On Elliptic Diophantine Equations That Defy Thue's Method: The Case of the Ochoa Curve

Roel J. Stroeker and Benjamin M. M. de Weger

CONTENTS

1991 Mathematics Subject Classification. Primary: 11D25; Secondary: 11G05, 11Y50

Key words and phrases. Diophantine equation, Thue equation, elliptic curve

The purpose of this paper is to show that elliptic diophantine equations cannot always be solved—in the most practical sense—by the Thue approach, that is, by solving each of the finitely many corresponding Thue equations of degree 4. After a brief general discussion, which is necessarily of a heuristic nature, to substantiate our claim, we consider the elliptic equation associated with the Ochoa curve. An explicit computational explanation as to the reasons for the failure of the Thue approach in this case is followed by a complete solution of the standard Weierstraß equation of this elliptic curve by a method which makes use of a recent lower bound for linear forms in elliptic logarithms.

1. INTRODUCTION

In this paper we are interested in efficient ways to solve the elliptic diophantine equation in short Weierstraß form

$$y^2 = f(x) \quad \text{with} \quad f(x) := x^3 + ax + b, \tag{1.1}$$

where $a, b \in \mathbb{Z}$ and the discriminant $4a^3 + 27b^2$ does not vanish, in rational integers x and y. We are also curious about the following question: Are there such equations for which the classical approaches fall short of providing a practical solution process—in other words, equations that defy the standard methods of factorization and diophantine approximation?

The answer to this question must surely be yes; it should be relatively easy to construct such examples. We insist, however, upon equations that have a "natural" appearance in that they at least do not give the impression of being specially concocted for the occasion. In particular, an interesting example

1058-6458/96 $0.50 per page

should have rather small Weierstraß coefficients, and it should not have solutions with exceptionally large coordinates.

Traditionally, the way to solve (1.1) for $(x, y) \in \mathbb{Z}^2$ is to reduce it to another problem in which one attempts to solve the finitely many associated Thue equations. These equations have the form $F(A, B) = m$, where $F \in \mathbb{Z}[A, B]$ is homogeneous of degree 4 and $m \neq 0$ belongs to a finite set. We call this the *Thue approach*.

This reduction may be achieved by the factorization of (1.1) in the number field $\mathbb{Q}(\alpha)$ for a root α of $f(x) = 0$, a process that has been described many times and may be found in the literature in many places, for instance [Stroeker 1984; Stroeker and Tzanakis 1988; Tzanakis and de Weger 1989]. When $\mathbb{Q}(\alpha) \neq \mathbb{Q}$, the Thue approach requires explicit knowledge of the unit group and sometimes of the class group of $\mathbb{Q}(\alpha)$, or at least of the class number of this field. Usually, this is no problem. However, even for a and b of reasonable size, the discriminant of f may be very large. Also, the class number is often small, so the regulator can be of considerable size. This means that, occasionally, rather sizable fundamental units may be expected. If, in addition, the discriminant of f contains many small prime divisors, the number of Thue equations to be investigated could be quite large.

Now, the resulting Thue equations have to be dealt with one at a time and the number fields associated with these equations may be related, but are generally distinct. Further, there are good reasons to be prepared for extremely large coefficients of a Thue equation whose corresponding field $\mathbb{Q}(\alpha)$ has a fundamental unit of exceptional size. So, although there are very good, efficient and almost certified ways to actually solve any Thue equation (at least in principle), it is conceivable that, if all the bad things mentioned above should happen simultaneously, even our modern, sophisticated computational equipment would break its back over a seemingly insignificant elliptic equation.

We had always considered the pessimistic picture just painted to be rather farfetched. Granted, with sufficient effort, it should be possible to construct such a monstrosity, but we had never come across an unsolvable elliptic equation and never expected to do so in the natural course of events. This until the day we tried to solve the Ochoa curve equation, which in its original form is

$$3Y^2 = 2X^3 + 385X^2 + 256X - 58195. \tag{1.2}$$

In [Guy 1990] Richard Guy explains how he became interested in this equation. Apparently, the problem of determining, with justification, the integer solutions of (1.2), was proposed for but not used at the 28th IMO (International Mathematical Olympiad) in Havana. Guy was intrigued how such a problem came to be asked, and tried to imagine how an IMO contestant might attack it. The construction used by the proposer, Juan Ochoa Melida, was based on “completing the square”, and turned out to be a special case of a method attributed to A. Néron, who mentions it in his thesis.

Realizing that he could not be sure of having discovered all integer solutions by this and other elementary methods, Guy contacted one of us (de Weger), asking whether the method described in [Tzanakis and de Weger 1989] could solve the problem. We soon found that the complete solution of (1.2) raises difficulties, and, since solving individual equations is usually of no great interest, we postponed further investigations. When a new method of solving elliptic equations was considered in [Stroeker and Tzanakis 1994], an approach in which the estimation of linear forms in elliptic logarithms plays a crucial role, we realized that the Ochoa curve might serve as an illustration of this new method.

Instead of the original equation, we prefer to consider the Weierstraß representation (1.1) of the Ochoa curve,

$$y^2 = x^3 - 440067x + 106074110. \tag{1.3}$$

This is equation (1.1) with $a = -3 \cdot 383^2$ and $b = 2 \cdot 5 \cdot 73 \cdot 145307$. The simple linear transformation $(x, y) = (6X + 385,\ 18Y)$ maps (1.2) to (1.3).

