On differences of perfect powers and prime powers

DOI:
10.48550/arXiv.2312.09985

ON DIFFERENCES OF PERFECT POWERS AND PRIME POWERS

PEDRO-JOSÉ CAZORLA GARCÍA

Abstract. Given a prime number q and a squarefree integer C_1, we develop a method to explicitly determine the tuples (y, n, α) for which the difference $y^n - q^\alpha$ has squarefree part equal to C_1. Our techniques include the combination of the local information provided by Galois representations of Frey–Hellegouarch curves with the effective resolution of Thue–Mahler equations, as well as the use of improved lower bounds for $q-$adic and complex logarithms. As an application of this methodology, we will completely resolve the case when $1 \leq C_1 \leq 20$ and $2 \leq q < 25$.

1. Introduction

1.1. **Historical background.** A very famous conjecture by Catalan [15], stated in 1844, asserts that the only non-zero consecutive integer perfect powers are 8 and 9. In terms of Diophantine equations, this is equivalent to claiming that the Diophantine equation

$$y^n - x^m = 1, \quad x, y, n, m \in \mathbb{Z}, \quad x, y > 0, \quad n, m \geq 2, \tag{1}$$

only has $(x, y, n, m) = (2, 3, 2, 3)$ as a solution. Mihăilescu [32] proved Catalan's conjecture in 2004, using an argument based on the theory of cyclotomic fields and Galois modules.

Even prior to Mihăilescu's proof of Catalan's conjecture, many researchers considered generalisations of (1). For instance, Pillai [40] conjectured that, for any value of $c > 0$, the Diophantine equation

$$y^n - x^m = c, \quad x, y, n, m \in \mathbb{Z}, \quad x, y > 0, \quad n, m \geq 2, \tag{2}$$

has only finitely many solutions provided that $(n, m) \neq (2, 2)$. To date, Pillai's conjecture remains an open problem, and, to the best of our knowledge, there are no results unless at least one of x, y, n or m is fixed.

If both $x = a > 0$ and $y = b > 0$ are fixed, Bennett [6] showed that there are at most two solutions to (2) provided that $a, b \geq 2$. This result built upon work by Pillai himself ([39]) and Herschfeld [23], and has since been generalised by Scott and Styer [42] to allow for x and y to be negative.

Date: December 18, 2023.

2010 *Mathematics Subject Classification.* Primary 11D61, Secondary 11D41, 11D59, 11F80, 11F11.

Key words and phrases. Exponential Diophantine equation, Galois representation, Frey–Hellegouarch curve, Lehmer sequences, modularity, level lowering, linear forms in logarithms, Baker's bounds, Thue–Mahler equation.

If neither x nor y is fixed, much of the existing work is linked to the study of the *Lebesgue–Nagell equation*

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

where $D > 0$ is a fixed integer. We note that (3) corresponds to the case $m = 2$ in (2). In addition, we set $c = D$ for historical reasons. We refer the reader to [26, Section 3] for a detailed exposition on the history of the Lebesgue–Nagell equation and its generalisations.

The Lebesgue–Nagell equation has been an active research topic since its first appearance in a paper by Lebesgue [27] in 1850. Indeeed, we highlight the contributions of Nagell [34, 35], Cohn [17, 18], Mignotte and de Weger [30] and Bennett and Skinner [4], which allowed for a complete resolution of (3) for D in the range $1 \leq D \leq 100$ for all but 19 values.

Amongst the techniques used by these researchers, two will be especially relevant for our work: the theorem on primitive divisors of Lucas–Lehmer sequences by Bilu, Hanrot and Voutier [10] and the modular approach based on Galois representations of Frey–Hellegouarch curves and modular forms, developed by Wiles, Breuil, Conrad, Diamond and Taylor [12, 48, 49].

The resolution of (3) in the range $1 \leq D \leq 100$ was finally completed by Bugeaud, Mignotte and Siksek [14], who dealt with the outstanding 19 cases by using an approach combining the aforementioned modular methodology with lower bounds on linear forms in complex logarithms, based upon Baker's theory [1, 2, 3].

Very recently, the development of a new Thue–Mahler equation solver by Gherga and Siksek [20] has allowed Bennett and Siksek to improve on this combined methodology and study two cases of (3) which we find particularly interesting. In [8], they consider the equation

$$x^2 + 2^{\alpha_2}3^{\alpha_3}5^{\alpha_5}7^{\alpha_7}11^{\alpha_{11}} = y^n, \quad x, y > 0, \quad \alpha_i \geq 0, \quad n \geq 3,$$

to be solved for $x, y, n, \alpha_2, \alpha_3, \alpha_5, \alpha_7$ and α_{11}. Note that the resolution of this equation completely determines which integers are differences of a perfect power and a square, while being furthermore supported only on the primes $2, 3, 5, 7$ and 11. With a similar set of techniques, in [7] the same authors study the Diophantine equation

$$x^2 + q^\alpha = y^n, \quad x, y > 0, \quad \alpha > 0, \quad n \geq 3, \tag{4}$$

where $2 \leq q < 100$ is a fixed prime number. The resolution of this equation completely determines which squares can be written as the difference of a perfect power and a power of q.

Finally, we note that the existing literature on generalisations of the Lebesgue–Nagell equation of the form

$$C_1x^2 + C_2 = y^n, \quad x, y > 0, \quad n \geq 3, \tag{5}$$

where $C_1 \neq 1$ is scarce. The first relevant result in this case is due to Patel [37], who studied (5) for fixed integers $1 \leq C_1 \leq 10$ and $1 \leq C_2 \leq 80$, subject to the additional constraint that $C_1C_2 \not\equiv 7 \pmod 8$. Her methods were similar to those in [18] and thus relied on the primitive divisor theorem.

In work in progress, the author and Patel [16] removed the restriction $C_1C_2 \not\equiv 7 \pmod 8$ and achieved a complete resolution of (5) for all values of C_1 and C_2 in the range $1 \leq C_1 \leq 20$ and $1 \leq C_2 \leq 28$. If $C_1C_2 \equiv 7 \pmod 8$, the primitive divisor theorem is no longer applicable. In these instances, the authors followed

an approach combining the modular methodology with bounds coming from the theory of linear forms in logarithms.

1.2. **The main result.** Our work in this paper extends [7] by considering a generalisation of (4) in the following manner. Given a positive integer C, we can write it as $C = C_1(C')^2$, where C_1 is squarefree, and consider the following Diophantine equation:

$$C_1x^2 + q^\alpha = y^n, \quad x, y > 0, \quad \alpha > 0, \quad n \geq 3, \tag{6}$$

where C_1 is a squarefree integer and q is a prime number, both fixed. We note that, when compared to (2), (6) corresponds to the case $x = q$ and $m = \alpha$. We remark that, at the expense of fixing $x = q$, we can consider all values of c with squarefree part C_1 simultaneously.

Equation (6) will be the main object of study of the present paper. We achieve a complete resolution of (6) in the range $1 \leq C_1 \leq 20$ and $2 \leq q < 25$. This is the main result of the paper and can be concisely stated as follows.

Theorem 1. *Let C_1, q be integers with $1 \leq C_1 \leq 20$ and $2 \leq q < 25$, with C_1 squarefree and q prime. Then, all integer solutions (x, y, α, n) to the equation:*

$$C_1x^2 + q^\alpha = y^n, \quad \gcd(C_1x, q, y) = 1, \quad x, y > 0, \quad \alpha > 0, \quad n \geq 3, \tag{7}$$

can be obtained from Tables 1 and 2.

We note that we can assume that either $n = 4$ or $n = p$ is an odd prime in (7), and so Tables 1 and 2 will only include these solutions. Solutions to (7) with composite n can then be easily read from those tables. Finally, we note that all solutions with $C_1 = 1$ were previously found in [7], but we include them here for completeness.

If $n = 3$ or $n = 4$, the explicit resolution of (6) can be reduced to the determination of $S-$integral points on certain elliptic curves. If $n \geq 5$ and y is odd, we may adapt the techniques developed in [37], which make use of the theorem on primitive divisors of Lehmer sequences, to bound n. For each outstanding value of n, we can then reduce the resolution of (6) to solving a finite number of Thue or Thue–Mahler equations.

After that, we need to deal with the much harder case of (6) where y is even and $n \geq 5$. In this situation, the primitive divisor theorem is no longer applicable, and we will employ an approach combining the resolution of Thue–Mahler equations with the local information provided by the modular method, as well as bounds on n coming from the results of Bugaud and Laurent [13] on lower bounds for linear forms in $q-$adic logarithms and from the newly improved lower bounds on linear forms in complex logarithms, developed by Mignotte and Voutier ([31]).

1.3. **Comparison with previously existing literature.** We now highlight the most relevant innovations in this paper with regards to the previously existing literature. In the case where y is odd, we adapt the methodology in [37] to the case where $C_2 = q^\alpha$, while also introducing several computational improvements. In many cases, and as we shall see in Section 3, this allows us to bypass the resolution of Thue–Mahler equations completely, with very relevant computational savings.

In order to obtain a bound for the exponent n in (7), we develop two methods which are successful in some situations where classical modular method techniques (e.g. Proposition 6.1) fail. These methods are based on similar techniques in work

in progress by the author and Patel [16]. Firstly, we define a new Frey–Hellegouarch curve as the quadratic twist of our original curve by an integer $\ell \mid C_1$, and use it to employ a multi-Frey approach. We present this in Section 6.3. Secondly, given a prime number ℓ, we use basic Galois theory to determine conditions under which the reduction of the Frey–Hellegouarch curve will have full $2-$torsion over $\mathbb{F}_\ell$. In Section 6.4, we explain how to exploit this additional structure to obtain a bound on n.

In Section 7.2, we explain a new way to combine the local information provided by the modular method with Thue–Mahler equations to prove the non-existence of solutions to (6). This is extremely useful in situations where Kraus's method (see Proposition 7.2) fails and where the explicit resolution of Thue–Mahler equations is computationally unfeasible.

Finally, if the modular methodology is unsuccessful in bounding n, we use the newly-improved lower bounds for linear forms in complex logarithms in [31] to bound n. Compared to previous applications of linear forms in logarithms to similar Diophantine equations (e.g. [14, 7, 8]), our bounds are around 50% smaller, giving a substantial saving in computation time. This is presented in Section 8.

1.4. **Structure of the paper.** The outline of this paper is as follows. In Section 2, we will find all solutions of (7) with $n = 3$ and $n = 4$ by reducing the problem to that of finding $S-$integral points on elliptic curves. In Section 3, we find all solutions of (7) with y odd in the range $1 \leq C_1 \leq 20$ and $2 \leq q < 25$ by applying results derived from the theorem on primitive divisors of Lucas-Lehmer sequences ([10]) and by refining the Thue–Mahler solver developed in [20]. In Section 4, we explain how to reduce (7) with y even to a Thue–Mahler equation and we solve the cases $n = 5$ and $n = 7$. In Section 5, we introduce the modular method which we will use in the following two sections to prove that there are almost no remaining solutions. In Section 6, we present four techniques involving the modular method that we may use to bound the exponent n in (7) for some values of C_1 and q. Then, in Section 7, we will develop some methodology to show that (7) has no solutions with y even for a fixed value of $n \geq 11$. In Section 8, we will use the new estimates for linear forms in complex logarithms in [31] in order to bound n and show that all solutions to (7) have been found in previous sections. Finally, in Section 9 we will compile all the previous results to prove Theorem 1.

All the code that we have used to perform computations in this paper is publicly available in https://github.com/PJCazorla/Differences-between-perfect-and-prime-powers.

Acknowledgements The author would like to thank Gareth Jones and Martin Orr for comments on a draft version of the paper, and Adela Gherga and Samir Siksek for useful discussions.

2. Small exponents: $n = 3$ and $n = 4$

In this section, let $S = \{q\}$. We shall explain how to solve (7) for $n = 3$ and $n = 4$ by reducing the problem to that of finding $S-$integral points on certain elliptic curves.

C_1	q	x	y	α	n	C_1	q	x	y	α	n
1	2	5	3	1	3	2	13	75090	2797	9	3
1	2	7	3	5	4	2	17	56	9	2	4
1	2	11	5	2	3	2	19	2	3	1	3
1	3	10	7	5	3	2	19	33	13	1	3
1	3	46	13	4	3	2	19	2981	261	3	3
1	7	1	2	1	3	2	19	1429	21	1	5
1	7	3	2	1	4	2	23	10	9	2	3
1	7	13	8	3	3	2	23	84	11	2	4
1	7	24	5	2	4	2	23	122	31	1	3
1	7	181	32	1	3	3	2	21	11	3	3
1	7	524	65	2	3	3	5	1	2	1	3
1	7	5	2	1	5	3	5	13	8	1	3
1	7	181	8	1	5	3	5	840211	12842	7	3
1	7	11	2	1	7	3	5	3	2	1	5
1	11	2	5	2	3	3	5	1	2	3	7
1	11	4	3	1	3	3	13	1	2	1	4
1	11	58	15	1	3	3	13	9	4	1	4
1	11	9324	443	3	3	3	13	51	10	3	4
1	13	70	17	1	3	3	13	245	82	5	3
1	17	8	3	1	4	3	13	4471	88	1	4
1	19	18	7	1	3	3	17	6	5	1	3
1	19	22434	55	1	5	3	23	208	19	2	4
1	23	2	3	1	3	5	2	43	21	4	3
1	23	588	71	3	3	5	3	1	2	1	3
1	23	6083	78	3	4	5	3	2596	323	7	3
1	23	3	2	1	5	5	3	1	2	3	5
1	23	45	2	1	11	5	3	5	2	1	7
2	3	7	5	3	3	5	3	19	2	5	11
2	3	25	11	4	3	5	7	2	3	1	3
2	3	146	35	5	3	5	11	1	2	1	4
2	3	21395	971	8	3	5	11	7	4	1	4
2	5	1	3	2	3	5	11	57	26	3	3
2	5	13	7	1	3	5	19	3	4	1	3
2	5	134	33	2	3	5	19	14423	1014	5	3
2	7	4	3	2	4	5	23	8	7	1	3
2	7	19	9	1	3	6	11	19	7	4	5
2	7	128060	3201	4	3	6	17	3	7	2	3
2	13	41	15	1	3	6	17	45	23	1	3
2	13	68	21	1	3	6	17	3084	385	2	3
2	13	804	109	3	3	6	19	51	25	1	3

TABLE 1. First part of solutions to (7) with n prime or $n = 4$, $1 \le C_1 \le 20$ and $2 \le q < 25$, with C_1 squarefree, q prime, $x, y > 0$, $\alpha > 0$ and $\gcd(C_1 x, q, y) = 1$.

C_1	q	x	y	α	n
6	23	4	5	2	4
6	23	105378	4057	6	3
6	23	843570	16223	3	3
7	3	1	2	2	4
7	3	5	4	4	4
7	3	38	31	9	3
7	3	430	109	6	3
7	5	1	2	2	5
7	5	17	2	2	11
7	11	1	2	2	7
7	13	4	5	1	3
7	13	7	8	2	3
7	17	21	20	3	3
10	3	1	13	7	3
10	3	71	37	5	3
10	11	474	131	3	3
10	11	646	161	2	3
10	17	1	3	1	3
10	17	48	113	5	3
11	2	1	3	4	3
11	2	85	43	5	3
11	3	2	5	4	3
11	5	1	2	1	4
11	5	8	9	2	3
11	5	19	8	3	4
11	5	19	16	3	3
11	5	59	14	3	4
11	7	1696	75	2	4
11	13	23	18	1	3
11	13	93	46	3	3
11	17	288	97	2	3
11	23	5644	705	2	3
13	2	3	5	3	3
13	2	67	45	15	3
13	3	1	2	1	4
13	3	1	4	5	4
13	3	71	16	1	4
13	5	6668	833	4	3
13	7	342	115	3	3
13	11	31	24	3	3
13	11	3	2	1	7
13	17	60	19	4	4
13	19	42	31	3	3
13	19	1	2	1	5
13	23	12	7	2	4
13	23	1032	61	2	4
14	5	2	3	2	4
14	11	6	5	2	4
14	13	1	3	1	3
14	13	902	225	2	3
14	19	4	3	1	5
15	7	1	4	2	3
15	7	136	23	4	4
15	7	33	4	2	7
15	11	3	4	2	4
15	13	2597	466	4	3
15	13	5124	733	3	3
15	17	1	2	1	5
15	17	7	4	2	5
15	23	103	76	4	3
17	2	1	3	6	4
17	2	9	7	10	4
17	2	231	31	14	4
17	3	8	11	5	3
17	7	1375	318	5	3
17	13	2	3	1	4
17	13	6	5	1	4
17	23	25	22	1	3
19	2	1	3	3	3
19	2	63	43	12	3
19	2	4095	683	9	3
19	2	76539	4931	33	3
19	3	28	25	6	3
19	5	2	3	1	4
19	5	91	54	3	3
19	7	2	5	2	3
19	7	16	17	2	3
19	13	468200376	1608937	6	3
19	13	1	2	1	5

TABLE 2. Second part of solutions to (7) with n prime or $n = 4$, $1 \leq C_1 \leq 20$ and $2 \leq q < 25$, with C_1 squarefree, q prime, $x, y > 0$, $\alpha > 0$ and $\gcd(C_1 x, q, y) = 1$.

