

**Solving a family of Thue equations
with an application to the equation $x^2 - Dy^4 = 1$**

by

A. TOGBE (Westville, IN), P. M. VOUTIER (London) and
P. G. WALSH (Ottawa)

1. Introduction. While the contributions of Wilhelm Ljunggren to the study of Diophantine equations are significant, perhaps what is as interesting are the problems that remain open from his work. In this paper, we look closely at one of Ljunggren's more notable theorems (see [9] or Theorem 9 in Chapter 28 from [12]), a result which represented a substantial breakthrough on the occurrence of squares in a special class of Lucas sequences. In the following result, ε_D denotes the fundamental unit in the ring of integers of the real quadratic field $\mathbb{Q}(\sqrt{D})$.

THEOREM (Ljunggren, 1936). *Let D denote a positive nonsquare integer. Then the equation*

$$(1.1) \quad X^2 - DY^4 = 1$$

has at most two solutions in positive integers X and Y . If two solutions (X_1, Y_1) and (X_2, Y_2) exist, with $Y_1 < Y_2$, then they are given either by

$$X_1 + Y_1^2\sqrt{D} = \varepsilon_D, \quad X_2 + Y_2^2\sqrt{D} = \varepsilon_D^2$$

or by

$$X_1 + Y_1^2\sqrt{D} = \varepsilon_D, \quad X_2 + Y_2^2\sqrt{D} = \varepsilon_D^4,$$

with the latter case occurring for only finitely many values of D .

The primary purpose of the present paper is to refine the statement of the above theorem. Evidently, this result does not cover the case that equation (1.1) has only one solution. That is to say, in the case that equation (1.1) has only one solution in positive integers, Ljunggren's theorem does not give any information from which power of the fundamental unit of $\mathbb{Q}(\sqrt{D})$ this solution arises. Therefore, we will provide a proof of the following sharpening of Ljunggren's theorem. In this formulation, and throughout the paper, we let $\varepsilon_D = T_1 + U_1\sqrt{D}$ denote the minimal unit greater than 1, of norm 1, in

$\mathbb{Z}[\sqrt{D}]$, and for $k \geq 1$, $\varepsilon_D^k = T_k + U_k\sqrt{D}$. In other words, $(X, Y) = (T_1, U_1)$ is the smallest positive integer solution to the Pell equation $X^2 - DY^2 = 1$.

THEOREM 1.1.

- (i) *There are at most two positive integer solutions (X, Y) to equation (1.1). If two solutions $Y_1 < Y_2$ exist, then $Y_1^2 = U_1$ and $Y_2^2 = U_2$, except only if $D = 1785$ or $D = 16 \cdot 1785$, in which case $Y_1^2 = U_1$ and $Y_2^2 = U_4$.*
- (ii) *If only one positive integer solution (X, Y) to equation (1.1) exists, then $Y^2 = U_l$ where $U_l = lv^2$ for some squarefree integer l , and either $l = 1$, $l = 2$, or $l = p$ for some prime $p \equiv 3 \pmod{4}$.*

The statement of this theorem appears in [18], but the details of the proof have never been published, and so it is the primary purpose of the present paper to provide those details. The proof depends on results concerning quartic equations of the type $aX^2 - bY^4 = c$ with $c \in \{\pm 1, 2\}$, most of which appear in the literature, and will be discussed in later sections. There is, however, a key result concerning solutions to the particular quartic equation $aX^4 - bY^2 = 1$, with a not a square, which does not appear in the literature, and so most of the present paper will be devoted to proving this new result.

In order to formulate this new result, we must make some preliminary remarks concerning the solvability of the equation

$$(1.2) \quad aX^4 - bY^2 = 1$$

in positive integers X, Y . The details concerning these remarks can be found in Section 2.3 of [18]. Let a denote a nonsquare positive integer, and b a positive integer for which the quadratic equation

$$(1.3) \quad aX^2 - bY^2 = 1$$

is solvable in positive integers X, Y . In this case, there is a minimal solution

$$\tau = \tau_{a,b} = v\sqrt{a} + w\sqrt{b},$$

that is, a solution with v and w positive integers, $\tau > 1$ minimal with this property, and $\tau^2 = \varepsilon_{ab}$ being the minimal solution to $X^2 - abY^2 = 1$. Moreover, as shown in [17], all solutions in positive integers of (1.3) are given by

$$\tau^{2k+1} = v_{2k+1}\sqrt{a} + w_{2k+1}\sqrt{b} \quad (k \geq 0).$$

Solving the quartic equation (1.2) is equivalent to the problem of determining all squares in the sequence $\{v_{2k+1}\}$. The case $(a, b) = (2, 1)$ was solved by Ljunggren in [8], wherein it was shown that $(X, Y) = (1, 1), (13, 239)$ are the only solutions in positive integers. For the case $(a, b) = (3, 2)$, Bumby [2] showed that the only squares in this sequence are v_1 and v_3 . In other words,

the only solutions in positive integers X, Y to the equation $3X^4 - 2Y^2 = 1$ are $(1, 1)$ and $(3, 11)$.

The following observation is contained in the work of Rotkiewicz [14], and can be traced back to Chao Ko's result in [5] on the equation $x^2 = y^n + 1$. The proof relies on clever manipulation of certain Jacobi symbols involving terms in a given Lucas sequence.

PROPOSITION 1.1. *If v_{2k+1} is a square for some $k \geq 0$, then v_1 is also a square.*

Assume now that equation (1.2) is solvable. By the preceding result, $\tau = \tau_{a,b}$ is of the form $\tau = x^2\sqrt{a} + w\sqrt{b}$. Put $t = x^4a - 1$; then $\tau = \sqrt{t+1} + \sqrt{t}$, and for $k \geq 0$,

$$\tau^{2k+1} = V_{2k+1}\sqrt{t+1} + W_{2k+1}\sqrt{t},$$

where for each $k \geq 0$, $V_{2k+1} = v_{2k+1}/v_1 = v_{2k+1}/x^2$. Proposition 1.1 can be reformulated as follows.

COROLLARY 1.1. *For $k \geq 0$, v_{2k+1} is a square if and only if V_{2k+1} is a square.*

Corollary 1.1 shows that in order to obtain information on the powers of $\tau_{a,b}$ which can yield solutions to equation (1.2), it is sufficient to consider equations of the form

$$(1.4) \quad (t+1)X^4 - tY^2 = 1,$$

which we will do for the remainder of this paper.

REMARK. It is not surprising that Bumby's equation $3X^4 - 2Y^2 = 1$ in [2] has the two solutions $(1, 1)$ and $(3, 11)$. More generally, if t is an integer of the form $t = m^2 + m$, with $m \geq 1$, then the equation

$$(1.5) \quad (m^2 + m + 1)X^4 - (m^2 + m)Y^2 = 1$$

has the two solutions $(X, Y) = (1, 1), (2m+1, 4m^2 + 4m + 3)$, which correspond to $\tau_{t+1,t}$ and $\tau_{t+1,t}^3$ respectively.

More generally, we state the following.

CONJECTURE 1.1. *Let $t > 1$ denote a positive integer. Then the only positive integer solution to*

$$(t+1)X^4 - tY^2 = 1$$

is $(X, Y) = (1, 1)$, unless $t = m^2 + m$ for some positive integer m , in which case there is also the solution $(X, Y) = (2m+1, 4m^2 + 4m + 3)$.

We remark that a solution to Conjecture 1.1 would provide the basis for a proof of the following, which represents what is likely the truth concerning Theorem 1.1, although one could refine the statement even further.