In Section 2, we shall try to convince the reader that any attempt to solve the Ochoa equation by adopting the traditional Thue approach is doomed to failure. Section 3 gives an alternative approach: instead of focusing merely on the Weierstraß equation (1.3), we incorporate knowledge of the group structure of the elliptic curve in the solution process. This allows us to prove the following result:

Theorem. *The complete set of solutions* (x,y) *of* (1.3), *with* $x,y \in \mathbb{Z}$ *and* $y>0$, *is*

$$\{(-761,504),\ (-745,4520),\ (-557,13356),\ (-446,14616),\ (-17,10656),\ (91,8172),\ (227,4228),\ (247,3528),\ (271,2592),\ (455,200),\ (499,3276),\ (523,4356),\ (530,4660),\ (599,7576),\ (751,14112),\ (1003,25956),\ (1862,75778),\ (3511,204552),\ (5287,381528),\ (23527,3607272),\ (64507,16382772),\ (100102,31670478),\ (1657891,2134685628).\}$$

In [Stroeker and Tzanakis 1994] we describe how an explicit lower bound for linear forms in elliptic logarithms that was recently obtained by S. David [1992] may be applied to solve elliptic equations. Here it is proper to credit Don Zagier, who came up with the idea of using elliptic logarithms to search for integral points on elliptic curves [Zagier 1987]. For more examples, see also [Gebel et al.].

2. SOME RELATED THUE EQUATIONS

We now explain why it is almost impossible to solve (1.3) by the Thue approach. Briefly, not only is the discriminant of $f(x)$ large and highly composite, as Richard Guy suggested, but also the fundamental units of the cubic field defined by a root of $f(x)=0$ are extraordinarily large.

Let ψ be a zero of the right-hand side of (1.3). We calculated the particulars of the number field $\mathbb{K}=\mathbb{Q}(\psi)$ using Pari-GP 1.38 [Batut et al. 1992], and assisted by Maple V3 [Char et al. 1991] for the checking of symbolic calculations. We found that $\mathbb{K}$ is also generated by the number θ defined by

$$\theta^3-\theta^2-8150\theta-212700=0, \tag{2.1}$$

$$\psi=-1085-\tfrac{26}{5}\theta+\tfrac{1}{5}\theta^2, \tag{2.2}$$

and that $\mathbb{K}$ has discriminant $1014134613 = 3\cdot 79\cdot 311\cdot 13759$. Further, setting

$$\omega=\tfrac{19}{30}\theta+\tfrac{1}{30}\theta^2, \tag{2.3}$$

we established that $\{1,\theta,\omega\}$ is an integral basis for $\mathbb{K}$, that the class group is trivial, and that a complete set of fundamental units is given by $\{\varepsilon_1,\varepsilon_2\}$, these numbers being defined in the sidebar below.

The large coefficients occurring in these unit expressions will give rise to coefficients of similar sizes at all stages of the present process of deriving Thue equations, as we shall see below. This will present us with enormous technical difficulties.

We let $(x,y)\in\mathbb{Z}^2$ be a solution to (1.3) and factor the equation over the field $\mathbb{K}$ as follows:

$$y^2=(x-\psi)(x^2+\psi x+\psi^2-3\cdot 383^2). \tag{2.4}$$

Let π be a prime in $\mathbb{K}$ dividing the greatest common divisor of the two factors in the right-hand side of (2.4). Then π divides

$$(x^2+\psi x+\psi^2-3\cdot 383^2)-(x+2\psi)(x-\psi)=3(\psi^2-383^2).$$

$$\begin{aligned}\varepsilon_1 = &-10206011481624738138599255396089544564125332455775-398696619893921487609546794448189124208538086359\,\theta\\ &-146398174838249319483906766573385628599646205307\,\omega,\\ \varepsilon_2 = &-2193154108081847288660158310454770017214394875593412406-856753033614558249751466666771678612159738253596986648\,\theta\\ &-31459278596762653698353622953979430870421158068590645\,\omega.\end{aligned}$$

Elements of a complete set of fundamental units of $\mathbb{K}=\mathbb{Q}(\psi)$, for ψ a root of the polynomial defining the Ochoa curve in Weierstraß form (1.3). The quantities θ and ω are defined in (2.1)–(2.3). The signs are chosen in such a way that $\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(\varepsilon_1)=\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(\varepsilon_2)=1$.

$$\begin{aligned}
\alpha_1 &= 22122052781614 + 864209912843\,\theta + 317368021099\,\omega\\
\alpha_2 &= 13449470246026409265104 22 + 912636225461111797314 5\,\theta - 5555257414014147550952\,\omega\\
\beta_1 &= -3743922028693350319 - 114915498960562510\,\theta + 37711773857425364\,\omega\\
\beta_2 &= -4151301567440027000178268598087676749 - 1621701000511899263930668277711421 73\,\theta\\
&\qquad - 5954754938014574393539963778223835 3\,\omega\\
\gamma_1 &= -2662607574182375754286414045995925016988 4 - 1040144469601822148169489088698257304264\,\theta\\
&\qquad - 3819326383010734063353386514565529366 95\,\omega\\
\gamma_2 &= 277495606323 + 10840332727\,\theta + 3980482519\,\omega\\
\gamma_3 &= 897605812664176863637051225 63 + 27549762991504448399865156 84\,\theta - 904109383173122142766939854\,\omega\\
\delta_1 &= 697669173088475199601257 6 + 473415048400256558585530\,\theta - 2881698517065343121911 7\,\omega\\
\delta_2 &= 2672572904273791547 7 + 181351889926422386\,\theta - 110389704347996444\,\omega\\
\zeta_1 &= -278293 - 1884\,\theta + 1152\,\omega\\
\zeta_2 &= -128563464484753 - 3946111739544\,\theta + 1294993929312\,\omega\\
\eta_1 &= -4889037142024122492 53 - 190989652183944793 80\,\theta - 701298558792919957 2\,\omega\\
\eta_2 &= -155047559921770455434857643417 - 4759011425578929813689745912\,\theta + 1561762897865462910564655032\,\omega
\end{aligned}$$

$\mathbb{K}$-prime factors of the rational prime factors of Norm$(383-\psi)$ and Norm$(383+\psi)$ (norms with respect to $\mathbb{K}/\mathbb{Q}$). We have Norm$(\alpha_1) = 2$, Norm$(\alpha_2) = 4$, Norm$(\beta_1) =$ Norm$(\beta_2) = 3$, Norm$(\gamma_1) =$ Norm$(\gamma_2) =$ Norm$(\gamma_3) = 7$, Norm$(\delta_1) =$ Norm$(\delta_2) = 79$, Norm$(\zeta_1) =$ Norm$(\zeta_2) = 311$, and Norm$(\eta_1) =$ Norm$(\eta_2) = 13759$.

