Diophantine equations of the form $aX^4 - bY^2 = \pm 1$.

P.G. Walsh
University of Ottawa

July 10, 2000

1991 Mathematics Subject Classification: 11D25, 11J86

1 Introduction

The problem of determining all integer solutions to cubic and quartic Diophantine equations has gained a considerable amount of interest in recent years. ¿From work of Tzanakis and de Weger [48], Gebel, Pethö, and Zimmer [20], Stroeker and Tzanakis [44], Tzanakis [47], and others, methods are now in place to completely solve Diophantine equations which are reducible to the problem of finding all integer points on an elliptic curve whose coefficients are not too large. On the other hand, classical methods of Ljunggren lend themselves to the simultaneous resolution of infinite families of elliptic curves given by certain quartic models. This resolution amounts to the determination of all squares in certain linear recurrences, a topic which has similarly attracted a considerable amount of attention.

In this paper we survey some of Ljunggren's most notable results on the class of Diophantine equations given in the title. As some of his proofs are not so accessible, we provide some details of his methods. Out of Ljunggren's work come some very interesting problems, some of which are treatable by current methods, and also some of which are yet unsolved. We discuss some of these recent advances, as well as isolate the unsolved problems in the form of conjectures. The basis for these conjectures is an effective version of the abc conjecture, which suggests precise results regarding these unsolved problems.

We have restricted our attention to equations of the form $aX^4 - bY^2 = c$ with $c = \pm 1$. There are a host of papers which deal with the cases $c = \pm 1, \pm 2, \pm 4$. The reader should consult [12], [13], [14], [16], [30], [31], [32], [33], [34], and [36], for details on this more general problem. For more general literature on this entire topic, the reader may wish to consult [35], [37], or [41].

2 Equations of the form $aX^4 - bY^2 = 1$

2.1 The equation $X^4 - dY^2 = 1$

We begin with a study of integer solutions to Diophantine equations of the form

$$X^4 - dY^2 = 1, \tag{2.1}$$

where d is a positive nonsquare integer. It is well known that the equation

$$X^2 - dY^2 = 1, \tag{2.2}$$

is always solvable in integers, and that all solutions can be obtained from a minimal solution. Let $(X, Y) = (T, U)$ denote the positive integer solution to (2.2) with U minimal, then $\epsilon_d = T + U\sqrt{d}$ is

the minimal unit greater than one in $\mathbf{Z}[\sqrt{d}]$ of positive norm, and all solutions of (2.2) are given by $(X, Y) = (T_k, U_k)$, where

$$\epsilon_d^k = T_k + U_k\sqrt{d}. \quad k \geq 1 \tag{2.3}$$

Thus, determining all solutions of (2.1) is equivalent to determining all squares in $\{T_k\}$. We will often refer to the units in (2.3) as being the solutions of (2.2).

In [28], Ljunggren proved the following remarkable result. We present the details of Ljunggren's proof, as [28] is rather inaccessible, and the original proof unfortunately contains some minor errors.

Theorem 2.1 *Let d denote a nonsquare positive integer. The Diophantine equation* (2.1) *has at most two solutions in positive integers (X, Y). In particular, there is at most one odd index k for which T_k is a square, at most one index $k \equiv 2 \pmod 4$ for which T_k is a square, and no indices $k \equiv 0 \pmod 4$ for which T_k is a square.*

Proof. The case $k \equiv 2 \pmod 4$ is identical to that for odd k by simply applying the proof to the square of the minimal solution to $X^2 - dY^2 = 1$. Thus, it suffices to consider the proof for odd indices k, and the case $k \equiv 0 \pmod 4$, which we do first.

Since $T_{4i} = 8T_i^4 - 8T_i^2 + 1$, it will be shown that the only solution in positive integers (x, y) to the equation

$$y^2 = 8x^4 - 8x^2 + 1$$

is $(x, y) = (1, 1)$. Note that this equation can be rewritten as $y^2 - 2(2x^2 - 1)^2 = -1$. For $i \geq 1$, define sequences $\{P_i\}$ and $\{Q_i\}$ by $(1 + \sqrt{2})^i = P_i + Q_i\sqrt{2}$. Thus,

$$2x^2 - 1 = Q_{2i+1}$$

for some $i \geq 0$, from which it follows that

$$2x^2 - 1 = P_{2i} + Q_{2i} = 2P_i^2 - (-1)^i + 2P_iQ_i.$$

If i is even, then $x^2 = P_i(P_i + Q_i)$, and so there are positive integers a and b such that $P_i = a^2$ and $Q_i = x^2 - a^2$. Since i is even, $P_i^2 - 2Q_i^2 = 1$, and so $a^4 - 2(x^2 - a^2)^2 = 1$, showing that either $a^2 + 1$ or $a^2 - 1$ is a square. This forces $a = P_i = 1$, $i = 0$, $Q_{2i+1} = 1$, and so $x = 1$.

If i is odd, then

$$x^2 = P_iQ_i + P_i^2 + 1 = P_iQ_i + 2Q_i^2 = Q_i(P_i + 2Q_i),$$

and so there are positive integers a and b such that $Q_i = a^2$ and $P_i = b^2 - 2a^2$. Since in this case $P_i^2 - 2Q_i^2 = -1$, it follows that $b^4 - 2(b^2 - a^2)^2 = 1$, from which we conclude as above that $b = 1$. This forces $a = 1$ and $P_i = -1$, which contradicts the fact that i is positive.

For the remainder of the proof of Theorem 2.1 we consider the case that k is odd.

We first show that all solutions of (2.1) are powers of a unit which is of the form $u^2 + v\sqrt{d}$. Assume that (2.1) is solvable, with $\epsilon_d^k = T_k + U_k\sqrt{d} = x^2 + U_k\sqrt{d}$ being a solution. Assume further that $\epsilon_d = l_0v_0^2 + U\sqrt{d}$, with l_0 squarefree. It follows from the binomial theorem that l_0 is odd. If $l_0 = 1$, the claim follows. If $l_0 > 1$, then by the binomial theorem it is easily deduced that l_0 divides k. Consider the unit $\epsilon_d^{l_0} = T_{l_0} + U_{l_0}\sqrt{d}$, and assume that $T_{l_0} = v_1l_1^2$ with l_1 odd and squarefree. If $l_1 = 1$, then the claim holds, otherwise $l_1 > 1$, and it follows that l_0l_1 divides k. Since k is finite this process must terminate, and there are squarefree odd positive integers $l_0, l_1, \ldots, l_t$, all greater than 1, such that $l_0l_1 \cdots l_t$ divides k, and $T_{l_0l_1\cdots l_t} = u^2$ for some integer u. This proves the claim.

Let $E = u^2 + v\sqrt{d}$ be the unit $\epsilon_d^{l_0l_1\cdots l_t}$ constructed in the previous paragraph, and let m denote an odd positive integer such that

$$E^m = x^2 + y\sqrt{d}.$$

¿From the binomial theorem it follows that

$$x^2 - 1 = (u^2 - 1)M^2, \;\; x^2 + 1 = (u^2 + 1)N^2 \tag{2.4}$$

for positive integers M and N. Let $\tau = \sqrt{u+1} + \sqrt{u-1}$, then $\tau^2 = 2E$, and similarly $(\sqrt{x+1} + \sqrt{x-1})^2 = 2E^m$. Therefore, $\sqrt{x+1} + \sqrt{x-1} = \tau E^{\frac{m-1}{2}}$, and so

$$x + 1 = (u + 1)R^2,$$

for some positive integer R. A similar argument shows that

$$x + i = (u + i)S^2,$$

for some Gaussian integer S. From the relation

$$(1 + i)(u + 1)R^2 - (1 + i)(u + i)S^2 = 2$$

one sees that

$$\xi = R^2(1 + i)(u + 1) - 1 + RS(1 + i)\sqrt{(u + 1)(u + i)}$$

is a unit in the order $\mathbf{Z}[1, i, \theta, i\theta]$ in the ring of integers of the field $\mathbf{Q}(\theta)$ whose norm to $\mathbf{Q}(i)$ is 1, where

