ACTA ARITHMETICA
139.1 (2009)

On the Diophantine equation $X^2 - (2^{2m} + 1)Y^4 = -2^{2m}$

by

Michael Stoll (Bayreuth), P. G. Walsh (Ottawa) and
Pingzhi Yuan (Guangzhou)

1. Introduction. Two classical results of Wilhelm Ljunggren [6], [7] are the complete solution in positive integers of the two Diophantine equations

$$X^2 - 2Y^4 = -1, \quad X^2 - 5Y^4 = -4.$$

In particular, Ljunggren proved that apart from $(X, Y) = (1, 1)$, only the former equation has another positive integer solution, with the only such solution being $(X, Y) = (239, 13)$. The solution of the latter equation can be viewed as the major hurdle in determining that 1 and 144 are the only perfect squares in the Fibonacci sequence. We remark that since Ljunggren completely solved the Diophantine equation $X^2 - 2Y^4 = -1$, many other proofs have been given, most recently in [2].

The two Diophantine equations above can be regarded as the first two members of the family of quartic equations

$$X^2 - (2^{2m} + 1)Y^4 = -2^{2m}. \tag{1.1}$$

In a recent paper [4], the authors used a recent theorem of Akhtari to prove that (1.1) has at most 12 solutions in odd positive integers (X, Y). It is worth noting that $(X, Y) = (103, 5)$ is the only non-trivial solution in the case $m = 2$, and moreover, that for all $3 \le m \le 17$, a MAGMA computation shows that (1.1) has only the solution $(X, Y) = (1, 1)$ in odd positive integers X, Y. One would therefore expect that the bound of 12 is not sharp, but rather an artifact of the method used in [4]. Indeed, it is the goal of this paper to prove the following result for the family of equations in (1.1).

Theorem 1.1. *For all $m \ge 0$, the equation $X^2 - (2^{2m} + 1)Y^4 = -2^{2m}$ has at most three solutions in odd positive integers (X, Y).*

2000 *Mathematics Subject Classification*: 11D25, 11B39.
Key words and phrases: quartic equations, Lucas sequences, Diophantine approximations.

DOI: 10.4064/aa139-1-5

2. Preliminary results. We begin our analysis with the following useful observation.

LEMMA 2.1. *If $(X,Y)\neq(1,1)$ is a solution in positive integers to*

$$X^2-(2^{2m}+1)Y^4=-2^{2m},$$

then we have

$$\pm X\pm 2ai=(1+2ai)(s\pm ri)^4,\qquad Y=s^2+r^2,\ r>s>0.$$

Proof. All coprime integer solutions (x,y) to the quadratic equation

$$x^2-(2^{2m}+1)y^2=-2^{2m}$$

are given by

$$x+y\sqrt{1+2^{2m}}=\pm(\pm1+\sqrt{1+2^{2m}})(2^m+\sqrt{1+2^{2m}})^{2i} \tag{2.1}$$

for some integer i (see [5] or [4]).

For brevity, let $a=2^{m-1}$, and let $\alpha=T+U\sqrt{1+2^{2m}}=2^m+\sqrt{1+2^{2m}}$. For $i\geq 0$, define sequences $\{T_i\}$ and $\{U_i\}$ by

$$\alpha^i=T_i+U_i\sqrt{1+2^{2m}}.$$

Therefore, a solution in odd positive integers $(X,Y)\neq(1,1)$ to $X^2-(2^{2m}+1)Y^4=-2^{2m}$ is equivalent to a solution to

$$Y^2=T_{2k}\pm U_{2k},\qquad X=(4a^2+1)U_{2k}\pm T_{2k} \tag{2.2}$$

for some $k\geq 1$, since $(4a^2+1)U_{2k}>T_{2k}>U_{2k}$.

