Journal of Integer Sequences, Vol. 18 (2015),
Article 15.4.4

Integer Solutions of the Equation $y^2 = Ax^4 + B$

Paraskevas K. Alvanos
1st Model and Experimental High School of Thessaloniki
Kleanthous 30
54453 Thessaloniki
Greece
alvanos@sch.gr

Konstantinos A. Draziotis
Department of Informatics
Aristotle University of Thessaloniki
54124 Thessaloniki
Greece
drazioti@csd.auth.gr

Abstract

Let $A \in \{k^2(k^2l^2+1), 4k^2(k^2(2l-1)^2+1)\}$, where k and l are positive integers, and let B be a non-zero square-free integer such that $|B| < \sqrt{A}$. In this paper we determine all the possible integer solutions of the equation $y^2 = Ax^4 + B$ by using terms of Lucas sequences of the form mx^2.

1 Introduction and statement of results

Diophantine equations of the form $Dy^2 = Ax^4 + B$ have been widely studied with a variety of methods. A number of innovative ideas have been developed in order to study such equations. For instance, Ljunggren [13, 14, 15], by studying units in quadratic and biquadratic fields, showed that the equation $x^2 - dy^4 = \pm 1$ has at most two solutions. Some equations of the previous form are given in Table 1.

Equation	Ref.	Equation	Ref.
$x^4 \pm 1 = (4r^2+1)y^2$	[10]	$y^2 - dx^4 = 1$	[8, 22]
$x^4 - 1 = dy^2$	[9]	$y^2 - dx^4 = -1$	[6]
$x^4 + 1 = dy^2$	[7]	$(m^2+m+1)x^4 - (m^2+m)y^2 = 1$	[25]
$ty^2 = (t+2)x^4 - 2$	[1]	$x^4 - dy^2 = 1$, d prime	[17]
$b^2x^4 - 1 = dy^2$	[2]	$x^4 - dy^2 = 1$, d prime or twice a prime	[18]

Table 1: Quartic equations of the form $\alpha X^2 + \beta Y^4 = \pm 1$.

Moreover, Tzanakis [23, 24] introduced a method for solving quartic elliptic equations by generalizing the elliptic logarithm method. Another method to treat equations of this type is to apply a reduction to the study of the squares of some binary linear recurrent sequence or to a family of Thue equations. In that case, either the Baker or the Thue-Siegel method is used. Also, there are elementary approaches, such as manipulations with Legendre symbol and reduction mod p. Note that in all the previous equations the constant term is very small (it belongs to the set $\{\pm 1, \pm 2\}$). In this paper we allow $|B|$ to be smaller than $\sqrt{A}$.

We shall determine all possible solutions of a large family of equations of the form

$$y^2 = Ax^4 + B, \tag{1}$$

where $A \in \{k^2(k^2l^2+1), 4k^2(k^2(2l-1)^2+1)\}$ $(k, l \in \mathbb{Z}_{>0})$ and $|B|$ is a non-zero square-free integer smaller than $\sqrt{A}$. In particular, for the cases where $k \in \{1, 2, 3, 6\}$, we give the set of possible solutions without any hard computation. For the rest of the cases the computation of a minimal unit in the ring of integers of a quadratic extension of $\mathbb{Q}$ is needed. The idea is that in order to compute the solutions of equation (1) we need to study the squares that occur to the denominators of the continued fraction of $\sqrt{A}$. Furthermore, A is chosen with period 1 or 2. The case with period 1 (part 1(a) of Theorem 1) is very easy and was already covered by the general result of Togbe et al. [22]. The case with period 2 gives two families of quartic elliptic curves. We provide the exact solutions for all possible square-free B's with $|B| < \sqrt{A}$.

One can also apply well known methods (e.g., reducing to finite number of Thue equations) in order to solve the equations $y^2 = Ax^4 + B$ for all the possible B's but one, one by one. In addition, we have the Magma [4] function, `SIntegralLjunggrenPoints([1,A,0,B], [])`, which returns the integer solutions of (1), but this function makes sense if we let A, B run in some (relatively) small intervals (the function uses linear forms of logarithms).

By K we denote the quadratic number field $\mathbb{Q}(\sqrt{A})$. Furthermore, let $\mathbb{O}_K$ be the ring of integers of K, $\varepsilon_d = y_1 + x_1\sqrt{d} \in \mathbb{Z}[\sqrt{A}]$ is the minimal unit > 1, with norm 1 and $\varepsilon_d^t = y_t + x_t\sqrt{d}$. The main theorem that we prove is the following.

Theorem 1. *Let k, l be positive integers, and (x, y) an integer solution of*

$$y^2 = Ax^4 + B,$$

where $0 \neq |B| < \sqrt{A}$ *and* B *is square-free.*

1. *Let* $A = k^2(k^2l^2+1)$.

   (a) *If* $k=1$, *then* $|x| \in \{0, 1, 13, \sqrt{2l}\}$. *Furthermore,* $|x| = 13$ *occurs only if* $A = 2, B = -1$.