$$\theta = \sqrt{(u + 1)(u + i)}.$$

Since $[\mathbf{Q}(\theta) : \mathbf{Q}] = 4$, and $\mathbf{Q}(\theta)$ has a complex embedding, it follows from Dirichlet's unit theorem that $\xi = \rho\alpha^r$, where α is a unit in $\mathbf{Z}[1, i, \theta, i\theta]$ whose norm to $\mathbf{Q}(i)$ is a fourth root of unity, $\rho = \pm 1$ or $\rho = \pm i$, and r is an integer. Since

$$\xi = \frac{1}{2}(R\sqrt{(1 + i)(u + 1)} + S\sqrt{(1 + i)(u + i)})^2,$$

and $R\sqrt{(1 + i)(u + 1)} + S\sqrt{(1 + i)(u + i)}$ does not lie in $\mathbf{Q}(\theta)$, r must be odd. Therefore there is no loss of generality in assuming that $\rho = \pm 1$, and moreover that the relative norm of α to $\mathbf{Q}(i)$ is 1. As $(x + 1) = R^2(u + 1)$, we have

$$\begin{aligned}
\xi &= (x + 1)(1 + i) - 1 + RS(1 + i)\theta = \pm\alpha^r, \\
\xi' &= (x + 1)(1 + i) - 1 - RS(1 + i)\theta = \pm(\alpha')^r, \\
\xi'' &= (x + 1)(1 - i) - 1 + RS''(1 - i)\theta_1 = \pm(\alpha'')^r, \\
\xi''' &= (x + 1)(1 - i) - 1 - RS''(1 - i)\theta_1 = \pm(\alpha''')^r,
\end{aligned}$$

where $\theta_1 = \sqrt{(u + 1)(u - i)}$, and for $\nu \in \mathbf{Q}(\theta)$, ν' denotes the image of ν under the mapping $\theta \to -\theta$, ν'' denotes the image of ν under complex conjugation, and ν''' is the image of ν under the composition of both mappings.

¿From these equations it follows that

$$\alpha^r + (\alpha')^r \pm 2 = i((\alpha'')^r + (\alpha''')^r \pm 2). \tag{2.5}$$

Note that from $\alpha\alpha' = 1$, there is no loss in generality in assuming in equation (2.5) that r is positive. Now let $\lambda = u + i(1 + u) + (1 + i)\theta$, then λ is a unit in the ring of integers of $\mathbf{Q}(\theta)$, $\lambda\lambda' = 1$, $|\lambda| > 1$ and hence $\lambda = \pm\alpha^s$ for some positive integer s. It is easy to see that the square of an element in $\mathbf{Z}[1, i, \theta, i\theta]$ cannot have $1 + i$ as the coefficient of θ, and so s must be odd. Replacing α by $-\alpha$ if necessary, we can assume that $\lambda = \alpha^s$.

We wish to show that $s = 1$. Assume on the contrary that $s > 1$. Let

$$\alpha = e + fi + (g + hi)\theta,$$

then

$$g = (\frac{\alpha - \alpha'}{4\theta}) + (\frac{\alpha'' - \alpha'''}{4\theta_1}),$$

and so it is readily deduced that

$$|g| < \frac{1 + |\lambda|^{\frac{1}{s}}}{2|\theta|} < \frac{1 + \sqrt{|\lambda}}{2|\theta|}.$$

¿From the definition of λ one has that

$$|\lambda| < 3(u + 1).$$

¿From the definition of θ

$$|\theta| = |\theta_1| = \sqrt{(u + 1)\sqrt{u^2 + 1}},$$

from which it follows that

$$|g| < \frac{1 + \sqrt{3(u + 1)}}{2\sqrt{(u + 1)\sqrt{u^2 + 1}}} < 1$$

since $u \geq 2$. Since g is an integer we deduce that $g = 0$. A similar argument shows that $h = 0$, from which it follows that $\alpha \in \mathbf{Q}(i)$, a contradiction. Therefore $s = 1$, and $\lambda = \alpha$.

¿From the definition of λ, and the fact that $\lambda = \alpha$,

$$\alpha + (\alpha') + 2 = i((\alpha'') + (\alpha''') + 2),$$

and so by equation (2.5) either

$$\frac{\alpha^r + (\alpha')^r + 2}{\alpha + (\alpha') + 2} = \frac{(\alpha'')^r + (\alpha''')^r + 2}{(\alpha'') + (\alpha''') + 2} \tag{2.6}$$

or

$$\frac{\alpha^r + (\alpha')^r - 2}{\alpha + (\alpha') + 2} = \frac{(\alpha'')^r + (\alpha''')^r - 2}{(\alpha'') + (\alpha''') + 2}. \tag{2.7}$$

In the case (2.7) holds, it follows that

$$\frac{\alpha^r + (\alpha')^r + 2}{\alpha + (\alpha') + 2} - \frac{(\alpha'')^r + (\alpha''')^r + 2}{(\alpha'') + (\alpha''') + 2} = \frac{4}{\alpha + (\alpha') + 2} - \frac{4}{(\alpha'') + (\alpha''') + 2} = -\frac{2i}{a}. \tag{2.8}$$

The lefthand side of (2.8) is a Gaussian integer, while the right hand side is of absolute value less than one since $a = u + 1 \geq 3$. Therefore, (2.8) is not possible.

In the case of (2.6), the identity

$$\frac{\alpha^r + (\alpha')^r + 2}{\alpha + (\alpha') + 2} = \sum_{h=0}^{r-1} \frac{r}{h + 1} \left(\begin{array}{c} r + h \\ 2h + 1 \end{array} \right) (\alpha + \alpha' + 2)^h (-1)^h,$$

it is deduced that

$$r^2 - \frac{r^2(r^2 - 1)}{4!} 2(\alpha + \alpha' + 2) + \frac{r^2(r^2 - 1)(r^2 - 2^2)}{6!} 2(\alpha + \alpha' + 2)^2 - \cdots =$$

$$r^2 - \frac{r^2(r^2-1)}{4!}2(\alpha'' + \alpha''' + 2) + \frac{r^2(r^2-1)(r^2-2^2)}{6!}2(\alpha'' + \alpha''' + 2)^2 - \cdots.$$

For brevity put $u+1 = a$, $1+i = \gamma$, $1-i = \delta$, then $\alpha + \alpha' + 2 = 2a\gamma$ and $\alpha'' + \alpha''' + 2 = 2a\delta$, which from the above results in

$$\frac{r^2(r^2-1)}{4!}2a(\gamma - \delta) - \frac{r^2(r^2-1)(r^2-2^2)}{6!}4a^2(\gamma^2 - \delta^2) + \cdots = 0.$$

¿From the definition of γ and δ we deduce finally that

$$\begin{aligned}\frac{r^2(r^2-1)}{4!} - \frac{r^2(r^2-1)(r^2-2^2)}{6!}4a + \frac{r^2(r^2-1)(r^2-2^2)(r^2-3^2)}{8!}8a^2 - 0 + \cdots \\ + \frac{r^2(r^2-1)\cdots(r^2-(4t+1)^2)}{(8t+4)!}(2a)^{4t}2^{2t}(-1)^t \\ - \frac{r^2(r^2-1)\cdots(r^2-(4t+2)^2)}{(8t+6)!}(2a)^{4t+1}2^{2t+1}(-1)^t \\ + \frac{r^2(r^2-1)\cdots(r^2-(4t+3)^2)}{(8t+8)!}(2a)^{4t+2}2^{2t+1}(-1)^t - 0 + \cdots = 0.\end{aligned}$$

Recall that r is odd. Let $\mu \geq 3$ denote the integer such that $r^2 - 1 = 2^\mu r'$, with r' odd. Then the leading term in the previous equation is exactly divisible by $2^{\mu-3}$, while it is readily checked that all further terms are divisible by $2^{\mu-2}$, showing that $r = 1$.