We first consider the case that the signs appearing in (2.2) are positive. By the well known identities $T_{2k}=T_k^2+(1+4a^2)U_k^2$ and $U_{2k}=2T_kU_k$, (2.2) shows that

$$Y^2=(T_k+U_k)^2+(2aU_k)^2,$$

and the terms involved in this equality are pairwise coprime since $a=2^{m-1}$, Y is odd and $\gcd(T_k,U_k)=1$. Thus, there are coprime non-negative integers r and s, of opposite parity, for which

$$Y=r^2+s^2,\qquad T_k+U_k=r^2-s^2,\qquad 2aU_k=2rs.$$

If r is even, then a divides r, and so by putting $R=r/a$, solving each of the expressions for T_k and U_k, substituting the result into $T_k^2-(1+4a^2)U_k^2=\pm1$, and then simplifying, we are led to the equation

$$(s^2+Rs-R^2a^2)^2-(1+4a^2)R^2s^2=\pm1,$$

or more simply

$$s^4+2s^3R-6a^2R^2s^2-2a^2R^3s+a^4R^4=\pm1.$$

This equation can be written as

$$(1+2ai)(s+ri)^4-(1-2ai)(s-ri)^4=\pm4ai,$$

where we have used the fact that $r = aR$. Let X_0 be the integer such that

$$2X_0 = (1 + 2ai)(s + ri)^4 + (1 - 2ai)(s - ri)^4;$$

then

$$\begin{aligned} X_0 &= s^4 - 8as^3r - 6s^2r^2 + 8asr^3 + r^4 \\ &= (T_k + U_k)^2 - 4a^2U_k^2 + 8a^2U_k(T_k + U_k) = X. \end{aligned}$$

We therefore deduce that

$$X \pm 2ai = (1 + 2ai)(s + ri)^4. \tag{2.3}$$

Now consider the case that s is even. Then a divides s, and so by putting $S = s/a$, solving each of the expressions for T_k and U_k, substituting the result into $T_k^2 - (1 + 4a^2)U_k^2 = \pm 1$, and then simplifying, we arrive at the equation

$$(r^2 - (Sr + S^2a^2))^2 - (1 + 4a^2)S^2r^2 = \pm 1,$$

or more simply

$$r^4 - 2r^3S - 6a^2S^2r^2 + 2a^2S^3r + a^4S^4 = \pm 1.$$

This equation can be rewritten as

$$(1 + 2ai)(r - si)^4 - (1 - 2ai)(r + si)^4 = \pm 4ai,$$

which upon multiplication by i^4 can be written as

$$(1 + 2ai)(s + ri)^4 - (1 - 2ai)(s - ri)^4 = \pm 4ai.$$

Therefore, we similarly have equation (2.3).

Next we consider the case that the signs appearing in (2.2) are negative. By the same argument as above, we have

$$(1 + 2ai)(s - ri)^4 - (1 - 2ai)(s + ri)^4 = \pm 4ai, \qquad Y = s^2 + r^2,\ s > r > 0.$$

Let X_0 be the integer such that

$$2X_0 = (1 + 2ai)(s - ri)^4 + (1 - 2ai)(s + ri)^4.$$

Similarly to the previous case, we have

$$\begin{aligned} X_0 &= s^4 + 8as^3r - 6s^2r^2 - 8asr^3 + r^4 \\ &= (T_k - U_k)^2 - 4a^2U_k^2 - 8a^2U_k(T_k - U_k) = -X, \end{aligned}$$

and therefore

$$-X \pm 2ai = (1 + 2ai)(s - ri)^4. \ \blacksquare$$

LEMMA 2.2. *Suppose that* (X_1, Y_1) *and* (X_2, Y_2) *are two solutions in odd positive integers to* $X^2 - (2^{2m}+1)Y^4 = -2^{2m}$, $Y_j = s_j^2 + r_j^2$, $s_j > r_j$ $(j = 1, 2)$ *and* $Y_2 > Y_1 > 1$. *Then* $Y_2 > 2Y_1^3$.