Let (x, y, α, n) be a solution to (7) with $n = 3$ and let us write $\alpha = 6k + i$, with $k \geq 0$ and $i \in \{0, 1, \ldots, 5\}$. Let $X = C_1 y/q^{2k}$ and $Y = C_1^2 x/q^{3k}$. Then, it follows that (X, Y) is an $S-$integral point on the elliptic curve

$$E_{C_1,q,i} : Y^2 = X^3 - C_1^3 q^i.$$

Similarly, if (x, y, α, n) is a solution to (7) with $n = 4$, we write $\alpha = 4l + j$ with $l \geq 0$ and $j \in \{0, 1, 2, 3\}$. Let $X = C_1 y^2/q^{2l}$ and $Y = C_1^2 xy/q^{3l}$. Then, (X, Y) is an $S-$integral point on the elliptic curve

$$F_{C_1,q,j} : Y^2 = X^3 - C_1^2 q^j X.$$

For each of these two cases, we may determine all $S-$integral points by using the algorithm presented in [38], based on lower bounds for linear forms in elliptic logarithms and upper bounds on the size of S-integral points of elliptic curves. We shall use the implementation of the algorithm on the computer algebra system `Magma` [11] in order to retrieve all solutions (x, y, α, n) where $x, y > 0$, $\alpha > 0$, $n = 3, 4$ and $\gcd(C_1 x, q, y) = 1$. This algorithm is successful in all but two cases, corresponding to the pairs $(C_1, q) = (7, 23)$ and $(C_1, q) = (19, 23)$ and the elliptic curves

$$E_{7,23,5} : Y^2 = X^3 - 2207665649,$$

and

$$E_{19,23,5} : Y^2 = X^3 - 44146876637.$$

In both cases, the `Magma` subroutine was able to determine that the curves had rank one but was unable to find a generator for the Mordell-Weil group. We can find such an element by computing Heegner points on the curves, following the algorithm of Gross and Zagier [21]. We succeed in both cases and proceed to find the $S-$integral points in the same manner as in the rest of the situations.

In this way, we obtain 164 solutions to (7) with $n = 3$ or $n = 4$, all of which are recorded in Tables 1 and 2.

3. The case where y is odd

In this section, we will solve Equation (7) under the assumption that y is odd. Our main tool to bound the exponent n in (7) is Theorem 1 in [37], which is based upon the theorem of Bilu, Hanrot and Voutier on the existence of primitive divisor of Lucas-Lehmer sequences ([10]). Then, we shall improve upon the computational methodology in [37] to reduce the resolution of (7) with y odd to a finite number of Thue and Thue–Mahler equations.

We can solve the former with the `Magma` in-built Thue solver and the latter with the Thue–Mahler solver developed in [20]. This will allow us to prove the following Proposition, which completely solves (7) if y is odd in the range $1 \leq C_1 \leq 20$ and $2 \leq q < 25$.

Proposition 3.1. *Let (x, y, α, n) be a solution to (7) with $1 \leq C_1 \leq 20$ squarefree, $2 \leq q < 25$ prime, $n \geq 5$, $x > 0$ and y odd. Then,*

$$(C_1, q, x, y, \alpha, n) \in \{(1, 19, 22434, 55, 1, 5), (2, 19, 1429, 21, 1, 5),$$
$$(6, 11, 19, 7, 4, 5), (14, 19, 4, 3, 1, 5)\}$$

and all of this solutions are included in Tables 1 and 2.

Given the results in Section 2, we will assume that $n = p \geq 5$ is a prime. Then, we can bound p by using the following result, which is an extension of Theorem 1 in [37], originally stated in [16]. We include the proof of that result here for convenience.

Theorem 2. *Let C_1 be a positive squarefree integer and C_2 a positive integer. Write $C_1C_2 = cd^2$ where c is squarefree. Let p be an odd prime for which the equation*

$$C_1x^2 + C_2 = y^p, \quad x,\ y > 0, \quad \gcd(C_1x^2, C_2, y^p) = 1,$$

has a solution (x, y), with either $C_1C_2 \not\equiv 7 \pmod 8$ or $C_1C_2 \equiv 7 \pmod 8$ and y is odd. 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) $p \mid \left(\ell - \left(\frac{-c}{\ell}\right)\right)$, where ℓ is some prime $\ell \mid d$ and $\ell \nmid 2c$.

Proof. If $C_1C_2 \not\equiv 7 \pmod 8$, the result follows by [37, Theorem 1]. Otherwise, we have by assumption that $C_1C_2 \equiv 7 \pmod 8$ and y is odd.

In this situation, we can apply the primitive divisor by Bilu, Hanrot and Voutier (BHV) in an identical manner to the proof of Theorem 1 in [37], as the key assumption there is precisely that y is odd. □

We may then apply Theorem 2 to (7), proving the following corollary.

Corollary 3.2. *Let $C_1 > 0$ be a squarefree integer and q a prime number. Suppose that (x, y, α, n) is a solution to (7) with $n = p$ a prime and y odd. Then, either:*

(a) $p \leq 5$, or
(b) $p = 7$ and $y = 3, 5$ or 9, or
(c) α is odd and p divides the class number of $\mathbb{Q}(\sqrt{-C_1q})$, or
(d) α is even and p divides the class number of $\mathbb{Q}(\sqrt{-C_1})$, or
(e) α is even, $q \neq 2$ and $p \mid \left(q - \left(\frac{-C_1}{q}\right)\right)$.

Proof. Conditions (i) and (ii) in Theorem 2 are identical to conditions (a) and (b) in the statement of the corollary, so suppose that none of the two hold. First, let us assume that $\alpha = 2k + 1$ with $k \geq 0$ an integer. Then, in the notation of Theorem 2, it follows that $C_2 = q^\alpha$ and that

$$c = C_1q, \quad d = q^k, \quad k \geq 0. \tag{8}$$

In addition, the only prime $\ell \mid d$ is $\ell = q$, which also divides $2c$. Consequently, condition (iii) on Theorem 2 necessarily holds and we get condition (c) in this corollary.

Suppose now that $\alpha = 2k$ with $k > 0$ an integer. Then, we have that $C_2 = q^\alpha$ and that

$$c = C_1, \quad d = q^k, \quad k > 0, \tag{9}$$

and the only prime $\ell \mid d$, $\ell \nmid 2c$ is $\ell = q$, provided that $q \neq 2$. Then, conditions (iii) and (iv) in Theorem 2 give rise to conditions (d) and (e), finishing the proof of the corollary.

□

We now explain how to adapt the computational methodology in Section 6 of [37] to our case. First, let us treat the case where p does not satisfy (c) or (d) in Corollary 3.2. This case is summarised in the following lemma.

Lemma 3.3. *Suppose that (x, y, α, n) is a solution to (7) with $n = p \geq 5$ prime and y odd. Let c, d be as in (8) if $\alpha = 2k+1$ for some $k \geq 0$ and as in (9) if $\alpha = 2k$ for some $k > 0$. Suppose furthermore that p does not divide the class number of $\mathbb{Q}(\sqrt{-c})$, and let us define $G(U, V) \in \mathbb{Z}[U, V]$ by the following expression:*

$$G(U,V) = \frac{(U + V\sqrt{-c})^p - (U - V\sqrt{-c})^p}{2\sqrt{-c}}. \tag{10}$$

Then, y satisfies

$$y = \frac{r^2 + cs^2}{C_1} \text{ if } -c \not\equiv 1 \pmod 4, \tag{11}$$

or

$$y = \frac{r^2 + cs^2}{4C_1} \text{ if } -c \equiv 1 \pmod 4. \tag{12}$$

and (r, s) satisfy the following non-reduced Thue–Mahler equation:

$$G(r,s) = C_1^{(p-1)/2} q^k, \quad \text{if} -c \not\equiv 1 \pmod 4,$$

or

$$G(r,s) = 2^p C_1^{(p-1)/2} q^k, \quad \text{if} -c \equiv 1 \pmod 4.$$

In addition, we have that $s \in S_{c,q}$, where the set $S_{c,q}$ is defined by:

$$S_{c,q} = \begin{cases} \{\pm 1, \pm q^k\}, & \text{if } -c \not\equiv 1 \pmod 4, \quad q \nmid p, \\ \{\pm 1, \pm q^{k-1}, \pm q^k\}, & \text{if } -c \not\equiv 1 \pmod 4, \quad q \mid p, \\ \{\pm 1, \pm 2, \pm q^k, \pm 2 \cdot q^k\}, & \text{if } -c \equiv 1 \pmod 4, \quad q \nmid 2p, \\ \{\pm 1, \pm 2, \pm q^{k-1}, \pm 2 \cdot q^{k-1}, \pm q^k, \pm 2 \cdot q^k\}, & \text{if } -c \equiv 1 \pmod 4, \quad q \mid p, \quad q \neq 2, \\ \{\pm 1, \pm 2, \ldots, \pm 2^{(p-3)/2}, \pm 2^{(p-1)/2}, \pm 2^{k+1}\}, & \text{if } -c \equiv 1 \pmod 4, \quad q = 2. \end{cases}$$

Proof. Since, by assumption, p does not divide the class number of $\mathbb{Q}(\sqrt{-c})$, this lands into **case I** in [37] and, as shown there, there exist integers r, s satisfying (12) or (11), depending on whether $-c \equiv 1 \pmod 4$ or not. In order to find r and s, we distinguish two cases. If $-c \not\equiv 1 \pmod 4$, we have, again by [37], that $s \mid q^k$ and r satisfies the following equation:

$$0 = f_s(r) = \frac{(r + s\sqrt{-c})^p - (r - s\sqrt{-c})^p}{2s\sqrt{-c}} - \frac{C_1^{(p-1)/2} q^k}{s}. \tag{13}$$

Similarly, if $-c \equiv 1 \pmod 4$, we have that $s \mid 2q^k$ and r satisfies:

$$0 = f_s(r) = \frac{(r + s\sqrt{-c})^p - (r - s\sqrt{-c})^p}{2s\sqrt{-c}} - \frac{2^p C_1^{(p-1)/2} q^k}{s}. \tag{14}$$

Multiplying both equalities by s, we obtain the non-reduced Thue–Mahler equations present in the statement of the Lemma.

Now, let us find the expressions for $S_{c,q}$. Suppose first that $q \nmid 2p$. Then, applying the binomial theorem yields that

$$\frac{(r + s\sqrt{-c})^p - (r - s\sqrt{-c})^p}{2s\sqrt{-c}} = pr^{p-1} + s^2 H(r,s), \tag{15}$$

for certain polynomial $H(r,s) \in \mathbb{Z}[r,s]$. Suppose for contradiction that $q \mid s$ and that $q^k \nmid s$. Then, $q \mid s^2 H(r,s)$ and either

$$q \mid \frac{C_1^{(p-1)/2} q^k}{s} \quad \text{if } -c \not\equiv 1 \pmod 4$$

or

$$q \mid \frac{2^p C_1^{(p-1)/2} q^k}{s} \quad \text{if } -c \equiv 1 \pmod 4.$$

These expressions, together with (13), (14) and (15), yield that $q \mid pr^{p-1}$. Since $q \nmid p$, it follows that $q \mid \gcd(r,s)$. By (11) and (12), along with the fact that C_1 is squarefree, we have that $q \mid y$, which is a contradiction with the fact that $\gcd(q,y) = 1$.

Consequently, either $q \nmid s$ or $q^k \mid s$. Since $s \mid q^k$ for $-c \not\equiv 1 \pmod 4$ and $s \mid 2q^k$ for $-c \equiv 1 \pmod 4$, we get the expressions for $S_{c,q}$ in the statement of the lemma.

If $q \mid p$ and $q \neq 2$, we follow an identical argument to show that either $q \nmid s$ or $q^{k-1} \mid s$. Finally, if $q = 2$, the same reasoning is valid if $-c \not\equiv 1 \pmod 4$. If $-c \equiv 1 \pmod 4$, we may adjust it to prove that either $2^{(p+1)/2} \nmid s$ or $2^{k+1} \mid s$. This gives the expressions for $S_{c,q}$ presented above, thereby concluding the proof. □

Now, we shall explain how to solve the non-reduced Thue–Mahler equation in each of the cases. First, we note that the expression for $G(U,V)$ in (10) can be rewritten as:

$$G(U,V) = V \cdot F(U,V),$$

where $F(U,V) \in \mathbb{Z}[U,V]$ has degree $p-1$. It is sufficient to solve the equation:

$$F(U,V) = \frac{C_1^{(p-1)/2} q^k}{s}, \quad \text{if} - c \not\equiv 1 \pmod 4, \tag{16}$$

or

$$F(U,V) = \frac{2^p C_1^{(p-1)/2} q^k}{s}, \quad \text{if} - c \equiv 1 \pmod 4, \tag{17}$$

for each value of s in $S_{c,q}$. If $s = \pm q^{k-1}, \pm 2 \cdot q^{k-1}, \pm q^k, \pm 2 \cdot q^k$, (16) and (17) reduce to Thue equations, since the right-hand-side of those identities no longer depends on k. We may solve these Thue equations with the `Magma` in-built Thue solver, which is based upon lower bounds on linear forms on elliptic logarithms. Given a solution (U,V) of the relevant Thue equation, it is then elementary to see if there are any values of k for which $V = s$ for our particular choice of s.

We emphasise that, in general, it is much more efficient computationally to solve Thue equations rather than Thue–Mahler equations, so this approach gives a significant improvement.

Suppose now that $s = \pm 1, \pm 2$ (or $s = \pm 1, \pm 2, \ldots, \pm 2^{(p-1)/2}$ in the case $q = 2$). Then, the right-hand side of (16) and (17) does depend on k, so the two expressions are now Thue–Mahler equations. As mentioned above, solving this is, in general, very expensive computationally, so we present a further trick that may allow us to bypass the solution of certain Thue–Mahler equations.

Indeed, let us define $f(U) = F(U,s) \in \mathbb{Z}[U]$ for our fixed value of s. If the polynomial $f(U)$ does not have roots in $\mathbb{Z}_q$, this means that there exists a constant $k_0 \geq 1$ for which the congruence equation

$$F(U,s) \equiv 0 \pmod{q^k}$$

does not have a solution for all $k \geq k_0$. It then follows that all solutions to (16) or (17) satisfy that $k < k_0$ and finding solutions for (16) and (17) amounts to finding roots of polynomials.

If $f(U)$ has roots in $\mathbb{Z}_q$, this trick is no longer possible, so we solve the Thue–Mahler equation with the tools developed in [20]. Given a solution (U, V) to the Thue–Mahler equation, it is then elementary to check whether $V = s$ for our fixed value of s.

Remark 3. Looking at Lemma 3.3, it seems that we have a substantial amount of information for s. One could ask if we could somehow use this information to simplify the computation if we need to solve a Thue–Mahler equation.

Unfortunately, this is apparently not the case, and it seems that we need to solve the Thue–Mahler equation disregarding our partial knowledge of s and then check if the solution (U, V) satisfies $V = s$. We would like to thank Adela Gherga for a very useful discussion on the subject.

The previous approach deals with alternatives (i), (ii) and (v) in Corollary 3.2, so let us consider alternatives (iii) and (iv). In these cases, p divides the class number of $\mathbb{Q}(\sqrt{-c})$, and we can adapt the computational methodology outlined in **Case II** of Section 6 in [37].

Note that, since we have that $d = q^k$, we do not obtain Thue equations as in [37], but Thue–Mahler equations. Indeed, we get $p - 1$ Thue–Mahler equations of degree p, of the following shape.

$$G_2(U, V) = a \cdot q^k, \tag{18}$$

where $G_2(U, V) \in \mathbb{Z}[U, V]$ is a homogeneous polynomial of degree p, $a \in \mathbb{Z}$ and k is such that $\alpha = 2k$ or $\alpha = 2k+1$. Once this equation is solved, there is an associated expression of the form

$$F_2(U, V) = C_1 \cdot a \cdot x, \tag{19}$$

where $F_2(U, V) \in \mathbb{Z}[U, V]$ and U, V and a are the same numbers are in (18). This allows us to recover the value of x in (7).