Thus, $r = 1$, and using the fact that $\lambda = \alpha$, it follows that $x = u$, and hence $m = 1$. Therefore, the only solution to (2.1) coming from an odd power of ϵ_d is $E = u^2 + v\sqrt{d}$. □

Remark. Ljunggren goes on to show, in the notation given in the proof above, that the only possible value for E is $\epsilon_d^{l_0}$. We forego these details since this is superceded by a newer and stronger result.

The following result is due to Chao Ko [21], but has been rediscovered in one form or another by Zhu [54], Le [24], Cohn [17], and Chen and Voutier [10]. It provides the basis for an improvement to Theorem 2.1. In what follows $(\frac{*}{*})$ denotes the Jacobi symbol.

Lemma 2.1 *Let d denote a positive nonsquare integer, and let $\{T_k\}$ denote the corresponding sequence, defined in (2.3). Assume that $T_1 = r^2 t$ with t odd and squarefree. Define a sequence $\{w_{2k+1}\}$ for $k \geq 0$ by*

$$w_{2k+1} = T_{2k+1}/T_1.$$

Then for all $k \geq 0$ with $\gcd(T_1, 2k+1) = 1$,
(i) $w_{2k+1} \equiv 1 \pmod 4$,
(ii) $(\frac{w_{2k+1}}{t}) = (\frac{t}{2k+1}) = (\frac{T_1}{2k+1})$, and
(iii) $\gcd(2l+1, 2k+1) = 1$ implies $(\frac{w_{2k+1}}{w_{2l+1}}) = 1$.

The details of the proof are readily available in [17], although it only involves simple inductive arguments. As an immediate consequence, we have following fundamental result.

Corollary 2.1 *If T_{2k+1} is a square for some $k \geq 0$, then so is T_1. If T_{4k+2} is a square for some $k \geq 0$, then so is T_2.*

Proof. We prove only the first statement, as the proof of the second statement is the same. Assume that $T_1 = r^2 t$ with t odd and squarefree (otherwise there is no term in $\{T_{2k+1}\}$ which can be a square).

If T_{2k+1} is a square, then by definition $w_{2k+1} = tz^2$ for some integer z. Therefore, for all integers l with $\gcd(2k+1, 2l+1) = 1$ and $\gcd(T_1, 2l+1) = 1$,

$$1 = (\frac{w_{2k+1}}{w_{2l+1}}) = (\frac{t}{w_{2l+1}}) = (\frac{w_{2l+1}}{t}) = (\frac{t}{2l+1}) = (\frac{T_1}{2l+1}).$$

By choosing l so that $l \equiv 1 \pmod 4$ and $2l+1$ is a quadratic nonresidue mod T_1, it follows that T_1 must be a square.□

Combining the results of Theorem 2.1 and Corollary 2.1, we deduce the following complete solution of equation (2.1), as was stated in [17].

Theorem 2.2 *Let d denote a positive squarefree integer, and let $\epsilon_d = T + U\sqrt{d}$ denote the minimal solution to (2.2). Then the only possible solutions to equation (2.1) are ϵ_d and ϵ_d^2. Solutions to (2.1) arise from both ϵ_d and ϵ_d^2 only for $d = 1785$, and hence apart from this exceptional value, there is only one solution to (2.1) in positive integers (X, Y), and it can be described explicitly.*

Proof. By Theorem 2.1 and Corollary 2.1, the only possible positive integers k for which T_k is a square are $k = 1$ and $k = 2$. If both are squares, then there are positive integers $a > 1$ and b for which $T_1 = a^2$ and $b^2 = T_2 = 2T_1^2 - 1 = 2a^4 - 1$. In [27], Ljunggren proved that the only positive integer solutions to $X^2 - 2Y^4 = -1$ are $(X, Y) = (1, 1)$ and $(X, Y) = (239, 13)$. Since, $a > 1$, it follows that $a = 13$, from which it follows that $T_1 = 169$. Since $169^2 - 1 = 4^2 \cdot 1785$, we deduce finally that $d = 1785$.□

2.2 The equation $b^2X^4 - dY^2 = 1$

One way of viewing Theorem 2.1 is via the equations in (2.4). Ljunggren proof shows that for a fixed integer $u > 1$, the only positive integer solution of the equation

$$(n-1, n, n+1) = ((u^2-1)X^2, Y^2, (u^2+1)Z^2)$$

is given by the trivial solution $(X, Y, Z, n) = (1, u, 1, u^2)$. Similarly, using the Jacobi symbol argument described at the end of the previous section, the above can be extended to show that for any positive integers a and b, the only integer $n > 1$ for which the equation $(n-1, n, n+1) = (aX^2, Y^2, bZ^2)$ is solvable in positive integers X, Y, Z is either $n = T_1$ or $n = T_2$ (but not both), where T_1 and T_2 come from the minimal or next to minimal solution of $X^2 - abY^2 = 1$. It is of interest to improve this result by allowing the middle term to be other than a square. Unfortunately, it does not seem possible to prove such a result by Ljunggren's method.

Recently, Bennett [2] has succeeded in proving such a generalization, and it provides the basis for studying the equation in the title of this section.

Lemma 2.2 *Let a, b, c denote positive integers. Then there is at most one solution in positive integers (X, Y, Z, n) to the equation*

$$(n-1, n, n+1) = (aX^2, bY^2, cZ^2).$$

The proof of this result uses a combination of several techniques. ¿From the theory of Pell equations, a solution to the above implies that

$$Y = \frac{\gamma^j + \gamma^{-j}}{2\sqrt{b}} = \frac{\alpha^k + \alpha^{-k}}{2\sqrt{b}},$$

where j and k are positive integers, and γ and α are the fundamental solutions to the respective Pell equations $cx^2 - by^2 = 1$, $bx^2 - ay^2 = 1$. It follows that the linear form

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

is extremely small in modulus. Applying estimates on lower bounds for linear forms in two logarithms of algebraic numbers [23], one deduces upper bounds for j and k in terms of γ and α. On the other hand, using the theory of continued fractions, it can be shown that exponents j_1 and k_1, corresponding to another solution to the original equation, are large enough to contradict the upper bounds computed earlier.

Combining Lemma 2.2, some elementary arguments on the solutions to Pell equations, and a Jacobi-symbol argument, as described in the latter part of the previous section, the following was proved in [5]. For a positive integer $b > 1$, we denote by $\beta(b)$ the minimal index k for which b divides T_k, if such an index exists.

Theorem 2.3 *Let $b > 1$ and $d > 1$ be squarefree integers. If $T_k = bX^2$ for some integer X, then $k = \beta(b)$. Consequently, the Diophantine equation*

$$b^2X^4 - dY^2 = 1$$

has at most one solution in positive integers X, Y, and such a solution can be given explicitly.

It is worth noting that Le [24] has proved a similar result, but with the requirement that $\max(b^2, d) > 2.374 \cdot 10^{10}$. In a somewhat different direction, Cao [8] showed that the equation $T_k = 2X^2$ implies $k = 1$. As a consequence of Theorem 2.3, and some computations on certain low genus hyperelliptic curves, the following improvement was given in [5].

Corollary 2.2 *Let $b = 2^r3^s5^t7^u11^v$ for some integers $r, s, t, u, v \in \{0, 1\}$, not all zero. Then any solution of $T_k = bX^2$ with $x \in \mathbf{Z}$ implies $k = 1$ 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 $T_3 = 55 \cdot 423^2$.

One could increase the set of primes considered in Corollary 2.2, but using the methods of [5] would involve finding all integer points on an increasingly large collection of hyperelliptic curves. Instead, using the results of Baker [1] on integer solutions to hyperelliptic equations, the following was proved in [5], generalizing Corollary 2.2.

