CLASSICAL AND MODULAR APPROACHES TO EXPONENTIAL DIOPHANTINE EQUATIONS II. THE LEBESGUE–NAGELL EQUATION

YANN BUGEAUD, MAURICE MIGNOTTE, SAMIR SIKSEK

ABSTRACT. This is the second in a series of papers where we combine the classical approach to exponential Diophantine equations (linear forms in logarithms, Thue equations, etc.) with a modular approach based on some of the ideas of the proof of Fermat's Last Theorem. In this paper we use a general and powerful new lower bound for linear forms in three logarithms, together with a combination of classical, elementary and substantially improved modular methods to solve completely the Lebesgue-Nagell equation

$$x^2 + D = y^n, \qquad x,\, y \text{ integers},\ n \geq 3,$$

for D in the range $1 \leq D \leq 100$.

1. Introduction

Arguably, the two most celebrated achievements of the 20th century in the field of Diophantine equations have been Baker's theory of linear forms in logarithms, and Wiles' proof of Fermat's Last Theorem. We call Baker's approach to Diophantine equations the 'classical approach'. The proof of Fermat's Last Theorem is based on what we term the 'modular approach'. The proponents of the classical approach are too many to mention; the modular approach is still in its infancy, but among the early contributers let us just mention Frey, Serre, Ribet, Darmon, Merel, Kraus, Bennett, Skinner, Ivorra, etc.

The motivation for our series of papers, of which this is the second, is that neither approach (on its own, and as it stands at the moment) is powerful enough to resolve unconditionally many of the outstanding exponential Diophantine equations. Our thesis is that one should, where possible, attack exponential Diophantine equations by a combination of classical and modular approaches. The precise aims of this series were formulated in our first paper [13] as follows:

- (I) To present theoretical improvements to some aspects of the classical approach.
- (II) To show how local information obtained through the modular approach can be used to reduce the size of the bounds, both for exponents and for variables, of solutions to exponential Diophantine equations.

Date: April 11, 2006.

2000 *Mathematics Subject Classification.* Primary 11D61, 11J86, Secondary 11D59, 11Y50.

Key words and phrases. Diophantine equations, Ramanujan–Nagell, Frey curves, level-lowering, linear forms in logarithms, Thue equations.

S. Siksek's work is funded by a grant from Sultan Qaboos University (IG/SCI/DOMS/02/06).

(III) To show how local information obtained through the modular approach can be pieced together to provide a proof that there are no missing solutions less than the bounds obtained in (I), (II).

(IV) To solve various famous exponential Diophantine equations.

In [13] we gave a new lower bound for linear forms in three logarithms, and used a combination of classical and modular methods to determine all the perfect powers in the Fibonacci and Lucas sequences. In the present paper, we apply a more general and powerful lower bound for linear forms in three logarithms due to Mignotte [38], together with a combination of elementary, classical, and substantially improved modular methods to study the following exponential Diophantine equation.

$$x^2 + D = y^n, \qquad x,\, y \text{ integers},\ n \geq 3. \tag{1}$$

Here, D denotes a non-zero integer. We have chosen to name this equation the Lebesgue–Nagell equation; the reason for the name Lebesgue–Nagell is given in Section 2, together with some historical remarks. But for now we mention that the equation has previously been solved for 81 values of D in the range $1 \leq D \leq 100$, using elementary, classical and modular methods; the remaining values are apparently beyond these methods as they stand. We prove the following Theorem.

Theorem 1. *All solutions to equation (1) with D in the range*

$$1 \leq D \leq 100 \tag{2}$$

are given in the Tables at the end. In particular, the only integer solutions (x, y, n) to the generalised Ramanujan–Nagell equation

$$x^2 + 7 = y^n, \qquad n \geq 3,$$

satisfy $|x| = 1,\ 3,\ 5,\ 11,\ 181$.

We choose to give a complete proof of Theorem 1, rather than treating the 19 remaining values of D in the range (2).

It is noted that the solutions for even n can be deduced quickly, for then D is expressible as a difference of squares. It is therefore sufficient to solve the equation

$$x^2 + D = y^p, \qquad x,\, y \text{ integers},\ \ p \geq 3 \text{ is prime}; \tag{3}$$

the solutions to (1) can then be recovered from the solutions to (3).

We give three modular methods for attacking (3). Two are refinements of known methods, and a third that is completely new. Using a computer program based on these modular methods, we can show—for any D in the above range—that the exponent p is large (showing that $p > 10^9$ is quite practical). Our modular approach also yields the following rather surprising result: either each prime factor of y divides $2D$, or $y > (\sqrt{p} - 1)^2$. We are then able to deduce not only that p is large, but also that y is large. This information helps us to reduce the size of the upper bound on p obtained from the lower bound for the linear forms in three logarithms, making the computation much more practical. This idea of using the modular approach to force lower bounds for solutions of Diophantine equations was used previously, for instance by Bennett [5]. Our total computer time for the computations in this paper is roughly 206 days on various workstations (the precise details are given in due course).

Using our approach should make it possible to solve (1) for any D, with $|D|$ not too large, that is **not** of the form $D = -a^2 \pm 1$; if D is of this form then the equation (1) has a solution $(x, y) = (a, \pm 1)$ for all odd values of the exponent n, and the modular methods we explain later are not very successful in this situation. To deal with this case requires further considerations which we leave for another paper. Notice, however, that the case $D = 1$ turns out to be quite easy and was solved in 1850 by V. A. Lebesgue [31]. Furthermore, equation (1) has been solved for some negative values of D of the form $D = -a^2 \pm 1$, including $D = -1$ and $D = -8$ (see for example [24] and [49]). However, proving that the only integer solutions to $x^2 - 2 = y^n$ with $n \geq 3$ satisfy $|x| = 1$ remains a challenging open question. For some modest progress on this question, due to the authors, see [50].

We would like to warmly thank Mihai Cipu and Attila Pethő for pointing many imperfections in a previous version of this paper, and Guillaume Hanrot for help with solving Thue equations. We are also grateful to the anonymous referee for many pertinent historical remarks and a very careful reading.

2. On the History of the Lebesgue–Nagell Equation

Equation (1) has a long and glorious history, and there are literally hundreds of papers devoted to special cases of this equation. Most of these are concerned with equation (1) either for special values of n or special values of y. For example, for $D = 2$ and $n = 3$, Fermat asserted that he had shown that the only solutions are given by $x = 5$, $y = 3$; a proof was given by Euler [20]. Equation (1) with $n = 3$ is the intensively studied Mordell equation (see [21] for a modern approach).

Another notable special case is the generalized Ramanujan–Nagell equation

$$x^2 + D = k^n, \tag{4}$$

where D and k are given integers. This is an extension of the Ramanujan–Nagell equation $x^2 + 7 = 2^n$, proposed by Ramanujan [43] in 1913 and first solved by Nagell [40] in 1948 (see also the collected papers of Nagell [41]). This equation has exactly five solutions with $x \geq 1$ (see [37] for a very simple proof) and is in this respect singular: indeed, Bugeaud and Shorey [14] established that equation (4) with D positive and k a prime number not dividing D has at most two solutions in positive integers x, n, except for $(D, k) = (7, 2)$. They also listed all the pairs (D, k) as above for which equation (4) has exactly two solutions. Much earlier, Apéry, [1] and [2], proved by p–adic arguments that $x^2 + D = k^n$, with k prime, has at most two positive integer solutions except if $(D, k) = (7, 2)$. We direct the reader to [14] for further results and references.

Returning to equation (1), the first result for general y, n seems to be the proof in 1850 by V. A. Lebesgue [31] that there are no non-trivial solutions for $D = 1$. The next cases to be solved were $D = 3, 5$ by Nagell [40] in 1923. It is for this reason that we call equation (1) the Lebesgue–Nagell equation. The case with $D = -1$ is particularly noteworthy: a solution was sought for many years as a special case of the Catalan conjecture. This case was finally settled by Chao Ko [25] in 1965.

The history of the Lebesgue–Nagell equation is meticulously documented in an important article by Cohn [17], and so we are saved the trouble of compiling an exhaustive survey. In particular, Cohn refines the earlier elementary approaches of various authors (especially of Ljunggren [33], [34]) and completes the solution for 77 values of D in the range $1 \leq D \leq 100$. The solution for the cases $D = 74$, 86 was completed by Mignotte and de Weger [39] (indeed, Cohn solved these two equations of type (3) except for $p = 5$, in which case difficulties occur since the class-numbers of the corresponding imaginary quadratic fields are divisible by 5). Bennett and Skinner (Proposition 8.5 of [6]) applied the modular approach to solve the cases $D = 55$ and 95. The 19 remaining values

$$7,\ 15,\ 18,\ 23,\ 25,\ 28,\ 31,\ 39,\ 45,\ 47,\ 60,\ 63,\ 71,\ 72,\ 79,\ 87,\ 92,\ 99,\ 100, \tag{5}$$

are clearly beyond the scope of Cohn's elementary method, though Cohn's method can still give non-trivial information even in these cases, and is revisited in Section 5. Moreover, as far as we can see, the modular method used by Bennett and Skinner (which is what we later on call Method I) is not capable of handling these values on it own, even though it still gives useful information in most cases.

Cohn, in the same paper, also makes a challenge of proving that the only solutions to the equation

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

have $|x| = 1, 3, 5, 11, 181$. This challenge was taken up by Lesage [32] who proved, by classical arguments, that if $x > 181$ then $5000 < n < 6.6 \times 10^{15}$ and also by Siksek and Cremona [51] who used the modular approach to show that there are no further solutions for $n \leq 10^8$ (consequently, n must be prime); they also suggested that an improvement to lower bounds in linear forms in three logarithms may finally settle the problem. With the benefit of hindsight, we know that they were almost—though not entirely—correct. The substantial improvement to lower bounds in linear forms in three logarithms used here was certainly needed. However, for this lower bound to be even more effective, a further insight obtained from the modular approach was also needed: namely that y is large as indicated in the Introduction; notice further that Lesage proved that $y > 10^9$ by classical arguments (linear forms in two 2–adic logarithms from [12]) and some heavy computer verification.

3. Reduction to Thue Equations

Our main methods for attacking equation (3) are linear forms in logarithms (to bound p) and the modular approach, though for some small values of p it is necessary to reduce the equation to a family of Thue equations. The method for reducing equation (3) to Thue equations is well-known. We do however feel compelled to give a succinct recipe for this, in order to set up notation that is needed later.

It is appropriate to point out that there are other approaches that could be used to solve equation (3) for small p. For $p = 3$ we can view the problem as that of finding integral points on an elliptic curve, a problem that is aptly dealt with in the literature (see [52] and [21]). For $p \geq 5$, the equation $x^2 + D = y^p$ defines a curve of genus ≥ 2; one can sometimes determine all rational points on this curve using the method of Chabauty [15], though this would require computing the Mordell–Weil group of the Jacobian as well (see [42], [45], [55], [56] and [57]).

We do not assume in this section that D is necessarily in the range (2), merely that $-D$ is not a square. We write (here and throughout the paper)

$$D = D_1^2 D_2, \qquad D_1,\ D_2 \text{ are integers, } D_2 \text{ square-free.}$$

Let $\mathcal{L} = \mathbb{Q}(\sqrt{-D_2})$, and $\mathcal{O}$ be its ring of integers. Throughout the present paper, we denote the conjugate of an element α (resp. of an ideal $\mathfrak{a}$) by $\overline{\alpha}$ (resp. by $\overline{\mathfrak{a}}$).

Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ be the prime ideals of $\mathcal{O}$ dividing $2D$. Let $\mathcal{A}$ be the set of integral ideals $\mathfrak{a}$ of $\mathcal{O}$ such that

- $\mathfrak{a} = \mathfrak{p}_1^{a_1} \cdots \mathfrak{p}_r^{a_r}$, with $0 \leq a_i < p$,

- the gcd $(\mathfrak{a}, \overline{\mathfrak{a}})$ divides $2\,D_1\sqrt{-D_2}$,
- the ideal $\mathfrak{a}\overline{\mathfrak{a}}$ is a perfect p–th power.

If (x, y) is a solution to equation (3), then one effortlessly sees that

$$(x + D_1\sqrt{-D_2})\mathcal{O} = \mathfrak{a}\mathfrak{b}^p$$

for some $\mathfrak{a} \in \mathcal{A}$ and some integral ideal $\mathfrak{b}$.

Now let $\mathfrak{b}_1, \ldots, \mathfrak{b}_h$ be integral ideals forming a complete set of representatives for the ideal class group of $\mathcal{O}$. Thus $\mathfrak{b}\mathfrak{b}_i$ is a principal ideal for some i, and so $\mathfrak{b}\mathfrak{b}_i = \beta'\mathcal{O}$ for some $\beta' \in \mathcal{O}$. The fractional ideal $\mathfrak{a}\mathfrak{b}_i^{-p}$ is easily seen to be also principal. The ideal $\mathfrak{b}$ is unknown, but the ideals, $\mathfrak{a}, \mathfrak{b}_1, \ldots, \mathfrak{b}_h$ are known. We may certainly determine which of the fractional ideals $\mathfrak{a}\mathfrak{b}_i^{-p}$ are principal. Let Γ' be a set containing one generator γ' for every principal ideal of the form $\mathfrak{a}\mathfrak{b}_i^{-p}$ ($\mathfrak{a} \in \mathcal{A}$ and $1 \leq i \leq h$). It is noted that the elements of Γ' are not necessarily integral, but we know that if (x, y) is a solution to equation (3) then

$$(x + D_1\sqrt{-D_2})\mathcal{O} = \gamma'\beta'^p\mathcal{O},$$

for some $\gamma' \in \Gamma'$ and some $\beta' \in \mathcal{O}$. Finally, define Γ as follows:

$$\Gamma = \begin{cases} \Gamma', & \text{if } D_2 > 0,\ D_2 \neq 3, \text{ or if } D_2 = 3 \text{ and } p \neq 3, \\ \Gamma' \cup \zeta\Gamma' \cup \zeta^{-1}\Gamma', & \text{if } D_2 = p = 3, \text{ where } \zeta = (1+\sqrt{-3})/2, \\ \cup_j\, \epsilon^j\Gamma', & \text{if } D_2 < 0, \text{ where } j \text{ runs over } -(p-1)/2, \ldots, (p-1)/2, \end{cases}$$

where if $D_2 < 0$ (and so $\mathcal{L}$ is real) we write ϵ for the fundamental unit.

We quickly deduce the following.

Proposition 3.1. *With notation as above, if (x, y) is a solution to equation (3) then there exist $\gamma \in \Gamma$ and $\beta \in \mathcal{O}$ such that*

$$x + D_1\sqrt{-D_2} = \gamma\beta^p.$$

Thus if we let 1, ω be an integral basis for $\mathcal{O}$ then for some $\gamma \in \Gamma$,

$$x = \tfrac{1}{2}\left(\gamma(U + V\omega)^p + \overline{\gamma}(U + V\overline{\omega})^p\right)$$

for some integral solution (U, V) to the Thue equation

$$\frac{1}{2\sqrt{-D_2}}\left(\gamma(U + V\omega)^p - \overline{\gamma}(U + V\overline{\omega})^p\right) = D_1.$$

3.1. **Results I.** If q is a prime we denote by $v_q : \mathbb{Z} \to \mathbb{Z}_{\geq 0} \cup \{\infty\}$ the normalized q–adic valuation.