Note that, as opposed to the case considered in Corollary 3.2, there is no possibility of avoiding the resolution of Thue–Mahler equations, since we do not have any information on the value of s. This is why this case is much more difficult in general.

Note that we need to consider both solutions of (18) where (U, V) are coprime but also those where they are not coprime. In order to solve the first situation, we simply use the Thue–Mahler solver developed in [20], which requires U and V to be coprime.

In the second situation, we need to consider all divisors $d \mid a$ such that $d^p | a$. Then, we solve the equation:

$$G_2(U', V') = \frac{a}{d^p} \cdot q^k,$$

with the Thue–Mahler solver in [20] and assuming that U', V' are coprime. We can then recover the original solution $(U, V) = (dU', dV')$, and find the corresponding value of x by (19).

Finally, we note that the Thue–Mahler solver in [20] requires the polynomial $G_2(U, V)$ in (18) to be irreducible. If this is not the case, we can factorise it as a

product of irreducible coprime factors.

$$G_2(U,V) = a_0 g_1(U,V)\dots g_r(U,V).$$

We may assume, by replacing the value of a in (18) by a/a_0, that $a_0 = 1$. Then, it is sufficient to solve the family of Thue equations:

$$g_i(U,V) = d,$$

where $d|a$ and $\gcd(a/d, d) = 1$. This is a consequence of unique factorisation and simplifies the resolution of the problem significantly, since we only have to deal with Thue equations, as opposed to Thue–Mahler equations. We emphasise that, even if it is not extremely common that G_2 is reducible, it does occur sometimes in practice so we have to account for this possibility.

With all these computational techniques, we are finally able to prove Proposition 3.1.

Proof. (of Proposition 3.1) There are 101 pairs (C_1, q) in the range $1 \leq C_1 \leq 20$ and $2 \leq q \leq 25$ with C_1 squarefree, q prime and $\gcd(C_1, q) = 1$. Note that, for each pair, we have to consider separately the cases where α is odd and where α is even.

Of these 202 cases, we have that p divides the class number of $\mathbb{Q}(\sqrt{-c})$ for precisely 10, and so we land in cases (c) or (d) of Corollary 3.2. We have to solve 4 Thue–Mahler equations of degree 5 for nine of those cases and 6 Thue–Mahler equations of degree 7 for one , giving a total of $9 \cdot 4 + 1 \cdot 6 = 42$ Thue–Mahler equations to consider.

For the remaining 192 pairs, we are able to use the local arguments outlined after the proof of Lemma 3.3 to avoid solving Thue–Mahler equations for 172 of them. The other 20 give rise to a total of 54 Thue–Mahler equations, totalling 96 Thue–Mahler equations amongst all pairs.

We proceed to solve all of them with the code associated to [20]. It is relevant to note that the majority of CPU time is spent solving the 42 Thue–Mahler equations where p divides the class number of $\mathbb{Q}(\sqrt{-c})$ since, on these cases, we have to account for the possibility that (U, V) are not coprime, which forces the resolution of additional Thue–Mahler equations.

After resolving all the equations, we recover only the four solutions in the statement of the Proposition, and all of them are included in Tables 1 and 2. □

4. The case where y is even and $p = 5$ or $p = 7$: reduction to Thue–Mahler equations

After the work in Sections 2 and 3, we are left with the case of (7) where y is even and $n = p \geq 5$ is a prime number. This case is considerably harder because we may no longer use the theorem of Bilu, Hanrot and Voutier [10] on primitive divisors of Lucas-Lehmer sequences, as in Section 3.

We note that, if y is even, a simple modulo 8 argument on (7) allows us to prove that $C_1 q^\alpha \equiv 7 \pmod 8$ and, consequently, either α is odd and (C_1, q) is one of the following pairs:

(20)
$$\begin{aligned}(C_1, q) =&(1,7),(1,23),(3,5),(3,13),(5,3),(5,11),(5,19),(7,17),(11,5),(11,13),\\ &(13,3),(13,11),(13,19),(15,17),(17,7),(17,23),(19,5),(19,13),\end{aligned}$$

or α is even and (C_1, q) is one of the following pairs:

$$(C_1,q) = (7,3),(7,5),(7,11),(7,13),(7,17),(7,19),(7,23) \\ (15,7),(15,11),(15,13),(15,17),(15,19),(15,23). \tag{21}$$

and these are the pairs that we shall consider for the rest of the paper. Even though the pairs $(1,7)$ and $(1,23)$ were solved in [7], our methodology applies to these cases and we will recover the same results.

We shall solve (7) with y even and $p \geq 11$ by using an approach combining the modular method, presented in Section 5, with upper bounds on p coming from the theory of linear forms in complex logarithms, that we shall exploit in Section 8. The success of this methodology has been shown in the following articles, amongst many others: [7], [8], [14].

This leaves only the cases $p = 5$ and $p = 7$, which we treat now by explaining how to reduce (7) to a Thue–Mahler equation. This will allow us to prove the following Lemma, which completely solves (7) in the range $1 \leq C_1 \leq 20$ and $3 \leq q < 25$ if y is even and $p = 5$ or $p = 7$.

Lemma 4.1. *Let C_1, q be integers with $1 \leq C_1 \leq 20$ and $3 \leq q < 25$, with C_1 squarefree and q prime. Then, all positive integer solutions (x, y, α, p) to the equation:*

$$C_1x^2 + q^\alpha = y^p, \quad \gcd(C_1x, q, y) = 1, \quad x, y, \alpha > 0, \quad y \text{ even}, \quad p = 5, 7. \tag{22}$$

are given by the following tuples:

$$(C_1,q,x,y,\alpha,p) = (1,7,5,2,1,5),(1,7,181,8,1,5),(1,7,11,2,1,7),(1,23,3,2,1,5), \\ (3,5,3,2,1,5),(3,5,1,2,3,7),(5,3,1,2,3,5),(5,3,5,2,1,7), \\ (7,5,1,2,2,5),(7,11,1,2,2,7),(13,11,3,2,1,7),(13,19,1,2,1,5), \\ (15,7,33,4,2,4),(15,17,1,2,1,5),(15,17,7,4,2,5),(19,13,1,2,1,5).$$

All of these tuples are included in Tables 1 and 2.

Proof. We let c and d be defined as in (8) if $\alpha = 2k + 1$ and as in (9) if $\alpha = 2k$. Let $K = \mathbb{Q}(\sqrt{-c})$, $\mathcal{O}_K$ denote its ring of integers, $Cl(K)$ its class group and h_K its class number.

We note that, for all pairs in (20) (if α is odd) and (21) (if α is even), we have that $-c \equiv 1 \pmod 4$, so that

$$\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{-c}}{2}\right].$$

Multiplying (22) by C_1 and dividing by 4, we obtain the following ideal factorisation in $\mathcal{O}_K$:

$$\left(\frac{C_1x + q^k\sqrt{-c}}{2}\right)\left(\frac{C_1x - q^k\sqrt{-c}}{2}\right)\mathcal{O}_K = \left(\frac{C_1y^p}{4}\right)\mathcal{O}_K. \tag{23}$$

Since $\gcd(C_1x, y) = 1$, we see that the only prime ideals dividing both ideals on the left-hand side of (23) are those dividing C_1. Consequently, we see that

$$\left(\frac{C_1x + q^k\sqrt{-c}}{2}\right)\mathcal{O}_K = \mathfrak{q}\cdot\mathfrak{p}_2^{p-2}\cdot\mathfrak{A}^p, \tag{24}$$

where $\mathfrak{q}$ is the product of all prime ideals over C_1, $\mathfrak{p}_2$ is one of the two prime ideals over 2 and $\mathfrak{A}$ is an ideal of norm $y/2$.

Let $\{\mathfrak{b}_1, \dots, \mathfrak{b}_{h_K}\}$ be a set of representatives for $Cl(K)$ which are integral ideals. Then, it follows that $\mathfrak{Ab}_i$ is principal for precisely one value of $i = 1, \dots, h_K$. For such an i, we let $\beta \in \mathcal{O}_K$ be a generator of $\mathfrak{Ab}_i$.

If we define $\mathfrak{B} = \mathfrak{q} \cdot \mathfrak{p}_2^{p-2}$, (24) yields that $\mathfrak{B}\mathfrak{b}_i^{-p}$ is a principal fractional ideal, say generated by $\gamma \in K$. Therefore,

$$\left(\frac{C_1 x + q^k\sqrt{-c}}{2}\right)\mathcal{O}_K = (\gamma\beta^p)\,\mathcal{O}_K,$$

and, since the units of $\mathcal{O}_K$ are ± 1 for all cases under consideration, we have that, after possibly replacing β with $-\beta$, (24) is equivalent to

$$C_1 x + q^k\sqrt{-c} = 2\gamma\beta^p, \tag{25}$$

We emphasise that we may compute γ explicitly, while we cannot do the same with β. However, since $\beta \in \mathcal{O}_K$, we may write

$$\beta = U + V \cdot \frac{1+\sqrt{-c}}{2}$$

for some integers U, V. By equating the imaginary parts in (25) and clearing denominators, we get the following expression:

$$a \cdot q^k = F(U, V), \tag{26}$$

where $a \in \mathbb{Z}$ and $F \in \mathbb{Z}[U, V]$ is a homogeneous polynomial of degree p, so that (26) is a Thue–Mahler equation in the variables U, V of degree p. If this equation is resolved, we may recover the solution x simply by equating the real values of the expression (25), giving rise to an expression of the form:

$$bx = G(U, V), \tag{27}$$

for some $b \in \mathbb{Z}$ and certain homogeneous polynomial $G \in \mathbb{Z}[U, V]$ of degree p.

We get one Thue–Mahler equation for each of the pairs in (20) and (21) and each exponent $p = 5$ or $p = 7$. This gives a total of 62 Thue–Mahler equations to consider. With the help of `Magma` and the Thue–Mahler solver developed in [20], we solve all of them and recover the solutions via (27). □

Remark 4. In principle, the previous argument would work for arbitrary p and so, in theory, we could reduce (7) to the resolution of Thue–Mahler equations.

However, solving Thue–Mahler equations of degree $p \geq 11$ is an extremely computationally intensive process, and it is practically impossible to carry out if $p \geq 17$. Even so, it is important to emphasise that the same argument applies for $p \geq 11$ and we will use it, in combination with the modular method, in Section 7.2.

5. The case where y is even and $p > 7$: the modular method

Our main tool to study (7) when y is even and $p \geq 11$ will be the modular method for Diophantine equations. An excellent exposition on the modular method and its applications can be found in [45].

Suppose that (x, y, α, p) is a putative solution to (7) with $p \geq 11$ prime and $x, y, \alpha > 0$, with y even. Then, we can associate the following Frey–Hellegouarch curve to it:

$$F_{x,\alpha} : Y^2 + XY = X^3 + \frac{C_1 x - 1}{4}X^2 + \frac{C_1 y^p}{64}X = X^3 + \frac{C_1 x - 1}{4}X^2 + \frac{C_1^2 x^2 + C_1 q^\alpha}{64}X. \tag{28}$$

This Frey–Hellegouarch curve is obtained by applying the recipes of Bennett and Skinner [4], which build upon the work of Wiles, Breuil, Conrad, Diamond and Taylor [12, 48, 49] on modularity of elliptic curves, on Ribet's level lowering theorem [41], and on Mazur's theorem [29]. The recipes of Bennett and Skinner are also reproduced in [45, Section 14.1].

Let f be a weight 2 newform. Then, following [45], we shall employ the notation $F_{x,\alpha} \sim_p f$ to mean

$$\overline{\rho}_p(F_{x,\alpha}) \cong \overline{\rho}_p(f),$$

where $\overline{\rho}_p(F_{x,\alpha})$ and $\overline{\rho}_p(f)$ are the mod$-p$ Galois representations attached to $F_{x,\alpha}$ and f, respectively. Then, by [45, Theorem 13], we have that either $0 < \alpha < p$ and $y = 1$ (which would correspond to the case of the curve $F_{x,\alpha}$ having complex multiplication) or $F_{x,\alpha} \sim_p f$ where f is a weight 2 newform of level

$$N = \begin{cases} 2qC_1^2 & \text{if } p \nmid \alpha, \\ 2C_1^2 & \text{if } p \mid \alpha. \end{cases} \tag{29}$$

It is straightforward to check that there are no solutions to (7) with $y = 1$, so from now onwards we may assume that $F_{x,\alpha} \sim_p f$.

For any prime number ℓ, we define $a_\ell(F) = \ell + 1 - \#F(\mathbb{F}_\ell)$. Also, we let f have a normalised cuspidal $q-$expansion given by:

$$f = q + \sum_{n=2}^{\infty} c_n q^n, \tag{30}$$

where c_n belong to some number field K_f, with ring of integers $\mathcal{O}_{K_f}$. Then, a standard consequence of the fact that $F_{x,\alpha} \sim_p f$ (see [25] and Propositions 5.1 and 5.2 of [45]) is that there is a prime ideal $\mathfrak{p}$ of $\mathcal{O}_{K_f}$ with $\mathfrak{p} \mid p$ and such that for all primes ℓ, we have that

$$\begin{cases} a_\ell(F) \equiv c_\ell \pmod{\mathfrak{p}} & \text{if } \ell \neq p \text{ and } \ell \nmid Ny, \\ c_\ell \equiv \pm(\ell + 1) \pmod{\mathfrak{p}} & \text{if } \ell \neq 2, p \text{ and } \ell \mid y. \end{cases} \tag{31}$$

Here, the level N is given by (29) and, in both cases, the assumption that $\ell \neq p$ can be removed if the newform is *rational*, that is, if $K_f = \mathbb{Q}$. For each pair (C_1, q) in (20) (if α is odd) and (21) (if α is even), we may use `Magma` to compute the conjugacy classes of rational and irrational newforms of weight 2 and level N that we need to consider.

Then, our aim in Sections 6 and 7 will be to exploit the local information provided by (31) in order to prove the following two Propositions. Note that both propositions together cover all pairs in (20) and (21).

Proposition 5.1. *Let C_1, q, α and p be positive integers with C_1 squarefree, q and p prime numbers and $q \geq 3$. Suppose that one of the following alternatives hold:*

(i) $p \mid \alpha$, *or*

(ii) α *is odd and* (C_1, q) *is one of the following pairs:*

$$(C_1, q) = (5, 19), (7, 17), (11, 13), (13, 19), (15, 17), (17, 7), (17, 23), (19, 5), (19, 13), \tag{32}$$

or,

(iii) α *is even and* (C_1, q) *is one of the following pairs:*

$$(C_1, q) = (7, 17), (7, 19), (15, 13), (15, 19), (15, 23). \tag{33}$$

Then, there are no solutions (x, y, α, p) to (7) with y even and $p \geq 11$.

Proposition 5.2. *Let C_1, q and α be positive integers with C_1 squarefree and $q \geq 3$ prime. Suppose that either α is odd and (C_1, q) is one of the following pairs:*

$$(C_1, q) = (1,7), (1,23), (3,5), (3,13), (5,3), (5,11), (11,5), (13,3), (13,11), \tag{34}$$

or α is even and (C_1, q) is one of the following pairs:

$$(C_1, q) = (7,3), (7,5), (7,11), (7,13), (7,23), (15,7), (15,11), (15,17). \tag{35}$$

Then, define $N_0(C_1, q)$ as follows:

$$N_0(C_1, q) = \begin{cases} 7.234157 \cdot 10^7 & \text{if } (C_1, q) = (1,7), \\ 1.514725 \cdot 10^8 & \text{if } (C_1, q) = (1,23), \\ 3.476178 \cdot 10^7 & \text{if } (C_1, q) = (3,5), \\ 1.243438 \cdot 10^8 & \text{if } (C_1, q) = (3,13), \\ 3.476178 \cdot 10^7 & \text{if } (C_1, q) = (5,3), \\ 8.334595 \cdot 10^7 & \text{if } (C_1, q) = (5,11), \\ 7.234157 \cdot 10^7 & \text{if } (C_1, q) = (7,3), \\ 7.083124 \cdot 10^7 & \text{if } (C_1, q) = (7,5), \\ 7.083124 \cdot 10^7 & \text{if } (C_1, q) = (7,11), \\ 7.236925 \cdot 10^7 & \text{if } (C_1, q) = (7,13), \\ 7.083124 \cdot 10^7 & \text{if } (C_1, q) = (7,23), \\ 8.334595 \cdot 10^7 & \text{if } (C_1, q) = (11,5), \\ 1.273969 \cdot 10^8 & \text{if } (C_1, q) = (13,3), \\ 3.499196 \cdot 10^8 & \text{if } (C_1, q) = (13,11), \\ 3.472013 \cdot 10^7 & \text{if } (C_1, q) = (15,7), \\ 3.472013 \cdot 10^7 & \text{if } (C_1, q) = (15,11), \\ 3.547538 \cdot 10^7 & \text{if } (C_1, q) = (15,17), \end{cases} \tag{36}$$

Then, the only solutions to (7) with y even and $11 \leq p \leq N_0(C_1, q)$ are given by the following tuples:

$$(C_1, q, x, y, \alpha, p) = (1,23,45,2,1,11), (5,3,19,2,5,11), (7,5,17,2,2,11), \tag{37}$$

and they are included in Tables 1 and 2.

