DIFFERENCES BETWEEN PERFECT POWERS : PRIME POWER GAPS

MICHAEL A. BENNETT AND SAMIR SIKSEK

Abstract. We develop machinery to explicitly determine, in many instances, when the difference $x^2 - y^n$ is divisible only by powers of a given fixed prime. This combines a wide variety of techniques from Diophantine approximation (bounds for linear forms in logarithms, both archimedean and non-archimedean, lattice basis reduction, methods for solving Thue-Mahler and S-unit equations, and the Primitive Divisor Theorem of Bilu, Hanrot and Voutier) and classical Algebraic Number Theory, with results derived from the modularity of Galois representations attached to Frey-Hellegoaurch elliptic curves. By way of example, we completely solve the equation
$$x^2 + q^\alpha = y^n,$$
where $2 \le q < 100$ is prime, and x, y, α and n are integers with $n \ge 3$ and $\gcd(x, y) = 1$.

Contents

1. INTRODUCTION

The *Lebesgue-Nagell* equation

$$(1) \qquad x^2 + D = y^n$$

has a very extensive literature, motivated, at least in part, by attempts to extend Mihăilescu's Theorem [33] (née Catalan's Conjecture) to larger gaps in the sequence of perfect powers, in an attempt to attack Pillai's conjecture [35]. In equation (1), we will suppose that x and y are coprime nonzero integers, and that the prime divisors of D belong to a fixed, finite set of primes S. Under these assumptions, bounds for linear forms in logarithms, p-adic and complex, imply that the set of integer solutions (x, y, n) to (1), with $|y| > 1$ and $n \geq 3$, is finite and effectively determinable. If, in addition, we suppose that D is positive and that y is odd, then these solutions may be explicitly determined, provided $|S|$ is not too large, through appeal to the Primitive Divisor Theorem of Bilu, Hanrot and Voutier [10], in conjunction with techniques from Diophantine approximation.

If either $D > 0$ and y is even, or if $D < 0$, the Primitive Divisor Theorem cannot be applied to solve equation (1) and we must work rather harder, appealing to either bounds for linear forms in logarithms or to results based upon the modularity of Galois representations associated to certain Frey–Hellegouarch elliptic curves. In a companion paper [6], we develop machinery for handling (1) in the first difficult case where $D > 0$ and y is even. Though the techniques we discuss in the present paper are more widely applicable, we will, for simplicity, restrict attention to the case where D in equation (1) is divisible by a single prime q, whilst treating both the cases $D < 0$ and $D > 0$. That is, we will concern ourselves primarily with the equation

$$(2) \qquad x^2 + (-1)^\delta q^\alpha = y^n, \qquad q \nmid x,$$

where $\delta \in \{0, 1\}$ and α is a nonnegative integer. In case $\delta = 0$, our main result is the following.

Theorem 1. *If x, y, q, α and n are positive integers with q prime, $2 \leq q < 100$, $q \nmid x$, $n \geq 3$ and*

$$(3) \qquad x^2 + q^\alpha = y^n,$$

then (q, α, y, n) is one of

$(2, 1, 3, 3), \ (2, 2, 5, 3), \ (2, 5, 3, 4), \ (3, 5, 7, 3), \ (3, 4, 13, 3), \ (7, 1, 2, 3), \ (7, 3, 8, 3), \ (7, 1, 32, 3),$

$(7, 2, 65, 3), \ (7, 1, 2, 4), \ (7, 2, 5, 4), \ (7, 1, 2, 5), \ (7, 1, 8, 5), \ (7, 1, 2, 7), \ (7, 3, 2, 9), \ (7, 1, 2, 15)$

$(11, 1, 3, 3), \ (11, 1, 15, 3), \ (11, 2, 5, 3), \ (11, 3, 443, 3), \ (13, 1, 17, 3), \ (17, 1, 3, 4), \ (19, 1, 7, 3),$

$(19, 1, 55, 5), \ (23, 1, 3, 3), \ (23, 3, 71, 3), \ (23, 3, 78, 4), \ (23, 1, 2, 5), \ (23, 1, 2, 11), \ (29, 2, 5, 7),$

$(31, 1, 4, 4), \ (31, 1, 2, 5), \ (31, 1, 2, 8), \ (41, 2, 29, 4), \ (41, 2, 5, 5), \ (47, 1, 6, 3), \ (47, 1, 12, 3),$

$(47, 1, 63, 3), \ (47, 2, 17, 3), \ (47, 3, 74, 3), \ (47, 1, 3, 5), \ (47, 1, 2, 7), \ (53, 1, 9, 3), \ (53, 1, 29, 3),$

$(53, 1, 3, 6), \ (61, 1, 5, 3), \ (67, 1, 23, 3), \ (71, 1, 8, 3), \ (71, 1, 6, 4), \ (71, 1, 3, 7), \ (71, 1, 2, 9),$

$(79, 1, 20, 3), \ (79, 1, 2, 7), \ (83, 1, 27, 3), \ (83, 1, 3, 9), \ (89, 1, 5, 3), \ (97, 2, 12545, 3), \ (97, 1, 7, 4).$

One might note that the restriction $q \nmid x$ can be removed, with a modicum of effort, at least for certain values of q. The cases where primitive divisor arguments are inapplicable correspond to

$q \in \{7, 23, 31, 47, 71, 79\}$ and y even (and this is where the great majority of work lies in proving Theorem 1). If $q = 7$, Theorem 1 generalizes recent work of Koutsianas [24], who established a like result under certain conditions upon α and q, and, in particular, showed that equation (3) has no solutions with $q = 7$ and prime $n \equiv 13, 23 \pmod{24}$. We note that the solution(s) with $q = 83$ were omitted in the statement of Theorem 1 of Berczes and Pink [9].

Our results for (2) with $\delta = 1$ are less complete, at least when α is odd.

Theorem 2. *Suppose that*

$$(4) \qquad q \in \{7, 11, 13, 19, 23, 29, 31, 43, 47, 53, 59, 61, 67, 71, 79, 83\}.$$

If x and n are positive integers, $q \nmid x$, $n \geq 3$ and

$$(5) \qquad x^2 - q^{2k+1} = y^n,$$

where y and k are integers, then (q, k, y, n) is one of

$$(7, 2, 393, 3), \ (7, 1, -3, 5), \ (11, 1, 37, 3) \ (11, 0, 5, 5), \ (11, 1, 37, 3), \ (13, 0, 3, 5),$$
$$(19, 0, 5, 3), \ (19, 2, -127, 3), \ (19, 0, -3, 4), \ (19, 0, 3, 4), \ (23, 1, 1177, 3), \ (31, 0, -3, 3),$$
$$(43, 0, -3, 3), \ (71, 0, 5, 3), \ (71, 1, -23, 3) \ or \ (79, 0, 45, 3).$$

To the best of our knowledge, these are the first examples of primes q for which equation (5) has been completely solved (though the cases with $k = 0$ are treated in the thesis of Barros [2]). There are eight other primes in the range $3 \leq q < 100$ for which we are unable to give a similarly satisfactory statement. For four of these, namely $q = 3, 5, 17$ and 37, the equation (5) has a solution with $y = \pm 1$. For such primes we are unaware of any results that would enable us to completely treat fixed exponents n of moderate size; this difficulty is well-known for the $D = -2$ case of (1). One should note that it is relatively easy to solve (5) for $q \in \{3, 5, 37\}$, under the additional assumption that y is even (and somewhat harder if $q = 17$ and y is even). For the other four primes, namely $q = 41, 73, 89$ and 97, we give a method which appears theoretically capable of success, but is alas prohibitively expensive, computationally-speaking. We content ourselves by proving the following modest result for these primes.

Theorem 3. *Let $q \in \{41, 73, 89, 97\}$. The only solutions to (5) with $q \nmid x$ and $3 \leq n \leq 1000$ are with (q, k, y, n) one of*

$$(41, 0, -2, 5), \ (41, 0, 2, 3), \ (41, 0, 2, 7), \ (41, 1, 10, 5), \ (73, 0, -6, 4),$$
$$(73, 0, -4, 3), \ (73, 0, 2, 3), \ (73, 0, 3, 3), \ (73, 0, 6, 3), \ (73, 0, 6, 4), \ (73, 0, 72, 3),$$
$$(89, 0, -4, 3), \ (89, 0, -2, 3), \ (89, 0, 2, 5), \ (89, 0, 2, 13) \ or \ (97, 0, 2, 7).$$

There are no solutions to equation (5) with $n > 1000$, $q \nmid x$ and either $q = 73$ and $y \equiv 0 \pmod 2$, or with $q = 97$ and $y \equiv 1 \pmod 2$.

The additional assumption that the exponent of our prime q is even simplifies matters considerably. In the case of equation (3), Berczes and Pink [8] deduced Theorem 1 for even values of α (whence primitive divisor technology works efficiently). For completeness, we extend this to $q < 1000$; the results for $q < 100$ are, of course, just a special case of Theorem 1.

Theorem 4. *If x, y, q, k and n are positive integers with q prime, $2 \leq q < 1000$, $q \nmid x$, $n \geq 3$ and*

$$(6) \qquad x^2 + q^{2k} = y^n,$$

then (q, k, y, n) is one of

$$(2, 1, 5, 3), (3, 2, 13, 3), (7, 1, 65, 3), (7, 1, 5, 4), (11, 1, 5, 3), (29, 1, 5, 7), (41, 1, 29, 4), (41, 1, 5, 5),$$
$$(47, 1, 17, 3), (97, 1, 12545, 3), (107, 1, 37, 3), (191, 1, 65, 3), (239, 1, 169, 4), (239, 1, 13, 8),$$
$$(431, 1, 145, 3), (587, 1, 197, 3) \ or \ (971, 1, 325, 3).$$

More interesting for us is the case where the difference $x^2 - y^n$ is positive (so that primitive divisor arguments are inapplicable and there are no prior results available in the literature). Here, we prove the following.

Theorem 5. *If x, q, k and n are positive integers with q prime, $2 \le q < 1000$, $q \nmid x$, $n \ge 3$ and*

$$(7) \qquad\qquad x^2 - q^{2k} = y^n,$$

where y is an integer, then (q, k, y, n) is one of

$(3, 1, -2, 3), (3, 1, 40, 3), (3, 1, \pm 2, 4), (3, 2, -2, 5), (5, 2, 6, 3), (7, 2, 15, 3), (7, 1, 2, 5), (11, 1, 12, 3),$
$(11, 2, 3, 5), (13, 1, 3, 3), (13, 1, 12, 5), (17, 1, -4, 3), (17, 1, \pm 12, 4), (17, 2, 42, 3), (29, 1, -6, 3),$
$(31, 1, 2, 7), (43, 1, -12, 3), (43, 1, 126, 3), (43, 4, 96222, 3), (47, 1, 6300, 3), (53, 1, 6, 3),$
$(71, 1, 30, 3), (71, 2, -136, 3), (89, 1, 84, 3), (97, 2, 3135, 3), (101, 1, 24, 3), (109, 1, 20, 3),$
$(109, 1, 35, 3), (109, 1, 570, 3), (127, 1, -10, 3), (127, 1, 8, 3), (127, 1, 198, 3), (127, 1, 2, 9),$
$(179, 1, -30, 3), (193, 1, 63, 3), (197, 1, 260, 3), (223, 1, 30, 3), (251, 1, -10, 3), (251, 1, -6, 5),$
$(257, 1, -4, 5), (263, 1, 2418, 3), (277, 1, -30, 3), (307, 1, 60, 3), (307, 1, 176, 3), (307, 2, 2262, 3),$
$(359, 1, -28, 3), (383, 2, 25800, 3), (397, 1, -42, 3), (431, 1, 12, 3), (433, 1, -12, 3),$
$(433, 1, 143, 3), (433, 2, 26462, 3), (479, 1, 90, 3), (499, 1, -12, 5), (503, 1, 828, 3), (557, 1, -60, 3),$
$(577, 1, \pm 408, 4), (593, 1, -70, 3), (601, 1, 72, 3), (659, 1, 42, 3), (683, 1, 193346, 3), (701, 1, 4452, 3),$
$(727, 1, 18, 3), (739, 1, 234, 3), (769, 1, 255, 3), (811, 1, -70, 3), (857, 1, -72, 3)$ *or* $(997, 1, 48, 3)$.

We note that, with sufficient computational power, there is no obstruction to extending the results of Theorems 4 and 5 to larger prime values q. Without fundamentally new ideas, it is not clear that the same may be said of, for example, Theorem 1. In this case, the bounds we obtain upon the exponent n via linear forms in logarithms, even for relatively small q, leave us with a computation which, while finite, is barely tractable.

Equation (8) has been completely resolved ([22], [39]) for $q = 2$, except for the case $(\alpha, \delta) = (1, 1)$ which corresponds to $D = -2$ in (1). The solutions for $q = 2$ in our theorems are included for completeness. For the remainder of the paper, we suppose that q is an odd prime. In particular, we are concerned with the equation

$$(8) \qquad\qquad x^2 + (-1)^{\delta} q^{\alpha} = y^n, \qquad \gcd(x, y) = 1, \quad \alpha > 0,$$

where q is a fixed odd prime, $n \ge 3$, and $\delta \in \{0, 1\}$.

Our proofs will use a broad combination of techniques, which include:
- Lower bounds for linear forms in complex and p-adic logarithms which yield bounds for the exponent n in (8).
- Frey–Hellegouarch curves and their Galois representations which provide a wealth of local information regarding solutions to (8).
- The celebrated Primitive Divisor Theorem of Bilu, Hanrot and Voutier, that can be used to treat most cases of (8) when y is odd and $\delta = 0$.
- Elementary descent arguments that reduce (8) for a fixed exponent n to Thue–Mahler equations, which are possible to resolve thanks to the Thue–Mahler solver associated to [20].

The outline of this paper is as follows. In Section 2, we solve the equation $x^2 + (-1)^{\delta} q^{\alpha} = y^n$ for $n \in \{3, 4\}$ and $3 \le q < 100$ by reducing the problem to the determination of S-integral points on elliptic curves. In Section 3, we solve the equation $x^2 - q^{2k} = y^n$, for q in the range $3 \le q < 1000$, with y odd using an elementary sieving argument; this completes the proof of Theorem 5 in case y is odd. Next, Section 4 provides a short overview of Lucas sequences, their ranks of apparition, and the Primitive Divisor Theorem of Bilu, Hanrot and Voutier. We make use of this machinery in Section 5 to solve the equation $x^2 + q^{2k} = y^n$ for q in the range $3 \le q < 1000$, thereby proving

Theorem 4. Section 6 reduces the equation $x^2 - q^{2k} = y^n$, for even values of y, to Thue–Mahler equations of the form

(9)
$$y_1^n - 2^{n-2}y_2^n = q^k.$$

In Section 7, we give a brief outline of the modular approach to Diophantine equations. Section 8 applies this modular approach, particularly the (n, n, n) Frey–Hellegouarch elliptic curves of Kraus [25] to equation (9); this allows us to deduce that there are no solutions for $3 \leq q < 1000$ except for possibly $q \in \{31, 127, 257\}$, where the mod n representation of the Frey–Hellegouarch curve arises from that of an elliptic curve with full 2-torsion and conductor $2q$. Before we can complete the proof of Theorem 5, we need an upper bound for the exponent n. We give a sharpening of Bugeaud's bound [13] for the equation $x^2 - q^{2k} = y^n$, which uses (9) and the theory of linear forms in real and p-adic logarithms. In Section 10, we complete the proof of Theorem 5; our approach makes use of a sieving technique that builds on the information obtained from the modular approach in Section 8 and the upper bound for n established in Section 9. The remainder of the paper is concerned with (8) where $\alpha = 2k + 1$, and for $3 \leq q < 100$. In Section 11 , we resolve $x^2 + q^{2k+1} = y^n$ with y odd with the help of the Primitive Divisor Theorem, and in Section 12 we solve $x^2 - q^{2k+1} = y^5$ by reducing to Thue–Mahler equations.

It remains, then, to handle the equations $x^2 - q^{2k+1} = y^n$ and $x^2 + q^{2k+1} = y^n$ where, in the latter case, we may additionally assume that y is even. In Section 13, we study the more general equation

(10)
$$y^n + q^\alpha z^n = x^2, \qquad \gcd(x, y) = 1$$

where q is prime, using Galois representations of Frey–Hellegouarch curves. Our approach builds on previous work of the first author and Skinner [7], and also on the work of Ivorra and Kraus [23]. We then restrict ourselves in Section 14 to the case $z = \pm 1$ and α odd in (10). In this section, we develop a variety of sieves based upon local information coming from the Frey–Hellegouarch curves that allows us, in many situations, to eliminate values of q from consideration completely and, in the more difficult cases, to solve equation (8) for a fixed pair (q, n). In particular, we employ this strategy to complete the proofs of Theorems 2 and 3. Finally, in Section 15, we return to bounds for linear forms in p-adic and complex logarithms to derive explicit upper bounds upon n in (8), and then report upon a (somewhat substantial) computation to use the arguments of Section 14 to solve (8) for all remaining pairs (q, n) required to finish the proof of Theorem 1.

2. Reduction to S-integral points on elliptic curves for $n \in \{3, 4\}$

In the following sections, it will be of value to us to assume that the exponent n in equation (8) is not too small. This is primarily to ensure that the Frey–Hellegouarch curve we attach to a putative solution has a corresponding mod n Galois representation that is irreducible. For suitably large prime values of n (typically, $n \geq 7$), the desired irreducibility follows from Mazur's isogeny theorem. In Section 4, such an assumption allows us to (mostly) ignore so-called *defective* Lucas sequences.

In this section, we treat separately the cases $n = 3$ and $n = 4$ for $q < 100$, where the problem of solving equation (8) reduces immediately to one of determining S-integral points on specific models of genus one curves; here $S = \{q\}$. This approach falters for many values of q in the range $100 < q < 1000$ as we are often unable to compute the Mordell–Weil groups of the relevant elliptic curves. Thus for the proofs of Theorems 4 and 5 for exponents $n = 3$, $n = 4$, where we treat values of q less than 1000, we shall employ different techniques including sieving arguments and reduction to Thue–Mahler equations.

2.1. **The case $n = 3$.** Supposing that we have a coprime solution to (8) with $n = 3$, we can write $\alpha = 6b + c$, where $0 \leq c \leq 5$. Taking $X = y/q^{2b}$ and $Y = x/q^{3b}$, it follows that (X, Y) is an

TABLE 1. Solutions to the equation $x^2 + (-1)^\delta q^\alpha = y^3$ for primes $2 \le q < 100$, $\delta \in \{0, 1\}$ and x, y, α integers satisfying $\alpha > 0$, $x > 0$, $y \ne 0$, and $\gcd(x, y) = 1$.

q	δ	α	x	y
2	0	1	5	3
2	0	2	11	5
2	1	1	1	-1
2	1	7	71	17
2	1	9	13	-7
2	1	3	3	1
3	0	4	46	13
3	0	5	10	7
3	1	1	2	1
3	1	2	1	-2
3	1	2	253	40
5	1	1	2	-1
5	1	4	29	6
7	0	1	1	2
7	0	1	181	32
7	0	2	524	65
7	0	3	13	8
7	1	4	76	15
7	1	5	7792	393
11	0	1	4	3
11	0	1	58	15
11	0	2	2	5
11	0	3	9324	443
11	1	2	43	12
11	1	3	228	37
13	0	1	70	17
13	1	2	14	3
17	1	1	3	-2
17	1	1	4	-1

q	δ	α	x	y
17	1	1	5	2
17	1	1	9	4
17	1	1	23	8
17	1	1	282	43
17	1	1	375	52
17	1	7	21063928	76271
17	1	1	378661	5234
17	1	2	15	-4
17	1	4	397	42
19	0	1	18	7
19	1	1	12	5
19	1	5	654	-127
23	0	1	2	3
23	0	3	588	71
23	1	3	40380	1177
29	1	2	25	-6
31	1	1	2	-3
37	1	1	6	-1
37	1	1	8	3
37	1	1	3788	243
37	1	3	228	11
41	1	1	7	2
43	1	1	4	-3
43	1	2	11	-12
43	1	8	30042907	96222
43	1	2	1415	126
47	0	1	13	6
47	0	1	41	12
47	0	1	500	63
47	0	2	52	17

q	δ	α	x	y
47	0	3	549	74
47	1	2	500047	6300
53	0	1	26	9
53	0	1	156	29
53	1	2	55	6
61	0	1	8	5
67	0	1	110	23
71	0	1	21	8
71	1	1	14	5
71	1	2	179	30
71	1	3	588	-23
71	1	4	4785	-136
73	1	1	3	-4
73	1	1	9	2
73	1	1	10	3
73	1	1	17	6
73	1	1	611	72
73	1	1	6717	356
79	0	1	89	20
79	1	1	302	45
83	0	1	140	27
89	0	1	6	5
89	1	1	5	-4
89	1	1	9	-2
89	1	1	33	10
89	1	1	408	55
89	1	2	775	84
97	0	2	1405096	12545
97	1	1	77	18
97	1	4	175784	3135

S-integral point on the elliptic curve

(11) $$Y^2 = X^3 + (-1)^{\delta+1} q^c,$$

where $S = \{q\}$. Here, for a particular choice of $\delta \in \{0, 1\}$ and prime q we may use the standard method for computing S-integral points on elliptic curves based on lower bounds for linear forms in elliptic logarithms (e.g. [34]). We made use of the built-in Magma ([11]) implementation of this method to compute these S-integral points on (11) for $\delta \in \{0, 1\}$ and $2 \le q < 100$. We obtained a total of 83 solutions to (8) for these values of q with $\alpha > 0$, $x > 0$, $y \ne 0$ and $\gcd(x, y) = 1$. These are given in Table 1.