We now eliminate all cases where it is inconvenient to carry out level-lowering.

Lemma 3.2. *Suppose $1 \leq D \leq 100$. Suppose (x, y, p) is a solution to equation (3) that is missing from our Tables at the end. Then p satisfies the following conditions:*

$$\begin{cases} p \geq 7, & \\ p \geq v_q(D) + 1, & \textit{for all primes } q, \\ p \geq v_2(D) + 7, & \textit{if } v_2(D) \textit{ is even.} \end{cases} \tag{6}$$

Proof. It is clear that for any particular D there are only a handful of primes p violating any of these conditions. We wrote a `pari/gp` [3] program that solved all the equations (3) for p violating (6): the program first reduces each such equation to a family of Thue equations as in Proposition 3.1 above. These are then solved using the built-in `pari/gp` function for solving Thue equations (this is an implementation of the method of Bilu and Hanrot [8]).

It is perhaps worthwhile to record here two tricks that helped us in this step. First, in writing down the set Γ appearing in Proposition 3.1 we needed a set of integral ideals $\mathfrak{b}_1, \ldots, \mathfrak{b}_h$ representing the ideal class group of the quadratic field $\mathcal{L}$. Both `pari/gp` and `MAGMA` [10] have built-in functions that amount to homomorphisms from the ideal class group as an abstract group, to the set of fractional ideals, and these can be used to construct the required set $\mathfrak{b}_1, \ldots, \mathfrak{b}_h$. We have found however that we get much simpler Thue equations if we search for the smallest prime ideal representing each non-trivial ideal class, and of course taking $1\mathcal{O}$ to represent the trivial ideal class.

To introduce the second trick, we recall that when one is faced with a Thue equation

$$a_0U^p + a_1U^{p-1}V + \cdots + a_pV^p = b$$

it is usual to multiply throughout by a_0^{p-1} and make the substitution $U' = a_0U$, thus obtaining a monic polynomial on the left-hand side. When a_0 is large, this greatly complicates the equation. The second trick is to first search for a unimodular substitution which makes the leading coefficient a_0 small.

After optimizing our program, we were able to complete the proof of Lemma 3.2 in about 22 minutes on a 1050 MHz UltraSPARC III computer. $\square$

4. Removing Common Factors

It is desirable when applying the modular approach to equation (3) to remove the possible common factors of the three terms in the equation. This desire leads to a subdivision of cases according to the possible common factors, as seen in the following elementary Lemma. Here and elsewhere, for a non-zero integer a, the product of the distinct prime divisors of a is called the radical of a, and denoted by $\operatorname{rad}(a)$, in particular $\operatorname{rad}(\pm 1) = 1$. Furthermore, $\left(\frac{\cdot}{\cdot}\right)$ stands for the Kronecker symbol.

Lemma 4.1. *Suppose that (x, y, p) is a solution to equation (3) such that $y \neq 0$ and p satisfies the condition (6). Then there are integers d_1, d_2 such that the following conditions are satisfied:*

(i) $d_1 > 0$,
(ii) $D = d_1^2 d_2$,
(iii) $\gcd(d_1, d_2) = 1$,
(iv) *for all odd primes $q \mid d_1$ we have* $\left(\frac{-d_2}{q}\right) = 1$,
(v) *if* $2 \mid d_1$ *then* $d_2 \equiv 7 \pmod 8$.

Moreover there are integers s, t such that

$$x = d_1 t, \qquad y = \operatorname{rad}(d_1) s,$$

and

$$t^2 + d_2 = es^p, \quad \gcd(t, d_2) = 1, \quad s \neq 0, \tag{7}$$

where

$$e = \prod_{\substack{q \text{ prime} \\ q \mid d_1}} q^{p-2v_q(d_1)} \qquad \text{and} \qquad \operatorname{rad}(e) = \operatorname{rad}(d_1). \tag{8}$$

Proof. Suppose (x, y, p) is a solution to equation (3) such that $y \neq 0$ and condition (6) is satisfied. It is straightforward to see that condition (6) forces $\gcd(x^2, D)$ to be a square, say d_1^2 with $d_1 > 0$. We can therefore write $x = d_1 t$ and $D = d_1^2 d_2$ for some integers t and d_2. Moreover, since

$$d_1^2 = \gcd(x^2, D) = \gcd(d_1^2 t^2, d_1^2 d_2) = d_1^2 \gcd(t^2, d_2),$$

we see that $\gcd(t, d_2) = 1$. Removing the common factors from $x^2 + D = y^p$ we obtain $t^2 + d_2 = es^p$ where e is given by (8). The integrality of e follows from the condition (6), and so does the equality of the radicals $\mathrm{rad}(e) = \mathrm{rad}(d_1)$. Note that (iii) follows from this equality of the radicals and the fact that t, d_2 are coprime. We have thus proven (i), (ii), (iii) and it is now easy to deduce (iv) and (v). Finally, the condition $s \neq 0$ follows from the condition $y \neq 0$. □

Definition. *Suppose D is a non-zero integer and (x, y, p) is a solution to equation (3) with $y \neq 0$ and p satisfying (6). Let d_1, d_2 be as in the above Lemma and its proof (thus $d_1 > 0$ and $\gcd(x, D) = d_1^2$ and $d_2 = D/d_1^2$). We call the pair (d_1, d_2) the signature of the solution (x, y, p). We call the pair (t, s) the simplification of (x, y) (or (t, s, p) the simplification of (x, y, p)).*

In this terminology, Lemma 4.1 associates to any D a finite set of possible signatures (d_1, d_2) for the solutions (x, y, p) of equation (3) satisfying (6) and $y \neq 0$. To solve (3) it is sufficient to solve it under the assumption that the solution's signature is (d_1, d_2) for each possible signature.

Example 1. For example, if $D = 25$, there are two possible signatures satisfying the conditions of Lemma 4.1; these are $(d_1, d_2) = (1, 25)$ or $(5, 1)$. If $(d_1, d_2) = (1, 25)$, then $x = t$, $y = s$ and we must solve the equation

$$t^2 + 25 = s^p, \quad 5 \nmid t,$$

already solved by Cohn. However, if $(d_1, d_2) = (5, 1)$, then $x = 5t$, $y = 5s$, and we must solve the equation

$$t^2 + 1 = 5^{p-2} s^p,$$

not solved by Cohn. In either case it is noted that the three terms of the resulting equation are relatively coprime, which is important to apply the modular approach.

5. A Simplification of Cohn

We will soon apply our modular machinery to equations (3) with D in the range (2). Before doing this it is helpful to introduce a simplification due to Cohn that will drastically reduce the amount of computation needed later. All the arguments presented in this Section are found in Cohn's papers [17], [18]. Cohn however assumed that $D \not\equiv 7 \pmod 8$; the result below is not subject to this restriction.

Proposition 5.1. *Let $D = D_1^2 D_2$ where D_2 is square-free and $D_2 > 0$. Suppose that (x, y, p) is a solution to equation (3) with p satisfying (6), and let (d_1, d_2) be the signature of this solution. Then either*

(i) $d_1 > 1$,
(ii) *or* $D \equiv 7 \pmod 8$ *and* $2 \mid y$,
(iii) *or* p *divides the class number* h *of the quadratic field* $\mathbb{Q}(\sqrt{-D_2})$,

(iv) *or* $y = a^2 + D_2 b^2$ *for some integers* a *and* b *such that* $b \mid D_1$, $b \neq \pm D_1$,

$$p \mid (D_1^2 - b^2) \quad \textit{and} \quad \frac{1}{2\sqrt{-D_2}}\left[(U + b\sqrt{-D_2})^p - (U - b\sqrt{-D_2})^p\right] = D_1,$$

(v) *or* $D = 1$, $(x, y) = (0, 1)$,

(vi) *or* $D_2 \equiv 3 \pmod 4$ *and* $y = (a^2 + D_2 b^2)/4$ *for some odd integers* a *and* b *such that* $b \mid D_1$, $p \mid (4D_1^2 - b^2)$ *and* a *is a solution of the equation*

$$\frac{1}{2\sqrt{-D_2}}\left[(U + b\sqrt{-D_2})^p - (U - b\sqrt{-D_2})^p\right] = 2^p D_1.$$

Proof. We only give a brief sketch. Suppose that (i), (ii), (iii) are false. Then $(x + D_1\sqrt{-D_2}) = \alpha^p$ for some α in the ring of integers of $\mathbb{Q}(\sqrt{-D_2})$. There are two possibilities. The first is that $\alpha = a + b\sqrt{-D_2}$ for some integers a and b. By equating the imaginary parts we deduce all of (iv) if $b \neq \pm D_1$. Thus suppose that $b = \pm D_1$. Letting $\beta = a - b\sqrt{-D_2}$ we see that

$$\frac{\alpha^p - \beta^p}{\alpha - \beta} = \pm 1.$$

If α/β is not a root of unity, then the left-hand side is the p–th term of a Lucas sequence (with $p \geq 7$) and a deep Theorem of Bilu, Hanrot and Voutier [9] on primitive divisors of Lucas and Lehmer sequences immediately gives a contradiction. Thus α/β is a root of unity, *i.e.* $\alpha/\beta = \pm 1$, $\pm i$, or $(\pm 1 \pm \sqrt{-3})/2$. Each case turns out to be impossible, except for $\alpha = -\beta$ which together with $b = \pm D_1$ implies (v).

The second possibility for α is that $\alpha = (a + b\sqrt{-D_2})/2$ with a, b odd integers (and $-D_2 \equiv 1 \pmod 4$). Now (vi) follows quickly by equating the imaginary parts of $(x + D_1\sqrt{-D_2}) = \alpha^p$. □

5.1. **Results II.**

Corollary 5.2. *Suppose* D *belongs to our range (2) and* (x, y, p) *is a solution to equation (3) with* p *satisfying the condition (6). If the solution* (x, y, p) *is missing from our Tables, then either* $D \equiv 7 \pmod 8$ *and* $2 \mid y$, *or* $d_1 > 1$, *where* (d_1, d_2) *is the signature of the solution.*

Proof. We apply Proposition 5.1. Using a short `MAGMA` program we listed all solutions arising from possibilities (iv)–(vi) of that Proposition with $1 \leq D \leq 100$. The only ones found in our range are $(x, y, p) = (0, 1, p)$ for $D = 1$ and $(x, y, p) = (\pm 8, 2, 7)$ for $D = 64$ and these are certainly in the Tables.

To prove the Corollary we merely have to take care of possibility (iii) of the Proposition. For $1 \leq D \leq 100$, and primes p satisfying (6), the only case when p could possibly divide the class number of $\mathbb{Q}(\sqrt{-D_2})$ is $p = 7$ and $D = 71$ (in which case $h = 7$). We solved the equation $x^2 + 71 = y^7$ by reducing to Thue equations as in Section 3. It took `pari/gp` about 30 minutes to solve these Thue equations, and we obtained that the only solutions are $(x, y) = (\pm 46, 3)$, again in our Tables. □

6. Level-Lowering

In this section we apply the modular approach to equation (7) under suitable, but mild, hypotheses. Ordinarily, one would have to construct a Frey curve or curves associated to our equation, show that the Galois representation is irreducible (under suitable hypotheses) using the results of Mazur and others [36], and modular

Table 1. Frey Curves with d_1, d_2 odd.

Case	Condition on d_2	Condition on t	Frey Curve E_t	L
(a)	$d_2 \equiv 1 \pmod 4$		$Y^2 = X^3 + 2tX^2 - d_2X$	2^5
(b)	$d_2 \equiv 3 \pmod 8$		$Y^2 = X^3 + 2tX^2 + (t^2 + d_2)X$	2^5
(c)	$d_2 \equiv 7 \pmod 8$	t even	$Y^2 = X^3 + 2tX^2 + (t^2 + d_2)X$	2^5
(d)	$d_2 \equiv 7 \pmod 8$	$t \equiv 1 \pmod 4$	$Y^2 + XY = X^3 + \left(\frac{t-1}{4}\right) X^2 + \left(\frac{t^2+d_2}{64}\right) X$	2

Table 2. Frey Curves with d_1 even, d_2 odd.

Case	Conditions on t, s, p	Frey Curve E_t	L
(e)	$t \equiv 1 \pmod 4$	$Y^2 + XY = X^3 + \left(\frac{t-1}{4}\right) X^2 + \left(\frac{t^2+d_2}{64}\right) X$	1

by the work of Wiles and others [60], [58], [11], and finally apply Ribet's level-lowering Theorem [44]. Fortunately we are saved much trouble by the excellent paper of Bennett and Skinner [6], which does all of this for equations of the form $Ax^n + By^n = Cz^2$; it is noted that equation (7) is indeed of this form.

Let D be a non-zero integer. We shall apply the modular approach to the Diophantine equation

$$x^2 + D = y^p, \qquad x^2 \nmid D, \quad y \neq 0, \quad \text{and } p \geq 3 \text{ is prime}, \tag{9}$$

or the equivalent equation for the simplification (s, t)

$$t^2 + d_2 = es^p, \qquad t \neq \pm 1, \quad \gcd(t, d_2) = 1, \quad s \neq 0, \tag{10}$$

under the additional assumption that p satisfies (6). The assumptions made about s, t in (10) are there to ensure the non-singularity of the Frey curves, and the absence of complex multiplication when we come to apply the modular approach later on. Before going on we note the following Lemma which in effect says that there is no harm in making these additional assumptions for D in our range (2).

Lemma 6.1. *There are no solutions to the equation (3) for D in the range (2) with $y = 0$, or $x^2 \mid D$, except those listed in the Tables at the end.*

Proof. Clearly $y \neq 0$. We produced our list of solutions with $x^2 \mid D$ using a short `MAGMA` program. □

Lemma 4.1 associates to each equation of the form (9) finitely many signatures (d_1, d_2) satisfying conditions (i)–(v), and corresponding equations (7). Following Bennett and Skinner [6] we associate a Frey curve E_t to any potential solution of equation (10) according to Tables 1, 2, 3.

The three tables are divided into cases (a)–(l). We know that d_1, d_2 are coprime, and hence at most one of them is even. The possibility that d_1, d_2 are both odd is dealt with in Table 1. In cases (a), (b), a simple modulo 8 argument convinces us that t is odd. However for cases (c) and (d) — where d_1 is odd and $d_2 \equiv 7 \pmod 8$ — the integer t can be either odd or even and we assign different Frey curves for each possibility. When t is odd (case (d)) we add the assumption that $t \equiv 1 \pmod 4$; this can be achieved by interchanging t with $-t$ if necessary.

TABLE 3. Frey Curves with d_1 odd, d_2 even.