Note that $\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(383-\psi) = -2^8 \cdot 79 \cdot 311$, and $\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(383+\psi) = -2^2 \cdot 3^4 \cdot 7^2 \cdot 13759$. We shall study the prime ideal factorization in $\mathbb{K}$ of the relevant rational primes. Using Pari we found:

$$\begin{aligned}
(2) &= (\alpha_1)(\alpha_2), & (79) &= (\delta_1)^2(\delta_2),\\
(3) &= (\beta_1)^2(\beta_2), & (311) &= (\zeta_1)^2(\zeta_2),\\
(7) &= (\gamma_1)(\gamma_2)(\gamma_3), & (13759) &= (\eta_1)^2(\eta_2),
\end{aligned}$$

where $\alpha_1, \ldots, \eta_2$ are given in the sidebar above. Further, we found

$$\begin{aligned}
(383-\psi) &= (\alpha_2)^4(\delta_1)(\zeta_1),\\
(383+\psi) &= (\alpha_2)(\beta_1)^3(\beta_2)(\gamma_1)(\gamma_3)(\eta_1).
\end{aligned}$$

This shows that we can restrict π to the set

$$\mathcal{P} = \{\alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_3, \delta_1, \zeta_1, \eta_1\}.$$

Returning to (2.4), we obtain the ideal equation

$$(x-\psi) = (\alpha)(\xi)^2, \tag{2.5}$$

where (α) is the square-free part of $(x-\psi)$. Clearly, from (2.4) and (2.5) it follows that (α) is also the square-free part of the second factor of the right-hand side of (2.4). Hence the prime divisors of α can only be those belonging to the set $\mathcal{P}$ above.

Assume $\delta_1 \mid \alpha$. Since α is square-free and $\delta_2 \nmid \alpha$, 79 divides $\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(x-\psi)$ to an odd power, which contradicts $\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(x-\psi) = y^2$. Hence $\delta_1 \nmid \alpha$, and similarly we can show that $\zeta_1 \nmid \alpha$ and $\eta_1 \nmid \alpha$.

Assume $\beta_1 \mid \alpha$. Then also $\beta_2 \mid \alpha$, because if $\alpha = \beta_1\chi$, then 3 divides $y^2 = \mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(x-\psi) = \mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(\alpha) \times \Box = 3\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(\chi) \times \Box$ to an even power, and hence $\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(\chi) \equiv 0 \pmod 3$, and $\beta_1 \nmid \chi$ as α is square-free. Similarly we prove that $\beta_1 \mid \alpha$ if and only if $\beta_2 \mid \alpha$, and $\gamma_1 \mid \alpha$ if and only if $\gamma_3 \mid \alpha$.

It follows that

$$\alpha = \pm\varepsilon_1^a\varepsilon_2^b\alpha_2^p(\beta_1\beta_2)^q(\gamma_1\gamma_3)^r \tag{2.6}$$

for $a, b, p, q, r \in \{0, 1\}$. Since $\varepsilon_1, \varepsilon_2, \alpha_2, \beta_1, \beta_2, \gamma_1, \gamma_3$ all have positive norm, it follows from

$$y^2 = \mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(\alpha)\,\mathrm{Norm}_{\mathbb{K}/\mathbb{Q}}(\xi^2)$$

that the ±-sign in (2.6) may be dropped. Hence we have to consider 32 cases for α, many of which, hopefully, will turn out to be impossible or trivial. For example, $q = r$ for all known solutions. However, we do not intend to follow through to the end each and every case, since our aim is to show the reader the seemingly insurmountable difficulties we encounter on our way, and this can be done most convincingly by means of no more than a few well-chosen cases.

The general argument continues as follows. From the ideal equation (2.5) and the fact that $\mathbb{K}$ has class number 1, we may write $x - \psi = \alpha\xi^2$, where α takes the form (2.6) without the ±-sign.

Now take a fixed α, and write it as $\alpha = a_1 + a_2\theta + a_3\omega$. Further, express ξ in terms of the integral basis $\{1, \theta, \omega\}$ as $\xi = u + v\theta + w\omega$, with variable coefficients $u, v, w \in \mathbb{Z}$. Next write out the equation $x - \psi = \alpha\xi^2$ in terms of the integral basis as

$$(x + 1085) + 9\theta - 6\omega = b_1 + b_2\theta + b_3\omega,$$

where $b_1 = b_1(u, v, w)$, $b_2 = b_2(u, v, w)$ and $b_3 = b_3(u, v, w)$ are given by

$$\begin{aligned}
b_1 = {} & a_1u^2 + 14180a_3uv + (14180a_2 + 18434a_3)uw \\
& + (212700a_2 + 141800a_3)v^2 \\
& + (14180a_1 + 283600a_2 + 4041300a_3)vw \\
& + (9217a_1 + 2020650a_2 + 5526655a_3)w^2, \\
b_2 = {} & a_2u^2 + (2a_1 - 38a_2 + 518a_3)uv \\
& + (518a_2 + 818a_3)uw \\
& + (-19a_1 + 8131a_2 + 7349a_3)v^2 \\
& + (518a_1 + 14698a_2 + 150522a_3)vw \\
& + (409a_1 + 75261a_2 + 222496a_3)w^2, \\
b_3 = {} & a_3u^2 + (60a_2 + 40a_3)uv \\
& + (2a_1 + 40a_2 + 570a_3)uw \\
& + (30a_1 + 30a_2 + 8170a_3)v^2 \\
& + (40a_1 + 16340a_2 + 35940a_3)vw \\
& + (285a_1 + 17970a_2 + 98622a_3)w^2.
\end{aligned}$$

