The Ramanujan Journal (2021) 56:585–596
https://doi.org/10.1007/s11139-021-00408-9

A Lucas–Lehmer approach to generalised Lebesgue–Ramanujan–Nagell equations

Vandita Patel[1]

Received: 22 January 2020 / Accepted: 3 February 2021 / Published online: 10 June 2021

Abstract
We describe a computationally efficient approach to resolving equations of the form $C_1x^2 + C_2 = y^n$ in coprime integers, for fixed values of C_1, C_2 subject to further conditions. We make use of a factorisation argument and the Primitive Divisor Theorem due to Bilu, Hanrot and Voutier.

Keywords Exponential equation · Lehmer sequences · Primitive divisor theorem · Thue equation

Mathematics Subject Classification Primary 11D61 · Secondary 11D41 · 11D59

1 Introduction

Ramanujan [16], in 1913, conjectured that the only positive integral solutions to the equation

$$x^2 + 7 = 2^n$$

are

$$(1, 3), \quad (3, 4), \quad (5, 5), \quad (11, 7), \quad (181, 15).$$

This was proven by Nagell [15] in 1948, and the equation is now called the Ramanujan–Nagell equation. More generally, equations of the form

$$C_1x^2 + C_2 = C_3^n, \tag{1}$$

✉ Vandita Patel
vandita.patel@manchester.ac.uk

[1] Department of Mathematics, University of Manchester, Oxford Road, Manchester M13 9PL, UK

where C_1, C_2, C_3 are fixed non-zero integers are referred to as generalised Ramanujan–Nagell equations. Various special cases of (1) have been considered by many authors using a variety of methods (see survey papers [3] and [11]). For any such C_1, C_2, C_3, it is straightforward to reduce (1) to solving S-unit equations. This allows us to conclude that the set of solutions to (1) is finite by a famous theorem of Siegel. It also gives an effective algorithm for solving the equation.

In this paper we consider the generalisation

$$C_1x^2 + C_2 = y^n, \tag{2}$$

where C_1, C_2 are fixed, but $x, |y| > 1, n \geq 3$ are unknown. Here Baker's theory gives astronomical bounds on the size of the solutions (x, y, n), but does not alone give a practical method for determining them. In fact, the earliest special case of (2) appears to be due to Victor Lebesgue [12] who in 1850 solved (2) for $C_1 = C_2 = 1$. In 1948, Nagell [15] solved the cases $C_1 = 1$, $C_2 = 3, 5$, and it is now usual to refer to the equation

$$x^2 + C = y^n \tag{3}$$

as the Lebesgue–Nagell equation. In a series of papers (culminating in [7]), Cohn solved (3) for many values of $C > 0$. After the appearance of the celebrated theorem of Bilu, Hanrot and Voutier (BHV) on primitive divisors of Lucas and Lehmer sequences [4], Cohn revisited (3) in [8], showing that BHV allows for an easy resolution for 77 values in the range $1 \leq C \leq 100$. The cases $C = 74$ and $C = 86$ were solved by Mignotte and de Weger [14]. Using the modular approach based on Galois representations of elliptic curves and modular forms, the cases $C = 55$ and $C = 95$ were solved by Bennett and Skinner [2]. The remaining 19 values were dealt with in a pioneering paper due Bugeaud et al. [5], which combines Baker's theory with the modular approach. Related work which relies heavily on BHV is due to Abu Muriefah et al. [1], and adapts Cohn's method to the equation $x^2 + C = 2y^n$ (see also [19,20] for related equations) and also due to Ghanmi and Abu Muriefah [10] who study the equation $Cx^2 + D = 2y^q$ using BHV and properties of the Fibonacci sequence.

In view of Cohn's work, it is natural to consider (2), which we refer to as the generalised Lebesgue–Ramanujan–Nagell equation. We extend Cohn's method so that it applies in far greater generality.

More precisely, we study equations of the form:

$$C_1x^2 + C_2 = y^n, \quad x,\ y \in \mathbb{Z}^+, \quad \gcd(C_1x^2, C_2, y^n) = 1, \quad n \geq 3. \tag{4}$$

We may assume without loss of generality that n is an odd prime, or that $n = 4$. We prove the following.