CONJECTURE 1.2. *Let $D > 1$ be a nonsquare positive integer, and let $T + U\sqrt{D}$ denote the minimal unit greater than 1 of norm 1 in $\mathbb{Z}[\sqrt{D}]$. If x and y are positive integers satisfying equation (1.1), then $x + y^2\sqrt{D} = (T + U\sqrt{D})^k$ for some positive integer $k \leq 3$, except only for $D = 1785$ and $D = 16 \cdot 1785$, in which cases (1.1) has solutions with exponents $k = 1$ and $k = 4$.*

2. Reduction to a family of Thue equations. One approach for determining all solutions to (1.4) is the hypergeometric method of Thue [16], when it applies. This is accomplished via the following reduction to a family of Thue equations. We include the details of the reduction not only for the sake of completeness, but also because we will make reference to certain aspects of the proof in what follows.

PROPOSITION 2.1. *Let $t \geq 1$ be a positive integer. If (X, Y) is a positive integer solution to (1.4) other than $(1, 1)$, then there is an integer solution (x, y) to the Thue equation*

$$(2.1) \quad x^4 + 4tx^3y - 6tx^2y^2 - 4t^2xy^3 + t^2y^4 = t_0^2,$$

where t_0 divides t and $t_0 \leq \sqrt{t}$.

Proof. The case $t = 1$ was solved by Chen and the second author in [3]. Define V_k for all $k \geq 0$ by

$$(2.2) \quad V_k = \frac{\tau^k + (-1)^{k+1}\tau^{-k}}{\tau + \tau^{-1}},$$

where $\tau = \sqrt{t+1} + \sqrt{t}$. This definition for V_k is the same as that given earlier. For $k \geq 0$, let

$$T_k + U_k\sqrt{t(t+1)} = \tau^{2k};$$

then $V_{2k} = \sqrt{t}U_k$ for all $k \geq 0$. With V_k as above, the relation

$$V_{2k+1} = V_{k+1}^2 + V_k^2$$

holds for all $k \geq 0$. Assume now that $V_{2k+1} = z^2$ for some integer $z > 1$. We will assume that k is even, $k = 2n$ say, as a similar argument holds in the case that k is odd. In this case

$$V_{4n+1} = z^2 = V_{2n+1}^2 + V_{2n}^2 = V_{2n+1}^2 + tU_n^2,$$

with $n > 0$. Therefore, $tU_n^2 = z^2 - V_{2n+1}^2$, and since $V_{2n+1} = T_n + tU_n$, it follows that

$$tU_n^2 = z^2 - (T_n + tU_n)^2.$$

Since $\gcd(U_n, T_n + tU_n) = 1$ and U_n is even and nonzero, there exist positive integers G, H, t_1, t_2 , with $U_n = 2GH$ and $t = t_1t_2$, such that

$$z - (T_n + tU_n) = 2t_1G^2, \quad z + (T_n + tU_n) = 2t_2H^2.$$

Therefore, $T_n + tU_n = t_2H^2 - t_1G^2$, and from $U_n = 2GH$ we deduce that

$$T_n = t_2H^2 - 2tGH - t_1G^2.$$

Substituting for T_n and U_n in the equation $T_n^2 - t(t+1)U_n^2 = 1$ and simplifying yields

$$t_1^2G^4 + 4tt_1G^3H - 6tG^2H^2 - 4tt_2GH^3 + t_2^2H^4 = 1.$$

Put $t_0 = \min(t_1, t_2)$ and multiply the previous relation by t_0^2 . Also, if $t_0 = t_1$, put $x = t_1G$ and $y = H$, otherwise put $x = -t_2H$ and $y = G$. Then x and y are integers satisfying $x^4 + 4tx^3y - 6tx^2y^2 - 4t^2xy^3 + t^2y^4 = t_0^2$.

It is important at this stage to determine a method to deal with the Thue equations in (2.1). In [3], Chen and the second author use the hypergeometric method of Thue in order to solve a parametric family of Thue equations which are derived from a solution of the quartic equation $X^2 - dY^4 = -1$. Quartic equations of the form $X^2 - dY^4 = -1$ are a subclass of the family of quartic equations given by (1.2). Therefore, it is natural to try to apply the hypergeometric approach in this more general setting.

In order to apply the hypergeometric method, one requires good rational approximations to the roots $\beta^{(i)}$, $i = 1, 2, 3, 4$, of the polynomial

$$(2.3) \quad p_t(x) = x^4 + 4tx^3 - 6tx^2 - 4t^2x + t^2,$$

which are given explicitly by

$$\begin{aligned} \beta^{(1)} &= \frac{\sqrt{t}}{\tau} (1 + \varrho), & \beta^{(3)} &= (-\tau + \varrho)\sqrt{t}, \\ \beta^{(2)} &= \frac{\sqrt{t}}{\tau} (1 - \varrho), & \beta^{(4)} &= -(\tau + \varrho)\sqrt{t}, \end{aligned}$$

where $\tau = \sqrt{t+1} + \sqrt{t}$ and $\varrho = \sqrt{\tau^2 + 1}$.

In the case that $t = m^2$ for some integer m , very good approximations to all 4 of these roots can be constructed, as was described in detail in [3], and independently in [21]. As a consequence, the authors of [3] completely solved the associated family of Thue equations, and proved the following result. We remark that the same family of Thue equations was solved independently by Lettl and Pethő in [6].

THEOREM (Chen–Voutier and Yuan). *Let $d > 2$ be a squarefree integer such that the Pell equation $X^2 - dY^2 = -1$ is solvable in positive integers, and let $\tau = v + u\sqrt{d}$ denote its minimal solution. The only possible integer solution to the equation $X^2 - dY^4 = -1$ is $(X, Y) = (v, \sqrt{u})$.*

Because of this theorem, we will assume throughout the paper that t is a nonsquare positive integer. We remark that Bennett and the third author [1] completely solved equation (1.4) in the case that $t+1$ is a perfect square, using lower bounds for linear forms in the logarithms of algebraic numbers.

Most of this paper will be devoted to applying Thue's method in order to obtain an effective measure of approximation to the two roots $\beta^{(3)}$ and $\beta^{(4)}$, as this is precisely what is required to prove Theorem 1.1. It is important to note that problems arise when one attempts to apply Thue's method to the entire family of equations (2.1). In particular, there is difficulty in obtaining an effective measure of approximation for the two roots $\beta^{(1)}$ and $\beta^{(2)}$. This is due to the fact that these roots approach \sqrt{t} as t goes to ∞ (see below), and therefore have no explicit rational approximations suitable for all choices of t . The authors of [3] are able to deal with the particular subclass of equations of the type $X^2 - dY^4 = -1$ because in this case, the parameter t in (1.4) is a square, in which case one can initiate the hypergeometric method using the rational approximation \sqrt{t} .

