THE DIOPHANTINE EQUATION $b^2X^4 - dY^2 = 1$

MICHAEL A. BENNETT AND GARY WALSH

(Communicated by David E. Rohrlich)

ABSTRACT. If b and d are given positive integers with $b > 1$, then we show that the equation of the title possesses at most one solution in positive integers X, Y. Moreover, we give an explicit characterization of this solution, when it exists, in terms of fundamental units of associated quadratic fields. The proof utilizes estimates for linear forms in logarithms of algebraic numbers in conjunction with properties of Pellian equations and the Jacobi symbol and explicit determination of the integer points on certain elliptic curves.

1. INTRODUCTION

In 1942, W. Ljunggren [13] applied a detailed analysis of units in certain quadratic and biquadratic fields to show that the Diophantine equation

$$(1) \qquad X^4 - dY^2 = 1$$

possesses, for a fixed integer d, at most two solutions in positive integers X and Y. Since, for $d = 1785$, we find the solutions $X = 13$, $Y = 4$ and $X = 239$, $Y = 1352$, this result is, in a certain sense, best possible. On the other hand, the techniques of [13] do not lend themselves to the problem of determining whether, for a given d, equation (1) actually possesses one solution, let alone two. Recently, J.H.E. Cohn [6] (see also [23]), through a clever argument utilizing properties of the Jacobi symbol, was able to sharpen Ljunggren's result. He proved

Theorem 1.1 (Cohn [6]). *Let the fundamental solution of the equation $v^2 - du^2 = 1$ be $a + b\sqrt{d}$. Then the only possible solutions of the equation $X^4 - dY^2 = 1$ are given by $X^2 = a$ and $X^2 = 2a^2 - 1$; both solutions occur in only one case, $d = 1785$.*

The purpose of this paper is to extend the result of Cohn to the Diophantine equation

$$(2) \qquad b^2X^4 - dY^2 = 1$$

where b and d are given integers. Our approach uses properties of the Jacobi symbol, much like [6], but differs essentially from that of Cohn in its appeal to the theory of linear forms in logarithms of algebraic numbers. It should be emphasized that while the main ingredients in our proof are similar to those used by M. Le [11]

to treat equation (2) for large values of b and d, our argument is fundamentally different.

Throughout the paper $d > 1$ will be a squarefree integer, $T + U\sqrt{d}$ will denote the fundamental solution to the Pell equation $X^2 - dY^2 = 1$, and, for $k \geq 1$, integers T_k and U_k will be defined via the equation $T_k + U_k\sqrt{d} = (T + U\sqrt{d})^k$.

We focus our attention on the sequence of integers $\{T_k\}$. Let $b > 1$ denote a positive integer and define the *divisibilty index* $\alpha(b)$ of b in $\{T_k\}$ to be the smallest positive integer k for which $b|T_k$. If, for all k, b fails to divide T_k, we set $\alpha(b) = \infty$. Note that in some instances in the literature (e.g. [12]), $\alpha(b)$ is referred to as the *rank of apparition* of b in T_k.

Our main result is

Theorem 1.2. *If $b, d > 1$ are squarefree integers, then there is at most one index k for which $T_k = bx^2$ for some $x \in \mathbb{Z}$, and, consequently, equation (2) has at most one solution in positive integers X, Y. Moreover, if such a solution exists, then $k = \alpha(b)$.*

The method of proof may be extended to the case $b = 1$ and serves to provide a new proof of the old result of Ljunggren [15] that the Diophantine equation $X^2 - 2Y^4 = -1$ has only the solutions $X = 1$, $Y = 1$ and $X = 239$, $Y = 13$ in integers (see also [5] and [19]). For fixed values of b, we can (much as for the case $b = 1$ discussed in Theorem 1.1) achieve a rather more explicit determination of the values of k in question. We have

Corollary 1.3. *Let $b = 2^r 3^s 5^t 7^u 11^v$ for some integers $r, s, t, u, v \in \{0, 1\}$, not all zero. Then any solution of $T_k = bx^2$ with $x \in \mathbb{Z}$ implies that $k = 1$ unless*

- *(i) $b = 7$, in which case either $k = 1$ or $k = 2$ (but not both),*
- *(ii) $b = 11$ and $d = 2$, in which case $T_3 = 11 \cdot 3^2$,*
- *(iii) $b = 55$ and $d = 1139$, in which case $T_3 = 55 \cdot 423^2$.*