Theorem 1 *Let C_1 be a positive squarefree integer and C_2 a positive integer. Write $C_1C_2 = cd^2$ where c is squarefree. We assume that $C_1C_2 \not\equiv 7 \pmod 8$. Let p be an odd prime for which the equation*

$$C_1x^2 + C_2 = y^p, \quad x,\ y \in \mathbb{Z}^+, \quad \gcd(C_1x^2, C_2, y^p) = 1 \tag{5}$$

has a solution (x, y). *Then either*

(i) $p \leq 5$, *or*
(ii) $p = 7$ *and* $y = 3, 5$ *or* 9, *or*
(iii) p *divides the class number of* $\mathbb{Q}(\sqrt{-c})$, *or*
(iv) $p \mid \left(q - \left(\frac{-c}{q}\right)\right)$, *where* q *is some prime* $q \mid d$ *and* $q \nmid 2c$.

In Sect. 6, we give an effective method that solves (4) for a given value of $n \geq 3$. Our algorithm relies on standard algorithms for solving Thue equations and determining integral points on elliptic curves. We implemented our method in `Magma` [6] which has inbuilt implementation of these algorithms (based on [9,18,21]) and together with Theorem 1, this determines the solutions to (4) for $2 \leq C_1 \leq 10, 1 \leq C_2 \leq 80$ subject to the restrictions: C_1 is squarefree, $\gcd(C_1, C_2) = 1$, and $C_1 C_2 \not\equiv 7 \pmod 8$. Our results are given in Sect. 7. We point out that the case $C_1 = 1$ and $1 \leq C_2 \leq 100$ is completely solved in [5], which incorporates the earlier work of Cohn, Bennett and Skinner, and Mignotte and de Weger.

The author thanks Yann Bugeaud and Szabolcs Tengely for useful conversations. The author also extends her thanks to the referee for a careful reading of the paper and for suggesting several improvements.

2 Primitive prime divisors of Lehmer sequences

A *Lehmer pair* is a pair of algebraic integers α, β, such that $(\alpha + \beta)^2$ and $\alpha\beta$ are non-zero coprime rational integers and α/β is not a root of unity. The *Lehmer sequence* associated to the Lehmer pair (α, β) is

$$\tilde{u}_n = \tilde{u}_n(\alpha, \beta) = \begin{cases} \frac{\alpha^n - \beta^n}{\alpha - \beta} & \text{if } n \text{ is odd,} \\ \frac{\alpha^n - \beta^n}{\alpha^2 - \beta^2} & \text{if } n \text{ is even.} \end{cases}$$

A prime p is called a *primitive divisor* of $\tilde{u}_n$ if it divides $\tilde{u}_n$ but does not divide $(\alpha^2 - \beta^2)^2 \cdot \tilde{u}_1 \cdots \tilde{u}_{n-1}$. We shall make use of the following celebrated theorem [4].

Theorem 2 *(Bilu, Hanrot and Voutier) Let* α, β *be a Lehmer pair. Then* $\tilde{u}_n(\alpha, \beta)$ *has a primitive divisor for all* $n > 30$, *and for all prime* $n > 13$.

A Lehmer pair (α, β) is called *n-defective* if $\tilde{u}_n(\alpha, \beta)$ does not have a primitive divisor. Two Lehmer pairs (α, β) and (α', β') are said to be *equivalent* if $\alpha/\alpha' = \beta/\beta' \in \{\pm 1, \pm\sqrt{-1}\}$. Table 2 of [4] gives all equivalence classes of *n-defective* Lehmer pairs for all $6 < n \leq 30$ except $n \neq 8, 10, 12$. In particular,

- there are no 11-defective Lehmer pairs;
- every 13-defective Lehmer pair is equivalent to $((\sqrt{a} + \sqrt{b})/2, (\sqrt{a} - \sqrt{b})/2)$ where $(a, b) = (1, -7)$;
- every 7-defective Lehmer pair is equivalent to $((\sqrt{a} + \sqrt{b})/2, (\sqrt{a} - \sqrt{b})/2)$ where $(a, b) = (1, -7), (1, -19), (3, -5), (5, -7), (13, -3), (14, -22)$.

3 Preliminary descent

Throughout Sects. 3 and 4 we maintain the following assumptions and notation:

(a) C_1 is a squarefree positive integer, C_2 is a positive integer and $\gcd(C_1, C_2) = 1$. We moreover suppose that $C_1C_2 \not\equiv 7 \pmod 8$. We write $C_1C_2 = cd^2$ where c, d are positive integers and c is squarefree.
(b) (x, y) satisfies (5).
(c) p is an odd prime. Moreover, if $p = 3$ then we suppose additionally that $C_1C_2/3$ is not a square.
(d) p does not divide the class number of $\mathbb{Q}(\sqrt{-c})$.