   (b) *If* $k \in \{2, 3, 6\}$, *then* $|x| \in \{0, 1, 6, 68, \sqrt{2l}\}$. *Furthermore,* $|x| = 6$ *occurs only if* $A = 20, B = 1$ *and* $|x| = 68$ *occurs only if* $A = 1305, B = 1$.

   (c) *If* $k \in \mathbb{N} - \{1, 2, 3, 6\}$ *then* $|x| \in \{0, 1, \sqrt{2l}, \sqrt{x_1}, \sqrt{x_2}, \sqrt{x_p}\}$ *where* $y_1 + x_1\sqrt{A} > 1$ *is the minimal unit of* $\mathbb{O}_K$ *of norm* 1 *and* p *is prime* $\equiv 3 \pmod 4$ *such that* $x_1 = pu^2$ *for some integer* u.

2. *Let* $A = 4k^2(k^2(2l-1)^2+1)$.

   (a) *If* $k \in \{1, 3\}$, *then* $|x| \in \{0, 1, \sqrt{2l-1}\}$.

   (b) *If* $k \in \mathbb{N} - \{1, 3\}$ *then* $|x| \in \{0, 1, \sqrt{2l-1}, \sqrt{x_1}, \sqrt{x_2}, \sqrt{x_p}\}$ *where* $y_1 + x_1\sqrt{A/4} > 1$ *is the minimal unit of* $\mathbb{O}_K$ *of norm* 1 *and* p *is prime* $\equiv 3 \pmod 4$ *such that* $x_1 = pu^2$ *for some integer* u.

The previous result uses the following proposition.

Proposition 2. *Let* B *be non-zero square-free integer, and let* A *be a non-square positive integer. Assume that* $|B| < \sqrt{A}$. *Let* $(x, y) \in \mathbb{Z}^2$, *such that* $y^2 = Ax^{2m} + B$. *Then* $x^m = q_n$, *for some positive integer* n, *where* p_n/q_n *is the* n*-th convergent of* $\sqrt{A}$.

We shall prove the following proposition.

Proposition 3. 1. *Let* (x, y) *be an integer solution to equation*

$$y^2 = k^2(k^2l^2+1)x^4 + B,$$

with B *square-free,* $k > 1$, *and* $0 \neq |B| \leq k^2l$. *Then* $B = 1$.

2. *Let* (x, y) *be an integer solution to equation* $y^2 = (l^2+1)x^4 + B$, *with* B *square-free, and* $0 \neq |B| \leq l$. *Then* $|B| = 1$.

3. *Let* $A = 4k^2(k^2(2l-1)^2+1)$. *Then the equation* $y^2 = Ax^4 + B$, *with* B *square-free,* $k > 3$, *and* $0 \neq |B| \leq 2k^2(2l-1)$ *has integers solutions only for* $B = 1$.

Another way to write Proposition 3 is as follows:

1. For $A = k^2(k^2l^2+1)$, if y^2, Ax^4 are not consecutive integers and their difference is square free, then $|y^2 - Ax^4| > \sqrt{A}$.

2. For $A = 4k^2(k^2(2l-1)^2+1)$ $(k > 3)$, if y^2, Ax^4 are not consecutive integers and the difference is square free, then $|y^2 - Ax^4| > \sqrt{A}$.

The previous proposition is not true for any value of A. For instance, the equation $y^2 = 6x^4 - 2$ has the solutions $|x| \in \{1, 3\}$.

The paper is organized as follows: in Section 2 we give some auxiliary results, in Section 3 we obtain the proof of Proposition 2 and in Section 4 the proof of the theorem. In Section 5 we provide the proof of Proposition 3, and finally in Section 6 we provide some examples.

2 Auxiliary results

We denote by $u_n(r, s)$ the *Lucas sequence*

$$u_0 = 0,\ u_1 = 1,\ u_{n+2} = ru_{n+1} + su_n,$$

and by $v_n(r, s)$ the *companion Lucas sequence*

$$v_0 = 2,\ v_1 = r,\ v_{n+2} = rv_{n+1} + sv_n,$$

where r, s are non-zero integers and $n \geq 0$. A well-known and useful identity containing both of the above sequences is

$$v_n^2 - (r^2 + 4s)u_n^2 = 4(-s)^n. \tag{2}$$

Lemma 4. *The even-indexed terms of the form kx^2 of a Lucas sequence are solutions of the equation*

$$y^2 - dx^4 = 1, \tag{3}$$

where

1. $d = k^2(k^2l^2 + 1)$*, if the Lucas sequence is* $\big(u_n(2kl, 1)\big)_{n\geq 0}$.
2. $d = k^2(k^2(2l - 1)^2 + 1)$*, if the Lucas sequence is* $\big(u_n(2k(2l - 1), 1)\big)_{n\geq 0}$.

