$ [6] and T is one of the finitely many torsion points. It is easy to see that the $\tilde{\phi}(T)$ are rational numbers with effectively bounded denominators. Then both $\tilde{\phi}(P)$ and $\tilde{\phi}(-P)$ are of the form

$$m_1\tilde{\phi}(P_1) + \cdots + m_r\tilde{\phi}(P_r) + m_0 + \frac{s}{t}, \tag{10}$$

where r is the rank of $\mathcal{E}$ over $\mathbb{Q}$, $m_j = \pm n_j$ $(j = 1, \ldots, r)$, $m_0 \in \mathbb{Z}$ is effectively bounded in terms of $N = \max_{1\le j\le r} |n_j|$, and s, t are relatively prime integers, effectively bounded by a small number; for a more detailed exposition, see [16].

Reminding the reader of the definition of Q_{0i} and, in general, of our discussion in Section 2.3, we now distinguish two cases:

1. $\boxed{e_1 \le x_{0i}}$ If $u(P) > M$ is sufficiently large (which, in practice, can easily be made completely explicit), then $e_1 < x(P)$, and hence

$$\begin{aligned}\int_{x(P)}^{x_{0i}} \frac{\mathrm{d}x}{\sqrt{q(x)}} &= \int_{x(P)}^{\infty} \frac{\mathrm{d}x}{\sqrt{q(x)}} - \int_{x_{0i}}^{\infty} \frac{\mathrm{d}x}{\sqrt{q(x)}} \\ &= \omega\phi(\sigma P) - \omega\phi(Q_{0i}) = \omega\tilde{\phi}(\sigma P) - \omega\tilde{\phi}(Q_{0i}).\end{aligned}$$

   Here $\sigma = 1$ or -1, depending on whether $y(P)$ is non-negative or negative respectively. This, combined with (10) and (9) shows that the integral in the left-hand side of (7) is equal to the linear form in elliptic logarithms

$$-\omega\tilde{\phi}(Q_{0i}) + (m_0 + \frac{s}{t})\omega + m_1\omega\tilde{\phi}(P_1) + \cdots + m_r\omega\tilde{\phi}(P_r), \tag{11}$$

   and all points appearing in it have algebraic coordinates. We shall denote this linear form by $\mathcal{L}(P)$.

2. $\boxed{e_3 \le x_{0i} \le e_2}$ For $u(P) > M$ sufficiently large (again, this can be made completely explicit), $x(P) \in (e_3, e_2)$ and

$$\begin{aligned}\int_{x(P)}^{x_{0i}} \frac{\mathrm{d}x}{\sqrt{q(x)}} &= \int_{x(P)}^{e_2} \frac{\mathrm{d}x}{\sqrt{q(x)}} - \int_{x_{0i}}^{e_2} \frac{\mathrm{d}x}{\sqrt{q(x)}} = \int_{x(P')}^{\infty} \frac{\mathrm{d}x}{\sqrt{q(x)}} - \int_{x(Q'_{0i})}^{\infty} \frac{\mathrm{d}x}{\sqrt{q(x)}} \\ &= \omega\phi(\sigma P') - \omega\phi(Q'_{0i}) = \omega\tilde{\phi}(\sigma P) - \omega\tilde{\phi}(Q_{0i}),\end{aligned}$$

   by which we have arrived at the same linear form $\mathcal{L}(P)$ as before (11).

Remark. Occasionally it may happen that $\tilde{\phi}(Q_{0i})$ is a rational linear combination of $\tilde{\phi}(P_1), \ldots, \tilde{\phi}(P_r)$. For example, if $kQ_{0i} \in \mathcal{E}(\mathbb{Q})$ for some integer $k \ge 1$, then

$$kQ_{0i} = k_1P_1 + \cdots + k_rP_r + \text{torsion}$$

[6] Not of $\mathcal{E}(\mathbb{Q})$ in general; cf. Section 2.1 and the remark there.

for certain explicit, generally small integers $k_1, \dots, k_r$. Hence

$$\tilde{\phi}(Q_{0i}) = \frac{k_1}{k}\tilde{\phi}(P_1) + \cdots + \frac{k_r}{k}\tilde{\phi}(P_r) + \frac{k_0}{k} + \frac{s'}{t'},$$

where k_0/k and s'/t' have analogous roles to those of m_0 and s/t in (10). If such is the case, the term $\tilde{\phi}(Q_{0i})$ in $\mathcal{L}(P)$ disappears, and the coefficients of $\omega, \tilde{\phi}(P_1), \dots, \tilde{\phi}(P_r)$ change to fractions with explicit, generally small denominators. Thus, this case can be included in a more general situation in which the coefficients of $\omega, \tilde{\phi}(P_1), \dots, \tilde{\phi}(P_r)$ in $\mathcal{L}(P)$ are rational numbers with explicit small denominators, and numerators that are bounded by a large constant N_0, for which

$$N_0 \le \alpha N + \beta, \tag{12}$$

as is easily verified. Here α and β are small positive constants that can be explicitly computed in every particular case.

