DIFFERENCES BETWEEN PERFECT POWERS : THE LEBESGUE-NAGELL EQUATION

MICHAEL A. BENNETT AND SAMIR SIKSEK

Abstract. We develop a variety of new techniques to treat Diophantine equations of the shape $x^2 + D = y^n$...

1. Introduction

Understanding the gaps in the sequence of positive perfect powers

$$1, 4, 8, 9, 16, 25, 27, 32, 36, 49, 64, 81, \ldots$$

is a problem at once classical and fundamentally difficult. Mihăilescu's Theorem [43] (née Catalan's Conjecture) tells us that 8 and 9 are the only consecutive integers here, but it is not, for instance, a consequence of current technology that there are at most finitely many gaps of length k, for any fixed integer $k > 1$ (though this was conjectured to be the case by Pillai; see e.g. [49]). If we simplify matters by considering instead gaps between squares and other perfect powers, then we can show that such gaps, if nonzero, grow as we progress along the sequence. Indeed, the same is even true of the greatest prime factor of the gaps. Specifically, we have the following, a special case of Theorem 2 of [12]; here, by $P(m)$ we denote the greatest prime divisor of a nonzero integer m.

Theorem 1 (Bugeaud)**.** *Let $n \geq 3$ be an integer. There exists an effectively computable positive constant $c = c(n)$ such that if x and y are coprime positive integers with $y \geq 2$, then*

$$P(x^2 - y^n) \geq c \log n$$

and, for suitably large x,

$$P(x^2 - y^n) \geq \frac{\log\log y}{30n}.$$

This result is a consequence of bounds for linear forms in logarithms, complex and p-adic. As such, it can be made completely explicit and leads to an algorithm for solving the *Lebesgue-Nagell equation*

$$x^2 + D = y^n, \tag{1}$$

where we suppose that x and y are coprime nonzero integers, and that either

(i) D is a fixed integer, or
(ii) all the prime divisors of D belong to a fixed set of primes S.

Date: July 5, 2021.

2010 *Mathematics Subject Classification.* Primary 11D61, Secondary 11D41, 11F80, 11F41.

Key words and phrases. Exponential equation, Lucas sequence, shifted power, Galois representation, Frey curve, modularity, level lowering, Baker's bounds, Hilbert modular forms, Thue equation.

The first-named author is supported by NSERC. The second-named author is supported by an EPSRC Grant EP/S031537/1 "Moduli of elliptic curves and classical Diophantine problems".

The terminology here stems from the fact that equation (1) with $D = 1$ was first solved by V. A. Lebesgue [37], while T. Nagell [45], [46] was the first researcher to study such equations in a systematic fashion.

Regrettably, this algorithm is still, in most instances, not a practical one. Even in the very special case $D = -2$, we are not able to completely solve equation (1) (though there are a number of partial results available in the literature; see e.g. Chen [16]). Almost all the (very extensive) literature on this problem concerns cases where $D > 0$ and y is odd in (1). Under these assumptions, we may solve the equation through appeal to a beautiful result of Bilu, Hanrot and Voutier [8] on primitive divisors in binary recurrence sequences, at least for all but a few small values of n. Proposition 5.1 of [14] (sharpening work of Cohn [19]) provides a very explicit summary of this approach – one bounds the exponent n in (1) in terms of the class numbers of a finite collection of imaginary quadratic fields, depending only upon the primes dividing D; see Section 3 for details. Smaller values of n may be treated via techniques from elementary or algebraic number theory, or through machinery from Diophantine approximation. By way of example, in cases (i) and (ii), equation (1), for fixed n, reduces to finitely many *Thue* or *Thue-Mahler* equations, respectively. These can be solved through arguments of Tzanakis and de Weger [61], [62], [63] (see also [26] for recent refinements).

In case either $D > 0$ and y is even, or if $D < 0$, the literature on equation (1) is much sparser, primarily since the machinery of primitive divisors is no longer applicable. In these cases, other than bounds for linear forms in logarithms, the only general results that we know to apply to equation (1) are derived from the modularity of Galois representations arising from associated Frey-Hellegouarch curves. These are obtained by viewing (1) as a ternary equation of signature $(n, n, 2)$, i.e. as $y^n - D \cdot 1^n = x^2$. Such an approach can work to solve equation (1) in one of two ways, either by

(a) producing an upper bound upon n that is sharper than that coming from linear forms in logarithms, leaving a feasible set of small n to treat, or
(b) failing to produce such an upper bound, but, instead, providing additional arithmetic information that allows one to solve all the remaining Thue or Thue-Mahler equations below the bound coming from linear forms in logarithms.

An example of situation (a) is the case where D is divisible by only the primes in $S = \{5, 11\}$ and y is even. Then Theorem 1.5 of [4] implies that equation (1) has no nontrivial solutions for all prime $n > 11$ and y even; work of Soydan and Tzanakis [59] treats smaller values of n and the case where y is odd. For situation (b), papers of Bugeaud, Mignotte and the second author [14], and of Barros [1] deal with a number of cases of equation (1) with D fixed and positive or negative, respectively.

In the paper at hand, we will concentrate on the first of the two difficult cases, namely when $D > 0$ and y is even in (1) (so that necessarily $D \equiv -1 \pmod 8$), under the additional hypothesis that D is divisible only by a few small primes. For completeness, we will also treat the easier situation where y is odd, under like hypotheses on D. In a companion paper [3], we will consider equation (1) in the other challenging situation where $D < 0$. Our main result in this paper is the complete resolution of equation (1) in case $D > 0$, $P(D) < 13$, $\gcd(x, y) = 1$ and $n \geq 3$. We prove the following.

Theorem 2. *There are precisely* 1240 *triples of positive integers* (x, y, n) *with* $n \geq 3$, $\gcd(x, y) = 1$, $y^n > x^2$ *and*

$$P(x^2 - y^n) < 13.$$

They are distributed as follows.

n	$\#(x,y)$	n	$\#(x,y)$	n	$\#(x,y)$	n	$\#(x,y)$
3	755	7	5	12	4	26	1
4	385	8	17	13	1		
5	11	9	1	14	4		
6	51	10	4	15	1		

This amounts to solving the equation

$$x^2 + 2^{\alpha_2}3^{\alpha_3}5^{\alpha_5}7^{\alpha_7}11^{\alpha_{11}} = y^n, \tag{2}$$

where x, y and n are positive integers, with $\gcd(x,y) = 1$, $n \geq 3$, and the α_i are nonnegative integers, i.e. equation (1), where $D > 0$ is supported only on primes in $S = \{2,3,5,7,11\}$. We note that earlier work along these lines with the exception of the aforementioned paper of Soydan and Tzanakis [59], either treat cases where there are no S-units congruent to $-1 \pmod 8$, so that the analogous equations cannot have y even (see e.g. work of Luca [38] for $S = \{2,3\}$), or simply omit these cases (see Pink [50] for $S = \{2,3,5,7\}$, where solutions with y even are termed *exceptional*). To solve equation (2) completely, we introduce a variety of new techniques, many of which are applicable in a rather more general setting.

2. (Very) small values of n

We begin by treating equation (2) in case $n \in \{3,4\}$. With these handled, we will thus be able to assume, without loss of generality, that $n \geq 5$ is prime. It is worth observing that our methods of proof in this section work equally well in the analogous situation where D is supported on $S = \{2,3,5,7,11\}$, but $D < 0$.

2.1. **Exponent $n = 3$.** If we suppose that $n = 3$ in equation (2), then the problem reduces to one of determining S-integral points on

$$3^{\#S} = 3^5 = 243$$

Mordell elliptic curves of the shape $y^2 = x^3 - k$, where

$$k = 2^{\delta_2}3^{\delta_3}5^{\delta_5}7^{\delta_7}11^{\delta_{11}}, \quad \text{for} \quad \delta_p \in \{0,1,2\}.$$

There are various ways to carry this out; if we try to do this directly using, say, the Magma computer algebra package [9], we very quickly run into problems arising from the difficulty of unconditionally certifying Mordell-Weil bases for some of the corresponding curves. We will instead argue somewhat differently.

Given a solution to equation (2) in coprime integers x and y, consider the Frey-Hellegouarch curve

$$E_{x,y} \;:\; Y^2 = X^3 - 3yX + 2x,$$

which has discriminant

$$\Delta_{E_{x,y}} \;=\; 2^{\alpha_2+6}3^{\alpha_3+3}5^{\alpha_5}7^{\alpha_7}11^{\alpha_{11}}.$$

This model has c-invariants

$$c_4 = 144y \;\text{ and }\; c_6 = -1728x.$$

We may check via Tate's algorithm that this curve is minimal at all primes $p \geq 3$ and, while possibly not minimal at 2, the fact that x and y are coprime implies that a corresponding minimal model over $\mathbb{Q}$ has either

$$c_4 = 144y,\; c_6 = -1728x \;\text{ or }\; c_4 = 9y,\; c_6 = -27x,$$

with the latter case occurring only if xy is odd.

The isomorphism classes of elliptic curves over $\mathbb{Q}$ with good reduction outside $\{2,3,5,7,11\}$ have recently been completely and rigorously determined using two independent approaches, by von Kanel and Matschke [30] (via computation of S-integral points on elliptic curves, based upon

bounds for elliptic logarithms), and by the first author, Gherga and Rechnitzer [5] (using classical invariant theory to efficiently reduce the problem to solutions of cubic Thue-Mahler equations). One finds that there are precisely 592192 isomorphism classes of elliptic curves over $\mathbb{Q}$ with good reduction outside $\{2,3,5,7,11\}$; details are available at e.g.

`https://github.com/bmatschke/s-unit-equations/blob/master/elliptic-curve-tables/good-reduction-away-from-first-primes/K_deg_1/curves_K_1.1.1.1_S_2_3_5_7.txt`

For each such class, we consider the corresponding c-invariants; if both $c_4 \equiv 0 \pmod{144}$ and $c_6 \equiv 0 \pmod{1728}$, we define

$$y = \frac{c_4}{144} \text{ and } x = \frac{|c_6|}{1728}, \tag{3}$$

while if at least one of $c_4 \equiv 0 \pmod{144}$ or $c_6 \equiv 0 \pmod{1728}$ fails to hold, but we have $c_4 \equiv 0 \pmod 9$ and $c_6 \equiv 0 \pmod{27}$, we define

$$y = \frac{c_4}{9} \text{ and } x = \frac{|c_6|}{27}. \tag{4}$$

For the resulting pairs (x,y), we check that $y > 0$ and $\gcd(x,y) = 1$. We find 755 such pairs, corresponding to 812 triples (x,y,n). There are 5 triples with $y > 10^9$, with the largest value of y corresponding to the identity

$$2802134365828801^2 + 2^{16} \cdot 3^6 \cdot 5 \cdot 7^8 \cdot 11^2 = 4282124641^3.$$

2.2. **Exponent $n = 4$.** In this case, we may rewrite equation (2) as

$$(y^2 - x)(y^2 + x) = 2^{\alpha_2} 3^{\alpha_3} 5^{\alpha_5} 7^{\alpha_7} 11^{\alpha_{11}}$$

and so either $\alpha_2 = 0$, in which case

$$u_1 + u_2 = 2y^2, \tag{5}$$

where u_i are coprime $\{3,5,7,11\}$-units, or we have

$$u_1 + u_2 = y^2, \tag{6}$$

where u_i are coprime $\{2,3,5,7,11\}$-units. In each case, since $xy \neq 0$, we may suppose that $u_1 > u_2$. To be precise, we have

$$u_1 u_2 = 3^{\alpha_3} 5^{\alpha_5} 7^{\alpha_7} 11^{\alpha_{11}}, \quad \sqrt{\frac{1}{2}(u_1 + u_2)} = y \quad \text{and} \quad \frac{1}{2}(u_1 - u_2) = x,$$

and

$$u_1 u_2 = 2^{\alpha_2 - 2} 3^{\alpha_3} 5^{\alpha_5} 7^{\alpha_7} 11^{\alpha_{11}}, \quad \sqrt{u_1 + u_2} = y \quad \text{and} \quad u_1 - u_2 = x,$$

in cases (5) and (6), respectively.

As for $n = 3$, we can write down corresponding Frey-Hellegouarch curves which have good reduction outside $\{2,3,5,7,11\}$ (and, additionally in this situation, have nontrivial rational 2-torsion). It is easier to attack this problem more directly. Both equations (5) and (6) take the form $a + b = c^2$, where a and b are $\{2,3,5,7,11\}$-units with $\gcd(a,b)$ square-free. Machinery for solving such problems has been developed by de Weger [64], [65]. Data from an implementation of this by von Kanel and Matschke [30] is available at

`https://github.com/bmatschke/solving-classical-diophantine-equations/blob/master/sums-of-units-equations/sumsOfUnitsBeingASquare__S_2_3_5_7_11.txt`

We find that there are 1418 pairs a, b such that $a+b$ is a square, $\gcd(a,b)$ is square-free, $a \geq b$, and the only primes dividing a and b lie in $\{2,3,5,7,11\}$. We further restrict our attention to those with additionally $a > b \geq 1$ and either $\gcd(a,b) = 1$ (in which case we take $x = a - b$, $y = \sqrt{a+b}$), or $\gcd(a,b) = 2$ (whence we choose $x = \frac{1}{2}(a-b)$ and $y = \sqrt{\frac{1}{2}(a+b)}$). This leads to 385 pairs of coprime, positive integers x, y with $y^4 > x^2$ and $P(y^4 - x^2) < 13$. These pairs actually

lead to 406 triples (x, y, n), since 17 of the values of y are squares and 4 of them are cubes. The largest y we find corresponds to the identity

$$1070528159^2 + 2^{18}3^37^411^2 = 32719^4.$$

For the remainder of the paper, we may therefore assume that the exponent n in equation (2) is prime and ≥ 5.

3. Primitive divisors : equation (2) with y odd

If the variable y is odd in (2), one may use work of Bilu, Hanrot and Voutier [8] on primitive divisors in binary recurrence sequences to quickly solve equation (2) for all but small n. To see this connection, observe that under certain hypotheses, equation (1) with $D > 0$ leads, after factoring over $\mathbb{Q}(\sqrt{-D})$, to an equation of the shape

$$\sum_{r=0}^{(n-1)/2} \binom{n}{2r+1} a^{n-2r-1}(-D)^r = \pm 1, \quad a \in \mathbb{Z},$$

or, equivalently,

$$\frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}} = \pm 1, \tag{7}$$

where $\alpha = a + \sqrt{-D}$. The term on the left-hand side of this latter equation is an element in a Lucas sequence and hence any result guaranteeing that such a quantity is divisible by a prime automatically contradicts equation (7).

