# An Improved Method for Solving the Family of Thue Equations $\mathbf{X^4 - 2rX^2Y^2 - sY^4 = 1}$

P. G. Walsh

## 1 Introduction

Since the groundbreaking work of Thue [13], the subject of solving those Diophantine equations of the form

$$F(X, Y) = m,$$

with $F \in Z[X, Y]$ a binary form of degree at least 3 and $m$ a nonzero integer, has received enormous interest, with many significant results. For a detailed history on this topic, the reader may wish to consult Halter-Koch et. al. [4], or Heuberger [5]. Under suitable hypotheses, such Diophantine equations have only finitely many solutions in integers $X$ and $Y$, and methods for determining all such solutions have been developed by Tzanakis and de Weger [14], Bilu-Hanrot [2], and others. Much of this research has centered around the problem of solving parametric families of Thue equations, as described in the work of E. Thomas [12]. We remark that in almost all examples solved in the literature, the coefficients are defined in terms of a single parameter.

At the 1988 NATO-ASI meeting in Banff, Stroeker [11] described a method to solve a class of quartic Thue equations given in the form

$$X^4 - 2rX^2Y^2 - sY^4 = 1. \tag{1.1}$$

If $r, s$ in (1.1) are such that $r^2 + s = t^2 d$, with $d > 0$, then Stroeker's method will work provided that $d \equiv 3 \pmod 4$, and also provided that certain other technical conditions hold during the course of his algorithm.

The purpose of the present paper is to provide a method to solve such equations using a combination of classical results of Ljunggren together with some recent refinements thereof. We will show how one can efficiently solve any equation of the type (1.1), thereby removing all of the special hypotheses required for Stroeker's method. Moreover, the method we describe can be used to deal not only with the more general equation

$$X^2 - 2rXY^2 - sY^4 = 1, \tag{1.2}$$

but also with

$$X^2 - rXY^2 - sY^4 = c \tag{1.3}$$

for $|c| \in \{1, 2, 4\}$. We will however restrict our attention to the former of these two equations. In the special case that $s = 1$ in (1.3), the complete solution in positive integers was determined in [17]. Thus the results of this paper also serve to improve on the results of [17].

We remark that in order to determine all solutions to (1.2) it is sufficient to determine all positive integer solutions $Y$, since the determination of corresponding values for $X$ then becomes a trivial task. By defining $Z = X - rY^2$ and $D = r^2 + s$, integer solutions $(X, Y)$ to (1.2) are in correspondence with integer solutions $(Z, Y)$ to

$$Z^2 - DY^4 = 1. \tag{1.4}$$

We will therefore focus our attention on the problem of determining all integer solutions to (1.4).

In what follows, let $r, s$ be the integers given in equation (1.2), and $D = r^2+s$. We will assume that $D$ is a nonsquare positive integer; otherwise solving equations (1.2) and (1.4) is trivial. Let $T_1 + U_1\sqrt{D}$ denote the minimal solution in positive integers to the Pell equation $X^2 - DY^2 = 1$. For $k \geq 1$ define

$$T_k + U_k\sqrt{D} = (T_1 + U_1\sqrt{D})^k.$$

**Theorem 1.** 1. *There are at most two positive integer solutions $(Z, Y)$ to equation (1.4). If two solutions $Y_1 < Y_2$ exist, then $Y_1^2 = U_1$ and $Y_2^2 = U_2$, except only if $D = 1785$ or $D = 16 \cdot 1785$, in which case $Y_1^2 = U_1$ and $Y_2^2 = U_4$.*

2. *If only one positive integer solution $(Z, Y)$ to equation (1.4) exists, 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 $p \equiv 3 \pmod 4$.*

Theorem 1 evidently provides an efficient algorithm for solving equation (1.4). Using the continued fraction expansion of $\sqrt{D} = \sqrt{r^2 + s}$, one can compute $T_1 + U_1\sqrt{D}$. Upon factoring $U_1$ in the form $U_1 = lv^2$, with $l$ squarefree, one only needs to determine if any of $U_1, U_2, U_4, U_l$ are squares. The shortcoming of this result is that evidence, such as an effective form of the abc conjecture, indicates that $U_k$ cannot be a square if $k > 4$. The reader is referred to [15] for more details concerning this connection.