Corollary 2.3 *Let $b > 1$ denote a squarefree integer. There exists an effectively computable positive constant $C = C(b)$, depending only on b such that if $d > C$ and $T_k = bX^2$ for some $X \in \mathbf{Z}$, then $k = 1$ or $k = 2$. The latter possibility can only occur if the equation $2U^2 - bV^2 = 1$ is solvable in positive integers U and V.*

2.3 The equation $aX^4 - bY^2 = 1$

In this section we assume that a is a positive nonsquare integer and that b is any positive integer. In this case, then provided that the equation

$$aX^2 - bY^2 = 1 \tag{2.9}$$

is solvable, there is 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 $\tau^2 = \epsilon_{ab}$ is the minimal solution to $X^2 - abY^2 = 1$. Moreover, as shown in [49], all solutions in positive integers of (2.9) are given by

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

In this section we discuss the problem of determining all squares in the sequence $\{v_{2k+1}\}$. In the case $(a, b) = (3, 2)$, Bumby [7] 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 $(3, 11)$. Bumby's proof is ingenious but seems to apply only to the specific equation in question. It is the goal of current work to prove a general result on the solvability of

$$aX^4 - bY^2 = 1 \qquad (2.10)$$

for an arbitrary choice of positive integers a and b.

The only general result appearing in the literature is that of Ljunggren [31], although this result falls considerably short of what is likely the truth on the problem, as we shall see.

Theorem 2.4 *Assume that the Pell equation $aX^2 - bY^2 = 4$ is solvable in odd positive integers X and Y. Then the only possible solution to (2.10) is $\tau_{a,b}$.*

This result is proved in a manner which is somewhat similar to that of Theorem 2.1. It is rather unfortunate that Ljunggren was unable to prove a general result without the restrictive hypothesis appearing in the statement of Theorem 2.4.

The following result was proved by Le in [24], although its proof requires nothing more than the well known Jacobi-symbol argument presented at the end of Section 2.1.

Proposition 2.1 *If v_{2k+1} is a square for some $k \geq 0$, then v_1 is also a square.*

Assume now that (2.10) is solvable. By the preceding result, $\tau = \tau_{a,b}$ is of the form $\tau = x^2\sqrt{a} + v\sqrt{b}$. Put $m = x^4a - 1$, then $\tau = \sqrt{m+1} + \sqrt{m}$, and for $k \geq 0$

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

where for each $k \geq 0$, $V_{2k+1} = v_{2k+1}/v_1 = v_{2k+1}/x^2$. ¿From Proposition 2.1 we immediately have

Corollary 2.4 *For $k \geq 0$, v_{2k+1} is a square if and only if V_{2k+1} is a square.*

By Corollary 2.4, in order to obtain a general bound for the number of solutions to (2.10), it is sufficient to consider equations of the form

$$(m+1)X^4 - mY^2 = 1, \qquad (2.11)$$

which we will do for the remainder of this section.

Remark. It is not surprising that Bumby's equation $3X^4 - 2Y^2 = 1$ in [7] has the two solutions $(1, 1)$ and $(3, 11)$. More generally, if m is an integer of the form $m = k^2 + k$, with $k \geq 1$, then the equation

$$(k^2+k+1)X^4 - (k^2+k)Y^2 = 1 \qquad (2.12)$$

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

One approach for determining all solutions to (2.11) is the hypergeometric method of Thue [46], when it applies. This is accomplished via the following reduction to a family of Thue equations.

Proposition 2.2 *If (X,Y) is a positive integer solution to (2.11) other than $(1,1)$, then there is an integer solution (x,y) to a Thue equation of the form*

$$x^4 + 4mx^3y - 6mx^2y^2 - 4m^2xy^3 + m^2y^4 = m_0^2, \tag{2.13}$$

where m_0 divides m and $m_0 \leq \sqrt{m}$.

Proof. Define V_k for all $k \geq 0$ by

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

where $\tau = \sqrt{m+1} + \sqrt{m}$. For $k \geq 0$, let

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

then $V_{2k} = \sqrt{m}U_k$ for all $k \geq 0$. Upon defining the V_k for all integers $k \geq 0$ as above, it is readily checked that

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

for all $k \geq 0$. Assume 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

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

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

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

Since, $\gcd(U_n, T_n + mU_n) = 1$ and U_n is even and nonzero, there exist positive integers G, H, m_1, m_2, with $U_n = 2GH$ and $m = m_1m_2$, such that

$$z - (T_n + mU_n) = 2m_1G^2,\ z + (T_n + mU_n) = 2m_2H^2.$$

Therefore, $T_n + mU_n = m_2H^2 - m_1G^2$, and from $U_n = 2GH$, we deduce that

$$T_n = m_2H^2 - 2mGH - m_1G^2.$$

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

$$m_1^2G^4 + 4mm_1G^3H - 6mG^2H^2 - 4mm_2GH^3 + m_2^2H^4 = 1. \tag{2.14}$$

Put $m_0 = \min(m_1, m_2)$ and multiply (2.14) by m_0^2. Also, if $m_0 = m_1$, put $x = m_1G$ and $y = H$, otherwise put $x = -m_2H$ and $y = G$. Then x and y are integers satisfying $x^4 + 4mx^3y - 6mx^2y^2 - 4m^2xy^3 + m^2y^4 = m_0^2$. □

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

$$P(x) = x^4 + 4mx^3 - 6mx^2 - 4m^2x + m^2,$$

which are given explicitly by

$$\eta^{(1)} = \frac{\sqrt{m}}{\tau}(1+\rho),\ \eta^{(2)} = \frac{\sqrt{m}}{\tau}(1-\rho),\ \eta^{(3)} = (-\tau+\rho)\sqrt{m},\ \eta^{(4)} = -(\tau+\rho)\sqrt{m},$$

where $\tau = \sqrt{m+1} + \sqrt{m}$ and $\rho = \sqrt{\tau^2 + 1}$.

In the case that $m = t^2$ for some integer t, then very good approximations to these roots can be constructed, as was described in detail in [10], althought is not too hard to see that the method will apply provided that m is sufficiently close to a square. As a consequence, the authors of [10] 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 Pethö in [26].

Theorem 2.5 (Chen and Voutier) *Let $d > 3$ 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 $(X, Y) = (v, \sqrt{u})$.*

This is a fairly large step forward, as previous to this, the only known general result was that of Ljunggren, stated above in Theorem 2.4, but in the special case that $b = 1$.

It is worth noting that problems with the hypergeometric method applied to the entire family in Proposition 2.2 only arise when one attempts to determine an effective measure of approximation for the two roots

$$\eta^{(1)} = \frac{\sqrt{m}}{\tau}(1+\rho), \;\; \eta^{(2)} = \frac{\sqrt{m}}{\tau}(1-\rho).$$

In other words, for the other two roots

$$\eta^{(3)} = (-\tau + \rho)\sqrt{m}, \;\; \eta^{(4)} = -(\tau + \rho)\sqrt{m},$$

the hypergeometric method will produce an effective measure of approximation better than Liouville's theorem, and hence find all solutions (x, y) to (2.13) with x/y close to $\eta^{(3)}$ and $\eta^{(4)}$. The details of this will be described in a forthcoming paper [6].

For $k \geq 0$ define polynomials $P_{2k+1}(x)$ and $Q_{2k+1}(x)$ by

$$(\sqrt{m+1} + \sqrt{m})^{2k+1} = P_{2k+1}(m)\sqrt{m+1} + Q_{2k+1}(m)\sqrt{m}. \tag{2.15}$$

For example,

$$P_1(x) = 1, \; P_3(x) = 4x + 1, \; P_5(x) = 16x^2 + 12x + 1, \; P_7(x) = 64x^3 + 80x^2 + 24x + 1,$$

and for $k \geq 1$,

$$P_{2k+3}(x) = (4x+2)P_{2k+1}(x) - P_{2k-1}(x).$$

An integer solution to equation (2.11) is equivalent to a triple of integers (x, y, k) for which $y^2 = P_{2k+1}(x)$. It is easy to show that a positive integer solution to $y^2 = P_{2k+1}(x)$ with k even will give rise to a solution (x_1, y_1) to (2.13) with (x_1/y_1) close to either $\eta_{(3)}$ or $\eta_{(4)}$, while a solution to $y^2 = P_{2k+1}(x)$ with k odd will give rise to a solution (x_1, y_1) to (2.13) with (x_1/y_1) close to either $\eta_{(1)}$ or $\eta_{(2)}$. Thus, by the above remark, the hypergeometric method, as described in [10], can be used to prove the following. The lengthy details will be given in [6].