More specifically, for our purposes, we have as a starting point a special case of Theorem 2 and Lemmata 2 and 4 of Pink [50] (see also Proposition 5.1 of [14] and Theorem 1 of Cohn [19]; the appeal to [8] is implicit).

Proposition 3.1. *Suppose that $D > 1$ is an integer and write $D = c^2d$ where d is square free. Let h denote the class number of the imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ and suppose that there exist positive integers x and y with y odd, and an odd prime $n \geq 5$ with $\gcd(x, D) = 1$, such that*

$$x^2 + D = y^n.$$

If n fails to divide h, then we have one of

- *there exist integers u and v such that $v \mid c$, $v \neq \pm c$, $x + c\sqrt{-d} = (u + v\sqrt{-d})^n$, $n \mid c^2 - v^2$ and $y = u^2 + dv^2$, or*
- *$(n, D, x) = (5, 19, 22434)$ or $(5, 341, 2759646)$.*

In the first case, we have additionally that

$$n \mid c \prod_{p \mid c} \left(1 - \frac{(-d/p)}{p}\right),$$

where $\left(\frac{\cdot}{p}\right)$ denotes the Kronecker symbol.

In our situation, we can write

$$2^{\alpha_2}3^{\alpha_3}5^{\alpha_5}7^{\alpha_7}11^{\alpha_{11}} = c^2d,$$

with c and d integers, and d squarefree. We verify via Magma that the corresponding quadratic fields $\mathbb{Q}(\sqrt{-d})$ have, in every case, class numbers h satisfying

$$h \in \{1, 2, 4, 8, 12, 32\}.$$

From Proposition 3.1, it thus follows that $n \in \{5, 7, 11\}$. More precisely, a solution to (2) can exist with y odd, $\gcd(x, y) = 1$ and $n \in \{5, 7, 11\}$ only if

- $n^2 \mid c$, or

- $n \,\|\, c$ and $n \mid d$, or
- $n = 5, 11 \mid c$ and $(-d/11) = 1$.

Comparing imaginary parts in the equation $x + c\sqrt{-d} = (u + v\sqrt{-d})^n$, we find that

$$5u^4 - 10u^2v^2d + v^4d^2 = \frac{c}{v} \quad \text{if } n = 5, \tag{8}$$

$$7u^6 - 35u^4v^2d + 21u^2v^4d^2 - v^6d^3 = \frac{c}{v} \quad \text{if } n = 7, \tag{9}$$

and

$$11u^{10} - 165dv^2u^8 + 462v^4d^2u^6 - 330v^6d^3u^4 + 55d^4v^8u^2 - d^5v^{10} = \frac{c}{v} \quad \text{if } n = 11, \tag{10}$$

while, comparing real parts, in each case we have $u \mid x$. Suppose $p \in \{2, 3, 5, 7, 11\}$, $p \neq n$ and that $p \mid c/v$. Since x and y are coprime, it follows that $p \nmid xy$, whence $p \nmid u$. From equations (8), (9) and (10), we have that $p \nmid dv$. If $p = 2$, we therefore have that $y = u^2 + dv^2$ is even, contradicting $p \mid c/v$ and $\gcd(x, y) = 1$. If $p = 3$, each of (8), (9) and (10) yields a contradiction, modulo 3. If $n = 5$, from (8),

$$(v^2d - 5u^2)^2 - 20u^4 \equiv 0 \pmod{p},$$

a contradiction for $p = 7$. If $n = 7$ and $p = 5$, we have that

$$2u^2 + u^2d^2 - v^2d^3 \equiv 0 \pmod{5},$$

again, a contradiction. Finally, if $p = n$ and $p^2 \mid c/v$, it follows that $p \mid dv$, whereby $p \mid u$, contradicting $\gcd(x, y) = 1$. Summarizing, equations (8), (9) and (10) reduce to the Thue-Mahler equations

$$5u^4 - 10u^2v^2d + v^4d^2 = \pm 5^{\delta}11^{\gamma_{11}}, \tag{11}$$

$$7u^6 - 35u^4v^2d + 21u^2v^4d^2 - v^6d^3 = \pm 7^{\delta}11^{\gamma_{11}} \tag{12}$$

and

$$11u^{10} - 165dv^2u^8 + 462v^4d^2u^6 - 330v^6d^3u^4 + 55d^4v^8u^2 - d^5v^{10} = \pm 11^{\delta}5^{\gamma_5}7^{\gamma_7}, \tag{13}$$

respectively, where $\delta \in \{0, 1\}$ and the γ_p are nonnegative integers (with $\gamma_p = 0$ if $p \mid d$). To solve these, we treat the equations

$$5X^4 - 10dX^2Y^2 + d^2Y^4 = \pm 5^{\delta}11^{\gamma_{11}}, \;\; \delta \in \{0, 1\}, \; \gamma_{11} \geq 0$$

and

$$X^4 - 10dX^2Y^2 + 5d^2Y^4 = \pm 11^{\gamma_{11}}, \;\; \gamma_{11} \geq 0,$$

where, in each case, $\gcd(X, Y) = 1$ and

$$d \in \{1, 2, 3, 6, 7, 11, 14, 21, 22, 33, 42, 66, 77, 154, 231, 462\}.$$

Additionally, we solve

$$7X^3 - 35X^2Y + 21XY^2 - Y^3 = \pm 7^{\delta}11^{\gamma_{11}}$$

and

$$11X^5 - 165X^4Y + 462X^3Y^2 - 330X^2Y^3 + 55XY^4 - Y^5 = \pm 11^{\delta}5^{\gamma_5}7^{\gamma_7},$$

in coprime integers X and Y, $\delta \in \{0, 1\}$ and $\gamma_p \geq 0$. In these latter two equations, we have taken $X = u^2$ and $Y = dv^2$.

Appealing to the Thue-Mahler equation solver, implemented in `Magma` and associated to the paper [26], we find solutions as follows :

$$n = 5, \;\; d = 2, \;\; (u, v) = (1, 1), (1, 2),$$
$$n = 5, \;\; d = 7, \;\; (u, v) = (3, 2),$$
$$n = 5, \;\; d = 10, \;\; (u, v) = (1, 1)$$

and

$$n = 5, \quad d = 30, \quad (u, v) = (1, 1).$$

These lead to solutions of equation (2) with

$$(x, y, n) = (1, 3, 5), (241, 9, 5), (241, 3, 10), (4443, 37, 5), (401, 11, 5) \text{ and } (4201, 31, 5).$$

We have thus proved the following.

Proposition 3.2. *The only solutions to (2) with $n \geq 5$ prime, $\gcd(x, y) = 1$ and y odd correspond to the identities*

$$1^2 + 2 \cdot 11^2 = 3^5, \quad 241^2 + 2^3 \cdot 11^2 = 9^5, \quad 401^2 + 2 \cdot 5^3 = 11^5,$$
$$4201^2 + 2 \cdot 3 \cdot 5^3 \cdot 11^4 = 31^5 \quad \textit{and} \quad 4443^2 + 2^2 \cdot 7 \cdot 11^6 = 37^5.$$

The remainder of the paper is devoted to equation (2) in the difficult case where y is even. Under this assumption, we may not appeal to the machinery of primitive divisors. We will instead use three main ingredients...

4. Reduction to Thue-Mahler equations: the case of even y

From the results of the preceding sections, we are left to treat (2) with y even and $n \geq 5$ prime. It therefore remains then to consider the equation

$$x^2 + 3^{\alpha_3} 5^{\alpha_5} 7^{\alpha_7} 11^{\alpha_{11}} = y^n \quad \text{with } y \text{ even}, \quad \gcd(x, y) = 1 \quad \text{and} \quad n \geq 5 \quad \text{prime}. \tag{14}$$

The purpose of this section and the next is to prove the following proposition.

Proposition 4.1. *The only solutions to* (14) *with $n < 2 \times 10^8$ correspond to the identities*

$$31^2 + 3^2 \cdot 7 = 4^5, \quad 5^2 + 7 = 2^5, \quad 181^2 + 7 = 8^5, \quad 17^2 + 3 \cdot 5 \cdot 7^2 = 4^5,$$
$$23^2 + 3^2 \cdot 5 \cdot 11 = 4^5, \quad 130679^2 + 3 \cdot 7^3 \cdot 11^7 = 130^5, \quad 47^2 + 3^4 \cdot 5^2 \cdot 7 = 4^7, \quad 11^2 + 7 = 2^7,$$
$$7^2 + 3^3 \cdot 5 \cdot 11^2 = 4^7, \quad 117^2 + 5 \cdot 7^2 \cdot 11 = 4^7, \quad 103^2 + 3 \cdot 5^2 \cdot 7 \cdot 11 = 4^7,$$
$$\textit{and} \quad 8143^2 + 3^3 \cdot 5 \cdot 7^2 \cdot 11^2 = 4^{13}.$$

We assume without loss of generality that $x \equiv 1 \pmod 4$. As before we shall write

$$3^{\alpha_3} 5^{\alpha_5} 7^{\alpha_7} 11^{\alpha_{11}} = c^2 d, \text{ where } d \text{ is squarefree and } c = 3^{\beta_3} 5^{\beta_5} 7^{\beta_7} 11^{\beta_{11}}. \tag{15}$$

Since y is even, it follows from (14) that $d \equiv -1 \pmod 8$, whence necessarily

$$d \in \{7, 15, 55, 231\}. \tag{16}$$

Let $M = M_d = \mathbb{Q}(\sqrt{-d})$. We note the structure of the class group of M:

$$\mathrm{Cl}(M) \cong \begin{cases} 1 & d = 7 \\ C_2 & d = 15 \\ C_4 & d = 55 \\ C_2 \times C_6 & d = 231. \end{cases}$$

Lemma 4.2. *Let $c' = \pm c$ with the sign chosen so that $c' \equiv 1 \pmod 4$. Let*

$$h = \begin{cases} 1 & d = 7 \\ 2 & d = 2 \\ 4 & d = 55 \\ 6 & d = 231 \end{cases} \quad \textit{and} \quad \eta = r + s\sqrt{-d}, \quad \textit{where} \quad (r, s) = \begin{cases} (1/4, -1/4) & d = 7 \\ (1/8, -1/8) & d = 15 \\ (3/32, 1/32) & d = 55 \\ (5/128, -1/128) & d = 231. \end{cases}$$

Let $0 \le \kappa_n \le h-1$ be the unique integer satisfying $\kappa_n \cdot n \equiv -2 \pmod{h}$. Then there is some non-zero $\mu \in \mathcal{O}_M$ such that

$$\frac{x + c'\sqrt{-d}}{2} \;=\; \eta^{(2+\kappa_n \cdot n)/h} \cdot \mu^n. \tag{17}$$

Moreover, η is supported only on prime ideals dividing 2 and μ is supported only on prime ideals dividing $2y$.

Proof. As $d \equiv -1 \pmod{8}$, the prime 2 splits in $\mathcal{O}_M$ as $2\mathcal{O}_M = \mathfrak{P} \cdot \overline{\mathfrak{P}}$, where

$$\mathfrak{P} \;=\; 2\mathcal{O}_M \;+\; \left(\frac{1+\sqrt{-d}}{2}\right) \cdot \mathcal{O}_M. \tag{18}$$

We may rewrite (14) as

$$\left(\frac{x + c'\sqrt{-d}}{2}\right)\left(\frac{x - c'\sqrt{-d}}{2}\right) \;=\; \frac{y^n}{4}. \tag{19}$$

Note that the two factors on the left hand-side of this last equation are coprime elements of $\mathcal{O}_M$. Since $x \equiv c' \equiv 1 \pmod{4}$, we see that $\mathfrak{P}$ divides the first factor on the left hand-side. We thus deduce that

$$\left(\frac{x + c'\sqrt{-d}}{2}\right) \cdot \mathcal{O}_M \;=\; \mathfrak{P}^{-2} \cdot \mathfrak{A}^n, \tag{20}$$

where $\mathfrak{A}$ is an integral ideal divisible by $\mathfrak{P}$, with $\mathfrak{A} \cdot \overline{\mathfrak{A}} = y\mathcal{O}_M$. The order of the class $[\mathfrak{P}]$ in $\mathrm{Cl}(M)$ is h. Thus $\mathfrak{P}^{-h}$ is principal, and η has been chosen so that $\mathfrak{P}^{-h} = \eta\mathcal{O}_M$. Let $\mathfrak{B} = \mathfrak{P}^{\kappa_n} \cdot \mathfrak{A}$. Then we may rewrite (20) as

$$\left(\frac{x + c'\sqrt{-d}}{2}\right) \cdot \mathcal{O}_M \;=\; \mathfrak{P}^{-(2+\kappa_n \cdot n)} \cdot \mathfrak{B}^n \;=\; \eta^{(2+\kappa_n \cdot n)/h} \cdot \mathfrak{B}^n.$$

Since n is a prime that does not divide the order of $\mathrm{Cl}(M)$, the ideal $\mathfrak{B}$ must be principal. Let μ be a generator for $\mathfrak{B}$. Then

$$\frac{x + c'\sqrt{-d}}{2} \;=\; \pm\eta^{(2+\kappa_n \cdot n)/h} \cdot \mu^n$$

and (17) follows on absorbing the sign into μ. It is clear that η is supported on $\mathfrak{P}$ only. Moreover $\mathfrak{B}$ is an integral ideal with norm $2^{\kappa_n} y$. It follows that μ is supported only on prime ideals dividing $2y$. □

Lemma 4.3. *The only solutions to equation (14) with $5 \le n \le 11$ prime are those given in Proposition 4.1.*

Proof. We drop our requirement that $x > 0$ and replace it with the assumption $x \equiv 1 \pmod{4}$, so that we can apply Lemma 4.2. For each exponent n, there are four cases to consider depending on the value of $d \in \{7, 15, 55, 231\}$ in (15). For each pair (n, d), Lemma 4.2 asserts that (x, c') satisfies (17) with $\mu \in \mathcal{O}_M$. We write

$$\mu = r + s(1 + \sqrt{-d})/2,$$

with r and s rational integers. We will show that $\gcd(r, s) = 1$. If $2 \mid r$ and $2 \mid s$ then $\overline{\mathfrak{P}} \mid \mu$ which contradicts the coprimality of the two factors in the left hand-side of (19). If $\ell \mid r$ and $\ell \mid s$, is an odd prime then again we contradict the coprimality of those two factors. Hence $\gcd(r, s) = 1$.