We showed above that the integral in the right-hand side of (7) equals the linear form $\mathcal{L}(P)$ in elliptic logarithms of points in $\mathcal{E}(\overline{\mathbb{Q}})$. It is quite straightforward to give an upper bound for $|\mathcal{L}(P)|$. Indeed, in view of Proposition 2.4.1, the integrand in the left-hand side of (7) is in absolute value at most $c_1 u^{-1-\delta}$ for an explicitly computable positive constant[7] c_1. Thus,

$$|\mathcal{L}(P)| \le c_1 \delta^{-1} |u(P)|^{-\delta}. \tag{13}$$

Next we need the following

Lemma 2.5.1. *Let $h(\cdot)$ denote the logarithmic height function. Then,*

$$h(x(P)) = h(\mathcal{X}(u(P), v(P))) \le c_2 + c_3 \log |u(P)| \tag{14}$$

for any point P with integer coordinates $u(P)$ and $v(P)$, where $u(P)$ is taken to be larger than a conveniently chosen explicit constant.

Proof. The proof we shall give below is not the most straightforward one we can give, but it is constructive, and it provides smaller values for the constants c_2 and c_3 than those implied by a theoretically simpler proof.

Assume that $u(P) \ge M$. Then, $v(P) = v_i(P)$ for some $i \in \{1, \dots, n\}$ (cf. Section 2.3). Consider first the usual case, in which $\mathcal{X}$ is a rational function of u and v with rational coefficients. Write $\mathcal{X} = F_1/F_2$ for some relatively prime polynomials with rational integer coefficients. For simplicity put $u(P) = u$ and $v(P) = v$, so that $h(\mathcal{X}(u(P), v(P)) \le \log \max\{|F_1(u,v)|, |F_2(u,v)|\} = \log |F_j(u,v)|$ for the proper choice of $j = 1, 2$. By (3), $|v| \le u^{-\mu_i/\nu_i}\gamma$, where γ is a small positive constant, provided u is sufficiently large[8]. Next, write $F_j(u,v) = \sum_{(k,l)} a_{k,l} u^k v^l$ and let c_3 be a positive integer not less than $\max_{(k,l)}\{k - l\mu_i/\nu_i\}$, where the maximum runs over all pairs (k,l) for which $a_{k,l} \ne 0$. Then, $|F_j(u,v)| \le C_2 u^{c_3}$, where $C_2 = \sum_{(k,l)} |a_{k,l}|\gamma^l$ and (14) holds with $c_2 = \log C_2$.

[7] The c_j's that appear in this paper denote explicitly computable constants that are positive, with the possible exception of c_7.

[8] Actually, γ is already very small for $u > 10$ or $u > 20$.

In the general case, we proceed as before, but now the coefficients of the polynomials F_1, F_2 are algebraic integers. Then, $h(x(P)) = h(F_1(u,v)/F_2(u,v)) \leq h(F_1(u,v)) + h(F_2(u,v))$. Let F be a polynomial in two variables, the coefficients of which are algebraic integers. Further, for rational integers u, v, write $F(u,v) = \sum_{(k,l)} a_{k,l} u^k v^l$. Then[9]

$$|F(u,v)| \leq \overline{|F(u,v)|} \leq \sum_{(k,l)} \overline{|a_{k,l}|} u^k |v|^l \leq C_2 u^{c_3} \ ,$$

where c_3 is as before and here $C_2 = \sum_{(k,l)} \overline{|a_{k,l}|} \gamma^l$. □

Finally we make use of the following relation between the Néron-Tate height and the logarithmic height (see e.g. [14][10]):

$$\hat{h}(P) - \tfrac{1}{2} h(x(P)) \leq c_4. \tag{15}$$

Recall that N is the maximum of absolute values of the coefficients n_j of P with respect to a given Mordell-Weil basis. It is well-known that $\hat{h}(P) \geq c_5 N^2$, where c_5 is the least eigenvalue of the height-pairing matrix corresponding to the chosen Mordell-Weil basis. This is a positive-definite form, hence c_5 is positive. Combining this with (13), (14) and (15), we obtain

$$|\mathcal{L}(P)| \leq \exp(-c_6 N^2 + c_7) \quad \text{with} \ \ c_6 = \frac{2c_5\delta}{c_3} \, , \, c_7 = \log c_1 - \log \delta + \frac{c_2 + 2c_4}{c_3}\delta \ . \tag{16}$$

The lower bound for $|\mathcal{L}(P)|$ is provided by S. David's Theorem [7], namely,

$$|\mathcal{L}(P)| > \exp(-c_8(\log N_0 + c_9)(\log\log N_0 + c_{10})^k) \ , \tag{17}$$

where N_0 is as in (12) and $k = r + 2$ if $\tilde{\phi}(Q_{0i})$ is a rational linear combination of $\tilde{\phi}(P_1), \ldots, \tilde{\phi}(P_r)$ [11] or $k = r + 3$, otherwise. Because of (12), the lower bound is expressed in terms of N. This lower bound is valid, provided N_0 is not less than a certain 'small' explicit constant. For a more detailed discussion of the constants appearing in the application of David's Theorem we refer the reader to the Appendix of [21]. Thus, either $N \leq c_{11}$, or both (16) and (17) hold—with $\alpha N + \beta$ in place of N_0—so that in combination they give an upper bound for N.