**Conjecture 1.** *If $D$ is a nonsquare positive integer, $\epsilon_D = T + U\sqrt{D}$ the minimal solution to $X^2 - DY^2 = 1$, and $\epsilon_D^k = T_k + U_k\sqrt{D}$ for $k \geq 1$, then the equation*

$$U_k = y^2$$

*implies that $k \leq 4$.*

To be more precise, there are infinitely many values $D$ for which $U_1$ (respectively $U_2$) is a square, namely $D = m^2 - 1$ (respectively $D = 4m^4 - 1$). Similarly, there are infinitely many values of $D$ for which $U_3$ is a square. For $k \geq 1$, put $t_k + u_k\sqrt{3} = (2 + \sqrt{3})^k$. Then for each $D_i = ((t_{4i+1}/2)^2 - 1)/9$, $i \geq 1$, it is easy to verify that the corresponding value $U_3$ is a square. Lastly, by the first part of Theorem 1, it is easy to prove that $U_4$ is a square only for $D = 1785$ and $D = 16 \cdot 1785$.

If Conjecture 1 were known to be true, it would facilitate the complete solution of equations (1.1), (1.2) and (1.4) considerably, since one would only need to verify if any of the numbers $U_i$, $1 \leq i \leq 4$, is a square. We will provide an example at the end of the paper illustrating this.

## 2 Preliminary Results

In this section we will collect those results which will be needed in the course of proving Theorem 1. It is worth noting that Ljunggren [6] proved a result which is close to Theorem 1, but does not deal with the case that only one solution to (1.4) exists. We therefore provide a somewhat different proof that is also based on Ljunggren's work, but in addition uses recent results of our own.

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

$$\epsilon_d = \tau^2,$$

*where*

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

*$c \in \{1, 2\}$, $d = mn$, $m$ is not a square, and $a^2m - b^2n = c$.*

*Proof.* This is well known; see, for example, Nagell [10]. □

**Lemma 2.** *Let $d > 1$ denote a nonsquare positive integer, $\epsilon_d = T + U\sqrt{d}$ be the minimal solution to $X^2 - dY^2 = 1$, and $T_k + U_k\sqrt{d} = \epsilon_d^k$ for $k \geq 1$. If $T_k = x^2$ for some integer $x$, then either $k = 1$ or $k = 2$.*

*Proof.* This is a recent result of Cohn [3], which improves on previous work of Ljunggren. For a detailed account of the entire proof, the reader is referred to the first section of [18]. □

Let $\{T_k\}$ and $\{U_k\}$ be as above. For a positive integer $b$ we define the rank of apparition of $b$ in $\{T_k\}$ (resp. $\{U_k\}$) to be the minimal index $k$ such

that $b$ divides some term $T_k$ (resp. $\{U_k\}$), provided such an index exists, and denote it by $\beta(b)$ (resp. $\alpha(b)$). It is well known that $\alpha(b)$ exists for all positive integers $b$, but $\beta(b)$ may or may not exist.

**Lemma 3.** *Let $d > 1$ denote a nonsquare positive integer, and $b > 1$ a squarefree integer.*

1. *If $T_k = bx^2$ for some integer $x$, then $k = \alpha(b)$. In particular, if $T_k = 2x^2$ for some integer $x$, then $k = 1$.*

2. *If $U_k = bx^2$ and $\alpha(b)$ is even, then $k = \alpha(b)$, except only in the case that $2T_1^2 - 1 = v^2$ for some integer $v$ and $T_1U_1 = bu^2$ for some integer $u$, in which case $U_4 = U_{2\alpha(b)} = b(2uv)^2$.*

*Proof.* For part 1, see [1], Theorem 1 and Corollary 1, while for part 2 see [16]. □