TABLE 2. Solutions to the equation $x^2 + (-1)^\delta q^\alpha = y^4$ for primes $2 \le q < 100$, $\delta \in \{0, 1\}$ and x, y, α integers satisfying $\alpha > 0$, $x > 0$, $y > 0$, and $\gcd(x, y) = 1$.

q	δ	α	x	y
2	0	5	7	3
2	1	3	3	1
3	1	1	2	1
3	1	5	122	11
3	1	2	5	2

q	δ	α	x	y
7	0	1	3	2
7	0	2	24	5
17	0	1	8	3
17	1	2	145	12
19	1	1	10	3

q	δ	α	x	y
23	0	3	6083	78
31	0	1	15	4
41	0	2	840	29
71	0	1	35	6
73	1	1	37	6
97	0	1	48	7

2.2. The case $n = 4$. Next we consider the case $n = 4$ separately. Write $\alpha = 4b + c$ where $0 \le c \le 3$. Let $X = (y/q^b)^2$, $Y = xy/q^{3b}$. Then (X, Y) is an S-integral point on the elliptic curve

$$(12) \qquad Y^2 = X(X^2 + (-1)^{\delta+1}q^c),$$

where $S = \{q\}$. We again appealed to the built-in `Magma` ([11]) implementation of this method to compute these S-integral points on (12) for $\delta \in \{0, 1\}$ and $2 \le q < 100$. We obtained a total of 16 solutions to (8) for these values of q with $\alpha > 0$, $x > 0$, $y > 0$ and $\gcd(x, y) = 1$. These are given in Table 2.

3. AN ELEMENTARY APPROACH TO $x^2 - q^{2k} = y^n$ WITH y ODD

In this section, we apply an elementary factorisation argument to prove Theorem 5 for y odd. In other words, we consider the following equation

$$(13) \quad x^2 - q^{2k} = y^n, \qquad x, k, n \text{ positive integers}, \quad n \ge 3, \quad \gcd(x, y) = 1, \quad y \text{ an odd integer}.$$

Here $q \ge 3$ is a prime. From this, we immediately see that

$$(14) \qquad\qquad x + q^k = y_1^n \quad \text{and} \quad x - q^k = y_2^n,$$

with $y = y_1 y_2$, so that we have

$$(15) \qquad\qquad y_1^n - y_2^n = 2q^k.$$

If $2 \mid n$, then $y_1^n \equiv y_2^n \equiv 1 \pmod 4$, a contradiction. We may suppose henceforth, without loss of generality, that n is an odd prime. Observe that

$$(16) \qquad (y_1 - y_2)(y_1^{n-1} + y_1^{n-2}y_2 + \cdots + y_2^{n-1}) = y_1^n - y_2^n = 2q^k.$$

Clearly $y_1 > y_2$ and, as they are both odd, $y_1 - y_2 \ge 2$ and $2 \mid (y_1 - y_2)$. Write

$$d = \gcd(y_1 - y_2, y_1^{n-1} + y_1^{n-2}y_2 + \cdots + y_2^{n-1})$$

so that $y_2 \equiv y_1 \pmod d$ and

$$0 \equiv y_1^{n-1} + y_1^{n-2}y_2 + \cdots + y_2^{n-1} \equiv ny_1^{n-1} \pmod d.$$

Similarly, we have $ny_2^{n-1} \equiv 0 \pmod d$ and so $d \in \{1, n\}$.

We first deal with the case $d = n$, whereby, from (16), $q = n$. Let $r = \text{ord}_n(y_1 - y_2) \ge 1$ and write $y_1 = y_2 + n^r \kappa$ where $n \nmid \kappa$. Then

$$\text{ord}_n(y_1^{n-1} + y_1^{n-2}y_2 + \cdots + y_2^{n-1}) = \text{ord}_n\left(\frac{(y_2 + n^r\kappa)^n - y_2^n}{n^r\kappa}\right) = 1.$$

Hence

$$(17) \qquad\qquad y_1 - y_2 = 2n^{k-1} \quad \text{and} \quad y_1^{n-1} + y_1^{n-2}y_2 + \cdots + y_2^{n-1} = n,$$

and so

$$n \ = \ \prod_{i=1}^{n-1} |y_1 - \zeta_n^i y_2| \ \geq \ ||y_1| - |y_2||^{n-1}.$$

Recall that y_1 and y_2 are both odd. If $y_2 \neq \pm y_1$, then the right hand-side of this last inequality is at least 2^{n-1}, which is impossible. Thus $y_2 = \pm y_1$, so that, from (17), $y_1^{n-1} \mid n$. It follows that $|y_1| = |y_2| = 1$, contradicting (14).

Thus $d = 1$, whence

(18) $$y_1 - y_2 = 2 \quad \text{and} \quad y_1^{n-1} + y_1^{n-2} y_2 + \cdots + y_2^{n-1} = q^k.$$

Since the polynomial $X^{n-1} + X^{n-2} + \cdots + 1$ has a root modulo q, the Dedekind–Kummer theorem tells us that q splits in $\mathbb{Z}[\zeta_n]$ and so $q \equiv 1 \pmod{n}$. We therefore have the following.

Proposition 3.1. *If x, y, q, k and n are positive integers satisfying* (13) *with n and q prime, then $n \mid q - 1$ and there exists an odd positive integer X such that $y = X(X + 2)$ and*

(19) $$(X + 2)^n - X^n = 2q^k.$$

This last result makes it an extremely straightforward matter to solve equation (7) in case y is odd.

Lemma 3.2. *The only solutions to* (13) *with $3 \leq q < 1000$ prime correspond to the identities*

$$76^2 - 7^4 = 15^3, \quad 122^2 - 11^4 = 3^5. \quad 14^2 - 13^2 = 3^3, \quad 175784^2 - 97^4 = 3135^3,$$

$$234^2 - 109^2 = 35^3, \quad 536^2 - 193^2 = 63^3, \quad 1764^2 - 433^2 = 143^3, \quad 4144^2 - 769^2 = 255^3.$$

Proof. Suppose first that $n = 3$, where equation (19) becomes

(20) $$3(X + 1)^2 + 1 = q^k.$$

From [17] and [18], we know that the equation $3u^2 + 1 = y^m$ has no solutions with $m \geq 3$. We conclude that $k = 1$ or 2. Solving equation (20) with $k = 1$ or 2 and $3 \leq q < 1000$ leads to the seven solutions with $n = 3$.

We now suppose that $n \geq 5$ is prime. By a theorem of the first author and Skinner [7, Theorem 2], the only solutions to the equation $X^n + Y^n = 2Z^2$ with $n \geq 5$ prime and $\gcd(X, Y) = 1$ are with either $|XY| = 1$ or $(n, X, Y, Z) = (5, 3, -1, \pm 11)$. We note that if k is even then (19) can be rewritten as $(X + 2)^n - X^n = 2(q^{k/2})^2$, and therefore $n = 5$, $X = 1$ and $q^{k/2} = 11$. This yields the solution $122^2 - 11^4 = 3^5$.

We may therefore suppose that k is odd. Recalling that $n \mid (q - 1)$ leaves us with precisely 191 pairs (q, n) to consider, ranging from $(11, 5)$ to $(997, 83)$. Fix one of these pairs (q, n) and let $\ell \nmid nq$ be an odd prime. Let $\mathcal{Z}_\ell$ be the set of $\beta \in \mathbb{Z}/(\ell - 1)\mathbb{Z}$ such that β is odd and the polynomial

$$(X + 2)^n - X^n - 2q^\beta$$

has a root in $\mathbb{F}_\ell$. We note that the value of q^k modulo ℓ depends only on the residue class of k modulo $\ell - 1$. From (19), we deduce that $(k \bmod \ell) \in \mathcal{Z}_\ell$. Now let $\ell_1, \ell_2, \ldots, \ell_m$ be a collection of odd primes with $\ell_i \nmid nq$ for $1 \leq i \leq m$. Let

(21) $$M = \mathrm{lcm}(\ell_1 - 1, \ell_2 - 1, \ldots, \ell_m - 1)$$

and set

(22) $$\mathcal{Z}_{\ell_1, \ldots, \ell_m} = \{\beta \in \mathbb{Z}/M\mathbb{Z} \ : \ (\beta \bmod \ell_i) \in \mathcal{Z}_{\ell_i} \text{ for } i = 1, \ldots, m\}.$$

It is clear that $(k \bmod M) \in \mathcal{Z}_{\ell_1, \ldots, \ell_m}$. We wrote a short `Magma` script which, for each pair (q, n), computed $\mathcal{Z}_{\ell_1, \ldots, \ell_m}$ where $\ell_1, \ell_2, \ldots, \ell_m$ are the odd primes ≤ 101 distinct from n and q. In all 191 cases we found that $\mathcal{Z}_{\ell_1, \ldots, \ell_m} = \emptyset$, completing the desired contradiction. □

4. Lucas Sequences and the Primitive Divisor Theorem

The Primitive Divisor Theorem of Bilu, Hanrot and Voutier [10] shall be our main tool for treating equation (8) when $\delta = 0$ and y is odd. In this section, we state this result and a related theorem of Carmichael that shall be useful later. A pair of algebraic integers (γ, δ) is called a **Lucas pair** if $\gamma + \delta$ and $\gamma\delta$ are non-zero coprime rational integers, and γ/δ is not a root of unity. We say that two Lucas pairs (γ_1, δ_1) and (γ_2, δ_2) are **equivalent** if $\gamma_1/\gamma_2 = \pm 1$ and $\delta_1/\delta_2 = \pm 1$. Given a Lucas pair (γ, δ) we define the corresponding **Lucas sequence** by

$$L_m = \frac{\gamma^m - \delta^m}{\gamma - \delta}, \qquad m = 0, 1, 2, \dots .$$

A prime ℓ is said to be a **primitive divisor** of the m-th term if ℓ divides L_m but ℓ does not divide $(\gamma - \delta)^2 \cdot L_1 L_2 \dots L_{m-1}$.

Theorem 6 (Bilu, Hanrot and Voutier [10]). *Let (γ, δ) be a Lucas pair and write $\{L_m\}$ for the corresponding Lucas sequence.*

(i) *If $m \geq 30$, then L_m has a primitive divisor.*
(ii) *If $m \geq 11$ is prime, then L_m has a primitive divisor.*
(iii) *L_7 has a primitive divisor unless (γ, δ) is equivalent to $\left((a - \sqrt{b})/2, (a + \sqrt{b})/2\right)$ where*

$$(23) \qquad\qquad (a, b) \in \{(1, -7), (1, -19)\}.$$

(iv) *L_5 has a primitive divisor unless (γ, δ) is equivalent to $\left((a - \sqrt{b})/2, (a + \sqrt{b})/2\right)$ where*

$$(24) \qquad (a, b) \in \{(1, 5), (1, -7), (2, -40), (1, -11), (1, -15), (12, -76), (12, -1364)\}.$$

Let ℓ be a prime. We define the **rank of apparition of** ℓ in the Lucas sequence $\{L_m\}$ to be the smallest positive integer m such that $\ell \mid L_m$. We denote the rank of apparition of ℓ by m_ℓ. The following theorem of Carmichael [16] will be useful for us; a concise proof may be found in [5, Theorem 8]

Theorem 7 (Carmichael [16]). *Let (γ, δ) be a Lucas pair, and $\{L_m\}$ the corresponding Lucas sequence. Let ℓ be a prime.*

(i) *If $\ell \mid \gamma\delta$ then $\ell \nmid L_m$ for all positive integers m.*
(ii) *Suppose $\ell \nmid \gamma\delta$. Write $D = (\gamma - \delta)^2 \in \mathbb{Z}$.*
    (a) *If $\ell \neq 2$ and $\ell \mid D$, then $m_\ell = \ell$.*
    (b) *If $\ell \neq 2$ and $\left(\frac{D}{\ell}\right) = 1$, then $m_\ell \mid (\ell - 1)$.*
    (c) *If $\ell \neq 2$ and $\left(\frac{D}{\ell}\right) = -1$, then $m_\ell \mid (\ell + 1)$.*
    (d) *If $\ell = 2$, then $m_\ell = 2$ or 3.*
(iii) *If $\ell \nmid \gamma\delta$ then*

$$\ell \mid L_m \iff m_\ell \mid m.$$

5. The equation $x^2 + q^{2k} = y^n$: the proof of Theorem 4

In this section, we prove Theorem 4 with the help of the Primitive Divisor Theorem. We are concerned with the equation

$$(25) \qquad x^2 + q^{2k} = y^n, \qquad x, k, n \text{ positive integers}, \quad n \geq 3, \quad \gcd(x, y) = 1.$$

Here $q \geq 3$ is a prime. Considering this equation modulo 8 immediately tells us that y is odd and x is even. Without loss of generality, we may suppose that $4 \mid n$ or that n is divisible by an odd prime.

Lemma 5.1. *Solutions to* (25) *with* $4 \mid n$ *and odd prime* q *satisfy* $k = 1$, $q^2 = 2y^{n/2} - 1$ *and* $x = (q^2 - 1)/2$. *In particular, the only solutions to* (25) *with* $4 \mid n$ *and prime* $3 \leq q < 1000$ *correspond to the identities*

$$24^2 + 7^2 = 5^4, \quad 840^2 + 41^2 = 29^4 \quad and \quad 28560^2 + 239^2 = 13^8 = 169^4.$$

Proof. Suppose that $4 \mid n$. Then $(y^{n/2} + x)(y^{n/2} - x) = q^{2k}$, and so

$$y^{n/2} + x = q^{2k} \quad and \quad y^{n/2} - x = 1.$$

Thus $2y^{n/2} = q^{2k} + 1$. By Theorem 1 of [7], the only solutions to the equation $A^r + B^r = 2C^2$ with $r \geq 4$, $ABC \neq 0$ and $\gcd(A, B) = 1$ are with $|AB| = 1$ or $(r, A, B, C) = (5, 3, -1, \pm 11)$. It follows that the equation $2y^{n/2} = q^{2k} + 1$ has no solutions with $k \geq 2$ and $4 \mid n$. Therefore $k = 1$, and hence $q^2 = 2y^{n/2} - 1$. The only primes in the range $3 \leq q < 1000$ such that $q^2 = 2y^{n/2} - 1$ with $4 \mid n$, are $q = 7$, 41 and 239, which lead to the solutions in the statement of the lemma. $\square$

Henceforth, we will suppose that n is an odd prime. Thus $x + q^k i = \alpha^n$, where we can write $\alpha = a + bi$, for a and b coprime integers with $y = a^2 + b^2$. Subtracting this equation from its conjugate yields

$$(26) \qquad\qquad q^k = b \cdot \frac{\alpha^n - \overline{\alpha}^n}{\alpha - \overline{\alpha}}.$$

Lemma 5.2. *Solutions to* (25) *with* $n = 3$ *and odd prime* q *must satisfy*

(i) *either* $q = 3$ *and* $(k, x, y) = (2, 46, 13)$;
(ii) *or* $q = 3a^2 - 1$ *for some positive integer* a *and* $(k, x, y) = (1, a^3 - 3a, a^2 + 1)$;
(iii) *or* $q^2 = 3a^2 + 1$ *for some positive integer* a *and* $(k, x, y) = (1, 8a^3 + 3a, 4a^2 + 1)$.

In particular, the only solutions to (25) *with* $n = 3$ *and prime* $3 \leq q < 1000$ *correspond to the identities*

$$46^2 + 3^4 = 13^3, \quad 524^2 + 7^2 = 65^3, \quad 2^2 + 11^2 = 5^3, \quad 52^2 + 47^2 = 17^3,$$

$$1405096^2 + 97^2 = 12545^3, \quad 198^2 + 107^2 = 37^3, \quad 488^2 + 191^2 = 65^3, \quad 1692^2 + 431^2 = 145^3,$$

$$2702^2 + 587^2 = 197^3 \quad and \quad 5778^2 + 971^2 = 325^3.$$

Proof. Let $n = 3$. Thanks to Table 1, we know that the only solution with $q = 3$ is the one given in (i). We may thus suppose that $q \geq 5$. Equation (26) gives

$$q^k = b(3a^2 - b^2).$$

By the coprimality of a and b, we have $b = \pm 1$ or $b = \pm q^k$. We note that $b = -1$ gives $q^k = 1 - 3a^2$ which is impossible. Also if $b = q^k$ then $3a^2 - q^{2k} = 1$ which is impossible modulo 3. Thus either $b = 1$ or $b = -q^k$. If $b = 1$, then

$$q^k = 3a^2 - 1,$$

and if $b = -q^k$ then

$$q^{2k} = 3a^2 + 1.$$

From Theorem 1.1 of [7], these equations have no solutions in positive integers if $k \geq 4$ or $k \geq 2$, respectively. If $k = 3$, the elliptic curve corresponding to the first equation has Mordell-Weil rank 0 over $\mathbb{Q}$ and it is straightforward to show that the equation has no integer solutions. We therefore have that $k = 1$ in either case. Thus $q = 3a^2 - 1$ or $q^2 = 3a^2 + 1$, and these yield the parametric solutions in (ii) and (iii). For $5 \leq q < 1000$, the primes q of the form $3a^2 - 1$ are

$$11, 47, 107, 191, 431, 587 \text{ and } 971.$$

For $5 \leq q < 1000$, the primes q satisfying $q^2 = 3a^2 + 1$ are $q = 7$ and 97. These yield the solutions given in the statement of the lemma. $\square$

We expect that there are infinitely many primes q of the form $3a^2 - 1$, but are very unsure about the number of primes q satisfying $q^2 = 3a^2 + 1$ (the only ones known are $7, 97$ and 708158977). Quantifying such results, in any case, is well beyond current technology.

In view of Lemma 5.2, we henceforth suppose that n is ≥ 5 and prime. The following lemma now completes the proof of Theorem 4.

Lemma 5.3. *Let (k, x, y, n) be a solution to (25) with prime $n \geq 5$ and odd prime q. Then k is odd,*

$$(27) \qquad \begin{cases} n \mid (q-1) & \text{if } q \equiv 1 \pmod 4 \\ n \mid (q+1) & \text{if } q \equiv 3 \pmod 4, \end{cases}$$

and there is an integer a such that

$$y = a^2 + 1, \qquad x = \frac{(a+i)^n + (a-i)^2}{2}, \qquad \frac{(a+i)^n - (a-i)^n}{2i} = \pm q^k.$$

In particular, the only solutions to (25) with prime $3 \leq q < 1000$ and prime $n \geq 5$ correspond to the identities

$$38^2 + 41^2 = 5^5, \qquad 278^2 + 29^2 = 5^7.$$

Proof. Suppose n is ≥ 5 and prime in (25). By Theorem 1 of [4], the equation $A^4 + B^2 = C^m$ has no solutions satisfying $\gcd(A, B) = 1$, $AB \neq 0$ and $m \geq 4$. We conclude that k is odd. We note that $(\alpha, \overline{\alpha})$ is a Lucas pair and write $\{L_m\}$ for the corresponding Lucas sequence. By Theorem 6, L_n must have a primitive divisor, and from (26) this primitive divisor is q. In particular, q does not divide $D = (\alpha - \overline{\alpha})^2 = -4b^2$. Thus by (26) we have $b = \pm 1$ and $D = -4$. Moreover, the rank of apparition of q in the sequence is n. By Theorem 7, we have $n \mid (q-1)$ if $q \equiv 1 \pmod 4$ and $n \mid (q+1)$ if $q \equiv 3 \pmod 4$.

We now let q be a prime in the range $3 \leq q < 1000$. There are 168 pairs (q, n) with q in this range and n a prime ≥ 5 satisfying (27), ranging from $(19, 5)$ to $(997, 83)$. For each of these pairs (q, n), and each sign $\eta = \pm 1$, we need to consider the equation

$$(28) \qquad \frac{(a+i)^n - (a-i)^n}{2i} = \eta \cdot q^k$$

where k is an odd integer. We shall follow the sieving approach of Lemma 3.2 to eliminate all but two of the possible $2 \times 168 = 336$ triples (q, n, η). Fix such a triple (q, n, η). Let $f_n \in \mathbb{Z}[X]$ be the polynomial

$$f_n(X) = \frac{(X+i)^n - (X-i)^n}{2i}.$$

Let $\ell \nmid nq$ be an odd prime, and let $\mathcal{Z}_\ell$ be the set $\beta \in \mathbb{Z}/(\ell-1)\mathbb{Z}$ such that β is odd and $f_n(X) - \eta \cdot q^\beta$ has a root in $\mathbb{F}_\ell$. It follows that $(k \pmod \ell) \in \mathcal{Z}_\ell$. Now let $\ell_1, \ell_2, \cdots, \ell_m$ be a collection of odd primes $\nmid qn$. Define M and $\mathcal{Z}_{\ell_1, \ldots, \ell_m}$ by (21) and (22) respectively. It is clear that $(k \pmod M) \in \mathcal{Z}_{\ell_1, \ldots, \ell_m}$. We wrote a short `Magma` script which, for each triple (q, n, η), computed $\mathcal{Z}_{\ell_1, \ldots, \ell_m}$ where $\ell_1 \ldots, \ell_m$ are the odd primes < 150 distinct from n and q. In all but two of the 336 cases we found that $\mathcal{Z}_{\ell_1, \ldots, \ell_m} = \emptyset$. The two exceptions are $(q, n, \eta) = (41, 5, 1)$ and $(29, 7, -1)$, and so these are the only two cases we need to consider. Let

$$F_n(X, Y) = \frac{(X + iY)^n - (X - iY)^n}{2iY}.$$

This is a homogeneous degree $n - 1$ polynomial belonging to $\mathbb{Z}[X, Y]$. Now (28) can be written as $F_n(a, 1) = \eta \cdot q^k$. Thus it is sufficient to solve the Thue–Mahler equations $F_n(X, Y) = \eta \cdot q^k$ for $(q, n, \eta) = (41, 5, 1)$ and $(29, 7, -1)$. Explicitly these equations are

$$(29) \qquad 5X^4 - 10X^2Y^2 + Y^4 = 41^k$$

and

$$(30) \qquad\qquad 7X^6 - 35X^4Y^2 + 21X^2Y^4 - Y^6 = -29^k.$$

Using the `Magma` implementation of the Thue–Mahler solver described in [20], we find that the solutions to (29) are $(X, Y, k) = (\pm 2, \pm 1, 1)$ and $(0, \pm 1, 0)$, and that the solutions to (30) are also $(X, Y, k) = (\pm 2, \pm 1, 1)$ and $(0, \pm 1, 0)$. These lead to the two solutions in the statement of the lemma.   □

6. The equation $x^2 - q^{2k} = y^n$ with y even: reduction to Thue–Mahler equations

Section 3 dealt with (7) in the case that y is odd, using purely elementary means. We now turn our attention to (7) with y even, and consider the equation

$$(31) \quad x^2 - q^{2k} = y^n, \qquad x, k, n \text{ positive integers}, \quad n \geq 3, \quad \gcd(x, y) = 1, \quad y \text{ an even integer}.$$

Here $q \geq 3$ is a prime and, without loss of generality, $n = 4$ or n is an odd prime.