Equating coefficients gives

$$b_1 = x + 1085, \qquad b_2 = 9, \qquad b_3 = -6,$$

and hence

$$2b_2 + 3b_3 = 0, \tag{2.7}$$

which is a quadratic equation homogeneous in the variables u, v, w. If this equation has a solution in rational integers, the discriminant of the left-hand side of expression (2.7), seen as a form in one of the variables, say w for instance, must be a perfect square. This gives an equation of type

$$p_0u^2 + p_1uv + p_2v^2 = z^2,$$

which can be treated further by factorization over the appropriate quadratic number field, or possibly over $\mathbb{Q}$ itself. All this will lead to expressions for u, v, w as binary quadratic forms, which, when substituted into $b_2 = 9$ yield a quartic Thue equation.

To get a feeling for this process, we consider the simplest case first.

The case $\alpha = 1$

When $\alpha = 1$, equation (2.7) gives

$$1673w^2 + (6u + 1156v)w + (4uv + 52v^2) = 0,$$

and hence

$$(6u + 1156v)^2 - 4 \cdot 1673(4uv + 52v^2) = z^2,$$

which implies

$$(18u - 3224v)^2 - (3z)^2 = 2^7 \cdot 7^2 \cdot 239v^2.$$

It can be easily seen that the only primes dividing both expressions $18u - 3224v \pm 3z$ belong to the set $\{2, 3, 7, 239\}$. This gives us a number of cases to consider, one of which we shall follow through (one in which a solution occurs), namely

$$\begin{aligned}
18u - 3224v - 3z &= 3346A^2, \\
18u - 3224v + 3z &= 7B^2, \\
8v &= AB.
\end{aligned}$$

We obtain

$$\begin{aligned}
u &= \tfrac{1673}{18}A^2 + \tfrac{403}{18}AB + \tfrac{7}{36}B^2, \\
v &= \tfrac{1}{8}AB, \\
z &= -\tfrac{1673}{3}A^2 + \tfrac{7}{6}B^2.
\end{aligned}$$

Substitution of these values into

$$w = \frac{-(6u + 1156v) \pm z}{2 \cdot 1673},$$

where only the +-case is considered (the other case is easily seen to be impossible) leads to

$$w = -\tfrac{1}{3}A^2 - \tfrac{1}{12}AB.$$

Again by substitution—in this case the expressions for u, v, w are plugged into the equation $b_2 = 9$ (or, equivalently, into $b_3 = -6$)—we arrive at the Thue equation

$$26176A^4 + 14040A^3B + 1581A^2B^2 + 28AB^3 = 5184.$$

This is a reducible Thue equation, easily seen to possess the single solution (up to sign) $A = -2$, $B = 92$. Via

$$u = -2102, \quad v = -23, \quad w = 14, \quad z = 7644,$$

this solution ultimately leads to the largest integral point $(x, y) = (1657891, 2134685628)$ on the Ochoa curve (see Theorem in Section 1). All this is not terribly complicated, but note that we took only one of several paths, each of which should be followed to the very end for fear of missing solutions.

A more difficult case: $\alpha = \varepsilon_2\alpha_2\beta_1\beta_2\gamma_1\gamma_3$

Here we obtain a Thue equation that is far from trivial. In fact, we know in advance that this choice will lead to a solution, namely the integral point $(x, y) = (751, 14112)$ on (1.3). For the sake of simplicity we change α slightly to become $\alpha = \varepsilon_2^{-1}\alpha_2\beta_1\beta_2\gamma_1\gamma_3$, which is permitted, as α is essentially determined up to a square. Among those expressions equal to α up to the square of a unit, this choice has the "smallest" coefficients a_1, a_2, a_3, namely:

$$\alpha = -2730673131953769919100100626448281153264694871637 6 - 8381495743013428455862116992237168787155552135317\,\theta \\ + 2750552144022919245142067916394363811146841891 36\,\omega.$$

We obtain the following quadratic forms:

$$\begin{aligned} b_1 = {} & -27306731319537699191001006264482811532646948716376\,u^2 + 390028294022449948961145230544720788420622180194848 0\,uv \\ & - 6814593141301192213917593897910935090718440936262036\,uw - 1392715850516506283600727053704125012607357211624411 00\,v^2 \\ & + 4866719685810769490026200003222418726621088951812039 20\,vw - 4251578039316887183011714087280923120036124012377135 62\,w^2 \\ b_2 = {} & -8381495743013428455862116992237168787155552135317\,u^2 + 1197148222447628466486331501107636637433034936817 42\,uv \\ & - 2091663141070207997610365046368263834228443393809 58\,uw - 4274785522930559039577562495604650556904048280690919\,v^2 \\ & + 1493785171566011973636277389095895590087218879715695 8\,vw - 1304974323753193883407033594484158887337099793508706 5\,w^2 \\ b_3 = {} & 2750552144022919245142067916394363811146841891 36\,u^2 - 3928676588198889375460443028784555747834576055358 0\,uv \\ & + 6864202659817728476764739073656443902145400496208 8\,uw + 1402854674851553762183452948782999381366094799690330\,v^2 \\ & - 4902148891247078297478147324373502722256250082186980\,vw + 4282529078519458974820591184636701180969531845156942\,w^2 \end{aligned}$$