3 Examples

Now that the general outline of $\mathfrak{Ellog}$ has been discussed in sufficient detail, the reader may be curious to learn how the method behaves in practice, especially under the pressure of

[9] For an algebraic number α we write $\overline{|\alpha|}$ to denote the so-called house of α, i.e. the maximum absolute value of all its algebraic conjugates over $\mathbb{Q}$.

[10] cf. also [27] and [28]

[11] In particular, if $Q_{0i} = \mathcal{O}$.

non-standard, unusual data. Numerous examples have been given (see [3], [8], [9], [15], [16], [17], [19],[20], [21]) of the way $\mathfrak{Ell}\mathfrak{og}$ works on quite regular elliptic equations. In opposition to this, here we are interested in more provocative equations that accentuate the general applicability of the method. It turned out to be rather difficult to find matching examples in the literature. By accident we stumbled on a fifth degree curve of genus 1 that is used to illustrate the singularities command of the MAPLE package `algcurves`. We approached Mark van Hoeij, author of this MAPLE package, who suggested another curve of genus 1. The latter is given by an equation with small coefficients but of rather high degree. In our view, both curves are unusual and, at the same time, sufficiently natural to serve our purpose well enough. If the reader happens to know other such curves of genus 1, we would be grateful to learn about them.

In the two examples of our choice only the non-standard parts are worked out in detail. To justify this we repeat (see the Introduction) that new in this paper is the general procedure leading from the initial equation to the linear form in elliptic logarithms and the upper bound for it. It is mainly this stage that we wish to illustrate in our examples, the remainder of the computational process is standard[12], which is amply illustrated by an abundance of examples in the literature (see the beginning of the Introduction). We therefore decided to show in detail how we obtained the linear form in elliptic logarithms and its upper bound, but not to give our computations beyond this point.

3.1 A degree 5 example

The example of this section has already been presented in [18, section 6.3], where we used a somewhat different notation. Since it is an interesting example, very appropriate in illustrating our general method, we once again include it here, adapted to the choices of notation and overall description of the present paper.

We want to solve $f(u,v)=0$ in integers, where

$$\begin{aligned} f(u,v) = {} & 8v^5+35v^4+(128u-82)v^3+19v^2+(207u^4-621u^3+521u^2-135u+28)v \\ & -180u^5+450u^4-369u^3+100u^2+7u-8. \end{aligned}$$

The short Weierstrass model of this curve is

$$y^2 = x^3 - \frac{620582882786025 61}{805306368}x + \frac{6185299411685832648139 8145}{59373627899904}$$

and

$$\begin{aligned} \mathcal{X}(u,v) = {} & \tfrac{43681}{49152}(103981u^5+15228u^4v+10284u^3v^2+1536u^2v^3+4128uv^4-316526u^4 \\ & +47412u^3v+67584u^2v^2+15468uv^3-2592v^4+368606u^3-71388u^2v \\ & -88968uv^2-13932v^3-206150u^2+2268uv+12636v^2+52681u \\ & +6480v-2592)\,/u(u^2+1)(u-1)^2\,, \end{aligned}$$

[12] See, however, the discussion on computational limitations in [17].

$$\begin{aligned}\mathcal{Y}(u,v) = \tfrac{9129329}{524288}(&2070033u^6 + 70533u^5v - 28045u^4v^2 + 45962u^3v^3 + 90616u^2v^4\\ &- 7973144u^5 + 1130670u^4v + 1634455u^3v^2 + 312517u^2v^3 - 117296uv^4\\ &+ 12052790u^4 - 2569492u^3v - 3224660u^2v^2 + 524456uv^3 + 33368v^4\\ &- 9090868u^3 + 1336366u^2v + 1787607uv^2 + 179353v^3 + 3599145u^2\\ &+ 115343uv - 162669v^2 - 691324u - 83420v + 33368)\,/u(u^2+1)(u-1)^3\,.\end{aligned}$$

