



ELSEVIER

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt



On the Diophantine equation $NX^2 + 2^L 3^M = Y^N$



Eva G. Goedhart*, Helen G. Grundman

Department of Mathematics, Bryn Mawr College, Bryn Mawr, PA 19010, United States

ARTICLE INFO

Article history:

Received 23 April 2013

Received in revised form 12

February 2014

Accepted 12 February 2014

Available online 2 April 2014

Communicated by David Goss

MSC:

11D41

11D61

Keywords:

Exponential Diophantine equations

Lehmer sequences

ABSTRACT

We prove that the Diophantine equation $NX^2 + 2^L 3^M = Y^N$ has no solutions (N, X, Y, L, M) in positive integers with $N > 1$ and $\gcd(NX, Y) = 1$, generalizing results of Luca, Wang and Wang, and Luca and Soydan. Our proofs use results of Bilu, Hanrot, and Voutier on defective Lehmer pairs.

© 2014 Elsevier Inc. All rights reserved.

1. Introduction

In this work, we prove the following theorem.

Theorem 1. *The equation*

$$NX^2 + 2^L 3^M = Y^N, \tag{1}$$

has no solution with $N, X, Y, L, M \in \mathbb{Z}^+$, $N > 1$, and $\gcd(NX, Y) = 1$.

* Corresponding author.

E-mail addresses: egoedhart@brynmawr.edu (E.G. Goedhart), grundman@brynmawr.edu (H.G. Grundman).

Eq. (1) is a variation of the equation $NX^2 + 2^K = Y^N$ studied by Wang and Wang [8] and by Luca and Soydan [5] and of the equation $X^2 + 2^L 3^M = Y^N$ studied by Luca [4]. Our proofs draw upon ideas from each of these papers.

We begin by showing that it suffices to prove Theorem 1 in the case where N is square-free, and by reviewing a needed result on Lehmer pairs. In Section 2, we prove the special case of Theorem 1 in which both of the exponents L and M are assumed to be even. Then in Section 3, we prove the remaining cases, thus completing the proof of Theorem 1.

Lemma 2. *If there exists a solution to $NX^2 + 2^L 3^M = Y^N$ as in Theorem 1, then there exists a solution with the same values of L and M , but with N square-free.*

Proof. Suppose that $(N, X, Y, L, M) = (n, x, y, \ell, m)$ is a solution to $NX^2 + 2^L 3^M = Y^N$, with $n, x, y, \ell, m \in \mathbb{Z}^+$, $n > 1$, and $\gcd(nx, y) = 1$. Note that $\ell, m > 0$ implies that $\gcd(n, 6) = 1$.

Let $n = uv^2$, with $u, v \in \mathbb{Z}^+$ and u square-free. Suppose that $u = 1$. Then $(N, X, Y, L, M) = (n, vx, y, \ell, m)$ is a solution to $X^2 + 2^L 3^M = Y^N$ with $N, X, Y, L, M \in \mathbb{Z}^+$, $N > 1$, and $\gcd(X, Y) = 1$. By [4, Theorem 2.1], this implies that $n = N = 3$ or 4 , contradicting that $\gcd(n, 6) = 1$. Thus $u > 1$.

Now, note that $u(vx)^2 + 2^\ell 3^m = y^n = (y^{v^2})^u$, and so $(N, X, Y, L, M) = (u, vx, y^{v^2}, \ell, m)$ is a solution to (1) with $\gcd(NX, Y) = \gcd(uvx, y^{v^2}) = 1$, and $N = u > 1$. \square

A key element in our proofs is the theory of Lehmer sequences and defective Lehmer pairs, which we now briefly describe. For a more detailed introduction, see [7].

A pair of algebraic integers (γ, δ) is called a Lehmer pair if $\gamma\delta \in \mathbb{Z} - \{0\}$, $(\gamma + \delta)^2 \in \mathbb{Z} - \{0\}$, $\gcd(\gamma\delta, (\gamma + \delta)^2) = 1$, and $\frac{\gamma}{\delta}$ is not a root of unity. Given a Lehmer pair, (γ, δ) , and $s \in \mathbb{Z}^+$, define

$$L_s(\gamma, \delta) = \begin{cases} \frac{\gamma^s - \delta^s}{\gamma - \delta}, & \text{if } s \text{ is odd,} \\ \frac{\gamma^s - \delta^s}{\gamma^2 - \delta^2}, & \text{if } s \text{ is even.} \end{cases}$$

The Lehmer pair (γ, δ) is s -defective if, for each $p \mid L_s(\gamma, \delta)$,

$$p \mid (\gamma^2 - \delta^2)^2 L_1(\gamma, \delta) \dots L_{s-1}(\gamma, \delta).$$

We need the following lemma [7, Theorem 1(ii)].