Case	Condition on d_2	Condition on t	Frey Curve E_t	L
(f)	$v_2(d_2) = 1$		$Y^2 = X^3 + 2tX^2 - d_2X$	2^6
(g)	$d_2 \equiv 4 \pmod{16}$	$t \equiv 1 \pmod 4$	$Y^2 = X^3 + tX^2 - \frac{d_2}{4}X$	2
(h)	$d_2 \equiv 12 \pmod{16}$	$t \equiv 3 \pmod 4$	$Y^2 = X^3 + tX^2 - \frac{d_2}{4}X$	2^2
(i)	$v_2(d_2) = 3$	$t \equiv 1 \pmod 4$	$Y^2 = X^3 + tX^2 - \frac{d_2}{4}X$	2^4
(j)	$v_2(d_2) = 4, 5$	$t \equiv 1 \pmod 4$	$Y^2 = X^3 + tX^2 - \frac{d_2}{4}X$	2^2
(k)	$v_2(d_2) = 6$	$t \equiv 1 \pmod 4$	$Y^2 + XY = X^3 + \left(\frac{t-1}{4}\right)X^2 - \frac{d_2}{64}X$	2^{-1}
(l)	$v_2(d_2) \geq 7$	$t \equiv 1 \pmod 4$	$Y^2 + XY = X^3 + \left(\frac{t-1}{4}\right)X^2 - \frac{d_2}{64}X$	1

Table 2 deals with the possibility of even d_1, and Table 3 with the possibility of even d_2. In both these cases t is necessarily odd, and the congruence condition on t can again be achieved by interchanging t with $-t$ if necessary.

Proposition 6.2. *Suppose D, d_1, d_2 are non-zero integers that satisfy (i)–(v) of Lemma 4.1. Suppose also p is a prime satisfying (6), and let e be as defined in (8). Suppose that (t, s) is a solution of equation (10) and satisfies the supplementary condition (if any) on t in Tables 1, 2, 3. Let E_t and L be as in these tables, and write $\rho_p(E_t)$ for the Galois representation on the p–torsion of E_t. Then the representation $\rho_p(E_t)$ arises from a cuspidal newform of weight 2 and level $N = L\,\mathrm{rad}(D)$.*

Proof. In [6], Bennett and Skinner give an exhaustive recipe for Frey curves and level-lowering for equations of the form $Ax^n + By^n = Cz^2$ under the assumption that the three terms in the equation are coprime. After a little relabeling, their results apply to equation (10) and the Lemma follows from Sections 2 and 3 of their paper. It is here that we need the assumptions $t \neq \pm 1$ and $s \neq 0$ made in (10). □

It is convenient to indulge in the following abuse of language.

Definition. *If (t, s, p) is a solution to equation (10) and if the representation $\rho_p(E_t)$ arises from a cuspidal newform f, then we say that solution (t, s, p) arises from the newform f (via the Frey curve E_t), or that the newform f gives rise to the solution (t, s, p). If (t, s, p) is the simplification of (x, y, p) then we say that (x, y, p) arises from the newform f. If the newform f is rational, and so corresponds to an elliptic curve E, then we also say that the solution (t, s, p) (or (x, y, p)) arises from E.*

6.1. **A Summary.** It may be helpful for the reader to summarize what we have done and where we are going. Given a non-zero integer D we would like to solve equation (9). We can certainly write down all solutions with $y = 0$ or with $x^2 \mid D$. We can also solve (at least in principle) all cases where p violates condition (6) by reducing to Thue equations as in Section 3. We can thus reduce to equation (9) and assume that p satisfies condition (6).

Next, we can write down a list of signatures (d_1, d_2) satisfying conditions (i)–(v) of Lemma 4.1. We reduce the solution of equation (9) to solving for each signature (d_1, d_2) the equation (10). Now we associate to the signature (d_1, d_2) one or more Frey curves E_t and levels N, so that any solution to (10) arises from some newform f at level N via the Frey curve E_t.

Finally (and this is to come) we must show how to solve (10) under the assumption that the solution arises from a newform f via a Frey curve E_t. If we can do this for each newform f at the necessary level and Frey curve E_t then we will have completed the solution of our equation (3).

As we shall see, the assumption that a solution arises from a particular newform is a very strong one, for it imposes congruence conditions on t modulo all but finitely many primes l.

6.2. **Congruences.** For an elliptic curve E and a prime of good reduction l we write $\sharp E(\mathbb{F}_l)$ for the number of points on E over the finite field $\mathbb{F}_l$, and let $a_l(E) = l + 1 - \sharp E(\mathbb{F}_l)$.

Lemma 6.3. *With notation as above, suppose that the Galois representation $\rho_p(E_t)$ arises from a cuspidal newform with Fourier expansion around infinity*

$$f = q + \sum_{n \geq 2} c_n q^n, \tag{11}$$

of level N (given by Proposition 6.2) and defined over a number field $K/\mathbb{Q}$. Then there is a place $\mathfrak{P}$ of K above p such that for every prime $l \nmid 2pD$ we have

$$\begin{aligned} a_l(E_t) &\equiv c_l \pmod{\mathfrak{P}}, \quad \textit{if } t^2 + d_2 \not\equiv 0 \pmod{l} \textit{ (or equivalently } l \nmid s\textit{)}, \\ l + 1 &\equiv \pm c_l \pmod{\mathfrak{P}}, \quad \textit{if } t^2 + d_2 \equiv 0 \pmod{l} \textit{ (or equivalently } l \mid s\textit{)}. \end{aligned}$$

Proof. The Lemma is standard (see [47, page 196], [6, page 7], [26, Proposition 5.4], etc.). The conditions $l \nmid 2D$ and $l \nmid s$ together imply that l is a prime of good reduction for E_t, whereas the conditions $l \nmid 2D$ and $l \mid s$ imply that l is a prime of multiplicative reduction. □

When the newform f is rational, there is an elliptic curve E defined over $\mathbb{Q}$ whose conductor is equal to the level of the newform f such that $a_l(E) = c_l$ for all primes of good reduction l. In this case we can be a little more precise than in Lemma 6.3, thanks to a result of Kraus and Oesterlé.

Lemma 6.4. *With notation as above, suppose that the Galois representation $\rho_p(E_t)$ arises from a rational cuspidal newform f corresponding to an elliptic curve $E/\mathbb{Q}$. Then for all primes $l \nmid 2\,D$ we have*

$$\begin{aligned} a_l(E_t) &\equiv a_l(E) \pmod{p}, \quad \textit{if } t^2 + d_2 \not\equiv 0 \pmod{l} \textit{ (or equivalently } l \nmid s\textit{)}, \\ l + 1 &\equiv \pm a_l(E) \pmod{p}, \quad \textit{if } t^2 + d_2 \equiv 0 \pmod{l} \textit{ (or equivalently } l \mid s\textit{)}. \end{aligned}$$

Proof. This Lemma does appear to be a special case of Lemma 6.3; however we do allow in this Lemma the case $l = p$ which was excluded before. In fact Lemma 6.3 together with a result of Kraus and Oesterlé [27, Proposition 3] implies that the representations $\rho_p(E_t)$ and $\rho_p(E)$ are semi-simply isomorphic. In this case the result of Kraus and Oesterlé also tells us that $a_l(E_t) \equiv a_l(E) \pmod{p}$ if the prime l is a prime of good reduction for both curves, and $a_l(E_t)a_l(E) \equiv l + 1 \pmod{p}$ if l is a prime of good reduction for one of them and a prime of multiplicative reduction for the other. Now since $l \nmid 2D$ we see that $l \nmid N$, the conductor N of E (which is also the level of the newform f as given by Proposition 6.2). If $l \mid s$ then l is a prime of multiplicative reduction for E_t and then $a_l(E_t) = \pm 1$. The Lemma follows. □

7. Eliminating Exponents: Method I

We now focus on equations of the form (10) where, as always, p satisfies (6). Proposition 6.2 tells us that if (t, s, p) is a solution to (10), then it arises from a newform of a certain level (or levels) and all these can be determined. Let us say that these newforms are $f_1, \ldots, f_n$. Then to solve equation (10) it is sufficient to solve it, for each i, under the assumption that the solution arises from the newform f_i. We give three methods for attacking equation (10) under the assumption that the solution arises from a particular newform f.

If successful, the first method will prove that the equation (10) has no solutions except possibly for finitely many exponents p and these are determined by the method. This method is actually quite standard. As far as we know the basic idea is originally due to Serre [47, pages 203–204]. It is also found in Bennett and Skinner [6, Proposition 4.3]. We shall however give a more careful version than is found in the literature, thereby maximizing the probability of success.

Proposition 7.1. (Method I) *Let D, d_1, d_2 be a triple of integers satisfying (i)–(v) of Lemma 4.1. Let f be a newform with Fourier expansion as in (11) having coefficients in the ring of integers of a number field K, and let $\mathcal{N}_{K/\mathbb{Q}}$ denote the norm map. If $l \nmid 2D$ is prime, let*

$$B_l''(f) = \operatorname{lcm}\left\{\mathcal{N}_{K/\mathbb{Q}}(a_l(E_t) - c_l) \ : \ t \in \mathbb{F}_l, \ t^2 + d_2 \not\equiv 0 \pmod{l}\right\},$$

$$B_l'(f) = \begin{cases} B_l''(f), & \text{if } \left(\frac{-d_2}{l}\right) = -1, \\ \operatorname{lcm}\left\{B_l''(f), \mathcal{N}_{K/\mathbb{Q}}(l+1+c_l), \mathcal{N}_{K/\mathbb{Q}}(l+1-c_l)\right\}, & \text{if } \left(\frac{-d_2}{l}\right) = 1, \end{cases}$$

and

$$B_l(f) = \begin{cases} l\, B_l'(f), & \text{if } K \neq \mathbb{Q}, \\ B_l'(f), & \text{if } K = \mathbb{Q}. \end{cases}$$

If p satisfies condition (6), and if (t, s, p) is a solution to equation (10) arising from the newform f then p divides $B_l(f)$.

Proof. The Proposition follows almost immediately from Lemmas 6.3, 6.4. □

Under the assumptions made (in this Proposition), Method I eliminates all but finitely many exponents p provided of course that $B_l(f)$ is non-zero. Accordingly, we shall say that Method I is successful if there exists some prime $l \nmid 2D$ so that $B_l(f) \neq 0$. There are two situations where Method I is guaranteed to succeed:

- If the newform f is not rational. In this case, for infinitely many primes l, the Fourier coefficient $c_l \notin \mathbb{Q}$ and so all the differences $a_l(E_t) - c_l$ and $l + 1 \pm c_l$ are certainly non-zero, immediately implying that $B_l(f) \neq 0$.
- Suppose that the newform f is rational, and so corresponds to an elliptic curve E defined over $\mathbb{Q}$. Suppose that E has no non-trivial 2–torsion. By the Čebotarev Density Theorem we know that $\sharp E(\mathbb{F}_l)$ is odd for infinitely many primes l. Let $l \nmid 2D$ be any such prime. From the models for the Frey curves E_t in Tables 1, 2, 3 we see that E_t has non-trivial 2–torsion, and so $l + 1 - a_l(E_t) = \sharp E_t(\mathbb{F}_l)$ is even for any value of $t \in \mathbb{F}_l$, $t^2 + d_2 \neq 0$. In this case $a_l(E_t) - c_l = a_l(E_t) - a_l(E)$ must be odd and cannot be zero. Similarly, the Hasse–Weil bound $|c_l| \leq 2\sqrt{l}$ implies that $l + 1 \pm c_l \neq 0$. Thus $B_l(f)$ is non-zero in this case and Method I is successful.

8. Eliminating Exponents: Method II

The second method is adapted from the ideas of Kraus [26] (see also [51]). It can only be applied to one prime (exponent) p at a time, and if successful it does show that there are no solutions to (10) for that particular exponent.

Let us briefly explain the idea of this second method. Suppose f is a newform with Fourier expansion as in (11), and suppose $p \geq 7$ is a prime. We are interested in solutions to equation (10) arising from f. Choose a small integer n so that $l = np + 1$ is prime with $l \nmid D$. Suppose (t, s) is a solution to equation (10) arising from f. Working modulo l we see that $d_1^2 t^2 + D = y^p$ is either 0 or an n–th root of unity. (Indeed $(y^p)^n = y^{l-1} \equiv 0$ or $1 \pmod{l}$.) Since n is small we can list all such t in $\mathbb{F}_l$, and compute c_l and $a_l(E_t)$ for each t in our list. We may then find that for no t in our list are the relations in Lemma 6.3 satisfied. In this case we have a contradiction, and we deduce that there are no solutions to equation (10) arising from f for the exponent p.

Let us now write this formally. Suppose $p \geq 7$ is a prime number, and n an integer such that $l = np + 1$ is also prime and $l \nmid D$. Define

$$\mu_n(\mathbb{F}_l) = \{\zeta \in \mathbb{F}_l^* \ : \ \zeta^n = 1\} \quad \text{and} \quad A(n, l) = \left\{\zeta \in \mu_n(\mathbb{F}_l) \ : \ \left(\frac{\zeta - D}{l}\right) = 0 \text{ or } 1\right\}.$$

For each $\zeta \in A(n, l)$, let δ_ζ be an integer satisfying

$$\delta_\zeta^2 \equiv (\zeta - D)/d_1^2 \pmod{l}.$$

It is convenient to write $a_l(\zeta)$ for $a_l(E_{\delta_\zeta})$. We can now give our sufficient condition for the insolubility of (10) for the given exponent p.

Proposition 8.1. (Method II) *Let D, d_1, d_2 be a triple of integers satisfying (i)–(v) of Lemma 4.1, and $p \geq 7$ be a prime satisfying condition (6). Let f be a newform with Fourier expansion as in (11) defined over a number field K. Suppose there exists an integer $n \geq 2$ satisfying the following conditions:*

(a) *The integer $l = np + 1$ is prime, and $l \nmid D$.*
(b) *Either $\left(\frac{-d_2}{l}\right) = -1$, or $p \nmid \mathcal{N}_{K/\mathbb{Q}}(4 - c_l^2)$.*
(c) *For all $\zeta \in A(n, l)$ we have*

$$\begin{cases} p \nmid \mathcal{N}_{K/\mathbb{Q}}(a_l(\zeta) - c_l), & \text{if } l \equiv 1 \pmod{4}, \\ p \nmid \mathcal{N}_{K/\mathbb{Q}}(a_l(\zeta)^2 - c_l^2), & \text{if } l \equiv 3 \pmod{4}. \end{cases}$$

Then the equation (10) does not have any solutions for the given exponent p arising from the newform f.

Proof. Suppose that the hypotheses of the Proposition are satisfied, and that (t, s) is a solution to equation (10).

First we show that $t^2 + d_2 \not\equiv 0 \pmod{l}$. Suppose otherwise. Thus $t^2 + d_2 \equiv 0 \pmod{l}$ and so $l \mid s$. In this case $\left(\frac{-d_2}{l}\right) = 1$, and from (b) we know that p does not divide $\mathcal{N}_{K/\mathbb{Q}}(4 - c_l^2)$. However, by Lemma 6.3 we know that $\pm c_l \equiv l + 1 \equiv 2 \pmod{\mathfrak{P}}$ for some place $\mathfrak{P}$ of K above p, and we obtain a contradiction showing that $t^2 + d_2 \not\equiv 0 \pmod{l}$.