This generalizes work of Z. Cao [4], who treated the case $b = 2$. We could, of course, extend this result to consider more choices for b, but this would involve solving an increasingly large collection of hyperelliptic equations, either by elementary techniques (when they apply), or by the more general method of linear forms in logarithms, as described in e.g. [8] and [18]. Instead, we prove

Theorem 1.4. *If $b > 1$ is a squarefree positive integer, then there exists an effectively computable constant $C = C(b)$ such that if $d > C$ and $T_k = bx^2$ for some $x \in \mathbb{Z}$, then $k = 1$ or $k = 2$. The latter possibility can only occur if the equation $2U^2 - bV^2 = 1$ is solvable in integers U and V.*

Along somewhat different lines, define a sequence of polynomials $P_n(x)$ by

$$P_n(x) = \frac{T_{2n+1}(x)}{x}$$

where $T_m(x)$ denotes the mth Tschebyscheff polynomial, satisfying

$$T_m(x) = \cos(m \arccos x) = x^m + \binom{m}{2} x^{m-2}(x^2 - 1) + \cdots$$

for m a nonnegative integer. We consider the family of hyperelliptic curves defined by

$$y^2 = P_n(x).$$

Since this equation defines a curve of genus $n - 1$, if $n \geq 2$ is fixed, a classic result of Siegel implies the existence of at most finitely many integral points. In our situation, Theorem 1.2 immediately implies

Corollary 1.5. *Let $n \geq 1$ be given. Then the only integral points on the curve*

$$y^2 = P_n(x)$$

are given by $(x, y) = (1, \pm 1)$ and, if $2n + 1 = m^2$ for m an odd integer, by $(x, y) = (0, \pm m)$.

2. A key proposition

The following result is the main theorem of [2]. It relies upon lower bounds for linear forms in logarithms of two algebraic numbers (specifically, those due to Laurent, Mignotte and Nesterenko [10]) in conjunction with a gap principle based on the theory of continued fractions.

Proposition 2.1. *If a, b and c are positive integers, then there is at most one positive integer n for which $(n - 1, n, n + 1) = (ax^2, by^2, cz^2)$ for some integers x, y and z.*

Roughly speaking, the proof of this result proceeds as follows. First, we note that, from the theory of Pellian equations, if there exists a triple of positive integers (x, y, z) such that $(n - 1, n, n + 1) = (ax^2, by^2, cz^2)$, then

$$y = \frac{\gamma^j - \gamma^{-j}}{2\sqrt{b}} = \frac{\beta^k + \beta^{-k}}{2\sqrt{b}}$$

where j and k are positive integers and γ and β are the fundamental solutions to the equations $cX^2 - bY^2 = 1$ and $bX^2 - aY^2 = 1$ (i.e. $\gamma = \sqrt{c}u_0 + \sqrt{b}v_0$ and $\beta = \sqrt{b}u_1 + \sqrt{a}v_1$ where (u_0, v_0) and (u_1, v_1) are the smallest solutions in positive integers to $cX^2 - bY^2 = 1$ and $bX^2 - aY^2 = 1$ respectively). It follows that the linear form

$$\Lambda = j \log \gamma - k \log \beta$$

is extremely small in modulus. Applying results from [10], we deduce upper bounds for the coefficients j and k in terms of γ and β. On the other hand, if (x_1, y_1, z_1) is another triple of positive integers such that $(m - 1, m, m + 1) = (ax_1^2, by_1^2, cz_1^2)$ for some positive m and, say, $y_1 > y$, then elementary arguments from the theory of continued fractions imply that the integers j_1 and k_1 corresponding to y_1 grow very quickly in terms of γ and β, enabling us to derive a contradiction.

We remark that the proof of Proposition 2.1 does not entail any particularly deep or involved computations. In fact, only a few rudimentary results on the convergents in the continued fraction expansions of certain real numbers are required. The reader is directed to [2] for more details.

3. More preliminary results

Before proceeding with the proof of Theorem 1.2, we require some elementary results concerning the behaviour of elements of binary linear recurrence sequences.