For $k \geq 0$ define polynomials $V_{2k+1}(t)$ and $W_{2k+1}(t)$ by

$$(2.4) \quad (\sqrt{t+1} + \sqrt{t})^{2k+1} = V_{2k+1}(t)\sqrt{t+1} + W_{2k+1}(t)\sqrt{t}.$$

For example,

$$\begin{aligned} V_1(t) &= 1, & V_5(t) &= 16t^2 + 12t + 1, \\ V_3(t) &= 4t + 1, & V_7(t) &= 64t^3 + 80t^2 + 24t + 1, \end{aligned}$$

and for $k \geq 1$,

$$V_{2k+3}(t) = (4t + 2)V_{2k+1}(t) - V_{2k-1}(t).$$

An integer solution to equation (1.4) is equivalent to a triple of integers (t, z, k) for which $z^2 = V_{2k+1}(t)$. We will show that a positive integer solution to $z^2 = V_{2k+1}(t)$ with k even gives rise to a solution (x_1, y_1) to (1.4) with x_1/y_1 close to either $\beta^{(3)}$ or $\beta^{(4)}$. A similar argument shows that a solution to $z^2 = V_{2k+1}(t)$ with k odd gives rise to a solution (x_1, y_1) to (1.4) with x_1/y_1 close to either $\beta^{(1)}$ or $\beta^{(2)}$.

To see this, first notice that from (2.2),

$$\begin{aligned} V_{k+1}/V_k - \tau &= \frac{\tau^{k+1} + (-1)^{k+2}\tau^{-(k+1)} - \tau^{k+1} - (-1)^{k+1}\tau^{-k+1}}{\tau^k + (-1)^{k+1}\tau^{-k}} \\ &= \frac{1 + \tau^{-2}}{\tau^{2k+1}(1 \pm \tau^{-2k})}, \end{aligned}$$

and so V_{k+1}/V_k is evidently very close to τ , which itself is approximately equal to $2\sqrt{t}$.

Now suppose that $z^2 = V_{4n+1}$, and that $t_1 \leq t_2$, so that $x = t_1G$ and $y = H$ in the above proof (a similar argument deals with the case $t_2 \leq t_1$). Therefore,

$$\frac{x}{y} = \frac{2t_1G^2}{2GH} = \frac{\sqrt{V_{4n+1}} - V_{2n+1}}{U_n} = \frac{\sqrt{V_{2n+1}^2 + V_{2n}^2} - V_{2n+1}}{V_{2n}/\sqrt{t}},$$

and after some algebraic manipulation, this last quantity is easily seen to be equal to

$$\frac{\sqrt{t}}{\sqrt{(V_{2n+1}/V_{2n})^2 + 1} + V_{2n+1}/V_{2n}},$$

from which it is evident that x/y is close to $1/4$.

We shall also need some inequalities for the location of the roots. For $t \geq 18$, the polynomial $p_t(x)$ from (2.3) changes sign between the bounds given below, and so we have

$$\begin{aligned} \sqrt{t} + \frac{1}{2} + \frac{1}{8\sqrt{t}} - \frac{2}{8t} &< \beta^{(1)} < \sqrt{t} + \frac{1}{2} + \frac{1}{8\sqrt{t}} - \frac{1}{8t}, \\ -\sqrt{t} + \frac{1}{2} - \frac{1}{8\sqrt{t}} - \frac{1}{8t} &< \beta^{(2)} < -\sqrt{t} + \frac{1}{2} - \frac{1}{8\sqrt{t}}, \\ \frac{1}{4} - \frac{5}{64t} + \frac{22}{512t^2} &< \beta^{(3)} < \frac{1}{4} - \frac{5}{64t} + \frac{23}{512t^2}, \\ -4t - \frac{5}{4} + \frac{21}{64t} - \frac{87}{512t^2} &< \beta^{(4)} < -4t - \frac{5}{4} + \frac{21}{64t} - \frac{84}{512t^2}. \end{aligned}$$

We conclude that an integer solution to $z^2 = V_{4n+1}$ with $t_1 < t_2$ forces x/y to be close to $\beta^{(3)}$. Similarly, a solution to $z^2 = V_{4n+1}$ with $t_2 < t_1$ forces x/y to be close to $\beta^{(4)}$.

We remark that one can show in a similar way that solutions to the equation $z^2 = V_{4n+3}$ correspond to approximations x/y which are close to $\beta^{(1)}$ and $\beta^{(2)}$. We do not seem to be able to apply the hypergeometric method in this case, and so the focus of this paper will be entirely on the equation $z^2 = V_{4n+1}$, which is all that we require for the proof of Theorem 1.1.

THEOREM 2.1. *For $n \geq 1$ and for $\{V_{2n+1}(t)\}$ defined by (2.4), the equation $z^2 = V_{4n+1}(t)$ has no solutions in positive integers (z, t) with $t > 1$.*

As a consequence of this result, we do get some information on the existence of squares in the sequence $\{V_{4n+3}(t)\}$. For the details of the proof, the reader is referred to Corollary 2.5 of [18].

COROLLARY 2.1. *For $n \geq 0$ and for $\{V_{2n+1}(t)\}$ defined by (2.4), if the equation $z^2 = V_{4n+3}(t)$ has a solution in positive integers (z, t) with $t > 1$, then $4n + 3$ is prime.*

We remark that the aforementioned result of Bennett and Walsh in [1] is equivalent to the statement that the equation $z^2 = V_{2n+1}(t^2)$ has no solutions in positive integers n, z and $t > 1$.

3. An effective measure of approximation. In this section we will apply the hypergeometric method to obtain effective measures of approximation to the two roots $\beta^{(3)}$ and $\beta^{(4)}$. Because of the relation $\beta^{(3)}\beta^{(4)} = -t$, we will only need to deal with one of the roots, say $\beta^{(3)}$.

NOTATION. For positive integers n and r , we put

$$X_{n,r}(x) = {}_2F_1(-r - r - 1/n; 1 - 1/n; x),$$

where ${}_2F_1$ denotes the classical hypergeometric function given by

$${}_2F_1(a, b; c; x) = \sum_{k=0}^{\infty} \frac{(a)_k (b)_k}{(c)_k} \frac{x^k}{k!},$$

with $(z)_k$ being the Pochhammer symbol representing the product

$$z(z+1) \cdots (z+k-1).$$

It is easy to see that $X_{n,r}(x)$ is a polynomial of degree r . We will often make reference to the homogenization of $X_{n,r}(x)$, which is given explicitly by

$$X_{n,r}(x, y) = y^r X_{n,r}(x/y).$$

This abuse of notation should not lead to any confusion, as it will be clear from the context whether a univariate or bivariate polynomial is being referred to.

Our first lemma is Thue's "Fundamentaltheorem" [16] together with its relation to the hypergeometric function, as discovered by Siegel.

LEMMA 3.1. *Let α_1, α_2, c_1 and c_2 be complex numbers with $\alpha_1 \neq \alpha_2$. For $n \geq 2$, we define the following polynomials:*

$$\begin{aligned} a(x) &= \frac{n^2 - 1}{6} (\alpha_1 - \alpha_2)(x - \alpha_2), & c(x) &= \frac{n^2 - 1}{6} \alpha_1(\alpha_1 - \alpha_2)(x - \alpha_2), \\ b(x) &= \frac{n^2 - 1}{6} (\alpha_2 - \alpha_1)(x - \alpha_1), & d(x) &= \frac{n^2 - 1}{6} \alpha_2(\alpha_2 - \alpha_1)(x - \alpha_1), \\ u(x) &= -c_2(x - \alpha_2)^n, & z(x) &= c_1(x - \alpha_1)^n. \end{aligned}$$

Putting $\lambda = (\alpha_1 - \alpha_2)^2/4$, for any positive integer r , we define

$$\begin{aligned} (\sqrt{\lambda})^r A_r(x) &= a(x)X_{n,r}(z, u) + b(x)X_{n,r}(u, z), \\ (\sqrt{\lambda})^r B_r(x) &= c(x)X_{n,r}(z, u) + d(x)X_{n,r}(u, z). \end{aligned}$$

Then, for any root β of $P(x) = z(x) - u(x)$, the polynomial

$$C_r(x) = \beta A_r(x) - B_r(x)$$

is divisible by $(x - \beta)^{2r+1}$.