By now it should be clear that without the use of symbolic computation we would not get very far. These rational functions $\mathcal{X}(u,v)$ and $\mathcal{Y}(u,v)$ are defined over $\mathbb{Q}$, which implies that $(x(P), y(P)) \in \mathcal{E}(\mathbb{Q})$ for any point P with $(u(P), v(P)) \in \mathcal{C}(\mathbb{Q})$. Therefore we need only consider a Mordell-Weil basis of $\mathcal{E}$ over $\mathbb{Q}$ instead of over a proper extension of $\mathbb{Q}$ (see the remark on page 4). This curve has trivial torsion and its rank is 5. A basis is given by

$$P_1 = \left(-\tfrac{84348011}{49152}, -\tfrac{566849166939}{524288}\right),\ P_2 = \left(\tfrac{406276981}{49152}, \tfrac{516236166963}{524288}\right),\ P_3 = \left(-\tfrac{240027095}{49152}, -\tfrac{37384602255}{32768}\right),$$
$$P_4 = \left(\tfrac{30445657}{49152}, \tfrac{32673868491}{32768}\right), \qquad P_5 = \left(\tfrac{589387733}{24576}, \tfrac{3778802730351}{1048576}\right)$$

with corresponding canonical heights bounded from above by 3.011, 3.019, 3.039, 3.214, 4.005, respectively.

Consider the case $u > 0$. According to Fact 2, we have the following five Puiseux expansions ($i = 1, \ldots, 5$)

$$v_i(u) = \rho_i u + d_0(\rho_i) + d_1(\rho_i)u^{-1} + d_2(\rho_i)u^{-2} + O(u^{-3}) \quad (u \to \infty), \tag{18}$$

where

$$\begin{aligned}d_0(\rho_i) &= \tfrac{117652915}{2647875132}\rho_i^4 + \tfrac{59690773}{294208348}\rho_i^3 + \tfrac{64881275}{294208348}\rho_i^2 - \tfrac{37533284}{73552087}\rho_i + \tfrac{3292350}{73552087},\\ d_1(\rho_i) &= \tfrac{2409249577008465}{86558552032889104}\rho_i^4 - \tfrac{143100375932054279}{41548104975786769 92}\rho_i^3 - \tfrac{3841218563243545585}{12464431492736030976}\rho_i^2\\ &\quad - \tfrac{442118719850886867}{692468416263112832}\rho_i + \tfrac{99742932488150451}{173117104065778208},\\ d_2(\rho_i) &= -\tfrac{463043679907914577326408 85}{366713979823704167352578 7648}\rho_i^4 + \tfrac{9187197904486184469752234 3}{183356989911852083676289382 4}\rho_i^3\\ &\quad + \tfrac{436668018807021308919326 91}{814919955163787038561286144}\rho_i^2 + \tfrac{283190018894103565189620835 7}{293371183858963333882063011 84}\rho_i\\ &\quad - \tfrac{213000092757640705570148071}{814919955163787038561286144},\end{aligned}$$

and $\rho_1, \ldots, \rho_5$ are the roots of $8X^5 + 207X - 180 = 0$, only one of which, ρ_1 say, is real. In the notation of Fact 2, $\nu_1 = 1$. The maximum modulus of the roots of the resultant $\mathrm{res}_v(f, \frac{\partial f}{\partial v})$ equals $M \approx 2.83$. According to Lemma 2.2.1, for any point $(u,v) \in \mathcal{C}(\mathbb{R})$ with $u > M$, v can be expressed as $v = v_1(u)$. The geometric meaning of this is that the graph of $C(\mathbb{R})$ has one infinite 'branch' in the positive direction.

From the expansions (18) it is clear that $\lim\limits_{u\to\infty} \dfrac{v_i(u)}{u} = \rho_i$. It is then straightforward to deduce that for $i = 1, \ldots, 5$

$$x_{0i} = \lim_{u\to\infty} \mathcal{X}(u, v_i(u)) = \tfrac{1878283}{512}\rho_i^4 + \tfrac{43681}{32}\rho_i^3 + \tfrac{37434617}{4096}\rho_i^2 + \tfrac{55431189}{4096}\rho_i + \tfrac{4541994061}{49152}.$$

The explicit coordinates of the point Q_{01} now easily follow (see Definition 2.3.2).

Finally we consider $\dfrac{g_1(u)}{f_v(u, v_1(u))}$ as a Puiseux series in u. With MAPLE's help we find

$$\frac{g_1(u)}{f_v(u, v_1(u))} = C(\rho)u^{-2} + O(u^{-3}) \quad (u \to \infty), \quad \text{with}$$
$$C(\rho) = -\tfrac{3208960}{19764496521}\rho_1^4 - \tfrac{3488000}{19764496521}\rho_1^3 + \tfrac{3609248}{6588165507}\rho_1^2 + \tfrac{18542144}{6588165507}\rho_1 - \tfrac{7380608}{2196055169}\,,$$

which shows that $\delta = 1 = 1/\nu_1$ (cf. Proposition 2.4.1).