Proof. Starting with equation (2) and by substituting r with $2kl$ and s with 1 we get

$$v_n^2 - (4k^2l^2 + 4)u_n^2 = 4.$$

Obviously v_n is even and therefore we can substitute v_n by $2y$. Moreover, we are interested in terms u_n of the form kx^2, so by substituting u_n by kx^2 we get $y^2 - k^2(k^2l^2 + 1)x^4 = 1$. The proof of part (2) is similar and it is omitted. $\square$

Lemma 5. *For $d \in \{k^2(k^2l^2 + 1), k^2(k^2(2l - 1)^2 + 1)\}$ the equation $y^2 - dx^4 = 1$ has at most two solutions such that $y + x^2\sqrt{d} \in \{\varepsilon_d, \varepsilon_d^2, \varepsilon_d^p\}$. Where, $\varepsilon_d = y_1 + x_1\sqrt{d}$ is the minimal unit greater than 1 of norm 1 in $\mathbb{Z}[\sqrt{d}]$ and p is a prime $\equiv 3 \pmod 4$ such that $x_1 = pu^2$, for some $u \in \mathbb{Z}$.*

Proof. If we have exactly two solutions of $y^2 - dx^4 = 1$ then we get $y + x^2\sqrt{d} \in \{\varepsilon_d, \varepsilon_d^2\}$ except if $d = 1785$ or $16 \cdot 1785$ [22, Thm. 1.1]. In that case we have $y + x^2\sqrt{d} \in \{\varepsilon_d, \varepsilon_d^4\}$. If we have exactly one solution, we get $y + x^2\sqrt{d} \in \{\varepsilon_d, \varepsilon_d^2, \varepsilon_d^p\}$, where p is prime such that $x_1 = pu^2$ for some $u \in \mathbb{Z}$, and $p \equiv 3 \pmod 4$. Since d cannot be equal to 1785 or $16 \cdot 1785$, the result follows. □

Lemma 6. *Let $r \geq 1$, $n \geq 4$, and let $m \in \{1, 2, 3, 6\}$. Assume that for some integer x we get $u_n(r, 1) = mx^2$. Then $(n, r, m) = (4, 1, 3)$, $(4, 2, 3)$, $(4, 4, 2)$, $(4, 24, 3)$, $(6, 1, 2)$, $(7, 2, 1)$ or $(12, 1, 1)$.*

Proof. [16, Thm. 1]. □

Lemma 7. *The doubling rate of the recurrence sequence $u_{n+2} = ru_{n+1} + su_n$ is*

$$u_{n+4} = (r^2 + 2s)u_{n+2} - s^2 u_n.$$

Proof. By definition, we have that $u_{n+4} = ru_{n+3} + su_{n+2}$. By substituting u_{n+3} with $ru_{n+2} + su_{n+1}$ we get

$$u_{n+4} = r^2 u_{n+2} + sru_{n+1} + su_{n+2}.$$

Notice that $ru_{n+1} = u_{n+2} - su_n$. So,

$$u_{n+4} = r^2 u_{n+2} + s(u_{n+2} - su_n) + su_{n+2}.$$

The result follows. □

Lemma 8. *Let $k, l \in \mathbb{Z}_{>0}$. The continued fraction of $\sqrt{A}$ is equal to:*

1. $[k^2 l; \overline{2l, 2k^2 l}]$ *for* $A = k^2(k^2 l^2 + 1)$ *and* $k \neq 1$.
2. $[4k^2 l - 2k^2; \overline{2l - 1, 8k^2 l - 4k^2}]$ *for* $A = 4k^2(k^2(2l-1)^2 + 1)$.
3. $[l; \overline{2l}]$ *for* $A = l^2 + 1$.

Proof. Let $[k^2 l; \overline{2l, 2k^2 l}]$ be the continued fraction of $\sqrt{A}$. Then

$$\sqrt{A} = k^2 l + \cfrac{1}{2l + \cfrac{1}{2k^2 l + \cfrac{1}{2l + \cdots}}}.$$

So the quantity $\sqrt{A} - k^2 l$ is a periodic fraction and by substituting it, in the initial fraction we get

$$\sqrt{A} - k^2 l = \cfrac{1}{2l + \cfrac{1}{2k^2 l + (\sqrt{A} - k^2 l)}}.$$

The result follows from the above equation.

The proof of part (2) is similar and it is omitted. The continued fraction in part (3) is a specific case of the first continued fraction for $k = 1$. The only difference is that in this case the period of the continued fraction is 1. Following the same procedure as in the first proof it turns out that the result follows from the equation

$$\sqrt{A} - l = \frac{1}{2l + (\sqrt{A} - l)}.$$

$\square$

Let θ be a quadratic irrational number and $[a_0, a_1, a_2, \ldots]$ its simple continued fraction. We denote by (p_n) the sequence of the numerators, and by (q_n) the sequence of the denominators of the convergents to θ. By the theory of the continued fractions we have that

$$\frac{p_n}{q_n} = [a_0, a_1, \ldots, a_n],$$

while $\gcd(p_n, q_n) = 1$. The convergents p_n and q_n can be computed from the recurrence relations

$$p_{-2} = 0,\ p_{-1} = 1,\ p_n = a_n p_{n-1} + p_{n-2},\ n \geq 0,$$

$$q_{-2} = 1,\ q_{-1} = 0,\ q_n = a_n q_{n-1} + q_{n-2},\ n \geq 0 \tag{4}$$

The continued fraction of a quadratic irrational θ has the form

$$[a_0; \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0}],$$

where the central term might appear either once or twice, see Burger [5, Lemma 8.6, p. 51].