Theorem 2.6 *For $k \geq 1$, the equation $y^2 = P_{4k+1}(x)$ has no solutions in positive integers x and y.*

Thus, for $k \geq 1$, the only possible indices $2k+1$ for which $y^2 = P_{2k+1}(m)$ is solvable are those indices $2k + 1 \equiv 3 \pmod 4$. For this set of indices we can at least prove the following as a consequence of Theorem 2.6.

Corollary 2.5 *For $k \geq 0$, the equation $y^2 = P_{4k+3}(m)$ is not solvable in integers y and m, unless $4k+3$ is prime.*

Proof. Let $4k+3 = np$ with p prime, $n \equiv 1 \pmod 4$, and assume that y and m are integers with $y^2 = P_{4k+3}(m)$. Let $M = Q_n(m)^2 m$, where $Q_m(x)$ is the polynomial defined in (2.15), then $M+1 = P_n(m)^2(m+1)$. Then

$$(\sqrt{m+1} + \sqrt{m})^n = P_n(m)\sqrt{m+1} + Q_n(m)\sqrt{m} = \sqrt{M+1} + \sqrt{M},$$

and

$$\begin{aligned}(\sqrt{m+1} + \sqrt{m})^{np} &= P_{np}(m)\sqrt{m+1} + Q_{np}(m)\sqrt{m} \\ &= P_p(M)\sqrt{M+1} + Q_p(M)\sqrt{M} \\ &= P_p(M)P_n(m)\sqrt{m+1} + Q_p(M)\sqrt{m+1},\end{aligned}$$

and hence

$$y^2 = P_{4k+3}(m) = P_{np}(m) = P_p(M)P_n(m).$$

Let q denote a prime dividing $\gcd(P_p(M), P_n(m))$, and assume that $q^\nu || P_n(m)$, $(\nu > 0)$. Then

$$q^{\nu+1} | P_{np}(m),$$

and by the divisibility properties of the sequence $\{P_i(m)\}$ by the prime q (for example see [49] or [53]), it follows that $q = p$. It follows that either $P_p(M) = pz^2$ and $P_n(m) = pw^2$, or $P_p(M) = z^2$ and $P_n(m) = w^2$ for some integers z and w. Since $P_i(m) \equiv 1 \pmod 4$ for all i, only the latter case can occur, and from Theorem 2.6 we deduce that $n = 1$.□

We remark that the methods described in [20] and [44] can be used to show that the equation $y^2 = 64m^3 + 80m^2 + 24m + 1$ has no solutions in positive integers if $m > 1$, and hence the equation $y^2 = P_7(m)$ is not solvable for $m > 1$.

We finish off this section by stating a conjecture on the general solvability of $aX^4 - bY^2 = 1$. The truth of this conjecture is indicated by an effective form of Elkies' version of the abc conjecture.

In recent years there has been much attention drawn to what is commonly refered to as the *abc conjecture*, which states that for $\epsilon > 0$, there is a positive constant $C > 0$, depending only on ϵ such that for all triples (a, b, c) of positive integers, with $\gcd(a, b, c) = 1$ and $a + b = c$,

$$c < C\mu(abc)^{1+\epsilon},$$

where $\mu(abc)$ represents the product of distinct primes dividing abc. In [19], Elkies proved the following consequence of the abc conjecture.

Proposition 2.3 *Let $P(x)$ denote a polynomial of degree $d > 1$, with integer coefficients, and with no multiple roots. The abc conjecture implies that for all $\epsilon > 0$, and $n \geq 1$,*

$$\mu(P(n))^{1+\epsilon} > n^{d-2}.$$

Assuming an effective form of Elkies' result it can be shown that there are only finitely many triples (k, x, y) of positive integers $(k \geq 11)$ such that $P_k(x) = y^2$. Some lengthy calculations indicate that, even for small values of x, $P_k(x)$ is almost a squarefree integer.

Conjecture 2.1 *Let $m > 1$ denote a positive integer. Then the only positive integer solution to*

$$(m+1)X^4 - mY^2 = 1$$

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

3 Equations of the form $aX^2 - bY^4 = 1$

3.1 The Diophantine equation $X^2 - dY^4 = 1$

We begin this half of the paper by considering the Diophantine equation

$$X^2 - dY^4 = 1. \tag{3.1}$$

Inspired by a well known theorem of Tartakowsky [45], which states that the equation

$$X^4 - dY^4 = 1$$

has at most one solution in positive integers X and Y, Ljunggren proved in his seminal paper [29] that for any positive integers a, b, and $c = 1$ or $c = 2$, there is at most one pair of positive integers X and Y satisfying

$$aX^4 - bY^4 = c.$$

It is worth noting that Bennett [3] has recently completed the work that was started in [4], which generalizes Ljunggren's result considerably. In particular, Bennett has shown that for any $n \geq 3$ and positive integers a, b, the Diophantine equation

$$|ax^n - by^n| = 1$$

has at most one solution in positive integers x and y.

Using his result stated above, Ljunggren proved the following theorem. In this context, ϵ_d denotes the fundamental unit in the quadratic field $\mathbf{Q}(\sqrt{d})$.

Theorem 3.1 *Let d denote a positive nonsquare integer. Then equation (3.1) 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*

$$X_1 + Y_1^2\sqrt{d} = \epsilon_d,\ X_2 + Y_2^2\sqrt{d} = \epsilon_d^2$$

or by

$$X_1 + Y_1^2\sqrt{d} = \epsilon_d,\ X_2 + Y_2^2\sqrt{d} = \epsilon_d^4,$$

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

We will forego the details of Ljunggren's proof here, as it appeared in the readily available paper [29]. Moreover, in a recent paper [50], the following generalization was proved using Theorem 3.1, together with Corollary 2.2.

Theorem 3.2 *Let d be a nonsquare positive integer with $d \notin \{1785, 7140, 28560\}$. Then there are at most two positive indices k for which $U_k = 2^\delta y^2$ with y an integer and $\delta = 0$ or 1. If two solutions $k_1 < k_2$ exist, then $k_1 = 1$ and $k_2 = 2$, and provided that $d \neq 5$, $T + U\sqrt{d}$ is the fundamental unit in $\mathbf{Q}(\sqrt{d})$, or its square. For $d \in \{1785, 7140, 28560\}$, the only solutions to $U_k = 2^\delta y^2$ are $k = 1$, $k = 2$, and $k = 4$.*

In order to get information on which indices i have the property that U_i is either a square or twice a square, Theorem 3.2 requires the assumption that two solutions exist. There is very little known in the case that only one solution exists.

It is a simple matter to construct an infinite family of discriminants D for which U_3 is a square or twice a square. Let $k > 1$ be an integer satisfying $k \equiv \pm 1 \ (mod\ 6)$. For such an integer k define integers a_k, b_k, D_k by

$$2a_k + b_k\sqrt{3} = (2 + \sqrt{3})^k,\ \ D_k = \frac{a_k^2 - 1}{9} \quad (\text{resp. } D_k = \frac{a_k^2 - 1}{36}).$$

By our choice of k, D_k is an integer, and $a_k + 3\sqrt{D_k}$ (resp. $a_k + 6\sqrt{D_k}$) is the minimal solution to the Pell equation $X^2 - D_k Y^2 = 1$. Upon cubing this minimal solution, it is easy to verify that $U_3 = (3b_k)^2$ (resp. $U_3 = 2(3b_k)^2$).