Setting the discriminant of $2b_2 + 3b_3$ with respect to w equal to a square, dividing through by the common factor 84^2, adjusting z accordingly, and completing the square, we find

$$(pu + qv)^2 + rv^2 = pz^2, \tag{2.8}$$

with

$$\begin{aligned} p &= 2609469946884159955900017189857006773, \\ q &= -667983597301133446142480918162530555 00, \\ r &= 16827808558102223166576378839076919623915428996448 64. \end{aligned}$$

One can factor (2.8) over $\mathbb{Q}(\sqrt{-r})$. There is a finite set of integral elements π in this field such that (2.8) is equivalent to the set of equations

$$pu + qv + v\sqrt{-r} = \pi(A + B\sqrt{-r})^2 \quad \text{for } A, B \in \mathbb{Z}.$$

We feel that in the determination of this complete set of equations we have come to a major bottleneck of the method. The reason is that this imaginary quadratic field is incredibly complicated to handle. For example, we tried to compute the class number with Pari, but gave up after a while.

Therefore, we restrict ourselves to the precise tracing of the known solution given by $x = 751$. We computed $751 - \psi = \alpha\xi^2$ with $\xi = \alpha_2^2\beta_1\gamma_1 = u + v\theta + w\omega$, where

$$\begin{aligned} u &= -5026852980896253432, \\ v &= -196373411473862169, \\ w &= -72106728755792390. \end{aligned}$$

Now we simply force this solution to match the solution $A = 1$, $B = 0$ of the final Thue equation, which means at most a linear transformation of the variables. In other words, we take

$$\begin{aligned}\pi &= pu + qv + v\sqrt{-r}\\ &= 678494116368502515458751386456138255888 4564\\ &\qquad - 196373411473862169\sqrt{-r},\end{aligned}$$

and write out, this time for unknown u, v, w, A, B:

$$pu + qv + v\sqrt{-r} = \pi(A + B\sqrt{-r})^2.$$

This yields expressions

$$\begin{aligned}u &= u_1A^2 + u_2AB + u_3B^2,\\ v &= v_1A^2 + v_2AB + v_3B^2,\\ z &= z_1A^2 + z_2AB + z_3B^2,\end{aligned}$$

where

$$\begin{aligned}&u_1 = -5026852980896253432, && u_2 = 34736781785204147769094463412620482808457 8784,\\ &u_3 = 845909196122476448427675952846967410853546184436986079167666094117324 8,\\ &v_1 = -196373411473862169, && v_2 = 1356988232737005030917502772912276511776912 8,\\ &v_3 = 33045341741835871127629066980936859787718010583881557799336858475001 6,\\ &z_1 = 6519943582905173680771260, && z_2 = 10971636242275535344670287691303328,\\ &z_3 = 7380572336078642221063263616167596178086 40.\end{aligned}$$

Solving equation (2.7) for w, we thus find $w = w_1A^2 + w_2AB + w_3B^2$, with

$$\begin{aligned}&w_1 = -72106728755792390, && w_2 = 4982751060253642907539610288312257567100720,\\ &w_3 = 1213398227253478850658154751554404694730901914586529446332613188915 20.\end{aligned}$$

Finally we substitute these expressions for u, v, w into the equation $b_3 = -6$, which gives the following Thue equation

$$A^4 + e_1A^3B + e_2A^2B^2 + e_3AB^3 + e_4B^4 = 1 \tag{2.9}$$

with coefficients

$$\begin{aligned}e_1 &= 27594236293804121976499441 6,\\ e_2 &= 72708984355867699445822358986209399390764659032344 96,\\ e_3 &= -46435052565917197638502267565129693732437899717209825163909008258319265948774 4,\\ e_4 &= 28317514086813842311869014435364451797678963938922601932308438463758587388002960945674175767198931394 56.\end{aligned}$$

Clearly, this Thue equation has the desired solution $A = 1$, $B = 0$. But, of course, the point is to find all solutions, not just one. The linear substitution

$$\begin{aligned}C &= A + 66812276206875247047658184B,\\ D &= -43466290552701157871808 40B\end{aligned}$$

transforms (2.9) into the apparently much more friendly Thue equation

$$C^4 - 2C^3D - 1125C^2D^2 - 12986CD^3 + 11041D^4 = 1. \tag{2.10}$$

Hence, the quartic field $\mathbb{F}$ generated by a zero of the left-hand side of (2.9) is also generated by a zero of the polynomial

$$x^4 - 2x^3 - 1125x^2 - 12986x + 11041. \tag{2.11}$$

In fact—at least Pari tells us so—amongst all polynomials sharing this property, polynomial (2.11) has the simplest form. The field discriminant of the quartic field $\mathbb{F}$ is $28622935317312 = 2^6 \cdot 3^3 \cdot 7^2 \cdot 79 \cdot 311 \cdot 13759$. However, we could not persuade Pari to come up with a set of fundamental units of this totally real field, but Henri Cohen informed us that Pari would have produced the required units if we had increased the number of digits precision sufficiently and persevered a little bit longer. Nevertheless, we still believe the friendly appearance of the Thue equation (2.10) to be misleading, an opinion supported by the fact that the regulator of the field $\mathbb{F}$ is approximately 51974.47, which is rather large. Possibly we have stumbled upon yet another major bottleneck of the Thue approach.

We could have treated (2.8) in other ways. For instance, it can be rewritten as

$$(pu+qv)^2 - pz^2 = -rv^2$$

and factored over $\mathbb{Q}(\sqrt{p})$, or as

$$(pz)^2 - prv^2 = p(pu+qv)^2,$$

and factored over $\mathbb{Q}(\sqrt{pr})$. However, we fail to see any advantage in doing so, because working in real quadratic fields usually is more complicated than working in imaginary quadratic fields of comparable absolute discriminant. Moreover, the resulting Thue equations are exactly the same—we checked this by following through the procedure described above for the particular solution associated with $x = 751$, working over these two real quadratic fields instead of the imaginary one.