Proposition 9. *Let θ be a quadratic irrational number, and let $[a_0; \overline{a_1, a_2, \ldots, a_s}]$ be its simple continued fraction with period s. Then the terms of the sequence (q_n) satisfy the linear recurrence*

$$q_{n+2s} - t q_{n+s} + (-1)^s q_n = 0,\ n \geq 1$$

where t is the trace of the matrix

$$M = \prod_{1 \leq j \leq s} \begin{bmatrix} a_j & 1 \\ 1 & 0 \end{bmatrix}.$$

Proof. [12, Thm. 1]. $\square$

Lemma 10. *Let (q_n) be the sequence of the denominators of the convergents to $\sqrt{A}$.*

1. *Let $\sqrt{A} = [k^2 l; \overline{2l, 2k^2 l}]$. Then*

$$q_n = \begin{cases} u_{n+1}, & n \text{ even;} \\ \frac{u_{n+1}}{k}, & n \text{ odd.} \end{cases}$$

Where u_n are the terms of the Lucas sequence $u_n(2kl, 1)$.

2. *Let* $\sqrt{A} = [4k^2l - 2k^2; \overline{2l-1, 8k^2l - 4k^2}]$. *Then*

$$q_n = \begin{cases} u_{n+1}, & n \text{ even;} \\ \frac{u_{n+1}}{2k}, & n \text{ odd.} \end{cases}$$

Where u_n *are the terms of the Lucas sequence* $u_n(2k(2l-1), 1)$.

3. *Let* $\sqrt{A} = [l; \overline{2l}]$. *Then* $q_n = u_{n+1}$*, where* u_n *are the terms of the Lucas sequence* $u_n(2l, 1)$.

Proof. From relation (4) we get $q_0 = 1,\ q_1 = 2l,\ q_2 = 4k^2l^2 + 1$. According to Proposition 9 the denominators $(q_n)_{n\geq 0}$ of the convergents to $\sqrt{A}$ satisfy the recurrence sequence

$$q_{n+2s} - tq_{n+s} + (-1)^s q_n = 0,\ n \geq 1,$$

where $s = 2$, and

$$t = trace\left(\begin{bmatrix} 2l & 1 \\ 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} 2k^2l & 1 \\ 1 & 0 \end{bmatrix} \right) = 4k^2l^2 + 2.$$

Thus, we get

$$q_{n+4} = (4k^2l^2 + 2)q_{n+2} - q_n = 0,\ n \geq 1. \tag{5}$$

On the other hand, the first terms of the Lucas sequence $u_n(2kl, 1)$ are $u_0 = 0,\ u_1 = 1$, $u_2 = 2klu_1 + u_0 = 2kl$, $u_3 = 2klu_2 + u_1 = 4k^2l^2 + 1$. From Lemma 7 we have

$$u_{n+4} = (4k^2l^2 + 2)u_{n+2} - u_n = 0,\ n \geq 1. \tag{6}$$

Since $u_1 = q_0$ and $u_3 = q_2$, inductively using ((5) and (6)), we can easily conclude that $q_{2n} = u_{2n+1}$, for all $n \geq 0$.

Next, we will show that $q_{2n-1} = u_{2n}/k$. Since $\sqrt{A} = [k^2l; \overline{2l, 2k^2l}]$, we have that $a_n = 2l$ for n odd and $a_n = 2k^2l$ for n even, $n > 1$. Now, let r be a positive integer. From (4) we have that $q_{2r+2} = a_{2r+2}q_{2r+1} + q_{2r}$ which implies that

$$q_{2r+2} = 2k^2lq_{2r+1} + q_{2r}$$

and by substituting q_{2r+1} with

$$a_{2r+1}q_{2r} + q_{2r-1} = 2lq_{2r+1} + q_{2r},$$

we get

$$q_{2r+2} = (4k^2l^2 + 1)q_{2r} + 2k^2lq_{2r-1}.$$

On the other hand, since $(u_n)_{n\geq 0}$ is a Lucas sequence, we have

$$u_{2r+3} = 2klu_{2r+2} + u_{2r+1}$$

which implies that

$$u_{2r+3} = (4k^2l^2 + 1)u_{2r+1} + 2klu_{2r}.$$

We have already proved that the $q_{2r+2} = u_{2r+3}$ and $q_{2r} = u_{2r+1}$. Hence, $q_{2r-1} = u_{2r}/k$. This proves part (1). The proof of part (2) is similar and we omit it.

Now we shall prove part (3). By Proposition 9 the denominators $(q_n)_{n\geq 0}$ of the convergents to $\sqrt{A}$ satisfy the recurrence sequence

$$q_{n+2s} - tq_{n+s} + (-1)^s q_n = 0,\ n \geq 1,$$

where $s = 1$ and $t = 2l$. Since $q_{-1} = 0$ and $q_{-2} = 1$ we get that $q_0 = 1$, $q_1 = 2l$, and so on. On the other hand the terms of the Lucas sequence are $u_0 = 0$, $u_1 = 1$, $u_2 = 2l$ etc. The result follows. $\square$

3 The proof of Proposition 2

Let A, B be non-zero integers. Assume that $A > 0$ non-square and B square-free with $|B| < \sqrt{A}$. From Lagrange [19, p. 377-535] or from Matthews [11], we get that the fraction y/x, where (x, y) is a positive solution of the Pell equation $y^2 - Ax^2 = B$, is equal to a convergent p_n/q_n for some n, of the continued fraction of $\sqrt{A}$. So, in our case it is $\dfrac{y}{x^m} = \dfrac{p_n}{q_n}$, where $\dfrac{p_n}{q_n}$ is the n-th convergent of $\sqrt{A}$. Let $\gcd(y, x^m) = d > 1$. Then

$$d^2y'^2 = d^4Ax'^{2m} + B,$$

so $d^2|B$. But B is square-free, which leads us to a contradiction. We conclude that $q_n = x^m$. The proposition follows.