**Lemma 4.** *Let $m$ and $n$ be positive integers, $m$ not a square, such that*

$$mX^2 - nY^2 = 1 \tag{2.1}$$

*is solvable in integers, and let $\tau = \tau_{m,n} = A\sqrt{m} + B\sqrt{n}$ denote its minimal solution with $A$ and $B$ positive integers. Then all positive integer solutions to (2.1) are given by*

$$\tau^{2k+1} = A_{2k+1}\sqrt{m} + B_{2k+1}\sqrt{n}. \quad (k \geq 0)$$

*Assume that $B = lv^2$ with $l$ squarefree, and suppose that $(x, y)$ is a solution to*

$$mX^2 - nY^4 = 1. \tag{2.2}$$

*Then $l$ is odd and $y^2 = B_l$.*

*Proof.* This is a theorem of Ljunggren [8]. The reader may wish to consult [18] for a detailed account of the proof and related problems. □

**Lemma 5.** *Let $m$ and $n$ be positive integers, $m$ not a square, such that*

$$mX^2 - nY^2 = 2 \tag{2.3}$$

*is solvable in odd integers $X$ and $Y$. Let $\tau_{m,n} = \frac{A\sqrt{m}+B\sqrt{n}}{\sqrt{2}}$ denote its minimal solution with $A$ and $B$ odd positive integers. (There is no ambiguity in using the notation $\tau_{m,n}$ once again, since at most one of equations (2.1) and (2.3) are solvable in integers.) Then all positive integer solutions to (2.3) are given by*

$$\tau^{2k+1} = \frac{A_{2k+1}\sqrt{m} + B_{2k+1}\sqrt{n}}{\sqrt{2}} \quad (k \geq 0).$$

*If* $(x, y)$ *is a solution to*

$$mX^2 - nY^4 = 2, \tag{2.4}$$

*then either* $y^2 = B_1$ *or* $y^2 = B_3$.

*Proof.* This has recently been proved [9], improving upon previous work of Ljunggren. □

**Lemma 6.** *Let* $m$ *and* $n$ *be positive integers,* $m$ *not a square, such that*

$$mX^2 - nY^2 = 1 \tag{5}$$

*is solvable in integers, and let* $\tau_{m,n} = A\sqrt{m} + B\sqrt{n}$ *denote its minimal solution. If*

$$mX^4 - nY^2 = 1 \tag{2.5}$$

*has a solution* $(x, y)$*, then* $x^2 = A_{2k+1}$ *for some* $k$*, where* $A_{2k+1}$ *is defined in Lemma 4, and either* $2k + 1 = 1$ *or* $2k + 1$ *is a prime* $p \equiv 3 \pmod 4$*. Furthermore, if* $A_{2k+1}$ *is a square for some index* $2k + 1$*, then* $A_1$ *is also a square.*

*Proof.* The reader is referred to [18] for the details of this. □

## 3 Proof of Theorem 1

Let $k$ denote an index with the property that $U_k = y^2$ for some integer $y$. If $k$ is even, $k = 2r$, then $y^2 = U_k = U_{2r} = 2T_rU_r$, from which it follows that $T_r$ is either a square or twice a square. By Lemma 2 and Lemma 3, we see that $r = 1$ or $r = 2$, and hence $k = 2$ or $k = 4$.

Let $D = w^2d$ with $d$ squarefree. Let $\epsilon_d = t + u\sqrt{d}$ denote the minimal solution to $X^2 - dY^2 = 1$, and define $r_D$ to be the positive integer for which $\epsilon_d^{r_D} = \epsilon_D$, i.e., $r_D = \log(\epsilon_D)/\log(\epsilon_d)$.

Assume first that $r_D$ is even. Let $t_k + u_k\sqrt{d} = (\epsilon_d)^k$. Then $U_k = y^2$ for some integer $y$ if and only if $u_{2k_1} = wz^2$ for some integer $z$, where $2k_1 = kr_D$. If $w$ divides $u_{k_1}$, then $t_{k_1}$ is a square, and Lemma 2 implies that $k_1 = 1$ or $k_1 = 2$. It follows that $k \in \{1, 2, 4\}$. If $w$ does not divides $u_{k_1}$, then the rank of apparition $\alpha^*(w)$ of $w$ in the sequence $\{u_k\}$ is even, and so by Lemma 3, either $2k_1 = 4$ or $2k_1 = \alpha^*(w)$. Since $2k_1 = kr_D$ and since $\alpha^*(w)$ clearly divides $r_D$, we see that $k \in \{1, 2, 4\}$.