Proof. Suppose that (X_1, Y_1) and (X_2, Y_2) are two solutions in odd positive integers to equation (1.1), with $Y_j = s_j^2 + r_j^2$, $s_j > r_j$ $(j = 1, 2)$ and

$Y_2 > Y_1 > 1$. By the remarks in the Introduction, we may assume that $m > 17$, thus $Y_2^2 > Y_1^2 \geq T_2 - U_2 = 1 + 8a^2 - 4a > 2^{2m} \geq 2^{36}$. Then by Lemma 2.1 we have

$$\pm X_j \pm 2ai = (1+2ai)(s_j \pm r_j i)^4, \qquad j = 1,2.$$

We will assume that

$$X_1 \pm 2ai = (1+2ai)(s_1 + r_1 i)^4, \qquad X_2 \pm 2ai = (1+2ai)(s_2 + r_2 i)^4,$$

as the arguments for the other cases are identical. It follows that

$$(1+2ai)(s_j + r_j i)^4 - (1-2ai)(s_j - r_j i)^4 = \pm 4ai, \qquad j = 1,2. \tag{2.4}$$

Let

$$\omega = \frac{1-2ai}{1+2ai} = e^{i\theta}, \qquad \omega^{1/4} = e^{i\theta/4}.$$

By (2.4) we have

$$\left|\omega - \left(\frac{s_j + r_j i}{s_j - r_j i}\right)^4\right| = \frac{4a}{\sqrt{1+4a^2}\,Y_j^2} < \frac{1}{2^{35}}, \qquad j = 1,2. \tag{2.5}$$

Let $t_j \in \{0,1,2,3\}$ be the integer such that

$$\left|\omega^{1/4} - e^{t_j\pi i/2}\,\frac{s_j + r_j i}{s_j - r_j i}\right| = \min_{0\leq k\leq 3}\left|\omega^{1/4} - e^{k\pi i/2}\,\frac{s_j + r_j i}{s_j - r_j i}\right|, \qquad j = 1,2.$$

By (2.5) we may assume that

$$\left|\omega^{1/4} - e^{t_j\pi i/2}\,\frac{s_j + r_j i}{s_j - r_j i}\right| \leq \frac{1}{2^8}, \qquad j = 1,2.$$

Since

$$\begin{aligned}\left|\omega - \left(\frac{s_j + r_j i}{s_j - r_j i}\right)^4\right| &= \left|\omega^{1/4} - e^{t_j\pi i/2}\,\frac{s_j + r_j i}{s_j - r_j i}\right| \\ &\quad\times \left|\omega^{1/4} - e^{t_j\pi i/2}\,\frac{s_j + r_j i}{s_j - r_j i} + 2e^{t_j\pi i/2}\,\frac{s_j + r_j i}{s_j - r_j i}\right| \\ &\quad\times \left|\omega^{1/4} - e^{t_j\pi i/2}\,\frac{s_j + r_j i}{s_j - r_j i} + (1+i)e^{t_j\pi i/2}\,\frac{s_j + r_j i}{s_j - r_j i}\right| \\ &\quad\times \left|\omega^{1/4} - e^{t_j\pi i/2}\,\frac{s_j + r_j i}{s_j - r_j i} + (1-i)e^{t_j\pi i/2}\,\frac{s_j + r_j i}{s_j - r_j i}\right|,\end{aligned}$$

it follows that

$$\begin{aligned}\left|\omega - \left(\frac{s_j + r_j i}{s_j - r_j i}\right)^4\right| &\geq \left(2 - \frac{1}{2^8}\right)\left(\sqrt{2} - \frac{1}{2^8}\right)^2\left|\omega^{1/4} - e^{t_j\pi i/2}\,\frac{s_j + r_j i}{s_j - r_j i}\right| \\ &\geq 3.8\left|\omega^{1/4} - e^{t_j\pi i/2}\,\frac{s_j + r_j i}{s_j - r_j i}\right|, \qquad j = 1,2,\end{aligned}$$

and so

$$\left|\omega^{1/4} - e^{t_j\pi i/2}\,\frac{s_j + r_j i}{s_j - r_j i}\right| < \frac{1}{1.9Y_j^2}, \qquad j = 1, 2,$$