From (17), we have

$$c' = \frac{1}{\sqrt{-d}}\left(\eta^m \cdot (r + s(1+\sqrt{-d})/2)^n \;-\; \overline{\eta}^m \cdot (r + s(1-\sqrt{-d})/2)^n\right)$$

where $m = (2+\kappa_n \cdot n)/h$. The expression on the right has the form $2^{-hm}F(r,s)$ where $F \in \mathbb{Z}[X,Y]$ is homogeneous of degree n. We therefore, in each case, obtain a Thue-Mahler equation of the form

$$F(r,s) \;=\; 2^{hm} \cdot c' \;=\; \pm 2^{hm} \cdot 3^{\beta_3} 5^{\beta_5} 7^{\beta_7} 11^{\beta_{11}}.$$

We solved these Thue-Mahler equations using the Thue-Mahler solver associated with the paper [26]. This computation took around one day and resulted in the solutions in Proposition 4.1 for $n \in \{5,7\}$; there were no solutions for $n = 11$. □

5. Frey-Hellegouarch curves and related objects

We continue to treat (2) with y even, i.e. equation (14), where we maintain the assumption that $x \equiv 1 \pmod 4$. Although the results of the previous section allow us to assume more, for now we merely impose the following constraint on the exponent: $n \geq 7$ is prime. Following the first author and Skinner [4], we associate to a solution (x,y,n) the Frey-Hellegouarch elliptic curve $F = F(x,y,n)$ defined via

$$F \;:\; Y^2 + XY = X^3 + \left(\frac{x-1}{4}\right) X^2 + \frac{y^n}{64} X. \tag{21}$$

The model here is minimal, semistable, and we note the following invariants,

$$c_4 = x^2 - \frac{3}{4} y^n, \qquad c_6 = -x^3 + \frac{9}{8} x y^n$$

and

$$\Delta_F \;=\; \frac{y^{2n}}{2^{12}}(x^2 - y^n) \;=\; -2^{-12} \cdot 3^{\alpha_3} 5^{\alpha_5} 7^{\alpha_7} 11^{\alpha_{11}} \cdot y^{2n}.$$

We invoke the results of the first author and Skinner [4] (which merely require that $n \geq 7$ is prime). These build on the modularity of elliptic curves over $\mathbb{Q}$ following Wiles and others [66], [10], Ribet's level lowering theorem [52], and the isogeny theorem of Mazur [40]. Write N for the conductor of E and let

$$N' = \frac{N}{\prod_{\substack{\ell \mid\mid N \\ n \mid \mathrm{ord}_\ell(\Delta_F)}} \ell}.$$

The results of the first author and Skinner assert the existence of a weight 2 newform f of level N' such that

$$\overline{\rho}_{F,n} \sim \overline{\rho}_{f,\mathfrak{n}}, \tag{22}$$

with $\mathfrak{n} \mid n$ a prime ideal in the ring of integers $\mathcal{O}_K$ of the Hecke eigenfield K of f.

Lemma 5.1. *$N' = 2R$ where $R \mid 3 \cdot 5 \cdot 7 \cdot 11$. Moreover, for $\ell \in \{3,5,7,11\}$, we have*

$$\ell \nmid N' \iff \alpha_\ell \equiv 0 \pmod n \iff 2\,\mathrm{ord}_\ell(c) + \mathrm{ord}_\ell(d) \equiv 0 \pmod n \tag{23}$$

where b, c are given in (15).

Proof. Since E is semistable, N is squarefree, and therefore N' is squarefree. Note that $\mathrm{ord}_2(\Delta_F) = 2n\,\mathrm{ord}_2(y) - 12$. Thus $2 \mid\mid N$ and $n \nmid \mathrm{ord}_2(\Delta_F)$. Thus $2 \mid\mid N'$.

Next let $\ell \geq 13$. Then $\mathrm{ord}_\ell(\Delta_F) = 2n\,\mathrm{ord}_\ell(y)$ and hence $\ell \nmid N'$. It follows that $N' = 2R$ with $R \mid 3 \cdot 5 \cdot 7 \cdot 11$.

To prove the second part of the lemma, note that, for $\ell \in \{3,5,7,11\}$,

$$\mathrm{ord}_\ell(\Delta) = \alpha_\ell + 2n\,\mathrm{ord}_\ell(y) = 2\,\mathrm{ord}_\ell(c) + \mathrm{ord}_\ell(d) + 2n\,\mathrm{ord}_\ell(y).$$

If $\alpha_\ell = 0$ and $\mathrm{ord}_\ell(y) = 0$, then $\ell \nmid N$ and so $\ell \nmid N'$, and therefore (23) holds. Suppose $\alpha_\ell > 0$ or $\mathrm{ord}_\ell(y) > 0$. Then $\ell \mid\mid N$. By the formula for N', we have $\ell \nmid N'$ if and only if $n \mid \mathrm{ord}_\ell(\Delta)$ which is equivalent to $n \mid \alpha_\ell$. This completes the proof. □

Let f be the weight 2 newform of level N' satisfying (22). Write

$$f = \mathfrak{q} + \sum_{m=2}^{\infty} c_m \mathfrak{q}^m \tag{24}$$

for the usual q-expansion of f. Then $K = \mathbb{Q}(c_1, c_2, \ldots)$, and the coefficients c_i belong to $\mathcal{O}_K$.

Lemma 5.2. *Let $\ell \nmid N'$ be a prime and write*

$$\mathcal{C}'_{f,\ell} = \begin{cases} (\ell+1)^2 - c_\ell^2 & \text{if } K = \mathbb{Q} \\ \ell \cdot ((\ell+1)^2 - c_\ell^2)) & \text{if } K \neq \mathbb{Q}. \end{cases}$$

Let d be as in (15)*, and set*

$$T_\ell(f) = \begin{cases} \{a \in \mathbb{Z} \cap [-2\sqrt{\ell}, 2\sqrt{\ell}] \ : \ \ell + 1 - a \equiv 0 \pmod 4\} & \text{if } (-d/\ell) = 1 \\ \{a \in \mathbb{Z} \cap [-2\sqrt{\ell}, 2\sqrt{\ell}] \ : \ \ell + 1 - a \equiv 0 \pmod 2\} & \text{if } (-d/\ell) = -1 \\ \emptyset & \text{if } \ell \mid d. \end{cases}$$

Let

$$\mathcal{C}_{f,\ell} \ = \ \mathcal{C}'_{f,\ell} \cdot \prod_{a \in T_\ell(f)} (a - c_\ell).$$

If $\overline{\rho}_{F,n} \sim \overline{\rho}_{f,\mathfrak{n}}$, then $\mathfrak{n} \mid \mathcal{C}_{f,\ell}$.

Proof. Suppose $\ell \nmid N'$ and write N for the conductor of F. Suppose $\overline{\rho}_{F,n} \sim \overline{\rho}_{f,\mathfrak{n}}$. A standard consequence [55, Propositions 5.1, 5.2] of this is that

$$\begin{cases} c_\ell \equiv a_\ell(F) \pmod{\mathfrak{n}} & \text{if } \ell \neq n \text{ and } \ell \nmid N \\ c_\ell \equiv \pm(\ell+1) \pmod{\mathfrak{n}} & \text{if } \ell \neq n \text{ and } \ell \mid N. \end{cases}$$

Here the restriction $\ell \neq n$ is unnecessary if $K = \mathbb{Q}$. It follows if $\ell \mid N$ that $\mathfrak{n} \mid \mathcal{C}'_{f,\ell}$. We observe that the discriminant of F can written as

$$\Delta \ = \ (-d) \cdot (cy^n/2^6)^2.$$

If $\ell \mid d$ then $\ell \mid N$ and so we take $\mathcal{C}_{f,\ell} = \mathcal{C}'_{f,\ell}$.

Suppose $\ell \nmid N$ and so $\ell \nmid d$. Thus $c_\ell \equiv a_\ell(F) \pmod{\mathfrak{n}}$. To complete the proof it is sufficient to show that $a_\ell(F) \in T_\ell(f)$. The model for F given in (21) is isomorphic to

$$F \ : \ Y^2 = X^3 + xX^2 + \frac{y^n}{4} X, \tag{25}$$

and so has a point of order 2. Thus $\ell + 1 - a_\ell(F) = \#F(\mathbb{F}_\ell) \equiv 0 \pmod 2$. Moreover, if $(-d/\ell) = 1$ then the discriminant is a square modulo ℓ, so $F/\mathbb{F}_\ell$ has full 2-torsion, whence $\#F(\mathbb{F}_\ell) \equiv 0 \pmod 4$. Thus $a_\ell(F) \in T_\ell(f)$. □

There are a total of 76 conjugacy classes of newforms f at the levels $N' = 2R$ with $R \mid 3 \cdot 5 \cdot 7 \cdot 11$, of which 59 are rational (and so correspond to elliptic curves). Since there are four possible values of $d \in \{7, 15, 55, 231\}$ this gives $4 \times 76 = 304$ pairs (f, d) to consider. We apply Lemma 5.2 to each pair (f, d), letting

$$\mathcal{C}_{f,d} = \sum \mathcal{C}_{f,\ell} \cdot \mathcal{O}_K$$

where the sum is over all primes $3 \leq \ell < 500$ not dividing N'. It follows from Lemma 5.2 that $\mathfrak{n} \mid \mathcal{C}_{f,d}$. We let

$$C_{f,d} = \mathrm{Norm}_{K/\mathbb{Q}}(\mathcal{C}_{f,d}).$$

Since $\mathfrak{n} \mid n$, we have that $n \mid C_{f,d}$. Of the 304 pairs (f, d), the integer $C_{f,d}$ is identically zero for 114 pairs, and non-zero for the remaining 190 pairs. For the 190 pairs (f, d) where $C_{f,d} \neq 0$, we find that the largest possible prime divisor of any of these $C_{f,d}$ is 11. By the results of the previous section we know all the solutions to (14) with $n \in \{7, 11\}$. We can therefore eliminate

these 190 pairs from further consideration. We focus on the 114 remaining pairs (f, d). Here, each f satisfies $K = \mathbb{Q}$ and so corresponds to an elliptic curve $E/\mathbb{Q}$ whose conductor is equal to the level N' of f. Moreover, each of these elliptic curve E has non-trivial rational 2-torsion. This is unsurprising in view of the remarks following [55, Proposition 9.1]. We observe that $\overline{\rho}_{f,n} \sim \overline{\rho}_{E,n}$. Thus we have 114 pairs (E, d) to consider, and if (x, y, n) is a solution to (14) with $n \geq 13$ prime then there is some pair (E, d) (among the 114) where d satisfies (15) and $E/\mathbb{Q}$ is an elliptic curve such that $\overline{\rho}_{F,n} \sim \overline{\rho}_{E,n}$. In particular, for any prime $\ell \nmid N'$,

$$\begin{cases} a_\ell(E) \equiv a_\ell(F) \pmod{n} & \text{if } \ell \nmid N \\ a_\ell(E) \equiv \pm(\ell + 1) \pmod{n} & \text{if } \ell \mid N. \end{cases}$$

5.1. **The Method of Kraus.**

Lemma 5.3. *Let $c' = \pm c$ with the sign chosen so that $c' \equiv 1 \pmod 4$. Let*

$$\gamma = u + v\sqrt{-d} \quad \textit{where} \quad (u, v) = \begin{cases} (1/8, 3/8) & d = 7 \\ (7/8, 1/8) & d = 15 \\ (3/8, 1/8) & d = 55 \\ (5/16, -1/16) & d = 231. \end{cases}$$

Choose $\epsilon_n \in \{1, -1\}$ to satisfy $n \equiv \epsilon_n \pmod 3$. Then there is some $\delta \in M^*$ such that

$$\frac{x + c'\sqrt{-d}}{x - c'\sqrt{-d}} = \begin{cases} \gamma \cdot \delta^n & \textit{if } d = 7, 15, 55 \\ \gamma^{(2+\epsilon_n \cdot n)/3} \cdot \delta^n & \textit{if } d = 231. \end{cases} \tag{26}$$

Moreover, δ is supported only on prime ideals dividing y.

Proof. From the proof of Lemma 4.2, and in particular (20), we have

$$\left(\frac{x' + c\sqrt{-d}}{x' - c\sqrt{-d}}\right) \cdot \mathcal{O}_M = (\overline{\mathfrak{P}}/\mathfrak{P})^2 \cdot \mathfrak{B}^n \tag{27}$$

with $\mathfrak{B} = \mathfrak{A}/\overline{\mathfrak{A}}$. Here $\mathfrak{P}$ is given by (18), and $\mathfrak{A}$ is an integral ideal dividing y. We observe that $\mathfrak{B}$ is supported only on prime ideals dividing y. First let $d = 7$, 15 or 55. In these cases the fractional ideal $(\overline{\mathfrak{P}}/\mathfrak{P})^2$ is principal, and we have chosen γ so that it is a generator. Since n is a prime not dividing the order of $\mathrm{Cl}(M)$ we have that $\mathfrak{B}$ is also principal. Let $\delta \in M^*$ be a generator of $\mathfrak{B}$. Then

$$\frac{x + c'\sqrt{-d}}{x - c'\sqrt{-d}} = \pm\gamma \cdot \delta^n,$$

and we complete the proof for $d = 7$, 15 and 55 by absorbing the $\pm$ sign into δ.

Suppose now that $d = 231$. The class of the fractional ideal $\overline{\mathfrak{P}}/\mathfrak{P}$ has order 3, and we have chosen γ to be a generator of $(\overline{\mathfrak{P}}/\mathfrak{P})^3$. We may rewrite (27) as

$$\frac{x + c'\sqrt{-d}}{x - c'\sqrt{-d}} = (\overline{\mathfrak{P}}/\mathfrak{P})^{2+\epsilon_n \cdot n} \cdot \mathfrak{C}^n$$

where $\mathfrak{C} = \mathfrak{B} \cdot (\mathfrak{P}/\overline{\mathfrak{P}})^{\epsilon_n}$. Note that $3 \mid (2 + \epsilon_n \cdot n)$ and hence

$$(\overline{\mathfrak{P}}/\mathfrak{P})^{2+\epsilon_n \cdot n} = \gamma^{(2+\epsilon_n \cdot n)/3} \cdot \mathcal{O}_M.$$

The ideal $\mathfrak{C}$ must be principal and hence we complete the proof by letting δ be a suitably chosen generator for $\mathfrak{C}$. We note that in all cases δ is supported only on primes of $\mathcal{O}_M$ dividing y. $\square$

Lemma 5.4. *Let $n \geq 13$ be a prime and (E, d) be one of the remaining 114 pairs. Let $q = kn+1$ be a prime. Suppose that $(-d/q) = 1$, and choose a such that $a^2 \equiv -d \pmod{q}$. Let g_0 be a generator for $\mathbb{F}_q^*$ and $g = g_0^n$. Let (u, v) be as in the statement of Lemma 5.3. If $d = 7$, 15 or 55 then let*

$$\Theta_q' \ = \ \left\{(u + va) \cdot g^i \ : \ i = 0, 1, \ldots, k-1\right\} \subset \mathbb{F}_q.$$

If $d = 231$, then set

$$\Theta_q' \ = \ \left\{(u + va)^{(2+\epsilon_n \cdot n)/3} \cdot g^i \ : \ i = 0, 1, \ldots, k-1\right\} \subset \mathbb{F}_q$$

and, in all cases, let

$$\Theta_q \ = \ \Theta_q' \setminus \{0, 1\}.$$

Suppose the following two conditions hold:

(i) $a_q(E)^2 \not\equiv 4 \pmod{n}$.
(ii) $a_q(E)^2 \not\equiv a_q(H_\theta)^2 \pmod{n}$ *for all* $\theta \in \Theta_q$, *where*

$$H_\theta \ : \ Y^2 = X(X+1)(X+\theta).$$

Then $\overline{\rho}_{F,n} \not\sim \overline{\rho}_{E,n}$.