Lemma 3.1 *Let (x, y) be a solution to (5). Let $\mathcal{O}_K$ be the ring of integers for the number field $K = \mathbb{Q}(\sqrt{-c})$. Then there is some $\delta \in \mathcal{O}_K$ such that*

$$C_1x + d\sqrt{-c} = \frac{\delta^p}{C_1^{(p-1)/2}}. \tag{6}$$

Moreover, we have

$$\frac{\delta^p}{C_1^{p/2}} - \frac{\bar{\delta}^p}{C_1^{p/2}} = 2d \cdot \frac{\sqrt{-c}}{\sqrt{C_1}}. \tag{7}$$

Proof Let $K = \mathbb{Q}(\sqrt{-c})$ and $\mathcal{O}_K$ its ring of integers. Let h_K be the class number of K and we assume that $p \nmid h_K$. As $C_1C_2 \not\equiv 7 \pmod 8$ we have that y is odd.

As C_1, c are both squarefree, $\gcd(C_1, C_2) = 1$ and $C_1C_2 = cd^2$ it follows that $C_1 \mid c$. Let $C_1 = p_1 \cdots p_r$ where we note that the primes $p_1, \ldots p_r$ ramify in K.

We factorise Eq. (5) in $\mathcal{O}_K$ as follows:

$$\left(C_1x + d\sqrt{-c}\right)\left(C_1x - d\sqrt{-c}\right) = C_1 \cdot y^p = p_1 \ldots p_r \cdot y^p.$$

Let us write $\mathfrak{p}_i$ for the prime ideal above p_i where $1 \leq i \leq r$. Let $\mathfrak{a} = \mathfrak{p}_1 \ldots \mathfrak{p}_r$ and we obtain

$$\begin{aligned}(C_1x + d\sqrt{-c})\mathcal{O}_K &= \mathfrak{p}_1 \ldots \mathfrak{p}_r \cdot \mathfrak{y}^p \\ &= \mathfrak{a}^{1-p} \cdot (\mathfrak{a}\mathfrak{y})^p \\ &= (C_1^{(1-p)/2}) \cdot (\mathfrak{a}\mathfrak{y})^p,\end{aligned}$$

where $\mathfrak{a}\mathfrak{y}$ is a principal ideal of $\mathcal{O}_K$. Indeed, $[\mathfrak{a}\mathfrak{y}]^p = 1$ in the class group. Therefore the class $[\mathfrak{a}\mathfrak{y}]$ has order dividing p. By assumption $p \nmid h_K$. Thus $\mathfrak{a}\mathfrak{y}$ is principal.

Therefore, we write $\mathfrak{a}\mathfrak{y} = \delta\mathcal{O}_K$. The unit group of $\mathcal{O}_K$ has order 2, 4 or 6, and is therefore p-divisible, unless $p = 3$. However, for $p = 3$ we have assumed that $C_1C_2/3$ is a non-square and therefore $K \neq \mathbb{Q}(\sqrt{-3})$, and so the order of the unit

group is 2 or 4. Thus in all cases the unit group is p-divisible. Thus adjusting δ by an appropriate unit we obtain (6). Subtracting the conjugate from (6), we get

$$\frac{\delta^p}{C_1^{(p-1)/2}} - \frac{\bar{\delta}^p}{C_1^{(p-1)/2}} = 2d\sqrt{-c},$$

which is equivalent to (7). This completes the proof of the lemma. □

Remark If $C_1C_2 \equiv 7 \pmod 8$, then it is possible for y to be even. In that case it is no longer true that we can express $(C_1x+d\sqrt{-c})\mathcal{O}_K$ in the form $\mathfrak{a}\mathfrak{y}^p$ where $\mathfrak{a}^2 = C_1\mathcal{O}_K$.

4 Satisfying the Lehmer condition

Let $K = \mathbb{Q}(\sqrt{-c})$ as before, and consider the extension, L/K, where $L = \mathbb{Q}(\sqrt{-c}, \sqrt{C_1})$. Observe that L/K is trivial if $C_1 = 1$, and is quadratic otherwise. We write $\mathcal{O}_L$ for its ring of integers and set $\alpha = \delta/\sqrt{C_1}$, $\beta = \bar{\delta}/\sqrt{C_1}$. Thus Eq. (7) becomes

$$\alpha^p - \beta^p = 2d \cdot \frac{\sqrt{-c}}{\sqrt{C_1}}. \tag{8}$$

For the remainder of this section, in the case $-c \not\equiv 1 \pmod 4$ we let

$$\delta = r + s\sqrt{-c}, \quad \bar{\delta} = r - s\sqrt{-c}, \tag{9}$$

where r, s are integers. In the case $-c \equiv 1 \pmod 4$ we let

$$\delta = \frac{r + s\sqrt{-c}}{2}, \quad \bar{\delta} = \frac{r - s\sqrt{-c}}{2}, \tag{10}$$

where r and s are either both odd or both even.