Lemma 3 (Voutier). *Let $s \in \mathbb{Z}^+$ such that $6 < s \leq 30$ and $s \neq 8, 10$, or 12 . If (γ, δ) is an s -defective Lehmer pair, then for some $k \in \{0, 1, 2, 3\}$, $i^k \gamma$ is one of the values listed in Table 1.*

Table 1
Possible values of $i^k \gamma$ in Lemma 3.

s	$i^k \gamma$, for $k \in \{0, 1, 2, 3\}$		
7	$\frac{1 \pm \sqrt{-7}}{2}$ $\frac{\sqrt{5} \pm \sqrt{-7}}{2}$	$\frac{1 \pm \sqrt{-19}}{2}$ $\frac{\sqrt{13} \pm \sqrt{-3}}{2}$	$\frac{\sqrt{3} \pm \sqrt{-5}}{2}$ $\frac{\sqrt{14} \pm \sqrt{-22}}{2}$
9	$\frac{\sqrt{5} \pm \sqrt{-3}}{2}$	$\frac{\sqrt{7} \pm \sqrt{-1}}{2}$	$\frac{\sqrt{7} \pm \sqrt{-5}}{2}$
13	$\frac{1 \pm \sqrt{-7}}{2}$		
14	$\frac{\sqrt{3} \pm \sqrt{-13}}{2}$ $\frac{\sqrt{7} \pm \sqrt{-5}}{2}$	$\frac{\sqrt{5} \pm \sqrt{-3}}{2}$ $\frac{\sqrt{19} \pm \sqrt{-1}}{2}$	$\frac{\sqrt{7} \pm \sqrt{-1}}{2}$ $\frac{\sqrt{22} \pm \sqrt{-14}}{2}$
15	$\frac{\sqrt{7} \pm \sqrt{-1}}{2}$	$\frac{\sqrt{10} \pm \sqrt{-2}}{2}$	
18	$\frac{1 \pm \sqrt{-7}}{2}$	$\frac{\sqrt{3} \pm \sqrt{-5}}{2}$	$\frac{\sqrt{5} \pm \sqrt{-7}}{2}$
24	$\frac{\sqrt{3} \pm \sqrt{-5}}{2}$	$\frac{\sqrt{5} \pm \sqrt{-3}}{2}$	
26	$\frac{\sqrt{7} \pm \sqrt{-1}}{2}$		
30	$\frac{1 \pm \sqrt{-7}}{2}$	$\frac{\sqrt{2} \pm \sqrt{-10}}{2}$	

2. Even exponents

In this section, we prove the following special case of Theorem 1.

Theorem 4. *The equation*

$$NX^2 + 2^{2L}3^{2M} = Y^N,$$

has no solution with $N, X, Y, L, M \in \mathbb{Z}^+$, $N > 1$, and $\gcd(NX, Y) = 1$.

Proof. Suppose that $(N, X, Y, L, M) = (n, x, y, \ell, m)$ is a solution to $NX^2 + 2^{2L}3^{2M} = Y^N$, with $n, x, y, \ell, m \in \mathbb{Z}^+$, $n > 1$, and $\gcd(nx, y) = 1$. It follows immediately that $y > 1$ and $nx^2 \equiv y^n \pmod{6}$. Since $\gcd(nx, y) = 1$, we have

$$n \equiv y \equiv \pm 1 \pmod{6} \quad \text{and} \quad x \equiv \pm 1 \pmod{6}.$$

By Lemma 2, we may assume that n is square-free.

We now apply the following lemma, proved by Heuberger and Le [3] and adapted to this form by Wang and Wang [8].

Lemma 5 (Heuberger & Le). *Let $d \in \mathbb{Z}$ be square-free such that $d > 1$, and let $k \in \mathbb{Z}$ be odd such that $k > 1$ and $\gcd(d, k) = 1$. Let $h(-4d)$ denote the number of classes of primitive binary quadratic forms of discriminant $-4d$. If the equation*

$$X^2 + dY^2 = kZ, \quad X, Y, Z \in \mathbb{Z}, \quad \gcd(X, Y) = 1, \quad Z > 0$$

has a solution, (X, Y, Z) , then there exist $X_1, Y_1, Z_1, t \in \mathbb{Z}^+$ and $\lambda_1, \lambda_2 \in \{+1, -1\}$, such that

