ACTA ARITHMETICA
137.3 (2009)

Addendum on the equation $aX^4 - bY^2 = 2$

by

S. Akhtari (Kingston, ON), A. Togbé (Westville, IN) and
P. G. Walsh (Ottawa, ON)

In a recent paper [2], we proved that for $t > 40\,000$, the Diophantine equation $(t+2)X^4 - tY^2 = 2$ has at most two solutions in positive integers X, Y. In this addendum, we recall a simple argument due to Ljunggren [4] which, together with an observation due to Voutier [5], shows that for any two positive integers a and b, the quartic equation $aX^4 - bY^2 = 2$ has at most two solutions in positive integers X, Y.

By the main result in [1], we restrict our attention to pairs of odd integers a, b, and furthermore, we need only consider those pairs a, b for which the quadratic equation $ax^2 - by^2 = 2$ is solvable in odd integers x, y. Given such a pair of integers a, b, let $(x, y) = (u_1, v_1)$ denote the smallest solution in positive integers to $ax^2 - by^2 = 2$, and define

$$\tau = \tau_{a,b} = \frac{u_1\sqrt{a} + v_1\sqrt{b}}{\sqrt{2}}.$$

For $i \ge 1$ odd, define sequences $\{u_i\}, \{v_i\}$ by

$$\tau^i = \frac{u_i\sqrt{a} + v_i\sqrt{b}}{\sqrt{2}}.$$

Then all positive integer solutions (x, y) to the quadratic equation $ax^2 - by^2 = 2$ are given by $(x, y) = (u_i, v_i)$.

Theorem 1. *If a, b are positive integers, then the equation*

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

has at most two solutions in positive integers X, Y.

As stated, Theorem 1 is best possible, since for the cases $(a, b) = (2m^2 + 2m + 2, 2m^2 + 2m)$ and $(a, b) = (2m^2 + 2m + 2, (m^2 + m)/2)$, there are the two positive integer solutions $(X, Y) = (1, 1), (2m + 1, 4m^2 + 4m + 3)$

2000 *Mathematics Subject Classification*: 11D41, 11B39.
Key words and phrases: Diophantine equation, elliptic curve, linear recurrence.

DOI: 10.4064/aa137-3-1

and $(X, Y) = (1, 2), (2m+1, 8m^2+8m+6)$ respectively to equation (1). However, in the primary case considered in this paper, namely that a and b are odd, we conjecture that there is at most one solution in positive integers to (1). This conjecture was verified for $(a, b) = (t+2, t)$, with t in the range $1 \leq t < 1200$.

Proof of Theorem 1. Let us first point out that Voutier [5] has refined the argument in [2], thereby proving that for all odd positive integers t, the quartic equation $(t+2)X^4 - tY^2 = 2$ has at most two solutions in odd positive integers X, Y.

We will now assume that a, b are odd positive integers for which there is at least one solution in odd integers (X, Y) to the equation $aX^4 - bY^2 = 2$. Thus, there is at least one odd positive integer k with the property that u_k is a square, and we assume that k represents the smallest such integer. The purpose for choosing the minimal such value is to first show that this integer k divides all indices k_1 for which u_{k_1} is a square, which will then allow us to associate to the equation $aX^4 - bY^2 = 2$ a minimal positive integer t, and a corresponding equation of the form $(t+2)X^4 - tY^2 = 2$, and describe a one-to-one correspondence between the positive integer solutions to these two equations. Given k as above, define the positive integer X_0 specifically by $u_k = X_0^2$.

Before proceeding, we remind the reader of two basic facts about the sequence $\{u_n\}$ defined above. These facts follow from the elementary theory of Lucas functions given in [3], and can easily be proved using binomial expansions. We forego the details, since the proofs are identical to those of Theorems 1.5 and 1.6 in [3]. The first property simply states that $\{u_n\}$ is a divisibility sequence, while the second is referred to as the *Law of Repetition.* We say that a prime power p^l *properly divides* a positive integer n if p^l divides n and $(p, n/p^l) = 1$.

- **I.** If m and n are odd, and m divides n, then u_m divides u_n.
- **II.** Let p denote an odd prime, l a positive integer with $\gcd(p, l) = 1$, and t a non-negative integer. If α is a positive integer for which p^α properly divides u_n, then $p^{\alpha+t}$ properly divides u_{lnp^t}.