Proof. This is a simplified version of Lemma 2.1 from [3], obtained by noting that if $P(x)$ satisfies the differential equation given there, with $U(x) = (x - \alpha_1)(x - \alpha_2)$, then $P(x)$ must be of the form given here, which allows us to determine the above expressions.

LEMMA 3.2 ([3, Lemma 2.5]). *With the above notation, put $w(x) = z(x)/u(x)$ and write $w(x) = \mu e^{i\varphi}$ with $\mu \geq 0$ and $-\pi < \varphi \leq \pi$. Put $w(x)^{1/n} = \mu^{1/n} e^{i\varphi/n}$.*

- (i) For any nonzero $x \in \mathbb{C}$ such that $w = w(x)$ is not a negative real number or zero,

$$(\sqrt{\lambda})^r C_r(x) = \{\beta(a(x)w(x)^{1/n} + b(x)) - (c(x)w(x)^{1/n} + d(x))\} X_{n,r}(u, z) - (\beta a(x) - c(x))u(x)^r R_{n,r}(w),$$

with

$$R_{n,r}(w) = \frac{\Gamma(r+1+1/n)}{r!\Gamma(1/n)} \int_1^w ((1-t)(t-w))^r t^{1/n-r-1} dt,$$

where the integration path is the straight line from 1 to w .

- (ii) Let $w = e^{i\varphi}$, $0 < \varphi < \pi$ and put $\sqrt{w} = e^{i\varphi/2}$. Then

$$|R_{n,r}(w)| \leq \frac{n\Gamma(r+1+1/n)}{r!\Gamma(1/n)} \varphi |1 - \sqrt{w}|^{2r}.$$

LEMMA 3.3 ([3, Lemma 2.6]). Let u , w and z be as above. Then

$$|X_{n,r}^*(u, z)| \leq 4|u|^r \frac{\Gamma(1-1/n)r!}{\Gamma(r+1-1/n)} |1 + \sqrt{w}|^{2r-2}.$$

LEMMA 3.4. Let $N_{4,r}$ be the greatest common divisor of the numerators of the coefficients of $X_{4,r}(1-2x)$ and let $D_{4,r}$ be the least common multiple of the denominators of the coefficients of $X_{4,r}(x)$. Then the polynomial $(D_{4,r}/N_{4,r})X_{4,r}(1-2x)$ has integral coefficients. Moreover, $N_{4,r} = 2^r$ and

$$D_{4,r} \frac{\Gamma(3/4)r!}{\Gamma(r+3/4)} < 0.8397 \cdot 5.342^r, \quad D_{4,r} \frac{\Gamma(r+5/4)}{\Gamma(1/4)r!} < 0.1924 \cdot 5.342^r.$$

Proof. Using the so-called Kummer transformation and expanding, we can write

$$X_{4,r}(1-2x) = \sum_{i=0}^r (-1)^i \frac{(r+1) \cdots (2r-i)}{3 \cdot 7 \cdots (4r-1)} \binom{r}{i} (4r-4i+1) \cdots (4r+1) 2^{2r-i} x^i.$$

Therefore, 2^r divides $N_{4,r}$ and by examining the coefficient of x^r , we see that $N_{4,r} = 2^r$. We now turn to the inequalities.

From the arguments in the proof of Proposition 2(c) in [7], we obtain

$$D_{4,r} < \exp(1.6708r + 3.43\sqrt[3]{r}) < 5.341227^r$$

for $r \geq 20000$. Since $\exp(0.000073r) > \exp(1.46) > 2$ for such values of r , the upper bound for $D_{4,r}$ holds for $r \geq 20000$.

For $r \geq 2$,

$$\begin{aligned} \frac{\Gamma(r+5/4)}{\Gamma(1/4)r!} &= \frac{5}{16} \prod_{i=2}^r \frac{i+1/4}{i} < \frac{5}{16} \exp\left(\int_1^r \log\left(\frac{x+1/4}{x}\right) dx\right) \\ &< \frac{5}{16} \exp\left(\int_1^r \frac{dx}{4x}\right) \leq \frac{5}{16} r^{1/4}. \end{aligned}$$

As a consequence, the inequalities in the statement of the lemma hold for $r \geq 20\,000$. A computation, similar to those described in the proof of Proposition 2 in [7], shows that the same inequalities hold for all smaller values of r .

LEMMA 3.5 ([3, Lemma 2.7]). *Let $\alpha_1, \alpha_2, A_r(x), B_r(x)$ and $P(x)$ be defined as in Lemma 3.1 and let a, b, c and d be complex numbers satisfying $ad - bc \neq 0$. Define*

$$K_r(x) = aA_r(x) + bB_r(x), \quad L_r(x) = cA_r(x) + dB_r(x).$$

If $(x - \alpha_1)(x - \alpha_2)P(x) \neq 0$, then

$$K_{r+1}(x)L_r(x) \neq K_r(x)L_{r+1}(x)$$

for all $r \geq 0$.

LEMMA 3.6 ([3, Lemma 2.8]). *Let $\theta \in \mathbb{R}$. Suppose that there exist $k_0, l_0 > 0$ and $E, Q > 1$ such that for all $r \in \mathbb{N}$, there are rational integers p_r and q_r with $|q_r| < k_0 Q^r$ and $|q_r \theta - p_r| \leq l_0 E^{-r}$ satisfying $p_r q_{r+1} \neq p_{r+1} q_r$. Then for any rational integers p and q with $|q| \geq 1/(2l_0)$, we have*

$$\left| \theta - \frac{p}{q} \right| > \frac{1}{c|q|^{\kappa+1}}, \quad \text{where } c = 2k_0 Q(2l_0 E)^\kappa \quad \text{and } \kappa = \frac{\log Q}{\log E}.$$

For the remainder of this section, we shall assume that t is a fixed integer greater than 204. We shall also simplify our notation here to reflect the fact that we have $n = 4$. We shall use R_r and X_r instead of $R_{4,r}$ and $X_{4,r}$.

We now determine the quantities defined in the Lemma 3.1. Put

$$\alpha_1 = \sqrt{-t}, \quad \alpha_2 = -\sqrt{-t}, \quad c_1 = (1 + \sqrt{-t})/2, \quad c_2 = (1 - \sqrt{-t})/2.$$

Then

$$P(x) = x^4 + 4tx^3 - 6tx^2 - 4t^2x + t^2,$$

which is precisely the polynomial in (2.3).

As in Section 2, we define

$$\tau = \sqrt{t} + \sqrt{t+1}, \quad \varrho = \sqrt{\tau^2 + 1}$$

for any positive integer t .