Lemma 6.1. *Write $\gamma = 1 + \sqrt{2}$. Any solution to (31) with $n = 4$ and q an odd prime must satisfy $k = 1$,*

$$(32) \qquad q = \frac{\gamma^{2m} + \gamma^{-2m}}{2}, \quad x = \frac{\gamma^{4m} + 6 + \gamma^{-4m}}{8} \quad and \quad y = \frac{\gamma^{2m} - \gamma^{-2m}}{2\sqrt{2}},$$

for some integer m. In particular, the only solutions with $3 \leq q < 1000$ correspond to the identities

$$5^2 - 3^2 = (\pm 2)^4, \quad 145^2 - 17^2 = (\pm 12)^4 \quad and \quad 166465^2 - 577^2 = (\pm 408)^4.$$

Proof. Suppose $n = 4$. Then $(x + y^2)(x - y^2) = q^{2k}$, and so, by the coprimality of x and y,

$$x + y^2 = q^{2k} \quad and \quad x - y^2 = 1,$$

or equivalently

$$(33) \qquad\qquad x = \frac{q^{2k} + 1}{2} \quad and \quad q^{2k} - 2y^2 = 1.$$

First we show that $k = 1$. From the second equation, we have $(q^k + 1)(q^k - 1) = 2y^2$. Since the greatest common divisor of the two factors on the left is 2 we see that one of the two factors must be a perfect square, i.e. $q^k + 1 = z^2$ or $q^k - 1 = z^2$ for some non-zero integer z, and it is easy to see that k must be odd. The impossiblity of these cases for $k \geq 3$ follows from Mihăilescu's theorem [33] (i.e. Catalan's conjecture). Hence $k = 1$.

The second equation in (33) implies that $q + y\sqrt{2}$ is a totally positive unit in $\mathbb{Z}[\sqrt{2}]$. Thus

$$(34) \qquad\qquad q + y\sqrt{2} = \gamma^{2m} \quad and \quad q - y\sqrt{2} = \gamma^{-2m},$$

for some integer m. The formulae for q and y in (32) follow from this, and the formula for x follows from the first relation in (33).

We focus on primes $3 \leq q < 1000$. From the first relation in (34),

$$|m| < \frac{\log(2q)}{2\log \gamma} < \frac{\log(2000)}{2\log(1 + \sqrt{2})} < 5.$$

Thus $-4 \leq m \leq 4$. The values $m = \pm 1, \pm 2, \pm 4$, respectively, give the three solutions in the statement of the Lemma. If $m = 0$ or ± 3, then we obtain $q = 1$ or 99 which are not prime.   □

In view of Lemma 6.1, we may henceforth suppose that $n \geq 3$ is odd. Let x' be either x or $-x$, chosen so that $x' \equiv q^k \pmod{4}$. From (31), we deduce the existence of relatively prime integers y_1 and y_2 for which

$$(35) \qquad\qquad x' + q^k = 2y_1^n \quad and \quad x' - q^k = 2^{n-1}y_2^n,$$

with $y = 2y_1 y_2$, so that we have

$$(36) \qquad y_1^n - 2^{n-2} y_2^n = q^k.$$

We have thus reduced the resolution of (31) for particular q and n to solving a degree n Thue–Mahler equation.

Lemma 6.2. *The only solutions to* (31) *with* $n \in \{3, 5\}$ *and* $3 \le q < 1000$ *an odd prime correspond to the identities*

$$53^2 - 3^2 = 40^3, \ 1^2 - 3^2 = (-2)^3, \ 7^2 - 3^4 = (-2)^5, \ 29^2 - 5^4 = 6^3, \ 9^2 - 7^2 = 2^5, \ 43^2 - 11^2 = 12^3,$$

$$499^2 - 13^2 = 12^5, \ 15^2 - 17^2 = -4^3, \ 397^2 - 17^4 = 42^3, \ 25^2 - 29^2 = (-6)^3, \ 11^2 - 43^2 = (-12)^3,$$

$$1415^2 - 43^2 = 126^3, \ 30042907^2 - 43^8 = 96222^3, \ 500047^2 - 47^2 = 6300^3, \ 55^2 - 53^2 = 6^3,$$

$$179^2 - 71^2 = 30^3, \ 4785^2 - 71^4 = (-136)^3, \ 775^2 - 89^2 = 84^3, \ 155^2 - 101^2 = 24^3,$$

$$13609^2 - 109^2 = 570^3, \ 141^2 - 109^2 = 20^3, \ 129^2 - 127^2 = 8^3, \ 123^2 - 127^2 = (-10)^3,$$

$$2789^2 - 127^2 = 198^3, \ 71^2 - 179^2 = (-30)^3, \ 4197^2 - 197^2 = 260^3, \ 277^2 - 223^2 = 30^3,$$

$$249^2 - 251^2 = (-10)^3, \ 235^2 - 251^2 = (-6)^5, \ 255^2 - 257^2 = -4^5, \ 118901^2 - 263^2 = 2418^3,$$

$$223^2 - 277^2 = (-30)^3, \ 2355^2 - 307^2 = 176^3, \ 143027^2 - 307^4 = 2262^3, \ 557^2 - 307^2 = 60^3,$$

$$327^2 - 359^2 = (-28)^3, \ 4146689^2 - 383^4 = 25800^3, \ 289^2 - 397^2 = (-42)^3, \ 433^2 - 431^2 = 12^3,$$

$$431^2 - 433^2 = (-12)^3, \ 4308693^2 - 433^4 = 26462^3, \ 979^2 - 479^2 = 90^3, \ 13^2 - 499^2 = (-12)^5,$$

$$23831^2 - 503^2 = 828^3, \ 307^2 - 557^2 = (-60)^3, \ 93^2 - 593^2 = (-70)^3, \ 857^2 - 601^2 = 72^3,$$

$$713^2 - 659^2 = 42^3, \ 85016415^2 - 683^2 = 193346^3, \quad 297053^2 - 701^2 = 4452^3, \quad 731^2 - 727^2 = 18^3,$$

$$3655^2 - 739^2 = 234^3, \ 561^2 - 811^2 = (-70)^3, \ 601^2 - 857^2 = (-72)^3 \quad and \quad 1051^2 - 997^2 = 48^3.$$

Proof. For $n \in \{3, 5\}$ and primes $3 \le q < 1000$, we solved the Thue–Mahler equation (36) using the `Magma` implementation of the Thue–Mahler solver described in [20]. The computation resulted in the solutions given in the statement of the lemma. $\square$

7. The modular approach to Diophantine equations: some background

Let $F/\mathbb{Q}$ be an elliptic curve over the rationals of conductor N_F and minimal discriminant Δ_F. Let $p \ge 5$ be a prime. The action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the p-torsion $F[p]$ gives rise to a 2-dimensional mod p representation

$$\overline{\rho}_{F,p} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_p).$$

Suppose $\overline{\rho}_{F,p}$ is irreducible (i.e. F does not have an p-isogeny); this can often be established by appealing to Mazur's isogeny theorem [30]. A standard consequence of Ribet's lowering theorem [36], building on the modularity of elliptic curves over $\mathbb{Q}$ due to Wiles and others [45], [12], is that $\overline{\rho}_{F,p}$ arises from a weight 2 newform of level

$$N = N_F \Big/ \prod_{\substack{\ell \, \| \, N_F \\ p \, | \, \mathrm{ord}_\ell(\Delta_F)}} \ell \, .$$

More precisely, there is a newform f of weight 2 and level N with normalized $\mathfrak{q}$-expansion

$$(37) \qquad f = \mathfrak{q} + \sum_{m=2}^{\infty} c_m \mathfrak{q}^m$$

such that

$$(38) \qquad \overline{\rho}_{F,p} \sim \overline{\rho}_{f,\mathfrak{p}}$$

where $\mathfrak{p}$ is a prime ideal above p of the ring of integers $\mathcal{O}_f$ of the Hecke eigenfield $K_f = \mathbb{Q}(c_1, c_2, \dots)$.

The original motivation for the great theorems of Ribet and Wiles included Fermat's Last Theorem. To motivate what is to come in later sections, we quickly sketch the deduction of FLT from the above. Let x, y and z be non-zero coprime rational integers satisfying $x^p + y^p + z^p = 0$ where $p \geq 5$ is prime. After appropriately permuting x, y and z, we may suppose that $2 \mid y$ and that $x^n \equiv -1 \pmod 4$. Let F be the Frey–Hellegouarch curve

$$Y^2 = X(X - x^p)(X + y^p).$$

It follows from Mazur's isogeny theorem and related results that $\bar{\rho}_{E,p}$ is irreducible. A short computation reveals that

$$\Delta_F = 2^{-8}(xyz)^{2p} \quad \text{and} \quad N_F = 2\,\mathrm{Rad}(xyz),$$

where $\mathrm{Rad}(m)$ denotes the product of the prime divisors of m. We find that $N = 2$. Thus $\bar{\rho}_{F,p}$ arises from a newform f of weight 2 and level 2; the nonexistence of such newforms provides the desired contradiction.

It is possible to use a similar strategy to treat various Diophantine problems including generalised Fermat equations $Ax^p + By^q = Cz^r$, for certain signatures (p, q, r). This is done by Kraus [25] for signature (p, p, p) and by the first author and Skinner [7] for signature $(p, p, 2)$. Fortunately, these papers provide recipes for the Frey–Hellegouarch curves F and for the levels N, and establish the required irreducibility of $\bar{\rho}_{F,n}$. We shall make frequent use of these recipes in later sections. It is known (and easily checked using standard dimension formulae) that there are no weight 2 newforms at levels

$$(39) \qquad\qquad 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 22, 25, 28, 60,$$

but there are newforms at all other levels. Thus, if the level N predicted by the recipes is not in the list (39) then we do not immediately obtain a contradiction. Instead, we may compute the possible newforms using implementations (e.g. in `Magma` or `SAGE`) of modular symbols algorithms due to Cremona [19] and Stein [42]. We then use the relation (38) to help us extract information about the solutions to our Diophantine equation. In doing this, we shall often make use of the following standard result, e.g. [27], [40, Section 5].

Lemma 7.1. *Let $F/\mathbb{Q}$ be an elliptic curve of conductor N_F. Let f be a weight 2 newform of level N having $\mathfrak{q}$-expansion as in (37). Suppose (38) holds for some prime $p \geq 5$. Let $\ell \neq p$ be a rational prime.*

　　(i) If $\ell \nmid N_F N$ then $a_\ell(F) \equiv c_\ell \pmod{\mathfrak{p}}$.
　　(ii) If $\ell \nmid N$ but $\ell \parallel N_F$ then $\ell + 1 \equiv \pm c_\ell \pmod{\mathfrak{p}}$.

If f is a rational newform (i.e. $K_f = \mathbb{Q}$) then (i), (ii) also hold for $\ell = p$.

We will also make frequent use of the following theorem of Kraus [25, Proposition 2].

Theorem 8 (Kraus). *Let f be a newform of weight 2 and level N with $\mathfrak{q}$-expansion as in (37), and Hecke eigenfield K_f with ring of integers $\mathcal{O}_f$. Write*

$$M = \mathrm{lcm}(4, N) \quad \text{and} \quad \mu(M) = M \cdot \prod_{\substack{r \mid M \\ r \ prime}} \left(1 + \frac{1}{r}\right).$$

Let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_f$ and suppose the following two conditions hold.

　　(i) For all primes $\ell \leq \mu(M)/6$, $\ell \nmid 2N$, we have

$$\ell + 1 \equiv c_\ell \pmod{\mathfrak{p}}.$$

(ii) For all primes $\ell \leq \mu(M)/6$, $\ell \mid 2N$, $\ell^2 \nmid 4N$, we have

$$(\ell + 1)(c_\ell - 1) \equiv 0 \pmod{\mathfrak{p}}.$$

Then $\ell + 1 \equiv c_\ell \pmod{\mathfrak{p}}$ for all primes $\ell \nmid 2N$.

8. The equation $x^2 - q^{2k} = y^n$ with y even: an approach via Frey curves

We are still concerned with equation (31). In view of the results of Section 6, we may suppose that $n \geq 7$ is prime. To show that (31) has no solutions for a particular pair (q, n), it is enough to show the same for (36). We shall think of (36) as a Fermat equation of signature (n, n, n) by writing it as $y_1^n - 2^{n-2}y_2^n = q^k \cdot 1^n$. This enables us to apply recipes of Kraus [25] for Frey–Hellegouarch curves and level lowering. The following lemma will eliminate some cases when applying those recipes.

Lemma 8.1. *Suppose $n \geq 7$ is prime. Then $\gcd(k, 2n) = 1$.*

Proof. Theorem 1.2 of [7] asserts that the equation $A^p + 2^\alpha B^p = C^2$ with prime $p \geq 7$ has no solutions in non-zero integers with $\gcd(A, B, C) = 1$ and $\alpha \geq 2$. It immediately follows from (36) that k is odd. Moreover, Theorem 3 of [37] asserts that the equation $A^p + 2^\alpha B^p + C^p = 0$ has no solutions with $ABC \neq 0$ for prime $p \geq 7$ and $2 \leq \alpha \leq p - 1$. It follows that $n \nmid k$. □

Following Kraus, we attach to a solution of (36) a Frey–Hellegouarch curve F, where

$$(40) \qquad F \;:\; Y^2 = X(X + y_1^n)(X + 2^{n-2}y_2^n)$$

if $q \equiv 1 \pmod 4$, and

$$(41) \qquad F \;:\; Y^2 = X(X - q^k)(X + 2^{n-2}y_2^n),$$

if $q \equiv 3 \pmod 4$. The Frey–Hellegouarch curve F is semistable, and has minimal discriminant and conductor respectively given by

$$(42) \qquad \Delta_F = 2^{2n-12}q^{2k}(y_1 y_2)^n \quad \text{and} \quad N_F = 2q \cdot \mathrm{Rad}_2(y_1 y_2),$$

where $\mathrm{Rad}_2(m)$ denotes the product of the odd primes dividing m. From Kraus [25], the mod n representation of F arises from a newform f of weight 2 and level $N = 2q$.

Let $\ell \nmid 2q$ be a prime. Write

$$T \;=\; \{a \in \mathbb{Z} \cap [-2\sqrt{\ell}, 2\sqrt{\ell}] \;:\; a \equiv \ell + 1 \pmod 4\}.$$

Let

$$\mathcal{D}'_{f,\ell} = ((\ell + 1)^2 - c_\ell^2) \cdot \prod_{a \in T}(a - c_\ell),$$

and

$$\mathcal{D}_{f,\ell} = \begin{cases} \ell \cdot \mathcal{D}'_{f,\ell} & \text{if } K_f \neq \mathbb{Q} \\ \mathcal{D}'_{f,\ell} & \text{if } K_f = \mathbb{Q}, \end{cases}$$

Lemma 8.2. *Let f be a newform of weight 2 and level $2q$, and suppose that (38) holds. Let $\ell \nmid 2q$ be a prime. Then $\mathfrak{n} \mid \mathcal{D}_{f,\ell}$.*

Proof. If $\ell \nmid y_1 y_2$, then $\ell \nmid N_F$ and so is a prime of good reduction for F. As F has full 2-torsion we deduce that $4 \mid (\ell + 1 - a_\ell(F))$. By the Hasse–Weil bounds, $a_\ell(F)$ belongs to the set T. If $\ell \mid y_1 y_2$, then $\ell \parallel N_F$. The lemma now follows from Lemma 7.1. □

It is straightforward from Lemma 8.2 and the fact that $\mathfrak{n} \mid n$ that $n \mid \mathrm{Norm}(\mathcal{D}_{f,\ell})$. Thus if $\mathcal{D}_{f,\ell} \neq 0$, we immediately obtain an upper bound upon the exponent n. This approach will result in a bound on the exponent n in (31) unless f corresponds to an elliptic curve over $\mathbb{Q}$ with full 2-torsion and conductor $N = 2q$; for this see [40, Section 9]. Mazur showed that such an elliptic curve exists if and only if $q \geq 31$ is a Fermat or a Mersenne prime; see for example [40, Theorem

8]. We note that 31, 127 and 257 are the only such primes in our range $3 \leq q < 1000$. We shall exploit this approach to prove the following.

Proposition 8.3. *Let $n \geq 7$ and $3 \leq q < 1000$ be primes.*

> (i) *If $q \notin \{31, 127, 257\}$, then (31) has no solutions.*
> (ii) *Suppose $q \in \{31, 127, 257\}$, write $q = 2^m + \eta$ where $\eta = \pm 1$, and let*

(43) $$E_q \ : \ Y^2 = X(X + 1)(X - \eta \cdot 2^m).$$

> *Suppose (k, x, y) is a solution to (31) and let F be as above. Then*

$$\overline{\rho}_{F,n} \sim \overline{\rho}_{E_q,n}$$

In Cremona's notation, these E_q are the elliptic curves `62a2`, `254d2` and `514a2`, for $q = 31, 127$ and 257, respectively.

Proof. There are no newforms of weight 2 and levels 6, 10 and 22. Therefore the proof is complete in the cases where $q \in \{3, 5, 11\}$. We may thus suppose that $7 \leq q < 1000$ is prime and that $q \neq 11$.

For a newform f of weight 2 and level $2q$, and a collection of primes $\ell_1, \ldots, \ell_m$ (all coprime to $2q$), we write $\mathcal{D}_{f,\ell_1,\ldots,\ell_m}$ for the ideal of $\mathcal{O}_f$ generated by $\mathcal{D}_{f,\ell_1}, \ldots, \mathcal{D}_{f,\ell_m}$. Let $\mathcal{B}_{f,\ell_1,\ldots,\ell_m} \in \mathbb{Z}$ be the norm of the ideal $\mathcal{D}_{f,\ell_1,\ldots,\ell_m}$. If $\overline{\rho}_{F,n} \sim \overline{\rho}_{f,\mathbf{n}}$, then $\mathfrak{n} \mid \mathcal{D}_{f,\ell_1,\ldots,\ell_m}$ by Lemma 8.2. As $\mathfrak{n} \mid n$, we deduce that $n \mid \mathcal{B}_{f,\ell_1,\ldots,\ell_m}$. In our computations we will take $\ell_1, \ldots, \ell_m$ to be all the primes < 200 distinct from 2 and q, and write $\mathcal{B}_f$ for $\mathcal{B}_{f,\ell_1,\ldots,\ell_m}$.

We wrote a short `Magma` script which computed, for all newforms f at all levels $2q$ under consideration, the integer $\mathcal{B}_f$. We found that $\mathcal{B}_f \neq 0$ for all newforms f except for three rational newforms of levels 62, 254 and 514 (corresponding to $q = 31, 127$ and 257, respectively). Thus, for all other newforms, we at least obtain a bound on n. In many cases this bound is already sharp enough to contradict our assumption that $n \geq 7$. We give a few examples.

Let $q = 13$. Then there are two eigenforms f_1, f_2 of level $2q = 26$, and

$$\mathcal{B}_{f_1} = 3 \times 5, \qquad \mathcal{B}_{f_2} = 3 \times 7.$$

Thus we eliminate f_1 from consideration, and also conclude that $n = 7$. It is natural to wonder if $n = 7$ can be eliminated by increasing the size of our set of primes $\ell_1, \ldots, \ell_m$, but this is not the case. The newform f_2 is rational and corresponds to the elliptic curve `26b1` with Weierstrass model

$$E' \ : \ Y^2 + XY + Y = X^3 - X^2 - 3X + 3.$$

The torsion subgroup of $E'(\mathbb{Q})$ is isomorphic to $\mathbb{Z}/7\mathbb{Z}$, generated by the point $(1, 0)$. In particular, for any prime $\ell \nmid 26$, we have $7 \mid (\ell + 1 - a_\ell(E'))$. Since $a_\ell(E') = c_\ell(f_2)$, we have $7 \mid \mathcal{B}_{f_2,\ell}$. Thus $7 \mid \mathcal{B}_{f,\ell_1,\ldots,\ell_n}$ regardless of the set of primes $\ell_1, \ldots, \ell_n$ that we choose. However we can still obtain a contradiction for $n = 7$ in this case. Indeed, we have $\overline{\rho}_{F,7} \sim \overline{\rho}_{f_2,7} \sim \overline{\rho}_{E',7}$. Since E' has non-trivial 7-torsion, the representation $\overline{\rho}_{E',7}$ is reducible. However, the representation of the Frey curve $\overline{\rho}_{F,7}$ is irreducible as shown by Kraus [25, Lemme 4], contradicting the fact that F has full rational 2-torsion.

For $q = 31$, there are two newforms, g_1 and g_2. We find that $\mathcal{B}_{g_1} = 0$ and $\mathcal{B}_{g_2} = 2^3 \times 3^2$; thus we may eliminate g_2 for consideration. The eigenform g_1 is rational and corresponds to the elliptic curve E_{31} with Cremona label `62a2`. Hence $\overline{\rho}_{F,p} \sim \overline{\rho}_{g_1,p} \sim \overline{\rho}_{E_{31},p}$, whence the proof is complete for $q = 31$.