In the notation of Section 2.5, $e_1 \approx -12630.87093889$ and $e_2, e_3 \notin \mathbb{R}$, which means (cf. Section 2.5) a Case 1 situation. Once we explicitly know the rational function $\mathcal{U}(x, y)$ it is easily checked that we may take the value 2.83 for the constant M (cf. **Notes**[3]). Then the function $u \mapsto x_1(u)$ (cf. the beginning of Section 2.4) maps the interval (M, ∞) bijectively onto the open interval $(x_1(M), x_{01})$, where $x_1(M) \approx 2.241652$ and $x_{01} \approx 113356.8$. Hence, every point $P \in \mathcal{C}(\mathbb{Q})$ with $u(P) > 2.83$ has $x(P) > e_1$ and the corresponding linear form is

$$\mathcal{L}(P) = -\omega\tilde{\phi}(Q_{01}) + m_0\omega + m_1\omega\tilde{\phi}(P_1) + \cdots + \omega\tilde{\phi}(P_5)\,.$$

From this point on we follow the steps described in Section 2.5 to compute the values $c_1, \ldots, c_{10}$. Nothing unusual occurred in or as a result of this computational process.

The case $u < 0$ can be dealt with analogously on putting $f'(u, v) = f(-u, v)$ and studying the solutions of $f'(u, v) = 0$ with $u > 0$. In particular, we now have the following five Puiseux expansions ($i = 1, \ldots, 5$):

$$v_i'(u) = -\rho_i u + d_0(\rho_i) - d_1(\rho_i)u^{-1} + d_2(\rho_i)u^{-2} + O(u^{-3}) \quad (u \to \infty),$$

where ρ_i and d_0, d_1, d_2 are as before. We then proceed exactly as in the case $u > 0$.

3.2 A degree 9 example

It was Mark van Hoeij who put us on the track of the unusual curve of genus 1 given by the equation $f(u, v) = 0$, where

$$f(u, v) = v^9 + (504u^2 + 168)v^6 + 405(3u^2 + 1)(u + 1)v^5 - 636(3u^2 + 1)^2v^3 + 324(3u^2 + 1)^2(u + 1)v^2 - \tfrac{243}{4}(u^2 + 2u + 1)(3u^2 + 1)^2v + 8(3u^2 + 1)^3.$$

In order to find a short Weierstrass model for this curve, we noticed that $(u, v) = (0, \frac{32}{81})$ is a regular point on the curve $g(u, v) = 0$, where

$$g(u, v) = u^6 f(u^{-1}, v).$$

Working with this point, it took van Hoeij's algorithm [12] as implemented in MAPLE 6 almost two and a half hours on a Pentium III 733 MHz desktop to find the corresponding Weierstrass equation

$$y^2 = x^3 - 2\,, \tag{19}$$

together with the birational transformation (2), and as it happens, $\mathcal{X}(u,v)$ and $\mathcal{Y}(u,v)$ are again defined over $\mathbb{Q}$. Both are too large to reproduce here. To give an impression of their sizes, the total degree of the numerator/denominator of $\mathcal{X}(u,v)$ and $\mathcal{Y}(u,v)$ is 20/19 and 21/20 respectively, and both have numerators with more than 100 terms[13].

As in the previous example, the coefficients of these rational functions are again rational, and therefore we need only consider a Mordell-Weil basis of $\mathcal{E}(\mathbb{Q})$. Actually, $\mathcal{E}/\mathbb{Q}$ has trivial torsion and rank 1 with generator of infinite order $P_1 = (3,5)$.

The remaining calculations only took a fraction of the time needed for the computation of the birational transformations.

Consider first the case $u > 0$. In this example we have, according to Fact 2, nine Puiseux expansions, namely:

$$v_1(u) = \tfrac{32}{81} + \tfrac{832}{19683}u^{-1} + \tfrac{735680}{43046721}u^{-2} + O(u^{-3}) \quad (u \to \infty),$$

and for $i = 2, \ldots, 9$:

$$\begin{aligned} v_i(u) = {} & \beta_i u^{3/4} - \beta_i^2(\tfrac{4}{3159}\beta_i^4 + \tfrac{56}{39})u^{2/4} + \beta_i^3(\tfrac{17}{9477}\beta_i^4 + \tfrac{4583}{2106})u^{1/4} \\ & - (\tfrac{10}{9477}\beta_i^4 + \tfrac{727}{1053}) + \beta_i(\tfrac{35}{85293}\beta_i^4 + \tfrac{3005}{6318})u^{-1/4} \\ & - \beta_i^2(\tfrac{128}{767637}\beta_i^4 + \tfrac{5701}{28431})u^{-2/4} + O(u^{-3/4}) \quad (u \to \infty), \end{aligned}$$

where $\beta_2, \ldots, \beta_9$ are the conjugates of the algebraic number β, satisfying

$$4\beta^8 + 4860\beta^4 - 2187 = 0.$$

Exactly two conjugates of β are real, say β_2 and $\beta_3 = -\beta_2$, and it is easy to see that $\beta_2 = \sqrt[4]{-\frac{1215}{2} + 351\sqrt{3}} \approx 0.818960467$.