Proof. We suppose that $\overline{\rho}_{F,n} \sim \overline{\rho}_{E,n}$ and derive a contradiction. Since $n \geq 11$, we note that, in particular, $q \notin \{2, 3, 5, 7, 11\}$. Suppose first that $q \mid y$. Then $q + 1 \equiv \pm a_q(E) \pmod{n}$. But $q+1 = kn+2 \equiv 2 \pmod{n}$ and hence $a_q(E)^2 \equiv 4 \pmod{n}$, contradicting hypothesis (i). We may therefore suppose that $q \nmid y$. In particular q is a prime of good reduction for the Frey curve F, and also for the curve E, whence $a_q(F) \equiv a_q(E) \pmod{n}$.

Since $a^2 \equiv -d \pmod{q}$, by the Dedekind-Kummer theorem the prime q splits in $\mathcal{O}_M$ as a product of two primes $q\mathcal{O}_M = \mathfrak{q} \cdot \overline{\mathfrak{q}}$ where we choose

$$\mathfrak{q} \ = \ q\mathcal{O}_M + (a - \sqrt{-d}) \cdot \mathcal{O}_M. \tag{28}$$

In particular $a \equiv \sqrt{-d} \pmod{\mathfrak{q}}$. Moreover, $\mathbb{F}_\mathfrak{q} = \mathbb{F}_q$. Since $\mathfrak{q} \mid q$ and $q \nmid 2y$, it follows from (19) that $\mathfrak{q} \nmid (x \pm c'\sqrt{-d})$. We let $\theta \in \mathbb{F}_q^*$ satisfy

$$\theta \ \equiv \ \frac{x + c'\sqrt{-d}}{x - c'\sqrt{-d}} \pmod{\mathfrak{q}}. \tag{29}$$

We will contradict hypothesis (ii), and complete the proof, by showing that $\theta \in \Theta_q$ and $a_q(F) = \pm a_q(H_\theta)$. If $\theta \equiv 1 \pmod{q}$ then $\mathfrak{q} \mid 2c'\sqrt{-d}$ giving that $q \mid 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$, which is impossible. Therefore $\theta \not\equiv 1 \pmod{q}$. Let (u, v), γ, δ be as in the statement of Lemma 5.3. Note that γ is supported only at the primes above 2 and that δ is supported at only at the primes above y. Since $\mathfrak{q} \nmid y$, we may reduce γ and δ modulo $\mathfrak{q}$. In particular,

$$\gamma \equiv u + av \pmod{\mathfrak{q}}.$$

Moreover, $\delta^n \pmod{\mathfrak{q}}$ belongs to the subgroup of $\mathbb{F}_q^*$ generated by $g = g_0^n$ of order k. The fact that θ belongs to Θ_q' (and therefore to Θ_q) follows from (29) and (26).

It remains to show that $a_q(F) = \pm a_q(H_\theta)$. The model for F in (21) is isomorphic to the model in (25). We note that the polynomial on the right hand-side of (25) can be factored as

$$X\left(X \ + \ \frac{x + c'\sqrt{-d}}{2}\right)\left(X \ + \ \frac{x - c'\sqrt{-d}}{2}\right). \tag{30}$$

Thus, $F \pmod{\mathfrak{q}}$ is a quadratic twist of H_θ, whence

$$a_q(F) = a_\mathfrak{q}(F) = \pm a_\mathfrak{q}(H_\theta) = \pm a_q(H_\theta),$$

completing the proof. □

Remark. We know by Dirichlet's theorem that the natural density of primes q satisfying the conditions $q = kn+1$ and $(-d/q) = 1$ is $1/2n$. We now give a heuristic estimate for the probability of succeeding to show that $\overline{\rho}_{F,n} \nsim \overline{\rho}_{E,n}$ using a single $q = kn + 1$ that satisfies $(-d/q) = 1$. The set Θ'_q has size k, and so Θ_q has size close to k. For a given $\theta \in \Theta_q$, we expect the probability that $a_q(E)^2 \not\equiv a_q(H_\theta)^2 \pmod{n}$ to be roughly $(1 - 2/n)$. Thus the probability of the criterion succeeding is around $(1-2/n)^k$. In particular, if k is large compared to $n/2$ then we expect failure, but if k is small compared to $n/2$ then we expect success. Moreover, if we fail with one particular value of q, we are likely to fail with larger values of q (which correspond to larger values of k).

However, this heuristic is likely to be inaccurate when $\sqrt{q}$ is small compared to n, since $a_q(E)$ and $a_q(H_\theta)$ both belong to the Hasse interval $[-2\sqrt{q}, 2\sqrt{q}]$, and the probability of the criterion succeeding is around $(1 - 1/\sqrt{q})^k$.

There are 11078932 primes n in the interval $13 \le n < 2 \times 10^8$. Recall that we have 114 remaining pairs (E, d) with $E/\mathbb{Q}$ an elliptic curve and $d \in \{7, 15, 55, 231\}$. We wrote a `Magma` script that applied the criterion of Lemma 5.4 to the $11078932 \times 114 = 1262998248 \approx 1.3 \times 10^9$ triples (E, d, n). For each such triple the script searches for a prime $q = kn+1$ with $k < 10^3$ such that the hypotheses of Lemma 5.4 are satisfied. This computation took around 7000 hours, but, since it was distributed over 114 processors, finished in less than three days. For all but 1230 of the 1262998248 triples (E, d, n) the script found some q satisfying the hypotheses of Lemma 5.4. We are therefore reduced to considering the remaining 1230 triples (E, d, n). While these are somewhat too numerous to record here, we note that the largest value of n appearing in any of these triples is $n = 1861$ and this corresponds to E being the elliptic curve with Cremona label `210A1` and $d = 15$.

5.2. **A refined sieve.** Our adaptation of the method of Kraus (Lemma 5.4) makes use of one auxiliary prime q satisfying $q = kn + 1$ and $(-k/q) = 1$. To treat the remaining 1230 triples (E, d, n), we will use a refined sieve that combines information from several such primes q.

Lemma 5.5. *Let (E, d, n) be one of the remaining 1230 triples. Let $q = kn + 1$ be a prime. Suppose that $(-d/q) = 1$ and choose a such that $a^2 \equiv -d \pmod{q}$. Let c', h, (r, s), κ_n be as in Lemma 4.2, $m = (2 + \kappa_n \cdot n)/h \in \mathbb{Z}$.and set*

$$\rho_1 = (r + sa)^m \quad \text{and} \quad \rho_2 = (r - sa)^m.$$

Let g_0 be a generator for $\mathbb{F}_q^*$ and $g = g_0^n$. Further, let us define

$$\Upsilon''_q \;=\; \left\{\left(\rho_1 \cdot g^i, \rho_2 \cdot g^j\right) \;:\; i = 0, 1, \ldots, k-1,\; j = 0, 1\right\} \subset \mathbb{F}_q \times \mathbb{F}_q,$$

$$\Upsilon'_q \;=\; \left\{(\theta_1, \theta_2) \in \Upsilon''_q \;:\; \theta_1\theta_2(\theta_1 - \theta_2) \neq 0\right\}$$

and

$$\Upsilon_q \;=\; \left\{(\theta_1, \theta_2) \in \Upsilon'_q \;:\; a_q(H_{\theta_1,\theta_2}) \equiv a_q(E) \pmod{n}\right\},$$

where $H_{\theta_1,\theta_2}/\mathbb{F}_q$ is the elliptic curve

$$H_{\theta_1,\theta_2} \;:\; Y^2 = X(X + \theta_1)(X + \theta_2).$$

Write

$$\Phi'_q \;=\; \left\{(\theta_1 - \theta_2)/a \cdot (\mathbb{F}_q^*)^{2n} \;:\; (\theta_1, \theta_2) \in \Upsilon_q\right\} \subset \mathbb{F}_q^*/(\mathbb{F}_q^*)^{2n}$$

and

$$\Phi_q \;=\; \begin{cases} \Phi'_q \cup \{(\omega/a) \cdot (\mathbb{F}_q^*)^{2n} \;:\; \omega = \rho_1,\ \rho_1 g,\ -\rho_2,\ -\rho_2 g\} & \text{if } a_q(E)^2 \equiv 4 \pmod{n} \\ \Phi'_q & \text{otherwise.} \end{cases}$$

If $\overline{\rho}_{F,n} \sim \overline{\rho}_{E,n}$, then necessarily

$$c' \cdot (\mathbb{F}_q^*)^{2n} \;\in\; \Phi_q. \tag{31}$$

Proof. Let $M = \mathbb{Q}(\sqrt{-d})$. Let $\mathfrak{q} \mid q$ be the prime ideal of $\mathcal{O}_M$ given by (28); thus $\mathcal{O}_M/\mathfrak{q} = \mathbb{F}_q$ and $\sqrt{-d} \equiv a \pmod{\mathfrak{q}}$. Let μ be as in Lemma 4.2. From (17) and its conjugate we have

$$\frac{x + c'\sqrt{-d}}{2} \equiv \rho_1 \cdot \mu^n, \qquad \frac{x - c'\sqrt{-d}}{2} \equiv \rho_2 \cdot \overline{\mu}^n \pmod{\mathfrak{q}}. \tag{32}$$

Suppose first that $q \nmid y$. Thus both F and E have good reduction at q, and so $a_q(F) \equiv a_q(E) \pmod{n}$. It follows from (19) that $\mathfrak{q} \nmid ((x \pm c'\sqrt{-d})/2)$ and that $\mathfrak{q} \nmid \mu$, $\overline{\mu}$. Recall that $g = g_0^n$ where g_0 is a generator for $\mathbb{F}_q^*$; it particular, g is a non-square, it generates $(\mathbb{F}_q^*)^n$, and has order k. We note that the class of $\overline{\mu}^n$ modulo $\mathfrak{q}$ is either in $(\mathbb{F}_q^*)^{2n}$ or in $g \cdot (\mathbb{F}_q^*)^{2n}$. Hence there is some $\phi \in (\mathbb{F}_q^*)^{2n}$, and some $0 \le j \le 1$ such that

$$\frac{x - c'\sqrt{-d}}{2} \equiv \rho_2 \cdot g^j \cdot \phi \pmod{\mathfrak{q}}.$$

Now the class of μ^n/ϕ modulo $\mathfrak{q}$ belongs to $(\mathbb{F}_q^*)^n$ and so is equal to g^i for some $0 \le i \le k-1$. We note that

$$\frac{x + c'\sqrt{-d}}{2} \equiv \rho_1 \cdot g^i \cdot \phi \pmod{\mathfrak{q}}.$$

Hence

$$\left(\frac{x + c'\sqrt{-d}}{2}, \frac{x - c'\sqrt{-d}}{2}\right) \equiv (\theta_1 \cdot \phi, \theta_2 \cdot \phi) \pmod{\mathfrak{q}}$$

where $(\theta_1, \theta_2) \in \Upsilon_q''$. Since $\mathfrak{q} \nmid ((x \pm c'\sqrt{-d})/2)$ we see that $\theta_1\theta_2 \neq 0$. Moreover, $\theta_1 - \theta_2 = c'\sqrt{-d}/\phi \in \mathbb{F}_q^*$. Thus $(\theta_1, \theta_2) \in \Upsilon_q'$. Now recall that the model for the Frey curve F in (21) is isomorphic to the model given in (25). The polynomial on the right hand-side of the latter model factors as in (30). Thus $F/\mathbb{F}_{\mathfrak{q}}$ is isomorphic to the elliptic curve

$$Y^2 = X(X + \theta_1\phi)(X + \theta_2\phi).$$

As ϕ is a square in $\mathbb{F}_q$, we see that this elliptic curve is in turn isomorphic to the elliptic curve H_{θ_1,θ_2}. Then $a_q(F) = a_{\mathfrak{q}}(F) = a_{\mathfrak{q}}(H_{\theta_1,\theta_2}) = a_q(H_{\theta_1,\theta_2})$. Since $a_q(E) \equiv a_q(F) \pmod{n}$, it follows that $(\theta_1, \theta_2) \in \Upsilon_q$. Moreover,

$$c' \;=\; \frac{1}{\sqrt{-d}} \cdot \left(\frac{x + c'\sqrt{-d}}{2} \;-\; \frac{x - c'\sqrt{-d}}{2}\right) \;\equiv\; \frac{\theta_1 - \theta_2}{a} \cdot \phi \pmod{\mathfrak{q}}.$$

Since $\phi \in (\mathbb{F}_q^*)^{2n}$ this proves (31).