We henceforth assume that both $k$ and $r_D$ are odd positive integers. In this case we can assume that $U_1$ is properly divisible by 2 to an even power, otherwise the binomial theorem shows that $U_k$ is properly divisible by 2 to

an odd power for all odd positive integers $k$. Appealing to Lemma 1, we see that $\epsilon_D = \tau^2$ with

$$\tau = \frac{A_1\sqrt{m} + B_1\sqrt{n}}{\sqrt{c}}, \quad c \in \{1, 2\},$$

$m$ a nonsquare positive integer, $A_1^2 m - B_1^2 n = c$, $D = 4^{2-c}mn$, $U_k = A_k B_k$, and $\gcd(A_k, B_k) = 1$ for all odd $k \geq 1$, where

$$\tau^k = \frac{A_k\sqrt{m} + B_k\sqrt{n}}{\sqrt{c}}.$$

Therefore, $U_k$ is a square precisely when both $A_k$ and $B_k$ are squares.

We will consider the cases $c = 1$ and $c = 2$ separately. Suppose first that $c = 1$. By Lemma 4, $B_k$ can only be a square when $k = l$, where $B_1 = lv^2$ for some squarefree positive integer $l$ and some integer $v$. By Lemma 6, if $A_k$ is a square, then so is $A_1$, and $k = 1$ or $k$ is a prime $p \equiv 3 \pmod 4$. Combining these two results shows that either $U_1 = W^2$ for some integer $W$ and $k = 1$, or $U_1 = A_1 B_1 = pW^2$ and $k = p$.

Now assume that $c = 2$. If $U_k$ is a square, then by the same reasoning as in the previous case, $A_k$ and $B_k$ must both be squares, and so Lemma 5 shows that $k = 1$ or $k = 3$. Since $A_3 = A_1(2A_1^2 - 3)$ is not a square for any value $A_1$, it follows that $k = 1$. This completes the proof of Theorem 1.

## 4 Remarks and Examples

**Example 1.** We consider the particular equation

$$X^4 + 2X^2Y^2 - 2Y^4 = 1. \tag{4.1}$$

This example was given in Stroeker's paper [11], and it was shown how the method described therein failed to produce all integer solutions.

Theorem 1 enables one to solve the more general equation

$$X^2 + 2XY^2 - 2Y^4 = 1. \tag{4.2}$$

In this case, $r = -1$, $s = 2$, $D = r^2 + s = 3$, $\epsilon_D = 2 + \sqrt{3}$, $U_1 = 1$, and so by Theorem 1, the only squares in the sequence $\{U_k\}$ are $U_1 = 1$ and $U_2 = 4$. Therefore, the only positive integer solutions $(X, Y)$ to (4.2) are $\{(1, 1), (3, 2)\}$, and hence the only positive integer solution $(X, Y)$ to (4.1) is $(1, 1)$.

**Example 2.** In this example, consider the quartic equation

$$X^2 - 2rXY^2 - sY^4 = 1, \tag{4.3}$$

where $r$ and $s$ are given as follows:

$$\begin{aligned} r = {} & 1234567891234567891234567891234567891234567891234567891234\,5 \\ & 6789123456789, \end{aligned}$$

$$\begin{aligned} s = {} & 226364439697770315346017004215449407873445137414432750451\,63 \\ & 961235604590451720979334022333056517936923044697680126977\,40 \\ & 012646548831702413162052015877384603746945155378663387516\,97 \\ & 477219305704696429548442806063514005754512764126174140864\,33 \\ & 749638985420889577434826612195426461522620385458986857176\,49 \\ & 6872025208937040867050307711852129127083491812432666057\,67. \end{aligned}$$

In this case, the discriminant $D = r^2 + s$ is given by

$$\begin{aligned} D = {} & 2263644396977703153460170042154494078734451374144327504516 \\ & 3961235604590451720979334022333056517936923044697680126977 \\ & 4001264654883170241316205201587738460374694515537866338751 \\ & 6974772193057046964295484428060635155299123908314940287514 \\ & 4216865017766190589355858847388273768235255283156541139050 \\ & 6043280677987191351600562507725800549396742886480386401679 \\ & 6288. \end{aligned}$$