For $q = 37$, there are two newforms, h_1 and h_2. We find that $\mathcal{B}_{h_1} = 3^3$ and $\mathcal{B}_{h_2} = 19$. Thus $n = 19$ and

(44) $$\overline{\rho}_{F,19} \sim \overline{\rho}_{h_2,19}.$$

The newform h_2 has $\mathfrak{q}$-expansion

$$h_2 = \mathfrak{q} + \mathfrak{q}^2 + \alpha\mathfrak{q}^3 + \mathfrak{q}^4 + (-3\alpha - 1)\mathfrak{q}^5 + \alpha\mathfrak{q}^6 + 2\alpha\mathfrak{q}^7 + \cdots, \quad \text{where} \quad \alpha = \frac{-1 + \sqrt{5}}{2},$$

and Hecke eigenfield $K = \mathbb{Q}(\sqrt{5})$. Let $\mathfrak{n}$ be the prime ideal $\mathfrak{n} = (4 - \alpha) \cdot \mathcal{O}_K$ having norm 19. We checked, using Theorem 8, that $\ell + 1 \equiv c_\ell \pmod{\mathfrak{n}}$ for all primes $\ell \nmid 2 \cdot 37$, where c_ℓ is the ℓ-th coefficient of h_2. From relation (44), we know that

$$a_\ell(F) \equiv c_\ell \pmod{\mathfrak{n}}$$

for all primes ℓ of good reduction for $F_{3,1}$. Thus $19 \mid (\ell + 1 - a_\ell(F_{3,1}))$ for all primes ℓ of good reduction. As before, this now implies that $\overline{\rho}_{F,19}$ is reducible [38, IV-6], giving a contradiction. The proof is thus complete for $q = 37$.

The above arguments allow us to prove (ii) in the statement of the proposition, and to obtain a contradiction for all $3 \leq q < 1000$, $q \notin \{31, 127, 257\}$, except when $n = 7$ and q belongs to the list

$$43, \ 101, \ 103, \ 139, \ 163, \ 379, \ 467, \ 509, \ 557, \ 569, \ 839, \ 937, \ 947, \ 977.$$

For $n = 7$ and these values of q, we checked using the aforementioned Thue–Mahler solver that the only solutions to (36) are $(y_1, y_2, k) = (1, 0, 0)$. Since $k \neq 0$ in (31), the proof is complete. $\square$

Symplectic criteria. When $q \geq 31$ is a Fermat or Mersenne prime, it does not seem to be possible, working purely with Galois representations of elliptic curves, to eliminate the possibility that $\overline{\rho}_{F,n} \sim \overline{\rho}_{E_q,n}$. However, the so-called 'symplectic method' of Halberstadt and Kraus [21] allows us to derive an additional restriction on the solutions to (31).

Lemma 8.4. *Let $q = 2^m + \eta$ be a Fermat or Mersenne prime. Let $n \geq 7$ be a prime $\neq q$. Suppose (x, y, k) is a solution to (31), and let F be the Frey–Hellegouarch curve constructed above, and E_q be given by (43). Suppose $\overline{\rho}_{F,n} \sim \overline{\rho}_{E_q,n}$. Then either $n \mid (m - 4)$ or*

$$(45) \qquad\qquad \left(\frac{(24 - 6m)k}{n}\right) = 1.$$

Proof. We note that the curves F and E_q have multiplicative reduction at both 2 and q. Write Δ_1 and Δ_2 for the minimal discriminants of F and E_q, respectively. By [21, Lemme 1.6], the ratio

$$\frac{\text{ord}_2(\Delta_1) \cdot \text{ord}_q(\Delta_1)}{\text{ord}_2(\Delta_2) \cdot \text{ord}_q(\Delta_2)}$$

is a square modulo n, provided $n \nmid \text{ord}_2(\Delta_i)$, $n \nmid \text{ord}_q(\Delta_i)$. It is in invoking this result of Halberstadt and Kraus that we require the assumption that $n \neq q$. We find that

$$\Delta_1 = 2^{2n-12} q^{2k} (y_1 y_2)^{2n} \quad \text{and} \quad \Delta_2 = 2^{2m-8} q^2.$$

We have previously noted that $n \nmid k$ by appealing to a result of Ribet. Suppose $n \nmid (m - 4)$. Then the valuations $\text{ord}_2(\Delta_i)$ and $\text{ord}_q(\Delta_i)$ are all indivisible by n. The result follows. $\square$

9. THE EQUATION $x^2 - q^{2k} = y^n$: AN UPPER BOUND FOR THE EXPONENT n

To help us complete the proof of Theorem 5, we begin by deriving an upper bound for n. Our approach is essentially a minor sharpening of Theorem 3 of Bugeaud [13] in a slightly special case. Since this result is valid for an arbitrary prime q, it may be of independent interest.

Theorem 9. *Let x, y, q, $k \geq 1$ and $n \geq 3$ be integers satisfying equation (7), with n and q prime, and $q \nmid x$. Then*

$$n \ < \ 1000 \, q \log q.$$

Proof. If $q = 2$, then we have that $n \leq 5$ from Theorem 1.2 of [7]. We may thus suppose that q is odd and, additionally, that y is even, or, via Proposition 3.1, we immediately obtain the much stronger result that $n \mid (q-1)$. We are therefore in case (35). By Proposition 8.3, we may suppose that $q = 31$ or that $q \geq 127$. Set $Y = \max\{|y_1|, |2y_2|\}$ and suppose first that

$$(46) \qquad\qquad q^k \geq Y^{n/2},$$

or equivalently

$$(47) \qquad\qquad 2k \log q \geq n \log Y.$$

We set

$$\Lambda = \frac{q^k}{(2y_2)^n} = \left(\frac{y_1}{2y_2}\right)^n - \frac{1}{4};$$

we wish to apply an upper bound for linear forms in q-adic logarithms to Λ, in order to bound k. To do this, we must first treat the case where $y_1/2y_2$ and $1/4$ are multiplicatively dependent, i.e. where $y_1 y_2$ has no odd prime divisors. Under this assumption, since y_1 is odd, we find from (36) that

$$2^j \pm 1 = q^k,$$

for an integer j with $j \equiv -2 \pmod{n}$. Via Mihailescu's theorem [33], if $n \geq 7$, necessarily $k = 1$, $y_1 = \pm 1$, $y_2 = -2^\kappa$ for some integer κ and

$$q = 2^{(\kappa+1)n-2} \pm 1.$$

In this case, we find a solution to equation (7) corresponding to the identity

$$(-q \pm 2)^2 - q^2 = 4 \mp 4q = \left(\mp 2^{\kappa+1}\right)^n,$$

whereby, certainly $n < 1000\, q \log q$.

Otherwise, we may suppose that $y_1/2y_2$ and $1/4$ are multiplicatively independent and that $Y \geq 3$. We will appeal to Théorème 4 of Bugeaud and Laurent [14], with, in the notation of that result, $(\mu, \nu) = (10, 5)$ (see also Proposition 1 of Bugeaud [13]). Before we state this result, we require some notation. 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 $\mathbb{Q}$, define the *absolute logarithmic height* of α via the formula

$$(48) \qquad\qquad h(\alpha) = \frac{1}{d}\left(\log|a_0| + \sum_{i=1}^{d} \log \max\left(1, |\alpha^{(i)}|\right)\right),$$

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 $\mathbb{C}$.

Theorem 10 (Bugeaud-Laurent). *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 apply this with

$$f = 1, \ D = 1, \ \alpha_1 = y_1/2y_2, \ \alpha_2 = 1/4, \ b_1 = n, \ b_2 = 1,$$

so that we may choose

$$\log A_1 = \max\{\log Y, \log q\}, \ \log A_2 = \max\{2\log 2, \log q\},$$

and

$$b' = \frac{n}{\log A_2} + \frac{1}{\log A_1}.$$

Let us assume now that

(49)
$$n \geq 1000 \, q \log q,$$

whilst recalling that either $q = 31$ or $q \geq 127$. We therefore have

$$b' < 1.001 \frac{n}{\log q}$$

and hence find that

(50)
$$k \leq 24 \frac{q}{\log^3 q} \left(\max\left\{\log n + 0.401, 10\log q\right\}\right)^2 \log A_1,$$

whence, from (47),

(51)
$$n \log Y \leq 48 \frac{q}{\log^2 q} \left(\max\left\{\log n + 0.401, 10\log q\right\}\right)^2 \log A_1.$$

Let us suppose first that

$$\log n + 0.401 \geq 10\log q.$$

If $q \geq Y$, we have that $\log A_1 = \log q$ and hence

$$\frac{n\log Y}{(\log n + 0.401)^2} \leq 48 \frac{q}{\log q}.$$

From (49), we thus have

$$\frac{\log^2 q}{(\log(1000q\log q) + 0.401)^2} \leq \frac{0.048}{\log Y} \leq \frac{0.048}{\log 3},$$

contradicting $q \geq 31$. If, on the other hand, $q < Y$, then $\log A_1 = \log Y$ and so

(52)
$$\frac{n}{(\log n + 0.401)^2} \leq 48 \frac{q}{\log^2 q}.$$

With (49), this implies that

$$\log^3 q < 0.048 \left(\log(1000q\log q) + 0.401\right)^2,$$

again contradicting $q \geq 31$.

We may therefore assume that

$$\log n + 0.401 < 10\log q,$$

so that

$$n\log Y \leq 4800 \, q \log A_1.$$

If $q \geq Y$, then, from (49),

$$\log Y < 4.8,$$

whereby $3 \leq Y \leq 121$. If $|y_1| \geq 2|y_2|$, it follows from equation (36) that

$$(53) \qquad q^k \geq |y_1|^n - \frac{1}{4}|y_1|^n = \frac{3}{4}Y^n.$$

Suppose, conversely, that $|y_1| \leq 2|y_2| - 1$ (so that $1 \leq |y_2| \leq 60$). If $y_1 > 0$ and $y_2 < 0$, it follows from (36) that

$$(54) \qquad q^k > \frac{1}{4}Y^n.$$

We may thus suppose that y_1 and y_2 have the same sign, whence, from (36), (49) and $|y_2| \leq 60$,

$$(55) \qquad q^k = 2^{n-2}|y_2|^n - |y_1|^n > 0.24 \cdot |2y_2|^n = 0.24 \cdot Y^n.$$

Combining (53), (54) and (55), we thus have from (50) that

$$n \log Y + \log(0.24) < k \log q \leq 2400 \, q \log q,$$

contradicting (49) and $q \geq 31$. If $q < Y$, then, via (49),

$$(56) \qquad 1000 \, q \log q \leq n \leq 4800 \, q,$$

a contradiction for $q \geq 127$. We may thus suppose that $q = 31$, $Y > 31$ and, from (52), $n \leq 12119$, which contradicts (49).

Next suppose that inequality (46) (and hence also inequality (47)) fails to hold. In this case, we will apply lower bounds for linear forms in two complex logarithms. Following Bugeaud, we take

$$\Lambda_1 = 4\Lambda = \frac{4q^k}{(2y_2)^n} = 4\left(\frac{y_1}{2y_2}\right)^n - 1,$$

so that

$$(57) \qquad \log|\Lambda_1| = 2\log 2 + k\log q - n\log(|2y_2|).$$

If $Y = \max\{|y_1|, |2y_2|\} = |y_1|$, then, from (35), it follows that

$$q^k \geq \frac{3}{4}|y_1|^n = \frac{3}{4}Y^n,$$

contradicting $q^k < Y^{n/2}$. It follows that $Y = |2y_2|$ and so, from (57),

$$(58) \qquad \log|\Lambda_1| = 2\log 2 + k\log q - n\log Y \leq 2\log 2 - \frac{n}{2}\log Y.$$

From (49), we have that $|\Lambda_1| \leq 1/2000$, so that

$$(59) \qquad \left| n\log\left|\frac{2y_2}{y_1}\right| - 2\log 2 \right| \leq |\log(1 - \Lambda_1)| \leq 1.001\,|\Lambda_1|.$$

We will appeal to Corollary 1 of Laurent [28] :

Theorem 11 (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

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

Applying this result to the left hand side of (59), with $(m, C) = (10, 32.3)$,

$$\beta_2 = |2y_2/y_1|, \ \beta_1 = 4, \ c_2 = n, \ c_1 = 1, \ D = 1,$$

$$\log B_2 = \log Y, \ \log B_1 = 2 \log 2 \ \text{ and } \ b' = \frac{n}{2 \log 2} + \frac{1}{\log Y} < \frac{1.001n}{2 \log 2},$$

we may conclude that

$$\log |\Lambda_1| \geq -0.001 - 44.8 \left(\max \{\log n - 0.11, 10\} \right)^2 \log Y.$$

Combining this with (58), we thus have

$$n \leq 89.6 \left(\max \{\log n - 0.11, 10\} \right)^2 + \frac{1.4}{\log Y}.$$

After a little work we find that

$$n \leq 8961,$$

contradicting (49) and $q \geq 31$. □

10. THE EQUATION $x^2 - q^{2k} = y^n$: PROOF OF THEOREM 5

In this section, we complete the proof of Theorem 5. Let $3 \leq q < 1000$ be a prime and let (k, x, y, n) be a solution to (7) where $x, k \geq 1$ and $n \geq 3$ are positive integers satisfying $q \nmid x$. Thanks to Lemmata 3.2, 6.1 and 6.2, we may suppose that y is even and that $n \geq 7$ is prime. It follows from Proposition 8.3 that $q = 31$, 127 or 257 and $\overline{\rho}_{F,n} \sim \overline{\rho}_{E_q,n}$, where E_q is given in (43), and F is the Frey–Hellegouarch curve given in (40) or (41) according to whether $q \equiv 1$ or 3 (mod 4). From Theorem 9, we have

$$n < 1000 \times 257 \times \log(257) < 1.5 \times 10^6.$$

We now give a method, which for given exponent n and prime $q \in \{31, 127, 257\}$, is capable of showing that (36) has no solutions. This is an adaptation of the method called 'predicting the exponents of constants' in [40, Section 13]. Let $n \geq 7$ be prime and choose $\ell \neq q$ to be a prime satisfying the following:

(i) $\ell = tn + 1$ for some positive integer t;
(ii) $n \nmid ((\ell + 1)^2 - a_\ell(E_q)^2)$.

For $\kappa \in \mathbb{F}_\ell$, $\kappa \notin \{0, 1\}$ set

$$E(\kappa) \ : \ Y^2 = X(X - 1)(X - \kappa).$$

Let g be a primitive root for ℓ (i.e. a generator for $\mathbb{F}_\ell^*$) and let $h = g^n$. Define $\mathcal{X}_\ell \subset \mathbb{F}_\ell^*$ via

$$\mathcal{X}_\ell = \{h^r/4 \ : \ 0 \leq r \leq t - 1 \text{ and } h^r \not\equiv 4 \pmod{\ell}\}$$

and

$$\mathcal{Y}_\ell = \left\{ (\kappa - 1) \cdot (\mathbb{F}_\ell^*)^n \ : \ \kappa \in \mathcal{X}_\ell \ \text{ and } \ a_\ell(E(\kappa))^2 \equiv a_\ell(E_q)^2 \pmod{n} \right\} \ \subset \ \mathbb{F}_\ell^*/(\mathbb{F}_\ell^*)^n.$$

Define further

$$\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{F}_\ell^*/(\mathbb{F}_\ell^*)^n \quad \text{via} \quad \phi(s) = q^s \cdot (\mathbb{F}_\ell^*)^n.$$

Finally, let

$$\mathcal{Z}_\ell = \left\{ s \in \phi^{-1}(\mathcal{Y}_\ell) \ : \ \left(\frac{(24 - 6m)s}{n} \right) = 1 \right\},$$

where $q = 2^m \pm 1$; thus $m = 5$, 7 and 8 for $q = 31$, 127 and 257, respectively. We note that $n \nmid (m - 4)$ in all cases, so that (45) holds.

Lemma 10.1. *Let $q \in \{31, 127, 257\}$ and $n \geq 7$, $n \neq q$ be prime. Let $\ell_1, \ldots, \ell_t$ be primes $\neq q$ satisfying (i) and (ii) above, and also*

$$(60) \qquad \bigcap_{i=1}^{t} \mathcal{Z}_{\ell_i} \;=\; \emptyset.$$

Then equation (7) has no solutions with $k \geq 1$ and $q \nmid x$.

Proof. From Proposition 8.3, $\bar{\rho}_{F,n} \sim \bar{\rho}_{E_q,n}$. The minimal discriminant and conductor of F are given in (42). Thus a prime $\ell \nmid 2q$ satisfies $\ell \,||\, N_F$ if and only if $\ell \mid y_1 y_2$, otherwise $\ell \nmid N_F$. Let $\ell \neq q$ be a prime satisfying (i) and (ii). By (ii) we know, thanks to Lemma 7.1, that $\ell \nmid y_1 y_2$, and so $a_\ell(F) \equiv a_\ell(E_q) \pmod{n}$. Let $\kappa \in \mathbb{F}_\ell$ satisfy

$$\kappa \equiv 2^{n-2} y_2^n / y_1^n \pmod{\ell}.$$

Then $E(\kappa)/\mathbb{F}_\ell$ is a quadratic twist of $F/\mathbb{F}_\ell$ and so $a_\ell(E(\kappa)) = \pm a_\ell(F)$. We conclude that $a_\ell(E(\kappa))^2 \equiv a_\ell(E_q)^2 \pmod{n}$.

Recall that $\ell = tn + 1$ and $h = g^n$, where g is a primitive root of $\mathbb{F}_\ell$. Observe that

$$4\kappa \equiv 2^n y_2^n / y_1^n \equiv h^r \pmod{\ell},$$

for some $0 \leq r \leq t - 1$. Moreover,

$$\kappa - 1 \;\equiv\; \frac{2^{n-2} y_2^n}{y_1^n} - 1 \;\equiv\; -\frac{q^k}{y_1^n} \not\equiv 0 \pmod{\ell}.$$

In particular, $\kappa \neq 1$ and so $\kappa \in \mathcal{X}_\ell$ and $q^k \cdot (\mathbb{F}_\ell^*)^n = (\kappa - 1) \cdot (\mathbb{F}_\ell^*)^n \in \mathcal{Y}_\ell$. Hence $s \in \phi^{-1}(\mathcal{Y}_\ell)$, where $s = \bar{k} \in \mathbb{Z}/n\mathbb{Z}$. Since k also satisfies (45), we conclude that $s \in \mathcal{Z}_\ell$. As this is true for $\ell = \ell_1, \ldots, \ell_t$, the element s belongs to the intersection (60) giving a contradiction. $\qquad\square$

Corollary 10.2. *For $q \in \{31, 127, 257\}$ and prime n with $7 \leq n < 1.5 \times 10^6$, equation (7) has no solutions with $k \geq 1$ and $q \nmid x$.*

Proof. For $n \neq q$, we ran a short `Magma` script that searches for suitable primes ℓ_i and verifies the criterion of Lemma 10.1. This succeeded for all the primes $7 \leq n < 1.5 \times 10^6$ in a few minutes, except for $(q, n) = (31, 7)$. In this case, we found that $\cap \mathcal{Z}_{\ell_i} = \{\bar{1}\}$ no matter how many primes ℓ_i we chose. The reason for this is that there is a solution to equation (36) with $n = 7$ and $k = 1$, namely $(-1)^7 - 2^5 \cdot (-1)^7 = 31^1$.

In case $n = q$, we are unable to appeal directly to Lemma 10.1 as we no longer necessarily have (45). We can however, still derive a slightly weaker analogue of Lemma 10.1 with the $\mathcal{Z}_\ell$ replaced by the (typically) larger sets

$$\mathcal{Z}'_\ell = \phi^{-1}\left(\mathcal{Y}_\ell\right).$$

For $n = q$, we find that

$$\mathcal{Z}'_{311} \cap \mathcal{Z}'_{373} = \emptyset, \quad \mathcal{Z}'_{509} \cap \mathcal{Z}'_{2287} = \emptyset \quad \text{and} \quad \mathcal{Z}'_{1543} = \emptyset,$$

for $q = 31, 127$ and 257, respectively. $\qquad\square$

To complete the proof of Theorem 5, it remains only to solve the Thue–Mahler equation

$$y_1^7 - 32 y_2^7 = 31^k.$$

Using the Magma implementation of [20], we find that the only solution with k positive is with $k = 1$ and $y_1 = y_2 = -1$, corresponding to the solution $(q, k, y, n) = (31, 1, 2, 7)$ to equation (7).

11. THE EQUATION $x^2 + q^{2k+1} = y^n$ WITH y ODD

In previous sections, we have completed the proofs of Theorems 4 and 5, therefore solving equation (8) with $3 \leq q < 1000$ prime, for even exponents α. The remainder of the paper is devoted to solving (8) for odd exponents α, and for the more modest range $3 \leq q < 100$. In this section, we focus on the equation

(61) $$x^2 + q^{2k+1} = y^n, \qquad x, \, y, \, k \text{ integers}, \quad k \geq 0, \quad \gcd(x, y) = 1, \quad y \text{ odd},$$

with exponent $n \geq 5$ prime; here $q \geq 3$ is prime.