$$X_1^2 + dY_1^2 = k^{Z_1}, \quad \gcd(X_1, Y_1) = 1,$$

$$Z = Z_1 t, \quad Z_1 \mid h(-4d), \quad \text{and}$$

$$X + Y\sqrt{-d} = \lambda_1(X_1 + \lambda_2 Y_1\sqrt{-d})^t.$$

By the lemma, since $(2^\ell 3^m)^2 + nx^2 = y^n$, with $n > 1$ square-free, $y > 1$ odd, and $\gcd(nx, y) = 1$, there exist $X_1, Y_1, Z_1, t \in \mathbb{Z}^+$ and $\lambda_1, \lambda_2 \in \{+1, -1\}$, such that

$$X_1^2 + nY_1^2 = y^{Z_1}, \quad \gcd(X_1, Y_1) = 1, \tag{2}$$

$$n = Z_1 t, \quad Z_1 \mid h(-4n), \quad \text{and} \tag{3}$$

$$2^\ell 3^m + x\sqrt{-n} = \lambda_1(X_1 + \lambda_2 Y_1\sqrt{-n})^t. \tag{4}$$

Note that, since $\gcd(n, 6) = 1, \gcd(t, 6) = \gcd(Z_1, 6) = 1$. Thus t is odd and $y^{Z_1} \equiv y \equiv n \equiv \pm 1 \pmod{6}$. For ease in notation, let $t = 2t_1 + 1$.

Expanding Eq. (4) and taking the absolute value of the real and imaginary parts of each side yields

$$2^\ell 3^m = \left| \sum_{j=0}^{t_1} \binom{t}{2j} X_1^{t-2j} (-nY_1^2)^j \right| = X_1 \left| \sum_{j=0}^{t_1} \binom{t}{2j} X_1^{t-2j-1} (-nY_1^2)^j \right|, \tag{5}$$

and

$$x = Y_1 \left| \sum_{j=0}^{t_1} \binom{t}{2j+1} X_1^{t-2j-1} (-nY_1^2)^j \right|. \tag{6}$$

By Eq. (5), 2 and 3 are the only possible prime divisors of X_1 . By Eq. (6) and $\gcd(x, 6) = 1, \gcd(6, Y_1) = 1$. Thus $Y_1 \equiv \pm 1 \pmod{6}$.

By Eq. (2), $X_1^2 + n \equiv n \pmod{6}$, and so $X_1 \equiv 0 \pmod{6}$.

Rewriting Eq. (5) as $2^\ell 3^m = X_1 |\mathcal{S}|$, with

$$\mathcal{S} = \sum_{j=0}^{t_1} \binom{t}{2j} X_1^{t-2j-1} (-nY_1^2)^j,$$

we have

$$\mathcal{S} \equiv \binom{t}{t-1} (-nY_1^2)^{t_1} \equiv \pm 1 \pmod{6}.$$

But then, $\gcd(\mathcal{S}, 6) = 1$ and so $X_1 = 2^\ell 3^m$ and $|\mathcal{S}| = 1$.

Let $\gamma = X_1 + Y_1\sqrt{-n}$ and let $\delta = -X_1 + Y_1\sqrt{-n}$.

Lemma 6. *The pair (γ, δ) is a t -defective Lehmer pair.*

Proof. An easy calculation shows that $\gamma\delta = -X_1^2 - nY_1^2 = -y^{Z_1}$ and $(\gamma + \delta)^2 = -4nY_1^2$, each of which is nonzero. Suppose that p is prime such that $p \mid \gcd(\gamma\delta, (\gamma + \delta)^2)$. Then, since $\gcd(n, y) = 1$ and y is odd, $p \mid Y_1$. Additionally, $p \mid (y^{Z_1} - nY_1^2)$ and so $p \mid X_1$. But $\gcd(X_1, Y_1) = 1$, and thus $\gcd(\gamma\delta, (\gamma + \delta)^2) = 1$. Note that since $n > 1$, $\gcd(n, 6) = 1$, and n is square-free, the only roots of unity in $\mathbb{Q}(\sqrt{-n})$ are ± 1 . Thus, $\frac{\gamma}{\delta}$ is not a root of unity. Therefore, (γ, δ) is a Lehmer pair.

Finally, by Eqs. (4) and (5),

$$|L_t(\gamma, \delta)| = \left| \frac{\gamma^t - \delta^t}{\gamma - \delta} \right| = \left| \frac{2\Re(\gamma^t)}{2\Re(\gamma)} \right| = \frac{X_1|\mathcal{S}|}{X_1} = 1.$$

Thus, (γ, δ) is a t -defective Lehmer pair. \square

By the work of Bilu, Hanrot and Voutier [1, Theorem 1.4], since there exists a t -defective Lehmer pair, we have that $t \leq 30$. Then, using Lemma 3 with the fact that $\gcd(t, 6) = 1$, it follows that $t \in \{1, 5\}$.