Lemma 3.1. *Let $\epsilon = T + U\sqrt{d}$ denote the fundamental solution of $X^2 - dY^2 = 1$. If T is odd, then there are positive integers A, B, r, s with $\epsilon = \tau^2$, where $\tau = A\sqrt{r} + B\sqrt{s}$, $A^2 r - B^2 s = 1$ and $d = rs$. If T is even, then there are odd positive integers A, B, r, s with $\epsilon = \tau^2/2$, where $\tau = A\sqrt{r} + B\sqrt{s}$, $A^2 r - B^2 s = 2$ and $d = rs$.*

Proof. This follows easily upon considering the factorization

$$T^2 - 1 = (T-1)(T+1) = U^2 d.$$

$\square$

Lemma 3.2. *Let d denote a squarefree positive integer with $d > 1$. If d is odd, then there are precisely two triples of nonnegative integers (r, s, δ) such that the equation $rX^2 - sY^2 = 2^\delta$, with $\delta \in \{0, 1\}$ and $d = rs$ is solvable in integers X, Y. If d is even, then there are precisely two pairs of positive integers (r, s) such that the equation $rX^2 - sY^2 = 1$ with $d = rs$ is solvable in integers X, Y.*

Proof. A somewhat more general version of this is an immediate consequence of Theorem 3 of [17]. $\square$

Lemma 3.3. *Let $b, d > 1$ be squarefree integers. Further, let $T + U\sqrt{d}$ denote the fundamental solution of $X^2 - dY^2 = 1$ and $T_k + U_k\sqrt{d} = (T + U\sqrt{d})^k$ for $k \geq 1$. Suppose that $T_k = by^2$ for some odd integer y. If, additionally, $T_l = bw^2$ for some integer w, then w is odd.*

Proof. Let $\alpha(b)$ denote the divisibility index of b in the sequence $\{T_k\}$. The set of k for which $b|T_k$ is precisely the set $\{t\alpha(b); t \text{ is odd }\}$. Furthermore, by the binomial theorem it is easy to see that if 2^a properly divides $T_{\alpha(b)}$, then 2^a properly divides $T_{t\alpha(b)}$ for all odd integers t, whence the result readily obtains. $\square$

The following two lemmata were deduced by Cohn [6] in the course of proving Theorem 1.1.

Lemma 3.4. *For $\{T_k\}$ as above and n an odd positive integer, define $w_n = T_n/T$. Let k be an odd positive integer with $\gcd(k, n) = 1$ and $(\frac{\cdot}{\cdot})$ denote the Jacobi symbol. Then*

$$(i) \ w_n \equiv (-1)^{\frac{n-1}{2}} n \pmod{4T}$$

and

$$(ii) \ \left(\frac{w_n}{k}\right) = \left(\frac{k}{n}\right).$$

Lemma 3.5. *If n and m are odd positive coprime integers, then $\gcd(w_n, w_m) = 1$ and $(\frac{w_n}{w_m}) = 1$.*

4. Proof of Theorem 1.2

The proof is in two parts. We first show that there is at most one solution to the equation of the title. Let x and y be integers such that $b^2 x^4 - dy^2 = 1$. If bx^2 is even, then $\gcd(bx^2 - 1, bx^2 + 1) = 1$, and so there are odd positive integers r, s, z and w such that $d = rs$, $bx^2 - 1 = rz^2$ and $bx^2 + 1 = sw^2$. If bx^2 is odd, then it is easily verified that there are positive integers r, s, z and w such that $d = rs$, $bx^2 - 1 = 2rz^2$ and $bx^2 + 1 = 2sw^2$. Thus, we have for bx^2 even that (rz^2, bx^2, sw^2) are three consecutive integers and, for bx^2 odd, that $(2rz^2, bx^2, 2sw^2)$ are three consecutive integers, with $d = rs$ in both cases.

