Computing all integer solutions of a general elliptic equation

R.J. Stroeker[1] and N. Tzanakis[2]

[1] Econometric Institute - Erasmus University
3000 DR Rotterdam, The Netherlands
stroeker@few.eur.nl
http://www.few.eur.nl/few/people/stroeker/

[2] Department of Mathematics, University of Crete
GR-71409 Iraklion, Crete, Greece
tzanakis@math.uch.gr
http://itia.math.uch.gr/~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 explore the possibility of extending this method to include any equation $f(u,v)=0$, where $f \in \mathbb{Z}[u,v]$ defines an irreducible curve of genus 1, independent of shape or degree of the polynomial f. We give a detailed description of the general features of our approach, putting forward along the way some claims (one of which conjectural) that are supported by the explicit examples added at the end.

1 Introduction

Throughout this paper, the term *elliptic equation* shall mean an equation $f(u,v)=0$ in rational integers u and v, where $f \in \mathbb{Z}[X,Y]$ is such that the plane curve defined by $f=0$ is an irreducible curve of genus 1. The *Elliptic Logarithm Method*—$\mathfrak{Ellog}$ for short—as a *practical* method for solving such equations, was first applied by Stroeker and Tzanakis [12] and, independently, by Gebel, Pethő and Zimmer [6]. Since then, it has been applied extensively to a variety of elliptic equations of degree 3 or 4; see [11], [16], [1], [7], [14], [15], [13]. In particular, a general treatment of the cubic elliptic equation can be found in [15].

Now that many equations have been successfully solved by application of $\mathfrak{Ellog}$, it seems natural to ask what we can learn from the experience acquired so far, so that we may distinguish the essential characteristics of the method which would make its successful application possible to any elliptic equation. We shall put forward some plausible suggestions, not all of which we can prove yet in full generality. Next we shall test our general observations by a few specific examples of non-standard elliptic equations.

2 Preliminaries

Let

$$f(u,v)=0, \text{ where } f \in \mathbb{Z}[u,v] \text{ is irreducible},$$

define an elliptic curve $\mathcal{C}$, birationally equivalent over a number field $\mathbb{K}$ of degree at most $\min\{\deg_u f, \deg_v f\}$ to

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

by means of a birational transformation

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

(see e.g. [9], Proposition 1).

Claim 1 *One can explicitly calculate a possibly large positive constant M, and finitely many parametrizations of $\mathcal{C}$ of the form*

$$u(t) = t^{-\nu}, \quad v(t) = \alpha t^{\mu} + \alpha' t^{\mu'} + \alpha'' t^{\mu''} + \ldots \tag{1}$$

for rational integers $\nu \geq 1$, $\mu < \mu' < \mu'' < \ldots$, and non-zero algebraic integers $\alpha, \alpha', \alpha'' \ldots$, such that every real point (u,v) on $\mathcal{C}$ with $|u| > M$ can be expressed as $(u(t), v(t))$ by means of one of the parametrizations (1) *for a suitable value of t.*

Although this claim seems quite classical (Puiseux), the crux lies in the effectiveness of the calculation of M. For a proof, see Lemma 5 of [2]. This result of Coates, however, is not useful for explicit computations, as it implies an extremely large M. Much smaller M is implied by subsequent results of W.M. Schmidt [8] or B.M. Dwork and A. van der Poorten [4][5]. In certain examples the numerical value of M implied by these improved results may be still very large. In our Example 3 of Section 6, for example, M is of the size of 10^{60}; this implies the need for a method that could detect, in some clever way, all integral solutions (u,v) with $|u| < M$. We cannot, at present, propose such a method.

Clearly, there is no loss of generality restricting our investigations to those solutions (u,v) of $f(u,v) = 0$ with $u > 0$. The above claim implies that, for a given point (u,v) on the curve and u sufficiently large, the equation $f(u,v) = 0$ can be solved for v, i.e. there exist differentiable functions $v_1(u), \ldots, v_k(u)$, $(k \leq \deg_v f)$, such that $f(u, v_i(u)) = 0$ identically in u for every $i \in \{1, \ldots, k\}$. Of course, this is also an immediate consequence of the *Implicit Function Theorem.* Let us put

$$x_{0i} = \lim_{u \to \infty} \mathcal{X}(u, v_i(u)).$$

¿From this point onwards $P \in \mathcal{C}$ will always denote a point with integral coordinates $(u(P), v(P))$. Since all points P with relatively small coordinates can be easily found explicitly, we may assume $u(P)$ to be sufficiently large, so that, for some $i \in \{1, \ldots, k\}$, $v(P) = v_i(u(P))$ and $x(P) = \mathcal{X}(u(P), v(P))$ is close to x_{0i}. Let us explain what we mean by 'close' in this context.