Here we finally lost faith and gave up.

3. AVOIDING THUE EQUATIONS

We have learned from the previous section that in the present state of affairs it seems very unlikely that the Thue approach ultimately leads to the complete solution of our problem. Although the Ochoa curve was chosen for this very reason, it would be rather unsatisfactory to leave it at this. One should discard Thue and look for alternative ways. Luckily, there is such an alternative way to effectively and unconditionally solve the Ochoa problem. We shall refrain from giving a detailed description of the method we have in mind, in which elliptic logarithms play a decisive role, because such an account can be found in [Stroeker and Tzanakis 1994]. We feel that an outline of its major points should suffice, in addition of course to a full description of the way in which the relevant constants were obtained. We shall follow the notation of [Stroeker and Tzanakis 1994] very closely.

Our first task is to obtain complete information about the Mordell–Weil group $E(\mathbb{Q})$ of the elliptic curve given by (1.2) or by the standard Weierstraß equation (1.3). Although it is generally well understood how this group $E(\mathbb{Q})$ can be calculated, the details may cause considerable difficulties. See for instance [Cassels 1991; Cremona 1992; Knapp 1992; Silverman 1986]. But we are fortunate in this case.

According to the Mordell–Weil theorem, we have the following isomorphism

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

where r is the rank of the curve $E/\mathbb{Q}$. The torsion subgroup $E_{\text{tors}}(\mathbb{Q})$ is always easily found, because it is finite and only a few possibilities need to be checked. In our case $E_{\text{tors}}(\mathbb{Q})$ is trivial. Obtaining the rank r and a set of generators for $E(\mathbb{Q})/E_{\text{tors}}(\mathbb{Q})$ is much harder [Cremona 1992]. We used the program Apecs 2.99 [Connell 1994] to search for a set of independent points of infinite order, which quickly established a lower bound of 4 for the rank. To obtain an upper bound, we assumed the truth of the standard conjectures of Birch–Swinnerton-Dyer and Taniyama–Weil, as well as the Generalized Riemann Hypothesis, so that the method of [Mestre 1986] could be applied. The conditional upper bound thus obtained confirmed our initial guess: we could be reasonably sure that $r = 4$. At the workshop on "Constructive Methods for Diophantine Equations", held in Rotterdam in June of 1994, we asked John Cremona to apply his rank algorithm [Cremona 1992, p. 68] (which, incidentally, is based on the technique originally used by Birch and Swinnerton-Dyer in their studies) to the Ochoa curve. His findings confirmed unconditionally the rank assumption.

Next a basis for $E(\mathbb{Q})/E_{\text{tors}}(\mathbb{Q})$ is needed. Again, Apecs offered help here. It found four independent points P_1, P_2, P_3, P_4, that minimize the canonical height-pairing Grammian $|\langle P_i, P_j\rangle|$. We recall that this height-pairing is defined by

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

with canonical height function $\hat{h}$. Further, Apecs succeeded in proving that these four points correspond to the successive minima. A theorem of Minkowski [Cassels 1978, p. 257] then implies that these four points constitute a free basis of $E(\mathbb{Q})$. Apecs found the following generators

$$P_1 = [247, 3528], \qquad P_2 = [499, 3276],$$
$$P_3 = [751, 14112], \qquad P_4 = [-761, 504],$$

where the coordinates correspond to the Weierstraß equation (1.3). From here on coordinates shall always be relative to this equation.

Let $P \in E(\mathbb{Q})$ with coordinates $x(P)$, $y(P) \in \mathbb{Z}$. Then

$$P = m_1P_1 + m_2P_2 + m_3P_3 + m_4P_4, \tag{3.1}$$

for $P_1, \ldots, P_4$ as just given and $m_1, \ldots, m_4 \in \mathbb{Z}$. Further, let $\gamma > \gamma' > \gamma''$ be the three real zeros of the right-hand side of (1.3), which we shall denote by $f(x)$, and define

$$E_0(\mathbb{Q}) = \{(x,y) \in E(\mathbb{Q}) \mid x \geq \gamma\} \cup \{\underline{0}\},$$

where $\underline{0}$ is the group identity of $E(\mathbb{Q})$.

If $P \notin E_0(\mathbb{Q})$, then

$$-761.1957 \approx \gamma'' < x(P) < \gamma' \approx 306.4170,$$

so such integral points are easily found by a simple direct search.

Now suppose that $P \in E_0(\mathbb{Q})$, and for convenience assume that

$$x(P) \geq 1524 > 2\max\{|\gamma|, |\gamma'|, |\gamma''|\} + 1$$

(see [Stroeker and Tzanakis 1994, Inequality 2]).

Let $\omega := 2\int_\gamma^\infty dt/\sqrt{f(t)} \approx 0.2850385$ be the real period of the Weierstraß $\wp$-function associated with (1.3). The isomorphism

$$\varphi : E_0(\mathbb{R}) \to \mathbb{R}/\mathbb{Z} \quad \text{(circle group)},$$

explicitly given by

$$\varphi(R) \equiv \begin{cases} 0 \pmod 1 & \text{if } R = \underline{0}, \\ \dfrac{1}{\omega}\displaystyle\int_{x(R)}^\infty \frac{dt}{\sqrt{f(t)}} \pmod 1 & \text{if } y(R) \geq 0, \\ -\varphi(-R) \pmod 1 & \text{if } y(R) \leq 0 \end{cases}$$