If $t = 5$, then

$$\mathcal{S} = \sum_{j=0}^2 \binom{5}{2j} (2^\ell 3^m)^{5-2j-1} (-nY_1^2)^j = 2^{4\ell} 3^{4m} - 10 \cdot 2^{2\ell} 3^{2m} nY_1^2 + 5n^2 Y_1^4.$$

Since $\mathcal{S} = \pm 1$ and n and Y_1 are both odd, $\pm 1 = \mathcal{S} \equiv 5n^2 Y_1^4 \equiv 5 \pmod{8}$, which is impossible.

Thus, $t = 1$. So, by Eq. (3), $Z_1 = n$ and, hence, $n \mid h(-4n)$. But, since n is greater than 1 and square-free, by [8, Lemma 3], $n > h(-4n)$, a contradiction. \square

3. Odd exponents

In this section, we prove the remaining cases of Theorem 1, as described in the following theorem.

Theorem 7. *The equation*

$$NX^2 + 2^L 3^M = Y^N,$$

has no solution with $N, X, Y, L, M \in \mathbb{Z}^+$, $N > 1$, $\gcd(NX, Y) = 1$, and L and M not both even.

We begin with a basic computational lemma.

Lemma 8. Let $t_1 \in \mathbb{Z}$ and let $t = 2t_1 + 1$. Then

$$\sum_{j=0}^{t_1} \binom{t}{2j+1} = 2^{t-1} \quad \text{and} \quad \sum_{j=0}^{t_1} \binom{t}{2j+1} (-1)^j = \pm 2^{t_1}.$$

Proof. First, let $f(t) = \sum_{j=0}^{t_1} \binom{t}{2j+1}$ and let $g(t) = \sum_{j=0}^{t_1} \binom{t}{2j} (-1)^j$. Then $f(t) + g(t) = (1+1)^t$ and $-f(t) + g(t) = (1-1)^t$. Solving these for $f(t)$ yields the first result.

Next, let $f_1(t) = \sum_{j=0}^{t_1} \binom{t}{2j+1} (-1)^j = -i \sum_{j=0}^{t_1} \binom{t}{2j+1} (i)^{2j+1}$ and $g_1(t) = -i \sum_{j=0}^{t_1} \binom{t}{2j} (i)^{2j}$. Then $f_1(t) + g_1(t) = -i(1+i)^t$ and $-f_1(t) + g_1(t) = -i(1-i)^t$. Solving for $f_1(t)$ completes the proof. \square

Proof of Theorem 7. Suppose that $(N, X, Y, L, M) = (n, x, y, \ell, m)$ is a solution to $NX^2 + 2^L 3^M = Y^N$, with $n, x, y, \ell, m \in \mathbb{Z}^+$, $n > 1$, $\gcd(nx, y) = 1$, and either ℓ or m odd.

Since ℓ and m are nonzero, $nx^2 \equiv y^n \pmod{6}$. This with $\gcd(nx, y) = 1$ yields

$$n \equiv y \equiv \pm 1 \pmod{6} \quad \text{and} \quad x \equiv \pm 1 \pmod{6}.$$

Since $n > 1$, this implies that, in fact, $n \geq 5$.

Let $\ell = 2k + e$ and $m = 2k' + e'$ with $k, k' \geq 0$ and $e, e' \in \{0, 1\}$. Set $w = 2^e 3^{e'} \in \{1, 2, 3, 6\}$. By assumption, ℓ and m cannot both be even. Hence, $w \in \{2, 3, 6\}$.

Set $a = 2^k 3^{k'} \sqrt{w} + x\sqrt{-n}$ and $b = 2^{k'} 3^{k'} \sqrt{w} - x\sqrt{-n}$. Then $ab = y^n$. Letting $E = \mathbb{Q}(\sqrt{w}, \sqrt{-n})$ and $F = \mathbb{Q}(\sqrt{-wn})$, we have $a, b \in \mathcal{O}_E$ and $a^2, b^2 \in \mathcal{O}_F$.

Suppose that there exists a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_E$ such that $\mathfrak{p} \mid a\mathcal{O}_E$ and $\mathfrak{p} \mid b\mathcal{O}_E$. Then, since $\mathfrak{p} \mid ab\mathcal{O}_E$, $\mathfrak{p} \mid y\mathcal{O}_E$ and, since $\mathfrak{p} \mid (a+b)\mathcal{O}_E$ and $w\mathcal{O}_E \mid 6\mathcal{O}_E$, $\mathfrak{p} \mid 6\mathcal{O}_E$. But this is not possible, since y is relatively prime to 6 in \mathbb{Z} . Hence $a\mathcal{O}_E$ and $b\mathcal{O}_E$ are relatively prime in \mathcal{O}_E . It follows easily that $a^2\mathcal{O}_F$ and $b^2\mathcal{O}_F$ are relatively prime in \mathcal{O}_F .