Let e_1 denote the only real root of $q(x) = 0$ if this equation has a single root only (the complex case), or the largest real root in case of three real roots (the real case); in the latter case the other two real roots are denoted by e_2 and e_3 and we assume $e_3 < e_2 < e_1$. In the complex case, $x_{0i} \geq e_1$ and by 'close' we mean that $x(P) \geq e_1$ as well. In the real case, $x_{0i} \in [e_3, e_2]$ and now 'close' means that $x(P) \in [e_3, e_2]$ too.

3 Two related elliptic integrals

It is not difficult to see that

$$\frac{\mathrm{d}x}{y} = G(u,v) \frac{\mathrm{d}u}{f_v(u,v)}, \tag{2}$$

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, the function $G(u,v) \in \mathbb{C}(\mathcal{C})$ is constant; see [12], [16] and [15]. For example, in case of a general cubic equation, $G(u,v) = \pm 2$.

Now fix $i \in \{1,\dots,k\}$. For u sufficiently large, $\mathcal{Y}(u, v_i(u))$ and $\mathcal{X}(u, v_i(u))$ are continuous functions of u; if we denote them by $y(u)$ and $x(u)$ respectively, then $y(u)^2 = x(u)^3 + Ax(u) + B = q(x(u))$. Hence $y(u) = \varepsilon\sqrt{q(x(u))}$ with $\varepsilon \in \{-1,1\}$. On putting

$$g_i(u) = G(u, v_i(u)),$$

we have, by (2) and our assumption on the size of $u(P)$,

$$\int_{u(P)}^{\infty} \frac{g_i(u)\mathrm{d}u}{f_v(u, v_i(u))} = \int_{x(P)}^{x_{0i}} \frac{\mathrm{d}x}{\varepsilon\sqrt{q(x)}}. \tag{3}$$

Here $x(P) = \mathcal{X}(u(P), v(P))$ of course.

4 Necessary conditions for the applicability of $\mathfrak{Ellog}$

For $\mathfrak{Ellog}$ to work it is essential that the integral in the left-hand side of (3) tends to zero as $u(P)$ tends to ∞.

Conjectural Claim 2

$$\frac{g_i(u)}{f_v(u, v_i(u))} = \mathcal{O}(u^{-1-\delta}) \tag{4}$$

for some $\delta > 0$.

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 [15] and [16], respectively).
It follows from (4) that the left-hand side of (3) is $\leq c_1 u^{-\delta}$. Here the constant c_1, as well as all other constants c_i in the sequel are effectively computable.

Claim 3 *Let* $h(\cdot)$ *denote the logarithmic height. Then,*

$$h(x(P)) = h(\mathcal{X}(u(P), v(P))) \leq c_2 + c_3 \log|u(P)|. \tag{5}$$

Inequality (5) is easily seen to be true. Indeed, write

$$f(u,v) = f_d(u)v^d + \ldots + f_1(u)v + f_0(u)$$

with $f_j(u) \in \mathbb{Z}[u]$ of degree j. If $(u,v) \in \mathbb{Z}^2$ and $f(u,v) = 0$, then v is an integral root of the polynomial $f_d(u)X^d + \cdots + f_1(u)X + f_0(u)$ with integer coefficients. Hence v divides $f_0(u)$, from which it follows that $|v| \leq |f_0(u)|$. This, combined with the fact that $\mathcal{X}(u,v)$ is a rational function of u and v with integer coefficients, implies inequality (5).

