ACTA ARITHMETICA
LXXXVII.2 (1998)

The Diophantine equation $X^2 - db^2Y^4 = 1$

by

Gary Walsh (Ottawa, Ont.)

1. Introduction. There is considerable research on the problem of determining the arithmetic structure of terms in binary linear recurrences. In this paper we consider those sequences which arise from solutions to Pell equations. For an extensive survey on this topic, the reader is referred to [11].

Let d denote a positive nonsquare integer. It is well known that the equation $X^2 - dY^2 = 1$ has infinitely many solutions in positive integers, all of which are generated by a minimal solution, which we denote by $\varepsilon_d = T + U\sqrt{d}$. Then all of the solutions in positive integers are given by $\varepsilon_d^k = T_k + U_k\sqrt{d}$, for $k \geq 1$. This notation will be used throughout the paper.

Based on a theorem of Ljunggren (see [9]), Cohn [4] proved the following result, determining the values in the sequence $\{T_k\}$ which can be perfect squares.

Theorem A (Cohn, 1996). *Let d be a nonsquare positive integer. If the equation $X^4 - dY^2 = 1$ is solvable in positive integers X, Y, then either $X^2 + Y\sqrt{d} = \varepsilon_d$ or ε_d^2. Solutions to $X^4 - dY^2 = 1$ arise from both ε_d and ε_d^2 only for $d \in \{1785, 7140, 28560\}$.*

Definition. For a positive integer b, the *rank of apparition* $\alpha(b)$ of b in the sequence $\{U_k\}$ is the minimal index k for which b divides U_k. Since the sequence $\{U_k \pmod b\}$ is periodic and satisfies $U_0 = 0$, it follows that $\alpha(b) < \infty$ for all $b \geq 1$. The rank of apparition $\beta(b)$ of b in the sequence $\{T_k\}$ is the minimal index k for which b divides T_k. We write $\beta(b) = \infty$ if no such k exists.

Theorem A has since been generalized as follows by Bennett and the author in [2].

Theorem B (Bennett and Walsh, 1998). *Let $b > 1$ and $d > 1$ be square-free integers. If $T_k = bx^2$ for some integer x, then $k = \beta(b)$. Also, there is*

1991 *Mathematics Subject Classification*: 11D25, 11J86.

a computable positive constant $c = c(b)$ depending on b such that if $d > c$ and $T_k = bx^2$, then $k = 1$ or $k = 2$.

The purpose of this paper is to study similar questions for the sequence $\{U_k\}$. The following theorem on the number of solutions to the equation $U_k = bx^2$ follows from a classical result of Ljunggren [7] and Theorem A.

PROPOSITION 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 B. 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 [10], Mignotte and Pethő 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 C (Mignotte and Pethő, 1993). *Let d be a nonsquare positive integer such that $\varepsilon_d = T + u^2\sqrt{d}$ 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 [10], the authors actually deal with the more general situation of taking powers of units of the form $(a + \sqrt{a^2 - 4})/2$. In the statement of Theorem C, we have only considered the case where a is even since we are restricting our attention to the study of solutions to the Pell equation $X^2 - dY^2 = 1$.

The following result will provide the basis for improving Theorem C. More importantly, it provides a different method of proof than that in [10], which is easily extendable to larger values of b.

THEOREM 1. *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 $\varepsilon_d = T + u^2\sqrt{d}$. If $U_k = bx^2$ for some $b \in \{1, 2, 3, 5, 6, 10\}$ and some integer x, then $k = \alpha(b)$, except in the following cases*:

1. *$(b, T) = (1, 2v^2)$ for some integer v, in which case $U_2 = (2vu)^2$, and $(b, T) = (1, 169)$, in which case U_4 is a square.*

2. *$(b, T) = (2, v^2)$ for some integer v, and u is even, in which case $U_2 = U_{2\alpha(2)} = 2(vu)^2$.*

3. $b = 3$, 3 *divides* u, *and* $4T^2 - 1 = 3v^2$ *for some integer* v, *in which case* $U_3 = U_{3\alpha(3)} = 3(vu)^2$.

4. $(b, T, d) = (5, 5, 24)$, *in which case* $U_4 = U_{2\alpha(5)} = 5(14)^2$.

Theorem 1 enables us to prove the following improvement of Theorem C.

COROLLARY 1. *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* $\varepsilon_d = T + u^2\sqrt{d}$. *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 1 is restricted in order to keep the proof brief, yet shows how such a result can be proved for any particular value of b. We conjecture that this result holds for any integer $b > 1$. That is, apart from the exceptional cases given here, the only possible value k for which $U_k = bx^2$ is $k = \alpha(b)$.

