ACTA ARITHMETICA
145.2 (2010)

On a Diophantine problem of Bennett

by

Yang Hai (Xi'an) and P. G. Walsh (Ottawa)

1. Introduction. In problem D23 of [3], Bennett asked for the complete set of solutions in integers x, y, z all greater than 1 to the Diophantine equation

$$\frac{x^2-1}{y^2-1} = (z^2-1)^2.$$

We reformulate the problem as follows. For a positive integer $y > 1$, define $\epsilon_y = y+\sqrt{y^2-1}$, and for $k \geq 1$, let $\epsilon_y^k = T_k+U_k\sqrt{y^2-1}$. Bennett's question can then be rephrased as determining all y, k, z for which

$$U_k = z^2 - 1, \tag{1.1}$$

where U_k is the sequence derived from y as above, which is why y is suppressed in (1.1). Equations such as (1.1) were studied in [8], where in particular, the equation $U_k = cz^2 \pm 1$ was completely solved for any even positive integer c.

The purpose of the present paper is to further the results in [8] by similarly dealing with the case of odd values of c. In so doing, not only can one solve the problem of Bennett, but in fact prove somewhat more than that. However, in the process of considering these problems, we arrived at a difficult case, whose solution eludes us. This will be elaborated on in the later part of the introduction.

Theorem 1.1. *For any odd positive integer $c > 1$, the equation $U_k = cz^2 \pm 1$ has at most one solution in positive integers k, z. In the case $c = 1$, the solution in positive integers $(k, z) = (3, 2y)$ to $U_k = z^2 - 1$ exists for all positive integers y, and a second solution exists to $U_k = z^2 \pm 1$ only when y is of the form $2t^2 + 2t$ or $2t^2 + 2t + 1$. In both of these cases, the second solution is given by $(k, z) = (2, 2t + 1)$.*

2010 *Mathematics Subject Classification*: 11B39, 11D25.
Key words and phrases: Diophantine equation, linear recurrence sequence.

DOI: 10.4064/aa145-2-3

Theorem 1.1 not only provides an affirmative answer to the question of Bennett, but somewhat more. For reference purposes, we state the following, which is an immediate consequence of Theorem 1.1.

COROLLARY 1.1. *If $x > 1$, $y > 1$, $z > 0$ are integers satisfying*

$$\frac{x^2 - 1}{y^2 - 1} = (z^2 \pm 1)^2,$$

then there is a positive integer t for which (x, y, z) is one of

$$(4t^3 - 2t, t, 2t), \quad (2(2t^2 + 2t)^2 - 1, 2t^2 + 2t, 2t + 1),$$
$$(2(2t^2 + 2t + 1)^2 - 1, 2t^2 + 2t + 1, 2t + 1).$$

One can similarly consider the case that the sequence U_k is replaced by u_k, defined as follows. Let $y \geq 1$ be a positive integer, and let $\beta_y = y + \sqrt{y^2 + 1}$, and for $k \geq 1$, define

$$\beta^k = t_k + u_k \sqrt{y^2 + 1}.$$

We are unable to prove a result as strong as Theorem 1.1, but we can prove enough in order to obtain an analogue of Corollary 1.1.

THEOREM 1.2. *All positive integer solutions to*

$$\frac{x^2 + 1}{y^2 + 1} = (z^2 \pm 1)^2$$

are given by

$$(x, y, z) = (4t^3 + 3t, t, 2t),$$

where t is a positive integer.

Given the statements in Corollary 1.1 and Theorem 1.2, it is natural to consider the more general equation

$$\frac{x^2 \pm 1}{y^2 \pm 1} = (z^2 \pm 1)^2.$$

In order to solve this completely, there are two remaining cases, one which is trivial to solve, and one which seems to be quite difficult to deal with. The first case is the equation

$$\frac{x^2 + 1}{y^2 - 1} = (z^2 \pm 1)^2,$$

which has no solutions in positive integers $x, y > 1$, and z, simply because $\sqrt{y^2 - 1}$ has a very short period in its continued fraction expansion, which implies that there are no units of norm -1 in any order of the form $\mathbb{Z}[\sqrt{y^2 - 1}]$.