(see also Eq. (5) of [Stroeker and Tzanakis 1994]), associates with each point R of $E_0(\mathbb{R})$ a unique real value between $-\frac{1}{2}$ and $\frac{1}{2}$, which in a sense measures the distance between R and the group identity $\underline{0}$. This distance, which is essentially an elliptic logarithm, can be explicitly calculated for each $R \in E_0(\mathbb{Q})$ by a very fast algorithm of Zagier using the binary expansion of $\varphi(R)$ [Zagier 1987, p. 430]. So, as $x(P) \in \mathbb{Z}$, saying that $|x(P)|$ is very large is equivalent to saying that $\varphi(P)$ is very close to $\varphi(\underline{0}) = 0$. In other words, if $|\varphi(P)|$ cannot be too small, then $|x(P)|$ cannot be too large. Referring to (3.1), what we want is an upper bound for

$$M := \max_{1 \leq i \leq 4} |m_i|,$$

and we shall deduce such a bound by combining upper and lower bounds for $|\varphi(P)|$ in terms of M. In order to express $\varphi(P)$ in terms of $m_1, \ldots, m_4$, we have to adapt (3.1) slightly, because, unlike P_2 and P_3, neither P_1 nor P_4 belongs to $E_0(\mathbb{Q})$. Writing

$$R_1 = -P_1 - P_4 = [523, 4356],$$
$$R_2 = P_2 = [499, 3276],$$
$$R_3 = P_3 = [751, 14112],$$
$$R_4 = -P_1 + P_4 = [530, 4660],$$

we see from the value of $\gamma \approx 454.7786$ that $R_1, \ldots, R_4 \in E_0(\mathbb{Q})$. Now (3.1) may be rewritten as

$$2P = (-m_1-m_4)R_1 + 2m_2R_2 + 2m_3R_3 + (-m_1+m_4)R_4.$$

Since $2P \in E_0(\mathbb{Q})$, we deduce that

$$\varphi(2P) = 2\varphi(P) = m_0 + (-m_1-m_4)\varphi(R_1) + 2m_2\varphi(R_2) + 2m_3\varphi(R_3) + (-m_1+m_4)\varphi(R_4)$$

for an integer m_0—indeed, $\varphi(R)$ is uniquely determined modulo 1. It follows from this equation that

$$|m_0| < |m_1+m_4|+2|m_2|+2|m_3|+|m_1-m_4| \le 8M+1,$$

and consequently, we may take $M' = 8M+1$ in [Stroeker and Tzanakis 1994, Eq. (14)]. An application of S. David's lower bound for $|\varphi(P)|$ (see David's Theorem in [Stroeker and Tzanakis 1994, Appendix]) yields

$$|\omega\varphi(P)| > \exp(-c_4(\log M' + 1)(\log\log M' + 1 + h_E)^6), \tag{3.2}$$

where $h_E \approx 35.6882$ is the naive height of

$$j_E = \frac{3156404426880769}{198770384148},$$

the j-invariant of $E/\mathbb{Q}$, and

$$c_4 = 2 \cdot 10^{43} \cdot \left(\frac{2}{e}\right)^{50} \cdot 6^{150} \cdot h_E^5.$$

On the other hand, an upper bound for $|\varphi(P)|$ in terms of M follows almost at once from the definition of φ; we simply reproduce [Stroeker and Tzanakis 1994, (12)]:

$$|\omega\varphi(P)| \le 4\sqrt{2}\exp(c_3 - c_1 M^2).$$

Here $c_1 = 0.4795$ and $c_3 = 4.9399$: see [Stroeker and Tzanakis 1994, Inequalities 1 and 3].

Combining this upper bound with (3.2), there emerges the following inequality for M [Stroeker and Tzanakis 1994, (16)]:

$$\begin{aligned} c_1 M^2 < c_3 &+ \log(4\sqrt{2}) \\ &+ c_4\left(\log(8M+1)+1\right) \\ &\qquad \times \left(\log\log(8M+1)+1+h_E\right)^6. \end{aligned}$$

From this we deduce that $M \le 0.5551 \times 10^{87}$. Applying the reduction process described in [de Weger 1989] or in [Stroeker and Tzanakis 1994] three times reduces the upper bound for M successively to 41, 9 and 8. For this reduction process we need the values of $\varphi(R_i)$, …, $\varphi(R_4)$ to a great precision. We programmed Zagier's algorithm as described in [Zagier 1987] in the very fast programming language Ubasic 8.30 to calculate these values, and subsequently applied the integer LLL–algorithm provided by Pari to obtain the reduced bases. The first reduction step required 450 decimal digits precision and the next only 25 decimal digits.

A final search for all integral points P of (1.3), subject to

$$x(P) \ge 1524$$

and (3.1) with $|m_i| \le 8$, revealed no points other than the ones listed in the Theorem (Section 1). Also, the remaining direct searches did not produce any unexpected points. The connections between the 23 integer points of the Theorem and the m_i-values of (3.1) are given in Table 1.

$x(P)$	$y(P)$	m_1	m_2	m_3	m_4
−761	504	0	0	0	1
−745	4520	−1	−1	0	0
−557	13356	1	0	1	0
−446	14616	0	−1	1	1
−17	10656	−1	1	0	0
91	8172	0	0	−1	−1
227	4228	−1	0	1	0
247	3528	1	0	0	0
271	2592	0	−1	0	1
455	200	−1	1	−1	−1
499	3276	0	1	0	0
523	4356	−1	0	0	−1
530	4660	−1	0	0	1
599	7576	0	−1	−1	0
751	14112	0	0	1	0
1003	25956	1	−1	0	1
1862	75778	−1	2	0	−1
3511	204552	0	1	−1	0
5287	381528	−1	0	−1	−1
23527	3607272	−1	1	1	−1
64507	16382772	1	1	0	−1
100102	31670478	1	1	0	1
1657891	2134685628	0	0	0	−2

TABLE 1. Integer points $P = (x(P), y(P))$ on the Ochoa curve (1.3), and the values of m_1, …, m_4 in (3.1) that lead to each point.