From equation (10) and the definition of e in (8) we see the existence of some $\zeta \in A(n, l)$ such that

$$d_1^2 t^2 + D \equiv \zeta \pmod{l} \quad \text{and} \quad t \equiv \pm\delta_\zeta \pmod{l}.$$

Replacing t by $-t$ in the Frey curve E_t has the effect of twisting the curve by -1 (this can be easily verified for each Frey curve in Tables 1, 2, 3). Thus $a_l(\zeta) = a_l(E_t)$ if $l \equiv 1 \pmod{4}$ and $a_l(\zeta) = \pm a_l(E_t)$ if $l \equiv 3 \pmod{4}$. Moreover, by Lemma 6.3, $a_l(E_t) \equiv c_l \pmod{\mathfrak{P}}$ for some place $\mathfrak{P}$ of K above p. This clearly contradicts (c). Hence there is no solution to (10) arising from f for the exponent p. □

If the newform f is rational and moreover corresponds to an elliptic curve with 2–torsion, then it is possible to strengthen the conclusion of Proposition 8.1 by slightly strengthening the hypotheses. The following variant is far less costly in computational terms as we explain below.

Proposition 8.2. (Method II) *Let D, d_1, d_2 be a triple of integers satisfying (i)–(v) of Lemma 4.1, and p be a prime satisfying condition (6). Let f be a rational newform corresponding to elliptic curve $E/\mathbb{Q}$ with 2–torsion. Suppose there exists an integer $n \geq 2$ satisfying the following conditions:*

(a) *The integer $l = np + 1$ is prime, $l \leq p^2/4$ and $l \nmid D$.*
(b) *Either $\left(\frac{-d_2}{l}\right) = -1$, or $a_l(E)^2 \not\equiv 4 \pmod{p}$.*
(c) *For all $\zeta \in A(n, l)$ we have*

$$\begin{cases} a_l(\zeta) \neq a_l(E), & \text{if } l \equiv 1 \pmod{4}, \\ a_l(\zeta) \neq \pm a_l(E), & \text{if } l \equiv 3 \pmod{4}. \end{cases}$$

Then the equation (10) does not have any solutions for the given exponent p arising from the newform f.

Proof. Comparing this with Proposition 8.1 we see that it is sufficient to show, under the additional assumptions, that if $a_l(\zeta)^2 \equiv a_l(E)^2 \pmod{p}$ then $a_l(\zeta) = \pm a_l(E)$, and if $a_l(\zeta) \equiv a_l(E) \pmod{p}$ then $a_l(\zeta) = a_l(E)$.

Suppose that $a_l(\zeta)^2 \equiv a_l(E)^2 \pmod{p}$ (the other case is similar). Hence $a_l(\zeta) \equiv \pm a_l(E) \pmod{p}$. Now note that both elliptic curves under consideration here have 2–torsion. Hence we can write $a_l(\zeta) = 2b_1$ and $a_l(E) = 2b_2$ for some integers b_1 and b_2. Moreover, by the Hasse–Weil bound we know that $|b_i| \leq \sqrt{l}$. Thus

$$b_1 \equiv \pm b_2 \pmod{p} \quad \text{and} \quad |b_1 + b_2|,\ |b_1 - b_2| \leq 2\sqrt{l} < p$$

since $l < p^2/4$. Thus $b_1 = \pm b_2$ and this completes the proof. □

It remains to explain how this improves our computation. To apply Proposition 8.1 for some p we need to find a prime l satisfying conditions (a), (b), (c). The computationally expensive part is to compute $a_l(E) = c_l$ and $a_l(\zeta)$ for all $\zeta \in A(n, l)$. Let us however consider the application of Proposition 8.2 rather than Proposition 8.1. The computation proceeds as before by checking conditions (a), (b) first. When we come to (c), we note that what we have to check is that

$$\begin{cases} \sharp E_\zeta(\mathbb{F}_l) \neq l + 1 - a_l(E), & \text{if } l \equiv 1 \pmod{4}, \\ \sharp E_\zeta(\mathbb{F}_l) \neq l + 1 \pm a_l(E), & \text{if } l \equiv 3 \pmod{4}, \end{cases}$$

for each $\zeta \in A(n, q)$. Rather than computing $a_l(\zeta)$ for each such ζ, we first pick a random point in $E_\zeta(\mathbb{F}_l)$, and check whether it is annihilated by $l + 1 - a_l(E)$ if $p \equiv 1 \pmod{4}$ and either of the integers $l + 1 \pm a_l(E)$ if $p \equiv 3 \pmod{4}$. Only if this is the case do we need to compute $a_l(\zeta)$ to test condition (c). In practice, for primes $p \approx 10^9$, this brings a 10–fold speed-up in program run time for Method II.

9. Eliminating Exponents: Method III

Occasionally, Methods I and II fail to establish the non-existence of solutions to an equation of the form (10) for a particular exponent p even when it does seem that this equation has no solutions. The reasons for this failure are not clear to us. We shall however give a third method, rather similar in spirit to Kraus' method (Method II), but requiring stronger global information furnished by Proposition 3.1.

Suppose that D, d_1, d_2 are integers satisfying conditions (i)–(v) of Lemma 4.1. Let E_t be one of the Frey curves associated to equation (10), and let f a newform of the level predicted by Proposition 6.2 with Fourier expansion as in (11), defined over a number field K. Define $\mathcal{T}_l(f)$ to be the set of $\tau \in \mathbb{F}_l$ such that

- either $p \mid \mathcal{N}_{K/\mathbb{Q}}(a_l(E_\tau) - c_l)$ and $\tau^2 + d_2 \not\equiv 0 \pmod{l}$,
- or $p \mid \mathcal{N}_{K/Q}(l + 1 \pm c_l)$ and $\tau^2 + d_2 \equiv 0 \pmod{l}$.

We suppose that $-D$ is not a square and follow the notation of Section 3. Fix a prime p satisfying (6). Suppose l is a prime satisfying the following conditions:

(a) $l \nmid 2D$.
(b) $l = np + 1$ for some integer n.
(c) $\left(\frac{-D_2}{l}\right) = 1$, thus l splits in $\mathcal{L} = \mathbb{Q}(\sqrt{-D_2})$, say $(l) = \mathfrak{l}_1\mathfrak{l}_2$.
(d) Each $\gamma \in \Gamma$ is integral at l; what we mean by this is that each γ belongs to the intersection of the localizations $\mathcal{O}_{\mathfrak{l}_1} \cap \mathcal{O}_{\mathfrak{l}_2}$.

We denote the two natural reduction maps by θ_1, $\theta_2 : \mathcal{O}_{\mathfrak{l}_1} \cap \mathcal{O}_{\mathfrak{l}_2} \to \mathbb{F}_l$. These of course correspond to the two square-roots for $-D_2$ in $\mathbb{F}_l$, and are easy to compute.

Now let Γ_l be the set of $\gamma \in \Gamma$ for which there exists $\tau \in \mathcal{T}_l(f)$ such that

- $(d_1\tau + D_1\theta_1(\sqrt{-D_2}))^n \equiv \theta_1(\gamma)^n$ or $0 \pmod{l}$, and
- $(d_1\tau + D_1\theta_2(\sqrt{-D_2}))^n \equiv \theta_2(\gamma)^n$ or $0 \pmod{l}$.

Proposition 9.1. (Method III) *Let p be a prime satisfying condition (6). Let S be a set of primes l satisfying the conditions (a)–(d) above. With notation as above, if the newform f gives rise to a solution (t, s) to equation (10), then $d_1t+D_1\sqrt{-D_2} = \gamma\beta^p$ for some $\beta \in \mathcal{O}$ and some $\gamma \in \cap_{l\in S} \Gamma_l$. In particular, if $\cap_{l\in S} \Gamma_l$ is empty, then the newform f does not give rise to any solution to equation (10) for this exponent p.*

Proof. Suppose that (t, s) is a solution to equation (10) arising from newform f via the Frey curve E_t. Clearly $\theta_1(t) = \theta_2(t)$ is simply the reduction of t modulo l. Let $\tau = \theta_1(t) = \theta_2(t) \in \mathbb{F}_l$. It follows from Lemma 6.3 that $\tau \in \mathcal{T}_l(f)$. Let (x, y) be the solution to equation (9) corresponding to (t, s). Thus $x = d_1t$. We know by Proposition 3.1 that

$$d_1t + D_1\sqrt{-D_2} = \gamma\beta^p,$$

for some $\gamma \in \Gamma$ and $\beta \in \mathcal{O}$. Applying θ_i to both sides and taking n–th powers (where we recall that $l = np + 1$) we obtain

$$(d_1\tau + D_1\theta_i(\sqrt{-D_2}))^n \equiv \theta_i(\gamma)^n\theta_i(\beta)^{l-1} \pmod{l} \text{ with } \theta_i(\beta)^{l-1} \equiv 0 \text{ or } 1 \pmod{l}.$$

Thus $\gamma \in \Gamma_l$ as defined above. The Proposition follows. ☐

10. Examples

It is clear that our three modular methods require computations of newforms of a given level. Fortunately the computer algebra suit `MAGMA` has a package completely devoted to such computations; the theory for these computations is explained by Cremona [19] for rational newforms, and by Stein [54] in the general case. As an alternative, we could have used William Stein's Modular Forms Database [53].

Example 2. Absence of Newforms

Lemma 4.1 and Proposition 6.2 lead us to associate solutions to equation (9), where p satisfies (6), with newforms of certain levels. If there are no newforms of the predicted levels, we immediately deduce that there are no solutions to equation (9).

With the help of a `MAGMA` program we found all $D = 1, 2, \ldots, 100$ where there are no newforms at the predicted levels. We deduce the following result.

Corollary 10.1. *Let D be an integer belonging to the list*

$$4,\ 16,\ 32,\ 36,\ 64.$$

Then the equation (9) does not have any solutions with p satisfying condition (6).

This Corollary does not add anything new, since equation (1) has already been solved by Cohn's method for $D = 4, 16, 32, 36, 64$ (but see [24], [49], [30]).

Example 3. Corollary 5.2 solves equation (3) for all values of D in the range (2) except for 21 values; these are the 19 values listed in (5) plus $D = 55, 95$. As indicated in Section 2 the cases $D = 55$ and 95 have been solved by Bennett and Skinner. It is however helpful to look at the case $D = 95$ again as it shows how Methods I, III work together in harmony. There is only one possible signature $(d_1, d_2) = (1, 95)$. Thus $t = x$, $s = y$ and we need to solve the equation

$$t^2 + 95 = s^p, \quad \text{where} \quad p \geq 7. \tag{12}$$

Since $d_1 = 1$, it follows from Corollary 5.2 that y is even, and so $t = x$ is odd. Replacing t by $-t$ if necessary, we can assume that $t \equiv 1 \pmod 4$. Table 1 leads us to associate the solution (t, s, p) with the Frey curve

$$E_t \;:\quad Y^2 + XY = X^3 + \left(\frac{t-1}{4}\right) X^2 + \left(\frac{t^2+95}{64}\right) X.$$

From Proposition 6.2, we know that any solution to equation (12) arises from a newform of level 190. Using `MAGMA` we find that there are, up to Galois conjugacy, precisely four newforms at level 190. These are

$$\begin{aligned}
f_1 &= q - q^2 - q^3 + q^4 - q^5 + q^6 - q^7 + O(q^8),\\
f_2 &= q + q^2 - 3\,q^3 + q^4 - q^5 - 3\,q^6 - 5\,q^7 + O(q^8),\\
f_3 &= q + q^2 + q^3 + q^4 + q^5 + q^6 - q^7 + O(q^8),\\
f_4 &= q - q^2 + \phi\, q^3 + q^4 + q^5 - \phi\, q^6 + \phi\, q^7 + O(q^8), \quad \text{where} \quad \phi^2 + \phi - 4 = 0.
\end{aligned}$$

The first three newforms above are rational, and so correspond to the three isogeny classes of elliptic curves of conductor 190. It turns out that none of these elliptic curves have non-trivial 2–torsion. By the remarks made after Proposition 7.1 we know that Method I will be successful in eliminating all but finitely many exponents p. Indeed we find (in the notation of Proposition 7.1) that $B_3(f_1) = B_3(f_3) = 15$. Thus we know that no solutions to equation (12) arise from the newforms f_1 or f_3, since otherwise, by Proposition 7.1, $p \mid 15$ which contradicts $p \geq 7$. We also find that $B_3(f_4) = 2^4 \times 3$ and $B_7(f_4) = 2^4 \times 7$. Thus no solution arises from f_4. But,

$$\begin{aligned}
&B_3(f_2) = 3 \times 7, && B_7(f_2) = 3^2 \times 5 \times 7, && B_{11}(f_2) = 0,\\
&B_{13}(f_2) = 3 \times 5 \times 7 \times 13, && B_{17}(f_2) = 3^2 \times 7 \times 11. &&
\end{aligned}$$

We deduce that there are no solutions arising from f_2 with exponent $p > 7$. It does however seem likely that there is a solution with $p = 7$. Moreover, an attempt to prove that there is no solution with $p = 7$ using Method II fails: we did not find any integer $2 \leq n \leq 100$ satisfying the conditions of Proposition 8.1.

We apply Method III (and follow the notation of Section 9). Write $\omega = \frac{1+\sqrt{-95}}{2}$. Taking $S = \{113, 127, 239, 337, 491\}$ we find that

$$\cap_{l \in S} \Gamma_l = \left\{ \frac{-528 - 2\omega}{2187} \right\}.$$

Thus if we have any solutions at all then, by Proposition 9.1, we know that

$$(t-1) + 2\omega = \left(\frac{-528 - 2\omega}{2187} \right) (U + V\omega)^7,$$

for some integers U, V. Equating imaginary parts and simplifying we get

$$\begin{aligned} -U^7 - 1855VU^6 - 5061V^2U^5 + 214165V^3U^4 + 416605V^4U^3 \\ - 2834013V^5U^2 - 2944375V^6U + 2818247V^7 = 2187. \end{aligned}$$

Using `pari/gp` we find that the only solution to this Thue equation is given by $U = -3$, $V = 0$. This shows that $(t, s) = (529, 6)$.

The reader will notice that $(t, s) = (-529, 6)$ is also a solution to equation (12) with $p = 7$ but it seems to have been 'missed' by the method. This is not the case; we are assuming that the sign of t has been chosen so that $t \equiv 1 \pmod 4$. The solution $(t, s) = (-529, 6)$ arises from some other newform (probably at some different level) and via a different Frey curve which we have not determined.