We also need the following relation between the Néron-Tate height and the logarithmic height (see e.g. [10]):

$$\hat{h}(x(P)) - \frac{1}{2}h(P) \leq c_4. \tag{6}$$

Now, the right-hand side of (3) is a so-called linear form in elliptic logarithms of points on $\mathcal{E}(\overline{\mathbb{Q}})$, say $\mathcal{L}(P)$. It has integer coefficients, which are essentially the coefficients of P with respect to a Mordell-Weil basis chosen well in advance, and we denote the maximum absolute value of these coefficients by N. A more detailed description of $\mathcal{L}$ is given in section 5.

By S. David's Theorem [3], we obtain a lower bound for $\mathcal{L}(P)$ of the shape

$$|\mathcal{L}(P)| > \exp(-c_5(\log N + c_6)(\log\log N + c_7)^k), \tag{7}$$

where $k = r+2$ or $r+3$ and r is the rank of the Mordell-Weil group. We also need an upper bound for $\mathcal{L}(P)$. This upper bound can be deduced from (3) and (4):

$$|\mathcal{L}(P)| \leq c_1(u(P))^{-\delta}.$$

Combining this with (5), (6) and the well-known fact that $\hat{h}(P) \geq c_8 N^2$, we obtain

$$|\mathcal{L}(P)| \leq \exp(-c_9 N^2 + c_{10}) \tag{8}$$

and finally (7) and (8) imply an upper bound for N. Much of the material found in this section and the next consists of straightforward adaptations from [12], [16] or [15].

5 The linear form $\mathcal{L}(P)$

In this section we discuss in some detail the linear form $\mathcal{L}(P)$, and we show that this form indeed qualifies as a suitable linear form in elliptic logarithms of points on $\mathcal{E}(\overline{\mathbb{Q}})$ to which S. David's theorem, mentioned in the previous section, can be applied.

The curve $\mathcal{E}(\mathbb{R})$, defined by $y^2 = q(x)$, has the identity component $\mathcal{E}_0(\mathbb{R})$ and in the real case—we remind the reader that $q(x) = 0$ then 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 e.g. [12]). 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 as follows:

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

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 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,

$$\tilde{\phi}(P) \text{ and } \tilde{\phi}(-P) \text{ are of the form } m_1\tilde{\phi}(P_1) + \cdots + m_r\tilde{\phi}(P_r) + m_0 + \frac{s}{t}, \tag{10}$$

where $m_j = \pm n_j$ $(j = 1, \ldots, r)$, $m_0 \in \mathbb{Z}$ is effectively bounded in terms of N, and s, t are relatively prime integers, effectively bounded by a small number.

Consider the integral in the right-hand side of (3) and recall that $f(u, v_i(u)) = 0$, provided u is sufficiently large.

Claim 4

$$x_{0i} \in \overline{\mathbb{Q}} \cup \{\pm\infty\}.$$

The truth of this statement depends only on the truth of Claim 1 as we shall see shortly. 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 whole curve $\mathcal{C}$ could be mapped into a line, which is impossible for a curve of genus 1. Next, by Claim 1, every point $(u, v_i(u)) \in \mathcal{C}$ with u near ∞ has a parametrization (1), where the coefficients and the exponents depend solely on the function v_i. On substituting the t-expressions for u and v of (1), the value of $\mathcal{X}(u, v_i(u))$ for u near ∞ can be seen to be given by an expression of the form

$$\frac{\beta t^{\lambda} + \beta' t^{\lambda'} + \beta'' t^{\lambda''} + \dots}{\gamma t^{\rho} + \gamma' t^{\rho'} + \gamma'' t^{\rho''} + \dots} \quad (t \text{ near zero}),$$

where $\beta, \beta', \beta'', \dots, \gamma, \gamma', \gamma'', \dots$ are non-zero algebraic numbers and $\lambda < \lambda' < \lambda'' < \dots$ and $\rho < \rho' < \rho'' < \dots$ are rational integers. This shows that

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

If $x_{0i} \neq \pm\infty$ we denote by Q_{0i} the point with x-coordinate x_{0i} and non-negative y-coordinate. If $x_{0i} = \pm\infty$ we set $Q_{0i} = \mathcal{O}$, the group identity.