The preliminary results above will now be used in order to obtain an effective measure of approximation to $\beta^{(3)}$. We will use the initial rational approximation $x = 0$ to $\beta^{(3)}$. By Lemma 3.2, it is desirable to have

$$\beta^{(3)} = \frac{c(x)w(x)^{1/4} + d(x)}{a(x)w(x)^{1/4} + b(x)},$$

and it is easy to see that for any particular value of x there is a fourth root $w(x)^{1/4}$ for which this identity holds. In the case of $x = 0$, we have

$$w = w(0) = \frac{1 + \sqrt{-t}}{-1 + \sqrt{-t}}, \quad \left(\frac{\tau - i}{\tau + i} \right)^2 = w, \quad \left(\frac{\tau - i}{\varrho} \right)^2 = \frac{\tau - i}{\tau + i},$$

and so

$$w^{1/4} = (i^j) \frac{\tau - i}{\varrho}$$

for some $0 \leq j \leq 3$. Using the fact that $\varrho^2 = \tau^2 + 1$, one can check that

$$\frac{-i\tau - 1 + i\varrho}{-\tau + i - \varrho} = -\tau + \varrho.$$

Now since

$$a(0) = -5t, \quad b(0) = -5t, \quad c(0) = -5t\sqrt{-t}, \quad d(0) = 5t\sqrt{-t},$$

it follows that with $j = 0$, and hence $w^{1/4} = (\tau - i)/\varrho$, the following identity holds:

$$\beta^{(3)} = \frac{c(0)w^{1/4} + d(0)}{a(0)w^{1/4} + b(0)}.$$

Therefore, the first term in the expression for $(-t)^{r/2}C_r(0)$ in Lemma 3.2 disappears. Moreover, we will see later that the above choice for the fourth root of $w(0)$ is extremely close to 1 in the complex plane, a property which is of critical importance.

We now construct our sequence of rational approximations to $\beta^{(3)}$.

By Lemmas 3.1 and 3.2, we see that $\lambda = -t$, and moreover

$$(3.1) \quad \begin{aligned} (-t)^{r/2}A_r(0) &= a(0)X_r(z(0), u(0)) + b(0)X_r(u(0), z(0)), \\ (-t)^{r/2}B_r(0) &= c(0)X_r(z(0), u(0)) + d(0)X_r(u(0), z(0)), \\ (-t)^{r/2}C_r(0) &= -(\beta^{(3)}a(0) - c(0))u(0)^r R_r(w). \end{aligned}$$

These quantities will form the basis for our approximations. We first eliminate some common factors. We can write $u(0) = -t^2(1 - \sqrt{-t})/2$ and $z(0) = t^2(1 + \sqrt{-t})/2$, and after some routine manipulations, we find that

$$\begin{aligned} (-t)^{r/2}A_r(0) &= \frac{-5t^{2r+1}N_{4,r}}{2^r D_{4,r}} \left\{ \frac{D_{4,r}}{N_{4,r}} \left[(-1)^r (1 - \sqrt{-t})^r X_r \left(1 - \frac{2}{1 - \sqrt{-t}} \right) \right. \right. \\ &\quad \left. \left. + (1 + \sqrt{-t})^r X_r \left(1 - \frac{2}{1 + \sqrt{-t}} \right) \right] \right\}, \\ (-t)^{r/2}B_r(0) &= \frac{5t^{2r+3/2}N_{4,r}}{2^r D_{4,r}} \left\{ \frac{D_{4,r}}{N_{4,r}} \left[(1 - \sqrt{-t})^r X_r \left(1 - \frac{2}{1 + \sqrt{t}} \right) \right. \right. \\ &\quad \left. \left. - (-1)^r (1 - \sqrt{t})^r X_r \left(1 - \frac{2}{1 - \sqrt{t}} \right) \right] \right\}. \end{aligned}$$

By Lemma 3.4, the quantities inside the braces can be expressed as

$$(-1)^r (e - f\sqrt{-t}) \pm (e - f\sqrt{-t}),$$

where e and f are rational integers, and recalling from Lemma 3.4 that $N_{4,r} = 2^r$, considering the cases of r being even or odd separately, we find

that

$$(3.2) \quad P_r = \frac{D_{4,r}B_r(0)}{10t^{[3r/2+3/2]}}, \quad Q_r = \frac{D_{4,r}A_r(0)}{10t^{[3r/2+3/2]}}$$

are rational integers. We note for future reference that if r is even, then P_r will be divisible by t .

The numbers in (3.2) are those that will be used as the rational approximations to $\beta^{(3)}$. We have

$$Q_r\beta^{(3)} - P_r = S_r, \quad \text{where} \quad S_r = \frac{D_{4,r}C_r(0)}{10t^{[3r/2+3/2]}}.$$

We want to show that these are good approximations, and we do this by estimating $|P_r|$, $|Q_r|$ and $|S_r|$ from above. It is readily verified that

$$|1 + \sqrt{w(0)}|^2 = 2 + 2\sqrt{t/(t+1)},$$

and hence

$$|u(0)(1 + \sqrt{w(0)})^2| = t^2(\sqrt{t+1} + \sqrt{t}).$$

Using this expression, the expressions for $a(0)$, $b(0)$, $c(0)$ and $d(0)$, Lemma 3.3, and the triangle inequality, we find, for $t \geq 204$, that

$$(3.3) \quad |Q_r| < 1.0013D_{4,r} \frac{\Gamma(3/4)r!}{\Gamma(r+3/4)} (\sqrt{t+1} + \sqrt{t})^r \\ \leq 0.85\{5.342(\sqrt{t+1} + \sqrt{t})\}^r.$$

Similarly, for $t \geq 204$ one obtains

$$(3.4) \quad |P_r| < 0.85\sqrt{t}\{5.342(\sqrt{t+1} + \sqrt{t})\}^r.$$

By Lemma 3.2 and the expressions in (3.1), we obtain

$$|S_r| \leq 2D_{4,r} \frac{\Gamma(r+5/4)}{r!\Gamma(1/4)} \varphi |\beta^{(3)} - \sqrt{-t}| \left| \frac{u(0)}{t^2} (1 - \sqrt{w(0)})^2 \right|^r,$$

and as above,

$$|u(0)(1 - \sqrt{w(0)})^2| = t^2(\sqrt{t+1} - \sqrt{t}).$$

With φ as in Lemma 3.2, it can be shown that $2\varphi/\pi \leq \sin \varphi$ and $\sin \varphi = \text{Im } w(0) = -2\sqrt{t}/(t+1)$. From our estimates for the $\beta^{(i)}$'s, we know that $0 < \beta^{(3)} < 0.25$, and so

$$\varphi |\beta^{(3)} - \sqrt{-t}| < \pi.$$

Combining these inequalities with Lemma 3.4, we obtain

$$(3.5) \quad |S_r| < 1.21\{5.342(\sqrt{t+1} - \sqrt{t})\}^r = 1.21 \left\{ \frac{\sqrt{t+1} + \sqrt{t}}{5.342} \right\}^{-r}.$$

Note also that since $\beta^{(3)}\beta^{(4)} = -t$, we have

$$(3.6) \quad tQ_r + \beta^{(4)}P_r = -\beta^{(4)}S_r.$$

We now apply Lemma 3.6 to prove the following theorem.

THEOREM 3.1. *Suppose that $t \geq 204$. Define*

$$\kappa = \frac{\log(5.342(\sqrt{t+1} + \sqrt{t}))}{\log((\sqrt{t+1} + \sqrt{t})/5.342)}.$$

For $j = 3$ and 4 , and for any rational integers p and q , we have

$$|p - \beta^{(j)}q| > \frac{1}{c_j|q|^\kappa}$$

for $|q| \geq 1$, where

$$c_3 = 18.2\sqrt{t}(0.91\sqrt{t})^\kappa, \quad c_4 = 195\sqrt{t}(1.37t)^\kappa.$$

Proof. In each case we will apply Lemmas 3.5 and 3.6. First notice that $P_rQ_{r+1} - P_{r+1}Q_r$ is a nonzero multiple of $A_{r+1}(0)B_r(0) - A_r(0)B_{r+1}(0)$. Applying Lemma 3.5, with $a = d = 1$, $b = c = 0$ and $x = 0$, we see that $P_rQ_{r+1} \neq P_{r+1}Q_r$.