So far we have considered only the case $q \nmid y$. We know that if $q \mid y$ then $a_q(E) \equiv \pm(q+1) \equiv \pm 2 \pmod{n}$. Thus if $a_q(E)^n \not\equiv 4 \pmod{n}$ then $q \nmid y$ and the proof is complete. Suppose $a_q(E)^2 \equiv 4 \pmod{n}$ and that $q \mid y$. In particular $\mathfrak{q} \mid \mu$ or $\mathfrak{q} \mid \overline{\mu}$, but cannot divide both by the coprimality of the factors on the right hand-side of (19). Suppose $\mathfrak{q} \mid \overline{\mu}$. Then $x \equiv c'\sqrt{d} \pmod{\mathfrak{q}}$ and so from (32) we have

$$c' \;\equiv\; \frac{\rho_1}{\sqrt{-d}} \cdot \mu^n \;\equiv\; \frac{\rho_1}{a} \cdot \mu^n \pmod{\mathfrak{q}}.$$

However, the class of μ^n modulo $\mathfrak{q}$ belongs to either $(\mathbb{F}_q^*)^{2n}$ or $g \cdot (\mathbb{F}_q^*)^{2n}$, establishing (31). The case $\mathfrak{q} \mid \mu$ is similar. This completes the proof. □

Lemma 5.6. *Let (E, d, n) be one of the remaining 1230 triples. Let $q = kn + 1$ be a prime. Suppose that $(-d/q) = -1$. Let $M = \mathbb{Q}(\sqrt{-d})$ and let $\mathfrak{q} = q\mathcal{O}_M$. Write $\mathbb{F}_{\mathfrak{q}} = \mathcal{O}_M/\mathfrak{q} \cong \mathbb{F}_{q^2}$. Let c', h, (r, s), κ_n be as in Lemma 4.2, and set $m = (2 + \kappa_n \cdot n)/h \in \mathbb{Z}$. Define $\rho_1 = (r + sa)^m$, choose g_0 to be a generator for $\mathbb{F}_{\mathfrak{q}}^*$, and set $g = g_0^n$. Define*

$$\Upsilon_q'' \;=\; \left\{\rho_1 \cdot g^i \;:\; i = 0, 1, \ldots, 2q+1\right\} \subset \mathbb{F}_{\mathfrak{q}}^*,$$

$$\Upsilon_q' \;=\; \left\{\theta \in \Upsilon_q'' \;:\; \theta \neq \theta^q\right\}$$

and

$$\Upsilon_q \;=\; \left\{\theta \in \Upsilon_q' \;:\; a_q(H_\theta) \equiv a_q(E) \pmod{n}\right\},$$

where $H_\theta/\mathbb{F}_q$ *is the elliptic curve*

$$H_\theta \;:\; Y^2 = X(X+\theta)(X+\theta^q).$$

Let

$$\Phi_q \;=\; \left\{(\theta-\theta^q)/\sqrt{-d}\cdot(\mathbb{F}_q^*)^{2n} \;:\; \theta \in \Upsilon_q\right\} \subset \mathbb{F}_q^*/(\mathbb{F}_q^*)^{2n}.$$

If $\overline{\rho}_{F,n} \sim \overline{\rho}_{E,n}$ *then necessarily* (31) *holds.*

Proof. We note that in $\mathbb{F}_\mathfrak{q}$ Galois conjugation agrees with the action of Frobenius. Thus if $\alpha \in \mathcal{O}_M$ and $\overline{\alpha}$ denotes its conjugate, then $\overline{\alpha} \equiv \alpha^q \pmod{\mathfrak{q}}$.

Since $(-d/q) = -1$ and $x^2 + c^2 d = y^n$ we observe that $q \nmid y$. Thus F and E both have good reduction at q, and so $a_q(F) \equiv a_q(E) \pmod{n}$. Let μ be as in Lemma 4.2. Thus $\mathfrak{q} \nmid \mu, \overline{\mu}$. Recall that $g = g_0^n$ where g_0 is a generator for $\mathbb{F}_\mathfrak{q}^*$. Hence $\mu^n \equiv g^j$ for some integer j. From (17)

$$\frac{x + c'\sqrt{-d}}{2} \equiv \rho_1 \cdot g^j \pmod{\mathfrak{q}} \quad \text{and} \quad \frac{x - c'\sqrt{-d}}{2} \equiv (\rho_1 \cdot g^j)^q \pmod{\mathfrak{q}}.$$

Write $j = i + (2q+2)t$, where $i \in \{0, 1, \ldots, 2q+1\}$ and t an integer. We note that

$$g^{2q+2} = (g_0^{q+1})^{2n}.$$

Moreover, $g_0^{q+1} = g_0 g_0^q \in \mathbb{F}_q^*$. Thus there is some $\theta \in \Upsilon_q''$ and some $\phi \in (\mathbb{F}_q^*)^{2n}$ such that

$$\frac{x + c'\sqrt{-d}}{2} \equiv \theta \cdot \phi \pmod{\mathfrak{q}} \quad \text{and} \quad \frac{x - c'\sqrt{-d}}{2} \equiv \theta^q \cdot \phi \pmod{\mathfrak{q}}.$$

Since $\mathfrak{q} \nmid c'\sqrt{-d}$, we see that $\theta \neq \theta^q$ and so $\theta \in \Upsilon_q'$. We note that the model for F in (25) can, over $\mathbb{F}_q$, be written as

$$Y^2 = X(X^2 + \phi\cdot(\theta+\theta^q)X + \phi\cdot(\theta\theta^q)),$$

where the coefficients are fixed by Frobenius and so do indeed belong to $\mathbb{F}_q$. This model is a twist by ϕ of H_θ. As ϕ is a square in $\mathbb{F}_q^*$, we have $a_q(H_\theta) = a_q(F) \equiv a_q(E) \pmod{n}$. Thus $\theta \in \Upsilon_q$. Finally,

$$c' \;=\; \frac{1}{\sqrt{-d}} \cdot \left(\frac{x + c'\sqrt{-d}}{2} \;-\; \frac{x - c'\sqrt{-d}}{2}\right) \;\equiv\; \frac{\theta - \theta^q}{\sqrt{-d}} \cdot \phi \pmod{\mathfrak{q}}.$$

Since $\phi \in (\mathbb{F}_q^*)^{2n}$, this proves (31). □

Lemma 5.7. *Let* (E, d, n) *be one of the remaining* 1230 *triples. Let* $q_1, q_2, \ldots, q_r$ *be primes satisfying* $q_i \equiv 1 \pmod{n}$. *Let*

$$\psi_q \;:\; (\mathbb{Z}/2n\mathbb{Z})^4 \to \mathbb{F}_q^*/(\mathbb{F}_q^*)^{2n}, \qquad \psi_q(x_1,x_2,x_3,x_4) = (-3)^{x_1}5^{x_2}(-7)^{x_3}(-11)^{x_4}\cdot(\mathbb{F}_q^*)^{2n}.$$

If $(-d/q) = 1$, *let* Φ_{q_i} *be as in Lemma 5.5 and if* $(-d/q) = -1$, *let* Φ_{q_i} *be as in Lemma 5.6. Suppose*

$$\bigcap_{i=1}^{r} \psi_{q_i}^{-1}(\Phi_{q_i}) \;=\; \emptyset.$$

Then $\overline{\rho}_{F,n} \nsim \overline{\rho}_{E,n}$.

Proof. Recall, from (14) and (15), that

$$c = 3^{\beta_3}5^{\beta_5}7^{\beta_7}11^{\beta_{11}}.$$

Thus $c \equiv (-1)^{\beta_3+\beta_7+\beta_{11}} \pmod{4}$ and hence, since we choose $c' = \pm c$ so that $c' \equiv 1 \pmod{4}$,

$$c' = (-1)^{\beta_3+\beta_7+\beta_{11}}\cdot 3^{\beta_3}5^{\beta_5}7^{\beta_7}11^{\beta_{11}} = (-3)^{\beta_3}5^{\beta_5}(-7)^{\beta_7}(-11)^{\beta_{11}}.$$

TABLE 1. This table gives the six triples (E, d, n) such that the intersection $\bigcap_{i=1}^{200} \psi_{q_i}^{-1}(\Phi_{q_i})$ is non-empty. Here the elliptic curve E is given in the first column in Cremona notation. We note that $n = 13$ for all six triples. Therefore the intersection given in the last column is a subset of $(\mathbb{Z}/26\mathbb{Z})^4$.

Elliptic Curve	d	n	$\displaystyle\bigcap_{i=1}^{200} \psi_{q_i}^{-1}(\Phi_{q_i})$
462b1	231	13	$\{ (7,2,19,3),\ (9,1,24,9) \}$
462f1	231	13	$\{ (0,15,25,13),\ (15,18,5,0) \}$
2310j1	231	13	$\{ (11,6,6,18),\ (24,19,19,5) \}$
2310l1	231	13	$\{ (10,5,22,8) \}$
2310m1	231	13	$\{(5,14,11,21),\ (7,21,19,19) \}$
2310o1	15	13	$\{ (1,0,1,1) \}$

Suppose $\overline{\rho}_{F,n} \sim \overline{\rho}_{E,n}$. Thus

$$\psi_q(\beta_3, \beta_5, \beta_7, \beta_{11}) = c' \cdot (\mathbb{F}_{q_i}^*)^{2n} \in \Phi_{q_i}$$

by (31). Therefore

$$((\beta_3, \beta_5, \beta_7, \beta_{11}) \bmod 2n) \ \in \ \bigcap_{i=1}^{r} \psi_{q_i}^{-1}(\Phi_{q_i})$$

giving a contradiction. □

We wrote a `Magma` script which for each of the 1230 remaining triples (E, d, n) recursively computes the intersections

$$\psi_{q_1}^{-1}(\Phi_{q_1}), \quad \bigcap_{i=1}^{2} \psi_{q_i}^{-1}(\Phi_{q_i}), \quad \bigcap_{i=1}^{3} \psi_{q_i}^{-1}(\Phi_{q_i}), \ldots$$

where the q_i are primes $\equiv 1 \pmod{n}$. It stops when the intersection is empty, or when we have used 200 primes q_i, whichever is first. If the intersection is empty, then we know from Lemma 5.7 that $\overline{\rho}_{F,n} \nsim \overline{\rho}_{E,n}$ and we may eliminate the particular triple (E, d, n) from further consideration. We reached an empty intersection in 1224 cases. Table 1 gives the details for the six triples (E, d, n) where the intersection is non-empty.

5.3. **Proof of Proposition 4.1.** We now complete the proof of Proposition 4.1. To summarise, Lemma 4.3 showed that the only solutions to (14) with exponent $n \in \{5, 7, 11\}$ are the ones given in the statement of Proposition 4.1. In view of the results of this section, it only remains to consider the six triples (E, d, n) given in Table 1. To eliminate further cases we make use of the following result of Halberstadt and Kraus [27, Lemme 1.6].

Theorem 3 (Halberstadt and Kraus)**.** *Let E_1 and E_2 be elliptic curves over the rationals and write Δ_j for the minimal discriminant of E_j. Let $n \geq 5$ be a prime such that $\overline{\rho}_{E_1,n} \sim \overline{\rho}_{E_2,n}$. Let q_1, $q_2 \neq n$ be distinct primes of multiplicative reduction for both elliptic curves such that $\mathrm{ord}_{q_i}(\Delta_j) \not\equiv 0 \pmod{n}$ for $i, j = 1, 2$. Then*

$$\frac{\mathrm{ord}_{q_1}(\Delta_1) \cdot \mathrm{ord}_{q_2}(\Delta_1)}{\mathrm{ord}_{q_1}(\Delta_2) \cdot \mathrm{ord}_{q_2}(\Delta_2)}$$

is congruent to a square modulo n.

We shall use Theorem 3 and Lemma 5.1 to eliminate the first five of the six outstanding triples (E, d, n) given in Table 1. In all these cases $n = 13$. We know from the proof of Lemma 5.7 that $(\beta_3, \beta_5, \beta_7, \beta_{11}) \pmod{26}$ belongs to the intersection in the last column of the table.

Consider the first triple, corresponding to the first row of the table. The $\beta_5 \equiv 1$ or $2 \pmod{26}$. But $\beta_5 = \mathrm{ord}_5(c)$. Thus $2\,\mathrm{ord}_5(c) + \mathrm{ord}_5(d) \equiv 2\beta_5 + \mathrm{ord}_5(231) \equiv 2$ or $4 \pmod{13}$ and so by Lemma 5.1, 5 must divide the conductor of E which is 462 giving a contradiction. The same argument eliminates the second triple.

Next we consider the third triple. Here $\beta_7 \equiv 6$ or $19 \pmod{26}$, and so $\mathrm{ord}_7(c) \equiv \beta_7 \equiv 6 \pmod{13}$. Then $2\,\mathrm{ord}_7(c) + \mathrm{ord}_7(d) \equiv 2\beta_7 + \mathrm{ord}_7(231) \equiv 0 \pmod{13}$. By Lemma 5.1, 7 does not divide the conductor of E which is 2310 giving a contradiction.

We next consider the fourth triple. Here the elliptic curve E with Cremona reference `231011` has minimal discriminant

$$\Delta_E = 2^4 \times 3^{12} \times 5^3 \times 7 \times 11.$$

We apply Theorem 3 with $E_1 = F$, $E_2 = E$, $q_1 = 2$ and $q_2 = 3$. From the proof of Lemma 5.1 we have

$$\mathrm{ord}_2(\Delta_F) \equiv -12 \equiv 1 \pmod{13}, \qquad \mathrm{ord}_3(\Delta_F) = 2\beta_3 + \mathrm{ord}_3(231) \equiv 2 \times 10 + 1 \equiv 8 \pmod{13}.$$

Hence

$$\frac{\mathrm{ord}_2(\Delta_F) \cdot \mathrm{ord}_3(\Delta_F)}{\mathrm{ord}_2(\Delta_E) \cdot \mathrm{ord}_3(\Delta_E)} \equiv \frac{1 \times 8}{4 \times 12} \equiv 11 \pmod{13}$$

which is a non-square modulo 13, contradicting Theorem 3.

Next we consider the fifth triple. Here there are two possibilities for $(\beta_3, \beta_5, \beta_7, \beta_{11})$. In the second possibility we have $\beta_7 \equiv 19 \pmod{26}$ which leads to a contradiction via Lemma 5.1. We focus on the first possibility. The minimal discriminant of the curve E is

$$\Delta_E = 2^4 \times 3^8 \times 5 \times 7^3 \times 11.$$

We obtain a contradiction by applying Theorem 3 with $q_1 = 2$ and $q_2 = 3$.

We are left with the last triple, which we have been unable to eliminate by appealing to Theorem 3 or Lemma 5.1 or by further sieving. In fact (14) has the solution

$$8143^2 + 3^3 \cdot 5 \cdot 7^2 \cdot 11^2 = 4^{13}. \tag{33}$$

Here $n = 13$, $d = 15$ and $c = 3 \cdot 7 \cdot 11$. We note that the vector of exponents for this value of c is $(\beta_3, \beta_5, \beta_7, \beta_{11}) = (1, 0, 1, 1)$ which agrees with prediction in the last column of the table. Moreover, letting $x = -8143 \equiv 1 \pmod 4$, and $y^n = 4^{13}$ in the Frey curve F gives the elliptic curve `2310o1`. To complete the proof we need to solve (14) with $d = 15$ and $n = 13$. We do this by reducing this case to a Thue-Mahler equation using the approach in the proof of Lemma 4.3. After possibly changing the sign of x so that $x \equiv 1 \pmod 4$, we have that

$$\frac{x + c'\sqrt{-15}}{2} = \left(\frac{1 - \sqrt{-15}}{8}\right)\left(r + s \cdot \frac{(1 + \sqrt{-15})}{2}\right)^{13}, \qquad y = r^2 + rs + 4s^2$$

for some integers r and s satisfying

$$F_{13}(r, s) = \sum_{i=0}^{13} a_i r^{13-i} s^i = \pm 4 \cdot 3^{\beta_3} \cdot 5^{\beta_5} \cdot 7^{\beta_7} \cdot 11^{\beta_{11}},$$

where

i	a_i	i	a_i	i	a_i
0	1	5	36036	10	195624
1	0	6	−34320	11	−95160
2	−312	7	−226512	12	−51428
3	−1144	8	−66924	13	924.
4	8580	9	340340		

We solved this Thue-Mahler equation using the `Magma` package associated to the paper [26]. The only solution is with

$$r = 0, \quad s = \pm 1, \quad \beta_3 = 1, \quad \beta_5 = 0, \quad \beta_7 = 1, \quad \beta_{11} = 1.$$

This corresponds to the identity (33) and completes the proof of Proposition 4.1.