We distinguish two cases:

1. $e_1 \leq x_{0i}$. Then, because $u(P)$ is assumed to be sufficiently large, we have $e_1 < x(P) = \mathcal{X}(u(P), v(P))$ 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 $y(P) = \mathcal{Y}(u(P), v(P))$ is non-negative or negative, respectively. This, combined with (10) and (9) shows that the integral in the right-hand side of (3) is equal to a linear form in elliptic logarithms
$$-\omega\tilde{\phi}(Q_{0i}) + (m_0 + \frac{s}{t})\omega + m_1\omega\tilde{\phi}(P_1) + \dots + m_r\omega\tilde{\phi}(P_r), \tag{11}$$
and all points appearing in it have algebraic coordinates.
2. $x_{0i} \in [e_3, e_2]$. Then, because $u(P)$ is sufficiently large, $x(P) \in (e_3, e_2)$ and
$$\begin{aligned}\int_{x(P)}^{x_{0i}} \frac{\mathrm{d}x}{\sqrt{q(x)}} = \int_{x(P)}^{e_2} \frac{\mathrm{d}x}{\sqrt{q(x)}} - \int_{x_{0i}}^{e_2} \frac{\mathrm{d}x}{\sqrt{q(x)}} &= \int_{x(P')}^{\infty} \frac{\mathrm{d}x}{\sqrt{q(x)}} - \int_{x(Q'_{0i})}^{\infty} \frac{\mathrm{d}x}{\sqrt{q(x)}} \\ = \omega\phi(\sigma P') - \omega\phi(Q'_{0i}) &= \omega\tilde{\phi}(\sigma P) - \omega\tilde{\phi}(Q_{0i})\end{aligned}$$
and we arrive at the same conclusion (11) as before.

6 Examples

It is not easy to find in the literature non-trivial examples of irreducible curves of genus 1 of an unusual shape, that is given by equations of degree at least 5. Therefore, with the exception of the third example, we have generated a few examples by ourselves. Further, we shall only discuss solutions (u, v) with $u > 0$ and sufficiently large.

We have chosen not to take $\mathfrak{Ellog}$ 'all the way', for the simple reason that, once we have checked the various claims —and this is what we actually do below, except for the values of the various M's[1] —completing the computations is merely a routine matter, be it a tedious one.

We have implemented in Maple a procedure for computing parametrizations (1), using Newton polygons (see e.g. [17]).

6.1 Three simple examples

We have grouped the following three equations because of their similarity; each provides a straightforward example of an elliptic equation of unusual form. In the table below we have gathered the relevant information.

Three simple elliptic equations $f(u, v) = 0$

$f(u,v)$	$u^5 + u^4 - 2v^3$	$u^6 + u^3 - 2v^2$	$u^7 + u^4 - 2v^2$
Singular points $[u,v]$ (multiplicity)	$[0,0](3), \infty(2)$	$[0,0](2), \infty(4)$	$[0,0](2), \infty(5)$
Rank r	0	1	1
Weierstrass A, B	$0, 1$	$0, 8$	$0, 8$
Birational transformation			
$\mathcal{X}(u,v)$	$-2\frac{v}{u(u+1)}$	$2\frac{2u^3+u^2+u+4v}{u(u-1)^2}$	$2\frac{u^4+u^3+2u^2+4v}{u^2(u-1)^2}$
$\mathcal{Y}(u,v)$	$\frac{u-1}{u+1}$	$4\frac{4u^4+3u^2+u+5uv+3v}{u(u-1)^3}$	$4\frac{u^5+3u^4+4u^2+3uv+5v}{u^2(u-1)^3}$
Claim 1			
ν	3	1	2
$\mu, \mu', \mu'', \ldots$	$-5, -2, 1, 4, 7, \ldots$	$-3, 0, 3, 6, 9, \ldots$	$-7, -1, 5, 11, 17, \ldots$
$\alpha, \alpha', \alpha'', \ldots$	$\rho, \frac{\rho}{3}, -\frac{\rho}{9}, \frac{5\rho}{81}, -\frac{10\rho}{243}, \ldots$	$\rho, \frac{\rho}{2}, -\frac{\rho}{8}, \frac{\rho}{16}, -\frac{5\rho}{128}, \ldots$	$\rho, \frac{\rho}{2}, -\frac{\rho}{8}, \frac{\rho}{16}, -\frac{5\rho}{128}, \ldots$
ρ	$1/\sqrt[3]{2}$	$\pm 1/\sqrt{2}$	$\pm 1/\sqrt{2}$
k	1	2	2
Conjectural Claim 2			
δ	$1/3$	1	$1/2$
Claim 4			
$x_{i0}(u \to \infty)$	0	$4 \pm 4\sqrt{2}$	2