Applying Proposition 2.1 and Lemma 3.2, then, we conclude that there are at most two solutions to $b^2 X^4 - dY^2 = 1$, and, if two solutions exist, that one of the triples of consecutive integers given above must be of the form $(2dz^2, bx^2, 2w^2)$. By Lemma 3.3, another solution $X = u, Y = v$ to $b^2 X^4 - dY^2 = 1$ must have u odd

and so, by the analysis given in the above paragraph, the corresponding triple of consecutive integers $(bu^2 - 1, bu^2, bu^2 + 1)$ must be of the form $(2rz_1^2, bu^2, 2sw_1^2)$ for positive squarefree integers r and $s > 1$ with $d = rs$. Since $sw_1^2 - rz_1^2 = 1$ and $s \neq 1$, it follows from Lemma 3.1 and Lemma 3.2 that $\epsilon = T + U\sqrt{d}$, the fundamental solution of $X^2 - dY^2 = 1$, is of the form $\epsilon = \tau^2$, where $\tau = A\sqrt{r} + B\sqrt{s}$ with $B^2 s - A^2 r = 1$. Since $z_1\sqrt{r} + w_1\sqrt{s}$ is necessarily an odd power of τ, we have that

$$\left(z_1\sqrt{r} + w_1\sqrt{s}\right)^2 = bu^2 + 2z_1 w_1 \sqrt{d}$$

is an odd power of ϵ. Noting that $b > 1$ and arguing as in the proof of Lemma 3.3, we conclude that $bx^2 + 2zw\sqrt{d}$ is also an odd power of ϵ.

If w is even, then since $w^2 - dz^2 = 1$, it follows that T is even, which contradicts Lemma 3.1. We therefore have that w is odd. But

$$(2dz^2, bx^2, 2w^2) = (2w^2 - 2, 2w^2 - 1, 2w^2)$$

and so

$$bx^2 + 2zw\sqrt{d} = bx^2 + 4w\sqrt{\frac{w^2 - 1}{4}} = (2w^2 - 1) + 4w\sqrt{\frac{w^2 - 1}{4}}$$

$$= \left(w + 2\sqrt{\frac{w^2 - 1}{4}}\right)^2 .$$

This shows that $bx^2 + 2zw\sqrt{d}$ is an even power of ϵ, a contradiction.

We conclude, therefore, that there is at most one solution in integers to $b^2 X^4 - dY^2 = 1$, provided $b > 1$.

To complete the proof of Theorem 1.2, we now demonstrate that if a solution to $b^2 X^4 - dY^2 = 1$ exists, then $T_{\alpha(b)} = bx^2$ for some $x \in \mathbb{Z}$. We will assume that m is an integer for which $T_{m \cdot \alpha(b)} = bx_1^2$ and show that there is an integer x for which $T_{\alpha(b)} = bx^2$. The desired result then follows from the uniqueness of the solution.

Let $t = T_{\alpha(b)}$ and $u = U_{\alpha(b)}$ and define $t_k + u_k \sqrt{d} = (t + u\sqrt{d})^k$ for $k \geq 1$. If, for $n \geq 1$ odd, we define $w_n = t_n / t$, then it is evident that the conclusion of Lemma 3.4 remains valid for the sequence $\{w_n\}$.

From $T_{m \cdot \alpha(b)} = bx_1^2$, it follows that $t_m = bx_1^2$. Further, the definition of t implies that $t = bl$ for some integer l. If n is a positive integer with $\gcd(n, tm) = 1$, then

$$\gcd(w_n, bl) = \gcd(w_n, t_m) = 1$$

whence

$$\left(\frac{b}{w_n}\right) = \left(\frac{bx_1^2}{w_n}\right) = \left(\frac{t_m}{w_n}\right).$$

Applying Lemma 3.5, we have

$$1 = \left(\frac{w_m}{w_n}\right) = \left(\frac{w_m t_1^2}{w_n}\right) = \left(\frac{t_m}{w_n}\right)\left(\frac{t_1}{w_n}\right) = \left(\frac{b}{w_n}\right)\left(\frac{t_1}{w_n}\right) = \left(\frac{b}{w_n}\right)^2 \left(\frac{l}{w_n}\right),$$

and so $\left(\frac{l}{w_n}\right) = 1$. Since $t_m = bx_1^2$, $t_1 = bl$ and, arguing as in the proof of Lemma 3.3, we have $\text{ord}_2 \, t_m = \text{ord}_2 \, t_1$, it follows that $l = 2^{2\mu} l_1$ for some $\mu \in \mathbb{Z}$ and l_1 odd. Therefore, from Lemma 3.4 and quadratic reciprocity,

$$1 = \left(\frac{l}{w_n}\right) = \left(\frac{l_1}{w_n}\right) = \left(\frac{w_n}{l_1}\right) = \left(\frac{l_1}{n}\right) = \left(\frac{l}{n}\right).$$

This is only possible if l is the square of an integer, since otherwise we may choose $n \equiv 1 (\mathrm{mod}\ 4)$ such that $\gcd(n, tm) = 1$ and n is a quadratic non-residue modulo l. This completes the proof of Theorem 1.2.