Example 4. For our last example we look at the case where $D = 25$. This, like 18 other cases, must be resolved by a combination of the modular approach and our lower bound for linear forms in three logarithms which is to come. We assume that $p \geq 7$, and so p satisfies conditions (6). There are now two possible signatures $(d_1, d_2) = (1, 25)$ and $(5, 1)$ satisfying the conditions of Lemma 4.1. However, by Corollary 5.2, we may suppose that $d_1 > 1$ and so $d_1 = 5$, $d_2 = 1$. We write $t = x/5$, $s = y/5$ where we know that t, s are integral by Lemma 4.1. Equation (10) becomes

$$t^2 + 1 = 5^{p-2} s^p, \quad t \neq \pm 1.$$

Following Table 1, we associate with any solution to this equation the Frey curve

$$E_t : \qquad Y^2 = X^3 + 2tX^2 - X,$$

and we know by Proposition 6.2 that any solution must arise from a newform of level 160. Using the computer algebra system `MAGMA` we find that there are up to Galois conjugacy three such newforms:

$$\begin{aligned} f_1 &= q - 2q^3 - q^5 - 2q^7 + O(q^8), \\ f_2 &= q + 2q^3 - q^5 + 2q^7 + O(q^8), \\ f_3 &= q + 2\sqrt{2}q^3 + q^5 - 2\sqrt{2}q^7 + O(q^8). \end{aligned}$$

The first two newforms are rational, corresponding respectively to elliptic curves 160A1 and 160B1 in Cremona's tables [19]. The third has coefficients in $K = \mathbb{Q}(\sqrt{2})$ and is straightforward to eliminate using Method I. In the notation of Proposition 7.1 we find that if f_3 does give rise to any solutions (t, s, p) then $p \mid B_3(f_3) = 24$. This is impossible as $p \geq 7$, and so f_3 does not give rise to any solutions.

We were unable to eliminate newforms f_1 and f_2 using Method I. Instead using our implementation of Method II in `MAGMA` we showed that there are no solutions arising from either form with $7 \leq p \leq 100$. With our implementation of the improved Method II (Proposition 8.2) in `pari/gp` we showed that there are no solutions with $100 \leq p \leq 163762845$; this took roughly 26 hours on 2.4 GHz

TABLE 4. Computational details for Lemma 11.1 and its proof.

D	(d_1, d_2)	E [a]	p_0	Machine [b]	Time
7	$(1,7)$	14A1	181 000 000	P1	26h, 43mn
15	$(1,15)$	30A1	624 271 465	S1	252h, 50mn
18	$(3,2)$	384D1, 384A1, 384G1, 384H1	306 111 726	S3	293h, 14mn
23	$(1,23)$	46A1	855 632 066	S2	477h, 36mn
25	$(5,1)$	160A1, 160B1	163 762 845	P2	25h, 58mn
28	$(2,7)$	14A1	315 277 186	P1	55h, 41mn
31	$(1,31)$	62A1	860 111 230	S3	242h, 2mn
39	$(1,39)$	78A1	852 830 725	P1	193h, 41mn
45	$(3,5)$	480B1, 480F1, 480G1, 480H1	340 749 424	S1	448h, 43mn
47	$(1,47)$	94A1	1 555 437 629	S3	451h, 34mn
60	$(2,15)$	30A1	358 541 296	S1	130h, 30mn
63	$(1,63)$	42A1	292 825 735	S1	99h, 45mn
71	$(1,71)$	142C1	2 343 468 548	S3	697h, 26mn
72	$(3,8)$	96A1, 96B1	451 620 034	S1	316h, 27mn
79	$(1,79)$	158E1	1 544 381 661	S3	448h, 47mn
87	$(1,87)$	174D1	1 148 842 108	S3	329h, 45mn
92	$(2,23)$	46A1	996 255 151	S3	285h, 10mn
99	$(3,11)$	1056B1, 1056F1	593 734 622	P2	138h, 46mn
100	$(5,4)$	20A1	163 762 845	P1	21h, 23mn

[a] We give here the Cremona code for the elliptic curves E as in his book [19] and his online tables: `http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html`

[b] The machines are as follows

P1 2.2 GHz Intel Pentium PC.
P2 2.4 GHz Intel Pentium PC.
S1 Dual processor 750MHz UltraSPARC III.
S2 650 MHz UltraSPARC IIe.
S3 UltraSPARCIII with 12 processors of 1050 MHz speed.

Pentium IV PC. The choice of where to stop the computation is of course not arbitrary, but comes out of our bound for the linear form in logarithms. We will later prove that $p \leq 163762845$ thereby completing the resolution of this case.

11. RESULTS III

We applied the methods of the previous sections to solve all equations (3) with D is our range (2).

Lemma 11.1. *Suppose* $1 \leq D \leq 100$ *and* p *is a prime satisfying (6). If* (x, y, p) *is a solution to equation (3) that is not included in the tables, then* D *is one of*

(13) 7, 15, 18, 23, 25, 28, 31, 39, 45, 47, 60, 63, 71, 72, 79, 87, 92, 99, 100.

Moreover (x, y, p) *has signature* (d_1, d_2) *and arises from an elliptic curve* E *and* $p > p_0$ *where* E, p_0 *and* (d_1, d_2) *are given by Table 4.*

Proof. We wrote a MAGMA program that does the following: For each D in the range (2) we write down the set of possible signatures (d_1, d_2) satisfying the conditions of Lemma 4.1.

For each such pair (d_1, d_2) write down the (one or two) Frey curves given by the Tables 1, 2, 3, bearing in mind the information given by Corollary 5.2.

For each Frey curve we compute the conductor (given by Proposition 6.2) of the newforms giving rise to possible solutions, and then write down all these newforms.

We attempt to eliminate each newform f using Method I. This involves searching for primes $l \nmid 2D$ such that (in the notation of Proposition 7.1) $B_l(f) \neq 0$. If we are successful and find such primes $l_1, \ldots, l_m$ then by Proposition 7.1 this exponent divides all the $B_{l_i}(f)$, and so divides their greatest common divisor B (say). If B is divisible by any prime p that satisfies condition (6) then we attempt to eliminate this possible p using Method II: this involves searching for an integer $2 \leq n \leq 100$ satisfying conditions (a), (b), (c) of Proposition 8.1. If one such n is found then we know that there are no solutions for the exponent p. Otherwise we apply Method III (Proposition 9.1) to write down Thue equations leading to possible solutions.

As predicted by the comments made after Proposition 7.1, Method I succeeded with all non-rational newforms and all rational newforms corresponding to elliptic curves with only trivial 2–torsion (it also succeeded with some rational newforms corresponding to elliptic curves with non-trivial 2–torsion). Indeed, we found no solutions arising from non-rational newforms for D in our range $1 \leq D \leq 100$.

We are left only with rational newforms f that correspond to elliptic curves E having some non-trivial 2–torsion. The details of these are documented in Table 4. For primes $p < 100$ satisfying condition (6) we attempt to show that there are no solutions arising from E for the particular exponent p using Method II (as before). If this fails for a particular exponent p, then we use Method III to write down the Thue equations leading to the possible solutions.

Our proof that $p \geq 100$ is now complete except that there are some Thue equations to solve. We had to solve Thue equations of degree 7 for $D = 7$, 47, 79 and 95. These were solved using pari/gp and the solutions are incorporated in our Tables. We also had to solve a Thue equation of degree 11 for $D = 23$, of degree 17 for $D = 28$, and of degree 13 for $D = 92$. We were unable to (unconditionally) solve these three Thue equations using the built-in functions of pari/gp. The reason is that, in each case, it was impossible for pari/gp to prove that the system of units it had found—though of correct rank—was maximal. We are grateful to Dr. Guillaume Hanrot for sending us his pari program for solving Thue equations without the full unit group. This program, based on [23], solved all three equations in a few minutes.

For the next step we implemented our improved Method II (Proposition 8.2) in pari/gp (see the remark after the proof). To complete the task and show that $p > p_0$ for any missing solution we used our pari/gp program to disprove the existence of any missing solution for each prime $100 \leq p \leq p_0$. We ran this pari/gp program on various machines as indicated in Table 4. The total computer time for this step is roughly 206 days. □

Remark. The reader may be surprised that some of the computations were done in MAGMA while others were carried out in pari/gp. As stated earlier, MAGMA has a package for computing modular forms. This is essential for us, and is unavailable in pari/gp.

For showing that $p > p_0$, it is simply not practical to use `MAGMA`. Here we are using the improved Method II (Proposition 8.2). The main bottle-neck in Method II is computing $a_l(E)$ for primes l that can be about 10^{11} (recall l is a prime satisfying $l \equiv 1 \pmod p$). For this `pari/gp` uses the theoretically slower Shanks-Mestre method [16] rather than the theoretically faster Schoof-Elkies-Atkin [46] method used by `MAGMA`. But for primes of the indicated size it seems that `pari/gp` is about 10 times faster than `MAGMA`.

The reader may also note that two of the machines we used are multiprocessor machines. The computation for each D could have been speeded up considerably by parallelising. We however decided against this, so as to keep our programs simple and transparent.

12. The 'Modular' Lower Bound for y

In this section we would like to use the modular approach to prove a lower bound for y with D in the range (2). Before doing this we prove a general result for arbitrary non-zero D.

Proposition 12.1. *Suppose D is a non-zero integer, and d_1, d_2 satisfy (i)–(v) of Lemma 4.1. Suppose (t, s, p) is a solution to equation (10) arising from a* **rational** *newform f via a Frey curve E_t. Then either* $\mathrm{rad}(s) \mid 2d_1$ *or* $|s| > (\sqrt{p} - 1)^2$.

Proof. Since the newform is rational we know that the newform f corresponds to an elliptic curve $E/\mathbb{Q}$ whose conductor equals the level of f.

Suppose $\mathrm{rad}(s)$ does not divide $2d_1$. Since t and d_2 are coprime we see that there is some prime $l \mid s$ so that $l \nmid 2D$. By Lemma 6.4 we see that p divides $l+1 \pm a_l(E)$. It follows from the Hasse–Weil bound that $l + 1 \pm a_l(E) \neq 0$, and so

$$p \le l + 1 \pm a_l(E) < (\sqrt{l} + 1)^2,$$

using again Hasse–Weil. Thus $l > (\sqrt{p} - 1)^2$. The Proposition follows as $l \mid s$. □

Corollary 12.2. *Suppose D is one of the values in (13). If (x, y, p) is a solution to equation (9) not in the Tables below then $y > (\sqrt{p} - 1)^2$.*

Proof. Suppose D is in the range (2) and (x, y, p) is some solution to equation (9) not in the below Tables. From the preceding sections we know that this solution must satisfy condition (6). Moreover by Lemma 4.1, $x = d_1 t$, and $y = \mathrm{rad}(d_1)s$, where (t, s, p) satisfy equation (10) for some d_1 and d_2 satisfying conditions (i)–(v) of that Lemma.

We have determined for $1 \le D \le 100$ all solutions to (10) arising from non-rational newforms (indeed there were none). Thus we may suppose that our putative solution arises from a rational newform. By Proposition 12.1 we see that either $|y| \ge |s| > (\sqrt{p} - 1)^2$ or $\mathrm{rad}(s) \mid 2d_1$. We must prove that the second possibility does not arise.

Suppose that $\mathrm{rad}(s) \mid 2d_1$. From Lemma 4.1 we see that $\mathrm{rad}(y) \mid 2d_1$. We first show that $\mathrm{rad}(y) \neq 2$. For in this case we have reduced to an equation of the form $x^2 + D = 2^m$. For $|D| < 2^{96}$, Beukers [7, Corollary 2] shows that $m \le 18 + 2\log|D|/\log 2$. A short `MAGMA` program leads us to all the solutions to this equation for $1 \le D \le 100$ and we find that these are already in our tables.

Thus we may suppose that $\mathrm{rad}(y) \mid 2d_1$ and $\mathrm{rad}(y) \neq 2$. An examination of the possible cases reveals the following possibilities

$$D = 18,\ 45,\ 72,\ 99 \text{ and } \mathrm{rad}(y) = 3, \qquad D = 25,\ 100 \text{ and } \mathrm{rad}(y) = 5.$$

On removing the common factors, each case quickly reduces to an equation that has already been solved. For example, we must solve $x^2 + 100 = y^p$ under the assumption that $\mathrm{rad}(y) = 5$ or equivalently the equation $x^2 + 100 = 5^m$. Removing the common factor reduces to the equation $X^2 + 4 = 5^{m-2}$. But $X^2 + 4 = Y^n$ has already been solved and has only the solutions $(X, Y, n) = (2, 2, 3)$, $(11, 5, 3)$. We quickly see that the only solution to $x^2 + 100 = 5^p$ is $(x, p) = (55, 5)$. □

13. The Linear Form in Logarithms

It is useful at this point to recap what we have done so far. We would like to complete the proof of Theorem 1 by showing that our Tables at the end are not missing any solutions. So let us suppose that our Tables at the end are missing some solution (x, y, p) to equation (3) for some value of D in our range (2). We have proved (Lemma 11.1) that D is one of the values in (13). Moreover, (again by Lemma 11.1 and by Corollary 12.2) any missing solution (x, y, p) must satisfy

$$p > p_0, \qquad y \geq (\sqrt{p} - 1)^2, \tag{14}$$

with p_0 given by Table 4. Our aim is to show that $p \leq p_0$: a contradiction.

From the table of values of p_0 we know that

$$|x|,\ p \geq 10^8 \tag{15}$$

and indeed much more, though this inequality is sufficient for much of our later work. In the remainder of this paper we assume that D is one of the remaining values (13), and always write (as before) $D = D_1^2 D_2$, where D_2 is square-free. The triple (x, y, p) will always be a solution to equation (3) supposedly missing from our Tables and hence satisfying the above inequalities.

In this section we write down the linear form in logarithms corresponding to the equation (3) and apply a Theorem of Matveev to obtain upper bounds for the exponent p. These upper bounds obtained from Matveev's Theorem are not small enough to contradict our lower bounds for p obtained in Lemma 11.1 but they are needed when we come to apply our bounds for linear forms in three logarithms given in the next section.