6.2 A parametric family of degree 5 curves

In the course of constructing suitable examples, we struck on the following parametric family of elliptic equations:

$$f(u, v) = v^2(v - u - 1)(v + (2\tau - 1)u - 1) + \tau u^2(v^3 - 1) = 0. \qquad (12)$$

For each value of the parameter $\tau \neq 0$, $\tau \in \mathbb{Z}$, this equation represents an elliptic curve $\mathcal{C}_\tau$. The singular points of $\mathcal{C}_\tau$ are $(u, v) = (0, 0)$ and $(0, 1)$, both of multiplicity

[1] We actually believe that the various series $v_i(t)$ do converge for $|t|$ less than some number of the order 0.1 say, but we cannot prove this.

2, and the point at infinity is a singular point of multiplicity 3. The birational equivalent curve $\mathcal{E}_\tau$ is

$$y^2 = x^3 + A_\tau x + B_\tau, \quad \text{with } A_\tau = -\tfrac{1}{3}\tau^4 \text{ and } B_\tau = \tfrac{2}{27}\tau^6 + \tau^3,$$

and the corresponding birational transformations are (one way only) given by

$$\mathcal{X}(u,v) = \frac{1}{3}\tau^2 - \tau v, \quad \mathcal{Y}(u,v) = \frac{\tau v(-1+\tau u - u + v)}{u}.$$

In this example $k = 2$, i.e. there exist two parametrizations near $u = \infty$. The first parametrization is given by[2]

$$\begin{aligned}
u_1(t) &= t^{-1},\\
v_1(t) &= -\tau t^{-2} - 2(\tau-1)t^{-1} + \frac{1}{\tau} + 2\frac{(\tau-1)^2}{\tau^2}t - \frac{(4\tau-5)(\tau-1)^2}{\tau^3}t^2\\
&\quad +2\frac{(4\tau-7)(\tau-1)^3}{\tau^4}t^3 - \frac{16\tau^5 - 104\tau^4 + 259\tau^3 - 310\tau^2 + 182\tau - 42}{\tau^5}t^4\\
&\quad +2\frac{(\tau-1)(16\tau^5 - 120\tau^4 + 333\tau^3 - 430\tau^2 + 270\tau - 66)}{\tau^6}t^5\\
&\quad -\frac{64\tau^7 - 688\tau^6 + 2928\tau^5 - 6495\tau^4 + 8288\tau^3 - 6174\tau^2 + 2508\tau - 429}{\tau^7}t^6\\
&\quad + O(t^7)\ (t \to 0).
\end{aligned}$$

It is obvious from this that

$$x_{10} = \lim_{u\to\infty} \mathcal{X}(u, v_1(u)) = \infty.$$

For this parametrization we find

$$\begin{aligned}
\frac{g(u,v_1(u))}{f_v(u,v_1(u))} &= \frac{2}{\tau}u^{-2} - 4\frac{\tau-1}{\tau^2}u^{-3} + 2\frac{4\tau^2 - 9\tau + 6}{\tau^3}u^{-4}\\
&\quad -\frac{8}{3}\frac{6\tau^3 - 16\tau^2 + 17\tau - 7}{\tau^4}u^{-5} + O(u^{-6})\ (u \to \infty),
\end{aligned}$$