The minimal solution $\epsilon_D = T + U\sqrt{D}$ of $X^2 - DY^2 = 1$ has

$$\begin{aligned} T = {} & 2216324016290861089596684730856465101474477829908452902263 \\ & 2132451800826406112717500206747625422118049303216056909611 \\ & 7159149515792961916027607349248013349199331751316985850160 \\ & 6089926157583645638589834884012635329337923888554974335871 \\ & 1605366605878985823520757981991050666551741832903191640251 \\ & 650115098381039406508535596283881794337783\,67 \end{aligned}$$

and

$$\begin{aligned} U = {} & 4658318199794601635610324114917852765980845781453402566063\,4 \\ & 6403168960639474901657613600005639439673397383294328998705\,7 \\ & 876940998121733559776547199715239540709\,9. \end{aligned}$$

In order to completely solve (4.3) using Theorem 1, we need to determine first if any of $U_1, U_2$ or $U_4$ are squares, and a simple calculation on Maple shows that they are not. Next, we need to write $U$ in the form $U = lv^2$ for

some squarefree integer $l$, and check whether $U_l$ is a square. Unfortunately, the problem of writing $U$ in the prescribed form is polynomially equivalent to the problem of factoring $U$, which is (currently) a difficult computational problem. We leave it as a challenge for the reader to determine if (4.3) has any integer solutions with $Y \neq 0$.

## 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] Y. Bilu and G. Hanrot, *Solving Thue equations of high degree*, J. Number Theory **60** (1996), 373–392.

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

[4] F. Halter-Koch, G. Lettl, A. Pethö, and R. F. Tichy, *Thue equations associated with Ankeny-Brauer-Chowla number fields*, J. London Math. Soc. **60** (1999), 1–20.

[5] C. Heuberger, *On a conjecture of E. Thomas concerning parametrized Thue equations*, Acta Arith. **98** (2001), 375–394.

[6] W. Ljunggren, *Einige Eigenschaften der Einheiten reeller quadratischer und rein biquadratischer Zahl-Körper usw.*, Oslo Vid.-Akad. Skrifter (1936).

[7] ———, *Über die Gleichung* $x^4 - Dy^2 = 1$, Arch. Math. Naturv. **45** (1942), No. 5.

[8] ———, *Ein Satz über die Diophantische Gleichung* $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$, Tolfte Skand. Matemheikerkongressen, Lund, 1954, pp. 188–194.

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

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

[11] R. J. Stroeker, *On the Diophantine equations of type* $x^4 - 2ax^2y^2 - by^4 = 1$, Number Theory and Applications (R. A. Mollin, ed.), NATO-ASI Series C, vol. 265, Kluwer Publishers, Boston, 1989, pp. 547–554.

[12] E. Thomas, *Complete solutions to a family of cubic Diophantine equations*, J. Number Theory **34** (1990), 235–250.

[13] A. Thue, *Ein Fundamentaltheorem zur Bestimmung von Annäherungswerten aller Wurzeln gewisser ganzer Funktionen*, J. Reine Angew. Math. **138** (1910), 96–108.

[14] N. Tzanakis and B. M. de Weger, *On the practical solution of the Thue equation*, J. Number Theory **31** (1989), 99–132.

[15] P. G. Walsh, *A note on Ljunggren's theorem about the Diophantine equation* $aX^2 - bY^4 = 1$, C. R. Math. Acad. Sci. Soc. R. Canada **20** (1998), 113–119.

[16] ———, *The Diophantine equation* $X^2 - db^2Y^4 = 1$, Acta Arith. **57** (1999), 179–188.

[17] ———, *A note on a theorem of Ljunggren and the Diophantine equations* $x^2 - kxy^2 + y^4 = 1, 4$, Arch. Math. **72** (1999), 1–7.

[18] ———, *Diophantine equations of the form* $aX^4 - bY^2 = \pm 1$, Proceedings of the International Conference held in Graz, August 30 to September 5, 1998 (F. Halter-Koch and R. F. Tichy, eds.), Walter de Gruyter, 2000, pp. 531–554.