Remark 11. A similar result holds for $Ay^2 = x^{2m} + B$, under the same constraints for B. So we can have a similar result, as in Theorem 1, for equations of the form $Ay^2 = x^4 + B$ under the same constraints for A, B.

4 The proof of Theorem 1

By p_n/q_n we denote the convergents of the continued fraction of $\sqrt{A}$, where $A \in \{k^2(k^2l^2 + 1), 4k^2(k^2(2l-1)^2 + 1)\}$ $(k, l \in \mathbb{Z}_{>0})$. Since $0 \neq |B| < \sqrt{A}$, by Proposition 2 for $m = 2$ we have that $x^2 = q_s$ for some positive integer s. That is, in order to compute the solutions (x, y) of the equation $y^2 = Ax^4 + B$ it is enough to find the denominators of the convergents of $\sqrt{A}$ that are perfect squares.

Proof. **Part 1.** According to Lemma 10 (1), the even-indexed terms q_s are equal to the odd-indexed terms u_n of the Lucas sequence $u_n(2kl, 1)$, while the odd-indexed terms q_s are equal to the even-indexed terms u_n of the Lucas sequence $u_n(2kl, 1)$ divided by k. So, in order to compute q_s that are perfect squares, we need to compute the odd-indexed terms of $u_n(2kl, 1)$ that are of the form x^2 and the even-indexed terms of $u_n(2kl, 1)$ that are of the form kx^2.

In order to prove the case (a) of part (1), we consider the case where $k = 1$, which implies that $A = l^2 + 1$. From Lemma 6 we conclude that the only possible case for $n \geq 4$ is $(n, 2l, 1) = (7, 2, 1)$. Thus $l = 1$, $A = 2$ and $u_7 = 169$, which implies $|x| = 13$. For $l = k = 1$ we get the sequence $u_n(2, 1)$ which is A000129 in Sloane's *Online Encyclopedia of Integer Sequences* [21]. Now let $n < 4$. For $n = 3$ we have $u_3 = 4l^2 + 1$ which is not a perfect square unless $l = 0$ which contradicts the fact that l is positive. For $n = 2$ we have $u_2 = 2l$ and for $n = 1$ we have $u_1 = 1$. Including the trivial solution $x = 0$, we conclude that $|x| \in \{0, 1, 13, \sqrt{2l}\}$, while $|x| = 13$ occurs only if $A = 2, B = 1$.

In order to prove the case (b) we consider $k \in \{2, 3, 6\}$. We assume first that n is odd ≥ 4. Thus we have to solve $u_n = x^2$ for some integer x and $u_n = u_n(2kl, 1)$. According to Lemma 6 (applying it for $m = 1$) we get $(n, 2kl, 1) = (7, 2, 1)$, which implies that $k = l = 1$, contradicting the fact that $k > 1$. Thus there are no possible terms u_n of the form x^2.

For n even we need to compute the terms of the Lucas sequence $u_n(2kl, 1)$ such that $u_n = kx^2$ for some integer x. For n even and ≥ 4 by Lemma 6 we get the triplets $(n, 2kl, 2) = (4, 4, 2)$ and $(n, 2kl, 3) = (4, 2, 3), (4, 24, 3)$. If we have the triplet $(4, 4, 2)$, we get $u_4(4, 1) = 72 = 2x^2$, which implies $|x| = 6$. The sequence $u_4(4, 1)$ appears in Sloane's database [21] as A001076. In this case we have to solve the equation $y^2 = A \cdot 6^4 + B$ for $A = 20$ and $|B| \leq 4$. For this equation there is a unique solution, which is $(x, y, B) = (6, 161, 1)$. For the triplet $(4, 2, 3)$ we have $kl = 1$, which is a contradiction. For the triplet $(4, 24, 3)$ we have $u_4(24, 1) = 13872 = 3x^2$ which implies that $|x| = 68$.

For $x = 68$, $k = 3$, $l = 4$, we get $A = k^2(k^2l^2 + 1) = 1305$. For $|B| \leq \sqrt{1305} < 37$ the equation $y^2 = Ax^4 + B$ has a unique solution $(|x| = 68, |y| = 167041)$.

Now let $n < 4$. For $n = 3$ we have $u_3 = 4k^2l^2 + 1$, which is not a perfect square, since k, l are positive integers. For $n = 2$, $u_2 = 2kl$ must be of the form kx^2, which implies that $|x| = \sqrt{2l}$. For $n = 1$ we have that $|x| = 1$. Including the trivial solution $x = 0$, we conclude that $|x| \in \{0, 1, 6, \sqrt{2l}\}$, where the solution $|x| = 6$ occurs only when $A = 20, B = 1$.