so that $\delta = 1$ in this case.
The second parametrization is

$$\begin{aligned}
u_2(t) &= t^{-1},\\
v_2(t) &= \rho_\tau - \frac{2(\tau-1)(4\tau^2\rho_\tau^2 - 10\tau\rho_\tau^2 + 4\rho_\tau^2 + 17\tau^2\rho_\tau + 2\rho_\tau - 8\tau\rho_\tau - 6\tau + 3\tau^2)}{59\tau^3 - 48\tau^2 + 24\tau - 4}t\\
&\quad + \frac{1}{\tau(59\tau^3 - 48\tau^2 + 24\tau - 4)^2}(-80\rho_\tau^2 + 864\tau\rho_\tau^2 + 10328\tau^3\rho_\tau^2 + 16574\tau^5\rho_\tau^2\\
&\qquad -17000\tau^4\rho_\tau^2 - 3904\tau^2\rho_\tau^2 - 8711\tau^6\rho_\tau^2 + 1588\tau^7\rho_\tau^2\\
&\qquad +2088\tau^7\rho_\tau - 3458\tau^4\rho_\tau + 6074\tau^5\rho_\tau + 1192\tau^3\rho_\tau\\
&\qquad -5270\tau^6\rho_\tau - 208\tau^2\rho_\tau + 16\tau\rho_\tau + 1132\tau^7 + 80\tau\\
&\qquad +7588\tau^5 + 2808\tau^3 - 4695\tau^6 - 752\tau^2 - 6192\tau^4)t^2\\
&\qquad + O(t^3)\ (t \to 0),
\end{aligned}$$

where ρ_τ satisfies the cubic equation $X^3 + (1/\tau - 2)X^2 - 1 = 0$. For this parametrization we find

$$x_{20} = \lim_{u\to\infty} \mathcal{X}(u, v_2(u)) = \frac{1}{3}\tau^2 - \rho_\tau\tau.$$

---

[2] Although not really necessary, we calculated quite a number of terms in order to see what they are like and to demonstrate Maple's capabilities.

and

$$\frac{g(u, v_2(u))}{f_v(u, v_2(u))} = d_2 u^{-2} + O(u^{-3}) \ (u \to \infty),$$

where d_2 can be (and was) explicitly calculated by Maple, but is too complicated to be included here. Because $d_2 \neq 0$, $\delta = 1$ for this parametrization as well.

6.3 An example taken from Maple's Help facility

The Help Topic of the Maple V Release 5.1 command **algcurves[singularities]** makes use of the following curve of rank 5:

$$\begin{aligned} f(u,v) = {} & 180u^5 - 207u^4 v - 8v^5 - 450u^4 + 621u^3 v - 128uv^3 - 35v^4 + \\ & 369u^3 - 521u^2 v + 82v^3 - 100u^2 + 135uv - 19v^2 - 7u - 28v + 8 = 0. \end{aligned}$$

Singular points (all of multiplicity 2) are $(u,v) = (0,1), (1,0), (1,-1)$ and the two complex points $(u,v) = (i,i), (-i,-i)$. A short Weierstrass model of this curve is

$$y^2 = x^3 - \frac{62058288278602561}{805306368} x + \frac{6185299411685832648139814 5}{59373627899904}.$$

The corresponding birational transformations are given by

$$\begin{aligned} \mathcal{X}(u,v) &= \frac{43681 \ \mathrm{Num}X(u,v)}{49152u(u^2+1)(u-1)^2}, \\ \mathcal{Y}(u,v) &= \frac{9129329 \ \mathrm{Num}\mathcal{Y}(u,v)}{524288u(u^2+1)(u-1)^3}, \end{aligned}$$

with

$$\begin{aligned} \mathrm{Num}\mathcal{X}(u,v) = {} & 103981u^5 + 15228u^4 v + 10284u^3 v^2 + 1536u^2 v^3 \\ & + 4128uv^4 - 316526u^4 + 47412u^3 v + 67584u^2 v^2 + 15468uv^3 \\ & - 2592v^4 + 368606u^3 - 71388u^2 v - 88968uv^2 - 13932v^3 \\ & - 206150u^2 + 2268uv + 12636v^2 + 52681u + 6480v - 2592, \\ \mathrm{Num}\mathcal{Y}(u,v) = {} & 2070033u^6 + 70533u^5 v - 28045u^4 v^2 \\ & + 45962u^3 v^3 + 90616u^2 v^4 - 7973144u^5 + 1130670u^4 v \\ & + 1634455u^3 v^2 + 312517u^2 v^3 - 117296uv^4 + 12052790u^4 \\ & - 2569492u^3 v - 3224660u^2 v^2 + 524456uv^3 + 33368v^4 \\ & - 9090868u^3 + 1336366u^2 v + 1787607uv^2 + 179353v^3 \\ & + 3599145u^2 + 115343uv - 162669v^2 - 691324u - 83420v + 33368. \end{aligned}$$