Lemma 13.1. *Let (d_1, d_2) be the signature of our supposedly missing solution (x, y, p) (which we know from Lemma 11.1). Define*

$$d = \begin{cases} d_1, & \text{for } D \not\equiv 7 \pmod 8, \\ 2d_1, & \text{for } D \equiv 7 \pmod 8. \end{cases} \tag{16}$$

Then d is a prime power, say $d = q^c$ for some prime q, where moreover, q splits in $\mathcal{L} = \mathbb{Q}(\sqrt{-D_2})$, say $(q) = \mathfrak{q}\bar{\mathfrak{q}}$. Let k_0 be the smallest positive integer such that the ideal $\bar{\mathfrak{q}}^{k_0}$ is principal, say $\bar{\mathfrak{q}}^{k_0} = (\alpha_0)$. Also let

$$k = \begin{cases} k_0, & \text{if } k_0 \text{ is odd}, \\ k_0/2, & \text{if } k_0 \text{ is even}, \end{cases} \quad \text{and} \quad \kappa = \begin{cases} 2, & \text{if } k_0 \text{ is odd}, \\ 1, & \text{if } k_0 \text{ is even}, \end{cases} \quad \text{so that } k = \frac{\kappa k_0}{2}.$$

Then there exists $\gamma \in \mathcal{L}$ such that

$$\left(\frac{x - D_1\sqrt{-D_2}}{x + D_1\sqrt{-D_2}}\right)^k = \alpha^\kappa \gamma^p, \quad \text{where } \alpha = \bar{\alpha}_0/\alpha_0,\ \mathrm{h}(\alpha) = \frac{k_0 \log d}{2},\ \mathrm{h}(\gamma) = \frac{k \log y}{2}.$$

Proof. We begin with the factorization

$$(x + D_1\sqrt{-D_2})(x - D_1\sqrt{-D_2}) = y^p.$$

Our first step is to show that any prime divisor q of y splits in $\mathcal{L}$. Suppose otherwise, then we may write $(q) = \mathfrak{q}$ or $(q) = \mathfrak{q}^2$ for some prime ideal $\mathfrak{q}$ satisfying $\bar{\mathfrak{q}} = \mathfrak{q}$. If $p = 2r + 1$ then clearly $\mathfrak{q}^r$ divides both factors on the left-hand side above, and so divides $2D_1\sqrt{-D_2}$. This is impossible in view of the fact that p is enormous, and $1 \leq D \leq 100$. Thus we have shown that every prime divisor q of y splits in $\mathcal{L}$. Put

$$y = \prod_{i\in I} {q_i}^{a_i} \quad \text{and} \quad (q_i) = \mathfrak{q}_i\bar{\mathfrak{q}}_i, \ \ \mathfrak{q}_i \neq \bar{\mathfrak{q}}_i, \ \ i \in I, \ \ \text{then} \ \ (x + D_1\sqrt{-D_2}) = \prod_{i\in I}({\mathfrak{q}_i}^{b_i}\bar{\mathfrak{q}}_i^{c_i}),$$

where we assume (for ease of notation) that $b_i \geq c_i$ for all i. Thus

$$(x - D_1\sqrt{-D_2}) = \prod_{i\in I}({\mathfrak{q}_i}^{c_i}\bar{\mathfrak{q}}_i^{b_i}), \quad \text{with} \quad b_i + c_i = pa_i, \quad \text{for all } \ i \in I.$$

Then, clearly,

$$\mathfrak{d} := \gcd\left(x + D_1\sqrt{-D_2}, x - D_1\sqrt{-D_2}\right) = \prod_{i\in I}(\mathfrak{q}_i\bar{\mathfrak{q}}_i)^{c_i} = \prod_{i\in I}(q_i)^{c_i}.$$

This shows that $\mathfrak{d} = (d)$ where $d \in \mathbb{Z}$. We would like to calculate this d and verify that its value is in agreement with (16). From the definition of $\mathfrak{d}$ we see that $d \mid 2x$ and $d \mid 2D_1$. However, by our definition of signature, $\gcd(x^2, D) = d_1^2$. It follows that $d^2 \mid 4d_1^2$ and so $d \mid 2d_1$. But $d_1 \mid x$ and $d_1 \mid D_1$. Hence $d_1 \mid \mathfrak{d}$ and so $d_1 \mid d$. Thus $d = d_1$ or $d = 2d_1$. We note the following cases:

- If $D_2 \not\equiv 7 \pmod 8$ then $2 \nmid y$. Thus $2 \nmid d$ and so $d = d_1$.
- Suppose $D_2 \equiv 7 \pmod 8$. Now from Lemma 4.1 and its proof we know that $D = d_1^2 d_2$ and $x = d_1 t$ where $\gcd(t, d_2) = \gcd(d_1, d_2) = 1$. Clearly $d_2 = d_3^2 D_2$ with $d_3 = D_1/d_1$ integral. Suppose first that d_1 is even. It follows easily that t, d_2 are odd and

$$(d) = \mathfrak{d} = 2d_1\left(\frac{t + d_3\sqrt{-D_2}}{2}, \frac{t - d_3\sqrt{-D_2}}{2}\right). \quad \text{Hence } \ (2d_1) \mid d \ \text{ and so } \ d = 2d_1.$$

- The only case left to consider is $D_2 \equiv 7 \pmod 8$ and d_1 is odd. By examining Table 4 we see that $d_1 = 1$. Thus $2 \mid y$ by Corollary 5.2. Clearly x is odd, and the same argument as above shows that $d = 2 = 2d_1$.

This proves that d satisfies (16). By looking again at the possible values of d_1 in Table 4 we see that d is a prime-power in all cases. Let $j \in I$ such that $d = q_j^{c_j}$. Thus $c_i = 0$ for all $j \neq i$. Then

$$(x + D_1\sqrt{-D_2}) = \bar{\mathfrak{q}}_j^{c_j} \cdot {\mathfrak{q}_j}^{b_j} \cdot \prod_{j\neq i} {\mathfrak{q}_i}^{pa_i},$$

whence

$$(x + D_1\sqrt{-D_2}) = (\bar{\mathfrak{q}}_j\, {\mathfrak{q}_j}^{-1})^{c_j} \cdot \prod_{i\in I} {\mathfrak{q}_i}^{pa_i} = (\mathfrak{a}\,\bar{\mathfrak{a}}^{-1})\,\mathfrak{g}^p,$$

where $\mathfrak{a}$ and $\mathfrak{g}$ are integral ideals with $\mathfrak{a} = \bar{\mathfrak{q}}_j^{c_j}$, $\mathcal{N}(\mathfrak{a}) = {q_j}^{c_j} = d$, $\mathcal{N}(\mathfrak{g}) = y$, and $\mathcal{N}$ denotes the norm. Thus, as ideals,

$$\left(\frac{x - D_1\sqrt{-D_2}}{x + D_1\sqrt{-D_2}}\right) = (\bar{\mathfrak{a}}\,\mathfrak{a}^{-1})^2\,(\bar{\mathfrak{g}}\,\mathfrak{g}^{-1})^p.$$

We define $k_0,\ k,\ \kappa,\ \alpha_0$ as in the statement of the Lemma. Thus $\mathfrak{a}^{k_0} = (\alpha_0)$ and we have the relation (between ideals)

$$(x + D_1\sqrt{-D_2})^k = (\mathfrak{a}/\bar{\mathfrak{a}})^k \mathfrak{g}^{kp} = \mathfrak{a}^{2k}(\mathcal{N}(\mathfrak{a}))^{-k}\mathfrak{g}^{kp} = (\alpha_0)^\kappa (d)^{-k}\, \mathfrak{g}^{kp}.$$

However p is an enormous prime certainly not dividing the class number. This shows that $\mathfrak{g}^k$ is also principal, $\mathfrak{g}^k = (\gamma_0)$, say, where γ_0 is an algebraic integer chosen so that the following equality of elements of $\mathcal{L}$ holds

$$(x + D_1\sqrt{-D_2})^k = \alpha_0^\kappa d^{-k}\gamma_0^p, \quad \text{with} \quad \mathcal{N}(\alpha_0) = d^{k_0} \ \text{ and } \ \mathcal{N}(\gamma_0) = y^k.$$

Put $\alpha = \bar{\alpha}_0/\alpha_0$ and $\gamma = \pm\bar{\gamma}_0/\gamma_0$. The proof of the Lemma is complete except for the statements about the heights of $\alpha,\ \gamma$. These follow from Lemma 13.2 below. □

Lemma 13.2. *Let α be an algebraic number whose conjugates are all (including α itself) of modulus equal to* 1*, then* $\mathrm{h}(\alpha) = (\log a)/\deg\alpha$*, where a is the leading coefficient of the minimal polynomial of α. In particular, if $\alpha = \bar{\alpha}_0/\alpha_0$ where α_0 is a non-real quadratic irrationality, then* $\mathrm{h}(\alpha) = \frac{1}{2}\log\mathcal{N}(\alpha_0)$.

Proof. Set $d = \deg\alpha$. By hypothesis α is a root of a polynomial of $\mathbb{Z}[X]$ of the form $P(X) = aX^d + \cdots$. We have $\mathrm{h}(\alpha) = \frac{1}{d}\log\mathrm{M}(P)$, where M is Mahler's measure, and the first result easily follows since the roots of P are of modulus 1. This proves the first assertion. The (easy) proof of the second assertion is omitted. □

We now write the linear form in three logarithms. Define

$$\Lambda = \log\left(\frac{x - D_1\sqrt{-D_2}}{x + D_1\sqrt{-D_2}}\right),$$

where we have taken the principal determination of the logarithm.

Lemma 13.3.

$$\log|\Lambda| \le -\frac{p}{2}\log y + \log\big(2.2\, D_1\sqrt{D_2}\big).$$

Proof. We will rely on the lower bounds (15). Clearly

$$\left|\frac{x - D_1\sqrt{-D_2}}{x + D_1\sqrt{-D_2}} - 1\right| < 2\,\frac{D_1\sqrt{D_2}}{|x|}.$$

A standard inequality ([52], Lemma B.2) shows that $|\Lambda| < 2.1\,\frac{D_1\sqrt{D_2}}{|x|}$, so that

$$\log|\Lambda| < -\log|x| + \log\big(2.1\, D_1\sqrt{|D_2|}\big).$$

Using the fact that $y^p - x^2 = D$, and a similar argument to the one above, we deduce the Lemma. □

To bound p we use the theory of linear forms of (at most three) logarithms. We need the special case of three logarithms of a Theorem of Matveev.

Theorem 2 (Matveev)**.** *Let $\lambda_1,\ \lambda_2,\ \lambda_3$ be $\mathbb{Q}$–linearly independent logarithms of non-zero algebraic numbers and let $b_1,\ b_2,\ b_3$ be rational integers with $b_1 \ne 0$. Define $\alpha_j = \exp(\lambda_j)$ for $j = 1,\ 2,\ 3$ and*

$$\Lambda = b_1\lambda_1 + b_2\lambda_2 + b_3\lambda_3.$$

Let $\mathcal{D}$ be the degree of the field $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$ over $\mathbb{Q}$. Put $\chi = [\mathbb{R}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{R}]$. Let $A_1,\ A_2,\ A_3$ be positive real numbers, which satisfy

$$A_j \ge \max\big\{\mathcal{D}\mathrm{h}(\alpha_j), |\lambda_j|, 0.16\big\} \quad (1 \le j \le 3).$$

Assume that $B \geq \max\Big\{1, \max\big\{|b_j| A_j/A_1;\ 1 \leq j \leq 3\big\}\Big\}$. *Then*

$$\log|\Lambda| > -C_1\,\mathcal{D}^2\,A_1\,A_2A_3\,\log\big(1.5\,e\mathcal{D}B\log(e\mathcal{D})\big),$$

$$\text{where}\quad C_1 = \frac{5\times 16^5}{6\chi}\,e^3\,(7+2\chi)\left(\frac{3e}{2}\right)^{\chi}\Big(20.2+\log\big(3^{5.5}\mathcal{D}^2\log(e\mathcal{D})\big)\Big).$$

In particulmar, for $\mathcal{D}=2$ *and* $\chi=2$, *this gives*

$$\log|\Lambda| > -1.80741\times 10^{11} A_1\,A_2A_3\,\log(13.80736\,B). \tag{17}$$

Proof. See [35]. □

13.1. **A Preliminary Bound for p.** It follows from Lemma 13.1 that

$$k\Lambda = \kappa\log\alpha + p\log\gamma + iq\pi = \kappa\log\alpha + p\log\gamma + r\log(-1), \quad r\in\mathbb{Z},$$

which appears as a linear form of logarithms. But a small transformation of this form leads to better estimates. Write

$$k\Lambda = \kappa\log(\varepsilon_1\alpha) + p\log(\varepsilon_2\gamma) + iq\pi, \quad q\in\mathbb{Z},$$

where ε_1 and $\varepsilon_2 = \pm 1$ are chosen so that $|\log(\varepsilon_1\alpha)| < \pi/2$ and $|\log(\varepsilon_2\gamma)| < \pi/2$, where we take principal values for the logarithms, and q such that $|\Lambda|$ is minimal.

Remark. Indeed, we can take any roots of unity in $\mathcal{L}$ for ε_1 and ε_2. The only relevant case for our set of outstanding values of D are $D = 25,\ 100$, where $\mathcal{L} = \mathbb{Q}(\sqrt{-1})$, whence we can realize $|\log(\varepsilon_1\alpha)| < \pi/4$ and $|\log(\varepsilon_2\gamma)| < \pi/4$, and we write

$$\Lambda = 2\log\alpha + p\log\gamma + q\log\zeta, \qquad \text{where } \zeta = e^{i\pi/2}.$$

We now return to the general case. By Lemma 13.3

$$\log|k\Lambda| \leq -\frac{p}{2}\,\log y + \log(2.2\,kD_1\sqrt{D_2}).$$

Our lower bounds for x, y and p imply that $\log|k\Lambda|$ is very small and it is straightforward to deduce that $|r| \leq (p+1)/2$. We can write $k\Lambda$ in the form

$$k\Lambda = b_1\lambda_1 + b_2\lambda_2 + b_3\lambda_3$$

with $b_1 = \kappa$ (= 1 or 2), $\alpha_1 = \varepsilon_1\alpha$, $b_2 = p$, $\alpha_2 = \varepsilon_2\gamma$, $b_3 = q$, $\alpha_3 = -1$ and

$$\mathrm{h}(\alpha_1) = \frac{k}{\kappa}\log d,\ \lambda_1 = \log\alpha_1,\ \ \mathrm{h}(\alpha_2) = \frac{k\log y}{2},\ |\lambda_2| < \pi/2,\ \ \mathrm{h}(\alpha_3) = 0,\ \lambda_3 = i\pi,$$

except for the case $\mathcal{L} = \mathbb{Q}(\sqrt{-1})$ studied in the previous remark where $\lambda_3 = i\pi/2$.

Applying Theorem 2, we have $\mathcal{D} = \chi = 2$ and we can take

$$A_1 = \max\left\{\frac{2k\log d}{\kappa}, \frac{\pi}{2}\right\}, \quad A_2 = \max\left\{k\log y, \frac{\pi}{2}\right\}, \quad A_3 = \pi$$

and (using some change of notation in Theorem 2) $B = p+1$ (this choice of B is justified by the inequality $|q| \leq (p+1)/2$ proved above), and we get

$$p \leq C_2 k^2\log(2D_1)\log p.$$

This implies $p \leq C_3 k^2\log(2D_1)\log\big(k^2\log(2D_1)\big)$, and thus

$$p \leq C_4 D_2\log(2D_1)\log\big(D_2\log(2D_1)\big), \tag{18}$$

where the constants ared easily made explicit.

Lemma 13.4. *Suppose D is one of the remaining values (13) and (x,y,p) is a solution to (9) missing from our Tables.*

- *If* $D = 7$ *then* $p < 6.81 \times 10^{12}$.
- *Otherwise, if* D *is square-free then* $p < 1.448 \times 10^{15}$.
- *For other values of* D*, we have* $p < 3.966 \times 10^{14}$.