We now write $u_1 = l_1 s_1^2$ with l_1 a positive squarefree integer. Note that since $\{u_n\}$ is a divisibility sequence, u_1 divides u_k. If $l_1 = 1$, then u_1 is a square, and hence $k = 1$. We observe in this case that $l_1 = 1$ divides k. Assume now that $l_1 > 1$, and let p denote a prime dividing l_1. Then p divides u_1 exactly to an odd power, say $2e+1$. Since u_1 divides u_k, we see that p^{2e+1} divides u_k, but as u_k is a square, it follows that p^{2e+2} must divide u_k. By property **II**, it follows that p divides k, and since this holds for all p dividing l_1, it follows that l_1 divides k.

If $l_1 > 1$, write $u_{l_1} = l_2 s_2^2$ with l_2 a positive squarefree integer. Since l_1 divides k, we see that u_{l_1} divides u_k. Also, note that $\gcd(l_1, l_2) = 1$, since, by the Law of Repetition, each prime dividing l_1 divides $u_{l_1} = l_2 s_2^2$ exactly to an even power. By precisely the same reasoning as that given in the previous paragraph, it follows that the squarefree integer $l_1 l_2$ divides k, and that $u_{l_1 l_2}$ divides u_k. Now if $l_2 = 1$, then u_{l_1} is a square, and so $l_1 = k$. Otherwise, if $l_2 > 1$, then we write $u_{l_1 l_2} = l_3 s_3^2$ with l_3 squarefree, and just as above, it follows that l_1, l_2, l_3 are pairwise coprime, that the squarefree integer $l_1 l_2 l_3$ divides k, and that $u_{l_1 l_2 l_3}$ divides u_k. Since k is finite, this process evidently must stop, and we conclude that there are pairwise coprime squarefree integers $l_1, \ldots, l_j$ such that $k = l_1 \cdots l_j$. We remark that by arguing exactly as above, if k_1 is any odd positive integer for which u_{k_1} is a square, then $k = l_1 \cdots l_j$ is a divisor of k_1.

With k and $u_k = X_0^2$ as above, define t by

$$t = a u_k^2 - 2 = a X_0^4 - 2 = b v_k^2,$$

and put

$$\gamma = \frac{\sqrt{t+2} + \sqrt{t}}{\sqrt{2}}.$$

We note that $\gamma = \tau^k$, and remark that the sequence $\{v_n\}$ is also a divisibility sequence. For $i \geq 1$ odd, we define new sequences $\{U_i\}, \{V_i\}$ by

$$\gamma^i = \frac{U_i \sqrt{t+2} + V_i \sqrt{t}}{\sqrt{2}}.$$

Then

$$\begin{aligned} \frac{U_i \sqrt{t+2} + V_i \sqrt{t}}{\sqrt{2}} = \gamma^i = \tau^{ki} &= \frac{u_{ki}\sqrt{a} + v_{ki}\sqrt{b}}{\sqrt{2}} \\ &= \frac{(u_{ki}/u_k)\sqrt{t+2} + (v_{ki}/v_k)\sqrt{t}}{\sqrt{2}}, \end{aligned}$$

from which it follows that for each odd $i \geq 1$,

$$U_i u_k = U_i X_0^2 = u_{ki}.$$

Therefore, u_{ki} is a square precisely when U_i is a square. As remarked at the end of the previous paragraph, the set of squares in the sequence $\{u_i\}$ is contained in the subsequence $\{u_{ki}\}$, and hence there is a one-to-one correspondence between the set of squares in $\{u_i\}$ and the set of squares in $\{U_i\}$.

To complete the proof, we observe that by Voutier's recent refinement [5] of the main result of [2], the sequence $\{U_i\}$ contains at most two squares, from which Theorem 1 now follows by the correspondence given in the previous paragraph.

Acknowledgements. The first author would like to thank Michael Bennett for his guidance and support. The second author is partially supported by Purdue University North Central. The third author gratefully acknowledges support from the Natural Sciences and Engineering Research Council of Canada.

References

[1] S. Akhtari, *The equation* $aX^4 - bY^2 = 1$, J. Reine Angew. Math., to appear.

[2] S. Akhtari, A. Togbé and P. G. Walsh, *On the equation* $aX^4 - bY^2 = 2$, Acta Arith. 131 (2008), 145–169.

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

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

[5] P. M. Voutier, *A further note on "On the equation* $aX^4 - bY^2 = 2$*"*, Acta Arith. 137 (2009), 203–206.

Department of Mathematics, Jeffery Hall
Queens University
99 University Avenue
Kingston, Ontario, Canada, K7L 3N6
E-mail: akhtari@mast.queensu.ca

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

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

Received on 8.3.2008
and in revised form on 9.10.2008 (5420a)