On the other hand, the second case, which is the equation

$$\frac{x^2-1}{y^2+1} = (z^2 \pm 1)^2,$$

appears to be resistant to the methods we use to prove Corollary 1.1 and Theorem 1.2, primarily because of the absence of suitable identities which will be used in the proofs of the above results. Therefore, we can only state the following as an open problem.

Open Problem. Determine the set of integer solutions $x > 1$, $y > 0$, $z > 0$ to

$$\frac{x^2-1}{y^2+1} = (z^2 \pm 1)^2.$$

2. Preliminaries. We state here a number of results which will be used in the proofs of the theorems stated above. For a positive integer $y > 1$, define

$$\epsilon_y = y + \sqrt{y^2-1},$$

and for $k \geq 1$,

$$\epsilon_y^k = T_k + U_k\sqrt{y^2-1}.$$

Similarly, define

$$\tau_y = \frac{\sqrt{y+1}+\sqrt{y-1}}{\sqrt{2}},$$

and for $k \geq 1$ odd, let

$$\tau_y^k = \frac{A_k\sqrt{y+1}+B_k\sqrt{y-1}}{\sqrt{2}}.$$

Note that $\tau_y^2 = \epsilon_y$.

Lemma 2.1.

(1) *If a prime p divides A_k or B_k for some k, then p does not divide T_i for any $i \geq 1$.*
(2) *If P and Q denote the set of primes dividing some term in the sequence $\{A_k\}$ and $\{B_k\}$ respectively, then P and Q are disjoint.*
(3) *T_k is odd for all even indices k, and if 2^a properly divides T_1, then 2^a properly divides T_k for all odd k.*
(4) *U_k is odd for all odd k. If $a > 1$, 2^a properly divides k, and 2^b properly divides y, then 2^{a+b} properly divides U_k.*
(5) *For all odd $k \geq 1$, $\gcd(T_k, U_{k+1}) = \gcd(T_k, U_{k-1}) = T_1$.*
(6) *For all $k \geq 0$, $U_{2k+1} + 1 = 2T_kU_{k+1}$ and $U_{2k+1} - 1 = 2T_{k+1}U_k$.*
(7) *For all $k \geq 1$, $U_{2k} + 1 = A_{2k-1}B_{2k+1}$ and $U_{2k} - 1 = A_{2k+1}B_{2k-1}$.*

Proof. (1) The fact that $\tau_y^2 = \epsilon_y$ implies that $A_kB_k = 2^\delta U_k$ for odd k, where $\delta = 0, 1$ depending on whether y is odd or even respectively. Therefore,

if p divides one of A_k or B_k, then p divides U_k. Note that k is odd. If p were to divide T_i say, then the identity $U_{2i} = 2T_iU_i$ implies that p divides U_{2i}, which further implies that p divides $(U_k, U_{2i}) = U_{\gcd(k,2i)}$. Since k is odd, $\gcd(k, 2i)$ is odd, and so $U_{\gcd(k,2i)}$ divides U_i, showing that p divides U_i, contradicting the fact that $\gcd(T_i, U_i) = 1$.

(2) Assume that p divides both A_i and B_j. Then p also divides A_{ij} and B_{ij}, contradicting the fact that $\gcd(A_k, B_k) = 1$.

(3), (4) This is well known and can be found in the seminal paper of Lehmer [4].

(5) We refer to Lemma 1 in [8].

(6) We refer to the proof of Theorem 1 in [8].