Lemma 4.1 *Let α, β be as above. Then, α and β are algebraic integers. Moreover,*

$$\alpha\beta = y, \qquad \sqrt{C_1}x + \sqrt{-C_2} = \alpha^p, \qquad \sqrt{C_1}x - \sqrt{-C_2} = \beta^p.$$

Proof By the proof of Lemma 3.1, $\mathfrak{a}^2 = C_1\mathcal{O}_K$ and so $\sqrt{C_1}\mathcal{O}_L = \mathfrak{a}\mathcal{O}_L$ which divides $\mathfrak{a}\mathfrak{y}\mathcal{O}_L = \delta\mathcal{O}_L$. Hence $\alpha = \delta/\sqrt{C_1}$ is an algebraic integer.

Dividing (6) by $\sqrt{C_1}$ gives $\sqrt{C_1}x+\sqrt{-C_2} = \alpha^p$ and applying complex conjugation gives $\sqrt{C_1}x - \sqrt{-C_2} = \beta^p$. Multiplying the two equations gives $y^p = (\alpha\beta)^p$. But as α, β are complex conjugates, $y, \alpha\beta$ are both positive, so $y = \alpha\beta$ as required. □

Lemma 4.2 *Let α, β be as above. Then, $(\alpha + \beta)^2$ is a non-zero rational integer.*

Proof By Lemma 4.1, $(\alpha+\beta)^2$ is an algebraic integer. However,

$$(\alpha+\beta)^2 = \left(\frac{\delta+\bar{\delta}}{\sqrt{C_1}}\right)^2 = \begin{cases} 4r^2/C_1 & \text{if } -c \not\equiv 1 \pmod 4 \\ r^2/C_1 & \text{if } -c \equiv 1 \pmod 4, \end{cases}$$

and thus $(\alpha+\beta)^2$ is a rational number as well as being an algebraic integer. Thus it is a rational integer.

Next, we suppose that $(\alpha+\beta)^2 = 0$. Then δ is purely imaginary, and (6) implies that $x = 0$. This contradicts our assumption that x is positive. □

The following is immediate from Lemma 4.1.

Lemma 4.3 *Let α, β be as above. Then, $\alpha\beta$ is a non-zero rational integer.*

Lemma 4.4 *Let α, β be as above. Then, $(\alpha+\beta)^2$ and $\alpha\beta$ are coprime. Moreover α/β is not a unit.*

Proof Suppose that $(\alpha+\beta)^2$ and $\alpha\beta$ are not coprime. Then there exists a prime $\mathfrak{q}$ of $\mathcal{O}_L$ which divides both. Thus, $\mathfrak{q} \mid \alpha, \beta$. By Lemma 4.1, $\mathfrak{q} \mid y$ and $\mathfrak{q} \mid (2\sqrt{C_1}x)$. As we saw previously, y must be odd. Hence $\mathfrak{q} \mid y$ and $\mathfrak{q} \mid C_1x^2$, contradicting our coprimality assumption.

Finally suppose α/β is a unit. In particular $\alpha \mid \beta$ and $\beta \mid \alpha$. We claim that α is a unit. Suppose otherwise, and let $\mathfrak{q} \mid \alpha$ be a prime of $\mathcal{O}_L$. Then $\mathfrak{q} \mid \beta$ and we obtain a contradiction as above. Hence α must be a unit and so β is a unit. Therefore $y = \alpha\beta$ is a unit in $\mathbb{Z}$. Thus $y = \pm 1$. This contradicts $C_1x^2 + C_2 = y^p$ and the positivity assumption for the solution. □

Lemmata 4.1, 4.2, 4.3, 4.4 provide a proof to the following:

Proposition 4.5 *Let α, β be as above. Then α and β are algebraic integers. Moreover, $(\alpha+\beta)^2$ and $\alpha\beta$ are non-zero, coprime, rational integers and α/β is not a unit.*