More generally, 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 [5]), but we omit the details.

CONJECTURE 1. *Let* d *denote a positive nonsquare integer such that the minimal solution of the Pell equation* $X^2 - dY^2 = 1$ *is* $\varepsilon_d = T + U\sqrt{d}$. *For a squarefree integer* b, *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 B. The following is an example of such a result for the case where $\alpha(b)$ is even.

THEOREM 2. *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 where $2T^2 - 1 = v^2$ 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 $k = 2$.

2. Properties of certain recurrence sequences. As above, let d be a nonsquare positive integer, and $\varepsilon_d = T + U\sqrt{d}$ the minimal solution of $X^2 - dY^2 = 1$. For $k \geq 1$, let $\varepsilon^k = T_k + U_k\sqrt{d}$. For a prime p not dividing d, we let $\delta = \left(\frac{d}{p}\right)$ denote the Legendre symbol.

LEMMA 1. *For any odd prime p, with $\gcd(p, d) = 1$, p divides $U_{(p-\delta)/2}$, i.e. $\alpha(p)$ divides $(p - \delta)/2$. If p divides d, then $\alpha(p) = 1$ or $\alpha(p) = p$.*

Proof. If p divides d, the result can easily be obtained from the binomial theorem. Assume that $\gcd(p, d) = 1$, then it is well known (see [6]) that p divides $U_{p-\delta} = 2T_{(p-\delta)/2}U_{(p-\delta)/2}$, and so it suffices to prove that p does not divide $T_{(p-\delta)/2}$.

Assume first that p divides T. Then from the relation $T^2 - dU^2 = 1$, it follows that $\left(\frac{-d}{p}\right) = 1$, hence 4 divides $p - \delta$, showing that $(p - \delta)/2$ is even. Since $\gcd(T, T_{2k}) = 1$ for all integers k, p cannot divide $T_{(p-\delta)/2}$.

Now assume that p does not divide T. From the binomial theorem it is easy to show that $T_p \equiv T_1 \pmod p$. Furthermore, from the obvious relation $\varepsilon^p = \varepsilon^{p-\delta} \cdot \varepsilon^\delta$, it follows that $T_p = T_{p-\delta}T_1 + \delta U_{p-\delta}U_1 d$, and hence $T_{p-\delta}T_1 \equiv T_p \equiv T_1 \pmod p$, showing that $T_{p-\delta} \equiv 1 \pmod p$. If p divides $T_{(p-\delta)/2}$, then since $T_{p-\delta} = 2T^2_{(p-\delta)/2} - 1$, we deduce that $T_{p-\delta} \equiv -1 \pmod p$, contradicting the fact that p is an odd prime.

The following result is easily proved using the binomial theorem.

LEMMA 2. *Let $k \geq 1$, $a \geq 1$, and let p be any prime number. If $p \parallel U_k$, then for any integer $t \geq 0$, and positive integer l with $\gcd(p, l) = 1$, $p^{a+t} \parallel U_{p^t kl}$.*

For further results on the divisibility properties of recurrence sequences, the reader is referred to the well known paper of Lehmer [6].

3. Squares in recurrence sequences. We present some results used in the proof of Theorem 1. In [7], Ljunggren showed that for a given nonsquare positive integer d, the equation $X^2 - dY^4 = 1$ has at most two solutions in positive integers X and Y. This was improved upon in [12], as follows.

LEMMA 3. *Let D be a nonsquare 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*

$\mathbb{Q}(\sqrt{D})$, *or its square. For* $D \in \{1785, 7140, 28560\}$, *there is a third solution* $k_3 = 4$.

The following is a simple consequence of Theorem B. The reader is directed to Corollary 1 of [2] for more details.

LEMMA 4. *If* $T_k = bx^2$ *for some* $b \in \{2, 3, 5, 6, 10\}$ *and some integer* x, *then* $k = 1$.

LEMMA 5. *For* $k \geq 1$, *let* $V_k + W_k\sqrt{2} = (1 + \sqrt{2})^k$. *The only odd values of* k *for which* $W_k = bx^2$ *for some integer* x *and* $b \in \{1, 2, 3, 5, 6, 10\}$ *are* $k = 1, 3$ *and* 7.