5. Proof of Corollary 1.3

To prove Corollary 1.3, we appeal to the following moderately explicit characterization of the divisibility index $\alpha(p)$ of a prime p in the sequence $\{T_k\}$. The result is quite standard; for a proof, the reader is directed to the classic paper of Lehmer [12].

Lemma 5.1. *Let $\epsilon = T + U\sqrt{d}$ denote the fundamental solution to $X^2 - dY^2 = 1$, and $T_k + U_k\sqrt{d} = \epsilon^k$ for $k \geq 1$. Let p be prime and $\alpha(p)$ denote, as before, the divisibility index of p in the sequence $\{T_k\}$.*

    (i)   If $p = 2$, then $\alpha(p) = 1$ or ∞.

    (ii)   If $p > 2$ divides d, then $\alpha(p) = \infty$.

    (iii) If $p > 2$ fails to divide d, then either $\alpha(p) | \frac{p - (\frac{d}{p})}{2}$ or $\alpha(p) = \infty$.

Here $(\frac{d}{p})$ denotes the usual Legendre symbol.

We are now in position to establish Corollary 1.3. Let b be of the form given in the statement of the corollary and assume that $T_k = bx^2$ for some integer x. Suppose first that k is even, $k = 2l$, say. Then $T_k = 2T_l^2 - 1 = bx^2$. Since 2 must be a quadratic residue of the prime divisors of $2T_l^2 - 1$, b must be a product of primes congruent to ± 1 modulo 8. Thus, except for $b = 7$, there is no solution to $T_k = bx^2$ with k even. Since the preceding lemma implies that $\alpha(7) = 1, 2, 3, 4$ or ∞, it remains, from Theorem 1.2, to show that the equation $T_4 = 8T^4 - 8T^2 + 1 = 7x^2$ possesses no solutions in integers, which follows trivially upon considering the equation modulo 4.

Assume now that k is odd. By Lemma 5.1, $\alpha(2) = 1$ or ∞, $\alpha(3) = 1, 2$ or ∞, $\alpha(5) = 1, 2, 3$ or ∞, $\alpha(7) = 1, 2, 3, 4$ or ∞, and $\alpha(11) = 1, 2, 3, 5, 6$ or ∞. By Theorem 1.2, $k = \alpha(b)$, and it follows from the fact that k is odd that either $k = 1, 3, 5$ or 15. For the values of b under consideration, we first show that there are no solutions with $k = 5$ (which also eliminates the possibility of $k = 15$, since $T_{15} = T_5(T_3)$). Suppose that $T_5 = bx^2$ for some $T > 1$ and $x \in \mathbb{Z}$. Since $T_5 = T\left(16T^4 - 20T^2 + 5\right)$ and

$$\gcd\left(16T^4 - 20T^2 + 5,\ 2 \cdot 3 \cdot 7 \cdot 11\right) = 1,$$

it follows that

$$16T^4 - 20T^2 + 5 = 5^\delta u^2$$

for some $u \in \mathbb{Z}$ and $\delta \in \{0, 1\}$ and so

$$\left(8T^2 - 5\right)^2 - 5 = 5^\delta (2u)^2.$$

If $\delta = 0$, this implies that $T = \pm 1$, contradicting $T > 1$. If, however, $\delta = 1$, then $T = 5v$ for some $v \in \mathbb{Z}$ and so

$$(2u)^2 - 5(40v^2 - 1)^2 = -1.$$

Since it is readily proved by induction that all integer solutions to $X^2 - 5Y^2 = -1$ satisfy $Y \equiv 1(\mathrm{mod}\ 8)$ (upon, for instance, noting that the smallest solution corresponds to $2 + \sqrt{5}$), we obtain the desired contradiction.