Proof. This is a simple application of Matveev's Theorem 2. If $D = 7$ it is easy to show that the α_0 arising in Lemma 13.1 is (up to conjugation) $(1 + \sqrt{-7})/2$, we know that $k = 1$; thus $\mathcal{N}(\alpha_0) = 2$ and $\Im(\log \alpha_0) = 1.2094292028\ldots$ Then we can apply (17) with $A_1 = \pi/2$, $A_2 = \log y$, $\log A_3 = \pi$ and $B = p + 1$. After a few iterations we get the stated bound on p.

In the application of Theorem 2, we can take, for all the squarefree values of D,

$$A_1 = \begin{cases} 7 \log 2, & \text{if } k_0 \text{ is odd,} \\ 8 \log 2, & \text{if } k_0 \text{ is even,} \end{cases} \qquad A_2 = \begin{cases} 7 \log y, & \text{if } k_0 \text{ is odd,} \\ 4 \log y, & \text{if } k_0 \text{ is even,} \end{cases} \qquad A_3 = \pi,$$

so that $A_1 A_2 \le 49 \log 2 \times \log y$, and then we get $p < 1.448 \times 10^{15}$.

For all the remaining values of D, we can take

$$A_1 = \begin{cases} \log 10, & \text{if } h = 1, \\ \pi/2, & \text{if } h = 2, \\ 3 \log 2, & \text{if } h = 3, \end{cases} \qquad A_2 = \begin{cases} \log y, & \text{if } h = 1, \\ \log y, & \text{if } h = 2, \\ 3 \log y, & \text{if } h = 3, \end{cases} \qquad A_3 = \pi,$$

so that $A_1 A_2 \le 9 \log 2 \times \log y$, and we get now $p < 3.966 \times 10^{14}$. □

14. A new estimate on linear forms in three logarithms

14.1. **Statement of the result.** We shall apply the following theorem.

Theorem 3. *We consider three non-zero algebraic numbers* α_1, α_2 *and* α_3, *all* $\neq 1$ *which are either all real or all complex of modulus one. Moreover, we assume that*

$$(\mathbf{M}) \qquad \begin{cases} \textit{either } \alpha_1,\ \alpha_2 \textit{ and } \alpha_3 \textit{ are multiplicatively independent, or} \\ \textit{two multiplicatively independent, the third a root of unity } \neq 1. \end{cases}$$

We also consider three non-zero rational integers b_1, b_2, b_3 *with* $\gcd(b_1, b_2, b_3) = 1$, *and the linear form*

$$\Lambda = b_1 \log \alpha_1 + b_2 \log \alpha_2 + b_3 \log \alpha_3 \neq 0,$$

where the $\log \alpha_i$*'s are arbitrary determinations of the logarithm, but which are all real or all purely imaginary. Without loss of generality, we assume that*

$$b_2 |\log \alpha_2| = |b_1 \log \alpha_1| + |b_3 \log \alpha_3| \pm |\Lambda|.$$

Let K, L, R, R_1, R_2, R_3, S, S_1, S_2, S_3, T, T_1, T_2, T_3 *be rational integers which are all* ≥ 3, *with*

$$L \ge 5, \quad R > R_1 + R_2 + R_3, \quad S > S_1 + S_2 + S_3, \quad T > T_1 + T_2 + T_3.$$

Let $\rho > 2$ *be a real number. Assume first that*

$$\left(\frac{KL}{2} + \frac{L}{4} - 1 - \frac{2K}{3L}\right) \log \rho \ \ge (\mathcal{D} + 1) \log N + gL(a_1 R + a_2 S + a_3 T) + \mathcal{D}(K - 1) \log b - 2 \log(e/2), \tag{19}$$

where $N = K^2L$, $\mathcal{D} = [\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{Q}] \,/\, [\mathbb{R}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{R}]$, $e = \exp(1)$,

$$g = \frac{1}{4} - \frac{N}{12RST}, \qquad b = (b_2\eta_0)(b_2\zeta_0)\left(\prod_{k=1}^{K-1} k!\right)^{-\frac{4}{K(K-1)}},$$

with

$$\eta_0 = \frac{R-1}{2} + \frac{(S-1)b_1}{2b_2}, \qquad \zeta_0 = \frac{T-1}{2} + \frac{(S-1)b_3}{2b_2},$$

and

$$a_i \geq \rho|\log\alpha_i| - \log|\alpha_i| + 2\mathcal{D}\,\mathrm{h}(\alpha_i), \qquad i = 1,\ 2,\ 3.$$

If, *for some positive real number* χ, *and* $V := \big((R_1+1)(S_1+1)(T_1+1)\big)^{1/2}$,

(i) $(R_1+1)(S_1+1)(T_1+1) > K\max\{R_1+S_1+1, S_1+T_1+1, R_1+T_1+1, \chi V\}$,

(ii) $\mathrm{Card}\left\{\alpha_1^r\alpha_2^s\alpha_3^t \,:\, 0 \leq r \leq R_1,\, 0 \leq s \leq S_1,\, 0 \leq t \leq T_1\right\} > L$,

(iii) $(R_2+1)(S_2+1)(T_2+1) > 2K^2$,

(iv) $\mathrm{Card}\left\{\alpha_1^r\alpha_2^s\alpha_3^t \,:\, 0 \leq r \leq R_2,\, 0 \leq s \leq S_2,\, 0 \leq t \leq T_2\right\} > 2KL$, *and*

(v) $(R_3+1)(S_3+1)(T_3+1) > 6K^2L$,

then either

$$\Lambda' > \rho^{-KL},$$

where

$$\Lambda' = |\Lambda| \cdot \max\left\{\frac{LRe^{LR|\Lambda|/(2b_1)}}{2|b_1|}, \frac{LSe^{LS|\Lambda|/(2b_2)}}{2|b_2|}, \frac{LTe^{LT|\Lambda|/(2b_3)}}{2|b_3|}\right\},$$

or *at least one of the following conditions* (**C1**), (**C2**), (**C3**) *hold:*

(**Ci**) $\qquad |b_1| \leq R_i$ *and* $|b_2| \leq S_i$ *and* $|b_3| \leq T_i$, $\qquad (i = 1, 2)$

(**C3**) **either** *there exist two non-zero rational integers* r_0 *and* s_0 *such that*

$$r_0b_2 = s_0b_1, \quad \text{with}$$

$$|r_0| \leq B_S := \frac{(R_1+1)(T_1+1)}{\chi V - \max\{R_1, T_1\}} \quad \text{and} \quad |s_0| \leq B_R := \frac{(S_1+1)(T_1+1)}{\chi V - \max\{S_1, T_1\}},$$

or *there exist rational integers* r_1, s_1, t_1 *and* t_2, *with* $r_1s_1 \neq 0$, *such that*

$$(t_1b_1 + r_1b_3)s_1 = r_1b_2t_2, \qquad \gcd(r_1, t_1) = \gcd(s_1, t_2) = 1,$$

which also satisfy, for $\delta = \gcd(r_1, s_1)$,

$$0 < |r_1s_1|/\delta \leq B_T := \frac{(R_1+1)(S_1+1)}{\chi V - \max\{R_1, S_1\}}, \quad |s_1t_1|/\delta \leq B_R \quad \text{and} \quad |r_1t_2|/\delta \leq B_S.$$

Proof. A detailed proof can be found in [38]. It contains many technical improvements when compared to the result proved in [13], but the main progress is a zero-lemma due to M. Laurent [28] which improves [22] and provides an important improvement on the zero-lemma used in our previous paper [13]. $\square$

14.2. **How to use Theorem 3.** To apply the Theorem, we consider an integer $L \geq 5$ and real parameters $m > 0$, $\rho > 2$ (then one can define the a_i) and we put

$$K = \lfloor mLa_1a_2a_3 \rfloor, \qquad \text{with } \ ma_1a_2a_3 \geq 2.$$

To simplify the presentation, we also assume $m \geq 1$ and $a_1,\, a_2,\, a_3 \geq 1$, and put

$$\begin{aligned} R_1 &= \lfloor c_1a_2a_3 \rfloor, \quad & S_1 &= \lfloor c_1a_1a_3 \rfloor, \quad & T_1 &= \lfloor c_1a_1a_2 \rfloor, \\ R_2 &= \lfloor c_2a_2a_3 \rfloor, \quad & S_2 &= \lfloor c_2a_1a_3 \rfloor, \quad & T_2 &= \lfloor c_2a_1a_2 \rfloor, \\ R_3 &= \lfloor c_3a_2a_3 \rfloor, \quad & S_3 &= \lfloor c_3a_1a_3 \rfloor, \quad & T_3 &= \lfloor c_3a_1a_2 \rfloor, \end{aligned}$$

where the c_i's satisfy the conditions (i) up to (v) of the Theorem.

Clearly, condition (i) is satisfied if

$$\big(c_1^3(a_1a_2a_3)^2\big)^{1/2} \geq \chi m a_1a_2a_3L, \quad c_1^2 \cdot a \geq 2mL, \quad \text{where } \ a = \min\{a_1, a_2, a_3\}.$$

Condition (ii) is true when $2c_1^2a_1a_2a_3 \cdot \min\{a_1, a_2, a_3\} \geq L$; we can take

$$c_1 = \max\left\{ (\chi mL)^{2/3}, (2mL/a)^{1/2} \right\}.$$

To satisfy (iii) and (iv) we can take

$$c_2 = \max\left\{ 2^{1/3}(mL)^{2/3}, \sqrt{m/a}\, L \right\}.$$

Finally, because of the hypothesis (**M**), condition (v) holds for

$$c_3 = (6m^2)^{1/3}\, L.$$

Remark. When α_1, α_2, α_3 are multiplicatively independent then it is enough to take c_1 and c_3 as above and $c_2 = 2^{1/3}(mL)^{2/3}$.

Then we have to verify the condition (19). When this inequality holds, one obtains the lower bound $|\Lambda'| > \rho^{-KL}$, and we get

$$\log|\Lambda| > -KL\log\rho - \log\big(\max\{R, S, T\} \cdot L\big),$$

except maybe if at least one of the conditions (**C1**), (**C2**) or (**C3**) holds.

15. Completion of the Proof of Theorem 1

Having given our new bounds for linear forms in three logarithms we now use them to complete the proof of Theorem 1. We have indeed shown in Lemma 11.1 that if (x, y, p) is a missing solution then $p > p_0$ where p_0 is given in Table 4. To complete the proof it is enough to show that $p \leq p_0$. In Section 13 we wrote down the linear form in logarithms we obtain for each outstanding value of D. We will content ourselves by giving the details of this calculation for $D = 7$. The other cases are practically identical (but with different constants).

We have seen in Lemma 13.3 that

$$\Lambda := \log \frac{x - \sqrt{-7}}{x + \sqrt{-7}} \quad \text{satisfies} \quad \log|\Lambda| \leq -\frac{p}{2}\log y + \log\big(2.2\sqrt{7}\big).$$

Writing $\alpha_0 = (1 + \sqrt{-7})/2$ we saw that the linear form is given by

$$\Lambda = 2\log(\varepsilon_1\bar{\alpha}_0/\alpha_0) + p\log(\varepsilon_2\bar{\gamma}/\gamma) + iq\pi, \quad \varepsilon_1,\, \varepsilon_2 = \pm 1,$$

for some rational integer q with $|q| < p$, and we get

$$\log|\Lambda| > -KL\log\rho - \log\big(\max\{R, S, T\} \cdot L\big),$$

except maybe if at least one of the conditions (**C1**), (**C2**) or (**C3**) holds.

Now we proceed effectively to the computation of an upper bound for p. The first step is to recall that we have proved in Lemma 13.4, by applying Matveev's Theorem (Theorem 2), that

$$p < 6.81 \times 10^{12}.$$

We then apply our Theorem 3 with the initial condition $p < 6.81 \times 10^{12}$ and with the lower bound $y \geq 22$; note that we do not yet assume our lower bound (14) obtained through the modular approach. There are two reasons for this:

- The first reason is that we would like to demonstrate how powerful our new lower bound for linear forms in three logarithms is, even without the help of the modular approach.
- The second reason is that when we later make the assumption (14), and apply our lower bound for linear forms in three logarithms, the reader will appreciate the saving brought by the 'modular lower bound' for y.

So for now we assume simply that $y \geq 22$ which holds because y is even, not a power of 2 and that -7 is a quadratic residue for every odd prime factor of y (see [32]). In a few steps we can prove that

$$p < 4.2 \times 10^{8}.$$

The reader should compare this bound with the bound $p < 6.81 \times 10^{12}$ obtained by Matveev's Theorem.

We now assume our 'modular ' lower bound for y in (14), with $p > 1.3 \times 10^{8}$, and then we shall obtain a much better bound for p. We give much more details.

We have to distinguish two cases

$$\text{(I)} \qquad b_1 = 2,\ \alpha_1 = \varepsilon'\bar{\alpha}/\alpha, \quad b_2 = p,\ \alpha_2 = \varepsilon\bar{\gamma}/\gamma, \quad b_3 = q,\ \alpha_3 = -1,$$

and

$$\text{(II)} \qquad b_1 = 2,\ \alpha_1 = \varepsilon'\bar{\alpha}/\alpha, \quad b_2 = q,\ \alpha_2 = -1, \quad b_3 = p,\ \alpha_3 = \varepsilon\bar{\gamma}/\gamma.$$

Let us first consider case (I). Applying Theorem 3 we get

$$p < 4.3 \times 10^{8}$$

with the choices $L = 110$, $\rho = 6$, $m = 71.60226532$, $\chi = 0.7$ and

$$R_1 = 178896,\ S_1 = 29587,\ T_1 = 47734,\ R_2 = 285899,\ S_2 = 47284,\ T_2 = 76285$$

$$\text{and} \quad R_3 = 1975684, \quad S_3 = 326756, \quad T_3 = 527164,$$

unless at least one of the conditions (**C1**), (**C2**), (**C3**) holds. For these values, it is clear that — since we know that $p > 10^{8}$ — conditions (**C1**) and (**C2**) do not hold [1]. The values of B_R and B_T defined in Theorem 3 are equal to

$$B_R = 127, \quad B_T = 483.$$

The first case of condition (**C3**) implies $p \leq B_R = 127$, contradiction. Thus we have to consider the last alternative:

$$(t_1 b_1 + r_1 b_3) s_1 = r_1 t_2 b_2.$$

[1] To be more precise we can take the above values for S_1, S_2 and S_3 independently of y but the R_i's and T_i's have to be increased for $y > 1.3 \times 10^{8}$, as can be seen on the definition of the parameters given in the previous section [a_1 and a_3 are independent of y but not a_2]. Luckily, the larger y is, the better our resulting estimate for p will be and thus we can always replace y by some lower bound for it.

Putting $r_1 = \delta r_1'$ and $s_1 = \delta s_1'$ and simplifying, we get here

$$(2t_1 + \delta r_1' q)s_1' = r_1' t_2 p.$$

which shows that $s_1' = 1$ and $r_1' = 1$ or 2, and gives

$$(2/r_1')t_1 + \delta q = t_2 p, \quad \text{with } |t_2| \le B_T/2.$$

We write $\delta\Lambda = \delta b_1 \log\alpha_1 + \delta b_2 \log\alpha_2 + \big(t_2 b_2 - (b_1/r_1')t_1\big)\log\alpha_3$, that is

$$\delta\Lambda = \frac{2}{r_1'}\log\left(\alpha_1^{r_1'\delta}/\alpha_3^{t_1}\right) + p\log\left(\alpha_2^{\delta}\alpha_3^{t_2}\right) = \text{a linear form in two logarithms}$$

and we apply [29] (with $L = 10$ and $\rho = 16$), which gives now $p < 3\times 10^8$.