P r o o f. For odd values of k, $V_k^2 - 2W_k^2 = -1$, and so W_k is a product of primes congruent to 1 modulo 4. Thus, the only candidates for b are 1 and 5. If $b = 1$, then by the result of Ljunggren [8], the only values for k are 1 and 7. It follows from the main result of [3] that the only integer solution of $X^2 - 50Y^4 = 1$ is $(X, Y) = (7, 1)$, resulting in $k = 3$.

LEMMA 6. *If* $\varepsilon_d = T + u^2\sqrt{d}$ *for some integer* u, *then for any integer* $b > 1$ *there is at most one solution* k *to* $U_k = bx^2$.

P r o o f. This follows from Proposition 1.

LEMMA 7. *The only positive integer solution to* $5Y^2 = 16X^4 - 12X^2 + 1$ *is* $(X, Y) = (1, 1)$.

P r o o f. The polynomial $16x^4 - 12x^2 + 1$ factors as $16x^4 - 12x^2 + 1 = (4x^2 - 2x - 1)(4x^2 + 2x - 1)$, and for any integer x, we have $\gcd(4x^2 - 2x - 1, 4x^2 + 2x - 1) = 1$. Therefore, if X and Y are integers satisfying $5Y^2 = 16X^4 - 12X^2 + 1$, either $4X^2 - 2X - 1 = Z^2$ or $4X^2 + 2X - 1 = Z^2$ for some integer Z. This is equivalent to either $(4X - 1)^2 - 5 = 4Z^2$ or $(4X + 1)^2 - 5 = 4Z^2$ for some integer Z. It is evident that only the former is solvable with $X = 1$, forcing $Y = 1$.

4. Proofs

Proof of Proposition 1. In [7], Ljunggren showed that for a positive non-square integer D, the equation $X^2 - DY^4 = 1$ has at most two solutions, and if two solutions exist, then they are given by ε_D and ε_D^2, or by ε_D and ε_D^4, the latter occurring for only finitely many D. It follows from Theorem A that the latter can only occur for $T = 169$, and hence $D \in \{1785, 4 \cdot 1785, 16 \cdot 1785\}$.

Fix an integer $b \geq 1$, and let $D = db^2$. If $U_k = bx^2$, then this gives rise to a solution of $X^2 - DY^4 = 1$, and so by Ljunggren's result, there is at most one solution to $U_k = bx^2$ except if one of two situations arise. The first is that $U_2 = bz^2$ and $U = by^2$ for some integers z and y. Since $U_2 = 2TU$, it follows that $T = 2t^2$ for some integer t. This is precisely the first exceptional case given in the statement of the proposition. The other

possibility, according to Ljunggren's theorem, is that $T = 169$, in which case U and U_4 are both either a square or twice a square.

Proof of Theorem 1. For $b \in \{1, 2\}$, the result is immediate from Lemma 3, together with the fact that $U = U_1$ is a square. We now consider $b > 2$, and in so doing, we consider each value of b separately.

Let us first assume that $\alpha(b)$ is even, $\alpha(b) = 2r$, say. Let $U_{2r} = bm^2n$ with n squarefree, and assume that $U_k = bx^2$. By Lemma 2, it follows that $k = 2rnc$ for some integer c. It follows that either T_{rnc} or U_{rnc} is a square, or twice a square, and so by Theorem A and Lemma 4, either $rnc \in \{1, 2\}$, or $rnc = 4$ and $T = 169$.

If $rnc = 1$ we are done. Assume that $rnc = 2$. Then if $n = 1$ we are done, so assume that $n = 2$ and that $r = c = 1$. Thus, $U_2 = 2bm^2$ and $U_4 = bx^2$. From $U_4 = 2T_2U_2$, it follows that $T_2 = z^2$ for some integer z. Also, since $2bm^2 = U_2 = 2TU = 2Tu^2$, it follows that $T = bv^2$ for some integer v. From the relation $T_2 = 2T^2 - 1$, we deduce finally that $z^2 = 2b^2v^4 - 1$. By Lemma 5, it follows that $b = 5, v = 1$, and hence $T + u^2\sqrt{d} = 5 + \sqrt{24}$, which is one of the exceptional cases given.

It remains to consider the case $rnc = 4$ and $T = 169$. In this case, $U = 1$ or 4, and it is sufficient to consider the former case. We find that $k = 2rnc = 8$, and that $U_k = 2^3 \cdot 13^2 \cdot 239^2 \cdot 9601 \cdot 679681$ is not of the form bx^2 with $b \in \{3, 5, 6, 10\}$. Thus, the theorem holds in the case where $\alpha(b)$ is even.

We now consider each value of b separately.