Remark 5. In Section 8, we will prove that, in fact, $p < N_0(C_1, q)$ for each of the cases covered in Proposition 5.2. This, in combination with Propositions 5.1 and 5.2, along with our work in previous sections, is enough to finish the proof of Theorem 1.

6. Bounding the exponent p

In this section, we use the modular method to try to attain a sharp bound for the exponent p in (7). We succeed precisely when $p \mid \alpha$ or if (C_1, q) is one of the pairs in (32) (if α is odd) or in (33) (if α is even). In this situation, we avoid a significantly worse bound coming from linear forms in complex logarithms, so there is a very significant computational improvement. We emphasise that the four techniques that we present are used to obtain a sharp bound for the exponent p for at least one pair (C_1, q).

6.1. **A preliminary modular bound.** The first method is quite standard and was originally applied by Serre [43, pp. 203–204]. The version that we present here is an adaptation from that of Bennett and Skinner [4, Proposition 4.3], which is also [45, Proposition 9.1]. This technique exploits the local information provided by (31), along with the fact that the Frey–Hellegouarch curve (28) has a $\mathbb{Q}-$rational point of order 2, in order to obtain a bound on p.

Proposition 6.1. *Suppose that (x, y, α, p) is a solution to (7) with $x, y > 0$, y even and $n = p \geq 11$ prime. Let f be a newform of level N, where N is given in (29), with field of coefficients K_f. Let $F_{x,\alpha}$ be the Frey–Hellegouarch curve in (28) and suppose that $F_{x,\alpha} \sim_p f$. Then, for any prime number $\ell \nmid N$, we define*

$$B'_\ell(f) = \mathrm{Norm}_{K_f/\mathbb{Q}}\left((\ell+1)^2 - c_\ell^2\right) \cdot \prod_{\substack{|a|<2\sqrt{\ell} \\ 2|a}} \mathrm{Norm}_{K_f/\mathbb{Q}}(a - c_\ell).$$

and

$$B_\ell(f) = \begin{cases} B'_\ell(f) & \text{if } f \text{ is rational.} \\ \ell B'_\ell(f) & \text{otherwise.} \end{cases}$$

Then, $p \mid B_\ell(f)$.

Remark 6. It is well-known in the literature (see, for example, the considerations after Proposition 9.1 in [45]) that Proposition 6.1 will succeed in bounding the exponent p if either f is irrational or if f is rational and, via the Modularity Theorem [49], corresponds to an elliptic curve E which is not isogenous to an elliptic curve with a $\mathbb{Q}-$rational point of order 2.

If f is irrational, this is true because $c_\ell \notin \mathbb{Q}$ for infinitely many values of ℓ. Therefore, there exists a prime number ℓ such that $B_\ell(f) \neq 0$ and we can always bound p. If f is rational and the corresponding elliptic curve E is not isogenous to an elliptic curve with a $\mathbb{Q}-$rational point of order 2, we have by [44, IV.6] that the set

$$\{\ell \text{ prime} : 2 \mid c_\ell(E)\}$$

is finite. Therefore, we can always find a prime number ℓ for which $B_\ell(f) \neq 0$ and once more we can bound the exponent p.

Consequently, we shall assume for the remainder of the section that f is a rational newform with corresponding elliptic curve E, and we will write $F_{x,\alpha} \sim_p E$ to mean $F_{x,\alpha} \sim_p f$.

6.2. **An image of inertia argument.** We shall try to disprove $F_{x,\alpha} \sim_p E$ by showing that the corresponding Galois representations have different images for some inertia subgroup of $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$. This approach was originally used in [4] and has been used extensively since (see for example [9] and [33]). We shall use the following proposition, which is Proposition 4.4 in [4].

Proposition 6.2. *(Bennett and Skinner, [4]) Let $\ell \geq 3$ be a prime, $F_{x,\alpha}$ be the Frey–Hellegouarch curve (28) and E be an elliptic curve such that $F_{x,\alpha} \sim_p E$. Then, the denominator of the $j-$invariant $j(E)$ is not divisible by any prime $\ell \neq p$ dividing C_1.*

6.3. **Studying quadratic twists.** In this section, we will prove that certain quadratic twists of the Frey–Hellegouarch curve $F_{x,\alpha}$ are, again, Frey–Hellegouarch curves. Then, we will use the two Frey–Hellegouarch curves together to try to bound the exponent p. The following Proposition goes in this direction and is similar to [16, Proposition 6.3].

Proposition 6.3. *Suppose that (x, y, α, p) is a solution to (7) with y even and $p \geq 17$ prime. Also, let d be an integer dividing C_1 with $d \equiv 1 \pmod 4$. Then, if we denote by $F_{x,\alpha}^{(d)}$ the quadratic twist of the Frey–Hellegouarch curve (28) by d, there exists a newform f' of level N, where N is given by (29), with*

$$F_{x,\alpha}^{(d)} \sim_p f'.$$

Proof. By combining standard facts about quadratic twists (see [46]) with a careful application of Tate's algorithm (see [19]), we may find that the elliptic curve $F_{x,\alpha}^{(d)}$ has an integral model and conductor given by $N' = 2C_1^2 q \operatorname{Rad}_2(y)$ if $p \nmid \alpha$ or $N' = 2C_1^2 \operatorname{Rad}_2(y)$ if $p \mid \alpha$. Here, $\operatorname{Rad}_2(y)$ denotes the product of all odd primes dividing y.

Since $p \geq 17$, a result of Mazur [29] implies that the mod-p Galois representation attached to $F_{x,\alpha}^{(d)}$ will be irreducible if $j_{F_{x,\alpha}^{(d)}} \notin \mathbb{Z}[1/2]$. This is elementary to check and so we conclude that $\overline{\rho}_p(F_{x,\alpha}^{(d)})$ is irreducible.

Then, Ribet's Level Lowering Theorem [41] yields the existence of a newform f' of level N such that

$$\overline{\rho}_p(F_{x,\alpha}^{(d)}) \cong \overline{\rho}_p(f'),$$

which is precisely the definition of $F_{x,\alpha}^{(d)} \sim_p f'$. □

Remark 7. Let us assume that $F_{x,\alpha} \sim_p E$. Then, Proposition 6.3 will give a sharp bound on the exponent p provided that $E^{(d)}$ has a conductor different from N. This is due to the fact that

$$F_{x,\alpha}^{(d)} \sim_p E^{(d)},$$

since the corresponding mod$-p$ Galois representations are

$$\overline{\rho}_p(F_{x,\alpha}) \otimes \left(\frac{d}{\cdot}\right) \quad \text{and} \quad \overline{\rho}_p(E) \otimes \left(\frac{d}{\cdot}\right), \tag{38}$$

where $(d/\cdot)$ denotes the Legendre character. The two Galois representations above are isomorphic because $F_{x,\alpha} \sim_p E$ and, consequently, $\overline{\rho}_p(F_{x,\alpha}) \cong \overline{\rho}_p(E)$. Then, Proposition 6.3 yields that

$$F_{x,\alpha}^{(d)} \sim_p f',$$

or, equivalently,

$$\overline{\rho}_p(F_{x,\alpha}) \otimes \left(\frac{d}{\cdot}\right) \cong \overline{\rho}_p(f') \tag{39}$$

Combining (38) and (39), we get that

$$\overline{\rho}_p(E) \otimes \left(\frac{d}{\cdot}\right) \cong \overline{\rho}_p(f').$$

which amounts to the fact that

$$E^{(d)} \sim_p f'. \tag{40}$$

If the conductor of $E^{(d)}$ is different to the level of f', there will be a prime number ℓ with $a_\ell(E^{(d)}) - c_\ell(f') \neq 0$. In this instance, we can always bound p by using (40) together with the congruence conditions (31).

6.4. **Using Galois theory.** In this section, we aim to use Galois theory to refine the technique in Proposition 6.1. Note that, in that proposition, the condition $2 \mid a$ in the computation of $B'_\ell(f)$ appears merely due to the fact that $F_{x,\alpha}(\mathbb{Q})$ has a point of order 2 and, consequently, $2 \mid \#F_{x,\alpha}(\mathbb{F}_\ell)$ for all finite fields $\mathbb{F}_\ell$. We will use Galois theory to determine conditions for primes ℓ which guarantee that $4 \mid \#F_{x,\alpha}(\mathbb{F}_\ell)$ and, therefore, the condition $2 \mid a$ in Proposition 6.1 can be strengthened to $4 \mid a$. This is the application of the following proposition, which originally appeared as [16, Proposition 6.4] with a more complicated proof.

Proposition 6.4. *Let E be an elliptic curve defined over $\mathbb{Q}$ with discriminant Δ, and let ℓ be a prime of good reduction for E. Furthermore, assume that E has at least one $\mathbb{Q}-$rational point of order 2. Then, the reduced curve $\overline{E}(\mathbb{F}_\ell)$ has full 2-torsion, if, and only if its discriminant Δ is a square mod ℓ.*

Proof. Since the curve E has a $\mathbb{Q}-$rational point of order 2, we may assume that it has a model of the following form:

$$E : y^2 = f(x) = xg(x),$$

for some polynomials $f, g \in \mathbb{Z}[x]$ of degree 3 and 2 respectively. Since isomorphisms between short Weierstrass models of elliptic curves change the discriminant by a square factor (see Chapter 3 of [46]), it is sufficient to prove the claim for curves in this model. In addition, we can check by direct computation that the discriminant Δ of E and the discriminant Δ_g of the polynomial $g(x)$ differ only by a square factor.

Let $\alpha \in \overline{\mathbb{F}_\ell}$ be an element with $\alpha^2 \equiv \Delta_g \pmod{\ell}$ and let K be the splitting field of $\overline{g}(x)$. Since $\overline{g}$ is a quadratic polynomial, we have that

$$K = \mathbb{F}_\ell(\alpha)$$

which means that the polynomial $\overline{g}(x)$ will split completely in $\mathbb{F}_\ell$ if, and only if, the discriminant Δ is a square modulo ℓ. Since roots of $\overline{g}(x)$ correspond to the remaining $2-$torsion elements of $E(\mathbb{F}_\ell)$, we conclude the proof.

□

Remark 8. As stated in the beginning of this section, we will try to compute the quantity $B_\ell(f)$ in Proposition 6.1 for primes ℓ for which the discriminant of the Frey–Hellegouarch curve is a square modulo ℓ. By [45, Theorem 16(a)], this discriminant is given by:

$$\Delta_{F_{x,\alpha}} = -2^{-12} \cdot C_1^3 \cdot q^\alpha \cdot y^{2n},$$

and, therefore, it is clearly sufficient to check whether $-C_1 q$ or $-C_1$ are squares modulo ℓ, depending on whether α is odd or even. For these primes, we have that $4 \mid \#F_{x,\alpha}(\mathbb{F}_\ell)$ by Proposition 6.4 and we can replace the condition $2 \mid a$ in Proposition 6.1 with the stronger condition $4 \mid a$.

6.5. **Applying the techniques.** Let us apply the four techniques presented in this section in order to achieve a bound on p. The following lemma, that we will need to prove Propositions 5.1 and 5.2, records our findings.

(C_1, q)	Level	No. newforms		6.1		6.2	6.3	6.4	Remaining
		Rat.	Irrat.	Rat.	Irrat.				
$(1,7)$	14	1	0	1	0	1	1	1	1
$(1,23)$	46	1	0	1	0	0	0	0	0
$(3,5)$	90	3	0	3	0	2	2	2	2
$(3,13)$	234	5	0	3	0	2	2	2	2
$(5,3)$	150	3	0	3	0	2	2	2	2
$(5,11)$	550	13	1	2	0	2	2	2	2
$(5,19)$	950	5	9	0	0	0	0	0	0
$(7,17)$	1666	14	13	6	0	1	0	0	0
$(11,5)$	1210	13	9	2	0	2	2	2	2
$(11,13)$	3146	16	21	0	0	0	0	0	0
$(13,3)$	1014	7	8	3	0	2	2	2	2
$(13,11)$	3718	20	23	2	0	2	2	2	2
$(13,19)$	6422	10	34	1	0	0	0	0	0
$(15,17)$	7650	68	26	23	0	5	4	0	0
$(17,7)$	4046	20	21	8	0	3	2	0	0
$(17,23)$	13294	12	42	6	0	3	2	0	0
$(19,5)$	3610	9	27	0	0	0	0	0	0
$(19,13)$	9386	14	42	1	0	0	0	0	0

TABLE 3. Number of conjugacy classes of newforms for each pair (C_1, q) where $p \nmid \alpha$, α is odd and p can be sharply bounded with each technique.

(C_1, q)	Level	No. newforms		6.1		6.2	6.3	6.4	Remaining
		Rat.	Irrat.	Rat.	Irrat.				
$(7,3)$	294	7	0	3	0	2	2	2	2
$(7,5)$	490	11	2	3	0	2	2	2	2
$(7,11)$	1078	13	11	5	0	2	2	2	2
$(7,13)$	1274	15	8	3	0	2	2	2	2
$(7,17)$	1666	14	13	6	0	1	0	0	0
$(7,19)$	1862	11	13	0	0	0	0	0	0
$(7,23)$	2254	7	21	7	0	3	2	2	2
$(15,7)$	3150	44	2	24	0	9	8	4	4
$(15,11)$	4950	47	15	20	0	8	4	4	4
$(15,13)$	5850	55	17	25	0	2	0	0	0
$(15,17)$	7650	68	26	23	0	5	4	4	4
$(15,19)$	8550	39	37	26	0	2	0	0	0
$(15,23)$	10350	49	44	23	0	1	0	0	0

TABLE 4. Number of conjugacy classes of newforms for each pair (C_1, q) where $p \nmid \alpha$, α is even and p can be sharply bounded with each technique.

Lemma 6.5. *Let C_1 and q be integers with C_1 squarefree and q prime. Suppose that (x, y, α, p) is a solution to (7) with $x, y > 0$, y even and $p \geq 11$ prime. Then, the following is true:*

C_1	Level	No. newforms		6.1		6.2	6.3	6.4	Remaining
		Rat.	Irrat.	Rat.	Irrat.				
1	2	0	0	0	0	0	0	0	0
3	18	0	0	0	0	0	0	0	0
5	50	2	0	0	0	0	0	0	0
7	98	1	1	1	0	0	0	0	0
11	242	2	4	0	0	0	0	0	0
13	338	6	2	0	0	0	0	0	0
15	450	1	0	1	0	0	0	0	0
17	578	1	8	1	0	0	0	0	0
19	722	6	8	0	0	0	0	0	0

TABLE 5. Number of conjugacy classes of newforms for each value of C_1 where $p \mid \alpha$ and p can be sharply bounded with each technique.

(i) *If $p \mid \alpha$, then $p \leq 19$.*
(ii) *If $p \nmid \alpha$, α is odd and (C_1, q) is one of the pairs in* (32)*, then $p \leq 19$.*
(iii) *If $p \nmid \alpha$, α is even and (C_1, q) is one of the pairs in* (33)*, then $p \leq 47$.*
(iv) *If $p \nmid \alpha$, α is odd and (C_1, q) is one of the pairs in* (34)*, then either $p \leq 19$ or $F_{x,\alpha} \sim_p E_{C_1,q}$, for some $E_{C_1,q}$ whose Cremona reference is recorded in Table 6.*
(v) *If $p \nmid \alpha$, α is even and (C_1, q) is one of the pairs in* (35)*, then either $p \leq 47$ or $F_{x,\alpha} \sim_p E_{C_1,q}$, for some $E_{C_1,q}$ whose Cremona reference is recorded in Table 7.*

Proof. First, let us assume that $p \nmid \alpha$. We then apply the four techniques outlined in this section to all pairs in (20), assuming that α is odd, and to all pairs in (21), assuming that α is even. Results can be seen in Tables 3 and 4 respectively, where we record the number of conjugacy classes of newforms for which a sharp bound was not attained after the application of each technique, as well as the number of conjugacy classes of newforms which we were not able to bound. Note that the pairs in (32) and (33) are precisely those for which a sharp bound is attained, while we were unable to bound p using the modular method alone for the pairs in (34) and (35).