An effective version of Langevin's version of the abc conjecture (see [22]) implies that the following holds. We omit the details.

Conjecture 3.1 *Let d denote a positive nonsquare integer such that $d \notin \{1785, 7140, 28560\}$. Let $T + U\sqrt{d}$ denote the minimal solution to $X^2 - dY^2 = 1$, and $T_k + U_k\sqrt{d} = (T + U\sqrt{d})^k$ for $k \geq 1$. If $k \geq 4$, then U_k is neither a square, nor twice a square.*

3.2 The Equation $X^2 - db^2Y^4 = 1$

In the previous section we considered the problem of bounding the number of solutions and the size of the index k to the equation $U_k = 2^\delta y^2$, with $\delta \in \{0, 1\}$.

In this section we discuss the similar problem $U_k = by^2$, with b any positive integer. The following result is a simple consequence of Theorem 2.3 and Theorem 3.1. The details can be found in [51].

Proposition 3.1 *Let b, d denote positive squarefree integers. There is at most one index k for which $U_k = bx^2$, except in the following cases;*
1. $T = 2t^2$ for some integer t and $U = by^2$ for some integer y, in which case there is the second solution $U_2 = b(2ty)^2$.
2. $T = 169$, in which case U_1 and U_4 are both squares for $d = 1785$ and $d = 16 \cdot 1785$, and both twice a square for $d = 7140$.

When a solution to $U_k = bx^2$ does occur, it would be interesting to prove analogous results on the value for k, as was done in Theorem 2.3. This unfortunately seems to be more difficult, mainly because of the lack of a "Jacobi-symbol" argument, as is available for the sequence $\{T_k\}$. In [34], Mignotte and Pethö make some progress on this question by proving the following, which is a slight reformulation of their result in order to coincide with the notation and results of this paper.

Theorem 3.3 *Let d denote a nonsquare positive integer such that $\epsilon_d = T + u^2\sqrt{d}$ for some integers T and u. A solution to $U_k = bx^2$ for some $b \in \{1, 2, 3, 6\}$ and some integer x, with $k > 3$, exists only when $T = 169$ and $k = 4$.*

In [34], the authors actually deal with the more general situation of taking powers of units of the form $\frac{a+\sqrt{a^2-4}}{2}$, and it is worth noting that Ribenboim [38] has recently discovered an elementary proof of the main result in [34]. In the statement of Theorem 3.3, we have only considered the case that a is even since we are restricting our attention to the study of solutions to the Pell equation $X^2 - dY^2 = 1$. Using Theorem 2.3 and Theorem 3.2, the following improvement to Theorem 3.3 can be easily proved, as is described in [51].

Theorem 3.4 *Let d denote a positive nonsquare integer such that the minimal solution of the Pell equation $X^2 - dY^2 = 1$ is of the form $\epsilon_d = T + u^2\sqrt{d}$. Assume that $U_k = bx^2$ for some $b \in \{1, 2, 3, 5, 6, 10\}$ and some integer x. Then $k \leq 2$ except in the following cases;*
1. $T = 169$ in which case U_4 is a square.
2. 3 divides u and $4T^2 - 1 = 3y^2$ for some integer y, in which case $U_3 = 3(uy)^2$.
3. $(b, d) = (5, 24)$, in which case $U_4 = 5(14)^2$.

The set of integers b considered in Theorem 3.4 can be extended, but the proof as given in [51] becomes exceedingly long, dealing with many cases. It would be of interest to prove a similar result for any value

of b. Removing the restriction that U is a square, we pose the following conjecture. It is worth noting that this conjecture follows from an effective form of Langevin's theorem about the abc conjecture (see [22]). For an integer $b > 1$ we denote by $\alpha(b)$ the minimal index k for which b divides U_k. Note that $\alpha(b)$ always exists.

Conjecture 3.2 *Let d denote a positive nonsquare integer such that the minimal solution of the Pell equation $X^2 - dY^2 = 1$ is $\epsilon_d = T + U\sqrt{d}$. For a squarefree integer $b > 1$, the only possible solution to $U_k = bx^2$ is $k = \alpha(b)$, except for the following cases;*
1. $T = 169$ and $b \in \{1, 2\}$, in which case U_2 and U_4 are also solutions.
2. $T + U\sqrt{d} = 2v^2 + bu^2\sqrt{d}$ or $T + U\sqrt{d} = v^2 + 2bu^2\sqrt{d}$ for some integers v and u, in which case $U_2 = b(2vu)^2$.
3. $4T^2 - 1 = 3v^2$ and $U = 3bu^2$ for some integers v and u, in which case $U_3 = b(3vu)^2$.
4. $2T^2 - 1 = v^2$ and $TU = bu^2$ for some integers v and u, in which case $b(2vu)^2 = U_4 = U_{2\alpha(b)}$.
Furthermore, there is a positive constant $c = c(b)$ with the property that $d > c$ and $U_k = bx^2$ implies $k \leq 3$.

Some partial results in this direction can be obtained by the methods of this paper, relying heavily on Theorem 2.3. The following is an example of such a result for the case that $\alpha(b)$ is even.

Theorem 3.5 *Let d be a nonsquare positive integer, and let b be a squarefree positive integer such that $\alpha(b)$ is even. If $U_k = bx^2$ for some integer x, then $k = \alpha(b)$ except in the case that $2T^2 - 1 = v^2$ and $TU = bu^2$ for some integers u and v, in which case $U_4 = b(2uv)^2 = U_{2\alpha(b)}$. Also, there is a computable constant $c = c(b)$ with the property that $d > c$ and $U_k = bx^2$ implies $k = 2$.*

3.3 The Equation $aX^2 - bY^4 = 1$

In [30], Ljunggren proved some remarkable results on the solvability of Diophantine equations of the form $aX^2 - bY^4 = c$, for $c = 1, 2, 4$. In this paper we consider the case $c = 1$. For this case, Ljunggren's proof gives the following precise statement on the solvability of the equation of the title.

Theorem 3.6 *Let a and b be positive integers, with a nonsquare, such that the equation $aX^2 - bY^2 = 1$ is solvable in positive integers. Let (v, w) be the solution in positive integers of $aX^2 - bY^2 = 1$ with v minimal, and put $\tau = v\sqrt{a} + w\sqrt{b}$. Let $w = n^2 l$ with l odd and squarefree. The Diophantine equation*

$$aX^2 - bY^4 = 1 \tag{3.2}$$

has at most one solution in positive integers. If a solution (x, y) to (3.2) exists, then

$$x\sqrt{a} + y^2\sqrt{b} = \tau^l. \tag{3.3}$$

Proof. For $k \geq 0$, let

$$\tau^{2k+1} = v_{2k+1}\sqrt{a} + w_{2k+1}\sqrt{b},$$

and assume that there is a $j \geq 0$ for which w_{2j+1} is a square. Similar to that given in the proof of Theorem 2.1, there is an odd positive integer t such that w_{tl} is a square, and all indices $2i + 1$ for which w_{2i+1} is a square are divisible by tl. Let

$$\eta = \tau^{tl} = \sqrt{m + 1} + \sqrt{m},$$

where $m = w_{tl}^2 b$, and for $k \geq 0$, let

$$\eta^{2k+1} = P_{2k+1}(m)\sqrt{m + 1} + Q_{2k+1}(m)\sqrt{m}.$$

We first show that $y^2 = Q_{2k+1}(m)$ is not solvable in integers y and m for any $k > 0$. For k odd, $Q_{2k+1}(m) \equiv 3 \pmod 4$, and so it suffices to consider the case that k is even.