Case 1: $b = 3$. Assume that $U_k = 3x^2$ for some integer x. From Lemma 1 we know that $\alpha(3) = 1$, 2, or 3, and so we consider each odd case separately. Assume first that $\alpha(3) = 1$. Since U_1 is a square, it follows from Lemma 2 that 3 divides k. Therefore, by Lemma 2, $U_{k/3} = y^2$ for some integer y, and it follows from the above case $b = 1$ that $k/3 = 1$, 2, or 4, i.e. $k = 3$, 6, or 12. If $U_6 = 3x^2$, then since $U_6 = 2T_3U_3$, 3 divides U_3 and the highest power of 2 dividing U_3 is even, it follows that $T_3 = 2y^2$ for some integer y, contradicting Lemma 4. Similarly, if $U_{12} = 3x^2$, then $T_6 = 2y^2$, which again contradicts Lemma 4. Thus, the only possibility is that $U_3 = 3x^2$, so that $k = 3\alpha(3)$. Furthermore, in this case, it is easy to verify that $U_3 = (4T^2 - 1)u^2$, and so $4T^2 - 1 = 3y^2$ for some integer y, which is one of the exceptional cases given in the statement of the theorem.

To complete the analysis of Case 1, we must deal with the possibility that $\alpha(3) = 3$. Again let $U_3 = 3m^2n$ with n squarefree. Then $U_k = 3x^2$ implies $k = 3nl$ for some integer l. Applying Lemma 2, it follows that $U_{nl} = y^2$ for some integer y, forcing $nl \in \{1, 2, 3, 4\}$, and hence $k \in \{3, 6, 9, 12\}$. If $U_{12} = 3x^2$, then since U_6 is divisible by 6, it follows that T_6 is a perfect square, which is not possible by Theorem A. If $U_9 = 3x^2$, then Lemma 4

implies that U_3 is a square, which is not possible by Lemma 3 since U_1 is a square. If $U_6 = 3x^2$, then since 3 divides U_3, it follows that T_3 is either a square or twice a square, neither of which is possible. Therefore, the only possible value for k is $\alpha(3) = 3$.

The analysis for $b = 6$ is similar.

Case 2: $b = 5$. Assume that $U_k = 5x^2$ for some integer x. From Lemma 1 we know that $\alpha(3) = 1$, 2, 3, or 5, and so we consider each odd case separately. Assume that $\alpha(5) = 1$, $U = 5m^2n$ with n squarefree. By Lemma 2, if $U_k = 5x^2$, then $k = nl$ for some integer l. Since $U = u^2$, it follows that $n = 5$, and so $U_{5l} = 5x^2$. It follows from Lemma 2 that $U_l = y^2$ for some integer y, and hence $l = 1, 2$ or 4. If $l = 1$, then $U_5 = 5x^2$, and hence $5(x/u)^2 = U_5/U = 16T^4 - 12T^2 + 1$, which by Lemma 7 implies that $T = 1$, which contradicts the fact that $T > 1$.

Assume that $\alpha(5) = 3$, so that $U_3 = 5m^2n$ with n squarefree. By Lemma 2, if $U_k = 5x^2$, then $k = 3nl$ for some integer l. By Lemma 2, $U_{nl} = y^2, 3y^2, 5y^2$ or $15y^2$ for some integer y. By Lemma 6, $5y^2$ is not possible. By Lemma 2, $U_{nl} = 15y^2$ implies 3 divides nl, and $U_{(nl)/3} = 5z^2$ for some integer z, which is not possible by Lemma 6. If $U_{nl} = 3y^2$, then by the results above, $nl = 1, 2$ or 3. The case $nl = 1$ is not possible, since $U = U_1$ is a square. If $nl = 3$, then $U_3 = 3y^2$, together with $U_3 = 5m^2n$ above, implies that 15 divides n, a contradiction. Thus, the only possibility is $nl = 2$. If $n = 1$, then $3 = \alpha(5)$, and we are done. Otherwise, $n = 2$, and $U_3 = 10m^2$, which is not possible since the highest power of 2 dividing U, and hence U_3, is even.