All four techniques were applied one after the other, and so the latter methods were only used if the former were unsuccessful. If one of the techniques were ommitted, at least one of the pairs in (32) or in (33) would be unboundable, and we would then have to appeal to bounds coming from linear forms in logarithms, which entail more intensive and unnecessary computations.

In all situations, an application of the presented methodology yields that $p \leq 19$ for pairs in (32) and that $p \leq 47$ for pairs in (33). For the pairs in (34) and (35), we see in Tables 3 and 4 that there are at most four newforms which are unboundable. For any other newform, the methods outlined successfully yield the same bounds as above. By Remark 6, these remaining newforms are necessarily rational.

Consequently, we may conclude that, for all pairs in (34), either $p \leq 19$ or $F_{x,\alpha} \sim_p E_{C_1,q}$, where the Cremona reference of $E_{C_1,q}$ is given in Table 6. Similarly, we have that, for all pairs in (35), either $p \leq 47$ or $F_{x,\alpha} \sim_p E_{C_1,q}$, where the Cremona reference of $E_{C_1,q}$ is given in Table 7. We note that, by Proposition 6.3, all

the elliptic curves in Tables 6 and 7 are quadratic twists of each other by some $d \mid C_1$.

Finally, we treat the case $p \mid \alpha$. The expression in (29) does not depend on q, so we may try to bound p irrespective of the value of q and α. We apply the four techniques described in this section and record all results in Table 5. We obtain that $p \leq 19$ in all cases.

□

(C_1, q)	$E_{C_1,q}$
(1, 7)	14a1
(1, 23)	46a1
(3, 5)	90a1 or 90b1
(3, 13)	234b1 or 234c1
(5, 3)	150a1 or 150b1
(5, 11)	550g1 or 550l1
(11, 5)	1210a1 or 1210h1
(13, 3)	1014c1 or 1014g1
(13, 11)	3718c1 or 3718r1

TABLE 6. Cremona references for the possible elliptic curves $E_{C_1,q}$ for which $F_{x,\alpha} \sim_p E_{C_1,q}$ in the case where α is odd.

(C_1, q)	$E_{C_1,q}$
(7, 3)	294f1 or 294g1
(7, 5)	490g1 or 490j1
(7, 11)	1078l1 or 1078m1
(7, 13)	1274j1 or 1274m1
(7, 23)	2254d1 or 2254e1
(15, 7)	3150e1, 3150i1, 3150z1 or 3150bd1
(15, 11)	4950e1, 4950g1, 4950bb1, 4950bc1
(15, 17)	7650h1, 7650i1, 7650bo1 or 7650bp1

TABLE 7. Cremona references for the possible elliptic curves $E_{C_1,q}$ for which $F_{x,\alpha} \sim_p E_{C_1,q}$ in the case where α is even.

7. Solving for specific exponents

In this section, we will develop techniques that prove that there are no solutions to (7) with y even for a fixed exponent p. Then, we will apply these techniques in combination with the results in Lemma 6.5 to finish the proof of Propositions 5.1 and 5.2.

Note that, in principle, we could simply solve a degree p Thue–Mahler equation, as explained in Section 4. However, as we have discussed, this gets very computationally intensive and completely impractical for $p \geq 17$.

This is why we will present three techniques that exploit the local information provided by the modular method to prove that there are no solutions to (7) for

a specific exponent p, which are more computationally efficient. Throughout this section, we let p denote a fixed prime exponent.

7.1. **A modification of Kraus's method.** The technique that we present here is a combination of the symplectic method, due to Halberstadt and Kraus (Lemme 1.6 of [22]), along with a different idea by Kraus [24], and is inspired by the method called "Predicting exponents of constants" in [45]. Before presenting the technique, let us prove an auxiliary Lemma, which gives more detail on the structure of the reduction of the Frey–Hellegouarch curve (28) over $\mathbb{F}_\ell$.

Lemma 7.1. *Let (x, y, α, p) be a solution to (7) with y even and $p \geq 11$ prime, and let ℓ be a prime number satisfying the following conditions.*

- $\ell = 2mp + 1$ *for some integer* $m > 0$.
- $\ell \nmid 2qC_1y$.

Also, let β be the unique integer in $\{0, 1, \ldots, 2p-1\}$ satisfying that $\beta \equiv \alpha \pmod{2p}$. Then, there exists a number $\omega \in \{0, 1, \ldots, \ell - 1\}$ satisfying

$$(C_1\omega^2 + q^\beta)^{2m} \equiv 1 \pmod{\ell},$$

such that the reduction of the Frey–Hellegouarch curve $F_{x,\alpha}$ over $\mathbb{F}_\ell$ is either isomorphic to the curve

$$F_{\omega,\beta}/\mathbb{F}_\ell : Y^2 + XY = X^3 + \frac{C_1\omega - 1}{4}X^2 + \frac{C_1^2\omega^2 + C_1q^\beta}{64}X,$$

or a quadratic twist of it by $q \pmod{\ell}$.

Proof. Let us write $\alpha = 2pu+\beta$ for certain integers $u \geq 0$ and $\beta \in \{0, 1, \ldots, 2p-1\}$. Then, and since $\ell \neq q$, we have that $q^{pu} \not\equiv 0 \pmod{\ell}$, and so we may define $\omega = x/q^{pu} \pmod{\ell}$. Then, we see that

$$y^p = C_1x^2 + q^\alpha \equiv q^{2pu}(C_1\omega^2 + q^\beta) \pmod{\ell}.$$

From this, we have that

$$C_1\omega^2 + q^\beta \equiv \left(\frac{y}{q^{2u}}\right)^p \pmod{\ell}, \tag{41}$$

and, since $\ell \nmid y$, it follows that

$$\frac{y}{q^{2u}} \not\equiv 0 \pmod{\ell},$$

and so $(C_1\omega^2 + q^\beta)^{2m} \equiv 1 \pmod{\ell}$ by Fermat's Little Theorem. Now, let $F_{x,\alpha}^{(1/q^{pu})}$ denote the quadratic twist of the Frey–Hellegouarch curve $F_{x,\alpha}$ by $1/q^{pu}$. Then, a standard formula on quadratic twists (see [46]) yields that

$$F_{x,\alpha}^{(1/q^{pu})} : Y^2 + XY = X^3 + \frac{C_1x/q^{pu} - 1}{4}X^2 + \frac{C_1y^p/q^{2pu}}{64}X.$$

Now, over $\mathbb{F}_\ell$, the definition of ω, together with (41), give that

$$F_{x,\alpha}^{(1/q^{pu})} \cong Y^2 + XY = X^3 + \frac{C_1\omega - 1}{4}X^2 + \frac{C_1^2\omega^2 + C_1q^\beta}{64}X,$$

which is precisely the expression of $F_{\omega,\beta}$.

If either q is a square modulo ℓ or u is even, then $F_{x,\alpha} \cong F_{x,\alpha}^{(1/q^{pu})} \cong F_{\omega,\beta}$ over $\mathbb{F}_\ell$. Otherwise, $F_{x,\alpha}$ is a quadratic twist of $F_{\omega,\beta}$ by $q \pmod{\ell}$, as we wanted to show. □

We remark that in Lemma 7.1, the value of β only depends on p and not on ℓ. This is why, in the following Proposition, we shall use different ℓ to show that no β can exist and, consequently, that there are no solutions to (7). This will allow us to rule out most exponents $p \leq 1000$.

Proposition 7.2. *Let (x, y, p, α) be a solution to (7) with y even and $p \geq 11$. Suppose furthermore that $F_{x,\alpha} \sim_p f$ for some newform f with coefficients c_n as in (30) and field of coefficients K_f, with ring of integers $\mathcal{O}_{K_f}$. If $K_f = \mathbb{Q}$, we denote by E the minimal model of the elliptic curve associated to f via the Modularity Theorem [49], and we denote the discriminant of E by $\Delta(E)$.*

Let ℓ be a prime number satisfying the following conditions:

- *$\ell = 2mp + 1$ for some integer $m > 0$.*
- *$\ell \nmid 2qC_1$.*
- *Either $N_{K_f/\mathbb{Q}}(c_\ell^2 - 4) \not\equiv 0 \pmod{p}$ or $-C_1 q^s$ is not a square modulo ℓ, where s is defined as the unique integer in $\{0, 1\}$ satisfying that $s \equiv \alpha \pmod 2$.*

Then, let us define the following sets:

(42)
$$A' = \begin{cases} \left\{a \in \{1, \dots, p-1\} \mid \left(\frac{-3a\nu_2(\Delta(E))\nu_q(\Delta(E))}{p}\right) = 1\right\} & \text{if } K_f = \mathbb{Q} \text{ and } p \nmid \alpha. \\ \{0\} & \text{if } p \mid \alpha. \\ \{0, \dots, p-1\} & \text{if } K_f \neq \mathbb{Q}. \end{cases}$$

(43)
$$A = \{\beta \in \{0, \dots, 2p-1\} \mid \beta \equiv a \pmod{p} \text{ for some } a \in A' \text{ and } \beta \equiv \alpha \pmod 2\},$$

and the following sets which depend on the prime ℓ:

$$\mathcal{X}_\ell = \{(\omega, \beta) \in \{0, \dots, \ell-1\} \times A \mid (C_1\omega^2 + q^\beta)^{2m} \equiv 1 \pmod{\ell}\}, \tag{44}$$

$$\mathcal{Y}_\ell = \{(\omega, \beta) \in \mathcal{X}_\ell \mid N_{K/\mathbb{Q}}(a_\ell(F_{\omega,\beta})^2 - c_\ell^2) \equiv 0 \pmod{p}\} \tag{45}$$

$$\mathcal{Z}_\ell = \{\beta \in \{0, \dots, 2p-1\} \mid (\omega, \beta) \in \mathcal{Y}_\ell \text{ for some } \omega \in \{0, \dots, \ell-1\}\}. \tag{46}$$

Then, we have that:

$$\alpha \pmod{2p} \in \bigcap_\ell \mathcal{Z}_\ell,$$

where the intersection is over all prime numbers ℓ satisfying the conditions outlined in this Proposition. In particular, if

$$\bigcap_\ell \mathcal{Z}_\ell = \emptyset,$$

it follows that there are no solutions (x, y, p, α) to (7).

Proof. Firstly, we need to show that $\alpha \pmod{2p} \in A$. This follows directly by definition except in the case where $K_f = \mathbb{Q}$ and $p \nmid \alpha$. In this situation, we need to apply the symplectic method, as presented in Section 12 of [45] and based on Lemma 1.6 in [22].

In order to apply it, we need the minimal discriminant of the Frey–Hellegouarch curve $F_{x,\alpha}$, which may be computed using Tate's algorithm (see [19]), and is

$$\Delta(F_{x,\alpha}) = -2^{-12} \cdot C_1^3 q^\alpha y^{2p}.$$

Since $p \nmid \alpha$, the conductor of $F_{x,\alpha}$ is $2C_1^2 q\,\mathrm{Rad}_2(y)$, so the primes 2 and q have multiplicative reduction and thus the symplectic method yields that

$$\frac{\nu_2(\Delta(E))\nu_q(\Delta(E))}{(2p\nu_2(y)-12)\alpha}$$

is congruent to a square modulo p. From this, it is immediate to conclude that $\alpha \pmod p \in A'$ and, therefore, that $\alpha \pmod{2p} \in A$.

Now, let ℓ be a prime with the conditions stated in the Proposition. Suppose first that $\ell \mid y$. Then, by (31), we have that

$$c_\ell^2 \equiv (\ell+1)^2 \equiv 4 \pmod{\mathfrak{p}},$$

for some ideal $\mathfrak{p}$ of $\mathcal{O}_{K_f}$ over p. Here, we used the fact that $\ell = 2mp+1$. This is a contradiction with the third condition on ℓ.

Consequently, we have that $\ell \nmid y$. Then, we can use Lemma 7.1 to conclude that $F_{x,\alpha}$ is isomorphic, over $\mathbb{F}_\ell$, to certain quadratic twist of $F_{\omega,\beta}$ for some $(\omega,\beta) \in \mathcal{X}_\ell$ satisfying that $\beta \equiv \alpha \pmod{2p}$.

Since quadratic twists change a_ℓ by a factor of ± 1, it follows that $c_\ell \equiv \pm a_\ell(F_{\omega,\beta}) \pmod{\mathfrak{p}}$ for some prime ideal $\mathfrak{p}$ of $\mathcal{O}_{K_f}$ with $\mathfrak{p} \mid p$, so in particular, we have that

$$N_{K_f/Q}(a_\ell(F_{\omega,\beta})^2 - c_\ell^2) \equiv 0 \pmod p,$$

and, consequently,

$$\alpha \pmod{2p} \in \mathcal{Z}_\ell,$$

just like we wanted to show. □

Remark 9. Note that, if q is a square modulo ℓ, Lemma 7.1 actually yields that $F_{x,\alpha} \cong F_{\omega,\beta}$ over $\mathbb{F}_\ell$, so that the set $\mathcal{Y}_\ell$ in (45) can be replaced by

$$\mathcal{Y}_\ell = \{(\omega,\beta) \in \mathcal{X}_\ell \mid N_{K_f/\mathbb{Q}}(a_\ell(F_{\omega,\beta}) - c_\ell) \equiv 0 \pmod p\}, \tag{47}$$

which can be stronger in certain cases. We shall exploit this in the upcoming Section.

Remark 10. Note that we showed in Lemma 6.5 that either $p \leq 47$ or f is rational and corresponds to an elliptic curve E with a point of order 2. Since the computational complexity of this method increases with p, we shall present a shortcut for the latter case and bigger values of p, which, in many cases, will allow us to completely bypass the computation of $a_\ell(F_{\omega,\beta})$. This is inspired by a similar trick in Lemma 14.3 of [7].

If $p > 47$, we may assume that $F_{x,\alpha} \sim_p E$ for certain elliptic curve E. Since both E and $F_{x,\alpha}$ have a point of order 2, we have that:

$$a_\ell(F_{x,\alpha}) \equiv a_\ell(E) \pmod 2.$$

Now, combining this with the fact that $F_{x,\alpha} \sim_p E$ and Lemma 7.1, we have that

$$a_\ell(F_{\omega,\beta}) \equiv \pm a_\ell(E) \pmod{2p}. \tag{48}$$

On the other hand, the Hasse bounds (see [46]) yield that:

$$|a_\ell(F_{\omega,\beta}) \mp a_\ell(E)| < 4\sqrt{\ell},$$

and, if we furthermore assume that $p^2 > 4\ell$, then (48) implies that $a_\ell(F_{\omega,\beta}) = \pm a_\ell(E)$. In turn, this means that either:

$$\#F_{\omega,\beta}(\mathbb{F}_\ell) = \#E(\mathbb{F}_\ell),$$

or

$$\#F_{\omega,\beta}(\mathbb{F}_\ell) = 2\ell + 2 - \#E(\mathbb{F}_\ell).$$

To check whether any of these two equalities hold for a pair (ω, β), we pick a random point $Q \in F_{\omega,\beta}(\mathbb{F}_\ell)$ and check whether either $\#E(\mathbb{F}_\ell) \cdot Q = 0$ or $(2\ell + 2 - \#E(\mathbb{F}_\ell)) \cdot Q = 0$. If the pair (ω, β) does not pass this test, we do not need to compute $a_\ell(F_{\omega,\beta})$.

7.2. **Combining the modular method with Thue–Mahler equations.** The methodology presented in Proposition 7.2 is successful for the majority of values of $p \leq 1000$. However, it occassionally fails for some values of p which are too large to solve with the Thue–Mahler approach explained in Section 4. Consequently, we present another method that combines the local information from the modular method with Thue–Mahler equations.

