COLLOQUIUM MATHEMATICUM

VOL. 105 2006 NO. 1

ON THE DIOPHANTINE EQUATION $x^2 - dy^4 = 1$ WITH PRIME DISCRIMINANT II

BY

D. POULAKIS (Thessaloniki) and P. G. WALSH (Ottawa)

Abstract. Let p denote a prime number. P. Samuel recently solved the problem of determining all squares in the linear recurrence sequence $\{T_n\}$, where T_n and U_n satisfy $T_n^2 - pU_n^2 = 1$. Samuel left open the problem of determining all squares in the sequence $\{U_n\}$. This problem was recently solved by the authors. In the present paper, we extend our previous joint work by completely solving the equation $U_n = bx^2$, where b is a fixed positive squarefree integer. This result also extends previous work of the second author.

1. Introduction. Ljunggren [5] proved that the Diophantine equation

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

has at most two solutions in positive integers, and gave precise information on the location of the solutions when two solutions exist. This general theorem has recently been improved substantially in [11]. Specifically, in that paper the assumption of the existence of two solutions has been removed, and a conclusion similar to that in Ljunggren's result has been proved.

We first define some notation that will be used throughout the paper. For a positive nonsquare integer d, we denote by $\varepsilon_d = T + U\sqrt{d}$ the minimal unit in $\mathbb{Z}[\sqrt{d}]$ of norm 1, and for $k \geq 1$, we define $T_k + U_k\sqrt{d} = (T + U\sqrt{d})^k$.

THEOREM A (Togbe, Voutier, Walsh).

(i) *There are at most two positive integer solutions* (x, y) *to equation* (1). *If two solutions* $y_1 < y_2$ *exist, then* $y_1^2 = U_1$, $y_2^2 = U_2$, *except only if* $d = 1785$ *or* $d = 16 \cdot 1785$, *in which case* $y_1^2 = U_1$, $y_2^2 = U_4$.

(ii) *If only one positive integer solution* (x, y) *exists to equation* (1), *then* $y^2 = U_l$, *where* $U_1 = lv^2$ *for some squarefree integer* l, *and either* $l = 1$, $l = 2$, *or* $l = p$ *for some prime* $p \equiv 3 \pmod 4$.

P. Samuel [10] has proved a number of interesting related results in the case that d is prime, or twice a prime, but for equation (1), with d a prime, these results fall short of what is the best possible result. More recently

2000 *Mathematics Subject Classification*: 11D41, 11B39.

Key words and phrases: Pell equation, linear recurrence sequence, Diophantine equation.

we established in [9] a sharp result on the solutions of equation (1) in the case that d is prime, improving upon Theorem 5.2 in [10]. In particular, we proved that apart from one exceptional case, the equation $U_k = y^2$ implies that $k = 1$.

Let $\{T_k\}$ and $\{U_k\}$ be the sequences defined above. For a positive integer b, we define the *rank of apparition* of b in $\{T_k\}$ to be the smallest index k for which b divides T_k, should such an index exist, and denote it as $\beta(b)$. If no such index exists, we write $\beta(b) = \infty$. Similarly, we define the rank of apparition of b in $\{U_k\}$ as the smallest index k for which b divides U_k, and denote this as $\alpha(b)$.

Note that $\alpha(b)$ is always a positive integer. In [1], it was shown that for $b > 1$, an integer solution to the equation $T_k = bx^2$ implies that $k = \beta(b)$. In [12], a similar result was proved for the sequence $\{U_k\}$ under the added assumption that $\alpha(b)$ is even. Moreover, a precise conjecture on the remaining case was given, which remains open. The purpose of the present paper is to extend the main result of [9] to equations of the form $U_k = by^2$ in the case that the discriminant d is prime, and thereby prove Conjecture 1 in [12] for the case that d is prime.

THEOREM 1. *Let p be a prime number, b a positive integer, and*

$$T_k + U_k\sqrt{p} = (T + U\sqrt{p})^k,$$

where $T + U\sqrt{p}$ is the minimal unit in $\mathbb{Z}[\sqrt{p}]$ greater than 1, and of norm 1. If x is an integer for which $U_k = bx^2$, then $k = \alpha(b)$ except only in the following specific cases:

(i) $(p, b) = (3, 1)$, *in which case* $U_2 = U_{2\alpha(b)} = 2^2$,
(ii) $(p, b) = (7, 3)$, *in which case* $U_2 = U_{2\alpha(b)} = 3 \cdot 4^2$,
(iii) $(p, b) = (5, 2)$, *in which case* $U_2 = U_{2\alpha(b)} = 2 \cdot 6^2$,
(iv) $(p, b) = (29, 910)$, *in which case* $U_2 = U_{2\alpha(b)} = 910 \cdot 198^2$.