by (2.5). Now, by the inequality

$$\begin{aligned}\frac{1}{\sqrt{Y_1Y_2}} &\le \left|e^{t_1\pi i/2}\,\frac{s_1 + r_1 i}{s_1 - r_1 i} - e^{t_2\pi i/2}\,\frac{s_2 + r_2 i}{s_2 - r_2 i}\right| \\ &\le \left|\omega^{1/4} - e^{t_1\pi i/2}\,\frac{s_1 + r_1 i}{s_1 - r_1 i}\right| + \left|\omega^{1/4} - e^{t_2\pi i/2}\,\frac{s_2 + r_2 i}{s_2 - r_2 i}\right|,\end{aligned}$$

we derive

$$Y_2 > 2Y_1^3. \ \blacksquare$$

3. Proof of the main theorem. We now prove Theorem 1.1.

A MAGMA computation shows that the theorem holds for $0 \le m \le 17$, so we may assume that $m > 17$ in the following proof.

Suppose that (X_1, Y_1), (X_2, Y_2) and (X_3, Y_3) are solutions in odd positive integers to $X^2 - (2^{2m}+1)Y^4 = -2^{2m}$, with $Y_j = s_j^2 + r_j^2$, $s_j > r_j$ $(j = 1, 2, 3)$ and $Y_3 > Y_2 > Y_1 > 1$. Then by Lemma 2.1 we have

$$\pm X_j \pm 2ai = (1 + 2ai)(s_j \pm r_j i)^4, \qquad j = 1, 2, 3.$$

We will assume that

$$X_1 \pm 2ai = (1 + 2ai)(s_1 + r_1 i)^4, \qquad X_3 \pm 2ai = (1 + 2ai)(s_3 + r_3 i)^4,$$

as the arguments for the other cases are identical. It follows that

$$\begin{aligned}(1 + 2ai)(s_1 + r_1 i)^4 - (1 - 2ai)(s_1 - r_1 i)^4 &= \pm 4ai, \\ (1 + 2ai)(s_3 + r_3 i)^4 - (1 - 2ai)(s_3 - r_3 i)^4 &= \pm 4ai.\end{aligned}$$

Since $X_1 \pm 2ai = (1 + 2ai)(s_1 + r_1 i)^4$, we have

$$(X_1 \pm 2ai)(s_1 - r_1 i)^4(s_3 + r_3 i)^4 - (X_1 \mp 2ai)(s_1 + r_1 i)^4(s_3 - r_3 i)^4 = \pm Y_1^4 4ai.$$

Define x, y by

$$x + yi = (s_1 - r_1 i)(s_3 + r_3 i).$$

It follows that

$$|(X_1 \pm 2ai)(x + yi)^4 - (X_1 \mp 2ai)(x - yi)^4| = 4aY_1^4. \tag{3.1}$$

Now recall that $X_1 = (1+4a^2)U_{2k} \pm T_{2k}$, $k \ge 1$. Assuming that $k > 1$, we apply Corollary 2.3 of [8] to equation (3.1) with $A = 2X_1$, $B = a$, $N = aY_1^4$. Then, since $m > 17$,

$$\begin{aligned}A = 2X_1 &\ge 2(4a^2 + 1)U_4 - 2T_4 = 16a(4a^2 + 1)(8a^2 + 1) - 4(8a^2 + 1)^2 + 2 \\ &> 308(2a)^4 > 308B^4,\end{aligned}$$

the hypothesis of Corollary 2.3 of [8] is satisfied and we find that

$$x^2 + y^2 = Y_1 Y_3 \leq \max\left\{\frac{100X_1^2}{64a^2}, \frac{4a^2Y_1^8}{2X_1}\right\},$$

and the fact that $X_1^2 < (4a^2+1)Y_1^4$ shows that $Y_3 \leq 2a^2Y_1^7/X_1$. It follows from Lemma 2.2 that

$$16Y_1^9 \leq 2Y_2^3 \leq Y_3 \leq 2a^2Y_1^7/X_1,$$

which is impossible, and hence that $k = 1$.