Finally, to prove the case (c) of part (1), we consider the case where $k \notin \{1, 2, 3, 6\}$. As in the previous case, we need to compute the square terms of the Lucas sequence $u_n(2kl, 1)$ with an odd index. By Lemma 6 we conclude that there are no possible solutions for $n \geq 4$, and the cases where $n = 3$ or $n = 1$ are the same with case (a).

For n even we need to compute the terms of the form kx^2 of the Lucas sequence $u_n(2kl, 1)$. The integer x is a solution of the equation $y^2 - dx^4 = 1$, where $d = k^2(k^2l^2 + 1)$ (Lemma 4). By Lemma 5 we get $|x| \in \{\sqrt{x_1}, \sqrt{x_2}, \sqrt{x_p}\}$, where $y_1 + x_1\sqrt{d} = \varepsilon_d$ is the minimal unit (> 1) of the ring $\mathbb{Z}[\sqrt{d}]$ and $\varepsilon_d^t = y_t + x_t\sqrt{d}$. The solutions for $n < 4$ and $m \neq 1, 2, 3, 6$ are analogous to the previous cases, so $|x| \in \{0, 1, \sqrt{2l}, \sqrt{x_1}, \sqrt{x_2}, \sqrt{x_p}\}$.

Part 2. According to Lemma 10 (2), the even-indexed terms q_s are equal to the odd-indexed terms u_n of the Lucas sequence $u_n(2k(2l-1), 1)$, while the odd-indexed terms q_s are equal to the even-indexed terms u_n of the Lucas sequence $u_n(2k(2l-1), 1)$ divided by $2k$.

So, in order to compute q_s that are perfect squares, we need to compute the odd-indexed terms of $u_n(2kl, 1)$ that are of the form x^2, and the even-indexed terms of $u_n(2k(2l-1), 1)$ that are of the form $2kx^2$.

Now consider the case (a) of part (2). Since $k \in \{1, 3\}$, by Lemma 6 for $m = 1$ we get that the only possible case for n odd and $n \geq 4$ is $(n, 2k(2l-1), 1) = (7, 2, 1)$. So $l = k = 1$, $A = 8$ and $u_7 = 169 = x^2$. We easily conclude that there are no integral solutions of $y^2 = 8x^4 + B$ for $x = 13$ and $|B| < \sqrt{A}$. For $n = 3$ we have $u_3 = 4k^2(2l-1)^2 + 1$, which is clearly not a perfect square since $k \neq 0$, and for $n = 1$, we have $u_1 = 1$, which is obviously a perfect square.

Now let n be even. We need to compute the terms of the Lucas sequence $u_n(2k(2l-1), 1)$, such that $u_n = 2kx^2$ for some integer x. For $n \geq 4$ according to Lemma 6 for $m = 2k$ (since $k \in \{1, 3\}$ we get $m \in \{2, 6\}$) we can easily deduce that there is no possible triplet of the form $(n, 2k(2l-1), 2k)$. For $n = 2$, we have $u_2 = 2k(2l-1)$, which is of the form $2kx^2$ for $|x| = \sqrt{2l-1}$. Including the trivial solution $x = 0$, we conclude that $|x| \in \{0, 1, \sqrt{2l-1}\}$.

Finally, consider the case where $k \notin \{1, 3\}$ (case (b)). As in the previous case (a), according to Lemma 6 there are no possible solutions for n odd, $n \geq 4$, and the cases where $n = 3$ or $n = 1$ are also the same with the previous case. For n even we work as in case (c) of part (1). Including the trivial solution $x = 0$, we conclude that $|x| \in \{0, 1, \sqrt{2l-1}, \sqrt{x_1}, \sqrt{x_2}, \sqrt{x_p}\}$. $\square$

5 The proof of Proposition 3

Initially, we recall Euler's theorem about continued fractions as it is provided by Burger [5, p. 52].

Theorem 12. *(Euler's theorem). Let α be a quadratic irrational, and let $\alpha_0 = \alpha$, $a_0 = \lfloor \alpha_0 \rfloor$. Then $\alpha_0 = (r_0 + \sqrt{d})/s_0$, where d is not a perfect square and $s_0 | d - r_0^2$. Let $\alpha_{n+1} = 1/(\alpha_n - a_n)$, $a_{n+1} = \lfloor \alpha_{n+1} \rfloor$. Further, we consider two sequences s_n, r_n such that*

$$r_{n+1} = a_n s_n - r_n, \quad s_{n+1} = \frac{d - r_{n+1}^2}{s_n}.$$

Then for all $n \geq 0$ it follows that:

1. *$\alpha = [a_0, a_1, a_2, \ldots]$.*
2. *$r_n, s_n \in \mathbb{Z}$ with $s_n \neq 0$ and $s_n | d - r_n^2$.*
3. *$\alpha_n = (r_n + \sqrt{d})/s_n$ and $a_n = \lfloor (r_n + \sqrt{d})/s_n \rfloor$.*
4. *If $r_0 = 0, s_0 = 1$ we set p_n/q_n to be the n-th convergent of $\sqrt{d}$. Then for all $n \geq 0$ we get*
$$p_n^2 - dq_n^2 = (-1)^{n-1} s_{n+1}. \tag{7}$$
Further, if the second part of equation (7) is ± 1, then $n = ts - 1$ for some $t \geq 0$, where s is the period of the continued fraction of $\sqrt{d}$.