(7) It can be seen that

$$U_{2k} = \frac{\epsilon_y^{2k} - \epsilon_y^{-2k}}{\epsilon_y - \epsilon_y^{-1}},$$

and that

$$A_{2k-1}B_{2k+1} = \left(\frac{\tau_y^{2k-1} + \tau_y^{-2k+1}}{\tau_y + \tau_y^{-1}}\right)\left(\frac{\tau_y^{2k+1} - \tau_y^{-2k-1}}{\tau_y - \tau_y^{-1}}\right),$$

and the result follows by simplifying the latter expression, and using $\tau_y^2 = \epsilon_y$.

LEMMA 2.2.

(1) *The quartic equation $aX^4 - bY^4 = 2$ has at most one solution in positive integers X, Y for any given positive integers a, b.*
(2) *The quartic equation $a^2X^4 - bY^2 = 1$ has at most one solution in positive integers X, Y for any given positive integers $a > 1$, $b > 1$.*
(3) *The quartic equation $aX^2 - bY^4 = 1$ has at most one solution in positive integers X, Y for any given positive integers $a > 1, b$.*
(4) *If y is even, then the only possible squares in $\{B_k\}$ are B_1 and B_3. If y is odd, then only square in $\{B_k\}$ is B_1.*

Proof. (1) If a is odd, this follows from the main result in [6]. If $a = 2$, it follows from Ljunggren's theorem on $X^4 - dY^2 = 1$, and Cohn's refinement of it in [2]. If $a > 2$ is even, then it follows from Ljunggren's theorem in [5] on $aX^2 - bY^4 = 1$. Alternatively, the reader may refer to Theorem 15 on p. 274 of [7].

(2) This is the main result in [1].

(3) This is the main result in [5].

(4) If y is even, then this is the main result in [6], while if y is odd, then it follows from the main result in [5].

3. Proof of Theorem 1.1. The proof of Theorem 1 in [8], precisely as given there, can be used to show that the equation $U_{2k+1} = cx^2 \pm 1$ has

at most one solution in integers $k \geq 0$ and $x > 0$. Therefore, in order to complete the proof, we need only deal with the two cases

$$U_{2k} = cx_1^2 \pm 1, \quad U_{2l} = cx_2^2 \pm 1, \tag{3.1}$$

and

$$U_{2k} = cx_1^2 \pm 1, \quad U_{2l+1} = cx_2^2 \pm 1. \tag{3.2}$$

For (3.1), we consider the particular case

$$U_{2k} = cx_1^2 - 1, \quad U_{2l} = cx_2^2 - 1, \tag{3.3}$$

as the proof for the other possibilities works in exactly the same manner. Now, (3.3) together with the identity $U_{2i}+1 = A_{2i-1}B_{2i+1}$ shows that there are positive integers a, b, A, B, u, v, z, w, with $c = ab = AB$, for which

$$A_{2k-1} = au^2, \quad B_{2k+1} = bv^2, \quad A_{2l-1} = Az^2, \quad B_{2l+1} = Bw^2.$$

By (2) of Lemma 2.1, the sets of prime factors dividing terms in $\{A_i\}$ and $\{B_i\}$ are disjoint, and so it follows that $a = A$ and $b = B$. Therefore, $(X, Y) = (u, v)$ and (z, w) are two solutions in positive integers to the quartic equation

$$a^2(y+1)X^4 - b^2(y-1)Y^4 = 2,$$

which is not possible by (1) of Lemma 2.2.

We now deal with (3.2). Assume first that k, l, x_1, x_2 are solutions to

$$U_{2k} = cx_1^2 - 1, \quad U_{2l+1} = cx_2^2 + 1.$$

Then, by (6) and (7) of Lemma 2.1,

$$U_{2k} + 1 = A_{2k-1}B_{2k+1} = cx_1^2, \quad U_{2l+1} - 1 = 2T_lU_{l+1} = cx_2^2.$$