Now, $(a^2\mathcal{O}_F)(b^2\mathcal{O}_F) = y^{2n}\mathcal{O}_F = (y\mathcal{O}_F)^{2n}$. By the unique factorization of ideals in \mathcal{O}_F , there exists an ideal $I \subseteq \mathcal{O}_F$ such that $a^2\mathcal{O}_F = I^{2n}$. Let s be the order of the ideal class of I in the class group of \mathcal{O}_F . Then there exists $\alpha \in \mathcal{O}_F$ such that $I^s = \alpha\mathcal{O}_F$. Since $a^2\mathcal{O}_F$ is principal, we have $s \mid 2n$, and so $2n = st$ for some $t \in \mathbb{Z}^+$. Further, $a^2\mathcal{O}_F = I^{2n} = (I^s)^t = \alpha^t\mathcal{O}_F$, and so there exists a unit $\varepsilon \in \mathcal{O}_F$ such that $a^2 = \varepsilon\alpha^t$. Since $F = \mathbb{Q}(\sqrt{-wn})$ with wn square-free and $n \geq 5$, $\varepsilon = \pm 1$.

Suppose t is even, so $t = 2t_0$ for some $t_0 \in \mathbb{Z}^+$. Then

$$\left(\frac{a}{\alpha^{t_0}}\right)^2 = \varepsilon = \pm 1.$$

But, as is easily verified, E does not contain a square root of -1 . So $\varepsilon = 1$ and $a = \pm\alpha^{t_0} \in F$, contradicting the definition of a . Thus t is odd and so s is even. Further, since $t \mid 2n$, $\gcd(t, 6) = 1$.

Replacing α with $-\alpha$, if necessary, we may assume, without loss of generality, that $\varepsilon = 1$. Thus $a^2 = \alpha^t$.

Suppose that $t = 1$. Then $s = 2n$ and so $2n \mid h_F$, the class number of \mathcal{O}_F . In particular, $2n \leq h_F$. Let $d = \text{disc}(\mathcal{O}_F)$. Then $d = -wn$ or $d = -4wn$. By the class number formula and a basic bound on $L(1, \chi_d)$ [6], we have

$$h_F = \frac{\sqrt{|d|}}{\pi} L(1, \chi_d) \leq \frac{\sqrt{|d|}}{\pi} (2 + \log |d|) = \frac{2\sqrt{|d|}}{\pi} (1 + \log \sqrt{|d|}).$$

Thus, since $|d| \leq 4wn \leq 24n$,

$$2n \leq h_F \leq \frac{2\sqrt{|d|}}{\pi} (1 + \log \sqrt{|d|}) \leq \frac{2\sqrt{24n}}{\pi} (1 + \log \sqrt{24n})$$

and so

$$\frac{\sqrt{24}}{\pi\sqrt{n}} (1 + \log \sqrt{24n}) \geq 1.$$

Since $\frac{\sqrt{24}}{\pi\sqrt{51}} (1 + \log \sqrt{24 \cdot 51}) < 1$ and $\frac{\sqrt{24}}{\pi\sqrt{n}} (1 + \log \sqrt{24n})$ is a decreasing function of n , for $n \geq 1$, we have a contradiction for $n > 50$.

For $n \leq 50$ or, equivalently, $wn \leq 300$, we consult a class number table (for example [2, Table 4]) to find that $h_F \leq 22$. Since $2n \leq h_F$, we have $n \leq 11$ and so $wn \leq 66$. Again consulting the table, we have $h_F \leq 8$ and so $n \leq 4$, a contradiction.

Thus, $t \neq 1$.

Since t is odd, there exists $t_1 \in \mathbb{Z}^+$, such that $t = 2t_1 + 1$. Define $\gamma = \frac{a}{\alpha^{t_1}} \in E$. Note that

$$\gamma^2 = \frac{a^2}{\alpha^{2t_1}} = \frac{\alpha^t}{\alpha^{2t_1}} = \alpha,$$

and therefore, $\gamma \in \mathcal{O}_E$.