2. Preliminary results. In this section we will collect those results which will be needed in the course of proving Theorem 1.

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

$$\varepsilon_d = \tau^2,$$

where

$$\tau = \frac{a\sqrt{m} + b\sqrt{n}}{\sqrt{c}},$$

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

Proof. This is well known, for example see Nagell [8].

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

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

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

Proof. This has recently been proved in [6], improving upon previous work of Ljunggren.

The following is a beautiful generalization of the aforementioned result of Ljunggren on the equation $x^2 - 2y^4 = -1$. The extensive details of the proof are in [2], or alternatively in [13], where this result was proved independently.

LEMMA 3 (Chen–Voutier and Yuan). *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 $(X, Y) = (v, \sqrt{u})$.*

LEMMA 4. *The equations $x^2 - 2y^4 = 1$ and $x^4 - 2y^2 = 1$ have no solutions in positive integers, the only positive integer solution to the equation $x^4 - 2y^2 = -1$ is $(x, y) = (1, 1)$, and the only positive integer solutions to the equation $x^2 - 2y^4 = -1$ are $(x, y) = (1, 1), (239, 13)$.*

These are all trivial except for the last equation, which Ljunggren first solved in [4].

3. Proof of Theorem 1. Assume first that $\alpha(b)$ is even. By Theorem 2 of [12], either $k = \alpha(b)$, or $k = 4 = 2\alpha(b)$, and in the latter case, $2T^2 - 1 = v^2$ for some integer v, and $TU = bu^2$ for some integer u. Therefore,

$$v^4 - 1 = (v^2 - 1)(v^2 + 1) = (2T^2 - 2)(2T^2) = p(2TU)^2,$$

and by Theorem 2.1 of [10], either $p = 5$ and $v = 3$, or $p = 29$ and $v = 99$. In either case we see that $v^2 + 1$ is not of the form $2T^2$, and so $k = 4 = 2\alpha(b)$ cannot occur. We will henceforth assume that $\alpha(b)$ is odd.

We first show that if k is even, then $k = 2$. Let $k = 2l$; then $bx^2 = U_{2l} = 2T_lU_l$, and since $\alpha(b)$ is odd, $\gcd(b, T_i) = 1$ for all i, and so $T_l = z^2$ or $2z^2$ for some integer z. By Corollary 1.3 of [1] and the main result of [3], it follows that $l = 1$, in which case $k = 2$, or else $l = 2$, and in this case $T_l = z^2$, which we show is impossible. If $T_l = T_2 = z^2$, then $U_k = U_4 = bx^2$, and $U_l = U_2 = 2T_1U_1 = 2bz_1^2$ or $(b/2)z_1^2$ for some integer z_1. Since $\alpha(b)$ is odd, this forces $T_1 = z_2^2$ or $2z_2^2$ for some integer z_2. Since $T_2 = 2T_1^2 - 1$, the only possibility is $T_1 = 13^2$, by Ljunggren's [4] theorem on the quartic equation $X^2 - 2Y^4 = -1$, and hence the discriminant p is forced to be 1785, which is not prime. Therefore, $l = 1$ and $k = 2$ as asserted.

Now assume that $U_2 = bx^2$ for some integer x, and that $\alpha(b) = 1$. Then $\gcd(T_1, b) = 1$, and since $U_2 = 2T_1U_1$, it follows that T_1 is either a square, or twice a square. Appealing to Theorems 2.1 and 2.2 of [10], we obtain the specific cases given in the statement of Theorem 1.

We will henceforth assume that k is odd. We will consider two cases separately, depending on the value of c in Lemma 1.

CASE 1: $c = 2$. Assume that k is an integer for which $U_k = bx^2$, and let $\tau = (a_1 + b_1\sqrt{p})/\sqrt{2}$ denote the minimal solution to $X^2 - pY^2 = \pm 2$, and note that $\tau^2 = T + U\sqrt{p}$. For $i \geq 1$, let

$$\tau^{2i+1} = \frac{a_{2i+1} + b_{2i+1}}{\sqrt{2}}.$$

We will assume that $X^2 - pY^2 = 2$ is solvable, as the argument presented holds equally well in the case that $X^2 - pY^2 = -2$ is solvable.