In the notation of Fact 2, $\nu_1 = 1$ and $\nu_i = 1/4$ for $i = 2, \ldots, 9$. The maximum modulus of the roots of the resultant $\mathrm{res}_v(f, \frac{\partial f}{\partial v})$ equals $M = 1.375120737$. According to Lemma 2.2.1, for any point $(u,v) \in \mathcal{C}(\mathbb{R})$ with $u > M$, v can be expressed as $v = v_j(u)$ for some $j = 1, 2$ or 3. From a geometric point of view, this means that the graph of $C(\mathbb{R})$ has three infinite 'branches' in the positive direction.

Working in the way we explained in the example of Section 3.1 we find

$$\begin{aligned} x_{01} &= \infty, \\ x_{0i} &= \tfrac{19}{351}\beta_i^4 + \tfrac{5399}{78} \quad (i = 2, \ldots, 9). \end{aligned}$$

Since we are interested only in expansions $v_i(u)$ with real coefficients (see Definition 2.3.2), we only list

$$Q_{01} = \mathcal{O} \text{ and } Q_{02} = Q_{03} = (\tfrac{109}{3} + 19\sqrt{3}, 285 + \tfrac{1513}{9}\sqrt{3}). \tag{20}$$

[13]The interested reader may find them on our homepages.

Finally, we consider the expansion of $\dfrac{g_i(u)}{f_v(u, v_i(u))}$ as a Puiseux series in u. Careful comparison of degrees, and with the indispensable help of MAPLE we find

$$\frac{g_i(u)}{f_v(u, v_i(u))} = \begin{cases} \frac{16}{729}u^{-2} + O(u^{-3}) \ (u \to \infty) & \text{for } i = 1, \\ \frac{\beta_i}{18}u^{-5/4} + O(u^{-3/2}) \ (u \to \infty) & \text{for } i = 2, 3, \end{cases}$$

which again shows that $\delta = 1/\nu_i$ in all cases (cf. Proposition 2.4.1).

In the notation of Section 2.5, $e_1 = \sqrt[3]{2}$ and $e_2, e_3 \notin \mathbb{R}$. Again, this is the Case 1 situation, and, for a general point $P \in \mathcal{C}(\mathbb{Q})$, our linear form has one of the two forms

$$\mathcal{L}(P) = \begin{cases} m_0\omega + m_1\omega\tilde{\phi}(P_1) \\ -\omega\tilde{\phi}(Q_0) + m_0\omega + m_1\omega\tilde{\phi}(P_1), \end{cases}$$

where $Q_0 = Q_{02} = Q_{03}$ (cf. (20)). From this point on we follow the steps described in Section 2.5 to compute the values $c_1, \ldots, c_{10}$. As we mentioned at the beginning of this section, there is no point in giving the details of these calculations. The only somewhat 'unfriendly' value is that of c_3, which, in one instance is as large as 15.5. This is due, basically, to the complicated form of the rational function $\mathcal{X}(u, v)$ (cf. the proof of Lemma 2.5.1) . As a consequence, a comparatively small value for c_6 is obtained which, in turn, results in a large upper bound for N (approximately 10^{42}), rather unusual for a rank 1 curve. This, combined with the fact that c_1 is very small (its smallest value is 0.046), requires checking multiples $n \cdot P_1$ in the reduction process with n as large as 70.

The case $u < 0$ is treated analogously on putting $f'(u, v) = f(-u, v)$ and studying the solutions of $f'(u, v) = 0$ with $u > 0$. The Puiseux expansions are similar as before, namely

$$v_1'(u) = \tfrac{32}{81} - \tfrac{832}{19683}u^{-1} + \tfrac{735680}{43046721}u^{-2} + O(u^{-3}) \quad (u \to \infty),$$

and for $i = 2, \ldots, 9$

$$\begin{aligned} v_i'(u) = {} & \beta_i' u^{3/4} - \beta_i'^2 (\tfrac{4}{3159}\beta_i'^4 - \tfrac{56}{39})u^{2/4} + \beta_i'^3(-\tfrac{17}{9477}\beta_i'^4 + \tfrac{4583}{2106})u^{1/4} \\ & - (-\tfrac{10}{9477}\beta_i'^4 + \tfrac{727}{1053}) + \beta_i'(\tfrac{35}{85293}\beta_i'^4 - \tfrac{3005}{6318})u^{-1/4} \\ & - \beta_i'^2(-\tfrac{128}{767637}\beta_i'^4 + \tfrac{5701}{28431})u^{-2/4} + O(u^{-3/4}) \quad (u \to \infty), \end{aligned}$$

where $\beta_2', \ldots, \beta_9'$ are the conjugates of the algebraic number β' with defining equation

$$4\beta'^8 - 4860\beta'^4 - 2187 = 0.$$

Exactly two conjugates of β' are real, say $\beta_2' = \sqrt[4]{\frac{1215}{2} + 351\sqrt{3}}$ and $\beta_3' = -\beta_2'$, and we proceed exactly as before.