For $\beta^{(3)}$, we put $p_r = P_r$ and $q_r = Q_r$. Since $\sqrt{t+1} + \sqrt{t} < 2.0025\sqrt{t}$, for $t \geq 204$, from (3.3) and (3.4), we can take $k_0 = 0.85$, $l_0 = 1.21$, $E = 0.3749\sqrt{t}$ and $Q = 10.698\sqrt{t}$. Hence we can use c_0 for the quantity c in Lemma 3.6. As well, $1/(2l_0) < 1$, which gives us the lower bound for $|q|$.

For $\beta^{(4)}$, we take advantage of the fact that P_{2r} is divisible by t . In this case let $p_r = -Q_{2r}$ and $q_r = P_{2r}/t$. Since $-4t - 2 < \beta^{(4)} < -4t$, we put $k_0 = 0.85/\sqrt{t}$, $l_0 = 1.21\beta^{(3)}/t < 4.86$, $E = 0.1406t$ and $Q = 114.45t$. Here κ is the same as in the case of $\beta^{(3)}$ and we can use c_2 for the quantity c in Lemma 3.6. Since l_0 is larger in this case, the same lower bound for $|q|$ remains valid.

4. Proof of Theorem 2.1. We have just used the hypergeometric method to determine how close a rational number x/y can possibly be to one of the roots of the polynomial $p_t(X)$ in (2.3). Let us now estimate how close such a rational number *must* be in order that (x, y) is a solution of (2.1). As noted before, the closest root to x/y must be either $\beta^{(3)}$ or $\beta^{(4)}$. By abuse of notation, we denote by $p_t(X, Y)$ the bivariate polynomial in (2.1). Henceforth, X and Y are indeterminates, while x and y represent integer solutions to equation (2.1). We will assume that $t \geq 204$, since for smaller values of t we verified Conjecture 1.1 using a SIMATH's program *faintp* on the curves $Y^2 = X^3 - t^2(t+1)X$, and doublechecked this computation using KANT's program *ThueSolve* on all Thue equations of the form given in (2.1).

We begin by proving a lower bound for $|y|$ in terms of t . We do this as follows; this is essentially Runge's method. For each of $1 \leq n \leq 21$, we compute the Puiseux expansions at infinity of the algebraic function $z(t)$ defined by $z^2 = V_{4n+1}(t)$ in order to obtain, for each n , a positive integer r_n

and integer polynomials $f_{4n+1}(t), g_{4n+1}(t)$ with the property that

$$2^{2r_n} V_{4n+1}(t) = (f_{4n+1}(t))^2 + g_{4n+1}(t),$$

with $2 \deg f_{4n+1}(t) = \deg V_{4n+1}(t) = 2n$, and $\deg g_{4n+1}(t) = n - 1$. We verified that each of the polynomials $g_{4n+1}(t)$ has no positive integer roots. We then computed positive integers c_1, \dots, c_{21} with the property that $|2f_{4n+1}(t)| > |g_{4n+1}(t)|$ for $t > c_n$, and that $z^2 = V_{4n+1}(t)$ has no integer solutions for $1 \leq t \leq c_n$. This computation was performed using MAGMA, and to be precise, we used the (integer) polynomials $V_{4n+1}(t/4)$ rather than $V_{4n+1}(t)$, as they provided smaller values for each of the c_i . In particular, the positive integers c_i increase roughly geometrically in size, with $c_1 = 1$ and $c_{21} < 3.2 \cdot 10^9$. It follows from this computation that each of the equations $z^2 = V_{4n+1}(t)$ ($1 \leq n \leq 21$) has no solutions in positive integers (z, t) .

Now, using equation (2.2), it is readily verified that for $t \geq 204$ and $k \geq 3$, one has

$$(4.1) \quad .9\tau^{k-1} < V_k \leq 1.1\tau^{k-1}.$$

In order to prove a lower bound for $|y|$, we notice that y was defined in the proof of Proposition 2.1 as either $y = H$, where

$$\sqrt{V_{4n+1}} + V_{2n+1} = 2t_2 H^2 \quad \text{if } t_1 \leq t_2,$$

or $y = G$, where

$$\sqrt{V_{4n+1}} - V_{2n+1} = 2t_1 G^2 \quad \text{if } t_2 \leq t_1.$$

We will deal only with the latter case, as the former can be dealt with in the same way, and actually produces a larger lower bound for $|y|$.

It is easy to see that

$$\sqrt{V_{4n+1}} - V_{2n+1} = \frac{V_{2n}}{\sqrt{(V_{2n+1}/V_{2n})^2 + 1} + V_{2n+1}/V_{2n}},$$

and so from (4.1), we deduce that

$$2t_1 y^2 > (1/4)\tau^{2n-2} > (1/4)2^{2n-2}(\sqrt{t})^{2n-2}.$$

Since $t_1 \leq t$ and $n \geq 22$, we finally deduce that

$$(4.2) \quad |y| > 2^{19} t^{10}.$$

We now estimate how close x/y must be to $\beta^{(3)}$ and $\beta^{(4)}$. The inequality in (4.2) shows that we need only deal with $|y| \geq 4$. Let us assume first that (x, y) is a solution of equation (2.1) with x/y closest to $\beta^{(3)}$. In this case, $|x - \beta^{(3)}y| \leq t^{1/4}$, for otherwise $|p_t(x, y)| > t$, and so x/y is greater than $\beta^{(3)} - t^{1/4}/4$. Therefore,

$$\left| \frac{x}{y} - \beta^{(4)} \right| > \beta^{(3)} - \frac{t^{25}}{4} - \beta^{(4)} > 4t - \frac{t^{25}}{4} + \frac{3}{2} - \frac{13}{32t} + \frac{53}{256t^2},$$

by our estimates for the size of the roots.

Similarly, we also have

$$\left| \frac{x}{y} - \beta^{(1)} \right|, \left| \frac{x}{y} - \beta^{(2)} \right| > \sqrt{t} - \frac{t^{.25}}{4} + \frac{1}{2} + \dots,$$

and upon combining the above, assuming that $t \geq 204$,

$$\prod_{i \neq 3} \left| \frac{x}{y} - \beta^{(i)} \right| > 3.9t^2.$$

Therefore, if $|p_t(x, y)| = t_0^2 \leq t$, with $t \geq 204$, then

$$(4.3) \quad \left| \frac{x}{y} - \beta^{(3)} \right| < \frac{y^{-4}}{3.9t}.$$

Equation (4.3) shows that if x/y is closest to $\beta^{(3)}$ and $|y| \geq 4$, then x/y must be a convergent in the continued fraction expansion of $\beta^{(3)}$, since the right-hand side of (4.3) is less than $1/(2y^2)$ for such values of y .