5 Proof of Theorem 1

In this section we prove Theorem 1. We suppose $p > 5$ and $p \nmid h_K$. We would like to show that $(p, y) = (7, 3), (7, 5), (7, 9)$ or there is some prime $q \mid d$, $q \nmid 2c$ such that $p \mid B_q$ where

$$B_q = \begin{cases} q-1 & \text{if } \left(\frac{-c}{q}\right) = 1, \\ q+1 & \text{if } \left(\frac{-c}{q}\right) = -1. \end{cases}$$

Let (α, β) be as above. Proposition 4.5 tells us that (α, β) is indeed a Lehmer pair. We denote by $\tilde{u}_k$ the associated Lehmer sequence. From (9), (10) we have

$$\alpha - \beta = \begin{cases} \frac{2s\sqrt{-c}}{\sqrt{C_1}} & \text{if } -c \not\equiv 1 \pmod 4 \\ \frac{s\sqrt{-c}}{\sqrt{C_1}} & \text{if } -c \equiv 1 \pmod 4. \end{cases} \tag{11}$$

Combining with (8) gives

$$\tilde{u}_p = \frac{\alpha^p - \beta^p}{\alpha - \beta} = \begin{cases} \frac{d}{s} & \text{if } -c \not\equiv 1 \pmod 4, \\ \frac{2d}{s} & \text{if } -c \equiv 1 \pmod 4. \end{cases} \tag{12}$$

We suppose first that (α, β) is not p-defective. Thus there is a prime $q \mid \tilde{u}_p$ such that $q \nmid (\alpha^2 - \beta^2)^2$ and $q \nmid \tilde{u}_1 \tilde{u}_2 \ldots \tilde{u}_{p-1}$. We claim that $q \neq 2$. Suppose $q = 2$. Let $\mathfrak{q}$ be a prime of $\mathcal{O}_L$ dividing q. Then

$$\alpha^p \equiv \beta^p \pmod{\mathfrak{q}}, \qquad \alpha \not\equiv \beta \pmod{\mathfrak{q}}.$$

Hence α/β has order p in $(\mathcal{O}_L/\mathfrak{q})^*$. This group has order $\mathrm{Norm}(\mathfrak{q}) - 1$. As L has degree 4, $\mathrm{Norm}(\mathfrak{q}) = 2$ or 4 or 16. Thus $p = 3$ or 5 which contradicts $p > 5$. Therefore $q \neq 2$.

Next we claim that $q \nmid C_1$. Suppose $q \mid C_1$. Let $\mathfrak{q}$ be a prime of $\mathcal{O}_L$ dividing q. Then $\alpha^p \equiv \beta^p \pmod{\mathfrak{q}}$ and $\sqrt{C_1} \equiv 0 \pmod{\mathfrak{q}}$. By Lemma 4.1, $\mathfrak{q} \mid 2\sqrt{-C_2}$. Hence $q \mid C_1$ and $q \mid (2C_2)$. But C_1, C_2 are coprime and $q \neq 2$ giving a contradiction. Thus $q \nmid C_1$.

From (11), the fact that $q \nmid C_1$ and $q \nmid (\alpha^2 - \beta^2)^2$ we deduce that $q \nmid c$ as required.

Let $\mathfrak{q}$ be a prime of K above q. Then $\delta/\overline{\delta} \not\equiv 1 \pmod{\mathfrak{q}}$ and $(\delta/\overline{\delta})^p \equiv 1 \pmod{\mathfrak{q}}$. If $(-c/q) = 1$ then $\mathbb{F}_{\mathfrak{q}} = \mathbb{F}_q$ and so $p \mid (q-1)$. If $(-c/q) = -1$ then $\mathbb{F}_{\mathfrak{q}} = \mathbb{F}_{q^2}$. However, $\delta/\overline{\delta} \pmod{\mathfrak{q}}$ belongs to the kernel of the norm map $\mathbb{F}_{q^2}^* \to \mathbb{F}_q^*$ which has order $q+1$. Thus in this case, $p \mid (q+1)$. Hence $p \mid B_q$.