Thus we have proved that, in case I,

$$p < 4.3\times 10^8.$$

Concerning case (II), we first notice that in the non-degenerate case we obtain $p < 4.3\times 10^8$ as before. Then we notice that (**C1**) or (**C2**) implies $p \le \max\{T_1, T_2\}$, (the present T_i's play the role of the previous S_i's, and both are bounded independently of y.) Now we study condition (**C3**). For the first alternative $r_0 b_2 = s_0 b_1$, we get $|q| < B_R$, and we can apply [29] to the linear form in two logarithms

$$\Lambda = \Big(\log(\varepsilon'\bar{\alpha}/\alpha)^2 + q\log(-1)\Big) + p\log(\varepsilon\bar{\gamma}/\gamma),$$

which works quite well. Consider now the second alternative, which gives here (we have $t_2 \neq 0$: if $t_2 = 0$, then $p < 10^8$)

$$(2/r_1')t_1 + \delta p = t_2 q', \quad \text{with } |s_1| \le B_S/2 \quad \text{and} \quad q = s_1' q',\ r_1' = 1 \text{ or } 2.$$

We write now $t_2\Lambda = t_2 b_1 \log\alpha_1 + t_2 b_2 \log\alpha_2 + \big(s_1 b_3 + (b_1/r_1')s_1' t_1\big)\log\alpha_3$, that is

$$t_2\Lambda = \frac{2}{r_1'}\log\left(\alpha_1^{r_1' t_2}\alpha_3^{s_1' t_1}\right) + p\log\left(\alpha_2^{t_2}\alpha_3^{s_1}\right)$$

and we apply [29] (again with $L = 10$ and $\rho = 16$), which gives now $p < 2\times 10^8$.

Thus we have proved that, in all cases

$$p < 4.3\times 10^8.$$

Iterating this process four times we obtain that, in all cases

$$p < 1.3\times 10^8,$$

which is indeed better than the upper bound used in the modular computation.

Remark. We notice that without the modular lower bound for y we were able to show that $p < 1.11\times 10^9$, but with this modular lower bound we were able to improve this to $p < 1.81\times 10^8$. Whilst it is certainly possible to reach the former target with the methods of this paper, it would have taken about 6 times as long as it took to reach the latter. From this it is a plausible guess that without the modular lower bound for y the computational part for the entire proof for all the values of $1 \le D \le 100$ might have taken at least 800 days rather than 206 days.

16. Tables

D	Solutions $(\lvert x\rvert, \lvert y\rvert, n)$
1	$(0, 1, n)$
2	$(5, 3, 3)$
3	
4	$(2, 2, 3), (11, 5, 3)$
5	
6	
7	$(1, 2, 3), (181, 32, 3), (3, 2, 4), (5, 2, 5), (181, 8, 5), (11, 2, 7), (181, 2, 15)$
8	$(0, 2, 3)$
9	
10	
11	$(4, 3, 3), (58, 15, 3)$
12	$(2, 2, 4)$
13	$(70, 17, 3)$
14	
15	$(7, 4, 3), (1, 2, 4), (7, 2, 6)$
16	$(0, 2, 4), (4, 2, 5)$
17	$(8, 3, 4)$
18	$(3, 3, 3), (15, 3, 5)$
19	$(18, 7, 3), (22434, 55, 5)$
20	$(14, 6, 3)$
21	
22	
23	$(2, 3, 3), (3, 2, 5), (45, 2, 11)$
24	
25	$(10, 5, 3)$
26	$(1, 3, 3), (207, 35, 3)$
27	$(0, 3, 3)$
28	$(6, 4, 3), (22, 8, 3), (225, 37, 3), (2, 2, 5), (6, 2, 6), (10, 2, 7), (22, 2, 9), (362, 2, 17)$
29	
30	
31	$(15, 4, 4), (1, 2, 5), (15, 2, 8)$
32	$(7, 3, 4), (0, 2, 5), (88, 6, 5)$
33	
34	
35	$(36, 11, 3)$
36	
37	
38	
39	$(5, 4, 3), (31, 10, 3), (103, 22, 3), (5, 2, 6)$
40	$(52, 14, 3)$
41	
42	
43	
44	$(9, 5, 3)$
45	$(96, 21, 3), (6, 3, 4)$
46	
47	$(13, 6, 3), (41, 12, 3), (500, 63, 3), (14, 3, 5), (9, 2, 7)$
48	$(4, 4, 3), (148, 28, 3), (4, 2, 6)$
49	$(524, 65, 3), (24, 5, 4)$
50	

D	Solutions $(\lvert x\rvert, \lvert y\rvert, n)$
51	
52	
53	$(26, 9, 3), (156, 29, 3), (26, 3, 6)$
54	$(17, 7, 3)$
55	$(3, 4, 3), (419, 56, 3), (3, 2, 6)$
56	$(76, 18, 3), (5, 3, 4)$
57	
58	
59	
60	$(2, 4, 3), (1586, 136, 3), (14, 4, 4), (50354, 76, 5), (2, 2, 6), (14, 2, 8)$
61	$(8, 5, 3)$
62	
63	$(1, 4, 3), (13537, 568, 3), (31, 4, 5), (1, 2, 6), (31, 2, 10)$
64	$(0, 4, 3), (0, 2, 6), (8, 2, 7)$
65	$(4, 3, 4)$
66	
67	$(110, 23, 3)$
68	
69	
70	
71	$(21, 8, 3), (35, 6, 4), (46, 3, 7), (21, 2, 9)$
72	$(12, 6, 3), (3, 3, 4)$
73	
74	$(985, 99, 3), (13, 3, 5)$
75	
76	$(7, 5, 3), (1015, 101, 3)$
77	$(2, 3, 4)$
78	
79	$(89, 20, 3), (7, 2, 7)$
80	$(1, 3, 4)$
81	$(46, 13, 3), (0, 3, 4)$
82	
83	$(140, 27, 3),\ (140, 3, 9)$
84	
85	
86	
87	$(16, 7, 3), (13, 4, 4), (13, 2, 8)$
88	
89	$(6, 5, 3)$
90	
91	
92	$(6, 2, 7), (90, 2, 13)$
93	
94	
95	$(11, 6, 3), (529, 6, 7)$
96	$(23, 5, 4)$
97	$(48, 7, 4)$
98	
99	$(12, 3, 5)$
100	$(5, 5, 3), (30, 10, 3), (198, 34, 3), (55, 5, 5)$

References

[1] R. Apéry, *Sur une équation diophantienne*, C. Rend. Acad. Sci. Paris **251** (1960), 1263–1264.

[2] R. Apéry, *Sur une équation diophantienne*, C. Rend. Acad. Sci. Paris **251** (1960), 1451–1452.

[3] C. Batut, K. Belabas, D. Bernardi, H. Cohen and M. Olivier, *User's guide to PARI-GP*, version 2.1.1. (See also `http://www.parigp-home.de/`.)

[4] C. D. Bennett, J. Blass, A. M. W. Glass, D. B. Meronk, R. P. Steiner, *Linear forms in the logarithms of three positive rational numbers*, J. Théor. Nombres Bordeaux **9** (1997), 97–136.

[5] M. A. Bennett, *Products of consecutive integers*, Bull. London Math. Soc., to appear.

[6] 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.

[7] F. Beukers, *On the generalized Ramanujan–Nagell equation I*, Acta Arith. **XXXVIII** (1981), 389–410.

[8] Yu. Bilu, G. Hanrot, *Solving Thue equations of high degree*, J. Number Theory **60** (1996), 373–392.

[9] Yu. Bilu, G. Hanrot and P. M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*. With an appendix by M. Mignotte. J. reine angew. Math. **539** (2001), 75–122.

[10] W. Bosma, J. Cannon and C. Playoust, *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://www.maths.usyd.edu.au:8000/u/magma/`.)

[11] 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 No.4** (2001), 843–939.

[12] Y. Bugeaud and M. Laurent, *Minoration effective de la distance p–adique entre puissances de nombres algébriques*, J. Number Theory **61** (1996), 311–342.

[13] Y. Bugeaud, M. Mignotte and S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Annals of Math., to appear.

[14] Y. Bugeaud and T. N. Shorey, *On the number of solutions of the generalized Ramanujan–Nagell equation*, J. reine angew. Math. **539** (2001), 55–74.

[15] J. W. S. Cassels and E. V. Flynn, *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2, LMS Lecture Notes Series **230**, Cambridge University Press, 1996.

[16] H. Cohen, *A Course in Computational Algebraic Number Theory*, GTM **138**, Springer-Verlag, 1993.

[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. E. Cremona, *Algorithms for modular elliptic curves*, 2nd edition, Cambridge University Press, 1996.

[20] L. Euler, *Vollständige Einleitung zur Algebra*, Vol. 2., 1770.

[21] J. Gebel, A. Pethő and H. G. Zimmer, *On Mordell's equation*, Compositio Math. **110** (1998), no. 3, 335–367.

[22] N. Gouillon, *Un lemme de zéros*, C. Rend. Acad. Sci. Paris, Ser. I, **335** (2002), 167–170.

[23] G. Hanrot, *Solving Thue equations without the full unit group*, Math. Comp. **69** (2000), 395–405.

[24] W. Ivorra, *Sur les équations $x^p+2^\beta y^p=z^2$ et $x^p+2^\beta y^p=2z^2$*, Acta Arith. **108** (2003), 327–338.

[25] Chao Ko, *On the diophantine equation $x^2=y^n+1$*, $xy\neq 0$, Sci. Sinica (Notes) **14** (1964), 457–460.

[26] A. Kraus, *Sur l'équation $a^3+b^3=c^p$*, Experimental Mathematics **7** (1998), No. 1, 1–13.

[27] A. Kraus and J. Oesterlé, *Sur une question de B. Mazur*, Math. Ann. **293** (1992), 259–275.

[28] M. Laurent, Personal communication, Nov. 2003.

[29] M. Laurent, M. Mignotte and Yu. Nesterenko, *Formes linéares en deux logarithmes et déterminants d'interpolation*, J. Number Theory **55** (1995), 255–265.

[30] M. Le, *On Cohn's conjecture concerning the Diophantine equation $x^2+2^m=y^n$,* Arch. Math. (Basel) **78** (2002), no. 1, 26–35.

[31] V. A. Lebesgue, *Sur l'impossibilité en nombres entiers de l'équation $x^m=y^2+1$*, Nouvelles Annales des Mathématiques (1) **9** (1850), 178–181.

[32] J.-L. Lesage, *Différence entre puissances et carrés d'entiers*, J. of Number Th. **73** (1998), 390–425.

[33] W. Ljunggren, *On the diophantine equation $y^2-k=x^3$*, Acta Arith. **VIII** (1963), 451–463.

[34] W. Ljunggren, *On the diophantine equation* $Cx^2 + D = y^n$, Pacific J. Math. **14** (1964), 585–596.
[35] 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.
[36] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.
[37] M. Mignotte, *Une nouvelle résolution de l'équation* $x^2+7 = 2^n$, Sem. Rend. Fac. sc. Cagliari, **54.2** (1984), 41–43.
[38] M. Mignotte, *A kit on linear forms in three logarithms*, Publ. IRMA, Strasbourg, to appear.
[39] 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.
[40] T. Nagell, *Løsning til oppgave nr 2, 1943, s. 29*, Nordisk Mat. Tidskr. **30** (1948), 62–64.
[41] T. Nagell, *Collected papers of Trygve Nagell*, Vol. 1–4, Edited by Paulo Ribenboim, Queen's Papers in Pure and Applied Mathematics **121**, Queen's University, Kingston, ON, 2002.
[42] B. Poonen and E. F. Schaefer, *Explicit descent on cyclic covers of the projective line*, J. reine angew. Math. **488** (1997), 141–188.
[43] S. Ramanujan, *Question 464*, J. Indian Math. Soc. **5** (1913), 120.
[44] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.
[45] E. F. Schaefer, 2*–Descent on the Jacobians of Hyperelliptic Curves*, J. Number Theory **51** (1995), 219–232.
[46] R. Schoof, *Counting points on elliptic curves over finite fields,* Journal de Théorie des Nombres de Bordeaux **7** (1995), no. 1, 219–254.
[47] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.
[48] T. N. Shorey and R. Tijdeman, *Exponential Diophantine equations*, Cambridge Tracts in Mathematics 87, Cambridge University Press, Cambridge, 1986.
[49] S. Siksek, *On the diophantine equation* $x^2 = y^p + 2^k z^p$, Journal de Théorie des Nombres de Bordeaux **15** (2003), 839–846.
[50] S. Siksek, *The modular approach to Diophantine equations*, in *Explicit Methods in Number Theory*, Panoramas et Synthèses, Société Mathématique De France, to appear.
[51] S. Siksek and J. E. Cremona, *On the Diophantine equation* $x^2 + 7 = y^m$, Acta Arith. **109.2** (2003), 143–149.
[52] N. Smart, *The Algorithmic Resolution of Diophantine Equations*, LMS Student Texts **41**, Cambridge University Press, 1998.
[53] W. A. Stein, *Modular Forms Database*, `http://modular.fas.harvard.edu/Tables`
[54] W. A. Stein, *An introduction to computing modular forms using modular symbols*, to appear in an MSRI proceedings.
[55] M. Stoll, *On the arithmetic of the curves* $y^2 = x^l + A$ *and their Jacobians*, J. reine angew. Math. **501** (1998), 171-189.
[56] M. Stoll, *Implementing 2-descent for Jacobians of hyperelliptic curves*, Acta Arith. **98** (2001), 245-277.
[57] M. Stoll, *On the arithmetic of the curves* $y^2 = x^l + A$*, II* J. Number Theory **93** (2002), 183-206.
[58] R. L. Taylor and A. Wiles, *Ring theoretic properties of certain Hecke algebras*, Annals of Math. **141** (1995), 553–572.
[59] M. Waldschmidt, *Diophantine approximation on linear algebraic groups*, Springer, Berlin, 2000.
[60] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.

Yann Bugeaud, Université Louis Pasteur, U. F. R. de mathématiques, 7, rue René Descartes, 67084 Strasbourg Cedex, France
E-mail address: `bugeaud@math.u-strasbg.fr`

Maurice Mignotte, Université Louis Pasteur, U. F. R. de mathématiques, 7, rue René Descartes, 67084 Strasbourg Cedex, France
E-mail address: `mignotte@math.u-strasbg.fr`

Samir Siksek, Department of Mathematics and Statistics, College of Science, Sultan Qaboos University, P.O. Box 36, Al-Khod 123, Oman
E-mail address: siksek@squ.edu.om