If the closest root to x/y is $\beta^{(4)}$, then $|x - \beta^{(4)}y| < t^{.25}$, and so x/y must be less than $\beta^{(4)} + t^{.25}/4$. Therefore,

$$\left| \frac{x}{y} - \beta^{(3)} \right| > \beta^{(3)} - \frac{t^{.25}}{4} - \beta^{(4)} > 4t - \frac{\sqrt{t}}{4} + \frac{3}{2} - \frac{13}{32t} + \frac{53}{256t^2},$$

and we also have

$$\left| \frac{x}{y} - \beta^{(1)} \right|, \left| \frac{x}{y} - \beta^{(2)} \right| > 4t - \frac{t^{.25}}{4} - \dots.$$

We similarly conclude that for $t \geq 204$,

$$\prod_{i \neq 4} \left| \frac{x}{y} - \beta^{(i)} \right| > 63.9t^3,$$

and also, if $|p_t(x, y)| = t_0^2 \leq t$, then

$$(4.4) \quad \left| \frac{x}{y} - \beta^{(4)} \right| < \frac{|y|^{-4}}{63.9t^2}.$$

As before, we deduce that if x/y is closest to $\beta^{(4)}$ and $|y| \geq 4$, then x/y must be a convergent in the continued fraction expansion of $\beta^{(4)}$.

By Theorem 3.1, (4.3) and (4.4), if (x, y) is any further solution of equation (2.1), arising from the equation $z^2 = V_{4n+1}(t)$, then x/y is either a convergent to $\beta^{(3)}$ and

$$(4.5) \quad |y|^{3-\kappa} < \frac{18.2\sqrt{t}}{3.9t} (0.91\sqrt{t})^\kappa,$$

or a convergent to $\beta^{(4)}$ and

$$(4.6) \quad |y|^{3-\kappa} < \frac{195\sqrt{t}}{63.9t^2} (1.37t)^\kappa,$$

provided that $t \geq 204$.

Combining (4.5) with the lower bound for $|y|$ in (4.2) shows that $t \leq 240$, while combining (4.6) with (4.2) shows that $t \leq 262$. We therefore used the programs *faintp* in SIMATH and *ThueSolve* in KANT once again to verify Conjecture 1.1 for t in the range $204 \leq t \leq 262$.

This completes the proof of Theorem 2.1.

5. Further auxiliary results. In this section we will collect those results which will be needed in the course of proving Theorem 1.1.

LEMMA 5.1. *Let $d > 1$ be a squarefree integer, and let $\varepsilon_d = T + U\sqrt{d}$ denote the minimal unit (> 1) in $\mathbb{Q}(\sqrt{d})$. Then*

$$\varepsilon_d = \tau^2, \quad \text{where } \tau = \frac{a\sqrt{m} + b\sqrt{n}}{\sqrt{c}},$$

$c \in \{1, 2\}$, a, b are positive integers for which $U = 2ab/c$, m, n are positive integers for which $d = mn$, m is not a square if $c = 1$, and $a^2m - b^2n = c$.

Proof. This is well known; for example see Nagell [13].

LEMMA 5.2. *Let $d > 1$ denote a nonsquare positive integer, $\varepsilon_d = T + U\sqrt{d}$ be the minimal solution to $X^2 - dY^2 = 1$, and $T_k + U_k\sqrt{d} = \varepsilon_d^k$ for $k \geq 1$. If $T_k = x^2$ for some integer x , then either $k = 1$ or $k = 2$.*

Proof. This is in [4], and proved independently by Sun and Yuan [15]. This result improves upon classical work of Ljunggren. For a detailed account of the entire proof, the reader is referred to the first section of [18].

Let $\{T_k\}$ and $\{U_k\}$ be as above. For a positive integer b we define the rank of apparition of b in $\{T_k\}$ (resp. $\{U_k\}$) to be the minimal index k such that b divides some term T_k (resp. U_k), provided such an index exists, and denote it by $\beta(b)$ (resp. $\alpha(b)$). It is well known that $\alpha(b)$ exists for all positive integers b , but $\beta(b)$ may or may not exist.

LEMMA 5.3. *Let $d > 1$ denote a nonsquare positive integer, and $b > 1$ a squarefree integer.*

- (i) *If $T_k = bx^2$ for some integer x , then $k = \alpha(b)$. In particular, if $T_k = 2x^2$ for some integer x , then $k = 1$.*
- (ii) *If $U_k = bx^2$ and $\alpha(b)$ is even, then $k = \alpha(b)$, except only in the case that $2T_1^2 - 1 = v^2$ for some integer v , and $T_1U_1 = bu^2$ for some integer u , in which case $U_4 = U_{2\alpha(b)} = b(2uv)^2$.*

Proof. For part (i), see [1, Theorem 1 and Corollary 1], while for part (ii) see [19].

LEMMA 5.4. *Let a and b be positive integers, a nonsquare, such that*

$$aX^2 - bY^2 = 1$$

is solvable in integers, and let $\tau_{a,b} = V\sqrt{a} + U\sqrt{b}$ denote its minimal solution with V and U positive integers, and

$$\tau^{2k+1} = V_{2k+1}\sqrt{a} + U_{2k+1}\sqrt{b} \quad (k \geq 0).$$

Write U in the form $U = lv^2$ with l odd and squarefree. If (x, y) is a positive integer solution of the quartic equation $aX^2 - bY^4 = 1$, then l is odd and $y^2 = U_l$.

Proof. This is a theorem of Ljunggren [10]. The reader may wish to consult [18] for a detailed account of the proof and related problems.

We remark that the *abc* conjecture suggests that if the value l in Lemma 5.4 is greater than 5, then the equation $aX^2 - bY^4 = 1$ cannot have any positive integer solutions. A proof of this open problem would provide an approach to prove Conjecture 1.2 which is quite different than the approach using Conjecture 1.1, which was suggested in Section 1. The reader is referred to [20] for more details.

LEMMA 5.5. *Let a and b be odd positive integers, such that $aX^2 - bY^2 = 2$ is solvable in odd integers X and Y . Let $\tau_{a,b} = (V\sqrt{a} + U\sqrt{b})/\sqrt{2}$ denote its minimal solution with V and U odd positive integers, and*

$$\tau^{2k+1} = \frac{V_{2k+1}\sqrt{a} + U_{2k+1}\sqrt{b}}{\sqrt{2}} \quad (k \geq 0).$$

If (x, y) is a positive integer solution of the quartic equation $aX^2 - bY^4 = 2$, then either $y^2 = U_1$ or $y^2 = U_3$.

Proof. This has recently been proved in [11], improving upon previous work of Ljunggren.

The last result we state in this section is a consequence of Corollaries 1.1 and 2.1.

LEMMA 5.6. *Let a and b be positive integers, a nonsquare, such that the equation $aX^2 - bY^2 = 1$ is solvable in positive integers X, Y , and let $\tau_{a,b} = V\sqrt{a} + U\sqrt{b}$ denote its minimal solution, and $\tau_{a,b}^{2k+1} = V_{2k+1}\sqrt{a} + U_{2k+1}\sqrt{b}$. If the quartic equation $aX^4 - bY^2 = 1$ has a solution (x, y) , then $x^2 = V_{2k+1}$ for some k , and either $2k + 1 = 1$ or $2k + 1$ is a prime $p \equiv 3 \pmod{4}$. Furthermore, if V_{2k+1} is a square for some index $2k + 1$, then V_1 is also a square.*

6. Proof of Theorem 1.1. Let k denote an index with the property that $U_k = y^2$ for some integer y . If k is even, $k = 2r$, then $y^2 = U_k = U_{2r} = 2T_r U_r$, from which it follows that T_r is either a square or twice a square. By Lemma 5.2, we see that $r = 1$ or $r = 2$, and hence $k = 2$ or $k = 4$.