Theorem 12 (Arif and Abu Muriefah). *Suppose $q \geq 3$ and $n \geq 5$ are prime, and that n does not divide the class number of $\mathbb{Q}(\sqrt{-q})$. Then the only solution to* (61) *corresponds to the identity*

(62) $$22434^2 + 19 = 55^5.$$

Proof. The proof given by Arif and Abu Muriefah [1] is somewhat lengthy and slightly incorrect. For the convenience of the reader we give a corrected and simplified proof. Let $M = \mathbb{Q}(\sqrt{-q})$ and suppose that n does not divide the class number of M. This and the assumptions in (61) quickly lead us to conclude that

$$x + q^k \sqrt{-q} = \alpha^n$$

for some $\alpha \in \mathcal{O}_M$ with $\text{Norm}(\alpha) = y$. Thus

(63) $$\alpha^n - \overline{\alpha}^n = 2q^k \sqrt{-q}.$$

If $\alpha/\overline{\alpha}$ is a root of unity, then by the coprimality of α and $\overline{\alpha}$, we can conclude that α is a unit and so $y = 1$ giving a contradiction. Thus $\alpha/\overline{\alpha}$ is not a root of unity. Therefore

$$u_m = \frac{\alpha^m - \overline{\alpha}^m}{\alpha - \overline{\alpha}}$$

is a Lucas sequence. Since $\alpha\overline{\alpha} = y$, we note that $\alpha\overline{\alpha}$ is coprime to $2q$. Suppose that the term u_n has a primitive divisor ℓ. By definition, this is a prime ℓ dividing u_n that does not divide $(\alpha - \overline{\alpha})^2 \cdot u_1 u_2 \cdots u_{n-1}$. However $\alpha = u + v\sqrt{-q}$ or $\alpha = (u + v\sqrt{-q})/2$ where $u, \, v \in \mathbb{Z}$. Thus $(\alpha - \overline{\alpha})^2 = -4q$ or $-q$ respectively. In particular $\ell \neq q$. It follows from (26) that $\ell = 2$. By Theorem 7 and the primality of n, we have $n = m_2$, the rank of apparition of $\ell = 2$ in the sequence u_n. Again by Theorem 7, $n = m_2 = 2$ or 3 contradicting our assumption that $n \geq 5$. It follows that u_n does not have a primitive divisor.

We now invoke the Primitive Divisor Theorem (Theorem 6) to conclude that $n = 5$ or 7 and that $(\alpha, \overline{\alpha})$ is equivalent to $((a - \sqrt{b})/2, (a + \sqrt{b})/2)$ where possibilities for (a, b) are given by (24) if $n = 5$, and by (23) if $n = 7$. For illustration, we take $n = 5$ and $(a, b) = (12, -76)$. Thus $\alpha = (\pm 12 \pm \sqrt{-76})/2 = \pm 6 \pm \sqrt{-19}$, whence $q = 19$ and $y = \text{Norm}(\alpha) = 55$, quickly giving the solution in (62). The other possibilities for (a, b) in (23) and (24) do not yield solutions to (61). $\square$

Corollary 11.1. *The only solutions to* (61) *with $3 \leq q < 100$ and $n \geq 5$ prime correspond to the identities*

$$22434^2 + 19 = 55^5, \quad 14^2 + 47 = 3^5 \quad and \quad 46^2 + 71 = 3^7.$$

Proof. Write h_q for the class number of $M = \mathbb{Q}(\sqrt{-q})$. Thanks to Theorem 12, if $n \nmid h_q$ then the only corresponding solution is $22434^2 + 19 = 55^5$. Thus we may suppose that $n \mid h_q$. The only values of q in our range with h_q divisible by a prime ≥ 5 are $q = 47$, 71 and 79, where $h_q = 5$, 7 and 5, respectively. We therefore reduce to considering the three cases $(q, n) = (47, 5)$, $(71, 7)$ and $(79, 5)$, with $h_q = n$ in all three cases. From (61), we have

$$(x + q^k \sqrt{q}) \cdot \mathcal{O}_M = \mathfrak{A}^n.$$

If $\mathfrak{A}$ is principal, then we are in the situation of the proof of Theorem 12 and we obtain a contradiction. Thus $\mathcal{A}$ is not principal. Now for the three quadratic fields under consideration the class group is generated by the class $[\mathfrak{P}]$ where

$$\mathfrak{P} \ = \ 2 \cdot \mathcal{O}_M + \frac{(1 + \sqrt{-q})}{2} \cdot \mathcal{O}_M$$

is one of the two prime ideals dividing 2. We conclude that $[\mathfrak{A}] = [\mathfrak{P}]^{-r}$ for some $1 \le r \le n - 1$. Observe that $\mathfrak{C}\overline{\mathfrak{C}}$ is principal for any ideal $\mathfrak{C}$ of $\mathcal{O}_M$, so $[\overline{\mathfrak{C}}] = [\mathfrak{C}]^{-1}$. We choose $\mathfrak{B} = \mathfrak{A}$ or $\overline{\mathfrak{A}}$ so that $[\mathfrak{B}] = [\mathfrak{P}]^{-r}$ where $1 \le r \le (n-1)/2$. We note that

$$(x \pm q^k \sqrt{-q}) \cdot \mathcal{O}_M \ = \ \mathfrak{B}^n \ = \ (\mathfrak{P}^{-n})^r \cdot (\mathfrak{P}^r \mathfrak{B})^n$$

where the $\pm$ sign is $+$ if $\mathfrak{B} = \mathfrak{A}$ and $-$ is $\mathfrak{B} = \overline{\mathfrak{A}}$. We note that both $\mathfrak{P}^{-n}$ and $\mathfrak{P}^r \mathfrak{B}$ are principal. We find that $\mathfrak{P}^{-n} = 2^{-n-1}(u + v\sqrt{-q}) \cdot \mathcal{O}_M$ where u, v are

$$(u, v) = \begin{cases} (-9, 1) & \text{if } q = 47, \\ (-21, 1) & \text{if } q = 71, \\ (7, 1) & \text{if } q = 79. \end{cases}$$

The ideal $\mathfrak{P}^r \mathfrak{B}$ is integral as well as principal, and so has the form $(X' + Y'\sqrt{-q}) \cdot \mathcal{O}_M$ where X' and Y' are either both integers, or both halves of odd integers. We conclude that

$$2^{s+rn+r}(x \pm q^k \sqrt{-q}) \ = \ (u + v\sqrt{-q})^r \cdot (X + Y\sqrt{-q})^n$$

where $X, Y \in \mathbb{Z}$ and $s = 0$ or n. Equating imaginary parts gives

$$G_r(X, Y) = \pm 2^{s+rn+r} q^k$$

where $G_r \in \mathbb{Z}[X, Y]$ is a homogeneous polynomial of degree n. We solved this Thue–Mahler equation using the Thue–Mahler solver associated to the paper [20], for each of our three pairs (q, n) and each $0 \le r \le (n-1)/2$. For illustration, we consider the case $q = 47$, $n = 5$, $r = 2$. Thus $(u, v) = (-9, 1)$. We find

$$G_2(X, Y) = 2(-9X^5 + 85X^4Y + 4230X^3Y^2 - 7990X^2Y^3 - 99405XY^4 + 37553Y^5)$$

and are therefore led to solve the Thue–Mahler equation

$$-9X^5 + 85X^4Y + 4230X^3Y^2 - 7990X^2Y^3 - 99405XY^4 + 37553Y^5 \ = \ \pm 2^j q^k.$$

We find that the solutions are

$$(X, Y, j, k) \ = \ (1, 1, 16, 0) \quad \text{and} \quad (-1, -1, 16, 0),$$

and compute $G_2(1, 1) = -2^{17}$, $G_2(-1, -1) = 2^{17}$. We note that $17 = n + rn + r$, therefore $s = n = 5$. We deduce that

$$x \pm 47^k \sqrt{-47} = \pm(-9 + \sqrt{-47})^2 \cdot (1 + \sqrt{-47})^5 = \pm(14 - \sqrt{-47}).$$

Thus $x = \pm 14$ and $k = 0$, giving the solution $14^2 + 47 = 3^5$. The other cases are similar. $\qquad \square$

12. The equation $x^2 + (-1)^\delta q^{2k+1} = y^5$

We will soon apply Frey–Hellegouarch curves to study the equation $x^2 + (-1)^\delta q^{2k+1} = y^n$ for prime exponents $n \ge 7$, and for q a prime in the range $3 \le q < 100$. In Section 2, we have solved this equation for $n \in \{3, 4\}$. This leaves only exponent $n = 5$ which we now treat through reduction to Thue–Mahler equations.

Lemma 12.1. *Let $3 \leq q < 100$ be a prime. The only solutions to the equation*

$$x^2 - q^{2k+1} = y^5, \qquad x, \ y, \ k \ \text{integers}, \quad k \geq 0, \quad \gcd(x,y) = 1,$$

correspond to the identities

$$2^2 - 3 = 1^5, \quad 2^2 - 5 = (-1)^5, \quad 10^2 - 7^3 = (-3)^5, \quad 56^2 - 11 = 5^5, \quad 16^2 - 13 = 3^5,$$
$$4^2 - 17 = (-1)^5, \quad 7^2 - 17 = 2^5, \quad 6^2 - 37 = (-1)^5, \quad 3788^2 - 37 = (27)^5,$$
$$3^2 - 41 = (-2)^5, \quad 411^2 - 41^3 = 10^5 \ \text{and} \ 11^2 - 89 = 2^5.$$

Proof. Let $M = \mathbb{Q}(\sqrt{q})$. For q in our range, the class number of M is 1, unless $q = 79$ in which case the class number is 3. Suppose first that y is odd. Then

$$(x + q^k \sqrt{q})\mathcal{O}_M = \mathfrak{A}^5$$

where $\mathfrak{A}$ is an ideal of $\mathcal{O}_M$. Since the class number is not divisible by 5, we see that $\mathfrak{A}$ is principal and conclude that

(64) $$x + q^k \sqrt{q} = \epsilon^r \cdot \alpha^5,$$

where ϵ is some fixed choice of a fundamental unit for M, $-2 \leq r \leq 2$, and $\alpha \in \mathcal{O}_M$. Note that

$$-x + q^k \sqrt{q} = \epsilon^{-r} \cdot \beta^5,$$

where β is one of $\pm\bar{\alpha}$. Thus we may without loss of generality suppose that $0 \leq r \leq 2$. The case $r = 0$ is easily shown not to lead to any solutions by following the approach in the proof of Theorem 12. Thus we suppose $r = 1$ or 2.

Let

$$\theta = \begin{cases} \sqrt{q} & \text{if } q \equiv 3 \pmod 4 \\ (1 + \sqrt{q})/2 & \text{if } q \equiv 1 \pmod 4. \end{cases}$$

Then $\{1, \theta\}$ is a $\mathbb{Z}$-basis for $\mathcal{O}_M$ and so we may write $\alpha = X + Y\theta$ where $X, Y \in \mathbb{Z}$. It follows that

$$\epsilon^r \cdot \alpha^5 = F_r(X, Y) + G_r(X, Y)\theta,$$

where F_r, G_r are homogeneous degree 5 polynomials in $\mathbb{Z}[X, Y]$. Equating the coefficients of θ in (64) yields the Thue–Mahler equations

$$G_r(X, Y) = \begin{cases} q^k & \text{if } q \equiv 3 \pmod 4 \\ 2q^k & \text{if } q \equiv 1 \pmod 4. \end{cases}$$

Solving these equations for prime $3 \leq q < 100$ and for $r \in \{1, 2\}$ leads to the solutions given in the statement of the theorem with y odd.

Next we consider the case when y is even, so that $q \equiv 1 \pmod 8$. The possible values of q in our range are 17, 41, 73, 89 and 97 (where, in each case, M has class number 1). We can rewrite the equation $x^2 - q^{2k+1} = y^5$ as

$$\left(\frac{x + q^k \sqrt{q}}{2} \right) \left(\frac{x - q^k \sqrt{q}}{2} \right) = 2^3 y_1^5$$

where $y_1 = y/2$. The two factors on the left-hand side are coprime. Let β be a generator of

$$\mathfrak{P} = 2\mathcal{O}_M + \left(\frac{1 + \sqrt{q}}{2} \right) \cdot \mathcal{O}_M$$

which is one of the two prime ideals above 2. After possibly replacing x by $-x$ we obtain

$$\frac{x - q^k}{2} + q^k \theta = \frac{x + q^k \sqrt{q}}{2} = \epsilon^r \beta \alpha^5$$

where $-2 \leq r \leq 2$. Writing $\alpha = X + Y\theta$ and equating the coefficients of θ on both sides gives, for each choice of q and r, a Thue–Mahler equation. Solving these leads to the solutions in the statement of the theorem with y even. □

Lemma 12.2. *Let $3 \leq q < 100$ be a prime. The only solutions to the equation*

$$x^2 + q^{2k+1} = y^5, \qquad x, \ y, \ k \ integers, \quad k \geq 0, \quad \gcd(x, y) = 1,$$

correspond to the identities

$$5^2 + 7 = 2^5, \qquad 181^2 + 7 = 8^5, \qquad 22434^2 + 19 = 55^5,$$
$$3^2 + 23 = 2^5, \qquad 1^2 + 31 = 2^5 \quad and \quad 14^2 + 47 = 3^5.$$

Proof. By Corollary 11.1 we know that the only solutions when y is odd correspond to the identities $22434^2 + 19 = 55^5$ and $14^2 + 47 = 3^5$. Thus we may suppose y is even, and write $y = 2y_1$. It follows that $q = 7, 23, 31, 47, 71, 79$. Let $M = \mathbb{Q}(\sqrt{-q})$. Let $\theta = (1 + \sqrt{-q})/2$, so that $1, \theta$ is a $\mathbb{Z}$-basis for $\mathcal{O}_M$. Observe that

$$\left(\frac{x + q^k \sqrt{-q}}{2} \right) \left(\frac{x - q^k \sqrt{-q}}{2} \right) = 2^3 y_1^5,$$

where the two factors on the left hand-side generate coprime ideals. Let

$$\mathfrak{P} = 2\mathcal{O}_M + \theta \cdot \mathcal{O}_M;$$

this is one of the two primes above 2. Thus, after possibly changing the sign of x,

$$\left(\frac{x + q^k \sqrt{-q}}{2} \right) \cdot \mathcal{O}_M = \mathfrak{P}^3 \cdot \mathfrak{A}^5$$

for some ideal $\mathfrak{A}$ of $\mathcal{O}_M$. The class number of $\mathcal{O}_M$ is $1, 3, 3, 5, 7, 5$ according to whether $q = 7$, $23, 31, 47, 71, 79$. In all cases the class group is cyclic and generated by $[\mathfrak{P}]$. If $q = 47$ or 79 then the class number is 5, and so $\mathfrak{A}^5$ is principal. Hence $\mathfrak{P}^3$ is principal which is a contradiction. Thus there are no solutions for $q = 47$ or 79. Let

$$\mathfrak{C} = \begin{cases} 1 \cdot \mathcal{O}_M & q = 7, 23, 31 \\ \mathfrak{P}^2 & q = 71. \end{cases}$$

Note that $\mathfrak{P}^3 \mathfrak{C}^{-5}$ is principal and we write $\mathfrak{P}^3 \mathfrak{C}^{-5} = (u + v\theta) \cdot \mathcal{O}_M$. Thus

$$\left(\frac{x + q^k \sqrt{-q}}{2} \right) \cdot \mathcal{O}_M = (u + v\theta) \cdot (\mathfrak{C}\mathfrak{A})^5.$$

As the class number is coprime to 5, we see that $\mathfrak{C}\mathfrak{A}$ is principal. Write $\mathfrak{C}\mathfrak{A} = (X + Y\theta) \cdot \mathcal{O}_K$. After possibly changing the signs of X, Y, we have

$$\frac{x - q^k}{2} + q^k \theta = \frac{x + q^k \sqrt{-q}}{2} = (u + v\theta)(X + Y\theta)^5.$$

Comparing the coefficients of θ yields a degree 5 Thue–Mahler equation. Solving these Thue–Mahler equations as before gives the claimed solutions with y even. □

13. Frey–Hellegouarch curves for a ternary equation of signature $(n, n, 2)$

In studying equation (7), we employed a factorisation argument which reduced to (36) (which in turn we treated as a special case of a Fermat equation having signature (n, n, n)). In the remainder of the paper, we are primarily interested in the equation $x^2 + (-1)^\delta q^{2k+1} = y^n$, where q is a prime. We shall treat this, for prime $n \geq 7$, as a Fermat equation of signature $(n, n, 2)$ by rewriting this as $y^n + q^{2k+1}(-1)^{(\delta+1)n} = x^2$, a special case of

$$(65) \qquad\qquad y^n + q^\alpha z^n = x^2, \qquad\qquad \gcd(x, y) = 1.$$

Equation (65) has previously been studied by Ivorra and Kraus [23], and by the first author and Skinner [7]. In this section, we recall some of these results and strengthen them slightly before specialising them to the case $z = \pm 1$ in forthcoming sections.

Theorem 13 (Ivorra and Kraus). *Suppose that q is a prime with the property that q cannot be written in the form*

$$q = |t^2 \pm 2^k|,$$

where t and k are integers, with $k = 0$, $k = 3$ or $k \geq 7$. Then there are no solutions to the Diophantine equation (65) in integers x, y, z, n and α with n prime satisfying

$$(66) \qquad n > \left(\sqrt{8(q+1)} + 1 \right)^{2(q-1)}.$$

To verify whether or not a given prime q can be written as $|t^2 - 2^k|$, an old result of Bauer and the first author [3] can be helpful. We have, from Corollary 1.7 of [3], if t and k are positive integers with $k \geq 3$ odd,

$$\left| t^2 - 2^k \right| > 2^{13k/50},$$

unless

$$(t, k) \in \{(3, 3), (181, 15)\}.$$

In particular, a short computation reveals that Theorem 13 is applicable to the following primes $q < 100$:

$$(67) \qquad q \in \{11, 13, 19, 29, 43, 53, 59, 61, 67, 83\}.$$

We shall make Theorem 13 more precise for these particular values of q. To this end we attach to a solution of (65) a certain Frey–Hellegouarch curve, following the recipes of the first author and Skinner. If yz is even in (65), then we define, assuming, without loss of generality, that $x \equiv 1 \pmod 4$,

$$(68) \qquad F \;:\; Y^2 + XY = X^3 + \left(\frac{x-1}{4} \right) X^2 + \frac{y^n}{64} X, \quad \text{if } y \text{ is even,}$$

and

$$F \;:\; Y^2 + XY = X^3 + \left(\frac{x-1}{4} \right) X^2 + \frac{q^\alpha z^n}{64} X, \quad \text{if } z \text{ is even.}$$

If, on the other hand, yz is odd, we define

$$(69) \qquad F \;:\; Y^2 = X^3 + 2x X^2 + q^\alpha z^n X$$

or

$$(70) \qquad F \;:\; Y^2 = X^3 + 2x X^2 + y^n X,$$

depending on whether $y \equiv 1 \pmod 4$ or $y \equiv -1 \pmod 4$, respectively. Let

$$(71) \qquad \kappa = \begin{cases} 1 & \text{if } yz \text{ is even} \\ 5 & \text{if } yz \text{ is odd.} \end{cases}$$

By the results of [7], in each case, we may suppose that $n \nmid \alpha$ and that the mod n representation of F arises from a newform f of weight 2 and level $N = 2^\kappa \cdot q$. Let the $\mathfrak{q}$-expansion of f be given by (37). As before, we denote the Hecke eigenfield by $K_f = \mathbb{Q}(c_1, c_2, \dots)$ and its ring of integers by $\mathcal{O}_f$. In particular, there is a prime ideal $\mathfrak{n}$ of $\mathcal{O}_f$ such that (38) holds. Let $\ell \nmid 2q$ be prime and

$$T = \{a \in \mathbb{Z} \cap [-2\sqrt{\ell}, 2\sqrt{\ell}] \;:\; a \equiv 0 \pmod 2\}.$$

We write

$$\mathcal{D}'_{f, \ell} = ((\ell + 1)^2 - c_\ell^2) \cdot \prod_{a \in T} (a - c_\ell),$$

and

$$\mathcal{D}_{f,\ell} = \begin{cases} \ell \cdot \mathcal{D}'_{f,\ell} & \text{if } K_f \neq \mathbb{Q} \\ \mathcal{D}'_{f,\ell} & \text{if } K_f = \mathbb{Q}. \end{cases}$$

Lemma 13.1. *Let f be a newform of weight 2 and level $N = 2^\kappa \cdot q$. Let $\ell \nmid 2q$ be a prime. If $\overline{\rho}_{F,n} \sim \overline{\rho}_{f,\mathfrak{n}}$ then $\mathfrak{n} \mid \mathcal{D}_{f,\ell}$.*

Proof. The proof is almost identical to the proof of Lemma 8.2. The only difference is the definition of T which takes into account the fact F has a single rational point of order 2 instead of full 2-torsion. $\qquad\square$

The following is a slight refinement of Theorem 1.3 of [7].

Proposition 13.2. *Suppose that q belongs to (67). Then there are no solutions to equation (65) in integers x, y, z, n and α with $\gcd(x, y) = 1$ and $n \geq 7$ prime, unless, possibly, $n = 7$ and $q \in \{29, 43, 53, 59, 61\}$, or one of the following holds*

$$q = 11, \; n = 7 \; \text{and} \; yz \equiv 1 \;(\text{mod } 2), \; \text{or}$$
$$q = 19, \; n = 7 \; \text{and} \; yz \equiv 1 \;(\text{mod } 2), \; \text{or}$$
$$q = 43, \; n = 11 \; \text{and} \; yz \equiv 1 \;(\text{mod } 2), \; \text{or}$$
$$q = 53, \; n = 17 \; \text{and} \; yz \equiv 1 \;(\text{mod } 2), \; \text{or}$$
$$q = 59, \; n = 11 \; \text{and} \; yz \equiv 0 \;(\text{mod } 2), \; \text{or}$$
$$q = 61, \; n = 13 \; \text{and} \; yz \equiv 1 \;(\text{mod } 2), \; \text{or}$$
$$q = 67, \; n \in \{7, 11, 13, 17\} \; \text{and} \; yz \equiv 1 \;(\text{mod } 2), \; \text{or}$$
$$q = 83, \; n = 7 \; \text{and} \; yz \equiv 1 \;(\text{mod } 2).$$

Proof. For a weight 2 newform f of level N and primes $\ell_1, \ldots, \ell_m$ (all coprime to $2q$), write $\mathcal{D}_{f,\ell_1,\ldots,\ell_m}$ for the ideal of $\mathcal{O}_f$ generated by $\mathcal{D}_{f,\ell_1}, \ldots, \mathcal{D}_{f,\ell_m}$. Let $\mathcal{B}_{f,\ell_1,\ldots,\ell_m} \in \mathbb{Z}$ be the norm of the ideal $\mathcal{D}_{f,\ell_1,\ldots,\ell_m}$. If $\overline{\rho}_{F,n} \sim \overline{\rho}_{f,\mathfrak{n}}$ then $\mathfrak{n} \mid \mathcal{D}_{f,\ell_1,\ldots,\ell_m}$ by Lemma 13.1. Write $\mathcal{B}_{f,\ell_1,\ldots,\ell_m} = \text{Norm}(\mathcal{D}_{f,\ell_1,\ldots,\ell_m})$. Thus $n \mid \mathcal{B}_{f,\ell_1,\ldots,\ell_m}$. In our computations, we take $\ell_1, \ldots, \ell_m$ to be the primes < 100 coprime to $2q$, and we let $\mathcal{B}_f = \mathcal{B}_{f,\ell_1,\ldots,\ell_m}$. If $\mathcal{B}_f \neq 0$, then we certainly have a bound on n. If $\mathcal{B}_f$ is divisible only by primes ≤ 5, then we know that (38) does not hold for that particular f, and we can eliminate it from further consideration.