Let $A, B \in \mathbb{Q}$ such that

$$\alpha = A + B\sqrt{-wn}$$

and note that since $\alpha^t = a^2$, $A, B \neq 0$. Let $A_1, B_1, C_1, D_1 \in \mathbb{Q}$ such that $\gamma = A_1\sqrt{w} + B_1\sqrt{-n} + C_1\sqrt{-wn} + D_1$. A simple calculation, using $\gamma^2 = \alpha$, yields that either $A_1 = B_1 = 0$ or $C_1 = D_1 = 0$. If the former holds, then $\gamma \in \mathcal{O}_F$ and $I^{s/2} = \gamma\mathcal{O}_F$, contrary to the definition of s . Thus

$$\gamma = A_1\sqrt{w} + B_1\sqrt{-n}.$$

Expanding $\gamma^2 = \alpha$ and equating real and imaginary parts yields

$$A = A_1^2w - B_1^2n \quad \text{and} \quad B = 2A_1B_1. \tag{7}$$

Since $B \neq 0$, we have $A_1, B_1 \neq 0$.

Now, unless $w = 3$ and $n \equiv 1 \pmod{4}$, $\mathcal{O}_F = \mathbb{Z}[\sqrt{-wn}]$. So $A, B \in \mathbb{Z}$. Further, considering the possible integral bases for E , in this case, $A_1 \in \mathbb{Z}$ and $2B_1 \in \mathbb{Z}$. But, by Eq. (7), $B_1^2 n = A_1^2 w - A \in \mathbb{Z}$ and so $B_1 \in \mathbb{Z}$.

If we do have $w = 3$ and $n \equiv 1 \pmod{4}$, then $\mathcal{O}_F = \mathbb{Z}[\frac{1+\sqrt{-3n}}{2}]$ and $\mathcal{O}_E = \mathbb{Z}[\sqrt{3}, \frac{\sqrt{3+\sqrt{-n}}}{2}]$. So we have $2A, 2B, 2A_1, 2B_1 \in \mathbb{Z}$. Further, Eq. (7) implies that $A, B \in \mathbb{Z}$ if and only if $A_1, B_1 \in \mathbb{Z}$.

Expanding $2^t a^2 = (2\alpha)^t$, equating real and imaginary parts, yields

$$2^{\ell+t} 3^m - 2^t n x^2 = (2A) \sum_{j=0}^{t_1} \binom{t}{2j} (2A)^{t-2j-1} (2B)^{2j} (-wn)^j \tag{8}$$

and

$$2^{k+t+1} 3^{k'} x = (2B) \sum_{j=0}^{t_1} \binom{t}{2j+1} (2A)^{t-2j-1} (2B)^{2j} (-wn)^j. \tag{9}$$

By Eq. (8), $3 \nmid 2A$.

Suppose that $3 \nmid 2Bw$. From the definition of w , $3 \nmid w$ implies that $k' \neq 0$. So, reducing Eq. (9) modulo 3 yields

$$0 \equiv \sum_{j=0}^{t_1} \binom{t}{2j+1} (\pm 1)^j \pmod{3},$$

which is impossible, by Lemma 8. Thus $3 \mid 2Bw$.

Let $\delta = \bar{\gamma} = A_1 \sqrt{w} - B_1 \sqrt{-n}$. Then $\gamma\delta = A_1^2 w + B_1^2 n \in \mathbb{Q} \cap \mathcal{O}_E = \mathbb{Z}$. Since $(\gamma\delta)^{2t} = (ab)^2 = y^{2n}$ and $2 \nmid y$, we have $2 \nmid \gamma\delta$.

Recall that if $A_1, B_1 \notin \mathbb{Z}$, then $w = 3$, $n \equiv 1 \pmod{4}$, and $2A_1 \equiv 2B_1 \equiv 1 \pmod{2}$. Thus $4\gamma\delta = (2A_1)^2 w + (2B_1)^2 n \equiv 3 + n \pmod{8}$. Since $2 \nmid \gamma\delta$ implies that $8 \nmid (2\gamma)(2\delta)$, we have $n \not\equiv 5 \pmod{8}$. Thus, if $A_1, B_1 \notin \mathbb{Z}$, $n \equiv 1 \pmod{8}$.

Now,

$$\gamma^t = \left(\frac{a}{\alpha^{t_1}} \right)^t = \frac{a^{2t_1+1}}{(\alpha^t)^{t_1}} = \frac{a^{2t_1+1}}{a^{2t_1}} = a.$$

It follows that $\delta^t = b$. Further,

$$\frac{\gamma^t + \delta^t}{\gamma + \delta} = \sum_{j=0}^{t-1} (-\gamma)^j \delta^{t-j-1} \in \mathbb{Z},$$

since it is an algebraic integer fixed by every automorphism of E . Thus, since $\gamma^t + \delta^t = a + b = 2^{k+1}3^{k'}\sqrt{w}$, we find that, in \mathbb{Z} ,

$$\left(\frac{\gamma + \delta}{\sqrt{w}}\right) \mid \left(\frac{\gamma^t + \delta^t}{\sqrt{w}}\right).$$

Simplifying yields $2A_1 \mid 2^{k+1}3^{k'}$.