5. $s_n = 1 \Leftrightarrow s|n$.

Proof. For part (1),(2) and (3) see [5, Euler's theorem, Module 8]. For part (4) see [5, Thm. 8.11 and Cor. 8.12] and for part (5) see [5, Lemma 8.9 (iv)]. $\square$

Let x, y be integers that satisfy equation (1), and let $|B| < \sqrt{A}$. Then $y = p_n$ and $x^2 = q_n$. Thus $p_n^2 - Aq_n^2 = y^2 - Ax^4 = B$. Part 4 of the previous theorem, give us

$$p_n^2 - Aq_n^2 = (-1)^{n-1} s_{n+1},$$

so

$$B = (-1)^{n-1} s_{n+1}. \tag{8}$$

Therefore B is allowed to take specific discrete values. We shall prove that for the A's we have considered, B is finally equal to 1.

Lemma 13. *Let $A = k^2(k^2l^2 + 1)$, and let n be a positive integer. Then we get $\alpha_n = k^2\alpha_1$ for n even and $\alpha_n = \alpha_1$ for n odd.*

Proof. From Lemma 8 (1) we get $\sqrt{A} = [k^2l; \overline{2l, 2k^2l}]$. According to the notation of Theorem 12, $\alpha = \sqrt{A} = \alpha_0$. So

$$a_0 = k^2l,\ a_{2n+1} = 2l,\ a_{2n} = 2k^2l.$$

It is easy to see that

$$\alpha_1 = \frac{1}{\alpha_0 - a_0} = \frac{\sqrt{A} + k^2l}{k^2},\ \alpha_2 = \frac{1}{\alpha_1 - a_1} = k^2\alpha_1 \text{ and } \alpha_3 = \alpha_1.$$

By induction our result follows. $\square$

Lemma 14. *For $A = k^2(k^2l^2 + 1)$, we get*

$$s_n = \begin{cases} 1, & n \text{ even;} \\ k^2, & n \text{ odd.} \end{cases}$$

Further, $r_n = k^2l$ for every $n \geq 0$.

Proof. From the previous lemma

$$\alpha_n = \begin{cases} k^2\alpha_1, & n \text{ even;} \\ \alpha_1, & n \text{ odd.} \end{cases}$$

Also the equality $\alpha_n = \frac{r_n + \sqrt{A}}{s_n}$ holds. Since $\alpha_1 = \frac{k^2l + \sqrt{A}}{k^2}$, our result follows. $\square$

In order to prove part (1) of Proposition 3, first we remark that

$$|B| \leq \sqrt{A} = \sqrt{k^2(k^2l^2+1)} = k\sqrt{k^2l^2+1}.$$

Since $|B|$ is an integer, the closest integer to the boundary of $|B|$ is $k\sqrt{k^2l^2}$, so $|B| \leq k^2l$. From Lemma 14 and relation (8) we get $B \in \{1, -k^2\}$ and since B is square-free, Proposition 3 part (1) follows. The second part is similarly proved.

For the third part, we repeat some arguments of the proof of part (2b) of Theorem 1. First we consider the equation

$$p_n^2 - Aq_n^2 = (-1)^{n-1}s_{n+1} \tag{9}$$

with n even. So according to Lemma 10 part (2) we have to find the odd-indexed terms of the Lucas sequence $u_n(2k(2l-1), 1)$ which are perfect squares. But, such terms do not exist except when $n = 1$ (see the proof of part (2b) of Theorem 1). In the specific case where $n = 1$, a straightforward computation gives $s_2 = 1$, thus $B = 1$. For n odd, the index in the sequence in the right part of relation (9) is even. In that case, since the period of the continued fraction of $\sqrt{A}$ is 2, Theorem 12 part (5) gives $s_{n+1} = 1$. So in any case, from relation (8), we get $B = 1$.

6 Examples

Example 15. For $k = 1$, $l = 301$, and $A = 4k^2(k^2(2l-1)^2+1) = 1444808$. We consider the family $E_B : y^2 = Ax^4 + B$ with B square-free, and $|B| \leq 1202$. In this family there are elliptic curves with large rank. For instance if $B = 1$ we get an elliptic curve of rank 5. According to part 2 (a) of Theorem 1, we get $|x| \in \{0, 1\}$ (since $\sqrt{2l-1}$ is not an integer). Solutions occur only for the trivial case where $x = 0$. So, the solutions (x, y, B) are $(0, 1, 1)$ and $(0, -1, 1)$.