If $k = 1$, then

$$Y_1^2 = T_2 \pm 4a = (2a)^2 + (2a \pm 1)^2.$$

Since $a = 2^{m-1}$, we get

$$Y_1 + 2a \pm 1 = 2a^2, \qquad Y_1 - (2a \pm 1) = 2.$$

It follows that $2a \pm 1 = a^2 - 1$, and so $a = 2$. In this case the equation $X^2 - 17Y^4 = -16$ has a non-trivial positive solution $(X, Y) = (103, 5)$. This completes the proof of Theorem 1.1. ∎

Final Remark. The method presented here is considerably different than that used in [4]. For the sake of the reader, we wish to explain that the approach for bounding the number of solutions to (1.1) taken up in [4] can be refined considerably. In particular, using the arguments contained in the proof of the main result in [1], it can be shown that there are at most four integer solutions (s, R) to the Thue equation

$$s^4 + 2s^3R - 6a^2s^2R^2 - 2a^2sR^3 + a^4R^4 = \pm 1 \qquad (a = 2^{m-1})$$

which arise from positive integer solutions (X, Y) to (2.2) satisfying $k > 16$. Furthermore, it is easily verified that an integer solution to $Y^2 = T_{2k} \pm U_{2k}$, with $2 \leq k \leq 16$, gives rise to an integer point $(2^m, Y)$ on a hyperelliptic curve $Y^2 = P_{2k}(x)$, where $P_{2k}(x)$ is a polynomial of degree $2k$. Using the methods described in [3], one can determine the set of rational points on these curves with x-coordinate being a power of 2, thereby proving that $Y^2 = T_{2k} \pm U_{2k}$ is in fact not solvable for $2 \leq k \leq 16$ (we note that the case $k = 1$ was dealt with in the preceding section). Therefore, this analysis allows one to assert that there are at most four positive integer solutions (X, Y) to equation (1.1) other than the solution $(1, 1)$ (that is, at most one solution for each of the four roots of the dehomogenized quartic). Furthermore, using an elementary modular argument, it can be shown that integer solutions (s, R) to the above Thue equation which arise from solutions to equation (1.1) have the property that s/R can be close to only three of the four roots of the dehomogenized quartic, which therefore implies a bound of four positive integer solutions to (1.1) in total, falling just short of the bound in Theorem 1.1.

Acknowledgments. We are grateful to Bo He for his valuable suggestion. The second author gratefully acknowledges support from the Natural Sciences and Engineering Research Council of Canada. The third author is supported by the Guangdong Provincial Natural Science Foundation (no. 8151027501000114) and NSF of China (no. 10571180).

References

[1] S. Akhtari, *The method of Thue and Siegel for binary quartic forms*, Acta Arith., to appear.

[2] M. A. Bennett, *Irrationality via the hypergeometric method*, in: Diophantine Analysis and Related Fields—DARF 2007/2008, AIP Conf. Proc. 976, Amer. Inst. Phys., Melville, NY, 2008, 7–18.

[3] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll and Sz. Tengely, *Integral points on hyperelliptic curves*, Algebra Number Theory 2 (2008), 859–885.

[4] B. He, A. Togbé and P. G. Walsh, *On the Diophantine equation* $x^2 - (2^{2m} + 1)y^4 = -2^{2m}$, Publ. Math. Debrecen, to appear.

[5] L. K. Hua, *Introduction to Number Theory*, Springer, Berlin, 1982.

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

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

[8] P. Z. Yuan, *On algebraic approximations of certain algebraic numbers*, J. Number Theory 102 (2003), 1–10.

Mathematisches Institut
Universität Bayreuth
95440 Bayreuth, Germany
E-mail: Michael.Stoll@uni-bayreuth.de

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

School of Mathematics
South China Normal University
Guangzhou, 510631, P.R. China

Received on 29.9.2008
and in revised form on 24.2.2009 (5810)