Assume that $\alpha(5) = 5$, so that $U_5 = 5m^2n$ with n squarefree. Let $U_k = 5x^2$. Then it follows that $k = 5nl$ for some integer l. By Lemma 2, $U_{nl} = y^2$ for some integer y, forcing $nl \in \{1, 2, 4\}$, and hence $k \in \{5, 10, 20\}$. If $U_{20} = 5x^2 = 2T_{10}U_{10}$, then $T_{10} = z^2$ for some integer z, which is not possible by Theorem A. Similarly, if $U_{10} = 5x^2 = 2T_5U_5$, it follows that $T_5 = 2^\delta z^2$ for some $\delta \in \{0, 1\}$, which is not possible by Lemma 4 and Theorem A. Thus, the only possibility is $U_5 = 5x^2$, forcing $5(x/u)^2 = U_5/U = 16T^4 - 12T^2 + 1$, which by Lemma 7 yields $T = 1$, which is not possible.

The analysis for $b = 10$ is similar.

Proof of Corollary 1. Consider first the case $b \in \{1, 2\}$. The result is immediate from Lemma 3, and the fact that $U = u^2$ is a square.

Now assume that $b \in \{3, 5, 6, 10\}$. We consider each case separately.

Assume that $b = 3$. Then from Lemma 1 $\alpha(b) = 1, 2$ or 3. Thus by Theorem 1, if $U_k = 3x^2$, then $k = 1, 2$ or 3. Assume that $U_3 = 3x^2$. Since $3x^2 = U_3 = U(4T^2 - 1) = u^2(4T^2 - 1)$, it follows that $4T^2 - 1 = 3y^2$ for some integer y, which is one of the exceptional cases. Thus, aside from this case, $U_k = 3x^2$ implies $k \leq 2$.

Assume that $b = 5$, then by Lemma 1, $\alpha(b)$ is one of $1, 2, 3, 5$.

By Theorem 1, if $U_k = 5x^2$, then for $d \neq 24$, in which case $U_4 = 5(14)^2$, k is one of $1, 2, 3, 5$. We therefore must show that $U_3 = 5x^2$ and $U_5 = 5x^2$ cannot occur. If $U_5 = 5x^2$, then $5(x/u)^2 = U_5/U = 16T^4 - 12T^2 + 1$. By Lemma 7, $T = 1$, which is impossible. Assume that $U_3 = 5x^2$. It is easy to check that $U_3 = U(4T^2 - 1)$, and so $5x^2 = u^2(4T^2 - 1)$, and hence $(2T)^2 - 5(x/u)^2 = 1$. Since the minimal solution to $X^2 - 5Y^2 = 1$ is $9 + 4\sqrt{5}$, it follows that every solution to $X^2 - 5Y^2 = 1$ has X odd, showing that $U_3 = 5x^2$ is not possible.

Assume that $b = 6$, and that $U_k = 6x^2$. By Theorem 1, $k = \alpha(6)$, which implies that $k \in \{1, 2, 3, 6\}$. If $\alpha(6) = 6$ then it is easy to show that 3 divides U_3. Therefore, from the relation $U_6 = 2T_3U_3$, it follows that T_3 is a square or twice a square, contradicting Theorem A or Lemma 4. Assume now that $\alpha(6) = 3$ and that $U_3 = 6x^2$. It follows that 2 divides $U = u^2$ to an odd power, which is not possible. Therefore, the only possibilities for k are $k = 1$ and $k = 2$.

Assume that $b = 10$. Then the possible values for $\alpha(b)$ are $1, 2, 3, 5, 10$. If $\alpha(10) = 10$ it follows that 5 divides U_5, and hence T_5 is either a square or twice a square, which is not possible. If $\alpha(10) = 5$, and $U_5 = 10x^2$, then 2 divides $U = u^2$ to an odd power, which is not possible. Similarly, if $\alpha(10) = 3$, and $U_3 = 10x^2$, then 2 divides $U = u^2$ to an odd power, which is not possible. Thus, the only possible values for k are $k = 1$ and $k = 2$.

Proof of Theorem 2. Since $\alpha(b)$ is even, k is even; $k = 2l$ say. We first consider the case where $\alpha(b)$ divides l. Since $bx^2 = U_k = 2T_lU_l$, $\gcd(T_l, U_l) = 1$, and b divides U_l, it follows that T_l is a square or twice a square, forcing $l = 1$ or $l = 2$ by Theorem A and Lemma 4. Since $\alpha(b)$ divides l and is even, the only possibility is $l = 2$ and $k = 4$. This leads to the exceptional case given in the statement of the theorem.