For primes q in (67), we apply this with newforms f of levels $N = 2^\kappa q$, $\kappa \in \{1, 5\}$. We obtain the desired conclusion that equation (65) has no solutions provided $n \geq 7$ is prime, unless $q \in \{29, 43, 53, 59, 61\}$ and $n = 7$, or (q, n, κ) is one of

$(11, 7, 5), \; (13, 7, 1), \; (19, 7, 5), \; (43, 11, 1), \; (43, 11, 5), \; (53, 17, 5), \; (59, 11, 1), \; (61, 31, 1),$
$(61, 13, 5), \; (67, 17, 1), \; (67, 7, 5), \; (67, 11, 5), \; (67, 13, 5), \; (67, 17, 5), \; (83, 7, 1), \; (83, 7, 5).$

We show that the triples $(13, 7, 1)$, $(43, 11, 1)$, $(61, 31, 1)$, $(67, 17, 1)$ and $(83, 7, 1)$ do not have corresponding solutions; the remaining triples lead to the noted possible exceptions. For illustration, take $q = 83$ and $\kappa = 1$, so that $N = 2 \times 83 = 166$. There are three conjugacy classes of weight 2 newforms of level N, which we denote by f_1, f_2, f_3, which respectively have Hecke eigenfields $\mathbb{Q}$, $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\theta)$ where $\theta^3 - \theta^2 - 6\theta + 4 = 0$. We find

$$\mathcal{B}_{f_1} = 3^2 \times 5, \qquad \mathcal{B}_{f_2} = 5, \qquad \mathcal{B}_{f_3} = 7.$$

We therefore reduce that $f = f_3$ and $n = 7$. In fact, $\mathcal{D}_f = (7, 3 + \theta)$ is a prime ideal above 7, so we take $\mathfrak{n} = (7, 3 + \theta)$. A short calculation verifies the congruences in hypotheses (i) and (ii) of Theorem 8, whence $\ell + 1 \equiv c_\ell \;(\text{mod } \mathfrak{n})$ for all ℓ with $\ell \nmid 2 \cdot 83$. It follows from Lemma 7.1 that

$$a_\ell(F) \equiv c_\ell \;(\text{mod } \mathfrak{n})$$

for all primes ℓ of good reduction for F and hence $7 \mid (\ell + 1 - a_\ell(F))$ for all such primes ℓ of good reduction. This now implies that $\overline{\rho}_{F,7}$ is reducible [38, IV-6], giving a contradiction.

We argue similarly for

$$(q, n, \kappa) = (13, 7, 1), \ (43, 11, 1), \ (61, 31, 1) \ \text{and} \ (67, 17, 1).$$

In each case, Lemma 13.1 eliminates all but one class of newforms which are in turn treated via Theorem 8. $\hfill\square$

For other odd primes $q < 100$, outside the set (67), we can, in certain cases, still show that equation (65) has no nontrivial solutions for suitably large n, under the additional assumption that $yz \equiv 0 \pmod{2}$ or, for other q, under the assumption that $yz \equiv 1 \pmod{2}$. To be precise, we have

Proposition 13.3. *Suppose that $q \in \{3, 5, 37, 73\}$. Then there are no solutions to equation (65) in integers x, y, z, n and α with $yz \equiv 0 \pmod{2}$, $\gcd(x, y) = 1$ and $n \geq 7$ prime, unless, possibly, $(q, n) = (73, 7)$.*

and

Proposition 13.4. *Suppose that $q \in \{23, 31, 47, 71, 79, 97\}$. Then there are no solutions to equation (65) in integers x, y, z, n and α with $yz \equiv 1 \pmod{2}$, $\gcd(x, y) = 1$ and $n \geq 7$ prime, unless, possibly, $n = 7$ and $q \in \{23, 31, 47, 71, 97\}$, or $(q, n) = (79, 11)$, or $(q, n) = (97, 29)$.*

As in the case of Proposition 13.2, these results follow after a small amount of computation, by applying Lemma 13.1 and Theorem 8.

14. The equation $x^2 \pm q^{2k+1} = y^n$ and proofs of Theorems 2 and 3

We now specialize and improve on the results of Section 13, proving the following.

Proposition 14.1. *Let (x, y, k) be a solution to the equation*

$$(72) \qquad x^2 + (-1)^\delta q^{2k+1} = y^n, \qquad \delta \in \{0, 1\}, \quad k \geq 0, \quad \gcd(x, y) = 1$$

where q is a prime in the range $3 \leq q < 100$, and $n \geq 7$ is prime. Suppose moreover that

  (a) if y is odd then $\delta = 1$;
  (b) if $\delta = 1$ then $q \notin \{3, 5, 17, 37\}$.

If y is even, suppose without loss of generality that $x \equiv 1 \pmod{4}$. Write

$$(73) \qquad\qquad\qquad\qquad \kappa = \begin{cases} 1 & \text{if } y \text{ is even} \\ 5 & \text{if } y \text{ is odd.} \end{cases}$$

Let $v \in \{0, 1\}$ satisfy $k \equiv v \pmod{2}$. Attach to the solution (x, y, k) the Frey–Hellegouarch curve

$$G = G_{x,k} : \begin{cases} Y^2 = X^3 + 4xX^2 + 4(x^2 + (-1)^\delta q^{2k+1})X & \text{if } \kappa = 1, \\ Y^2 = X^3 - 4xX^2 + 4(x^2 + (-1)^\delta q^{2k+1})X & \text{if } \kappa = 5 \text{ and } q \equiv (-1)^\delta \bmod 4, \\ Y^2 = X^3 + 2xX^2 + (x^2 + (-1)^\delta q^{2k+1})X & \text{if } \kappa = 5 \text{ and } q \equiv (-1)^{\delta+1} \bmod 4. \end{cases}$$

Then either $n > 1000$ and $\overline{\rho}_{G,n} \sim \overline{\rho}_{E,n}$ where $E/\mathbb{Q}$ is an elliptic curve of conductor $2^\kappa q$ given in Table 3 or the solution (x, y, k) corresponds to one of the identities

$$11^2 + 7 = 2^7, \ 45^2 + 23 = 2^{11}, \ 13^2 - 41 = 2^7, \ 9^2 + 47 = 2^7,$$

$$7^2 + 79 = 2^7, \ 91^2 - 89 = 2^{13} \ \text{or} \ 15^2 - 97 = 2^7.$$

Before proceeding to the proof of this result, we make a few remarks on the assumptions in Proposition 14.1. Our eventual goal is to prove Theorems 1, 2 and 3, and thus we are interested in the equation $x^2 + (-1)^\delta q^\alpha = y^n$ where $3 \leq q < 100$. Theorems 4 and 5 (proved in Sections 5 and 10, respectively) treat the case where α is even, so we are reduced to $\alpha = 2k + 1$. The results of Sections 2, Corollary 11.1 and Lemmas 12.1, 12.2 allow us to restrict the exponent n to be a prime ≥ 7. Thanks to Theorem 12, we need not consider the case where $\delta = 0$ and y is odd,

TABLE 3. Data for Proposition 14.1. Here the elliptic curves E are given by their Cremona labels.

q	δ	κ	v	E		q	δ	κ	v	E
7	0	1	0	14a1		47	0	1	0	94a1
7	0	1	1	14a1		71	0	1	0	142c1
23	0	1	0	46a1		71	0	1	1	142c1
31	0	1	0	62a1		73	1	5	0	2336a1, 2336b1
31	0	1	1	62a1		73	1	5	1	2336a1, 2336b1
41	1	1	0	82a1		79	0	1	0	158e1
41	1	5	0	1312a1, 1312b1		89	1	1	0	178b1
41	1	5	1	1312a1, 1312b1		97	1	1	0	194a1

which explains the reason for assumption (a). With a view to proving the proposition, we will soon provide a method which is usually capable, for a fixed q, δ and n, of showing that (72) does not have a solution. If $\delta = 1$, and q is one of the values 3, 5, 17 or 37, then there is a solution to (72) for all odd values of the exponent n:

$$2^2 - 3 = 1^n, \quad 2^2 - 5 = (-1)^n, \quad 4^2 - 17 = (-1)^n \quad \text{and} \quad 6^2 - 37 = (-1)^n,$$

and so our method fails if $\delta = 1$ and q is one of these four values; this explains assumption (b) in the statement of the proposition.

We note that (72) is a special case of (65) with z specialised to the value $(-1)^{\delta+1}$, and with $\alpha = 2k+1$. The value κ in the statement of the proposition agrees with value for κ in (71) given in the previous section. We note that if y is odd, then $y \equiv (-1)^\delta \cdot q \pmod 4$. The Frey–Hellegouarch curve G is, up to isogeny, the same as the Frey–Hellegouarch curve F in the previous section, but is more convenient for our purposes. More precisely, the model G is isomorphic to F given in (68) if y even (i.e. $\kappa = 1$), and to F given in (70) if $y \equiv 3 \pmod 4$ (i.e. $\kappa = 5$ and $q \equiv (-1)^{\delta+1} \bmod 4$). It is 2-isogenous to F in (69) if $y \equiv 1 \pmod 4$ (i.e. $\kappa = 5$ and $q \equiv (-1)^\delta \bmod 4$). Thus $\overline{\rho}_{F,n} \sim \overline{\rho}_{G,n}$ in all three cases. We conclude from the previous section that $\overline{\rho}_{G,n} \sim \overline{\rho}_{f,\mathfrak{n}}$ where f is a weight 2 newform of level $N = 2^\kappa q$.

Note that if $\kappa = 1$ (i.e. y is even) then $1 + (-1)^\delta q \equiv 0 \pmod 8$. This together with the assumptions of Proposition 14.1 shows that we are concerned with 30 possibilities for the triple (q, δ, κ), namely

$$(74) \quad \begin{cases} (7,0,1), \ (7,1,5), \ (11,1,5), \ (13,1,5), \ (19,1,5), \ (23,0,1), \ (23,1,5), \ (29,1,5), \\ (31,0,1), \ (31,1,5), \ (41,1,1), \ (41,1,5), \ (43,1,5), \ (47,0,1), \ (47,1,5), \ (53,1,5), \\ (59,1,5), \ (61,1,5), \ (67,1,5), \ (71,0,1), \ (71,1,5), \ (73,1,1), \ (73,1,5), \ (79,0,1), \\ (79,1,5), \ (83,1,5), \ (89,1,1), \ (89,1,5), \ (97,1,1), \ (97,1,5). \end{cases}$$

Bounding the exponent n. In the previous section we defined an ideal $\mathcal{D}_{f,\ell_1,\dots,\ell_r}$ which if non-zero allows us to bound the exponent n in (65). That bound will also be valid for (72) since it is a special case of (65). We now offer a refinement that is often capable of yielding a better bound for (72).

Fix a triple (q, δ, κ) from the above list. We also fix $v \in \{0, 1\}$ and suppose that $k \equiv v \pmod 2$. Let f be a weight 2 newform of level $N = 2^\kappa q$ with $\mathfrak{q}$-expansion as in (37). Write K_f for the Hecke eigenfield of f, and $\mathcal{O}_f$ for the ring of integers of K_f. For a prime $\ell \neq 2, q$, define

$$\mathcal{S}_\ell = \{ a_\ell(G_{w,v}) \quad : \quad w \in \mathbb{F}_\ell, \quad w^2 + (-1)^\delta q^{2v+1} \not\equiv 0 \pmod \ell \}.$$

Let

$$\mathcal{T} = \mathcal{T}_\ell = \begin{cases} \mathcal{S}_\ell \cup \{\ell+1, -\ell-1\} & \text{if } (-1)^{\delta+1}q \text{ is a square modulo } \ell \\ \mathcal{S}_\ell & \text{otherwise.} \end{cases}$$

Let

$$\mathcal{E}'_\ell = \prod_{a \in \mathcal{T}} (a - c_\ell) \quad \text{and} \quad \mathcal{E}_\ell = \begin{cases} \ell \cdot \mathcal{E}'_\ell & \text{if } K_f \neq \mathbb{Q}, \\ \mathcal{E}'_\ell & \text{if } K_f = \mathbb{Q}, \end{cases}$$

where, as before, c_ℓ is the ℓ-th coefficient in the $\mathfrak{q}$-expansion of f.

Lemma 14.2. *Let $\mathfrak{n}$ be a prime ideal of $\mathcal{O}_f$ above n. If $\overline{\rho}_{G,n} \sim \overline{\rho}_{f,\mathfrak{n}}$ then $\mathfrak{n} \mid \mathcal{E}_\ell$.*

Proof. Write $k = 2u + v$ with $u \in \mathbb{Z}$. Let $w \in \mathbb{F}_\ell$ satisfy $w \equiv x/q^{2u} \pmod{\ell}$. Hence

$$y^n = x^2 + (-1)^\delta q^{2k+1} \equiv q^{4u} \cdot (w^2 + (-1)^\delta q^{2v+1}) \pmod{\ell}.$$

It follows that $\ell \mid y$ if and only if $w^2 + (-1)^\delta q^{2v+1} \pmod{\ell}$. Suppose first that $\ell \nmid y$. The elliptic curves $G_{x,k}/\mathbb{F}_\ell$ and $G_{w,v}/\mathbb{F}_\ell$ are isomorphic, and so $a_\ell(G_{x,k}) = a_\ell(G_{w,v})$. In particular, $a_\ell(G_{x,k}) \in \mathcal{T}_\ell$ and so $a_\ell(G_{x,k}) - c_\ell$ divides $\mathcal{E}_\ell$. Likewise, if $\ell \mid y$ (which can only happen if $(-1)^{\delta+1}q$ is a square modulo ℓ) then $(\ell+1)^2 - c_\ell^2$ divides $\mathcal{E}_\ell$. The lemma follows from Lemma 7.1. $\qquad\square$

A sieve. Lemma 14.2 will soon allow us to eliminate most possibilities for the newform f in a manner similar to Propositions 13.2, 13.3 and 13.4. We will still need to treat some cases for fixed exponent n. To this end, we will employ a sieving technique similar to the one in Section 10.

Fix a prime $n \geq 7$, and let $\mathfrak{n}$ be a prime ideal of $\mathcal{O}_f$ above n. Let $\ell \neq q$ be a prime. Suppose

(i) $\ell = tn + 1$ for some positive integer t;
(ii) either $\mathfrak{n} \nmid (4 - c_\ell^2)$, or $(-1)^{\delta+1}q$ is not a square modulo ℓ.

Let

$$A = \{m \in \{0, 1, \ldots, 2n-1\} \quad : \quad m \equiv v \pmod{2}, \quad n \nmid (2m+1)\},$$
$$\mathcal{X}_\ell = \{(z, m) \in \mathbb{F}_\ell \times A \ : \ (z^2 + (-1)^\delta q^{2m+1})^t \equiv 1 \pmod{\ell}\},$$
$$\mathcal{Y}_\ell = \{(z, m) \in \mathcal{X}_\ell \ : \ a_\ell(G_{z,m}) \equiv c_\ell \pmod{\mathfrak{n}}\},$$
$$\mathcal{Z}_\ell = \{m \ : \ \text{there exists } z \text{ such that } (z, m) \in \mathcal{Y}_\ell\}.$$

Lemma 14.3. *Let $\ell_1, \ldots, \ell_r$ be primes $\neq q$ satisfying (i), (ii). Let*

$$\mathcal{Z}_{\ell_1, \ldots, \ell_r} = \bigcap_{i=1}^r \mathcal{Z}_{\ell_i}.$$

If $\overline{\rho}_{G,n} \sim \overline{\rho}_{f,\mathfrak{n}}$ then

$$(k \bmod 2n) \in \mathcal{Z}_{\ell_1, \ldots, \ell_r}.$$

Proof. Let m be the unique element of $\{0, 1, \ldots, 2n-1\}$ satisfying $k \equiv m \pmod{2n}$. Let $\ell \neq q$ be a prime satisfying (i) and (ii). It is sufficient to show that $m \in \mathcal{Z}_\ell$. First we will demonstrate that $\ell \nmid y$. If $(-1)^{\delta+1}q$ is not a square modulo ℓ then $\ell \nmid y$ from (72). Otherwise, by (ii), $\mathfrak{n} \nmid (4 - c_\ell^2)$. However, from (i) and the fact that $\mathfrak{n} \mid n$ we have $\ell + 1 \equiv 2 \pmod{\mathfrak{n}}$ and so $\mathfrak{n} \nmid ((\ell+1)^2 - c_\ell^2)$. It follows from Lemma 7.1 that ℓ is a prime of good reduction for $G_{x,k}$ and so $\ell \nmid y$. We deduce from Lemma 7.1 that $a_\ell(G_{x,k}) \equiv c_\ell \pmod{\mathfrak{n}}$.

In the previous section, we observed that $n \nmid \alpha$ in equation 65 thanks to the results of [7], whence $n \nmid (2k+1)$. Since $k \equiv v \pmod{2}$, we know that $m \in A$. Write $k = 2nb + m$ with b a non-negative integer and let $z \in \mathbb{F}_\ell$ satisfy $z \equiv x/q^{2nb} \pmod{\ell}$. Then

$$z^2 + (-1)^\delta q^{2m+1} \equiv \frac{1}{q^{4nb}}(x^2 + (-1)^\delta q^{2k+1}) \equiv (y/q^{4b})^n \pmod{\ell}.$$

From (i), we deduce that

$$(z^2 + (-1)^\delta q^{2m+1})^t \equiv (y/q^{4b})^{\ell-1} \equiv 1 \pmod{\ell}.$$

Thus $(z, m) \in \mathcal{X}_\ell$. Moreover, we have that $G_{x,k}/\mathbb{F}_\ell$ and $G_{z,m}/\mathbb{F}_\ell$ are isomorphic elliptic curves, whence $a_\ell(G_{z,m}) = a_\ell(G_{x,k}) \equiv c_\ell \pmod{\mathfrak{n}}$. Thus $(z, m) \in \mathcal{Y}_\ell$ and so $m \in \mathcal{Z}_\ell$ as required. $\square$

Remarks. We would like to explain how to compute $\mathcal{Z}_\ell$ efficiently, given n and ℓ.

(1) In our computations, the value t will be relatively small compared to n and to $\ell = tn + 1$. Let g be a primitive root modulo ℓ (i.e. a cyclic generator for $\mathbb{F}_\ell^\times$), and let $h = g^n$. The set $\mathcal{X}_\ell$ consists of pairs $(z, m) \in \mathbb{F}_\ell \times A$ such that $(z^2 + (-1)^\delta q^m)^t \equiv 1 \pmod{\ell}$. Hence $z^2 + (-1)^\delta q^m$ is one of the values $1, h, h^2, \ldots, h^{(t-1)}$. Thus, to compute $\mathcal{X}_\ell$, we run through $i = 0, 1, \ldots, t - 1$ and $m \in A$ and solve $z^2 = h^i - (-1)^\delta q^m$. We note that the expected cardinality of $\mathcal{X}_\ell$ should be roughly $t \times \#A \approx t \times n \approx \ell$.

(2) It seems at first that, in order to compute $\mathcal{Y}_\ell$ and $\mathcal{Z}_\ell$, we need to compute $a_\ell(G_{z,m})$ for all $(z, m) \in \mathcal{X}_\ell$, and this might be an issue for large ℓ. There is in fact a shortcut that often means that we need to perform few of these computations. In fact we will need to compute $\mathcal{Z}_\ell$ for large values of ℓ only for rational newforms f that correspond to elliptic curves $E/\mathbb{Q}$ with non-trivial 2-torsion. In this case, we note that $a_\ell(G_{z,m}) \equiv a_\ell(E) \pmod 2$, as both elliptic curves have non-trivial 2-torsion. If $(z, m) \in \mathcal{Y}_\ell$, then $a_\ell(G_{z,m}) \equiv a_\ell(E) \pmod{2n}$. However, by the Hasse–Weil bounds,

$$|a_\ell(G_{z,m}) - a_\ell(E)| \leq 4\sqrt{\ell}.$$

Suppose moreover that $n^2 > 4\ell$ (which will be usually satisfied as t is typically small). Then, the congruence $a_\ell(G_{z,m}) \equiv c_\ell = a_\ell(E) \pmod{2n}$ is equivalent to the equality $a_\ell(G_{z,m}) = a_\ell(E)$, and so to $\#G_{z,m}(\mathbb{F}_\ell) = \#E(\mathbb{F}_\ell)$. To check whether the equality $\#G_{z,m}(\mathbb{F}_\ell) = \#E(\mathbb{F}_\ell)$ holds for a particular pair $(z, m) \in \mathcal{X}_\ell$, we first choose a random point $Q \in G_{z,m}(\mathbb{F}_\ell)$ and check whether $\#E(\mathbb{F}_\ell) \cdot Q = 0$. Only for pairs $(z, m) \in \mathcal{X}_\ell$ that pass this test do we need to compute $a_\ell(G_{z,m})$ and check the congruence $a_\ell(G_{z,m}) \equiv a_\ell(E) \pmod{n}$.