References

[1] A. Baker and J. Coates, Integer points on curves of genus 1, *Proc. Camb. Phil. Soc.* **67** (1970), 595–602.

[2] G.A. Bliss, Algebraic Functions, *American Mathematical Society Colloquium Publications* xvi, New York 1933.

[3] A. Bremner, R.J. Stroeker, and N. Tzanakis, On sums of consecutive squares, *J. Number Th.* **62** (1997), 39–70.

[4] C. Chevalley, Introduction to the theory of algebraic functions of one variable, *American Mathematical Society Mathematical Surveys* **6**, 1951.

[5] J. Coates, Construction of rational functions on a curve, *Proc. Camb. Phil. Soc.* **68** (1970), 105–123.

[6] J.W.S. Cassels, Lectures on Elliptic Curves, *London Math. Soc. Student Texts* **24**, Cambridge University Press, Cambridge 1991.

[7] S. David, Minorations de formes linéaires de logarithmes elliptiques, *Mémoires Soc. Math. France (N.S)* **62** (1995).

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

[9] J. Gebel, A. Pethő, and H.G. Zimmer, On Mordell's equation, *Compositio Math.* **110** (1998), 335–367.

[10] M. van Hoeij, An algorithm for computing an integral basis in an algebraic number field, *J. Symbolic Comp.* **18** (1994), 353–363.

[11] M. van Hoeij, Computing parametrizations of rational algebraic curves, *ISSAC '94 Proceedings* (1994), 187–190.

[12] M. van Hoeij, An algorithm for computing the Weierstrass normal form, *ISSAC '95 Proceedings* (1995), 90–95.

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

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

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

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

[17] R.J. Stroeker and N. Tzanakis, On the Elliptic Logarithm Method for Elliptic Diophantine Equations: Reflections and an improvement, *Experim. Math.* **8** (1999), 135–149.

[18] R.J. Stroeker and N. Tzanakis, Computing all integer solutions of a general elliptic equation, In: Algorithmic Number Theory (ed. Wieb Bosma), Proceedings of the 4th International Symposium, ANTS-IV, Leiden, The Netherlands, July 2000, *Lecture Notes in Computer Science* **1838**, 551–561.

[19] R.J. Stroeker and B.M.M. de Weger, Elliptic Binomial Diophantine Equations. *Math. Comp.* **68** (1999), 1257–1281.

[20] R.J. Stroeker and B.M.M. de Weger, Solving elliptic diophantine equations: the general cubic case, *Acta Arith.* **87** (1999), 339–365.

[21] N. Tzanakis, Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations. *Acta Arith.* **75** (1996), 165–190.

[22] R.J. Walker, Algebraic Curves, Springer-Verlag, New York, 1978.

[23] P.G. Walsh, A quantitative version of Runge's theorem on diophantine equations, *Acta Arithm.* **62** (1992), 157–172.

[24] P.G. Walsh, On the complexity of rational Puiseux expansions, *Pacific J. Math.* **188** (1999), 369–387.

[25] P.G. Walsh, A polynomial-time complexity bound for the computation of the singular part of a Puiseux expansion of an algebraic function, *Math. Comp.* **69** (2000), 1167–1182.

[26] P.G. Walsh, Irreducibility testing over local fields, *Math. Comp.* **69** (2000), 1183–1191.

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

[28] H.G. Zimmer and S. Schmitt, Height estimates for elliptic curves in short Weierstraß form over global fields and a comparison, *Arch. Math.* **77**(1) (2001), 22–31.

Notes

[1] **[cf. page 5]**
The following remarks refer to Fact 2.

(i) Statements (a), (b), and (c) are classical statements on Puiseux series. They can be found in classical books such as [2, Chapter II] and [22, Chapter IV], though in slightly different form. The authors of these books use the notion of parameterization in order to express the solutions (u, v), and instead of (3) write $u = t^{-\nu_i}$ and $v = v_i(t^{-\nu_i}) = \sum_{k=\mu_i}^{\infty} \alpha_{k,i} t^k$. Here we prefer following §3 of [23].

(ii) The Puiseux expansions (3) can be computed algorithmically by means of Newton polygons; see for instance [22, Chapter IV, §3]. An interesting refinement of this process is found in [25] with an added discussion on complexity matters; see also [24, §2] and [26, §3]. It is worth mentioning that the `algcurves` package of MAPLE computes the Puiseux expansions of an algebraic function.

(iii) Statement (d) seems widely known. However, we could not find an easily accessible reference where this is explicitly stated and proved. Implicitly it can be derived from, for example, [2, Chapter II] (especially §13).
Note that the non-vanishing of $\mathrm{res}_v(f, \frac{\partial f}{\partial v}) \in \mathbb{Z}[u]$ for a specific value u_0 of u (in particular for $|u_0| > M$) means that the coefficient $p_0(u_0)$ of v^n in $f(u, v)$ is non-zero. In particular this shows that $f(u_0, v)$ is a non-zero polynomial in v, and what is more, this polynomial has only simple roots.