Lemma 9. (γ, δ) is a $2t$ -defective Lehmer pair.

Proof. First recall that $\gamma\delta \in \mathbb{Z}$ and, since $2 \nmid \gamma\delta$, $\gamma\delta \neq 0$. Further, $(\gamma + \delta)^2 = 4A_1^2w \in \mathbb{Z} - \{0\}$. Suppose that $p \in \mathbb{Z}$ is prime such that $p \mid \gcd(\gamma\delta, (\gamma + \delta)^2)$. Then, since $2A_1 \mid 2^{k+1}3^{k'}$, $p = 2$ or $p = 3$. But $(\gamma\delta)^{2t} = (ab)^2 = y^{2n}$ and $\gcd(y, 6) = 1$. Hence no such p exists and therefore $\gcd(\gamma\delta, (\gamma + \delta)^2) = 1$. Note that $\frac{\gamma}{\delta} \in F$, in which the only roots of unity are ± 1 . It follows that $\frac{\gamma}{\delta}$ is not a root of unity, since $A_1, B_1 \neq 0$. Thus, (γ, δ) is a Lehmer pair.

Now suppose that p is a prime divisor of $L_{2t}(\gamma, \delta)$. Then, since

$$\begin{aligned} L_{2t}(\gamma, \delta) &= \frac{\gamma^{2t} - \delta^{2t}}{\gamma^2 - \delta^2} = \frac{(\gamma^t - \delta^t)(\gamma^t + \delta^t)}{(\gamma - \delta)(\gamma + \delta)} = L_t(\gamma, \delta) \frac{a + b}{\gamma + \delta} \\ &= L_t(\gamma, \delta) \frac{2^{k+1}3^{k'}\sqrt{w}}{2A_1\sqrt{w}} = \frac{2^{k+1}3^{k'}}{2A_1} L_t(\gamma, \delta), \end{aligned}$$

we have that $p = 2$, $p = 3$, or $p \mid L_t(\gamma, \delta)$.

Also, $(\gamma^2 - \delta^2)^2 = -16A_1^2B_1^2wn = -4B^2wn$. Since $3 \mid 2Bw$, $3 \mid (\gamma^2 - \delta^2)^2$. Further, if $A_1, B_1 \in \mathbb{Z}$, then $2 \mid (\gamma^2 - \delta^2)^2$. If, instead, $A_1, B_1 \notin \mathbb{Z}$, then $w = 3$ and $n \equiv 1 \pmod{8}$. Thus,

$$4L_3(\gamma, \delta) = 4 \frac{\gamma^3 - \delta^3}{\gamma - \delta} = 9(2A_1)^2 - (2B_1)^2n \equiv 9 - 1 \equiv 0 \pmod{8},$$

and so $2 \mid L_3(\gamma, \delta)$. Hence, in any case, $p \mid (\gamma^2 - \delta^2)^2 L_1(\gamma, \delta) \dots L_{2t-1}(\gamma, \delta)$. Thus (γ, δ) is a $2t$ -defective Lehmer pair. \square

By Bilu, Hanrot and Voutier [1, Theorem 1.4], since there exists a $2t$ -defective Lehmer pair, $2t \leq 30$. Then, by Lemma 3, the only candidates for γ with $2t > 12$ are of the form $\gamma = i^k(\sqrt{3} \pm \sqrt{-n})/2$ with $n \equiv 5 \pmod{8}$. But in each of these cases, $A_1, B_1 \notin \mathbb{Z}$ which, as shown above, implies that $n \equiv 1 \pmod{8}$. Thus, $2t \leq 12$. Finally, since $t \geq 5$ is odd, $t = 5$.