To complete the proof we need to consider the case where (α, β) is p-defective. By Theorem 2 and the discussion following it, we know that $p = 7$ or 13. Moreover (α, β) is equivalent to $(\alpha', \beta') = ((\sqrt{a} + \sqrt{b})/2, (\sqrt{a} - \sqrt{b})/2)$ where the possibilities for (a, b) are listed in that discussion. Recall $\alpha/\alpha' = \beta/\beta' \in \{\pm 1, \pm\sqrt{-1}\}$. Moreover, $y = \alpha\beta$. Thus if $\alpha/\alpha' = \beta/\beta' = \pm\sqrt{-1}$ we obtain $y = -\alpha'\beta'$. However, y is positive and $\alpha'\beta'$ is also positive in all cases. Thus $\alpha/\alpha' = \beta/\beta' = \pm 1$. Hence $y = \alpha'\beta' = (a-b)/4$. When $(a, b) = (1, -7), (13, -3), (3, -5)$, we have $y = 2$, 4, 2, respectively. This contradicts our assumption that $C_1 C_2 \not\equiv 7 \pmod 8$. We are reduced to the case where $p = 7$, and $(a, b) = (1, -19), (5, -7), (14, -22)$, which, respectively, give $y = 5, 3, 9$. This completes the proof.

We note in passing that it is not possible to eliminate the cases $p = 7$, $y = 5, 3, 9$. For example, for $p = 7$, $y = 5$, there are 59893 possibilities for a triple (C_1, C_2, x) which satisfies $C_1 x^2 + C_2 = y^p = 5^7$ and all our other restrictions.

6 Effectively determining solutions

In this section, we give an effective method that solves (4) for a given value of $n \geq 3$. We first define a *Thue equation* as a Diophantine equation of the form $f(x, y) = m$, where $f(x, y)$ is a homogenous polynomial of degree at least 3 with integer coefficients and m is a fixed integer. We recall Thue's original finiteness result [21]:

Theorem 3 (Axel Thue 1909) *Thue equations have finitely many integer solutions in* (x, y).

Thue's proof is unfortunately ineffective. However, the past century saw great advances in the effective resolution of Thue equations, most notably Baker's work on linear forms in logarithms and efficiencies gained from the LLL algorithm [13]. The effective resolution of Thue equations is described in great detail in [17] and readily implemented in `Magma` [6].

Let C_1, C_2 satisfy condition (a) of Sect. 3. Theorem 1 gives a list of possible odd prime exponents $n = p$ for which (4) might have solutions. As noted in the introduction, we may without loss of generality suppose that $n = p$ is an odd prime, or that $n = 4$. In this section, we outline a practical method to compute these solutions for fixed such value of n. We consider three cases.

Case I n is an odd prime $p \nmid h_K$, and if $p = 3$ then $C_1C_2/3$ is not a square. In this case the conditions (a)–(d) of Section 3 are all satisfied. Let r, s be as in (9), (10). Let

$$d' = \begin{cases} d & \text{if } -c \not\equiv 1 \pmod 4, \\ 2d & \text{if } -c \equiv 1 \pmod 4. \end{cases}$$

From (12) we obtain $s \mid d'$. Thus we have only a few possibilities for s. To determine the solutions we merely have to determine the possible values of r corresponding to each $s \mid d'$. We shall write down an explicit polynomial $f_s \in \mathbb{Z}[X]$ whose integer roots contain all the possible values of r corresponding to s.

Fix $s \mid d'$. If $-c \not\equiv 1 \pmod 4$, we let

$$f_s(X) = \frac{(X + s\sqrt{-c})^p - (X - s\sqrt{-c})^p}{2s\sqrt{-c}} - \frac{d \cdot C_1^{(p-1)/2}}{s}.$$

Clearly $f_s \in \mathbb{Z}[X]$. Moreover,

$$f_s(r) = \frac{\delta^p - \overline{\delta}^p}{\delta - \overline{\delta}} - \frac{d \cdot C_1^{(p-1)/2}}{s} = 0$$

using (7) and (9).

If $-c \equiv 1 \pmod 4$, we let

$$f_s(X) = \frac{(X + s\sqrt{-c})^p - (X - s\sqrt{-c})^p}{2s\sqrt{-c}} - \frac{2^p \cdot d \cdot C_1^{(p-1)/2}}{s}.$$

Again $f_s \in \mathbb{Z}[X]$ and

$$f_s(r) = \frac{(2\delta)^p - (2\overline{\delta})^p}{2(\delta - \overline{\delta})} - \frac{2^p \cdot d \cdot C_1^{(p-1)/2}}{s} = 0$$

using (7) and (10).