Let $\epsilon = \eta^2$, and $\epsilon' = \epsilon^{-1}$. Then $y^2 = Q_{4k+1}(m)$ yields

$$y^2 = Q_{4k+1}(m) = \frac{\tau^{4k+1} - \tau^{-4k-1}}{\tau - \tau^{-1}} = \frac{\epsilon^{4k+1} - 1}{\epsilon^{2k}(\epsilon - 1)},$$

and so

$$(\epsilon^{4k})\epsilon - y^2\epsilon^{2k}(\epsilon - 1) = 1.$$

Thus,

$$(y\epsilon^k\sqrt{\epsilon} + \epsilon^{2k}\sqrt{\epsilon - 1})^2$$

is a unit in the ring $\mathbf{Z}[1, \epsilon, \theta, \theta\epsilon]$, of relative norm 1, where $\theta = \sqrt{\epsilon(\epsilon - 1)}$. Note that the field $\mathbf{Q}(\theta)$ has a complex embedding. Similar to the proof of Theorem 2.1, it follows from Dirichlet's unit theorem that

$$\epsilon^{2k}\sqrt{\epsilon} + y\epsilon^k\sqrt{\epsilon - 1} + = (\sqrt{\epsilon} + \sqrt{\epsilon - 1})^s = \lambda^s \tag{3.4}$$

for some odd positive integer s. With λ defined as above, let

$$\lambda' = \sqrt{\epsilon} - \sqrt{\epsilon - 1},$$
$$\lambda'' = \sqrt{\epsilon'} + \sqrt{\epsilon' - 1},$$
$$\lambda''' = \sqrt{\epsilon'} - \sqrt{\epsilon' - 1}.$$

Let $N = \epsilon + \epsilon' - 2$, then N is a positive integer, and equation (3.4) implies that

$$(\lambda\lambda'')^s + (\lambda'\lambda''')^s - 2 = 2y^2 i\sqrt{N}$$

and

$$(\lambda\lambda'') + (\lambda'\lambda''') - 2 = 2i\sqrt{N}.$$

¿From the formula

$$\frac{p^s + q^s - 2}{p + q - 2} = \sum_{h=0}^{s-1} \frac{s}{h+1} \left(\begin{array}{c} s+h \\ 2h+1 \end{array} \right) (p + q - 2)^h, \quad (pq = 1)$$

evaluated at $p = \lambda\lambda''$, $q = \lambda'\lambda'''$, we obtain

$$y^2 = s^2 + \frac{s^2(s^2 - 1^2)}{4!}2(2i\sqrt{N}) + \cdots + \frac{s^2(s^2 - 1^2)\cdots(s^2 - h^2)}{(2h+2)!}2(2i\sqrt{N})^h + \cdots + (2i\sqrt{N})^{s-1}.$$

Since y^2 is real, the terms with $i\sqrt{N}$ to an odd power sum to zero, and so

$$0 = \frac{s^2(s^2 - 1^2)}{4!} - \frac{s^2(s^2 - 1^2)(s^2 - 2^2)(s^2 - 3^2)}{8!}4N + \cdots.$$

We now use an argument which is similar to that given in the proof of Theorem 2.1. Let $a \geq 3$ be an integer such that 2^a properly divides $s^2 - 1$. If $s > 1$, then the 2-adic order of the first term is $a - 3$, whereas, it is easily shown by induction that the 2-adic order of all succeeding terms is greater than $a - 3$, a contradiction. Thus, $s = 1$, and equation (3.4) shows that $k = 0$.

It follows that the only square in the sequence $\{w_{2k+1}\}$ is w_{tl}. The proof of the theorem will be complete once it shown that $t = 1$. Write τ in the form

$$\tau = \sqrt{m+1} + \sqrt{m},$$

so that

$$\tau^{tl} = P_{tl}(m)\sqrt{m+1} + Q_{tl}(m)\sqrt{m}.$$

The equation $w_{tl} = y^2$ implies that $Q_{tl}(m) = lz^2$ for some integer z. From an argument similar to that given in the proof of Corollary 2.5 we see that

$$lz^2 = Q_{tl}(m) = Q_l(M)Q_t(m),$$

where $M = Q_t(m)^2 m$. We will show that $Q_t(m) = x^2$ for some integer x, which will force $t = 1$, as required.

Let p denote a prime divisor of $Q_t(m)$. If p does not divide l, then p properly divides $Q_t(m)$ to an even power, and so we may assume that p divides l. In this case, since l is squarefree, and since l divides m, m divides M, the binomial theorem shows that p properly divides $Q_l(M)$. Therefore, p properly divides $Q_t(m)$ to an even power, and hence $Q_t(m)$ must be a square.□

It is worth noting that Theorem 3.6 has been rediscovered on various occasions. In a very recent unpublished paper [11], Chen and Voutier proved Theorem 3.6 by using the hypergeometric method of Thue. Analogous to Proposition 2.2, a solution to equation (3.2) reduces to a solution (x, y) to the Thue equation

$$x^4 + 4mx^3y + 6mx^2y^2 + 4m^2xy^3 + m^2y^4 = m_0^2.$$

Unlike the polynomial $x^4 - 4mx^3 - 6mx^2 + 4m^2x + m^2$, the roots of the polynomial $x^4 + 4mx^3 + 6mx^2 + 4m^2x + m^2$ can be sufficiently well approximated by rationals to enable the hypergeometric method, as described in [10] and [11], to completely solve the Thue inequality, and hence determine all solutions to equation (3.2).

We remark that in [18] and [8], Theorem 3.6 was rediscovered in the particular case that a is a perfect square. To set the record straight, we state the following immediate corollary of Ljunggren's theorem.

Corollary 3.1 *Let $d > 1$ denote a squarefree positive integer such that the Pell equation $X^2 - dY^2 = -1$ is solvable, and let $T + U\sqrt{d}$ denote its minimal solution. Assume that $T = v^2 l$, where l is an odd squarefree integer. Then the only possible solution in positive integers to the equation*

$$X^4 - dY^2 = -1$$

is $T_l + U_l\sqrt{d} = (T + U\sqrt{d})^l$.

In [11] the authors ask if the condition $x\sqrt{a} + y^2\sqrt{b} = \eta^l$ in Theorem 3.6 can be replaced by simply $x\sqrt{a} + y^2\sqrt{b} = \eta$. Some information on this question was given in [52], wherein the following was proved.

Theorem 3.7 *Let all of the notation be as above.*
1. For $l = 3$ and 5 there are infinitely many pairs a, b for which (3.2) is solvable.
2. If $l > 5$, then there are finitely many pairs a, b for which (3.2) is solvable. In particular, for $l = 7$ there are no pairs a, b for which (3.2) is solvable.

Example. Consider the case $l = 3$. Let $b = 2$, $a = 19$, and $\eta = \sqrt{19} + 3\sqrt{2}$. In this case, $\eta^3 = 73\sqrt{19} + 225\sqrt{2}$, and so $X = 73$, $Y = 15$ is a solution to $19X^2 - 2Y^4 = 1$.

Example. Consider the case $l = 5$. Let $b = 81968378998$ and $a = 1 + 25b = 2049209474951$, we find that the minimal solution to $aX^2 - bY^2 = 1$ is

$$\tau = \sqrt{2049209474951} + 5\sqrt{81968378998},$$

and that

$$\tau^5 = 671881515556222653537394 01\sqrt{2049209474951} + (18328686744505)^2\sqrt{81968378998}.$$

Therefore, the equation $2049209474951X^2 - 81968378998Y^4 = 1$ is solvable, and comes from the fifth power of the minimal solution of $2049209474951X^2 - 81968378998Y^2 = 1$.

It seems difficult to prove results for large values of l in Theorem 3.6. On the other hand, an effective version of Langevin's theorem [22] about the abc conjecture indicates that the following statement is likely true.

Conjecture 3.3 *Let a and b be positive integers, with a nonsquare, such that the equation $aX^2 - bY^2 = 1$ is solvable in positive integers, and let $\eta = u\sqrt{a} + v\sqrt{b}$ be the minimal solution, with $v = k^2 l$, l odd and squarefree. If $l \geq 7$, then there are no solutions to $aX^2 - bY^4 = 1$. In the case that $b = 1$, the equation $X^4 - aY^2 = -1$ is solvable if and only if $l = 1$.*

References

[1] A. Baker. *Bounds for the solutions of the hyperelliptic equation.* Proc. Camb. Phil. Soc. **65** (1969), 439-444.