A refined sieve. We note that if $\mathcal{Z}_{\ell_1,\ldots,\ell_r} = \emptyset$ then $\overline{\rho}_{G,n} \nsim \overline{\rho}_{f,\mathfrak{n}}$. In our computations, described later, we are always able to find suitable primes $\ell_1, \ldots, \ell_r$ satisfying (i), (ii), so that $\mathcal{Z}_{\ell_1,\ldots,\ell_r} = \emptyset$, at least for n suitably large. For smaller values of n (say less than 50), we occasionally failed. We now describe a refined sieving method that, whilst being somewhat slow, has a better chance of succeeding for those smaller values of the exponent n.

Let (q, δ, κ) be one of our 30 triples given in (74), and let $n \geq 7$ be a prime. Suppose that (x, y, k) is a solution to (72) where y is even if and only if $\kappa = 1$. Let $\phi = \sqrt{(-1)^{\delta+1}q}$ and set $M = \mathbb{Q}(\phi)$. Let $\mathfrak{P}$ be one of the prime ideals of $\mathcal{O}_M$ above 2.

Our first goal is to produce a finite set $\mathcal{S} \subset M^*$, such that

(75) $$x + q^k\phi = \gamma \cdot \alpha^n$$

for some $\gamma \in \mathcal{S}$ and $\alpha \in \mathcal{O}_M$. This is the objective of Lemmata 14.4 and 14.5. Both of these make an additional assumption on the class group, but this assumption will in fact be satisfied in all cases where we need to apply our refined sieve.

Lemma 14.4. . *Let $\kappa = 5$. Suppose that the class group $\mathrm{Cl}(\mathcal{O}_M)$ of $\mathcal{O}_M$ is cyclic and generated by the class $[\mathfrak{P}]$. Let $h = \#\mathrm{Cl}(\mathcal{O}_M)$ and set*

$$\mathcal{I} = \{0 \leq i \leq h - 1 \ : \ \mathfrak{P}^{-ni} \text{ is principal}\}.$$

Choose for each $i \in \mathcal{I}$ a generator β_i for $\mathfrak{P}^{-ni}$. Let ϵ be a fundamental unit for M (recall that if $\kappa = 5$ then $\delta = 1$ and so M is real). Let

$$\mathcal{S} = \{\epsilon^j \beta_i \ : \ -(n-1)/2 \leq j \leq (n-1)/2, \ i \in \mathcal{I}\}.$$

Then there is some $\gamma \in \mathcal{S}$ and $\alpha \in \mathcal{O}_M$ such that (75) holds. Moreover, $\mathrm{Norm}(\alpha) = 2^\mu y$ for some $\mu \geq 0$.

Proof. As $\kappa = 5$, we have that y is odd. Then

$$(x + q^k\phi)\mathcal{O}_M = \mathfrak{A}^n,$$

where $\mathfrak{A}$ is an ideal of $\mathcal{O}_M$ with norm y. Since $[\mathfrak{P}]$ generates the class group, the same is true of $[\mathfrak{P}]^{-1}$. Hence $[\mathfrak{A}] = [\mathfrak{P}]^{-i}$ for some $i \in \{0, 1, \ldots, h-1\}$. Now

$$(x + q^k\theta)\mathcal{O}_M = \mathfrak{P}^{-ni} \cdot (\mathfrak{P}^i \cdot \mathfrak{A})^n.$$

Since $\mathfrak{P}^i \cdot \mathfrak{A}$ is principal, it follows that $\mathfrak{P}^{-ni}$ is also principal. The lemma follows. $\square$

Lemma 14.5. *Let $\kappa = 1$. Suppose that the class group $\mathrm{Cl}(\mathcal{O}_M)$ of $\mathcal{O}_M$ is cyclic and generated by the class $[\mathfrak{P}]$. Let $h = \#\mathrm{Cl}(\mathcal{O}_M)$ and set*

$$\mathcal{I} = \{0 \leq i \leq h-1 \ : \ \mathfrak{P}^{n(1-i)-2} \text{ is principal}\}.$$

Choose for each $i \in \mathcal{I}$ a generator β_i for $\mathfrak{P}^{n(1-i)-2}$. Let

$$\mathcal{S}' = \{\beta_i : i \in \mathcal{I}\} \cup \{\overline{\beta_i} : i \in \mathcal{I}\},$$

where $\overline{\beta_i}$ denotes the Galois conjugate of β_i. Let

$$\mathcal{S} = \begin{cases} \{2 \cdot \beta \ : \ \beta \in \mathcal{S}'\} & \text{if } \delta = 0 \\ \{2 \cdot \epsilon^j \cdot \beta \ : \ -(n-1)/2 \leq j \leq (n-1)/2, \ \beta \in \mathcal{S}'\} & \text{if } \delta = 1, \end{cases}$$

where ϵ is a fundamental unit for M. Then there is some $\gamma \in \mathcal{S}$ and $\alpha \in \mathcal{O}_M$ such that (75) holds. Moreover, $\mathrm{Norm}(\alpha) = 2^\mu y$ for some $\mu \in \mathbb{Z}$.

Proof. As $\kappa = 1$, we have that y is even. Then

$$\left(\frac{x + q^k\phi}{2}\right)\mathcal{O}_M = \mathfrak{C}^{n-2}\mathfrak{A}^n$$

where $\mathfrak{A}$ is an ideal of $\mathcal{O}_M$ with norm $y/2$ and $\mathfrak{C}$ is one of $\mathfrak{P}, \overline{\mathfrak{P}}$. Since $[\mathfrak{P}]$ generates the class group so does $[\mathfrak{C}]^{-1}$. Hence $[\mathfrak{A}] = [\mathfrak{C}]^{-i}$ for some $i \in \{0, 1, \ldots, h-1\}$. Now

$$\left(\frac{x + q^k\phi}{2}\right)\mathcal{O}_M = \mathfrak{C}^{n(1-i)-2} \cdot (\mathfrak{C}^i\mathfrak{A})^n.$$

But $\mathfrak{C}^i \cdot \mathfrak{A}$ is principal, whence $\mathfrak{C}^{n(1-i)-2}$ is principal, and so $i \in \mathcal{I}$ and $\mathfrak{C}^{n(1-i)-2}$ is generated by either β_i or $\overline{\beta_i}$. The lemma follows. $\square$

We will now describe our refined sieve. Fix $m \in \{0, 1, \ldots, 2n\}$ and suppose $k \equiv m \pmod{2n}$. Let $\mathfrak{n}$ be a prime ideal of $\mathcal{O}_f$ above n. Let $\ell \neq q$ be a prime. Suppose

(a) $\ell = tn + 1$ for some positive integer t;
(b) $\mathfrak{n} \nmid (4 - c_\ell^2)$;
(c) $(-1)^{\delta+1}q$ is a square modulo ℓ.

We choose an integer s such that $s^2 \equiv (-1)^{\delta+1}q \pmod{\ell}$. Let

$$\mathfrak{L} = \ell\mathcal{O}_M + (s - \phi)\mathcal{O}_M.$$

By the Dedekind–Kummer theorem ℓ splits in $\mathcal{O}_M$ and $\mathfrak{L}$ is one of the two prime ideals above ℓ. In particular, $\mathcal{O}_M/\mathfrak{L} \cong \mathbb{F}_\ell$ and $\phi \equiv s \pmod{\mathfrak{L}}$. Let

$$\mathcal{X}_{\ell,m} = \{z \in \mathbb{F}_\ell \ : \ (z^2 + (-1)^\delta q^{2m+1})^t \equiv 1 \pmod{\ell}\},$$

$$\mathcal{Y}_{\ell,m} = \{z \in \mathcal{X}_{\ell,m} \ : \ a_\ell(G_{z,m}) \equiv c_\ell \pmod{\mathfrak{n}}\},$$

$$\mathcal{U}_{\ell,m} = \{(z, \gamma) \ : \ z \in \mathcal{Y}_{\ell,m}, \quad \gamma \in \mathcal{S}, \quad (z + q^m\phi)^t \equiv \gamma^t \pmod{\mathfrak{L}}\},$$

$$\mathcal{W}_{\ell,m} = \{\gamma \ : \ \text{there exists } z \text{ such that } (z, \gamma) \in \mathcal{U}_{\ell,m}\}.$$

Lemma 14.6. *Let $\ell_1, \ldots, \ell_r$ be primes $\neq q$ satisfying (a), (b) and (c) above. Let*

$$\mathcal{W} = \mathcal{W}_{\ell_1, \ldots, \ell_r} = \bigcap_{i=1}^{r} \mathcal{W}_{\ell_i}.$$

If $\overline{\rho}_{G,n} \sim \overline{\rho}_{f,\mathfrak{n}}$, then there is some $\gamma \in \mathcal{W}$ and some $\alpha \in \mathcal{O}_M$ such that (75) holds.

Proof. Suppose ℓ satisfies conditions (a), (b) and (c). As ℓ satisfies (a) and (b), it also satisfies hypotheses (i) and (ii) preceding the statement of Lemma 14.3. Write $k = 2nb + m$ where b is a non-negative integer, and let $z \equiv x/q^{2nb} \pmod{\ell}$. It follows from the proof of Lemma 14.3 that $\ell \nmid y$ and that $z \in \mathcal{Y}_{\ell,m}$. We know from Lemmata 14.4 and 14.5 that there is some $\gamma \in \mathcal{S}$ such that $x + q^k \phi = \gamma \alpha^n$ where $\alpha \in \mathcal{O}_M$ satisfies $\mathrm{Norm}(\alpha) = 2^\mu y$ for some $\mu \in \mathbb{Z}$. Note that γ is supported only on the prime ideals above 2. Since $\mathfrak{L} \mid \ell$, we have $\mathrm{ord}_{\mathfrak{L}}(\alpha) = \mathrm{ord}_{\mathfrak{L}}(\gamma) = 0$. Hence

$$z + q^m \phi \equiv \frac{1}{q^{2nb}}(x + q^k \phi) \equiv \gamma \cdot \left(\frac{\alpha}{q^{2b}} \right)^n \pmod{\mathfrak{L}}.$$

Since $(\mathcal{O}_M/\mathcal{L})^* \cong \mathbb{F}_\ell^*$ is cyclic of order $\ell - 1 = tn$, we have

$$(z + q^m \phi)^t \equiv \gamma^t \pmod{\mathcal{L}}.$$

Thus $(z, \gamma) \in \mathcal{U}_{\ell,m}$ and hence $\gamma \in \mathcal{W}_{\ell,m}$. The lemma follows. $\square$

Proof of Proposition 14.1. Our proof of Proposition 14.1 is the result of applying `Magma` scripts based on Lemmata 14.2, 14.3 and 14.6, as well as solving a few Thue–Mahler equations. Our approach subdivides the proof into 60 cases corresponding to 60 quadruples (q, δ, κ, v): here (q, δ, κ) is one of the 30 triples in (74), and $v \in \{0, 1\}$. Let (x, y, k) be a solution to (72) with prime exponent $n \geq 7$. Suppose that y is even if $\kappa = 1$ and y is odd if $\kappa = 5$. Suppose moreover that $k \equiv v \pmod{2}$. Our first step is to compute the newforms f of weight 2 and level $N = 2^\kappa q$. We know that for one these newforms f, we have $\overline{\rho}_{G,n} \sim \overline{\rho}_{f,\mathfrak{n}}$ where $G = G_{x,k}$ is the Frey–Hellegouarch curve given in Proposition 14.1, and $\mathfrak{n} \mid n$ is a prime ideal of $\mathcal{O}_f$, the ring of integers of the Hecke eigenfield K_f. Let $p_1, \ldots, p_s$ be the primes ≤ 200 distinct from 2, q and let

$$\mathcal{E}_f = \sum_{i=1}^{s} \mathcal{E}_{p_i},$$

where $\mathcal{E}_{p_i}$ is as in Lemma 14.2. It follows from Lemma 14.2 that if $\overline{\rho}_{G,n} \sim \overline{\rho}_{f,\mathfrak{n}}$ then $\mathfrak{n} \mid \mathcal{E}_f$, and so $n \mid \mathrm{Norm}(\mathcal{E}_f)$.

We illustrate this by taking $(q, \delta, \kappa, v) = (31, 1, 5, 0)$. There are 8 newforms $f_1, \ldots, f_8$ of weight 2 and level $2^\kappa q = 992$, which all happen to be irrational. We find that

$$\mathrm{Norm}(\mathcal{E}_{f_j}) = 7, \ 7, \ 2^{10}, \ 2^{10}, \ 2^3, \ 2^3, \ 2^6 \times 3^2, \ 2^6 \times 3^2,$$

respectively for $j = 1, 2, \ldots, 8$. Thus $n = 7$ and $f = f_1$ or f_2. We consider first

$$f = f_1 = \mathfrak{q} + \sqrt{2}\mathfrak{q}^3 - \mathfrak{q}^5 - (1 + \sqrt{2})\mathfrak{q}^7 - \mathfrak{q}^9 + 2(1 - \sqrt{2})\mathfrak{q}^{11} + \cdots,$$

with Hecke eigenfield $K_f = \mathbb{Q}(\sqrt{2})$ having ring of integers $\mathcal{O}_f = \mathbb{Z}[\sqrt{2}]$. We found that $\mathcal{E}_f = (1 + 2\sqrt{2})$ which is one of the two prime ideals above 7. Hence $\mathfrak{n} = (1 + 2\sqrt{2})$. Next we compute $\mathcal{Z} = \mathcal{Z}_{\ell_1, \ldots, \ell_{30}}$ as in Lemma 14.3 where $\ell_1, \ldots, \ell_{30} \neq 31$ are the 30 primes satisfying (i) and (ii) with $t \leq 200$. We find that $\mathcal{Z} = \{0, 8\}$. Thus, by Lemma 14.3, we have $k \equiv 0$ or $8 \pmod{14}$. Now for $m = 0$ and $m = 8$, we compute $\mathcal{W} = \mathcal{W}_{\ell_1, \ldots, \ell_{36}}$ as in Lemma 14.6, where $\ell_1, \ldots, \ell_{36} \neq 31$ are the 36 primes satisfying (a), (b) and (c) with $t \leq 800$. We found that $\mathcal{W} = \emptyset$ for $m = 0$ and that $\mathcal{W} = \{\epsilon^3\}$ for $m = 8$ where $\epsilon = 1520 + 273\sqrt{31}$ is the fundamental unit of $M = \mathbb{Q}(\sqrt{31})$. Hence we conclude, by Lemma 14.6, that $k \equiv 8 \pmod{14}$ and that

$$x + 31^k \sqrt{31} = (1520 + 273\sqrt{31})^3 (X + Y\sqrt{31})^7,$$

for some integers X, Y. Equating the coefficients of $\sqrt{31}$ on both sides results in a degree 7 Thue–Mahler equation with huge coefficients. However, using an algorithm of Stoll and Cremona [43] for reducing binary forms we discover that this Thue–Mahler equation can be rewritten as

$$31^k = -56U^7 + 112U^6V - 84U^5V^2 + 140U^4V^3 + 490U^3V^4 + 1596U^2V^5 + 2807UV^6 + 2119V^7,$$

where U, $V \in \mathbb{Z}$ are related to X, Y via the unimodular substition

$$U = 2X + 11Y \quad \text{and} \quad V = 7X + 39Y.$$

We applied the Thue–Mahler solver to this and found that it has no solutions. Next we take $f = f_2$ which also has Hecke eigenfield $K_f = \mathbb{Q}(\sqrt{2})$. We apply Lemmata 14.2, 14.3 and 14.6 using the same sets of primes p_j and ℓ_i as for f_1. We find $\mathcal{E}_f = (1 - 2\sqrt{2})$, and so $\mathfrak{n} = (1 - 2\sqrt{2})$ and $n = 7$. Again we obtain $\mathcal{Z} = \{0, 8\}$ on applying Lemma 14.3. We find that $\mathcal{W} = \emptyset$ for $m = 0$ and $\mathcal{W} = \{\bar{\epsilon}^3\}$ for $m = 8$. Again the corresponding Thue–Mahler equation has no solutions. Thus equation (72) has no solutions with $n \geq 7$ prime for $q = 31$, $\delta = 1$ and with y odd (i.e. $\kappa = 5$) and $k \equiv 0 \pmod{2}$. We used the above approach to deal with all the cases where $\mathcal{E}_f$ is non-zero. In all the cases where $\mathcal{E}_f = 0$, the newform f is rational, and in fact corresponds to an elliptic curve $E/\mathbb{Q}$ with non-trivial 2-torsion. These elliptic curves are listed in Table 3. Thus $\bar{\rho}_{G,n} \sim \bar{\rho}_{E,n}$. What is required for Proposition 14.1 is to show in these cases that there are no solutions with prime $7 \leq n < 1000$ apart from the ones listed in the statement of the proposition. We illustrate how this works by taking $(q, \delta, \kappa, v) = (7, 0, 1, 0)$. There is a unique newform f of weight 2 and level $N = 2^\kappa q = 14$ which corresponds to the elliptic curve

$$Y^2 + XY + Y = X^3 + 4X - 6$$

with Cremona label $\mathtt{14a1}$. For each prime $7 \leq n < 1000$ we computed $\mathcal{Z} = \mathcal{Z}_{\ell_1,\dots,\ell_r}$ with $\ell_1, \dots, \ell_r$ being the primes $\neq 7$ satisfying conditions (i), (ii) with $t \leq 200$. The results of this computation is summarized in Table 4. Note that by Lemma 14.3, $(k \pmod{2n}) \in \mathcal{Z}$. We deduce that there are no solutions for prime n satisfying $17 \leq n < 1000$, $n \neq 41$. For $n = 7$, 11, 13 and 41, and for each m in the corresponding $\mathcal{Z}$, we compute $\mathcal{W} = \mathcal{W}_{\ell_1,\dots,\ell_r}$ as in Lemma 14.6 where $\ell_1, \dots, \ell_r$ are now the primes $\neq q$ satisfying (a), (b) and (c) with $t \leq 800$. We found that $\mathcal{W} = \emptyset$ in all cases except for $n = 7$, $m = 0$, when $\mathcal{W} = 11 - \sqrt{-7}$. It follows from Lemma 14.6 that $x + 7^k\sqrt{-7} = (11 - \sqrt{-7}) \cdot \alpha^7$ where $\alpha \in \mathbb{Z}[\theta]$ where $\theta = (1 + \sqrt{-7})/2$. Write $\alpha = (X + Y\theta)$ with X, $Y \in \mathbb{Z}$. Thus

$$\frac{x - 7^k}{2} + 7^k \cdot \theta = (6 - \theta) \cdot (X + Y\theta)^7.$$

Equating the coefficients of θ on either side yields the Thue–Mahler equation

$$-X^7 + 35X^6Y + 147X^5Y^2 - 105X^4Y^3 - 595X^3Y^4 - 231X^2Y^5 + 161XY^6 + 45Y^7 = 7^k.$$

We find that the only solution is $(X, Y, k) = (-1, 0, 0)$. Hence $x = -11$, and the corresponding solution to (72) is $11^2 + 7 = 2^7$. We observe that $-11 \equiv 1 \pmod{4}$ which is consistent with our assumption $x \equiv 1 \pmod{4}$ if $\kappa = 1$, made in the statement of Proposition 14.1. The other cases are similar.

Proofs of Theorems 2 and 3. We now deduce Theorems 2 and 3 from Proposition 14.1. These two theorems concern the equation $x^2 - q^{2k+1} = y^n$ with $n \geq 3$ and $q \nmid x$. Thus we are in the $\delta = 1$ case of the proposition. By the remarks following the statement of the proposition we are reduced to the case $n \geq 7$ is prime. Theorem 2 is concerned with the primes q appearing in (4), whilst Theorem 3 deals with $q = 41, 73, 89$ and 97. A glance at Table 3 reveals that all the elliptic curves E appearing in Proposition 14.1 for the case $\delta = 1$ in fact correspond to the values $q = 41$, 73, 89 and 97. Theorems 2 and 3 now follow immediately from the proposition.

n	$\mathcal{Z}$
7	$\{0, 8, 12\}$
11	$\{8\}$
13	$\{4\}$
41	$\{44\}$
other values	$\emptyset$

TABLE 4.   For the quadruple $(q, \delta, \kappa, v) = (7, 0, 1, 0)$ and for prime $7 \leq n < 1000$ we computed $\mathcal{Z} = \mathcal{Z}_{\ell_1, \ldots, \ell_r}$ as given by Lemma 14.3. Here we chose $\ell_1, \ldots, \ell_r$ to be the primes $\neq q$ satisfying (i) and (ii) with $t \leq 200$.

A Remark. It is well-known that the exponent n can be explicitly bounded in (72) in terms of the prime q. For example, if $\delta = 1$ and $\kappa = 5$ (i.e. y is odd) then Bugeaud [13] shows that

$$(76) \qquad\qquad n \leq 4.5 \times 10^6 q^2 \log^2 q.$$

Let $(q, \delta, \kappa, v) = (73, 1, 5, 1)$ and E be the elliptic curve with Cremona label `2336a1`; this is one of the two outstanding cases from Table 3 for which the bound (76) is applicable. We are in fact able to substantially improve this bound for the case in consideration through a specialization and minor refinement (we omit the details) of Bugeaud's approach and deduce that

$$n < 6 \times 10^6.$$

Theorem 3 only resolves $x^2 - 73^{2k+1} = y^n$ for $3 \leq n \leq 1000$. It is natural to ask whether we can apply the same technique, namely Lemma 14.3, to show that there are no solutions for prime exponents n in the range $1000 < n < 6 \times 10^6$. Write n_u for the smallest prime $> 2^u$. For $10 \leq u \leq 22$ the prime $n = n_u$ belongs to the range $1000 < n < 6 \times 10^6$. For each of these 13 primes we computed primes $\ell_1, \ldots, \ell_r$ satisfying conditions (i) and (ii) such that $\mathcal{Z}_{\ell_1, \ldots, \ell_r} = \emptyset$, whence by Lemma 14.3 there are no solutions for that particular exponent n. Table 5 records the values of $\ell_1, \ldots, \ell_r$ as well as the time taken to perform the corresponding computation in `Magma` on a single processor. There are 412681 primes in the range $1000 < n < 6 \times 10^6$. On the basis of the timing in the table we crudely estimate that it would take around 60 years to carry out the computation (on a single processor) for all 412681 primes.