It remains to consider when $T_3 = T(4T^2 - 3) = bx^2$ for $T > 1$ and $x \in \mathbb{Z}$. Since $\gcd(4T^2 - 3, \, 2 \cdot 5 \cdot 7) = 1$, we therefore have

$$4T^2 - 3 = 3^a 11^b u^2$$

for some $u \in \mathbb{Z}$ and $a, b \in \{0, 1\}$. Considering this equation modulo 4, it follows that $a + b \equiv 0 \pmod 2$ and so $a = b = 0$ or $a = b = 1$. In the first instance, $T = \pm 1$, contradicting $T > 1$. In the second,

$$(3) \qquad\qquad 4T^2 - 3 = 33u^2$$

and so $11|b$. If $2|b$, then from $T(4T^2 - 3) = bx^2$, we have $2|T$ and so, from equation (3), $u^2 \equiv 5 \pmod 8$, a contradiction. Similarly, if $7|b$, then necessarily $7|T$ and so $u^2 \equiv 5 \pmod 7$, again a contradiction. It follows that $b \in \{11, 33, 55, 165\}$.

Let us suppose now that $b = 5^\delta \cdot 33$ for $\delta \in \{0, 1\}$. It follows that $T = 5^\delta 9v^2$ for some $v \in \mathbb{Z}$ and so

$$108 \left(5^\delta v^2\right)^2 - 11u^2 = 1.$$

Now the smallest solution to $108X^2 - 11Y^2 = 1$ corresponds to $15\sqrt{108} + 47\sqrt{11}$ and so we may show by induction that all solutions X, Y to this equation satisfy $X \equiv 3, 7 \pmod 8$. Since $5^\delta v^2 \equiv 0, 1, 4, 5 \pmod 8$, we reach the desired contradiction.

It remains only to consider when $b = 11$ or 55. Regarding these cases, we prove

Proposition 5.2. *(i) The only solution in positive integers to the equation*

$$T(4T^2 - 3) = 11x^2$$

is given by $T = 3$ and $x = 3$.

(ii) The only solution in positive integers to the equation

$$T(4T^2 - 3) = 55x^2$$

is given by $T = 135$ and $x = 423$.

Proof. We apply standard techniques for finding integer points on elliptic curves based on the theory of linear forms in elliptic logarithms, specifically following the exposition of Gebel, et al. [8] (see also [18] for a similar approach). We note that the bounds given in [8] are not quite correct as stated, so we actually utilize the revised constants given in Proposition 2 of [9]. To perform the necessary computations, we employ Ian Connell's Apecs, GP/PARI 1.38 and Maple V. Taking

$$X = 44T, \ Y = 22^2 x$$

and

$$X = 220T, \ Y = 110^2 x$$

in (i) and (ii) respectively, we are led to consider, in Weierstrass form, the elliptic curves

$$E_1 : \quad Y^2 = X^3 - 1452X$$

and

$$E_2 : \quad Y^2 = X^3 - 36300X.$$

The first of these has discriminant

$$\Delta = 195920474112 = 2^{12} 3^3 11^6,$$

modular invariant $j = 1728$, a two element torsion group generated by $T = (0,0)$ and, via 2-descent, rank 1. The Mordell-Weil group $E_1(\mathbb{Q})$ is generated, modulo torsion, by the point $P_1 = (132, 1452)$, with canonical height

$$\hat{h}(P_1) = 0.6811644354\ldots$$

and elliptic logarithm

$$u_1 = 0.17558123819156381213025583974497106901\ldots.$$

This last value may be computed quite quickly and accurately via the algorithm given in [22]. Related fundamental periods are

$$\omega_1 = 0.4247668014\ldots$$

and $\omega_2 = i\,\omega_1$, so that

$$\tau = \omega_2/\omega_1 = i.$$

Applying Theorem 2 of [9] (which depends crucially upon the lower bound for linear forms in elliptic logarithms of David [7]), if

$$P = n_1 P_1 + P_2$$

is an integral point on E_1 over $\mathbb{Q}$, for P_2 a torsion point, then

$$|n_1| \le 1.22 \times 10^{15}.$$

To dispose of the remaining "small" cases, we need only apply the continued fraction algorithm to u_1 or, roughly equivalently, lattice basis reduction à la de Weger [21] to the lattice corresponding to the 2×2 matrix

$$\begin{pmatrix} 1 & 0 \\ \lfloor c_0 u_1 \rfloor & c_0 \end{pmatrix}$$

for suitably chosen c_0. Taking $c_0 = 10^{33}$, we may argue as in Section 6 of [8] to conclude that in fact we have

$$|n_1| \le 5.$$

Since, for these values of n_1, we find only the integer points $(-11, \pm 121)$ and $(132, \pm 1452)$, we obtain the desired result (upon noting that only $(132, 1452)$ comes from a positive solution to the original equation).