[2] M.A. Bennett. *On consecutive integers of the form ax^2, by^2, cz^2.* To appear in Acta Arithmetica.

[3] M.A. Bennett. *Rational approximation to algebraic numbers of small height: The Diophantine equation $|ax^n - by^n| = 1$.* submitted.

[4] M.A. Bennett and B.M.M. de Weger. *On the Diophantine equation $|ax^n - by^n| = 1$.* Math. Comp. **67** (1998), 413-438.

[5] M.A. Bennett and P.G. Walsh. *The Diophantine equation $b^2X^4 - dY^2 = 1$.* To appear Proc. A.M.S.

[6] M.A. Bennett and P.G. Walsh. *New results on the solvability of the Diophantine equation $aX^4 - bY^2 = 1$.* (in preparation).

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

[8] Z.F. Cao. *A study of some Diophantine equations.* J. Harbin Inst. Tech. (1988), 1-7.

[9] J.H. Chen. *A new solution of the Diophantine equation $X^2+1 = 2Y^4$.* J. Number Theory **48** (1994), 62-74.

[10] 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.

[11] J.H. Chen and P.M. Voutier. *The complete solution of $aX^2 - bY^4 = 1$.* Preprint, 1997.

[12] J.H.E. Cohn. *On square Fibonacci numbers.* J. London Math. Soc. **39** (1964), 537-541.

[13] J.H.E. Cohn. *Eight Diophantine equations.* Proc. London Math. Soc. (3) **16** (1966), 153-166.

[14] J.H.E. Cohn. *Five Diophantine equations.* Math. Scand. **21** (1967), 61-70.

[15] J.H.E. Cohn. *Twelve Diophantine equations.* Arch. Math. **65** (1995), 130-133.

[16] J.H.E. Cohn. *Squares in some recurrent sequences.* Pacific J. Math. **41** (1972), 631-646. Arch. Math. **65** (1995), 130-133.

[17] J.H.E. Cohn. *The Diophantine equation $x^4 - Dy^2 = 1$ II.* Acta Arith. **78** (1997), 401-403.

[18] J.H.E. Cohn. *The Diophantine equation $x^4 + 1 = Dy^2$.* Math. Comp. **66** (1997), 1347-1351.

[19] N.D. Elkies. *ABC implies Mordell.* Intern. Math. Res. Notices **7** (1991), 99-109.

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

[21] C. Ko. *On the diophantine equation $x^2 = y^n + 1, xy \neq 0$,* Scientia Sinica (Notes) **14** (1965), 457-460.

[22] M. Langevin. *Cas d'inégalité pour le théorème de Mason et applications de la conjecture (abc).* C.R. Acad. Sci. Paris, t.317, Série I (1993) 441-444.

[23] M. Laurent, M. Mignotte, and Y. Nesterenko. *Formes linéares en deux logarithmes et déterminants d'interpolation.* J. Number Theory **55** (1995), 285-321.

[24] M.H. Le. *On the diophantine equation $D_1x^4 - D_2y^2 = 1$.* Acta Arith. **76** (1996), 1-9.

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

[26] G. Lettl and A. Pethö. *Complete solution of a family of quartic Thue equations.* Abh. Math. Se. Univ. Hamburg **65** (1995), 365-383.

[27] W. Ljunggren. *Zur Theorie der Gleichung $x^2 + 1 = Dy^4$.* Avh. Norsk. Vid. Akad. Oslo (1942), 1-27.

[28] W. Ljunggren. *Über die Gleichung $x^4 - Dy^2 = 1$.* Arch. Math. Naturv. **45** (1942) no.5.

[29] W. Ljunggren. *Einige Eigenschaften der Einheiten reeller quadratischer und reinbiquadratischer Zahl-Körper usw.* Oslo Vid.-Akad. Skrifter (1936), nr. 12.

[30] W. Ljunggren. *Ein Satz über die Diophantische Gleichung $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$* Tolfte Skand. Matemheikerkongressen, Lund, 1953, 188-194, (1954).

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

[32] W.L. McDaniel and P. Ribenboim. *Squares and double squares in Lucas sequences.* C.R. Math. Rep. Acad. Sci. Canada **14** (1992),104-108.

[33] W.L. McDaniel and P. Ribenboim. *The square terms in Lucas sequences.* J. Number Theory **58** (1996), 104-123.

[34] M. Mignotte and A. Pethö. *Sur les carrés dans certaines suites de Lucas.* J. Théorie Nombres Bordeaux **5** (1993), 333-341.

[35] L.J. Mordell. *Diophantine Equations,* Academic Press, New York, 1969.

[36] K. Nakamula and A. Pethö *Squares in binary recurrence sequences.* In *Number Theory, Diophantine, Computational, and Algebraic Aspects*, proceedings of a conference in Eger, Hungary, (Györy, Pethö, Sós, Ed's), Walter de Gruyter, Berlin, (1998), 409-422.

[37] P. Ribenboim. *Catalan's Conjecture.* Academic Press, New York, 1994.

[38] P. Ribenboim. *An algorithm to determine the points with integral coordinates on certain elliptic curves.* To appear in J. Number Theory.

[39] P. Ribenboim and P.G. Walsh. *The ABC conjecture and the powerful part of terms in binary recurring sequences.* To appear in J. Number Theory.

[40] A. Rotkiewicz. *Applications of Jacobi's symbol to Lehmer's numbers.* Acta Arith. **42** (1983), 163-187.

[41] T.N. Shorey and R. Tijdeman. *Exponential Diophantine Equations.* Cambridge University Press, **87**, New York, 1986.

[42] C.L. Siegel. *Die Gleichung $ax^n - by^n = c$.* Math. Ann. **114** (1937), 57-68.

[43] R. Steiner and N. Tzanakis. *Simplifying the solution of Ljunggren's equation $X^2 + 1 = 2Y^4$.* J. Number Theory **37** (1991), 123-132.

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

[45] V.A. Tartakowsky. *Auflösung der Gleichung $x^4 - \rho y^4 = 1$.* Izv. Akad. Nauk. SSSR, **20** (1926), 301-324.

[46] A. Thue. *Ein Fundamentaltheorem zur Bestimmung von Annäherungswerten aller Wurzeln gewisser ganzer Funktionen*, J. Reine Angew. Math. **138** (1910), 96-108.

[47] N. Tzanakis. *Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations.* Acta Arith. **75** (1996), no. 2, 165-190.

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

[49] D.T. Walker. *On the Diophantine equation $mX^2 - nY^2 = \pm 1$.* Amer. Math. Monthly **74** (1967), 504-513.

[50] P.G. Walsh. *A note on a theorem of Ljunggren and the Diophantine equations $x^2 - kxy^2 + y^4 = 1, 4$.* To appear in Archiv der Mathematik.

[51] P.G. Walsh. *The Diophantine equation $X^2 - db^2Y^4 = 1$.* To appear in Acta Arithmetica.

[52] P.G. Walsh. *A note on Ljunggren's theorem about the Diophantine equation $aX^2 - bY^4 = 1$.* To appear in Comptes Rendues Math. Rep. Acad. Sci. Canada.

[53] P.G. Walsh. *The Pell equation and powerful numbers.* Master's Thesis, University of Calgary, 1988.

[54] W.S. Zhu. *Necessary and sufficient conditions for the solvability of the Diophantine equation $x^4 - Dy^2 = 1$.* Acta Math. Sinica **28** (1985), 681-683.

P.G Walsh
Department of Mathematics
University of Ottawa
585 King Edward St.
Ottawa, Ontario, Canada
K1N-6N5
gwalsh@mathstat.uottawa.ca