Case II n is an odd prime p, with either $p \mid h_K$ or $p = 3$ and $C_1C_2/3$ is a square. In this case we explain how to reduce (5) to a finite number of Thue equations. These can be solved using standard methods for Thue equations such as in [17]. As in the proof of Lemma 3.1, write $C_1 = p_1 \dots p_r$ and let $\mathfrak{p}_i$ be the unique prime ideal of $\mathcal{O}_K$ above p_i. Let $\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_r$. We have

$$(C_1 x + d\sqrt{-c})\mathcal{O}_K = \mathfrak{a} \cdot \mathfrak{y}^p,$$

where $\mathfrak{y}$ is an ideal of $\mathcal{O}_K$. Let $\mathfrak{b}_1, \dots, \mathfrak{b}_h$ be ideals of $\mathcal{O}_K$ that form a system of representatives for the class group. Then, for some $1 \le i \le h = h_K$, we have $\mathfrak{y}\mathfrak{b}_i$ is principal. Therefore $\mathfrak{a}\mathfrak{b}_i^{-p}$ must be principal. We test the ideals $\mathfrak{a}\mathfrak{b}_i^{-p}$ for principality. Fix i such that $\mathfrak{a}\mathfrak{b}_i^{-p} = \epsilon\mathcal{O}_K$ where $\epsilon \in K^*$ and write $\mathfrak{y}\mathfrak{b}_i = \delta\mathcal{O}_K$, where $\delta \in \mathcal{O}_K$. Then

$$C_1 x + d\sqrt{-c} = \mu \cdot \epsilon \cdot \delta^p, \tag{13}$$

where μ is a unit. If $p \neq 3$ or $C_1C_2/3$ is a non-square, then μ is a p-th power and we can absorb this in the δ^p factor. In this case we suppose $\mu = 1$. Otherwise we also consider $\mu = 1, \omega = (-1 + \sqrt{-3})/2$ and ω^2. We write δ as in (9), (10) depending on whether $-c \not\equiv 1 \pmod 4$ or $-c \equiv 1 \pmod 4$. We then expand (13) and equate the coefficients of $\sqrt{-c}$ and clear denominators to obtain an equation of the form

$$F(r, s) = t,$$

where t is a positive integer, and $F \in \mathbb{Z}[X, Y]$ is a homogeneous polynomial of degree $p \ge 3$. This is a Thue equation. In our implementation we used Magma's inbuilt Thue solver which is an implementation of the algorithm in Smart's book [17, Chapter VII], which is based on linear forms in logarithms.

Case III $n = 4$. We write

$$X = C_1 y^2, \qquad Y = C_1^2 xy,$$

and note that (X, Y) is now an integral point on the elliptic curve

$$Y^2 = X^3 - C_1^2 C_2 X.$$

We apply Magma's inbuilt function for determining integral points on elliptic curves which is based on linear forms in elliptic logarithms, as described in Smart's book [17, Chapter XIII].

7 Solutions

We are interested in solving (4) for $2 \le C_1 \le 10$, $1 \le C_2 \le 80$ subject to the restrictions: C_1 is squarefree, $\gcd(C_1, C_2) = 1$, and $C_1C_2 \not\equiv 7 \pmod 8$. Recall that we are under the assumption $\gcd(C_1x^2, C_2, y^n) = 1$ in (4). As noted previously, we

may without loss of generality suppose that $n = 4$ or that $n = p$ is an odd prime. For each such pair (C_1, C_2), Theorem 1 yields a finite set $S(C_1, C_2)$ of odd primes p for which we need to solve (5). Thus for each such pair (C_1, C_2) we need only solve (4) for $n \in S(C_1, C_2) \cup \{4\}$, and for each such value n we may apply one of the methods explained in Sect. 6. We implemented our approach in `Magma` [6]. The results of our computation are given below.

C_1	C_2	x	y	n
2	1	11	3	5
2	5	13	7	3
2	7	19	9	3
2	13	68	21	3
2	13	41	15	3
2	19	1429	21	5
2	19	33	13	3
2	19	2	3	3
2	23	122	31	3
2	25	1	3	3
2	25	134	33	3
2	27	7	5	3
2	31	5	3	4
2	43	10	3	5
2	47	17	5	4
2	49	4	3	4
2	53	423	71	3
2	53	6	5	3
2	55	441	73	3
2	55	12	7	3
2	73	2	3	4
2	79	1	3	4
3	8	21	11	3
3	10	27	13	3
3	17	6	5	3
3	35	186	47	3
3	43	10	7	3
3	43	712	115	3
3	73	72	25	3
3	80	639	107	3
5	1	4	3	4
5	7	2	3	3
5	14	37	19	3
5	16	43	21	3
5	22	1	3	3
5	23	8	7	3
5	61	2	3	4
5	61	54	11	4
5	61	326	27	4
5	61	326	81	3
5	76	1	3	4
5	76	487	33	4