Remark. It is natural to ask if the case $n = 13$ could have been dealt with entirely using the Thue-Mahler approach, just as we did for $n \in \{5, 7, 11\}$ in Lemma 4.3. The Thue-Mahler solver that we are using can quickly deal with the Thue-Mahler equations associated to the pairs $(d, n) = (7, 13)$ and $(55, 13)$. However, the Thue-Mahler equation for the pair $(d, n) = (231, 13)$ appears to be somewhat beyond the capabilities of the Thue-Mahler solver. The approach in [26] reduces solving a Thue-Mahler equation to solving a certain number of S-unit equations. The Thue-Mahler equation for the pair $(d, n) = (15, 13)$ reduces to solving four S-unit equations. The Thue-Mahler equation for the pair $(d, n) = (231, 13)$ reduces to solving 2240 S-unit equations. This explains the effort we invested into eliminating $(d, n) = (231, 13)$ via sieving and appeals to Theorem 3 and Lemma 5.1.

6. Equation (2) with y even : large exponents

From the results of the preceding sections, it remains to solve equation (2) with y even and exponent n large and prime.

6.1. **Upper bounds for n : linear forms in logarithms, complex and q-adic.** Our first order of business will be to produce an upper bound for the exponent n. To this end, as it transpires, it will prove useful to have at our disposal a lower bound upon y. From the discussion following Lemma 5.2, we have that $\overline{\rho}_{F,n} \sim \overline{\rho}_{E,n}$ for $E/\mathbb{Q}$ with nontrivial rational 2-torsion.

Let us begin by supposing that we have a solution to

$$x^2 + 3^{\alpha_3} 5^{\alpha_5} 7^{\alpha_7} 11^{\alpha_{11}} = y^n$$

with $n \geq 7$ prime and $y = 2^\kappa$ for κ a positive integer. Then the Frey-Hellegouarch curve F has nontrivial rational 2-torsion and conductor

$$N = 2 \cdot 3^{\delta_3} 5^{\delta_5} 7^{\delta_7} 11^{\delta_{11}} \text{ where } \delta_i \in \{0, 1\},$$

so that

$$N \in \{14, 30, 42, 66, 70, 154, 210, 330, 462, 770, 2310\},$$

and minimal discriminant

$$-2^{2\kappa n - 12} 3^{\alpha_3} 5^{\alpha_5} 7^{\alpha_7} 11^{\alpha_{11}}.$$

A quick check of Cremona's tables reveals that we find such curves with minimal discriminant negative and divisible by precisely $2^{2\kappa n - 12}$, with $n \geq 7$ prime, only for 18 isomorphism classes of curves, given, in Cremona's notation, by

$$14a4,\ 210b5,\ 210e1,\ 210e6,\ 330c1,\ 330c6,\ 330e4,\ 462a1,\ 462d1,\ 462e1,$$
$$462g3,\ 770a1,\ 770e1,\ 770g3,\ 2310d4,\ 2310n1,\ 2310n6,\ 2310o1.$$

Most of these have $2\kappa n - 12 = 2$ and so $\kappa = 1$ and $n = 7$. Since $P(2^7 - x^2) > 11$ for $1 \leq x < 11$ odd, only the curve 14a4 with $\Delta = -2^2 \cdot 7$ corresponds to a solution, arising from the identity $11^2 + 7 = 2^7$. Four more curves have $2\kappa n - 12 = 16$ and so $\kappa = 2$ and $n = 7$. Corresponding identities are

$$7^2 + 3^3 \cdot 5 \cdot 11^2 = 2^{14},\ 47^2 + 3^4 \cdot 5^2 \cdot 11 = 2^{14},\ 103^2 + 3 \cdot 5^2 \cdot 7 \cdot 11 = 2^{14},\ 117^2 + 5 \cdot 7^2 \cdot 11 = 2^{14},$$

arising from the curves 330c1, 210e1, 2310n1 and 770e1, with discriminants

$$-2^{16} \cdot 3^3 \cdot 5 \cdot 11^2,\ -2^{16} \cdot 3^4 \cdot 5^2 \cdot 7,\ -2^{16} \cdot 3 \cdot 5^2 \cdot 7 \cdot 11 \text{ and } -2^{16} \cdot 5 \cdot 7^2 \cdot 11,$$

respectively. Neither 462d1 nor 462e1 lead to any solutions while 2310o1, with discriminant $-2^{40} \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 11^2$, corresponds to the identity

$$8143^2 + 3^3 \cdot 5 \cdot 7^2 \cdot 11^2 = 2^{26}.$$

We may thus suppose that y is divisible by an odd prime factor, provided $n \geq 17$.

Lemma 6.1. *If $n \geq 17$ and y is even, we have*

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

Proof. By our preceding remarks, there necessarily exists an odd prime $p \mid y$. Since $\overline{\rho}_{F,n} \sim \overline{\rho}_{E,n}$ where $E/\mathbb{Q}$ has nontrivial rational 2-torsion, the fact that $\gcd(x, y) = 1$, thus allows us to conclude that

$$a_p(E) \equiv \pm(p+1) \pmod{n}.$$

From the Hasse-Weil bounds, we have that $a_p(E)$ is bounded in modulus by $2\sqrt{p}$, so that, using the fact that $a_p(E)$ is even,

$$n < \frac{1}{2}(\sqrt{p}+1)^2 \leq \frac{1}{2}(\sqrt{y/2}+1)^2.$$

The desired inequality follows. □

As before, define c and d via (15), where, since y is even, $d \in \{7, 15, 55, 231\}$, and let $c' = \pm c$ with the sign chosen so that $c' \equiv 1 \pmod 4$.

To derive an upper bound upon n, we will begin by using (26) to find a "small" linear form in logarithms. We prove

Lemma 6.2. *If*

$$\Lambda = \log\left(\frac{x + c'\sqrt{-d}}{x - c'\sqrt{-d}}\right)$$

and we suppose further that

$$y^n > 100\, c^2 d, \tag{34}$$

then

$$\log|\Lambda| < 0.75 + \log c + \frac{1}{2}\log d - \frac{n}{2}\log y.$$

Proof. Assumption (34), together with, say, Lemma B.2 of Smart [57], implies that

$$|\Lambda| \leq -10\log(9/10)\left|\frac{x + c'\sqrt{-d}}{x - c'\sqrt{-d}} - 1\right| = -20\log(9/10)\frac{c\sqrt{d}}{y^{n/2}},$$

whence the lemma follows. □

To show that $\log|\Lambda|$ here is indeed small, we first require an upper bound upon exponents. From (26), we have that

$$\frac{2 \cdot c'\sqrt{-d}}{x - c'\sqrt{-d}} = \begin{cases} \gamma \cdot \delta^n - 1 & \text{if } d \in \{7, 15, 55\} \\ \gamma^{(2+\epsilon_n \cdot n)/3} \cdot \delta^n - 1 & \text{if } d = 231. \end{cases} \tag{35}$$

For prime q, let $\overline{\mathbb{Q}_q}$ denote an algebraic closure of the q-adic field $\mathbb{Q}_q$, and define ν_q to be the unique extension to $\overline{\mathbb{Q}_q}$ of the standard q-adic valuation over $\mathbb{Q}_q$, normalized so that $\nu_q(q) = 1$. For any algebraic number α of degree d over $\mathbb{Q}$, we define the *absolute logarithmic height* of α via the formula

$$h(\alpha) = \frac{1}{d}\left(\log|a_0| + \sum_{i=1}^{d} \log\max\left(1, |\alpha^{(i)}|\right)\right), \tag{36}$$

where a_0 is the leading coefficient of the minimal polynomial of α over $\mathbb{Z}$ and the $\alpha^{(i)}$ are the conjugates of α in $\mathbb{C}$. Since $\gcd(x,q)=1$, it follows from (35) that, if we set

$$\Lambda_1 = \begin{cases} \delta^n - (1/\gamma) & \text{if } d \in \{7,15,55\} \\ \delta^n - (1/\gamma)^{(2+\epsilon_n \cdot n)/3} & \text{if } d = 231, \end{cases}$$

then $\nu_q(\Lambda_1) \geq \alpha_q/2$, for $q \in \{3,5,7,11\}$.

To complement this with an upper bound for linear forms in q-adic logarithms, we will appeal to Proposition 1 of Bugeaud [11].

Theorem 4 (Bugeaud)**.** *Let q be a prime number and let α_1, α_2 denote algebraic numbers which are q-adic units. Let f be the residual degree of the extension $\mathbb{Q}_q(\alpha_1,\alpha_2)/\mathbb{Q}_q$ and put $D = [\mathbb{Q}_q(\alpha_1,\alpha_2) : \mathbb{Q}_q]/f$. Let b_1 and b_2 be positive integers and put*

$$\Lambda_1 = \alpha_1^{b_1} - \alpha_2^{b_2}.$$

Denote by $A_1 > 1$ and $A_2 > 1$ real numbers such that

$$\log A_i \geq \max\left\{ h(\alpha_i), \frac{\log q}{D} \right\}, \quad i \in \{1,2\},$$

and put

$$b' = \frac{b_1}{D \log A_2} + \frac{b_2}{D \log A_1}.$$

If α_1 and α_2 are multiplicatively independent, then we have the bound

$$\nu_q(\Lambda_1) \leq \frac{24q(q^f-1)}{(q-1)\log^4(q)} D^4 \left(\max\left\{ \log b' + \log\log q + 0.4, \frac{10 \log q}{D}, 5 \right\} \right)^2 \cdot \log A_1 \cdot \log A_2.$$

We will choose $q \in \{3,5,7,11\}$ and apply this result with the following choices of parameters :

$$f = 1, \quad D = 2, \ \alpha_1 = \delta, \quad \alpha_2 = 1/\gamma, \ b_1 = n$$

and

$$b_2 = \begin{cases} 1 & \text{if } d \in \{7,15,55\} \\ (2 + \epsilon_n \cdot n)/3 & \text{if } d = 231. \end{cases}$$

$$\log A_1 = \frac{k_d}{2} \log y$$

and

$$\log A_2 = \max\left\{ \frac{k_0(d) \log 2}{2}, \frac{\log q}{2} \right\}.$$

Let us suppose here and henceforth that

$$n > 10^8. \tag{37}$$

Then, in all cases, from Lemma 6.1 and

$$b' = \frac{n}{\max\{k_0(d)\log 2, \log q\}} + \frac{\kappa_d}{k_d \log y},$$

we have that

$$\log b' + \log\log q + 0.4 > 5 \log q$$

and, moreover, that

$$\log b' + \log\log q + 0.4 < \log n + 0.401.$$

Theorem 4 thus yields the inequalities

$$\nu_q(\Lambda_1) < c(d,q) \cdot (\log n + 0.401)^2 \log y,$$

where

$$c(d,q) = \begin{cases} \frac{96q}{\log^3 q} & \text{if } d = 7, \text{ or if } d = 15 \text{ and } q \in \{5,7,11\}, \\ \frac{576\log 2}{\log^4 3} & \text{if } d = 15,\ q = 3, \\ \frac{768q\log 2}{\log^4 q} & \text{if } d = 55, \\ \frac{1728q\log 2}{\log^4 q} & \text{if } d = 231. \end{cases}$$

It follows that

$$\sum_{q\in\{3,5,7,11\}} \alpha_q \log q < C(d)\cdot(\log n + 0.401)^2 \log y, \tag{38}$$

where

$$C(d) = 2\sum_{q\in\{3,5,7,11\}} c(d,q)\log q.$$

We have

$$C(7) = 2\left(\frac{288}{\log^2 3} + \frac{480}{\log^2 5} + \frac{672}{\log^2 7} + \frac{1056}{\log^2 11}\right) < 1571,$$

$$C(15) = 2\left(\frac{572\log 2}{\log^3 3} + \frac{480}{\log^2 5} + \frac{672}{\log^2 7} + \frac{1056}{\log^2 11}\right) < 1691,$$

$$C(55) = 2\left(\frac{2304\log 2}{\log^3 3} + \frac{3840\log 2}{\log^3 5} + \frac{5376\log 2}{\log^3 7} + \frac{8448\log 2}{\log^3 11}\right) < 5547$$

and

$$C(231) = 2\left(\frac{5184\log 2}{\log^3 3} + \frac{8640\log 2}{\log^3 5} + \frac{12096\log 2}{\log^3 7} + \frac{19008\log 2}{\log^3 11}\right) < 12480.$$

Now consider

$$\Lambda_2 = k_d\,\log\left(\frac{x - D_0\sqrt{-d}}{x + D_0\sqrt{-d}}\right) = n\log(\epsilon\gamma) + \kappa_d\log(-\gamma_d) + j\pi i, \tag{39}$$

where we take the principal branches of the logarithms, and $\epsilon \in \{-1,1\}$ and j are chosen so that

$$|\log(\epsilon\gamma)| < \frac{\pi}{2}$$

and $|\Lambda_2|$ is minimal. Note that we have

d	$\lvert\log(-\gamma_d)\rvert$
7	$\arccos(3/4)$
15	$\arccos(7/8)$
55	$\arccos(23/32)$
231	$\arccos(103/128)$

Assume first that inequality (34) fails to hold. Then, from (38), we have

$$n < \frac{2\log 10}{\log y} + C(d)\cdot(\log n + 0.401)^2,$$

contradicting Lemma 6.1, (37) and $C(d) < 12480$. It follows, then that we may assume that inequality (34) holds and hence conclude, from Lemma 6.2, that

$$\log|\Lambda_2| < 0.75 + \log k_d + \frac{1}{2}C(d)\cdot(\log n + 0.401)^2\log y - \frac{n}{2}\log y.$$

From Lemma 6.1 and (37), we find, in all cases, that

$$\log|\Lambda_2| < -0.4778\,n\,\log y. \tag{40}$$

It therefore follows from the definition of Λ_2 that

$$|j|\pi < \frac{\pi n}{2} + \arccos(23/32) + y^{-0.4778n} < \frac{\pi n}{2} + \pi,$$

and so

$$|j| \le \frac{n-1}{2}. \tag{41}$$

6.1.1. *Linear forms in three logarithms.* To deduce an initial lower bound upon the linear form in logarithms $|\Lambda_2|$, we will use the following, the main result (Theorem 2.1) of Matveev [39].