Therefore, since T_lU_{l+1} is even, l must be odd, and there are integers a, b, A, B, u, v, z, w, with $c = ab = AB$, for which either

$$A_{2k-1} = au^2, \quad B_{2k+1} = bv^2, \quad T_l = 2AT_1z^2, \quad U_{l+1} = BT_1w^2,$$

or

$$A_{2k-1} = au^2, \quad B_{2k+1} = bv^2, \quad T_l = AT_1z^2, \quad U_{l+1} = 2BT_1w^2.$$

If p is a prime dividing A, then by (1) of Lemma 2.1, p does not divide $A_{2k-1}B_{2k+1}$, which implies that p is not a divisor of either a or b. Since $c = ab = AB$, it follows that $A = 1$, and so by (5) of Lemma 2.1, either $T_l = 2T_1z^2$ or $T_l = T_1z^2$. The former possibility cannot happen since by (3) of Lemma 2.1, the same power of 2 properly divides both T_1 and T_l, and so $T_l = T_1z^2$. By (2) of Lemma 2.2, it follows that $l = 1$, and hence $cx_2^2 = 2T_lU_{l+1} = 2T_1U_2 = 2y(2y) = 4y^2$, forcing $c = 1$. The case

$$U_{2k} = cx_1^2 + 1, \quad U_{2l+1} = cx_2^2 + 1$$

can be dealt with in exactly the same manner.

Assume now that $k > 0$, $l \geq 0$, $x_1 > 0$, $x_2 > 0$ are integer solutions to

$$U_{2k} = cx_1^2 - 1, \quad U_{2l+1} = cx_2^2 - 1.$$

Then again by (6) and (7) of Lemma 2.1,

$$U_{2k} - 1 = A_{2k+1}B_{2k-1} = cx_1^2, \quad U_{2l+1} - 1 = 2T_{l+1}U_l = cx_2^2.$$

$T_{l+1}U_l$ is therefore even, from which it follows by (3) and (4) of Lemma 2.1 that l must be even. Arguing precisely as in the previous case, we deduce that there is a positive integer z for which either $T_{l+1} = 2T_1z^2$ or $T_{l+1} = T_1z^2$, which by (3) of Lemma 2.1 implies that $T_{l+1} = T_1z^2$. By (2) of Lemma 2.2, it follows that $l = 0$. The original equation becomes $U_{2l+1} = U_1 = 1 = cx_2^2 - 1$, which implies that $cx_2^2 = 0$, a contradiction. The same argument also shows that the simultaneous equations

$$U_{2k} = cx_1^2 + 1, \quad U_{2l+1} = cx_2^2 - 1$$

do not have solutions in positive integers.

The completion of the proof of Theorem 1.1 now only requires that we deal with the case $c = 1$.

Assume that k, x is a solution to $U_{2k+1} = x^2 - 1$. Then by (6) of Lemma 2.1,

$$U_{2k+1} + 1 = 2T_kU_{k+1} = x^2,$$

and (3) and (4) of Lemma 2.1 imply that k is odd. By (5) of Lemma 2.1, and the fact that the same power of 2 properly divides T_k and T_1, it follows that $T_k = T_1u^2$ for some integer u, which by (2) of Lemma 2.2 implies that $k = 1$, and hence that $x = 2y$.

Assume that k, x is a solution to $U_{2k+1} = x^2 + 1$. Then by (6) of Lemma 2.1,

$$U_{2k+1} - 1 = 2T_{k+1}U_k = x^2,$$

and in this case k must be even. It follows just as above that $T_{k+1} = T_1u^2$, forcing $k = 0$, which in turn implies that $x = 0$, a contradiction.