With D as in the statement of the theorem, let $D = dw^2$, with w a positive integer, and d a squarefree positive integer. Let $\varepsilon_d = t + u\sqrt{d}$ (resp. $\varepsilon_D = T + U\sqrt{d}$) denote the minimal solution to $X^2 - dY^2 = 1$ (resp. $X^2 - DY^2 = 1$), and define r_D to be the positive integer for which $\varepsilon_d^{r_D} = \varepsilon_D$, i.e. $r_D = \log(\varepsilon_D)/\log(\varepsilon_d)$.

Assume first that r_D is even. Let $t_k + u_k\sqrt{d} = (\varepsilon_d)^k$. Then $U_k = y^2$ for some integer y if and only if $u_{2k_1} = wz^2$ for some integer z , where $2k_1 = kr_D$. If w divides u_{k_1} , then t_{k_1} is a square, and Lemma 5.2 implies that $k_1 = 1$ or $k_1 = 2$. It follows that $k \in \{1, 2, 4\}$. If w does not divide u_{k_1} , then the rank of apparition $\alpha(w)$ of w in the sequence $\{u_k\}$ is even, and so by Lemma 5.3, either $2k_1 = 4$ or $2k_1 = \alpha(w)$. Since $2k_1 = kr_D$ and since $\alpha(w)$ clearly divides r_D , we see that $k \in \{1, 2, 4\}$.

We henceforth assume that both k and r_D are odd positive integers. In this case we can assume that U_1 is properly divisible by 2 to an even power, for otherwise the binomial theorem shows that U_k is properly divisible by 2 to an odd power for all odd positive integers k . Appealing to Lemma 5.1, we see that $\varepsilon_D = \tau^2$ with

$$\tau = \frac{A_1\sqrt{a} + B_1\sqrt{b}}{\sqrt{c}}, \quad c \in \{1, 2\},$$

a a nonsquare positive integer, $A_1^2a - B_1^2b = c$, $D = 4^{2-c}ab$, $U_k = A_kB_k$, and $\gcd(A_k, B_k) = 1$ for all odd $k \geq 1$, where

$$\tau^k = \frac{A_k\sqrt{m} + B_k\sqrt{n}}{\sqrt{c}}.$$

Therefore, U_k is a square precisely when both A_k and B_k are squares.

We will consider the cases $c = 1$ and $c = 2$ separately. Suppose first that $c = 1$. By Lemma 5.4, B_k can only be a square when $k = l$, where $B_1 = lv^2$ for some squarefree positive integer l and some integer v . By Lemma 5.6, if A_k is a square, then so is A_1 , and $k = 1$ or k is a prime $p \equiv 3 \pmod{4}$. Combining these two results shows that either $U_1 = W^2$ for some integer W and $k = 1$, or $U_1 = A_1B_1 = pW^2$ and $k = p$.

Now assume that $c = 2$. If U_k is a square, then by the same reasoning as in the previous case, A_k and B_k must both be squares, and so Lemma 5.5 shows that $k = 1$ or $k = 3$. Since $A_3 = A_1(2A_1^2 - 3)$ is not a square for any positive integer A_1 , it follows that $k = 1$. This completes the proof of Theorem 1.1.

Acknowledgements. We thank Karl Dilcher and Emanuel Herrmann for their help in computation and for encouragement. The third author gratefully acknowledges support from the Natural Sciences and Engineering Research Council of Canada.

References

- [1] M. A. Bennett and P. G. Walsh, *The Diophantine equation $b^2X^4 - dY^2 = 1$* , Proc. Amer. Math. Soc. 127 (1999), 3481–3491.
- [2] R. T. Bumby, *The Diophantine equation $3x^4 - 2y^2 = 1$* , Math. Scand. 21 (1967), 144–148.
- [3] J. H. Chen and P. M. Voutier, *A 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.
- [4] J. H. E. Cohn, *The Diophantine equation $x^4 - Dy^2 = 1$, II*, Acta Arith. 78 (1997), 401–403.
- [5] C. Ko, *On the diophantine equation $x^2 = y^n + 1$, $xy \neq 0$* , Sci. Sinica (Notes) 14 (1965), 457–460.
- [6] G. Lettl and A. Pethő, *Complete solution of a family of quartic Thue equations*, Abh. Math. Sem. Univ. Hamburg 65 (1995), 365–383.
- [7] G. Lettl, A. Pethő and P. M. Voutier, *Simple families of Thue inequalities*, Trans. Amer. Math. Soc. 351 (1999), 1871–1894.
- [8] W. Ljunggren, *Zur Theorie der Gleichung $x^2 + 1 = Dy^4$* , Avh. Norske Vid. Akad. Oslo 1942, no. 5, 1–27.
- [9] —, *Einige Eigenschaften der Einheiten reeller quadratischer und rein-biquadratischer Zahlkörper mit Anwendung auf die Lösung einer Klasse unbestimmter Gleichungen vierten Grades*, Oslo Vid.-Akad. Skrifter 1936, no. 12, 1–73.
- [10] —, *Ein Satz über die diophantische Gleichung $Ax^2 - By^4 = C$ ($C = 1, 2, 4$)*, Tolfte Skand. Matematikerkongressen, Lund, 1953, Lunds Universitets Matematiska Inst., Lund, 1954, 188–194.
- [11] F. Luca and P. G. Walsh, *Squares in Lehmer sequences and some Diophantine applications*, Acta Arith. 100 (2001), 47–62.
- [12] L. J. Mordell, *Diophantine Equations*, Academic Press, New York, 1969.
- [13] T. Nagell, *On a special class of Diophantine equations of the second degree*, Ark. Mat. 3 (1954), 51–65.
- [14] A. Rotkiewicz, *Applications of Jacobi's symbol to Lehmer's numbers*, Acta Arith. 42 (1983), 163–187.
- [15] Q. Sun and P. Z. Yuan, *A note on the Diophantine equation $x^4 - Dy^2 = 1$* , Sichuan Daxue Xuebao 34 (1997), 265–268.
- [16] A. Thue, *Ein Fundamentaltheorem zur Bestimmung von Annäherungswerten aller Wurzeln gewisser ganzer Funktionen*, J. Reine Angew. Math. 138 (1910), 96–108.
- [17] D. T. Walker, *On the Diophantine equation $mX^2 - nY^2 = \pm 1$* , Amer. Math. Monthly 74 (1967), 504–513.
- [18] P. G. Walsh, *Diophantine equations of the form $aX^4 - bY^2 = \pm 1$* , in: Algebraic Number Theory and Diophantine Analysis (Graz, 1998), de Gruyter, Berlin, 2000, 531–554.
- [19] —, *The Diophantine equation $X^2 - db^2Y^4 = 1$* , Acta Arith. 87 (1998), 179–188.

- [20] P. G. Walsh, *A note on Ljunggren's theorem about the Diophantine equation $aX^2 - bY^4 = 1$* , C. R. Math. Acad. Sci. Soc. R. Can. 20 (1998), 113–118.
- [21] P. Z. Yuan, *Rational and algebraic approximations of algebraic numbers and their application*, Sci. China Ser. A 40 (1997), 1045–1051.

Department of Mathematics
Purdue University North Central
1401 S. U.S. 421
Westville, IN 46391, U.S.A.
E-mail: atogbe@pnc.edu

UBS 100 Liverpool Street
London, EC2M 2RH, United Kingdom
E-mail: paul.voutier@ubs.com

Department of Mathematics
University of Ottawa
585 King Edward St.
Ottawa, Ontario, Canada, K1N 6N5
E-mail: gwalsh@mathstat.uottawa.ca

Received on 2.11.2004
and in revised form on 6.7.2005

(4879)