The case of E_2 follows similarly upon noting that we have discriminant

$$\Delta = 3061257408000000 = 2^{12}3^3 5^6 11^6,$$

modular invariant $j = 1728$, a two element torsion group generated by $(0,0)$ and, via 2-descent, rank 2. The group $E_2(\mathbb{Q})$ is generated, modulo torsion, by the points $P_1 = (550, 12100)$ and $P_2 = (825/4, 9075/8)$, with canonical heights

$$\hat{h}(P_1) = 0.6154894898\ldots$$

and

$$\hat{h}(P_2) = 1.2421525473\ldots$$

and elliptic logarithms

$$u_1 = \quad 0.08635867240993010940419215928845127756748774440725202868437458236701457446154769550433554 6\ldots$$

and

$$u_2 = \quad 0.16111211999739781225510441610829753797537345416396178946473928847048261083778599876234 0026\ldots$$

respectively. Related fundamental periods are

$$\omega_1 = 0.1899614885\ldots$$

and $\omega_2 = i\,\omega_1$, so again

$$\tau = \omega_2/\omega_1 = i.$$

Further, the smallest eigenvalue of the (positive definite) matrix associated with $\hat{h}$ and the basis P_1, P_2 is given by

$$\lambda_1 = 0.997595055\ldots.$$

Once again applying the main theorem of [8], if

$$P = n_1 P_1 + n_2 P_2 + P_3$$

is an integral point on E_2 over $\mathbb{Q}$, for P_3 a torsion point, then

$$\max\{|n_1|, |n_2|\} \le 4.09 \times 10^{28}.$$

Applying de Weger reduction to

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \lfloor c_0 u_1 \rfloor & \lfloor c_0 u_2 \rfloor & c_0 \end{pmatrix}$$

where here we take $c_0 = 10^{90}$, this enables us to conclude that in fact

$$\max\{|n_1|, |n_2|\} \le 12$$

from which a routine computation with Apecs confirms that the only integral points on E_2 are $(-50, \pm1300)$, $(-66, \pm1452)$, $(-176, \pm968)$, $(196, \pm644)$, $(550, \pm12100)$, $(726, \pm18876)$ and $(29700, \pm5118300)$. Since only the point $(29700, 5118300)$ corresponds to a solution to our original equation, this completes the proof. $\square$

6. Proof of Theorem 1.4

For $n \ge 1$, note that T_n is a polynomial in T of degree n, say $T_n = f_n(T)$. Moreover, from the fact that the polynomials $\{f_n\}$ satisfy the recurrence $f_{n+1}(T) = 2T \cdot f_n(T) - f_{n-1}(T)$, the height of f_n (that is, the maximum modulus of the coefficients) is bounded by 3^n.

Now assume that $T_n = bx^2$, with $n \ge 3$, $b > 1$ and b squarefree. Then Theorem 1.2 implies that $n = \alpha(b)$. If $b = p_1 p_2 \cdots p_s$ is the factorization of b into distinct primes, then $\alpha(b) \le \alpha(p_1) \cdots \alpha(p_s)$ and so, by Lemma 5.1, $\alpha(b) < b$. It follows that we have an integral solution T, x to the Diophantine equation $f_n(T) = bx^2$ for some $n < b$. Since the degree of $f_n(T)$ is bounded by b, the height of $f_n(T)$ is bounded by 3^b and its roots are readily seen to be distinct, we may apply standard results from the theory of linear forms in logarithms (see e.g. [1] or [20]) to conclude that x (and hence d) is bounded by $C = C(b)$, for some computable constant depending on b. This concludes the proof of Theorem 1.4.

7. Concluding remarks

The situation is somewhat less simple if we consider the more general equation

$$aX^4 - dY^2 = 1,$$

for a an arbitrary but fixed integer. Presumably, there are at most two solutions in positive integers X, Y (as, for instance, is the case when $a = 3$ and $d = 2$; see the paper of Bumby [3]), but an explicit statement to this effect is not, to our knowledge, available in the literature. On the other hand, the techniques of [13] could likely be applied to yield such a result (see e.g. [16] for further remarks along these lines).