(iv) Statement (e) is found, for example, in [2, Theorem 13.1] and what precedes this theorem. For the injectivity proof of $t \mapsto v_i(t^{-\nu_i})$ we need the somewhat technical requirement in (a) on the minimality of ν_i.

(v) Let ζ be a primitive ν_i-th root of unity, $m \in \{0, 1, \ldots, \nu_i - 1\}$, and $\sigma \in \mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. The formal series

$$v_i(u, m, \sigma) = \sum_{k=\mu_i}^{\infty} \sigma(\alpha_{k,i}) \zeta^{mk} u^{-k/\nu_i}$$

also satisfies $f(u, v_i(u, m, \sigma)) = 0$, and hence coincides with another series (3), say with $v_j(u) = v_j(u, 0, \mathrm{id})$. We then say that $v_j(u)$ and $v_i(u)$ belong to the same conjugacy class. The n series (3) are thus partitioned into disjoint conjugacy classes (see after relation (3.5) in [23]). Therefore, the computation of a smaller set of series (3) composed of representatives of each conjugacy class—this is what MAPLE actually does when it is asked to compute the Puiseux expansions of an algebraic function—suffices for the computation of all expansions (3).

[2] **[cf. page 5]**
The algorithm below, implicitly contained in the proof of Lemma 3 of [5], determines the finite extension of $\mathbb{Q}$, generated by the infinitely many $\alpha_{k,i}$'s that appear in Fact 2, once the integers ν_i and μ_i have been computed (e.g. by the first few steps in the construction of a Newton polygon).
Fix a subscript i in (3) and subsequently omit it in order to simplify notation. Write

$$f(u, v) = \sum_{j=0}^{n} p_j(u) v^{n-j}, \text{ with } p_j \in \mathbb{Z}[u] \ (j = 0, 1, \ldots, n).$$

Choose a non-negative integer N such that

$$-\nu \deg p_j + \mu(n - j) + N \geq 0 \quad (j = 0, \ldots, n)$$

with equality for at least one subscript j, and put

$$P_j(x) = p_j(x^{-\nu}) x^{\mu(n-j)+N} \ (j = 0, \ldots, n) \ \text{ and } \ F(x, y) = \sum_{j=0}^{n} P_j(x) y^{n-j}.$$

Then $F \in \mathbb{Z}[x, y]$, and it is straightforward to check that

$$F(x, y(x)) = 0 \text{ identically in } x, \text{ where } y(x) = \sum_{k=0}^{\infty} \alpha_{k+\mu} x^k. \tag{21}$$

Algorithm. *Let $m = \deg_x F$ and $\kappa = (2n-2)m+1$. For $k = 0, 1, 2, \dots$ determine recursively polynomials $F_k(x, y)$ and $H_k(y)$ as follows:*

Step 1. Put $k = 0$ and $F_k(x, y) = F(x, y)$.
Step 2. Write $H_k(y) = F_k(0, y)$, and let u_k be a zero of H_k.
Step 3. Compute $F_k(x, u_k + xy)$ and let x^g be the least x-power occurring in the resulting polynomial. Put $F_{k+1}(x, y) = x^{-g} F_k(x, u_k + xy)$, $k \leftarrow k + 1$. If $k \leq \kappa$, go to **Step 2**.

By the proof of Lemma 3 of [5], the polynomials H_k ($k = 0, 1, 2, \dots$) are not identically zero, their degrees are in non-increasing order and $\deg H_{k_0} = 1$ for some $k_0 \leq \kappa$, so that for all $k \geq k_0$ the polynomial H_k is of degree 1. Now for each $k \geq 0$, the algebraic number $\alpha_{k+\mu}$ in (21) is a root of H_k, and therefore assumes one of the possible values of u_k. By the linear character of H_k for all $k \geq k_0$, it follows that for $k > k_0$, $\alpha_{k+\mu}$ is uniquely determined by the previous α's and $\alpha_{k+\mu} \in \mathbb{Q}(\alpha_\mu, \alpha_{\mu+1}, \dots, \alpha_{\mu+k_0})$.

[3] **[cf. page 7]**
Consider the set S consisting of those of the following points of $\mathcal{E}$ that are not poles of $\mathcal{U}$: the zero point and the points $(e, 0)$, where e is a real zero of $q(x)$ (cf. (1)). For relation (7) to hold it suffices that $u(P) \geq M$, where M exceeds the u-coordinates of all finite points of $\mathcal{C}(\mathbb{R})$ that are poles for either $\mathcal{X}$ or $\mathcal{Y}$ (these poles are finite in number; cf. the beginning of the proof of Proposition 2.3.1) and the values of $\mathcal{U}$ at all (at most four) points of S.