Assume that k, x is a solution to $U_{2k} = x^2 + 1$. Then by (7) of Lemma 2.1,

$$U_{2k} - 1 = A_{2k+1}B_{2k-1} = x^2,$$

it follows that A_{2k+1} and B_{2k-1} are squares. By (4) of Lemma 2.2, B_{2k-1} can be a square for only $k = 1$ or $k = 2$. If $k = 2$, then $A_{2k+1} = A_5$, and it is easy to verify that $A_5 = 4y^2 - 2y - 1$, which can never be a square, since $y > 1$. So, the only possibility is $k = 1$. For the case $k = 1$, it is easy to verify that $A_3 = 2y - 1$ and $B_1 = 1$, and these are both squares precisely when $y = 2t^2 + 2t + 1$ for some integer t.

Assume that k, x is a solution to $U_{2k} = x^2 - 1$. Then by (7) of Lemma 2.1,

$$U_{2k} + 1 = A_{2k-1}B_{2k+1} = x^2,$$

and it follows that A_{2k-1} and B_{2k+1} are both squares. By (4) of Lemma 2.2, B_{2k+1} can be a square only for $k = 0$ and $k = 1$, and so the only possibility is $k = 1$, for otherwise $A_{2k-1} = A_{-1}$. In this case, $A_1 = 1$ and $B_3 = 2y + 1$ are squares precisely when $y = 2t^2 + 2t$ for some integer t.

4. Proof of Theorem 1.2. We will use analogous statements to (3)–(7) in Lemma 2.1. A solution to

$$\frac{x^2+1}{y^2+1} = (z^2 \pm 1)^2$$

is equivalent to the existence of an odd index $2i+1$ for which $u_{2i+1} = z^2 \pm 1$. It can proved, similar to (6) of Lemma 2.1, that $u_{2i+1} \pm 1$ is one of $2t_i u_{i+1}$ with i odd, or $2t_{i+1}u_i$ with i even. Therefore, either $z^2 = 2t_i u_{i+1}$ with i odd, or $z^2 = 2t_{i+1}u_i$ with i even. Also, for i odd, $\gcd(t_i, u_{i+1}) = t_1$, while for i even, $\gcd(t_{i+1}, u_i) = t_1$. Furthermore, 2 properly divides t_1 and t_i to the same power in the first case, and 2 properly divides t_1 and t_{i+1} to the same power in the second case. We deduce that there is an integer u for which $t_i = t_1 u^2$ in the first case, and $t_{i+1} = t_1 u^2$ in the second case. By (3) of Lemma 2.2, $i = 1$ in the first case, and $i + 1 = 1$ in the second case. We therefore see that the second case cannot occur, for otherwise it follows that $z = 0$. So, the only possibility is $i = 1$, which gives $u_{2i+1} = u_3 = 4y^2 + 1 = z^2 \pm 1$. Therefore, $z = 2y$, $x = t_3 = 4y^3 + 3y$, and the result follows by simply setting y to be a parameter t.

Acknowledgements. The first author would like to thank Prof. Zhang Wenpeng for his instruction and encouragement.

This work is supported by N.S.F. (No.10601039, 60472068) of P.R. China and 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] J. H. E. Cohn, *The Diophantine equation $x^4 - Dy^2 = 1$, II*, Acta Arith. 78 (1997), 401–403.

[3] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Springer, New York, 2004.

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

[5] W. Ljunggren, *Ein Satz über die diophantische Gleichung $Ax^2 - By^4 = C$ ($C = 1, 2, 4$)*, in: Tolfte Skandinaviska Matematikerkongressen (Lund, 1953), Lunds Universitets Matematiska Inst., Lund, 1954, 188–194.

[6] F. Luca and P. G. Walsh, *Squares in Lehmer sequences and some Diophantine applications*, Acta Arith. 100 (2001), 47–62.

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

[8] P. G. Walsh, *Near squares in linear recurrence sequences*, Glas. Mat. Ser. III 38 (2003), 11–18.

Yang Hai (corresponding author)
Research Center for Basic Science
Xi'an Jiaotong University
Xi'an, Shaanxi, 710049 P.R. China
E-mail: xjtu88yh@163.com

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

Received on 11.7.2009
and in revised form on 17.3.2010 (6082)