Acknowledgments

References

[1] A. Baker. Bounds for the solutions of the hyperelliptic equation. *Proc. Cambridge Philos. Soc.* **65** (1969), 439–444. MR **38:**3226

[2] M.A. Bennett. On consecutive integers of the form ax^2, by^2 and cz^2. submitted for publication.

[3] R.T. Bumby. The Diophantine equation $3x^4 - 2y^2 = 1$. *Math. Scand.* **21** (1967), 144–148. MR **39:**6818

[4] Z.F. Cao. A study of some Diophantine equations. *J. Harbin Inst. Tech.* (1988), 1–7. MR **90k:**11026

[5] J.H. Chen and P. Voutier. Complete solution of the Diophantine equation $X^2 + 1 = dY^4$ and a related family of quartic Thue equations. *J. Number Theory* **62** (1997), 71–99. MR **97m:**11039

[6] J.H.E. Cohn. The Diophantine equation $x^4 - Dy^2 = 1$ II. *Acta Arith.* **78** (1997), 401–403. MR **98e:**11033

[7] S. David. Minorations de formes linéaires de logarithmes elliptiques. *Publ. Math. Univ. Pierre et Marie Curie 106*, Problèmes diophantiens 1991–1992, exposé no. 3.

[8] J. Gebel, A. Pethő and H.G. Zimmer. Computing integral points on elliptic curves. *Acta Arith.* **68** (1994), 171–192. MR **95i:**11020

[9] J. Gebel, A. Pethő and H.G. Zimmer. On Mordell's equation. *Compositio Math.* **110** (1998), 335–367. CMP 98:07

[10] M. Laurent, M. Mignotte and Y. Nesterenko. Formes linéaires en deux logarithmes et déterminants d'interpolation. *J. Number Theory* **55** (1995), 285–321. MR **96h:**11073

[11] M.H. Le. On the Diophantine equation $D_1 x^4 - D_2 y^2 = 1$. *Acta Arith.* **76** (1996), 1–9. MR **97b:**11040

[12] D.H. Lehmer. An extended theory of Lucas functions. *Ann. Math.* **31** (1930), 419–448.

[13] W. Ljunggren. Über die Gleichung $x^4 - Dy^2 = 1$. *Arch. Math. Naturvid.* **45** (1942), No. 5, 61–70. MR **7:**471

[14] W. Ljunggren. Sätze über unbestimmte Gleichungen. *Skr. Norske Vid. Akad. Oslo. I.* (1942), No. 9. MR **6:**169e

[15] W. Ljunggren. Zur Theorie der Gleichung $x^2 + 1 = Dy^4$. *Avh. Norske Vid. Akad. Oslo. I.* (1942), No. 5. MR **8:**6f

[16] W. Ljunggren. On the Diophantine equation $Ax^4 - By^2 = C$ $(C = 1, 4)$. *Math. Scand.* **21** (1967), 149–158. MR **39:**6820

[17] T. Nagell. On a special class of Diophantine equations of the second degree. *Ark. Mat.* **3** (1954), 51–65. MR **15:**854e

[18] R.J. Stroeker and N. Tzanakis. Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. *Acta Arith.* **67** (1994), 177–196. MR **95m:**11056

[19] N. Tzanakis. Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations. *Acta Arith.* **75** (1996), 165–190. MR **96m:**11019

[20] P. Voutier. An upper bound for the size of integral solutions to $Y^m = f(X)$. *J. Number Theory* **53** (1995), 247–271. MR **96f:**11049

[21] B.M.M. de Weger. Algorithms for Diophantine equations. CWI Tract 65, Stichting Mathematisch Centrum, Amsterdam, 1989. MR **90m:**11205

[22] D. Zagier. Large integral points on elliptic curves. *Math. Comp.* **48** (1987), 425–436. MR **87k:**11062

[23] W. Zhu. Necessary and sufficient conditions for the solvability of the Diophantine equation $x^4 - Dy^2 = 1$. (Chinese) *Acta Math. Sinica* **28** (1985), 681–683. MR **87e:**11042

School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540
E-mail address: `mabennet@ias.edu`

Current address: Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801
E-mail address: `mabennet@math.uiuc.edu`

Department of Mathematics, University of Ottawa, Ottawa, Ontario, Canada K1N 6N5
E-mail address: `gwalsh@mathstat.uottawa.ca`