Theorem 5 (Matveev)**.** *Let $\mathbb{K}$ be an algebraic number field of degree D over $\mathbb{Q}$ and put $\chi = 1$ if $\mathbb{K}$ is real, $\chi = 2$ otherwise. Suppose that $\alpha_1, \alpha_2, \ldots, \alpha_{n_0} \in \mathbb{K}^*$ with absolute logarithmic heights $h(\alpha_i)$ for $1 \le i \le n_0$, and suppose that*

$$A_i \ge \max\{D\, h(\alpha_i), |\log \alpha_i|\},\ 1 \le i \le n_0,$$

for some fixed choice of the logarithm. Define

$$\Lambda = b_1 \log \alpha_1 + \cdots + b_{n_0} \log \alpha_{n_0},$$

where the b_i are integers and set

$$B = \max\{1, \max\{|b_i| A_i / A_{n_0}\ :\ 1 \le i \le n_0\}\}.$$

Define, with $e := \exp(1)$, further,

$$\Omega = A_1 \cdots A_{n_0},$$

$$C(n_0) = C(n_0, \chi) = \frac{16}{n_0! \chi} e^{n_0} (2n_0 + 1 + 2\chi)(n_0 + 2)(4n_0 + 4)^{n_0+1} (en_0/2)^{\chi},$$

$$C_0 = \log\left(e^{4.4n_0+7} n_0^{5.5} D^2 \log(eD)\right) \quad \text{and} \quad W_0 = \log\left(1.5eBD \log(eD)\right).$$

Then, if $\log \alpha_1, \ldots, \log \alpha_{n_0}$ are linearly independent over $\mathbb{Z}$ and $b_{n_0} \ne 0$, we have

$$\log |\Lambda| > -C(n_0)\, C_0\, W_0\, D^2\, \Omega.$$

We apply Theorem 5 to $\Lambda = \Lambda_2$ with

$$D = 2,\ \chi = 2,\ n_0 = 3,\ b_3 = n,\ \alpha_3 = \pm\gamma,\ b_2 = \kappa_d,\ \alpha_2 = -\gamma_d,\ b_1 = j,\ \alpha_1 = -1.$$

We may thus take

$$A_3 = \log y,\ A_2 = k_0(d) \log 2,\ A_1 = \pi \ \text{ and } \ B = n.$$

Since

$$4\, C(3)\, C_0 = 2^{18} \cdot 3 \cdot 5 \cdot 11 \cdot e^5 \cdot \log\left(e^{20.2} \cdot 3^{5.5} \cdot 4 \log(2e)\right) < 1.80741 \times 10^{11},$$

and

$$W_0 = \log(3en \log(2e)) < 2.63 + \log n,$$

we may therefore conclude that

$$\log |\Lambda_2| > -3.94 \times 10^{11} k_0(d)\, (2.63 + \log n) \log y.$$

It thus follows from (40) that

$$n < 8.25 \times 10^{11} k_0(d)(\log n + 2.63),$$

whence, in all cases, since $k_0(d) \le 6$,

$$n < 1.76 \times 10^{14}. \tag{42}$$

To improve this inequality, we appeal to a sharper but less convenient lower bound for linear forms in three complex logarithms, due to Mignotte (Theorem 2 of [42]).

Theorem 6 (Mignotte)**.** *Consider three non-zero algebraic numbers α_1, α_2 and α_3, which are either all real and > 1, or all complex of modulus one and all $\neq 1$. Further, assume that the three numbers α_1, α_2 and α_3 are either all multiplicatively independent, or that two of the numbers are multiplicatively independent and the third is a root of unity. We also consider three positive rational integers b_1, b_2, b_3 with $\gcd(b_1, b_2, b_3) = 1$, and the linear form*

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1 - b_3 \log \alpha_3,$$

where the logarithms of the α_i are arbitrary determinations of the logarithm, but which are all real or all purely imaginary. We assume that

$$0 < |\Lambda| < 2\pi/w,$$

where w is the maximal order of a root of unity in $\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3)$. Suppose further that

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

and put

$$d_1 = \gcd(b_1, b_2), \;\; d_3 = \gcd(b_3, b_2) \;\; \textit{and} \;\; b_2 = d_1 b_2' = d_3 b_2''$$

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 positive rational integers with

$$K \geq 3, \;\; L \geq 5, \;\; R > R_1 + R_2 + R_3, \;\; S > S_1 + S_2 + S_3 \;\; \textit{and} \;\; T > T_1 + T_2 + T_3$$

Let $\rho \geq 2$ be a real number. Let a_1, a_2 and a_3 be real numbers such that

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

where $D = [\mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{Q}] \, / \, [\mathbb{R}(\alpha_1, \alpha_2, \alpha_3) : \mathbb{R}]$, and set

$$U = \left(\frac{KL}{2} + \frac{L}{4} - 1 - \frac{2K}{3L} \right) \log \rho.$$

Assume further that

$$U \geq (D+1) \log(K^2 L) + gL(a_1 R + a_2 S + a_3 T) + D(K-1) \log b - 2 \log(e/2), \tag{43}$$

where

$$g = \frac{1}{4} - \frac{K^2 L}{12RST} \;\; \textit{and} \;\; b = (b_2' \eta_0)(b_2'' \zeta_0) \left(\prod_{k=1}^{K-1} k! \right)^{-\frac{4}{K(K-1)}},$$

with

$$\eta_0 = \frac{R-1}{2} + \frac{(S-1)b_1}{2b_2} \;\; \textit{and} \;\; \zeta_0 = \frac{T-1}{2} + \frac{(S-1)b_3}{2b_2}.$$

Put

$$\mathcal{V} = \sqrt{(R_1+1)(S_1+1)(T_1+1)}.$$

If, for some positive real number χ, we have

(i) $(R_1+1)(S_1+1)(T_1+1) > K\mathcal{M}$,

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

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

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

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

where

$$\mathcal{M} = \max\Big\{R_1 + S_1 + 1,\ S_1 + T_1 + 1,\ R_1 + T_1 + 1,\ \chi\,\mathcal{V}\Big\},$$

then either

$$|\Lambda| \cdot \frac{LSe^{LS|\Lambda|/(2b_2)}}{2|b_2|} > \rho^{-KL}, \tag{44}$$

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

*(***C1***)* $\quad |b_1| \le R_1$ *and* $|b_2| \le S_1$ *and* $|b_3| \le T_1$,

*(***C2***)* $\quad |b_1| \le R_2$ *and* $|b_2| \le S_2$ *and* $|b_3| \le T_2$,

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

$$r_0 b_2 = s_0 b_1 \tag{45}$$

with

$$|r_0| \le \frac{(R_1+1)(T_1+1)}{\mathcal{M} - T_1} \quad \textit{and} \quad |s_0| \le \frac{(S_1+1)(T_1+1)}{\mathcal{M} - T_1}, \tag{46}$$

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

$$(t_1 b_1 + r_1 b_3)s_1 = r_1 b_2 t_2, \qquad \gcd(r_1, t_1) = \gcd(s_1, t_2) = 1, \tag{47}$$

which also satisfy

$$|r_1 s_1| \le \gcd(r_1, s_1) \cdot \frac{(R_1+1)(S_1+1)}{\mathcal{M} - \max\{R_1, S_1\}},$$

$$|s_1 t_1| \le \gcd(r_1, s_1) \cdot \frac{(S_1+1)(T_1+1)}{\mathcal{M} - \max\{S_1, T_1\}}$$

and

$$|r_1 t_2| \le \gcd(r_1, s_1) \cdot \frac{(R_1+1)(T_1+1)}{\mathcal{M} - \max\{R_1, T_1\}}.$$

Moreover, when $t_1 = 0$ *we can take* $r_1 = 1$, *and when* $t_2 = 0$ *we can take* $s_1 = 1$.

To apply this result to $\Lambda = \Lambda_2$, we distinguish between two cases, depending on whether j is negative or nonnegative, respectively. In the first case ($j < 0$), we choose

$$b_1 = \kappa_d,\ \alpha_1 = -\gamma_d,\ b_2 = n,\ \alpha_2 = \pm\gamma \ \text{ and } \ b_3 = -j,\ \alpha_3 = -1. \tag{48}$$

In the second, we have

$$b_1 = \kappa_d,\ \alpha_1 = -\gamma_d,\ b_2 = j,\ \alpha_2 = -1 \ \text{ and } \ b_3 = n,\ \alpha_3 = \pm\gamma. \tag{49}$$

It follows, in case (48), that

$$h(\alpha_1) = \frac{k_0(d)\log 2}{2},\ h(\alpha_2) = \frac{1}{2}\log(y) \ \text{ and } \ h(\alpha_3) = 0.$$

Let us suppose that $d = 231$ (this should give the worst constants). We can take

$$a_1 = \rho \arccos(103/128) + 6\log(2),\ a_2 = \frac{1}{2}\rho\pi + \log(y) \ \text{ and } \ a_3 = \rho\pi.$$

As noted in [14], if we suppose that $m \ge 1$ and define

$$\begin{aligned} &K = [mLa_1a_2a_3],\ R_1 = [c_1a_2a_3],\ S_1 = [c_1a_1a_3],\ T_1 = [c_1a_1a_2],\ R_2 = [c_2a_2a_3], \\ &S_2 = [c_2a_1a_3],\ T_2 = [c_2a_1a_2],\ R_3 = [c_3a_2a_3],\ S_3 = [c_3a_1a_3] \ \text{ and } \ T_3 = [c_3a_1a_2], \end{aligned} \tag{50}$$

where

$$c_1 = \max\{(\chi mL)^{2/3}, (2mL/a_1)^{1/2}\},\ c_2 = \max\{2^{1/3}(mL)^{2/3}, (m/a_1)^{1/2}L\}$$
$$\text{and } c_3 = (6m^2)^{1/3}L, \tag{51}$$

then conditions (i)-(v) are automatically satisfied. It remains to verify inequality (43).

Define

$$R = R_1 + R_2 + R_3 + 1,\ S = S_1 + S_2 + S_3 + 1 \text{ and } T = T_1 + T_2 + T_3 + 1.$$

We choose

$$\rho = 7.5,\ L = 155,\ m = 15 \text{ and } \chi = 0.03,$$

so that

$$c_1 = (2mL/a_1)^{1/2},\ \ c_2 = 2^{1/3}(mL)^{2/3},$$

and we have

$$K = [K_1 + K_2 \log(y)],$$

where

$$K_1 = 5760812.3270\ldots \text{ and } K_2 = 488992.9376\ldots.$$

We thus have

$$S_1 = 4800,\ S_2 = 46505 \text{ and } S_3 = 360293.$$

Since Lemma 6.1 and (37) together imply that

$$\log y > 19.8068, \tag{52}$$

we find, after a little work, that $\mathcal{M} = R_1 + T_1 + 1$ and that $g < 0.2407$.

Since we have

$$d_1 = d_3 = 1,\ b_2' = b_2'' = n,$$

it follows from (37) that

$$\eta_0 = \frac{1}{2}(R_1 + R_2 + R_3) + \frac{1}{n}(S_1 + S_2 + S_3) < 23056 \log y + 271618$$

and, from $|j| \le (n-1)/2$,

$$\zeta_0 = \frac{1}{2}(T_1 + T_2 + T_3) + \frac{-j}{2n}(S_1 + S_2 + S_3) < 8735 \log y + 205800.$$

From Lemma 3.4 of [42], we have the inequality

$$\log\left(\prod_{k=1}^{K-1} k!\right)^{\frac{4}{K(K-1)}} \ge 2\log K - 3 + \frac{2\log\left(2\pi K/e^{3/2}\right)}{K-1} - \frac{2 + 6\pi^{-2} + \log K}{3K(K-1)}, \tag{53}$$

whence, from $K > 10^6$,

$$\log\left(\prod_{k=1}^{K-1} k!\right)^{\frac{4}{K(K-1)}} > 2\log K - 3.$$

It follows, appealing to (37) and (52), that

$$b < e^3 n^2 \frac{(23056\log y + 271618)(8735\log y + 205800)}{(5760812.3270 + 488992.9376\log y)^2} < 0.02323n^2 < 7.2 \times 10^{26},$$

where the last inequality is a consequence of (42). The right-hand-side of inequality (43) is thus bounded above by

$$4\log(K) + 5.4274 \times 10^8 + 4.6069 \times 10^7 \log(y) + 61.842K$$

while the left-hand-side satisfies

$$U > 156.146K + 76.062.$$

If inequality (43) fails to hold, it follows that

$$94.304K < 4\log(K) + 5.4274 \times 10^8 + 4.6069 \times 10^7 \log(y),$$

contradicting

$$K > 5760811.3270 + 488992.9376 \log y$$

and (52).