Assuming that $U_k = bx^2$ with k odd, we get $bx^2 = a_kb_k$, and so there are positive integers m, n, u, v with $b = mn$ for which $a_k = mu^2$, $b_k = nv^2$, hence

$$m^2u^4 - pn^2v^4 = 2.$$

By Lemma 2, $(X, Y) = (u^2, v^2)$ is either the minimal solution, or the third power of the minimal solution, of the quadratic equation

$$m^2X^2 - pn^2Y^2 = 2,$$

and an argument identical to that presented in [9] shows that the latter case is not possible. This is equivalent to the statement that $k = \alpha(b)$.

CASE 2: $c = 1$. Assume that k is an integer for which $U_k = bx^2$, and let $\tau = a_1 + b_1\sqrt{p}$ denote the minimal solution to $X^2 - pY^2 = -1$, and note that $\tau^2 = T + U\sqrt{p}$. For $i \geq 1$, let

$$\tau^{2i+1} = \frac{a_{2i+1} + b_{2i+1}}{\sqrt{2}}.$$

Assuming that $U_k = bx^2$ with k odd, we obtain $bx^2 = 2a_kb_k$, and so there are positive integers m, n, u, v with $mn = 2b$ if b is odd, $mn = b/2$ if b is even, and for which $a_k = mu^2$, $b_k = nv^2$. It follows that

$$m^2u^4 - pn^2v^4 = -1.$$

By Lemma 3, with $d = pn^2 > 2$ and $p > 2$, $(X, Y) = (u^2, v^2)$ must be the minimal solution of the quadratic equation

$$X^2 - pn^2Y^2 = -1.$$

This is equivalent to the statement that $k = \alpha(b)$. Assume now that $pn^2 = 2$; then by Lemma 4, the equation $m^2u^4 - pn^2v^4 = -1$ implies that $mu^2 + v^2\sqrt{2}$ is either $1 + \sqrt{2}$ or $239 + 169\sqrt{2}$, and $b = 2$ or 478 respectively. In either case, $k = \alpha(b)$.

Acknowledgements. The second author gratefully acknowledges support from the Natural Sciences and Engineering Research Council of Canada.

REFERENCES

[1] M. A. Bennett and P. G. Walsh, *The Diophantine equation* $b^2X^4 - dY^2 = 1$, Proc. Amer. Math. Soc. 127 (1999), 3481–3491.

[2] 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.

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

[4] W. Ljunggren, *Zur Theorie der Gleichung* $x^2 + 1 = Dy^4$, Avh. Norske Vid. Akad. Oslo 1942, no. 5, 1–27.

[5] —, *Einige Eigenschaften der Einheiten reeller quadratischer und rein-biquadratischer Zahlkörper mit Anwendung auf die Lösung einer Klasse unbestimmter Gleichungen vierten Grades*, Oslo Vid.-Akad. Skrifter 1936, no. 12, 1–73.

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

[9] D. Poulakis and P. G. Walsh, *A note on the Diophantine equation* $X^2 - dY^4 = 1$ *with prime discriminant*, C. R. Math. Acad. Sci. Soc. R. Can. 27 (2005), 54–57.

[10] P. Samuel, *Résultats élémentaires sur certaines équations diophantiennes*, J. Théor. Nombres Bordeaux 14 (2002), 629–646.

[11] A. Togbe, P. M. Voutier and P. G. Walsh, *Solving a family of Thue equations with an application to the equation* $x^2 - dy^4 = 1$, Acta Arith. 120 (2005), 39–58.

[12] P. G. Walsh, *The Diophantine equation* $X^2 - db^2Y^4 = 1$, ibid. 87 (1998), 179–188.

[13] P. Yuan, *Rational and algebraic approximations of algebraic numbers and their application*, Sci. China Ser. A 40 (1997), 1045–1051.

Department of Mathematics
Aristotle University of Thessaloniki
University Campus
541 24 Thessaloniki, Greece
E-mail: poulakis@ccf.auth.gr

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

Received 27 February 2005;
revised 1 July 2005 (4571)