Suppose that (x, y, p, α) is a solution to (7) with y even and $p \geq 11$. Then, let us write $\alpha = 2k$ or $\alpha = 2k + 1$, depending on whether α is even or odd. Then, (26) and (27) yield the following system of equations.

$$\begin{cases} aq^k = F(U, V) \\ bx = G(U, V) \end{cases}, \tag{49}$$

for certain $a, b \in \mathbb{Z}$ and $F, G \in \mathbb{Z}[U, V]$ which are homogeneous polynomials of degree p. Let us define $v'(\alpha)$ as the unique integer in $\{0, \ldots, p-1\}$ satisfying that

$$v'(\alpha) \equiv \begin{cases} \alpha/2 \pmod{p} & \text{if } \alpha \text{ is even.} \\ (\alpha - 1)/2 \pmod{p} & \text{if } \alpha \text{ is odd.} \end{cases} \tag{50}$$

It follows that $v'(\alpha)$ is the unique integer in $\{0, \ldots, p-1\}$ congruent to k modulo p, so we may write $k = pu + v'$ for certain $u \geq 0$. Now, if we divide the two equations in (49) by q^{pu} and exploit the fact that both F and G are homogeneous polynomials of degree p, we obtain

$$\begin{cases} aq^{v'} = F(U/q^u, V/q^u) \\ bx/q^{pu} = G(U/q^u, V/q^u). \end{cases} \tag{51}$$

Now, let ℓ be a prime number satisfying the following conditions:

- $\ell = 2mp + 1$ for some integer $m > 0$.
- $\ell \nmid 2qC_1$.

We note that these are the first two conditions presented in Proposition 7.2. Since we excluded the third condition, we now have to take into account the possibility that $\ell \mid y$. Let A' and A be given by (42) and (43). Then, we define the following set.

$$\mathcal{X}'_\ell = \{(\omega, \beta) \in \{0, \ldots, \ell - 1\} \times A \mid C_1\omega^2 + q^\beta \equiv 0 \pmod{\ell}\}.$$

Let $\mathcal{X}_\ell$ be defined as in (44), $\mathcal{Y}_\ell$ as in (47) if q is a square modulo ℓ and as in (45) otherwise. Finally, we let $\mathcal{Z}_\ell$ be defined by (46) with $\mathcal{Y}_\ell$ replaced by $\mathcal{Y}_\ell \cup \mathcal{X}'_\ell$. Then, a quick adaptation of our proofs of Lemma 7.1 and Proposition 7.2 show that:

$$(x/q^{pu} \pmod{\ell}, \quad \alpha \pmod{2p}) \in \mathcal{Y}_\ell \cup \mathcal{X}'_\ell.$$

Consequently, if we reduce (51) modulo ℓ, we find that there exists a pair $(\omega, \beta) \in \mathcal{Y}_\ell \cup \mathcal{X}'_\ell$ such that the following system of congruence equations has a solution $(\tilde{U}, \tilde{V})$

over $\mathbb{F}_\ell^2$:

$$S_{\omega,\beta} : \begin{cases} F(\tilde{U},\tilde{V}) \equiv aq^v \pmod{\ell}, \\ G(\tilde{U},\tilde{V}) \equiv b\omega \pmod{\ell}. \end{cases} \tag{52}$$

where $v = v'(\beta)$ as defined in (50). Then, we can define the following set:

$$\mathcal{W}_\ell = \{\beta \in \mathcal{Z}_\ell \mid \text{ there exists } \omega \text{ with } (\omega,\beta) \in \mathcal{Y}_\ell \cup \mathcal{X}'_\ell$$

$$\text{and } S_{\omega,\beta} \text{ as in (52) has solutions over } \mathbb{F}_\ell^2.\}$$

Our work here shows that, for any solution (x, y, p, α) to (7) with y even and $p \geq 11$, it follows that

$$\alpha \pmod{2p} \in \bigcap_\ell \mathcal{W}_\ell,$$

where the intersection is over all primes ℓ satisfying the conditions outlined above. Consequently, if

$$\bigcap_\ell \mathcal{W}_\ell = \emptyset,$$

it follows that (7) has no solutions (x, y, p, α). This, as we shall see in Section 7.4, allows us to cover many cases of p which were not amenable to Proposition 7.2.

While it seems that it would be sufficient to work only with primes ℓ satisfying the three conditions in Proposition 7.2, we found that allowing $\ell \mid y$ often gave better results. The same is true about extending the definition of $\mathcal{Y}_\ell$ to that in (47), which allows us to cover more cases than the original definition in (45).

7.3. **A method for bigger exponents.** The combination of the two previous techniques is very successful in ruling out the existence of solutions for relatively small exponents ($p < 1000$). Unfortunately, it is very computationally expensive for bigger exponents and is completely unfeasible[1] for $p > 10^5$, which justifies the need for a new methodology, which we present here. This section is a modification of Lemmas 15.5 and 15.6 in [7], and is essentially a refinement of Proposition 7.2 over number fields.

For this, we recover some notation from Section 4. Suppose that (x, y, α, p) is a solution to (7) with y even. Let c be given as in (8), if α is odd, or by (9), if α is even, and let $K = \mathbb{Q}(\sqrt{-c})$, with corresponding ring of integers $\mathcal{O}_K$, class group $Cl(K)$ and class number h_K. We recall that, by (24), we have that

$$\left(\frac{C_1 x + q^k\sqrt{-c}}{2}\right)\mathcal{O}_K = \mathfrak{q}\cdot\mathfrak{p}_2^{p-2}\cdot\mathfrak{A}^p, \tag{53}$$

where $\mathfrak{q}$ is the product of all prime ideals over C_1, $\mathfrak{p}_2$ is one of the two prime ideals over 2 and $\mathfrak{A}$ is some ideal of norm $y/2$.

At this point, it is important to remark that, for all values of C_1 and q under consideration, the group $Cl(K)$ is cyclic and generated by the class of $\mathfrak{p}_2$. Similarly, because $p > 1000$, we certainly have that $p \nmid h_K$ in all cases. These are key ingredients in the proof of the following Lemma, which transforms (53) into an expression about elements in K.

[1]To illustrate this, we note that an application of the previous two techniques to prove the non-existence of solutions to (7) where $C_1 = 3, q = 5$, $p = 1,000,033$ and y is even takes over 107 minutes on a 3 GHz Intel Xeon E5-2623 processor.

Lemma 7.3. *Keeping notation as above, assume that $p > 1000$. Let j be the unique integer in $\{0, 1, \ldots, h_K - 1\}$ satisfying*

$$\mathfrak{q}\mathfrak{p}_2^j = \omega\mathcal{O}_K$$

for certain $\omega \in \mathcal{O}_K$. Let i be the unique integer in $\{0, 1, \ldots, h_K - 1\}$ satisfying

$$pi \equiv -2 - j \pmod{h_K}.$$

Define $\delta \in \mathcal{O}_K$ to be such that $\mathfrak{p}_2^{h_K} = \delta\mathcal{O}_K$ and n^* by the expression

$$n^* = \frac{-2 - j - pi}{h_K}.$$

Then,

$$\frac{C_1 x + q^k\sqrt{-c}}{2} = \omega\gamma^p\delta^{n^*}, \tag{54}$$

for some element $\gamma \in \mathcal{O}_K$ of norm $2^i y$.

Proof. Note that we may rewrite (53) as

$$\left(\frac{C_1 x + q^k\sqrt{-c}}{2}\right)\mathcal{O}_K = \mathfrak{q}\mathfrak{p}_2^{-2}\mathfrak{B}^p, \tag{55}$$

where $\mathfrak{B}$ is some ideal of norm y. Since, as mentioned prior to the statement of this Lemma, $\mathfrak{p}_2$ is a generator for $Cl(K)$, it follows that there are unique integers $i, j \in \{0, \ldots, h_K - 1\}$ satisfying

$$\mathfrak{B}\mathfrak{p}_2^i = \gamma\mathcal{O}_K \quad \text{and} \quad \mathfrak{q}\mathfrak{p}_2^j = \omega\mathcal{O}_K. \tag{56}$$

for some $\gamma, \omega \in \mathcal{O}_K$. Note that since $\mathfrak{B}$ has norm y and $\mathfrak{p}_2$ has norm 2, we have that $N(\gamma) = 2^i y$. Then, it follows from (55) and (56) that $\mathfrak{p}_2^{-2-j-pi}$ is principal. Now, because $\mathfrak{p}_2$ is a generator of $Cl(K)$, we have that $h_K \mid -2-j-pi$, and, consequently, $j \equiv -2-pi \pmod{h_K}$, and so i is the unique integer in $\{0, 1, \ldots, h_K - 1\}$ satisfying $pi \equiv -2 - j \pmod{h_K}$. We may then rewrite (55) as follows.

$$\frac{C_1 x + q^k\sqrt{-c}}{2}\mathcal{O}_K = (\mathfrak{q}\mathfrak{p}_2^j)(\mathfrak{p}_2^i\mathfrak{B})^p\mathfrak{p}_2^{-2-j-pi},$$

and then (54) follows by definition of δ, ω, γ and n^*. □

With the previous Lemma, we are finally able to present a method to prove that there are no solutions to (7) for a given prime p, which is furthermore computationally feasible.

Proposition 7.4. *Let (x, y, p, α) be a solution to (7) with y even and $p > 1000$, and let ω, δ and n^* be given as in Lemma 7.3. Denote by $E = E_{C_1,q}$ the curve given in Table 6 if α is odd or in Table 7 if α is even. Consider a prime number $\ell \nmid 2C_1 q$ satisfying the following conditions:*

(I) $\ell = 2mp + 1$ *for some integer* $m > 0$.
(II) $\left(\frac{-c}{\ell}\right) = 1$, *so that the prime ℓ is split in $K = \mathbb{Q}(\sqrt{-c})$.*
(III) $a_\ell(E)^2 \not\equiv 4 \pmod{p}$.

Then, let $\mathfrak{L}$ be one of the two prime ideals over ℓ in $\mathcal{O}_K$, and let $\mathbb{F}_\mathfrak{L} = \mathcal{O}_K/\mathfrak{L} \cong \mathbb{F}_\ell$ denote the residue field. Let g be a generator of $\mathbb{F}_\mathfrak{L}^*$, define $h = g^p$ and let β and θ be given by

$$\beta \equiv \frac{\overline{\delta}}{\delta} \pmod{\mathfrak{L}} \quad \textit{and} \quad \theta \equiv \frac{\overline{\omega}}{\omega} \pmod{\mathfrak{L}}.$$

We then define the following set:

$$\mathcal{X}_{\ell,p} = \{\theta \cdot \beta^{n^*} \cdot h^j \mid j = 0, 1, \ldots, 2m-1\} \setminus \{\overline{1}\}.$$

For $\tau \in \mathcal{X}_{\ell,p}$, define the following elliptic curve defined over $\mathbb{F}_{\mathfrak{L}} \cong \mathbb{F}_\ell$:

$$E_\tau : Y^2 = X(X+1)(X+\tau).$$

Finally, let $\mathcal{Z}_{\ell,p}$ be the set defined by

$$\mathcal{Z}_{\ell,p} = \{\tau \in \mathcal{X}_{\ell,p} \mid a_{\mathfrak{L}}(E_\tau)^2 \equiv a_\ell(E)^2 \pmod{p}\}.$$

Then, $\mathcal{Z}_{\ell,p} \neq \emptyset$.

Proof. Remember that $F_{x,\alpha} \sim_p E$, where $F_{x,\alpha}$ is the Frey–Hellegouarch curve given in (28). First, we will show that $\ell \nmid y$. Suppose otherwise. Then, the congruence conditions (31) yield that

$$a_\ell(E) \equiv \pm(\ell+1) \pmod{p}.$$

If we combine this with condition (I) on ℓ, we get that

$$a_\ell(E) \equiv \pm 2 \pmod{p},$$

which is a contradiction with condition (III). Consequently, $\ell \nmid y$. Thus, the congruence conditions (31) imply that $a_\ell(F_{x,\alpha}) \equiv a_\ell(E) \pmod{p}$. Note that, apart from the model in 28, $F_{x,\alpha}$ also has the following model:

$$F_{x,\alpha} : Y^2 = X\left(X^2 + \frac{C_1 x}{4}X + \frac{C_1 y^p}{64}\right),$$

which can be rewritten over K as

$$F_{x,\alpha} : Y^2 = X\left(X + \frac{C_1 x + q^k\sqrt{-c}}{8}\right)\left(X + \frac{C_1 x - q^k\sqrt{-c}}{8}\right). \tag{57}$$

By Lemma 7.3, we have that:

$$\frac{C_1 x - q^k\sqrt{-c}}{C_1 x + q^k\sqrt{-c}} = \frac{\overline{\omega}\cdot\overline{\delta}^{n^*}\cdot\overline{\gamma}^p}{\omega\cdot\delta^{n^*}\cdot\gamma^p} = \left(\frac{\overline{\omega}}{\omega}\right)\left(\frac{\overline{\delta}}{\delta}\right)^{n^*}\left(\frac{\overline{\gamma}}{\gamma}\right)^p \equiv \theta\cdot\beta^{n^*}\cdot h^j \pmod{\mathfrak{L}}$$

for some $j = 0, 1, \ldots, 2m-1$. Note that $\theta \cdot \beta^{n^*} \cdot h^j \not\equiv 1 \pmod{\mathfrak{L}}$ since, if this were the case, we would have that $\mathfrak{L} \mid (2q^k\sqrt{-c})\mathcal{O}_K$, which is a contradiction with the fact that $\ell \nmid 2C_1 q$. Therefore, it follows that

$$\frac{C_1 x - q^k\sqrt{-c}}{C_1 x + q^k\sqrt{-c}} \pmod{\mathfrak{L}} \in \mathcal{X}_{\ell,p}.$$

Combining this with (57), we may see that, over $\mathbb{F}_{\mathfrak{L}}$, $F_{x,\alpha}$ is a quadratic twist of E_τ for certain $\tau \in \mathcal{X}_{\ell,p}$. Thus,

$$a_{\mathfrak{L}}(E_\tau)^2 \equiv a_\ell(E)^2 \pmod{p}$$

for some $\tau \in \mathcal{X}_{\ell,p}$ and it readily follows that the set $\mathcal{Z}_{\ell,p}$ is non-empty.

□

Remark 11. In order to show that (7) has no solution for a fixed value of p, it is therefore sufficient to prove that $\mathcal{Z}_{\ell,p} = \emptyset$ for some prime ℓ satisfying conditions (I), (II) and (III) in 7.4.

Note that, in principle, the proof of Proposition 7.4 does not require $p > 1000$ to work. However, we have found that this technique is often unsuccessful in practice

for smaller values of p, forcing us to use the sieving methods developed in Sections 7.1 and 7.2.

7.4. **Finishing the proof of Propositions 5.1 and 5.2.** With the techniques that we have developed in this section, we can finish the proof of Propositions 5.1 and 5.2.

Proof. (of Proposition 5.1) By Lemma 6.5, it is sufficient to consider the range $11 \leq p \leq 19$ for cases (i) and (ii) in the Proposition and the range $11 \leq p \leq 47$ for case (iii). We apply the techniques developed in Sections 7.1 and 7.2 for each value of p in the corresponding ranges. This successfully proves that there are no solutions in all cases but two, corresponding to the tuples

$$(C_1, q, p) = (11, 13, 11), (19, 5, 11),$$

α odd and $p \nmid \alpha$. Consequently, we need to solve two Thue–Mahler equations of degree 11, as in Section 4. Once more, we employ the Thue–Mahler solver developed in [20] and recover no solutions to (7), finishing the proof of the Proposition. □

Proof. (of Proposition 5.2) By Lemma 6.5, for all pairs in (34), corresponding to α odd, we have that either $p \leq 19$ or $F_{x,\alpha} \sim_p E_{C_1,q}$ for the curves $E_{C_1,q}$ given in Table 6. We deal with the first case identically as in the proof of Proposition 5.1. For the second case, we employ the methodology presented in Sections 7.1 and 7.2 for $11 \leq p < 1000$ and Proposition 7.4 for $1000 < p < N_0(C_1, q)$. We performed the computation on a 3 GHz Intel Xeon E5-2623 and the necessary times are recorded on Table 8. This method is successful in all but two cases, corresponding to the tuples

$$(C_1, q, p) = (1, 23, 11), (5, 3, 11).$$

The resolution of the corresponding Thue–Mahler equations gives rise to the following solutions:

$$(C_1, q, x, y, \alpha, p) = (1, 23, 1, 5, 1, 11), (5, 3, 19, 2, 5, 11).$$

Similarly, if α is even, Lemma 6.5 yields that, for all pairs in (35), either $p \leq 47$ or $F_{x,\alpha} \sim_p E_{C_1,q}$ for the curves $E_{C_1,q}$ in Table 7. We follow the same computational approach, where the CPU times on the same processor as above are recorded in Table 9. We succeed in all cases except two, corresponding to the pairs

$$(C_1, q, p) = (7, 5, 11), (7, 23, 11),$$

and whose corresponding Thue–Mahler equations gives rise only to the solution

$$(C_1, q, x, y, \alpha, p) = (7, 5, 17, 2, 2, 11).$$

Since the three solutions that we recovered are precisely those in (37), we conclude the proof of the Proposition. □

8. Linear forms in logarithms

After proving Propositions 5.1 and 5.2, our aim in this section is to prove that, for pairs in (34) and (35), we have that $p < N_0(C_1, q)$, therefore completing the proof of Theorem 1. This is the content of Proposition 8.1, which will be the main result in this section.