Assume that $\alpha(b)$ does not divide l. Then $k/\alpha(b)$ is an odd integer, which we will show is equal to 1 unless the exceptional case holds. Assume on the contrary that p is an odd prime dividing $k/\alpha(b)$. Note that since $\alpha(b)$ divides k/p, it follows that b divides $U_{k/p}$. We are assuming that $U_k = bx^2$, and so $bx^2 = 2T_{k/2}U_{k/2}$. Therefore, there is a positive integer b_1 dividing $2b$ such that $T_{k/2} = b_1y^2$ for some integer y. If $b_1 = 1$, then by Theorem A, $k = 2$ or $k = 4$, which entails either that $k = \alpha(b)$, or the exceptional case. Thus we may assume that $b_1 > 1$. By Lemma 4, $k/2 = \beta(b_1)$. The result will be proved by showing that b_1 divides $T_{k/(2p)}$, which contradicts $k/2 = \beta(b_1)$, thereby proving that no such prime p exists.

Let q denote a prime, and assume that q^a properly divides b_1. Then q^a divides $T_{k/2}$. If $q = 2$, it follows from the binomial theorem, similar to the proof of Lemma 2, that q^a divides $T_{k/(2p)}$. If q is an odd prime, then since

b_1 divides $2b$, q^a divides b, and from the remark above, q^a divides $U_{k/p}$. Since $U_{k/p} = 2T_{k/(2p)}U_{k/(2p)}$, either q^a divides $T_{k/(2p)}$ or it divides $U_{k/(2p)}$. If q^a divides $U_{k/(2p)}$, then it divides $U_{k/2}$, which contradicts the fact that q^a divides $T_{k/2}$. Therefore, the only possibility is that q^a divides $T_{k/(2p)}$, and since this holds for any prime dividing b_1, it follows that b_1 divides $T_{k/(2p)}$. As remarked above, this shows that p cannot exist, and hence $k = \alpha(b)$.

We now prove the last statement in Theorem 2. Assume first that the exceptional case holds. Then $U_4 = bx^2$, and since $U_4 = (2T^2 - 1)TU$, it follows that $(2T^2 - 1)T = b_1y^2$ for some integer y and b_1 dividing $2b$. By Baker's effective version of Siegel's theorem on integer solutions to hyperelliptic equations, there is a computable positive constant $c_1 = c_1(b)$, depending only on b, such that $T < c_1$. It follows for this case that $d < c_1^2$.

Otherwise, by the first part of the theorem, if $U_k = bx^2$, then $k = \alpha(b)$. By Lemma 1 and an inductive argument it follows that $\alpha(b) \leq b$ for any positive integer b, and so $U_k = bx^2$ for some k with $1 \leq k \leq b$. It is easy to show that U_k/U can be written as a squarefree polynomial $P_k(T)$ in T of degree $k - 1$. If p is a prime dividing $\gcd(P_k(T), U)$, then from Lemma 2, p divides k, and hence p divides $b!$. Therefore, the equation $U_k = bx^2$ implies that T satisfies a hyperelliptic equation $P_k(T) = vy^2$ with v dividing $b!$, $P_k(T)$ squarefree of degree $k - 1$, and $k \leq b$. If $k \geq 4$, then $P_k(T)$ has at least 3 distinct roots, and so Baker's theorem [1] implies that T, and hence d, is bounded by some computable constant c_2 depending only on b.

References

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

[2] M. A. Bennett and P. G. Walsh, *The Diophantine equation* $b^2X^4 - dY^2 = 1$, Proc. Amer. Math. Soc., to appear.

[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] M. Langevin, *Cas d'inégalité pour le théorème de Mason et applications de la conjecture* (*abc*), C. R. Acad. Sci. Paris Sér. I 317 (1993), 441–444.

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

[7] W. Ljunggren, *Einige Eigenschaften der Einheiten reeller quadratischer und reinbiquadratischer Zahlkörper mit Anwendung auf die Lösung einer Klasse unbestimmter Gleichungen vierten Grades*, Skr. Norske Vid.-Akad. Oslo 1936, no. 12, 1–73.

[8] —, *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$, Avh. Norske Vid. Akad. Oslo 1942, no. 5, 1–26.

[9] —, *Über die Gleichung* $x^4 - Dy^2 = 1$, Arch. Math. Naturv. 45 (1942), no. 5, 61–70.

[10] M. Mignotte et A. Pethő, *Sur les carrés dans certaines suites de Lucas*, J. Théor. Nombres Bordeaux 5 (1993), 333–341.
[11] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge Tracts in Math. 87, Cambridge Univ. Press, New York, 1986.
[12] P. G. Walsh, *A note on a theorem of Ljunggren and the Diophantine equations* $x^2 - kxy^2 + y^4 = 1, 4$, Arch. Math. (Basel), to appear.

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

Received on 21.7.1998 (3421)