Expanding $a^2 = \alpha^5$ and equating real and imaginary parts, we find

$$2^\ell 3^m - nx^2 = A \sum_{j=0}^2 \binom{5}{2j} A^{5-2j-1} B^{2j} (-wn)^j \tag{10}$$

and

$$2^{k+1}3^{k'}x = B \sum_{j=0}^2 \binom{5}{2j+1} A^{5-2j-1} B^{2j} (-wn)^j. \tag{11}$$

Similarly, expanding $a = \gamma^5$ yields

$$2^k 3^{k'} = A_1(A_1^4 w^2 - 10A_1^2 B_1^2 wn + 5B_1^4 n^2) \tag{12}$$

and

$$x = B_1(5A_1^4 w^2 - 10A_1^2 B_1^2 wn + B_1^4 n^2). \tag{13}$$

Suppose, first, that $A_1, B_1 \in \mathbb{Z}$. Since $B = 2A_1B_1$, $2 \mid B$. By Eq. (10), $\gcd(A, 6) = 1$ and so, by Eq. (11), $2^{k+1} \mid B$. To see that $3^{k'} \mid B$, suppose that $k' > 0$ and $3 \nmid B$. Reducing Eq. (11),

$$0 = B(5A^4 - 10A^2B^2wn + B^4w^2n^2) \equiv B(-1 - wn + w^2) \pmod{3}.$$

Thus, $3 \nmid w$ and so $w = 2$. Hence, $0 \equiv Bn \pmod{3}$, a contradiction. Therefore, if $k' > 0$, $3 \mid B$. Since $3 \nmid 5A^4$, Eq. (11) implies that $3^{k'} \mid B$.

By Eq. (13), $\gcd(B_1, 6) = 1$. Since $B = 2A_1B_1$ and $2^{k+1}3^{k'} \mid B$, we have $2^k 3^{k'} \mid A_1$. Hence, by Eq. (12),

$$A_1^4 w^2 - 10A_1^2 B_1^2 wn + 5B_1^4 n^2 = \pm 1.$$

If $k > 0$, then $2 \mid A_1$, and reducing modulo 8 yields a contradiction. If $k = 0$, then we have $2 \mid w$ and $2 \nmid A_1$. Again, reducing modulo 8 yields a contradiction, since $2wn \equiv 4 \pmod{8}$.

Now suppose that $A_1, B_1 \notin \mathbb{Z}$. Then we have $w = 3$, $n \equiv 1 \pmod{8}$, and $(2A_1)^2 \equiv (2B_1)^2 \equiv 1 \pmod{8}$. Eq. (13) becomes

$$\begin{aligned} 32x &= (2B_1)[5(2A_1)^4 w^2 - 10(2A_1)^2 (2B_1)^2 wn + (2B_1)^4 n^2] \\ &= (2B_1)[4((2A_1)^2 w)^2 + ((2A_1)^2 w - (2B_1)^2 n)^2 - 8(2A_1)^2 (2B_1)^2 wn]. \end{aligned}$$

Since $2B_1$ is odd, this implies that

$$4((2A_1)^2 w)^2 + ((2A_1)^2 w - (2B_1)^2 n)^2 - 8(2A_1)^2 (2B_1)^2 wn \equiv 0 \pmod{32}. \tag{14}$$

Reducing each term: since $(2A_1)^4 w^2 \equiv 1 \pmod{8}$, we have that $4((2A_1)^2 w)^2 \equiv 4 \pmod{32}$; since $(2A_1)^2 w - (2B_1)^2 n \equiv 2 \pmod{8}$, $((2A_1)^2 w - (2B_1)^2 n)^2 \equiv 4 \pmod{32}$; and since $-(2A_1)^2 (2B_1)^2 wn \equiv 5 \pmod{8}$, $-8(2A_1)^2 (2B_1)^2 wn \equiv 8 \pmod{32}$. Thus, reducing congruence (14), we find $0 \equiv 4 + 4 + 8 \equiv 16 \pmod{32}$, a contradiction, which completes the proof. \square

References

- [1] Y. Bilu, G. Hanrot, P.M. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers, with appendix by M. Mignotte, *J. Reine Angew. Math.* 539 (2001) 75–122.
- [2] Z.I. Borevich, I.R. Shafarevich, *Number Theory*, Academic Press, New York, 1966.
- [3] C. Heuberger, M.H. Le, On the generalized Ramanujan–Nagell equation $x^2 + D = p^z$, *J. Number Theory* 78 (3) (1999) 312–331.
- [4] F. Luca, On the equation $x^2 + 2^a 3^b = y^n$, *Int. J. Math. Math. Sci.* 29 (4) (2002) 239–244.
- [5] F. Luca, G. Soydan, On the Diophantine equation $2^m + nx^2 = y^n$, *J. Number Theory* 132 (2012) 2604–2609.
- [6] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, 3rd edition, Springer, New York, 2004.
- [7] P.M. Voutier, Primitive divisors of Lucas and Lehmer sequences, *Math. Comp.* 64 (1995) 869–888.
- [8] Y. Wang, T. Wang, On the Diophantine equation $nx^2 + 2^{2m} = y^n$, *J. Number Theory* 131 (2011) 1486–1491.