Throughout this section, and by Proposition 5.2, we shall assume that $p > 3 \cdot 10^7$ in all cases.

(C_1, q)	CPU time needed to get to $N_0(C_1, q)$
$(1, 7)$	22.96 hours
$(1, 23)$	54.26 hours
$(3, 5)$	10.47 hours
$(3, 13)$	43.55 hours
$(5, 3)$	13.51 hours
$(5, 11)$	32.89 hours
$(11, 5)$	33.65 hours
$(13, 3)$	51.60 hours
$(13, 11)$	168.55 hours

TABLE 8. Required time to prove that there are no solutions for $11 \leq p < N(C_1, q)$ for α odd.

(C_1, q)	CPU time needed to get to $N_0(C_1, q)$
$(7, 3)$	27.37 hours
$(7, 5)$	27.13 hours
$(7, 11)$	27.35 hours
$(7, 13)$	26.95 hours
$(7, 23)$	22.36 hours
$(15, 7)$	14.02 hours
$(15, 11)$	13.87 hours
$(15, 17)$	13.87 hours

TABLE 9. Required time to prove that there are no solutions for $11 \leq p < N(C_1, q)$ for α even.

Proposition 8.1. *Let (C_1, q) be one of the pairs in (34), if α is odd, or in (35), if α is even and let (x, y, p, α) be a solution to (7) with y even. Then, $p < N_0(C_1, q)$, where $N_0(C_1, q)$ is given in (36).*

In order to prove this, we will need to use the new estimates on lower bounds on linear forms in three complex logarithms available in [31], as well as estimates on linear forms in q-adic logarithms, following [7]. Before that, we shall build upon our work in Section 7.3 to prove the following lemma.

Lemma 8.2. *Let (x, y, α, p) be a solution to (7) with y even and $p > 3 \cdot 10^7$. Let $c, K, \mathcal{O}_K$, h_K and $\mathfrak{p}_2$ be given as in Section 7.3, and define s to be the smallest positive integer such that the ideal $\mathfrak{p}_2^{2s}$ is principal, say generated by $\delta \in \mathcal{O}_K$. Then,*

$$\left(\frac{C_1 x - q^k \sqrt{-c}}{C_1 x + q^k \sqrt{-c}} \right)^s = \beta \cdot \gamma^p,$$

for some $\gamma \in K$ and $\beta \in K$ given by

$$\beta = \frac{\delta}{\overline{\delta}}. \tag{58}$$

Proof. By (55), we have that

$$\left(\frac{C_1 x + q^k \sqrt{-c}}{2} \right) \mathcal{O}_K = \mathfrak{q} \mathfrak{p}_2^{-2} \mathfrak{B}^p,$$

where $\mathfrak{q}$ is the product of all prime ideals over C_1 and $\mathfrak{B}$ is some ideal of norm y. Then, we see that

$$\left(\frac{C_1x - q^k\sqrt{-c}}{C_1x + q^k\sqrt{-c}}\right)\mathcal{O}_K = \left(\frac{\mathfrak{p}_2}{\overline{\mathfrak{p}_2}}\right)^2\left(\frac{\overline{\mathfrak{B}}}{\mathfrak{B}}\right)^p,$$

so that, by definition of β, we have that

$$\left(\frac{C_1x - q^k\sqrt{-c}}{C_1x + q^k\sqrt{-c}}\right)^s\mathcal{O}_K = \beta\mathcal{O}_K\cdot\left(\frac{\overline{\mathfrak{B}}}{\mathfrak{B}}\right)^{sp}. \tag{59}$$

It readily follows that the fractional ideal

$$\left(\frac{\overline{\mathfrak{B}}}{\mathfrak{B}}\right)^{sp}$$

is principal. However, since $p > 3\cdot 10^7$, p does not divide the class number h_K for any of the cases under consideration. Consequently, the ideal

$$\left(\frac{\overline{\mathfrak{B}}}{\mathfrak{B}}\right)^{s}$$

is principal, say generated by $\gamma \in K$. This, combined with (59), shows that:

$$\left(\frac{C_1x - q^k\sqrt{-c}}{C_1x + q^k\sqrt{-c}}\right)^s = \pm\beta\gamma^p,$$

since the units of $\mathcal{O}_K$ are ± 1. Replacing γ by $-\gamma$ if necessary, this finishes the proof. □

Remark 12. As we mentioned immediately before Lemma 7.3 in Section 7.3, $\mathfrak{p}_2$ is a generator for $Cl(K)$, so either $s = h_K$ (if h_K is odd) or $s = h_K/2$.

In order to obtain a bound for the exponent p, we need a lower bound for y, which is given in the following Lemma. Its proof is identical to [7, Lemma 6.1], so we omit it.

Lemma 8.3. *Let (x, y, α, p) be a solution to (7), with y even and where y is not a power of 2. Then, we have that*

$$y > 4p - 4\sqrt{2p} + 2.$$

We note that we can safely assume that y is not a power of 2. This is because, if $y = 2^m$, then the Frey–Hellegouarch curve $F_{x,\alpha}$ given in (28) has conductor equal to $2C_1^2q$ and minimal discriminant given by $\Delta = -2^{2pm-12}\cdot C_1^3q$ and so we can determine m simply by inspecting Cremona's tables ([19]) for the corresponding conductor. All these solutions were previously obtained in Sections 4 and 7.

8.1. **Linear forms in q-adic logarithms.** In order to obtain an upper bound for p using the tools in [31], we previously need an upper bound for α. For this, we need to appeal to upper bounds on linear forms in q-adic logarithms, as in the following lemma.

Lemma 8.4. *Let (x, y, p, α) be a solution to (7) with y even, $p > 3\cdot 10^7$ and $\alpha = 2k$ or $\alpha = 2k+1$. Also, let s and $K = \mathbb{Q}(\sqrt{-c})$ be defined as in Lemma 8.2.*

In the notation of Theorem 10 in [7]*, let f be the residual degree of the extension $\mathbb{Q}_q(-c)/\mathbb{Q}_q$, and let $D = [\mathbb{Q}_q(-c) : \mathbb{Q}_q]/f$. Finally, let A_2 be given by:*

$$\log(A_2) = \max\left\{ s\log(2), \frac{\log(q)}{D} \right\}.$$

Then, we have that

$$k \leq \frac{48qs}{\log^4(q)} \frac{q^f - 1}{q-1} D^2 \log(A_2) \max\{\log(p) + \log(\log(q)) \\ - \log(D\log(A_2)) + 0.401, 5\log(q)\}^2 \log(y).$$

Proof. By Lemma 8.2, we have that

$$\left(\frac{C_1 x - q^k\sqrt{-c}}{C_1 x + q^k\sqrt{-c}} \right)^s - 1 = \beta\gamma^p - 1.$$

Now, we may rewrite the left-hand side of this equality as

$$\left(\frac{C_1 x - q^k\sqrt{-c}}{C_1 x + q^k\sqrt{-c}} \right)^s - 1 = \left(\frac{-2q^k\sqrt{-c}}{C_1 x + q^k\sqrt{-c}} \right) \sum_{i=0}^{s-1} \left(\frac{C_1 x - q^k\sqrt{-c}}{C_1 x + q^k\sqrt{-c}} \right)^i. \tag{60}$$

We note that, by (58), $\beta \in K$ satisfies $\beta\overline{\beta} = 1$ and is supported only on primes above 2, while the proof of Lemma 8.2 shows that γ is supported only on primes above y. Since y is even and $\gcd(q, y) = 1$, it follows that $\nu_{\mathfrak{q}}(\beta) = \nu_{\mathfrak{q}}(\gamma) = 0$. Then, multiplying (60) by $\overline{\beta}$ and using the fact that $\gcd(C_1 x, q) = 1$ yields that

$$\nu_{\mathfrak{q}}(\gamma^p - \overline{\beta}) \geq k,$$

and it is therefore sufficient to obtain an upper bound for $\nu_{\mathfrak{q}}(\gamma^p - \overline{\beta})$. For this purpose, we shall use Theorem 10 in [7], which is due to Bugeaud and Laurent and was originally presented in [13]. In the notation of this result, we let

$$\alpha_1 = \gamma, \quad \alpha_2 = \overline{\beta}, \quad b_1 = p, \quad b_2 = 1.$$

By Lemma 13.2 of [14], we can compute the absolute logarithmic heights of γ and $\overline{\beta}$ and see that

$$h(\gamma) = \frac{s}{2}\log(y) \quad \text{and} \quad h(\overline{\beta}) = s\log(2),$$

and, consequently, in the notation of Theorem 10 in [14], we may select the appropiate parameters as follows.

$$\log(A_1) = \max\left\{ h(\gamma), \frac{\log(q)}{D} \right\} = \frac{s}{2}\log(y),$$

by the lower bounds on y given in Lemma 8.3. Similarly,

$$\log(A_2) = \max\left\{ h(\overline{\beta}), \frac{\log(q)}{D} \right\} = \max\left\{ s\log(2), \frac{\log(q)}{D} \right\},$$

which is precisely the expression for $\log(A_2)$ given in the statement of this Lemma. Then, an application of Theorem 10 in [7] yields that

$$\nu_{\mathfrak{q}}(\gamma^p - \overline{\beta}) \leq \frac{12qs}{\log^4(q)} \frac{q^f - 1}{q-1} D^4 \log(A_2) \\ \max\left\{ \log(b') + \log(\log(q)) + 0.4, \frac{10}{D}\log(q) \right\}^2 \log(y). \tag{61}$$

where b' is given by

$$b' = \frac{p}{D\log(A_2)} + \frac{2}{Ds\log(y)}.$$

Note that the lower bound on y given by Lemma 8.3, combined with the fact that $p > 3\cdot 10^7$, give that:

$$b' \leq \frac{1.001}{D\log(A_2)}p,$$

and hence

$$\log(b') \leq \log(p) - \log(D\log(A_2)) + \log(1.001) \leq \log(p) - \log(D\log(A_2)) + 0.001.$$

If $D = 2$, combining this with (61) directly gives the desired result. If $D = 1$, the result follows from the observation that

$$\max\left\{\log(b') + \log(\log(q)) + 0.4, 10\log(q)\right\}^2 \leq \\ 4\max\left\{\log(b') + \log(\log(q)) + 0.4, 5\log(q)\right\}^2.$$

□

An immediate application of this Lemma is the following Corollary, which gives a lower bound for y^p in terms of c, q and k. We will need this in Section 8.2 to bound p.

Corollary 8.5. *Suppose that (x, y, α, p) is a solution to (7) where y is even and $p > 3\cdot 10^7$. Let $c = C_1 q$ if $\alpha = 2k+1$ and $c = C_1$ if $\alpha = 2k$. Then*

$$y^p > 100cq^{2k}.$$

Proof. Suppose for contradiction that $y^p \leq 100cq^{2k}$. Then, taking logarithms yields that

$$p\log(y) \leq \log(100) + \log(c) + 2k\log(q) \leq 2\log(10) + \log(C_1) + (2k+1)\log(q),$$

because $c \leq C_1 q$. Then, by Lemma 8.4, we have that

$$p \leq \frac{2\log(10)}{\log(y)} + \frac{\log(C_1)}{\log(y)} + \frac{\log(q)}{\log(y)} + \frac{96qs}{\log^3(q)}\frac{q^f - 1}{q-1}D^2\log(A_2)\cdot \\ \max\{\log(p) + \log(\log(q)) - \log(D\log(A_2)) + 0.401, 5\log(q)\}^2\log(y)$$

Using the lower bounds for y given in Lemma 8.3, we show that, for all the pairs in (34) and (35), $p \leq 10^7$. This is a contradiction with the assumption that $p > 3\cdot 10^7$, and so $y^p > 100cq^{2k}$. □

8.2. **Linear forms in complex logarithms.** Before applying the results on lower bounds on linear forms on three complex logarithms available in [31], we need to define the linear forms in logarithms that we shall be considering and find an upper bound for it. Using Lemma 8.2, we may do so now. Let Δ_2 be given by

$$\Delta_2 = s\log\left(\frac{C_1 x - q^k\sqrt{-c}}{C_1 x + q^k\sqrt{-c}}\right) = p\log(\varepsilon_1\gamma) + \log(\varepsilon_2\beta) + j\pi i, \tag{62}$$

where we consider the principal branches of the logarithm and $\varepsilon_2 \in \{\pm 1\}$ is chosen such that $|\log(\varepsilon_2\beta)| < \pi/2$, $\varepsilon_1 \in \{\pm 1\}$ is chosen such that $\log(\varepsilon_1\gamma)$ and $\log(\varepsilon_2\beta)$ have opposite signs and j is such that the quantity $|\Delta_2|$ is minimal. With this, we are able to prove the following Lemma.

Lemma 8.6. *Let (x, y, p, α) be a solution to (7), with y even and $p > 3 \cdot 10^7$. Then, either:*

- *α is odd and*

$$\log(|\Delta_2|) \leq \begin{cases} -0.49p\log(y) + 385.38\log(y) + 1.79 & \text{if } (C_1, q) = (1, 7), \\ -0.48p\log(y) + 1264.35\log(y) + 3.48 & \text{if } (C_1, q) = (1, 23), \\ -0.49p\log(y) + 486\log(y) + 2.17 & \text{if } (C_1, q) = (3, 5), \\ -0.49p\log(y) + 718.20\log(y) + 3.34 & \text{if } (C_1, q) = (3, 13), \\ -0.49p\log(y) + 784.34\log(y) + 2.17 & \text{if } (C_1, q) = (5, 3), \\ -0.49p\log(y) + 670\log(y) + 3.51 & \text{if } (C_1, q) = (5, 11), \\ -0.49p\log(y) + 469.25\log(y) + 3.51 & \text{if } (C_1, q) = (11, 5), \\ -0.48p\log(y) + 272.28\log(y) + 3.34 & \text{if } (C_1, q) = (13, 3), \\ -0.47p\log(y) + 1003.74\log(y) + 4.91 & \text{if } (C_1, q) = (13, 11), \end{cases}$$

- *or α is even and*

$$\log(|\Delta_2|) \leq \begin{cases} -0.49p\log(y) + 3900.88\log(y) + 1.79 & \text{if } (C_1, q) = (7, 3), \\ -0.49p\log(y) + 1458\log(y) + 1.79 & \text{if } (C_1, q) = (7, 5), \\ -0.49p\log(y) + 182.46\log(y) + 1.79 & \text{if } (C_1, q) = (7, 11), \\ -0.48p\log(y) + 2613.88\log(y) + 1.79 & \text{if } (C_1, q) = (7, 13), \\ -0.49p\log(y) + 223.36\log(y) + 1.79 & \text{if } (C_1, q) = (7, 23), \\ -0.49p\log(y) + 1541.51\log(y) + 2.165 & \text{if } (C_1, q) = (15, 7), \\ -0.49p\log(y) + 364.92\log(y) + 2.165 & \text{if } (C_1, q) = (15, 11), \\ -0.48p\log(y) + 2189.48\log(y) + 2.165 & \text{if } (C_1, q) = (15, 17), \end{cases}$$

Proof. Let us begin by defining Δ' and Δ by the following expressions.

$$\Delta' = \frac{C_1 x - q^k\sqrt{-c}}{C_1 x + q^k\sqrt{-c}}, \quad \Delta = \log(\Delta').$$

We note that

$$|\Delta' - 1| = \left|\frac{C_1 x - q^k\sqrt{-c}}{C_1 x + q^k\sqrt{-c}} - 1\right| = \frac{2q^k\sqrt{c}}{|C_1 x + q^k\sqrt{-c}|} = \frac{2q^k\sqrt{c}}{y^{p/2}}.$$

By Corollary 8.5, we have that $y^{p/2} > 10q^k\sqrt{c}$ and, consequently,

$$|\Delta' - 1| < \frac{1}{5}.$$

Then, applying Lemma B.2 in [47] gives that

$$|\Delta| = |\log(\Delta')| \leq -10\log\left(\frac{4}{5}\right)\frac{q^k\sqrt{c}}{y^{p/2}}.$$

If we then take logarithms and replace c by its definition in (8) if α is odd and by its definition in (9) if α is even, it follows that

$$\log(|\Delta|) \leq \begin{cases} 0.81 + \left(k + \frac{1}{2}\right)\log(q) + \frac{1}{2}\log(C_1) - \frac{p}{2}\log(y) & \text{if } \alpha \text{ is odd.} \\ 0.81 + k\log(q) + \frac{1}{2}\log(C_1) - \frac{p}{2}\log(y) & \text{if } \alpha \text{ is even.} \end{cases}$$

Now, the definition of Δ_2 in (62) gives that $\log(|\Delta_2|) = \log(s) + \log(\Delta)$. The result then follows for each case by considering the upper bound for k given in Lemma 8.4, as well as the appropiate values for C_1, q, f, D, s and A_2. □

The final ingredient that we will need before finishing the proof of Proposition 8.1 is an upper bound for $|j|$. This follows from the definition of Δ_2 and is the content of the following Lemma.