Example 16. Now let $k = 12$, $l = 1$, and $A = k^2(k^2l^2+1) = 20880$. We consider the family of the curves $E_B : y^2 = Ax^4 + B$, where B is as usual square-free and $|B| \leq 144$. For $B = -5$ we get a curve of rank 3. According to part 1 (c) of Theorem 1, we get $|x| \in \{0, 1, \sqrt{x_1}, \sqrt{x_2}, \sqrt{x_p}\}$, and $B = 1$ from the first part of Proposition 3. The fundamental solution of $y^2 - Ax^2 = 1$ is $289 + 2\sqrt{20880} > 1$. So $y_1 = 289$ and $x_1 = 2$. Since x_1 is not a perfect square and is not of the form pu^2 where $p \equiv 3 \pmod 4$, we only need to check x_2. Now, $(289 + 2\sqrt{20880})^2$ equals to $167041 + 1156\sqrt{20880}$. Thus $x_2 = 1156$ which is the square of 34. Therefore, the solutions (x, y, B) of $y^2 = 20880x^4 + B$ are $(0, \pm 1, 1)$ and $(\pm 34, \pm 167041, 1)$.

Example 17. Now we consider the equation $y^2 = (2^{4r+2}+1)x^4+n$, where $-2^{2r+1} \leq n \leq 2^{2r+1}$ and $n \neq 0$ square-free. Then our main result for $k = 1$ and $l = 2^{2r+1}$ gives $|x| \in \{0, 1, 2^{r+1}\}$. Further, from the second part of Proposition 3 we get $|n| = 1$. Thus, after some simple calculations we get $(|x|, |y|, n) = (0, 1, 1), (1, 2^{2r+1}, -1), \big(2^{r+1}, 2^{4r+3}+1, 1\big)$.

References

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

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

[3] M. A. Bennett, Powers in recurrence sequences: Pell equations, *Trans. Amer. Math. Soc.* **357** (2005), 1675–1691.

[4] W. Bosma, J. Cannon, and C. Playoust, The Magma algebra system. I. The user language, *J. Symbolic Comput.* **24** (1997), 235–265.

[5] E. B. Burger, *Exploring the Number Jungle: a Journey into Diophantine Analysis*, American Mathematical Society, 2000.

[6] J. Chen and P. Voutier, 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.

[7] J. H. E. Cohn, The Diophantine equation $x^4 + 1 = Dy^2$, *Math. Comp.* **66** (1997), 1347–1351.

[8] J. H. E. Cohn, The Diophantine equation $y^2 = Dx^4 + 1$ III, *Math. Scand.* **42** (1978), 180–188.

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

[10] T. Kagawa and N. Terai, Squares in Lucas sequences and some Diophantine equations, *Manuscripta Math.* **96** (1998), 195–202.

[11] K. Matthews, The Diophantine equation $x^2 - Dy^2 = N,\ D > 0$, *Expo. Math.* **18** (2000), 323–331.

[12] H. W. Lenstra and J. O. Shallit, Continued fractions and linear recurrences, *Math. Comp.* **61** (1993), 351–354.

[13] W. Ljunggren, Einige Eigenschaften der Einheiten reeller quadratischer und rein biquadratisher Zahlkörper, *Oslo Vid.-Akad. Skrifter* **12** (1936), 1–73.

[14] W. Ljunggren, Zur Theorie der Gleichung $x^2 + 1 = Dy^4$, *Avh. Norske Vid. Akad. Oslo. I* **5** (1942), 1–27.

[15] W. Ljunggren, Some remarks on the Diophantine equations $x^2+y^4 = 1$ and $x^4+Dy^2 = 1$, *J. Lond. Math. Soc.* **41** (1966), 542–544.

[16] K. Nakamula and A. Pethő, Squares in binary recurrence sequences. In K. Győry, A. Pethő, and V.T. Sós, eds., *Number Theory*, Walter de Gruyter, 1998, pp. 409–421.

[17] 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.

[18] P. Samuel, Resultats elémentaires sur certaines equations Diophantiennes, *J. Théor. Nombres Bordeaux* **4** (2002), 629–646.

[19] M. J.-A. Serret, eds., *Œuvres de Lagrange (Volume 2)*, Gauthier-Villars, 1868. Available at `https://archive.org/details/uvresdelagrange09natigoog`, February 6 2015.

[20] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, 1986.

[21] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, `http://oeis.org/`.

[22] 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.

[23] N. Tzanakis, Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. The case of quartic equations. *Acta Arith.* **75** (1996), 165–190.

[24] N. Tzanakis, *Elliptic Diophantine Equations. A Concrete Approach via the Elliptic Logarithm*, Walter de Gruyter, 2013.

[25] P. G. Walsh, An improved method for solving the family of Thue equations $X^4 - 2rX^2Y^2 - sY^4 = 1$. In *Number Theory for the Millennium III: Proc. of the Millennial Conference on Number Theory 2000*, A. K. Peters, 2002, pp. 375–383.

2010 *Mathematics Subject Classification*: Primary 11D25; Secondary 11D41, 11A55, 11B39.
Keywords: Lucas sequence, continued fraction, Diophantine equation, quartic elliptic curve.

(Concerned with sequences A000129 and A001076.)

Received November 4 2014; revised versions received January 31 2015; February 23 2015. Published in *Journal of Integer Sequences*, May 12 2015.

Return to Journal of Integer Sequences home page.