In this example there exists only one parametrization near $u = \infty$, given by

$$\begin{aligned} u_1(t) &= t^{-1}, \\ v_1(t) &= \rho t^{-1} + d_0(\rho) + d_1(\rho) t + d_2(\rho) t^2 + O(t^3) \ (t \to 0) \end{aligned}$$

with

$$\begin{aligned} d_0(\rho) = {} & \tfrac{117652915}{2647875132}\rho^4 + \tfrac{59690773}{294208348}\rho^3 + \tfrac{64881275}{294208348}\rho^2 - \tfrac{37533284}{73552087}\rho + \tfrac{3292350}{73552087}, \\ d_1(\rho) = {} & \tfrac{2409249577008465}{8655855203288910 4}\rho^4 - \tfrac{143100375932054279}{4154810497578676992}\rho^3 - \tfrac{384121856324354558 5}{12464431492736030976}\rho^2 \\ & - \tfrac{442118719850886867}{692468416263112832}\rho + \tfrac{99742932488150451}{173117104065778208}, \\ d_2(\rho) = {} & -\tfrac{4630436799079145773264088 5}{366713979823704167352578764 8}\rho^4 + \tfrac{918719790448618446975223 43}{183356989911852083676289382 4}\rho^3 \\ & + \tfrac{436668018807021308919326 91}{814919955163787038561286144}\rho^2 + \tfrac{283190018894103565189620835 7}{293371183858963333882063011 84}\rho \\ & - \tfrac{21300009275764070557014807 1}{814919955163787038561286144}, \end{aligned}$$

where ρ is the only real root of $8X^5 + 207X - 180 = 0$. Standard, but tedious computations yield

$$x_{10} = \lim_{u \to \infty} \mathcal{X}(u, v_1(u)) = \frac{43681}{49152}(4128\rho^4 + 1536\rho^3 + 10284\rho^2 + 15228\rho + 103981),$$

and finally

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

which in particular implies that $\delta = 1$.

References

1. Bremner, A., Stroeker, R.J., Tzanakis, N.: On sums of consecutive squares. J. Number Th. **62** (1997) 39–70
2. Coates, J.: Construction of rational functions on a curve. Proc. Camb. Philos. Soc. **68** (1970) 105–123
3. David, S.: Minorations de formes linéaires de logarithmes elliptiques. Mémoires Soc. Math. France (N.S) **62** (1995)
4. Dwork, B.M., van der Poorten, A.: The Eisenstein constant. Duke Math. J. **65** (1992) 23–43
5. Dwork, B.M., van der Poorten, A.: Corrections to "The Eisenstein constant". Duke Math. J. **76** (1994) 669–672
6. Gebel, J., Pethő, A., Zimmer, H.G.: Computing integral points on elliptic curves. Acta Arith. **68** (1994) 171–192
7. Gebel, J., Pethő, A., Zimmer, H.G.: On Mordell's equation. Compositio Math. **110** (1998) 335–367
8. Schmidt, W.M.: Eisenstein's theorem on power series expansions of algebraic functions. Acta Arithm. **56** (1990) 161–179
9. Schmidt, W.M.: Integer points on curves of genus 1. Compositio Math. **81** (1992) 33–59
10. Silverman, J.H.: The difference between the Weil height and the canonical height on elliptic curves. Math. Comp. **55** (1990) 723–743
11. Stroeker, R.J.: On the sum of consecutive cubes being a perfect square. Compositio Math. **97** (1995) 295–307
12. Stroeker, R.J., Tzanakis, N.: Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. Acta Arith. **67** (1994) 177–196
13. Stroeker, R.J., Tzanakis, N.: On the Elliptic Logarithm Method for Elliptic Diophantine Equations: Reflections and an improvement. Experim. Math. **8** (1999) 135–149
14. Stroeker, R.J., de Weger, B.M.M.: Elliptic Binomial Diophantine Equations. Math. Comp. **68** (1999) 1257–1281
15. Stroeker, R.J., de Weger, B.M.M.: Solving elliptic diophantine equations: the general cubic case. Acta Arith. **87** (1999) 339–365
16. Tzanakis, N: Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations. Acta Arith. **75** (1996) 165–190
17. Walker, R.J.: Algebraic Curves. Springer-Verlag, New-York 1978