Lemma 8.7. *Suppose that (x, y, α, p) is a solution to (7) with y even and $p > 3{\cdot}10^7$, and let Δ_2 be as in (62). Then,*

$$|j| \leq p.$$

Proof. By definition of Δ_2, along with the triangle inequality, we have that

$$|j|\pi \leq |\Delta_2| + |p\log(\varepsilon_1\gamma) + \log(\varepsilon_2\beta)| < \frac{\pi}{2} + p\pi = \left(p + \frac{1}{2}\right)\pi,$$

where the last inequality follows because $|\Delta_2| \leq \pi/2$ and due to the fact that $\log(\varepsilon_1\gamma)$ and $\log(\varepsilon_2\beta)$ have opposite signs. From here, it readily follows that $|j| \leq p$. □

With this, we are finally able to apply the techniques in [31] in order to finish the proof of Proposition 8.1.

Proof. (of Proposition 8.1) We will use the publicly available PARI/GP [36] code associated to [31], which will allow us to find an upper bound for p.

We note that this code makes use of Matveev's theorem (Theorem 2.1 in [31], originally presented in [28]), in order to obtain an initial upper bound for p. Then, it exploits the improved lower bounds for linear forms in three logarithms given in Theorem 4.1 of [31] to iteratively improve upon this upper bound of p, obtaining the final values of $N_0(C_1, q)$ given in (36). The correctness of this computation can be checked with the PARI/GP code available in the GitHub repository.

The following are the necessary input parameters which are common for all (C_1, q), in the notation of Theorem 4.1 in [31]:

$$b_1 = p, \quad b_2 = 1, \quad b_3 = j, \quad \alpha_1 = \varepsilon_1\gamma, \quad \alpha_2 = \varepsilon_2\beta, \quad \alpha_3 = -1.$$

$$\mathcal{D} = \frac{\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]}{\mathbb{R}[\alpha_1, \alpha_2, \alpha_3]} = \frac{2}{2} = 1.$$

As shown in the proof of Lemma 8.4, the heights of the α_i, which we also need for this computation, are given by

$$h(\alpha_1) = \frac{s}{2}\log(y), \quad h(\alpha_2) = s\log(2), \quad h(\alpha_3) = 0.$$

Also, $|j| \leq p$ by Lemma 8.7 and $\log(|\Delta_2|)$ is bounded above by the quantities in Lemma 8.6. Finally, in the notation of Matveev's theorem (Theorem 2.1 in [31]), we also have:

$$D = \chi = 2.$$

With this, we perform three iterations of the code for each pair (C_1, q). For the interested reader, we remark that the parameters L, m, χ and ρ obtained in each iteration (see Section 5.2 of [31]), as well as the estimate on p after each iteration, are recorded on Table 10 for α odd and in Table 11 for α even. This finishes the proof of the Proposition.

□

Remark 13. We note that the improved lower bounds available in [31] allow for a much better bound than that present in previous literature. For comparison, our values for $N_0(1, 7)$ and $N_0(1, 23)$ are between 50% and 70% smaller than the corresponding values in Proposition 15.2 of [8], allowing for a much more efficient computation.

(C_1, q)	L	m	ρ	χ	Upper bound on p
$(1,7)$	115	12.50	5.80	0.044	$2.089874 \cdot 10^8$
$(1,7)$	75	14.60	5.30	0.080	$7.979286 \cdot 10^7$
$(1,7)$	72	13.60	5.40	0.080	$7.234157 \cdot 10^7$
$(1,23)$	106	9.00	7.40	0.072	$4.524352 \cdot 10^8$
$(1,23)$	67	9.80	6.90	0.100	$1.663534 \cdot 10^8$
$(1,23)$	63	9.75	7.00	0.102	$1.514725 \cdot 10^8$
$(3,5)$	102	16.50	6.20	0.076	$1.151876 \cdot 10^8$
$(3,5)$	61	16.40	6.10	0.100	$3.915560 \cdot 10^7$
$(3,5)$	57	17.45	6.00	0.102	$3.476178 \cdot 10^7$
$(3,13)$	118	9.00	6.60	0.052	$3.641642 \cdot 10^8$
$(3,13)$	74	11.60	5.90	0.080	$1.372399 \cdot 10^8$
$(3,13)$	65	11.95	6.20	0.080	$1.243438 \cdot 10^8$
$(5,3)$	102	16.50	6.20	0.076	$1.151876 \cdot 10^8$
$(5,3)$	61	16.40	6.10	0.100	$3.915560 \cdot 10^7$
$(5,3)$	57	17.45	6.00	0.102	$3.476178 \cdot 10^7$
$(5,11)$	102	10.50	7.20	0.072	$2.659731 \cdot 10^8$
$(5,11)$	67	11.00	6.50	0.094	$9.270785 \cdot 10^7$
$(5,11)$	62	10.30	6.80	0.098	$8.334595 \cdot 10^7$
$(11,5)$	102	10.50	7.20	0.072	$2.659731 \cdot 10^8$
$(11,5)$	67	11.00	6.50	0.094	$9.270785 \cdot 10^7$
$(11,5)$	62	10.30	6.80	0.098	$8.334595 \cdot 10^7$
$(13,3)$	118	9.00	6.60	0.052	$3.71751 \cdot 10^8$
$(13,3)$	67	11.00	6.50	0.08	$1.40676 \cdot 10^8$
$(13,3)$	68	11.95	6.00	0.080	$1.273969 \cdot 10^8$
$(13,11)$	112	7.00	8.00	0.074	$1.020209 \cdot 10^9$
$(13,11)$	65	8.00	7.90	0.108	$3.816492 \cdot 10^8$
$(13,11)$	65	7.55	7.80	0.110	$3.499196 \cdot 10^8$

TABLE 10. Parameters obtained in each iteration of the code associated to [31] for α odd.

9. Conclusions

We compile all the work in previous sections to finish the proof of Theorem 1.

Proof. (of Theorem 1) After Sections 2, 3 and 4, we are left with the case of (7) where y is even and $p \geq 11$ is prime. Then, Propositions 5.1, 5.2 and 8.1 show that the only solutions with $p \geq 11$ are those corresponding to the tuples in (37). All of the solutions are in Tables 1 and 2, thereby finishing the proof. □

In theory, there would be no reason to restrict our analysis to $1 \leq C_1 \leq 20$ and $2 \leq q < 25$. However, we remark that there are some solutions to (7) with $C_1 = 21$ and exponent $p = 17$, such as the following

$$21 \cdot 79^2 + 11^1 = 2^{17}.$$

(C_1, q)	L	m	ρ	χ	Upper bound on p
$(7,3)$	115	12.50	5.80	0.044	$2.089874 \cdot 10^8$
$(7,3)$	74	14.60	5.30	0.08	$7.979286 \cdot 10^7$
$(7,3)$	72	13.60	5.40	0.08	$7.234157 \cdot 10^7$
$(7,5)$	116	13.25	5.65	0.044	$2.087874 \cdot 10^8$
$(7,5)$	78	14.00	5.20	0.056	$7.828204 \cdot 10^7$
$(7,5)$	75	14.50	5.10	0.056	$7.083124 \cdot 10^7$
$(7,11)$	116	13.25	5.65	0.044	$2.087874 \cdot 10^8$
$(7,11)$	78	14.00	5.20	0.056	$7.828204 \cdot 10^7$
$(7,11)$	75	14.50	5.10	0.056	$7.083124 \cdot 10^7$
$(7,13)$	116	13.25	5.65	0.044	$2.131371 \cdot 10^8$
$(7,13)$	74	14.75	5.30	0.056	$8.011225 \cdot 10^7$
$(7,13)$	70	14.10	5.40	0.056	$7.236925 \cdot 10^7$
$(7,23)$	116	13.25	5.65	0.044	$2.087874 \cdot 10^8$
$(7,23)$	78	14.00	5.20	0.056	$7.828204 \cdot 10^7$
$(7,23)$	75	14.50	5.10	0.056	$7.083124 \cdot 10^7$
$(15,7)$	109	14.75	6.15	0.076	$1.149974 \cdot 10^8$
$(15,7)$	61	15.00	6.30	0.100	$3.913906 \cdot 10^7$
$(15,7)$	56	16.50	6.20	0.104	$3.472013 \cdot 10^7$
$(15,11)$	109	14.75	6.15	0.076	$1.149974 \cdot 10^8$
$(15,11)$	61	15.00	6.30	0.100	$3.913906 \cdot 10^7$
$(15,11)$	56	16.50	6.20	0.104	$3.472013 \cdot 10^7$
$(15,17)$	103	15.50	6.30	0.076	$1.177119 \cdot 10^8$
$(15,17)$	60	16.25	6.20	0.100	$4.007117 \cdot 10^7$
$(15,17)$	58	16.10	6.10	0.102	$3.547538 \cdot 10^7$

TABLE 11. Parameters obtained in each iteration of the code associated to [31] for α even.

The same is true for the following value of q that we would need to consider if we were to extend the ranges ($q = 29$), since the following identity holds

$$3 \cdot 209^2 + 29^1 = 2^{17}.$$

Since there is a solution in both cases, all the techniques that we have developed in Section 7 would fail, forcing us to solve a Thue–Mahler equation of degree $p = 17$.

As of now, and without significant computational improvements, this is impossible to do. Therefore, extending the solution of (7) to bigger ranges is probably impossible unless significantly new techniques are introduced.

REFERENCES

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers. I*, Mathematika, **13** (2), 1966, 204–216.

[2] A. Baker, *Linear forms in the logarithms of algebraic numbers. II*, Mathematika, **14**, 1967, 102–107.

[3] A. Baker, *Linear forms in the logarithms of algebraic numbers. III*, Mathematika, **14** (2), 1967, 220–228.

[4] M. A. Bennett and C. M. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54.

[5] K. Belabas, F. Beukers, P. Gaudry, H. Lenstra, W. McCallum, B. Poonen, S. Siksek, M. Stoll, M. Watkins, *Explicit Methods in Number Theory: Rational Points and Diophantine Equations*, Panoramas et synthèses **36**, Société Mathématique de France, Paris, 2012.
[6] M. A. Bennett, *On some exponential equations of S. S. Pillai*, Canad. J. Math. **53** (2001), 897–922.
[7] M. A. Bennett and S. Siksek, *Differences between perfect powers: prime power gaps*, Algebra & Number Theory, to appear.
[8] M. A. Bennett and S. Siksek, *Differences between perfect powers: The Lebesgue-Nagell equation*, Transactions of the AMS, to appear.
[9] N. Billerey, I. Chen, L. Dieulefait, N. Freitas, *A multi-Frey approach to Fermat equations of signature* (r, r, p), Transactions of AMS **371**(2019), pp. 8651–8677.
[10] Yu. Bilu, G. Hanrot, and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine Angew. Math. **539** (2001), 75–122.
[11] W. Bosma, J. Cannon and C. Playoust, *The Magma algebra system. I. The user language*, Computational algebra and number theory (London, 1993), J. Symbolic Comput. **24**(3–4) (1997), 235–265.
[12] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over* $\mathbb{Q}$*: wild* 3*-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.
[13] Y. Bugeaud and M. Laurent. *Minoration effective de la distance p-adique entre puissances de nombres algébriques*. *J. Number Theory*, 61(2):311–342, 1996.
[14] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations II. The Lebesgue–Nagell equation*, Compositio Math. **142** (2006), 31–62.
[15] E. Catalan, *Note extraite d'une lettre adressée à l'éditeur*, J. reine angew. Math. **27**, 192 (1844).
[16] P. J. Cazorla-García and V. Patel, *On the generalised Lebesgue–Nagell equation*, in preparation.
[17] J. H. E. Cohn, *The Diophantine equation* $x^2 + C = y^n$, Acta Arith. **LXV.4** (1993), 367–381.
[18] J. H. E. Cohn, *The Diophantine equation* $x^2 + C = y^n$*, II*, Acta Arith. **109.2** (2003), 205–206.
[19] J. Cremona, *Algorithms for Modular Elliptic Curves*, Cambridge University Press (1997), `https://homepages.warwick.ac.uk/staff/J.E.Cremona/book/fulltext/index.html`.
[20] A. Gherha and S. Siksek, *Efficient resolution of Thue–Mahler equations*, 2022, `https://arxiv.org/abs/2207.14492`.
[21] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), 225–320.
[22] E. Halberstadt and A. Kraus, *Courbes de Fermat: résultats et problèmes*, J. reine angew. Math. **548** (2002), 167–234.
[23] A. Herschfeld, *The equation* $2^x - 3^y = d$, Bull. Amer. Math. Soc. **42** (1936), 231–234.
[24] A. Kraus, *Sur l'´équation* $a^3 + b^3 = c^p$, Experimental Mathematics **7** (1998), No. 1, 1–13.
[25] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275.
[26] M. Le and G. Soydan, *A brief survey on the generalized Lebesgue–Ramanujan–Nagell equation*, Surveys in Mathematics and its Applications **15** (2020), 473–523.
[27] V. A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation* $x^m = y^2 + 1$, Nouvelles Ann. des Math. **9** (1850), 178-181.
[28] E. M. Matveev, *An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II*, Izv. Ross. Akad. Nauk Ser. Mat. **64** (2000), 125–180. English transl. in Izv. Math. **64** (2000), 1217–1269.
[29] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), 129–162.
[30] M. Mignotte and B. M. M. de Weger, *On the Diophantine equations* $x^2 + 74 = y^5$ *and* $x^2 + 86 = y^5$, Glasgow Math. J. **38**(1) (1996), 77-85.
[31] M. Mignotte and P. Voutier, *A kit for linear forms in three logarithms*, 2022, https://arxiv.org/abs/2205.08899.
[32] P. Mihăilescu, Primary cyclotomic units and a proof of Catalan's conjecture, *J. Reine Angew. Math.* 572 (2004), 167–195.
[33] D. Mocanu, *Asymptotic Fermat for signatures* $(p, p, 2)$ *and* $(p, p, 3)$ *over totally real fields*, Mathematica **68**(4), pp. 1233–1257.
[34] T. Nagell. Sur l'impossibilité de quelques equations à deux indéterminées. *Norsk Mat. Forenings Skr.*, 13:65–82, 1923.

[35] T. Nagell. Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns. *Nova Acta Soc. Sci. Upsaliensis (4)*, 16(2):38, 1955.
[36] The PARI Group, PARI/GP version `2.14.0`, Univ. Bordeaux, 2021, `http://pari.math.u-bordeaux.fr/`.
[37] V. Patel, *A* Lucas-Lehmer approach to generalised Lebesgue-Ramanujan-Nagell equations, The Ramanujan Journal **56**(6) (2021), 585–596.
[38] A. Pethő, H. G. Zimmer, J. Gebel, and E. Herrmann, Computing all S-integral points on elliptic curves, *Math. Proc. Cambridge Philos. Soc.* 127 (1999), 383–402.
[39] S. S. Pillai, *On the inequality* $0 < a^x - b^y \leq n$, J. Indian Math. Soc. **19** (1931), 1–11.
[40] S. S. Pillai, *On* $a^x - b^y = c$, J. Indian Math. Soc. (N.S.) **2** (1936), 119–122 and 215.
[41] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.
[42] R. Scott and R. Styer, *On the generalized Pillay equation* $\pm a^x \pm b^y = c$, Journal of Number Theory **118** (2006), 236–265.
[43] J.-P. Serre, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$, Duke Math. J. **54** (1987), 179-–230.
[44] J.-P. Serre, *Abelian l-adic representations and elliptic curves,* W. A. Benjamin, New York, 1968.
[45] S. Siksek, *The modular approach to Diophantine equations*, pages 151–179 of [5].
[46] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Springer (2009).
[47] N. Smart, *The Algorithmic Resolution of Diophantine Equations: A Computational Cookbook*, Cambridge University Press (1998).
[48] R. L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.
[49] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Department of Mathematics, University of Manchester, Manchester, United Kingdom, M13 9PY

Email address: `pedro-jose.cazorlagarcia@manchester.ac.uk`