Note that we have

$$\frac{LSe^{LS|\Lambda_2|/(2b_2)}}{2|b_2|} = \frac{31898922.5\, e^{31898922.5|\Lambda_2|/n}}{n}$$

and hence, from (40),

$$\frac{LSe^{LS|\Lambda_2|/(2b_2)}}{2|b_2|} < \frac{31898922.5 \exp\left(\frac{31898922.5}{ny^{0.4778n}}\right)}{n} < 0.319,$$

where the last inequality is a consequence of Lemma 6.1 and (37). If we have inequality (44), it thus follows that

$$\log|\Lambda_2| > 1.14 - 312.31K.$$

Once again appealing to (40), we find that

$$0.4778\, n \log y < 312.31K - 1.14 < 312.31\,(5760812.3271 + 488992.9377 \log y)$$

and so

$$n < 3.1963 \times 10^8 + \frac{3.7656 \times 10^9}{\log y},$$

whence, from (52),

$$n < 5.10 \times 10^8. \tag{54}$$

If, on the other hand, inequality (44) fails to be satisfied, from inequality (37) and our choices of S_1 and S_2, necessarily (**C3**) holds. We have $\mathcal{M} = R_1 + T_1 + 1$ and hence if (45) holds then $n \mid s_0$, where

$$|s_0| \le \frac{(S_1+1)(T_1+1)}{R_1+1} < \frac{4801\,(2402 + 204\log y)}{6336 + 537\log y}.$$

From (52), the right-hand-side here is at most 1823, whence necessarily $s_0 = 0$, a contradiction. We thus have (47). In particular,

$$(\kappa_d t_1 - j r_1) s_1 = r_1 t_2 n, \tag{55}$$

for integers r_1, s_1, t_1, t_2 with $r_1 \mid 2$ and

$$|s_1 t_1| \le \gcd(r_1, s_1) \cdot \frac{(S_1+1)(T_1+1)}{R_1+1} < \gcd(r_1, s_1) \cdot 1823. \tag{56}$$

In particular, we have

$$|t_1| \le 1822. \tag{57}$$

Since s_1 is coprime to t_2 and $n > 10^8$ is prime, it follows that also $s_1 \mid r_1$, whence

$$n \mid \kappa_d t_1 - j r_1.$$

If $t_2 \ne 0$, we thus have, from (41),

$$n \le |j| + \kappa_d |t_1| \le \frac{n-1}{2} + 2|t_1| < \frac{n-1}{2} + 3644,$$

contradicting $n > 10^8$. If, on the other hand, $t_2 = 0$, then $j r_1 = \kappa_d t_1$ and so (again using $\kappa_d = 1$ for $d = 231$)

$$|j| \le \kappa_d |t_1| \le 1822.$$

We may thus rewrite Λ_2 as a linear form in two logarithms :

$$\Lambda_2 = n \log(\epsilon_1 \gamma) - \log(\alpha), \tag{58}$$

where we have defined α such that

$$-\kappa_d \log(-\gamma_d) - j\pi i = \log(\alpha).$$

For such an α, we have (use $d = 231$ so that $\kappa_d = 1$ and $k_0(d) = 6$)

$$h(\alpha) = 3 \log 2 \quad \text{and} \quad |\log \alpha| \leq \arccos(103/128) + |j|\pi.$$

We will appeal to Corollary 1 of Laurent [36] :

Theorem 7 (Laurent)**.** *Consider the linear form*

$$\Lambda = c_2 \log \beta_2 - c_1 \log \beta_1,$$

where c_1 and c_2 are positive integers, and β_1 and β_2 are multiplicatively independent algebraic numbers. Define $D = [\mathbb{Q}(\beta_1, \beta_2) : \mathbb{Q}] \,/\, [\mathbb{R}(\beta_1, \beta_2) : \mathbb{R}]$ and set

$$b' = \frac{c_1}{D \log B_2} + \frac{c_2}{D \log B_1},$$

where $B_1, B_2 > 1$ are real numbers such that

$$\log B_i \geq \max\{h(\beta_i), |\log \beta_i|/D, 1/D\}, \quad i \in \{1, 2\}.$$

Then

$$\log |\Lambda| \geq -CD^4 \left(\max\{\log b' + 0.21, m/D, 1\}\right)^2 \log B_1 \log B_2,$$

for each pair (m, C) in the following set

$$\{(10, 32.3), (12, 29.9), (14, 28.2), (16, 26.9), (18, 26.0), (20, 25.2), \\ (22, 24.5), (24, 24.0), (26, 23.5), (28, 23.1), (30, 22.8)\}.$$

We apply this to Λ_2 as in (58), with

$$D = 1, \ c_2 = n, \ \beta_2 = \epsilon_1 \gamma, \ c_1 = 1, \ \beta_1 = \alpha,$$

so that we may choose (again using $d = 231$ so that $k_d = 3$)

$$\log B_1 = \frac{3}{2} \log y, \quad \log B_2 = \arccos(103/128) + |j|\pi,$$

whence

$$b' = \frac{1}{\arccos(103/128) + |j|\pi} + \frac{2n}{3 \log y}.$$

We take

$$(m, C) = (10, 32.3),$$

so that, from (37), (40), (52) and $|j| \leq 1822$,

$$0.4778\, n \log y < 277358 \, \log^2 n \log y.$$

whence $n < 2.14 \times 10^8$.

Here, in all cases, we choose $\chi = 0.03$ and, for the other parameters,

ρ	L	m	upper bound upon n
7.5	155	15	5.10×10^8
7.7	89	16	1.91×10^8
7.8	86	15	1.73×10^8
7.7	90	14	1.71×10^8

7. Extending to include 13

We need to work in $\mathbb{Q}(\sqrt{-d})$ for (in addition to previous)

$$d \in \{39, 143, 455, 15015\}.$$

Conductor 30030 has 56 isogeny classes of elliptic curves with nontrivial rational 2-torsion. We have

$$\frac{5^2 + 39 \cdot 1^2}{4} = 2^4, \quad \frac{53^2 + 143 \cdot 3^2}{4} = 2^{10}, \quad \frac{1^2 + 455 \cdot 3^2}{4} = 2^{10}, \quad \frac{37^2 + 15015 \cdot 1^2}{4} = 2^{12}.$$

References

[1] C. F. Barros, On the Lebesgue-Nagell equation and related subjects, PhD thesis, University of Warwick, 2010.
[2] M. Bauer and M. A. Bennett, Applications of the hypergeometric method to the generalized Ramanujan-Nagell equation, *Ramanujan. J.* 6 (2002), 209–270.
[3] M. A. Bennett and S. Siksek, Differences between perfect powers : prime power gaps, in preparation.
[4] M. A. Bennett and C. Skinner, *Ternary Diophantine equations via Galois representations and modular forms*, Canad. J. Math. **56** (2004), no. 1, 23–54.
[5] M. A. Bennett, A. Gherga and A. Rechnitzer, Computing elliptic curves over $\mathbb{Q}$, *Math. Comp.* 88 (2019), 1341–1390.
[6] A. Berczes and I. Pink, On the diophantine equation $x^2 + p^{2k} = y^n$, *Arch. Math.* 91 (2008), 505–517.
[7] A. Berczes and I. Pink, On the diophantine equation $x^2 + d^{2l+1} = y^n$, *Glasgow Math. J.* 54 (2012), 415–428.
[8] Y. Bilu, G. Hanrot and P. Voutier, Existence of primitive divisors of Lucas and Lehmer numbers (with an appendix by M. Mignotte), *J. Reine Angew. Math.* 539 (2001), 75–122.
[9] 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://magma.maths.usyd.edu.au/magma/`)
[10] 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.
[11] Y. Bugeaud, On the diophantine equation $x^2 - p^m = \pm y^n$, *Acta Arith.* 80 (1997), 213–223.
[12] Y. Bugeaud, On the greatest prime factor of $ax^m - by^n$ II, *Bull. London Math. Soc.* 32 (2000), 673–678.
[13] Y. Bugeaud and M. Laurent, Minoration effective de la distance p-adique entre puissances de nombres algébriques, *J. Number Theory* 61 (1996), 311–342.
[14] Y. Bugeaud, M. Mignotte and S. Siksek, Classical and modular approaches to exponential Diophantine equations II. the Lebesgue-Nagell equation, *Compositio Math.* 142 (2006), 31–62.
[15] Y. Bugeaud, M. Mignotte, S. Siksek, M. Stoll and Sz. Tengely, Integral Points on Hyperelliptic Curves, *Algebra & Number Theory* 2 (2008), 859–885.
[16] I. Chen, On the equations $a^2 - 2b^6 = c^p$ and $a^2 - 2 = c^p$, *LMS J. of Comput. and Math.* 1, 158–171.
[17] H. Cohen, *Advanced Topics in Computational Algebraic Number Theory*, GTM **193**, Springer–Verlag, 2000.
[18] H. Cohen, *Number Theory, Volume II : Analytic and Modern Tools* , GTM **240**, Springer–Verlag, 2000.
[19] J. H. E. Cohn, The diophantine equation $x^2 + C = y^n$, II, *Acta Arith.* 109 (2003), 205–206.
[20] H. Darmon and L. Merel, Winding quotients and some variants of Fermat's last theorem, J. Reine Angew. Math. 490 (1997), 81–100.
[21] A. David, Caractère d'isogénie et crittéres d'irréductibilité, *arXiv:1103.3892v2 [math.NT].*
[22] L. Dembélé and J. Voight, Explicit methods for Hilbert modular forms, In *Elliptic curves, Hilbert modular forms and Galois deformations*, Adv. Courses Math. CRM Barcelona, pages 135–198. Birkhäuser/Springer, Basel, 2013.
[23] N. Freitas, B. Le Hung and S. Siksek, Elliptic curves over real quadratic fields are modular, *Invent. Math.* 201 (2015), 159–206.
[24] N. Freitas and S. Siksek, The Asymptotic Fermat's Last Theorem for Five-Sixths of Real Quadratic Fields, *Compositio Math.* 151 (2015), 1395–1415.
[25] N. Freitas and S. Siksek, Criteria for the irreducibility of mod p representations of Frey curves, *J. Théor. Nombres Bordeaux*, 27 (2015), 67–76.
[26] A. Gherga, R. von Känel, B. Matschke and S. Siksek, Efficient resolution of Thue-Mahler equations, to appear.
[27] E. Halberstadt and A. Kraus, Courbes de Fermat : résultats et problèmes, *J. reine Angew. Math.* 548 (2002), 167–234.
[28] W. Ivorra, Courbes elliptiques sur $\mathbb{Q}$, ayant un point d'ordre 2 rationnel sur $\mathbb{Q}$, de conducteur $2^N p$, Dissertationes Math. 429 (2004), 1–55.
[29] W. Ivorra and A. Kraus, Quelques résultats sur les équations $ax^p + by^p = cz^2$, *Canad. J. Math.* 58 (2006), 115–153.
[30] R. von Kanel and B. Matschke, ??

[31] A. Koutsianas, An application of the modular method and the symplectic argument to a Lebesgue-Nagell equation, *Mathematika* 66 (2020), 230–244.
[32] A. Kraus and J. Oesterlé, Sur une question de B. Mazur, *Math. Ann.* 293 (2002), 259–275.
[33] A. Kraus, Majorations effectives pour l'équation de Fermat généralisée, *Canadian J. Math.* 49 (1997), 1139–1161.
[34] A. Kraus, Sur l'équation $a^3 + b^3 = c^p$, *Experimental Math.* 7 (1998), 1–13.
[35] J. M. van Langen, On the sum of fourth powers in an arithmetic progression, *Int. J. Number Theory* 17 (2021), 191–231.
[36] M. Laurent, Linear forms in two logarithms and interpolation determinants. II, *Acta Arith.* 133 (2008), 325–348.
[37] V. A. Lebesgue, Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + 1$, *Nouv. Ann. de Math.* 9(1) (1850), 178–181.
[38] F. Luca, On the equation $x^2 + 2^a 3^b = y^n$, *Int. J. Math. and Math. Sci.* 29 (2002), 239–244.
[39] E. Matveev, An explicit lower bound for a homogeneous rational linear form in logarithms of algebraic numbers. II, *Izv. Math.* 64 (2000), 1217–1269.
[40] B. Mazur. Rational isogenies of prime degree, *Invent. Math.* 44 (1978), no. 2, 129–162.
[41] M. Mignotte, A note on the equation $ax^n - by^n = c$, *Acta Arith.* LXXV.3 (1996), 287–295.
[42] M. Mignotte, A kit on linear forms in three logarithms, 45 pp, available at `http://www-irma.u-strasbg.fr/~bugeaud/travaux/kit.ps`.
[43] P. Mihailescu, Primary cyclotomic units and a proof of Catalan's conjecture, *J. Reine Angew. Math.* 572 (2004), 167–195.
[44] F. Momose, Isogenies of prime degree over number fields, *Compositio Math.* 97 (1995), 329–348.
[45] T. Nagell, Sur l'impossibilité de quelques equations à deux indéterminées, *Norsk Mat. Forenings Skr.* 13 (1923), 65–82.
[46] T. Nagell, Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns, *Nova Acta Regiae Soc. Sci. Upsaliensis* 16(2) (1955), 1–70.
[47] A. Pethő, Perfect powers in second order linear recurrences, *J. Number Theory* 15 (1982), 5–13.
[48] A. Pethő, H. G. Zimmer, J. Gebel, and E. Herrmann, Computing all S-integral points on elliptic curves, *Math. Proc. Cambridge Philos. Soc.* 127 (1999), 383–402.
[49] S. S. Pillai, On the inequality $0 < a^x - b^y \leq n$, *J. Indian Math. Soc.* 19 (1931), 1–11.
[50] I. Pink, On the Diophantine equation $x^2 + 2^\alpha 3^\beta 5^\gamma 7^\delta = y^n$, *Publ. Math. Deb.* 70 (2007), 149–166.
[51] J. Quer, $\mathbb{Q}$-curves and abelian varieties of GL_2-type, *Proc. London Math. Soc.* 81 (2000), 285–317.
[52] K. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, *Invent. Math.* 100 (1990), 431–476.
[53] K. Ribet, On the equation $a^p + 2^\alpha b^p + c^p = 0$, *Acta Arith.* 79 (1997), 7–16.
[54] J.-P. Serre, *Abelian ℓ-adic representations of elliptic curves*, Addison-Wesley, 1989.
[55] S. Siksek, *The Modular Approach to Diophantine Equations*, in *Explicit Methods in Number Theory: Rational Points and Diophantine Equations*, ed. Belabas et al., Panoramas et synthèses **36**, 2012.
[56] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer-Verlag, New York, 1994.
[57] N. P. Smart, The Algorithmic Resolution of Diophantine Equations, Cambridge University Press, 1998.
[58] N. P. Smart and N. M. Stephens, Integral points on elliptic curves over number fields, *Mathematical Proceedings of the Cambridge Philosophical Society* 122 (1997), 9–16.
[59] G. Soydan and N. Tzanakis, Complete solution of the Diophantine equation $x^2 + 5^a 11^b = y^n$, *Bull. Hellenic Math. Soc.* 60 (2016), 125–151.
[60] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* 141 (1995), 553–572.
[61] N. Tzanakis and B.M.M. de Weger, On the practical solution of the Thue equation, *J. Number Theory* 31 (1989), 99–132.
[62] N. Tzanakis and B.M.M. de Weger, Solving a specific Thue-Mahler equation, *Math. Comp.* 57 (1991), 799–815.
[63] N. Tzanakis and B.M.M. de Weger, How to explicitly solve a Thue-Mahler equation, *Compositio Math.* 84 (1992), 223–288.
[64] B. M. M. de Weger. Algorithms for Diophantine equations, CWI Tract 65, Stichting Mathematisch Centrum, Amsterdam, 1989.
[65] B. M. M. de Weger. The weighted sum of two S-units being a square, *Indag. Mathem., N.S.*, 1 (1990), 243–262.
[66] A. Wiles. Modular elliptic curves and Fermat's Last Theorem, *Ann. of Math* 141 (1995), 443–551.

Department of Mathematics, University of British Columbia, Vancouver, B.C., V6T 1Z2 Canada
Email address: bennett@math.ubc.ca

Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom
Email address: S.Siksek@warwick.ac.uk