4. CONCLUSION

In contrast to our findings of the previous section, all values and constants directly related to the curve $E/\mathbb{Q}$ and its group $E(\mathbb{Q})$ are rather small. Only the initial M-bound is large, but this is inherent in the diophantine approximation technique employed and does not reflect on the curve. So, where the Ochoa curve is extremely awkward with respect to the Thue method, it is almost—but not quite—a push-over for the elliptic logarithm approach.

Conversely, there are elliptic equations for which the elliptic logarithm approach fails as a practical method for finding integral points. This is the case when a full set of generators for the Mordell–Weil group is very hard to find, because some of its generators have exceptionally large heights. In those cases the Thue approach could be more practical. Examples should be easy to find; we refer to [Bremner and Cassels 1984; Bremner 1989; Stroeker and Top 1994]. From this last paper we take the following two examples of rank 1:

$$y^2 = (x+p)(x^2+p^2) \quad \text{with } p = 167 \text{ and } p = 223.$$

For $p = 167$, the canonical height of a generator is as large as 47.3231 approximately, and when $p = 223$, the generator's canonical height is approximately 25.7153. So the elliptic logarithm approach, short of being a complete failure, requires an enormous effort in these cases. In contrast, the Thue approach seems straightforward, especially for $p = 223$; the Thue equations to be solved are

$$E^4 - 4E^2F^2 - 4F^4 = -p,$$
$$E^4 + 4pE^2F^2 - 4p^2F^4 = 1$$

(see [de Weger 1994]). Furthermore, the fundamental units of the associated quartic fields are easy to compute using Pari.

ACKNOWLEDGEMENT

We are grateful for the referee's valuable suggestions.

REFERENCES

[Batut et al. 1992] C. Batut, D. Bernardi, H. Cohen and M. Olivier, *User's Guide to Pari-GP.* This manual is part of the program distribution, available by anonymous ftp from the host pari@ceremab.u-bordeaux.fr.

[Bremner 1989] A. Bremner, "On the equation $Y^2 = X(X^2+p)$", pp. 3–23 in *Number Theory and Applications*, edited by R. A. Mollin, Kluwer, Dordrecht, 1989.

[Bremner and Cassels 1984] A. Bremner and J. W. S. Cassels, "On the equation $Y^2 = X(X^2+p)$", *Math. Comp.* **42** (1984), 257–264.

[Cassels 1978] J. W. S. Cassels, *Rational Quadratic Forms*, London Math. Soc. Monographs **13**, Academic Press, London and New York, 1978.

[Cassels 1991] J. W. S. Cassels, *Lectures on Elliptic Curves*, London Math. Soc. Student Texts **24**, Cambridge Univ. Press, Cambridge and New York, 1991.

[Char et al. 1991] B. W. Char et al., *Maple V Language Reference Manual* and *Maple V Library Reference Manual*, Springer, New York, 1991.

[Connell 1994] I. Connell, "Apecs (Arithmetic of Plane Elliptic Curves)". This large and very useful collection of Maple procedures can be obtained by anonymous ftp from the host math.mcgill.ca.

[Cremona 1992] J. E. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge Univ. Press, Cambridge and New York, 1992.

[David 1992] S. David, "Minorations de formes linéaires de logarithmes elliptiques", *Publications mathématiques de l'Université Pierre et Marie Curie* **106**, Problèmes diophantiens 1991–1992, exposé no. 3.

[Gebel et al.] J. Gebel, A. Pethő and H. G. Zimmer, "Computing integral points on elliptic curves", to appear in *Acta Arithmetica*.

[Guy 1990] R. K. Guy, "The Ochoa curve", *Crux Mathematicorum* **16**(3) (1990), 65–69.

[Knapp 1992] A. W. Knapp, *Elliptic Curves*, Mathematical Notes **40**, Princeton Univ. Press, Princeton, 1992.

[Mestre 1986] J.-F. Mestre, "Formules explicites et minorations de conducteurs de variétés algébriques", *Compositio Mathematica* **58** (1986), 209–232.

[Silverman 1986] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986.

[Stroeker 1984] R. J. Stroeker, "How to solve a diophantine equation", *Amer. Math. Monthly* **91** (1984), 385–392.

[Stroeker and Top 1994] R. J. Stroeker and J. Top, "On the equation $Y^2 = (X+p)(X^2+p^2)$", to appear in *Rocky Mountain J. Math.* (1994).

[Stroeker and Tzanakis 1988] R. J. Stroeker and N. Tzanakis, "On the application of Skolem's p-adic method to the solution of Thue equations", *J. Number Theory* **29** (1988), 166–195.

[Stroeker and Tzanakis 1994] R. J. Stroeker and N. Tzanakis, "Solving elliptic diophantine equations by estimating linear forms in elliptic logarithms", *Acta Arithmetica* **67**.2 (1994), 177–196.

[Tzanakis and de Weger 1989] N. Tzanakis and B. M. M. de Weger, "On the practical solution of the Thue equation", *J. Number Theory* **31** (2) (1989), 99–132.

[de Weger 1989] B. M. M. de Weger, "Algorithms for Diophantine equations", CWI Tract **65**, Stichting Mathematisch Centrum, Amsterdam, 1989.

[de Weger 1994] B. M. M. de Weger, "Solving Elliptic Diophantine Equations by Bilu's Method", Report 9469/B, Econometric Institute, Erasmus University Rotterdam, 17 pp.

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

Roel J. Stroeker, Econometrisch Instituut, Erasmus Universiteit, Postbus 1738, 3000 DR Rotterdam, The Netherlands (stroeker@wis.few.eur.nl)

Benjamin M. M. de Weger, Econometrisch Instituut, Erasmus Universiteit, Postbus 1738, 3000 DR Rotterdam, The Netherlands (dweger@wis.few.eur.nl)

Received July 15, 1994; accepted in revised from October 25