C_1	C_2	x	y	n
6	1	20	7	4
6	17	45	23	3
6	19	51	25	3
6	29	4	5	3
6	29	185	59	3
6	31	19	13	3
6	71	3	5	3
6	71	378	95	3
6	73	390	97	3
7	13	4	5	3
7	20	53	27	3
7	20	1	3	3
7	22	59	29	3
7	29	10	9	3
7	38	21	5	5
7	53	2	3	4
7	58	9	5	4
7	62	3	5	3
7	68	5	3	5
7	71	92	39	3
7	74	1	3	4
7	78	85	37	3
10	17	1	3	3
10	29	77	39	3
10	31	83	41	3
10	37	122	53	3
10	41	2	3	4
10	43	350	107	3
10	71	1	3	4
10	73	22	17	3

Data Availability Data sharing not applicable to this article as no datasets were generated or analysed during the current study.

References

1. Abu Muriefah, F.S., Luca, F., Siksek, S., Tengely, S.: On the Diophantine equation $x^2 + C = 2y^n$. Int. J. Number Theory **5**(6), 1117–1128 (2009)
2. Bennett, M.A., Skinner, C.M.: Ternary Diophantine equations via Galois representations and modular forms. Can. J. Math. **56**(1), 23–54 (2004)

3. Bérczes, A., Pink, I.: On generalized Lebesgue–Ramanujan–Nagell equations. An. Ştiinţ. Univ. "Ovidius" Constanţa Ser. Mat. **22**, 51–71 (2014)
4. Bilu, Yu., Hanrot, G., Voutier, P.M.: Existence of primitive divisors of Lucas and Lehmer numbers. J. Reine Angew. Math. **539**, 75–122 (2001)
5. Bugeaud, Y., Mignotte, M., Siksek, S.: Classical and modular approaches to exponential Diophantine equations II. Compos. Math. **142**, 31–62 (2006)
6. Bosma, W., Cannon, J., Playoust, C.: The Magma algebra system. I. The user language. J. Symbolic Comput **24**(3—-4), 235–265 (1997)
7. Cohn, J.H.E.: The Diophantine equation $x^2 + C = y^n$. Acta Arith. LXV. **4**, 367–381 (1993)
8. Cohn, J.H.E.: The Diophantine equation $x^2 + C = y^n$. II. Acta Arith. **109**(2), 205–206 (2003)
9. Gebel, J., Pethő, A., Zimmer, G.H.: Computing integral points on elliptic curves. Acta Arith. **68**(2), 171–192 (1994)
10. Ghanmi, N., Abu Muriefah, F.S.: On the Diophantine equation $Cx^2 + D = 2y^q$. Ramanujan J. **53**(2), 389–397 (2020)
11. Le, M., Soydan, G.: A brief survey on the generalized Lebesgue–Ramanujan–Nagell equation. Surv. Math. Appl. **15**, 473–523 (2020)
12. Lebesgue, V.A.: Sur l'impossibilité en nombres entiers de l'équation $x^m = y^2 + 1$. Nouvelles Ann. des Math. **9**, 178–181 (1850)
13. Lenstra, A.K., Lenstra Jr., H.W., Lovász, L.: Factoring polynomials with rational coefficients. Math. Ann. **261**(4), 515–534 (1982)
14. Mignotte, M., de Weger, B.M.M.: On the Diophantine equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$. Glasgow Math. J. **38**(1), 77–85 (1996)
15. Nagell, T.: Lϕsning til oppgave nr 2, 1943, s. 29. Nordisk Mat. Tidskr. **30**, 62–64 (1948)
16. Ramanujan, S.: Question 464. J. Indian Math. Soc. **5**, 120 (1913)
17. Smart, N.: Efficient Resolution of Diophantine Equations, LMSST 41. Cambridge University Press, Cambridge (1998)
18. Stroeker, R.J., Tzanakis, N.: Solving elliptic Diophantine equations by estimating linear forms in elliptic logarithms. Acta Arith. **67**, 177–196 (1994)
19. Tengely, S.: On the Diophantine equation $x^2 + a^2 = 2y^p$. Indag. Math. (N.S.), **15**, 291–304 (2004)
20. Tengely, S.: On the Diophantine equation $x^2 + q^{2m} = 2y^p$. Acta Arith **127**, 71–86 (2007)
21. Thue, A.: Über Annäherungswerte algebraischer Zahlen. J. Reine Angew. Math. **135**, 284–305 (1909)