We shall shortly give a substantially faster method for treating the case $\delta = 0$. Alas this method is not available for $\delta = 1$, as we explain in due course.

15. The proof of Theorem 1 : large exponents

We now complete the proof of Theorem 1 which is concerned, for prime $3 \leq q < 100$, with the equation $x^2 + q^\alpha = y^n$, subject to the assumptions that $q \nmid x$ and $n \geq 3$. The exponents $n = 3$ and $n = 4$ were treated in Section 2, so we may suppose that $n \geq 5$ is prime. The case $\alpha = 2k$ was handled in Section 5, so we suppose further that $\alpha = 2k + 1$. The case with y odd was the topic of Section 11, so we may assume that y is even. Finally, the case with exponent $n = 5$ was resolved in Section 12, whence we may suppose that $n \geq 7$ is prime. To summarize, we are reduced to treating the equation

$$(77) \qquad\qquad x^2 + q^{2k+1} = y^n, \qquad k \geq 0, \quad q \nmid x, \quad y \text{ even}, \ n \geq 7 \text{ prime.}.$$

By Proposition 14.1, we may in fact suppose that $n > 1000$ and that

$$(78) \qquad\qquad q \in \{7, 23, 31, 47, 71, 79\}.$$

For convenience, we restate Proposition 14.1 specialized to our current situation.

n	$\{\ell_1, \ldots, \ell_r\}$	Time
$2^{10} + 7 = 1031$	$\{2063, 12373, 30931\}$	0.18 seconds
$2^{11} + 5 = 2053$	$\{94439, 110863, 143711, 168347, 197089\}$	7.75 seconds
$2^{12} + 3 = 4099$	$\{73783, 98377, 114773\}$	4.390 seconds
$2^{13} + 17 = 8209$	$\{246271, 525377, 574631\}$	15.5 seconds
$2^{14} + 27 = 16411$	$\{98467, 459509, 590797\}$	6.19 seconds
$2^{15} + 3 = 32771$	$\{65543, 983131, 1179757\}$	3.91 seconds
$2^{16} + 1 = 65537$	$\{917519, 1310741, 1703963, 2359333\}$	57.51 seconds
$2^{17} + 29 = 131101$	$\{2097617, 9439273, 11799091, 12585697\}$	142.59 seconds
$2^{18} + 3 = 262147$	$\{1048589, 4194353, 6291529\}$	65.89 seconds
$2^{19} + 21 = 524309$	$\{6291709, 10486181, 23069597\}$	402.12 seconds
$2^{20} + 7 = 1048583$	$\{20971661, 25165993, 44040487\}$	1319.57 seconds
$2^{21} + 17 = 2097169$	$\{37749043, 176162197, 188745211\}$	2468.46 seconds
$2^{22} + 15 = 4194319$	$\{75497743, 92275019, 100663657\}$	4983.07 seconds

TABLE 5. Write n_u for the smallest prime $> 2^u$. For $10 \leq u \leq 22$ the prime $n = n_u$ belongs to the range $1000 < n < 6 \times 10^6$. The table lists the primes $n = n_u$ in this range and, for each, a set of primes $\ell_1, \ldots, \ell_r$ satisfying conditions (i), (ii) such that $\mathcal{Z}_{\ell_1, \ldots, \ell_r} = \emptyset$. It also records the time the computation took for each of these values of n, on a single processor.

Lemma 15.1. *Let q be one of the values in (78). Let (x, y, k) satisfy (77), where $n > 1000$ is prime. Suppose without loss of generality that $x \equiv 1 \pmod 4$. Attach to this solution the Frey–Hellegouarch elliptic curve*

$$G = G_{x,k} \; : \; Y^2 = X^3 + 4xX^2 + 4(x^2 + q^{2k+1})X.$$

Then $\bar{\rho}_{G,n} \sim \bar{\rho}_{E,n}$ where E is an elliptic curve of conductor $2q$ and non-trivial 2-torsion given in Table 6.

q	Cremona Label for E	A minimal model for E
7	14a1	$Y^2 + XY + Y = X^3 + 4X - 6$
23	46a1	$Y^2 + XY = X^3 - X^2 - 10X - 12$
31	62a1	$Y^2 + XY + Y = X^3 - X^2 - X + 1$
47	94a1	$Y^2 + XY + Y = X^3 - X^2 - 1$
71	142c1	$Y^2 + XY = X^3 - X^2 - X - 3$
79	158e1	$Y^2 + XY + Y = X^3 + X^2 + X + 1$

TABLE 6.

Upper bounds for n : linear forms in logarithms, complex and q-adic. We will appeal to bounds for linear forms in logarithms to deduce an upper bound for the prime exponent n in (77) where q belongs to (78).

Proposition 15.2. *Let q belong to the list* (78). *Let (x, y, k) satisfy* (77) *with prime exponent $n > 1000$. Then $n < U_q$ where*

(79)
$$U_q = \begin{cases} 2.8 \times 10^8 & \text{if } q = 7, \\ 1.1 \times 10^9 & \text{if } q = 23, \\ 5.0 \times 10^8 & \text{if } q = 31, \\ 2.2 \times 10^9 & \text{if } q = 47, \\ 2.3 \times 10^9 & \text{if } q = 71, \\ 2.2 \times 10^9 & \text{if } q = 79. \end{cases}$$

To obtain this result, our first order of business will be to produce a lower bound upon y.

Lemma 15.3. *If there exists a solution to equation* (77), *then $y > 4n - 4\sqrt{2n} + 2$.*

Proof. We suppose without loss of generality that $x \equiv 1 \pmod 4$, so that we can apply Lemma 15.1. We first show that y is divisible by an odd prime. Suppose otherwise and write $y = 2^\mu$ with $\mu \geq 1$. Then the Frey–Hellegouarch curve $G_{x,k}$ has conductor $2q$ and minimal discriminant $-2^{2n\mu - 12}q^{2k+1}$. A short search of Cremona's tables [19] reveals that there are no such elliptic curves for the values q in (78) (recall that $n > 1000$). Thus, there necessarily exists an odd prime $p \mid y$; since $q \nmid y$, we observe that $q \neq p$. By Lemma 7.1,

$$a_p(E) \equiv \pm(p+1) \pmod n,$$

where E is given by Table 6. As E has non-trivial 2-torsion, we conclude that $2n \mid (p+1 \mp a_p(E))$. However, from the Hasse–Weil bounds

$$0 < p + 1 \mp a_p(E) < (\sqrt{p} + 1)^2 \leq (\sqrt{y/2} + 1)^2,$$

and therefore $2n < (\sqrt{y/2} + 1)^2$. The desired inequality follows. $\qquad\square$

Now let q be any of the values in (78), write $M = \mathbb{Q}(\sqrt{-q})$, and let $\mathcal{O}_M$ be its ring of integers. Note that the units of $\mathcal{O}_M$ are ± 1. Fix $\mathfrak{P}$ to be one of the two prime ideals of $\mathcal{O}_M$ above 2. After possibly replacing x by $-x$ we have

(80)
$$\frac{x + q^k \sqrt{-q}}{2} \cdot \mathcal{O}_M = \mathfrak{P}^{n-2} \cdot \mathfrak{A}^n,$$

where $\mathfrak{A}$ is an ideal of $\mathcal{O}_M$ with norm $y/2$. Hence

$$\frac{x - q^k \sqrt{-q}}{x + q^k \sqrt{-q}} = \left(\frac{\mathfrak{P}}{\overline{\mathfrak{P}}}\right)^2 \cdot \left(\frac{\overline{\mathfrak{P}} \cdot \overline{\mathfrak{A}}}{\mathfrak{P} \cdot \mathfrak{A}}\right)^n.$$

For all six values of q under consideration, the class group is cyclic and generated by the class $[\mathfrak{P}]$. Let h_q be the class number of M; this value is respectively 1, 3, 3, 5, 7 and 5 for q in (78) (see Table 7). As $n > 1000$ is prime, $\gcd(n, h_q) = 1$. Since $\mathcal{O}_M$ has class number h_q, it follows that $\mathfrak{P}^{h_q}$ is principal, say $\mathfrak{P}^{h_q} = (\alpha_q) \cdot \mathcal{O}_M$. We fix our choice of $\mathfrak{P}$ so that α_q is given by Table 7. Write $\beta_q = \alpha_q / \overline{\alpha_q}$. Thus

(81)
$$\left(\frac{x - q^k \sqrt{-q}}{x + q^k \sqrt{-q}}\right)^{h_q} = \beta_q^2 \gamma^n,$$

where $\gamma \in M$ is some generator for the principal ideal $((\overline{\mathfrak{P}} \cdot \overline{\mathfrak{A}})/(\mathfrak{P} \cdot \mathfrak{A}))^{h_q}$.

To derive an upper bound upon n, we will begin by using (81) to find a "small" linear form in logarithms. Write

$$\Lambda = \log\left(\frac{x - q^k \sqrt{-q}}{x + q^k \sqrt{-q}}\right).$$

q	h_q	α_q	q	h_q	α_q
7	1	$\frac{1+\sqrt{-7}}{2}$	47	5	$\frac{9+\sqrt{-47}}{2}$
23	3	$\frac{3+\sqrt{-23}}{2}$	71	7	$\frac{21+\sqrt{-71}}{2}$
31	3	$\frac{1+\sqrt{-31}}{2}$	79	5	$\frac{7+\sqrt{-79}}{2}$

TABLE 7. Here, h_q denotes the class number of $M = \mathbb{Q}(\sqrt{-q})$, and α_q is a generator for the principal ideal $\mathfrak{P}^{h_q}$, where $\mathfrak{P}$ is one of the two prime ideals of $\mathcal{O}_M$ above 2.

Lemma 15.4. *If there exists a solution to equation (77) with $y^n > 100\,q^{2k+1}$, then*

$$\log|\Lambda| < 0.75 + (k+1/2)\log q - \frac{n}{2}\log y.$$

Proof. The assumption that $y^n > 100\,q^{2k+1}$, together with, say, Lemma B.2 of Smart [41], implies that

$$|\Lambda| \le -10\log(9/10)\left|\frac{x - q^k\sqrt{-q}}{x + q^k\sqrt{-q}} - 1\right| = -20\log(9/10)\frac{q^k\sqrt{q}}{y^{n/2}},$$

whence the lemma follows. $\qquad\square$

To show that $\log|\Lambda|$ here is indeed small, we first require an upper bound upon k. From (81), we have that

$$\left(\frac{x - q^k\sqrt{-q}}{x + q^k\sqrt{-q}}\right)^{h_q} - 1 = \beta_q^2\gamma^n - 1$$

and so

$$(82) \qquad \frac{-2q^k\sqrt{-q}}{x + q^k\sqrt{-q}}\sum_{i=0}^{h_q-1}\left(\frac{x - q^k\sqrt{-q}}{x + q^k\sqrt{-q}}\right)^i = \beta_q^2\gamma^n - 1.$$

Since $\gcd(x, q) = 1$, it follows from (82) that, if we set

$$\Lambda_1 = \gamma^n - \overline{\beta_q}^{-2},$$

then $\nu_q(\Lambda_1) \ge k$. To complement this with an upper bound for linear forms in q-adic logarithms, we will appeal to Theorem 10, with

$$q \in \{7, 23, 31, 47, 79\}, \quad f = 1, \quad D = 2, \quad \alpha_1 = \gamma, \quad \alpha_2 = \overline{\beta_q}, \quad b_1 = n, \quad b_2 = 2,$$

$$\log A_1 = \frac{h_q}{2}\log y, \quad \log A_2 = \frac{1}{2}\log q \quad \text{and} \quad b' = \frac{n}{\log q} + \frac{2}{h_q\log y}.$$

Here, we use Lemma 13.2 of Bugeaud, Mignotte and Siksek [15] which implies that

$$h(\alpha_1) = \frac{h_q}{2}\log(y) \quad \text{and} \quad h(\alpha_2) = \frac{h_q}{2}\log 2.$$

In case $q = 71$, we make identical choices except to take $\log A_2 = \frac{7}{2}\log 2$, whence

$$b' = \frac{n}{7\log 2} + \frac{2}{7\log y}.$$

Theorem 10 thus yields the inequality

$$\nu_q(\Lambda_1) \le \frac{96\,q\,h_q}{\log^3 q}\cdot\left(\max\left\{\log(b') + \log\log q + 0.4, 5\log q\right\}\right)^2\log y,$$

for $q \in \{7, 23, 31, 47, 79\}$, and

$$\nu_{71}(\Lambda_1) \le 701.2\cdot\left(\max\left\{\log(b') + \log\log 71 + 0.4, 5\log 71\right\}\right)^2\log y,$$

if $q = 71$.

Let us now suppose that

$$(83) \qquad n > 10^8,$$

which will certainly be the case if $n \geq U_q$, for U_q as defined in (79). Then, from Lemma 15.3, in all cases we have that

$$b' < 1.001 \frac{n}{\log q}$$

and hence obtain the inequalities

$$(84) \qquad k < \frac{96\, q\, h_q}{\log^3 q} \cdot (\max\{\log(n) + 0.4001, 5\log q\})^2 \log y, \quad \text{if} \quad q \in \{7, 23, 31, 47, 79\}$$

and

$$(85) \qquad k < 701.2 \cdot (\max\{\log(n) + 0.4001, 5\log 71\})^2 \log y, \quad \text{if} \quad q = 71.$$

Now consider

$$(86) \qquad \Lambda_2 = h_q \log\left(\frac{x - q^k \sqrt{-q}}{x + q^k \sqrt{-q}}\right) = n \log(\epsilon_1 \gamma) + 2 \log(\epsilon_2 \beta_q) + j\pi i,$$

where we take the principal branches of the logarithms and the integers $\epsilon_i \in \{-1, 1\}$ and j are chosen so that $\mathrm{Im}(\log(\epsilon_1 \gamma))$ and $\mathrm{Im}(\log(\epsilon_2 \beta_q))$ have opposite signs, and we have both

$$|\log(\epsilon_2 \beta_q)| < \frac{\pi}{2}$$

and $|\Lambda_2|$ minimal. Explicitly,

q	ϵ_2	$|\log(\epsilon_2 \beta_q)|$	q	ϵ_2	$|\log(\epsilon_2 \beta_q)|$
7	-1	$\arccos(3/4)$	47	1	$\arccos(17/64)$
23	-1	$\arccos(7/16)$	71	1	$\arccos(185/256)$
31	-1	$\arccos(15/16)$	79	-1	$\arccos(15/64)$

Assume first that

$$y^n \leq 100\, q^{2k+1}.$$

If $q \in \{7, 23, 31, 47, 79\}$, it follows from (84) that

$$n < \frac{2\log 10}{\log y} + \frac{\log q}{\log y} + \frac{192\, q\, h_q}{\log^2 q} \cdot (\max\{\log(n) + 0.4001, 5\log q\})^2,$$

in each case contradicting Lemma 15.3 and (83). We obtain a like contradiction in case $q = 71$ upon considering (85).

It follows, then that we may assume $y^n > 100\, q^{2k+1}$ and hence conclude, from Lemma 15.4, that

$$\log|\Lambda_2| < \log h_q + 0.75 + (k + 1/2)\log q - \frac{n}{2}\log y.$$

If $q \in \{7, 23, 31, 47, 79\}$, (84) thus implies that

$$\log|\Lambda_2| < \log h_q + 0.75 + \frac{1}{2}\log q + \frac{96\, q\, h_q}{\log^2 q} \cdot (\max\{\log(n) + 0.4001, 5\log q\})^2 \log y - \frac{n}{2}\log y.$$

An analogous inequality holds for $q = 71$, upon appealing to (85). From Lemma 15.3 and (83), we find that

$$(87) \qquad \log|\Lambda_2| < -\kappa_q\, n \log y,$$

where

$$(88) \qquad \kappa_q = \begin{cases} 0.499 & \text{if } q = 7, \\ 0.497 & \text{if } q \in \{23, 31\}, \\ 0.494 & \text{if } q = 47, \\ 0.486 & \text{if } q = 71, \\ 0.490 & \text{if } q = 79. \end{cases}$$

It therefore follows from the definition of Λ_2 that

$$|j|\pi < \pi n + 2\arccos(15/64) + y^{-0.486n} < \pi n + \pi,$$

and so

$$(89) \qquad\qquad |j| \le n.$$

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 [29].

Theorem 14 (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,

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

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

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

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 14 to $\Lambda = \Lambda_2$ with

$$D = 2, \ \chi = 2, \ n_0 = 3, \ b_3 = n, \ \alpha_3 = \epsilon_1\gamma, \ b_2 = -2, \ \alpha_2 = \epsilon_2\beta_q, \ b_1 = j \ \text{and} \ \alpha_1 = -1.$$

We may thus take

$$A_3 = \log y, \ A_2 = \max\{h_q \log 2, |\log(\epsilon_2\beta_q)|\}, \ A_1 = \pi \ \text{and} \ B = n.$$

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

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

we may therefore conclude that

$$\log|\Lambda_2| > -5.68 \times 10^{11} \max\{h_q \log 2, |\log(\epsilon_2\beta_q)|\} (2.63 + \log n) \log y.$$

It thus follows from (87) that

$$n < \kappa_q^{-1} \, 5.68 \times 10^{11} \max\{h_q \log 2, |\log(\epsilon_2\beta_q)|\} (2.63 + \log n)$$

and hence

(90)
$$n < \begin{cases} 2.77 \times 10^{13} & \text{if } q = 7, \\ 8.24 \times 10^{13} & \text{if } q \in \{23, 31\}, \\ 1.42 \times 10^{14} & \text{if } q \in \{47, 79\} \\ 2.02 \times 10^{14} & \text{if } q = 71. \end{cases}$$

To improve these inequalities, we appeal to a sharper, rather complicated lower bound for linear forms in three complex logarithms, due to Mignotte (Theorem 2 of [31]). Our argument is very similar to that employed in a recent paper of the authors [6]. We note that recent work of Mignotte and Voutier [32] would substantially improve our bounds (and reduce our subsequent computations considerably).

Theorem 15 (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

(91)
$$b_2 |\log \alpha_2| = b_1 |\log \alpha_1| + b_3 |\log \alpha_3| \pm |\Lambda|$$

and put

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

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

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

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

(92)
$$U \geq (D+1) \log(K^2 L) + gL(a_1 R + a_2 S + a_3 T) + D(K-1) \log b - 2 \log(e/2),$$

where

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

with

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

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

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

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

(93)
$$|\Lambda| \cdot \frac{LS e^{LS|\Lambda|/(2b_2)}}{2|b_2|} > \rho^{-KL},$$

*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*

(94)
$$r_0 b_2 = s_0 b_1$$

with

(95)
$$|r_0| \le \frac{(R_1 + 1)(T_1 + 1)}{\mathcal{M} - T_1} \quad and \quad |s_0| \le \frac{(S_1 + 1)(T_1 + 1)}{\mathcal{M} - T_1},$$

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

(96)
$$(t_1 b_1 + r_1 b_3)s_1 = r_1 b_2 t_2, \qquad \gcd(r_1, t_1) = \gcd(s_1, t_2) = 1,$$

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* $s_1 = 1$.

We will apply this result to $\Lambda = \Lambda_2$. For simplicity, we will provide full details for the case $q = 7$; the arguments for the other values of q under consideration. are similar and follow closely their analogues in [6]. If $j = 0$, then Λ_2 immediately reduces to a linear form in two logarithms and we may appeal to Theorem 11, with (in the notation of that result)

$$c_2 = n, \;\; \beta_2 = \epsilon_1 \gamma, \;\; c_1 = 2, \;\; \beta_1 = \frac{1}{\epsilon_2 \beta_q}, \;\; D = 1,$$

whence we may choose

$$\log B_2 = \frac{1}{2} \log y \quad \text{and} \quad \log B_1 = 1.$$

We thus have, from (83) and Lemma 15.3,

$$b' = \frac{4}{\log y} + n < 1.001n.$$

From Theorem 11 with $(m, C) = (10, 32.3)$, it follows, again from (83), that

$$\log |\Lambda_2| \geq -64.6 \left(\log n + 0.211\}\right)^2 \log y.$$

Combining this with inequality (87) contradicts (83). We argue similarly if $j = \pm n$, again reaching a contradiction via bounds for linear forms in two complex logarithms.

We may thus suppose that $j \neq 0$ and $|j| < n$ (so that, in particular, $\gcd(j, n) = 1$), and hence choose

(97) $$b_1 = 2, \quad \alpha_1 = \frac{1}{\epsilon_2 \beta_q}, \quad b_2 = n, \quad \alpha_2 = \epsilon_1 \gamma, \quad b_3 = -j \quad \text{and} \quad \alpha_3 = -1,$$

whence, from the fact that $\mathrm{Im}(\log(\epsilon_1 \gamma))$ and $\mathrm{Im}(\log(\epsilon_2 \beta_q))$ have opposite signs, (91) is satisfied and we have

$$d_1 = d_3 = 1 \quad \text{and} \quad b_2' = b_2'' = n.$$

It follows that

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

and hence we can take

$$a_1 = \rho \arccos(3/4) + \log(2), \; a_2 = \rho\pi + \log(y) \; \text{ and } \; a_3 = \rho\pi.$$

As noted in [15], if we suppose that $m \geq 1$ and define

(98)
$$K = [mL a_1 a_2 a_3], \; R_1 = [c_1 a_2 a_3], \; S_1 = [c_1 a_1 a_3], \; T_1 = [c_1 a_1 a_2], \; R_2 = [c_2 a_2 a_3],$$

$$S_2 = [c_2 a_1 a_3], \; T_2 = [c_2 a_1 a_2], \; R_3 = [c_3 a_2 a_3], \; S_3 = [c_3 a_1 a_3] \; \text{ and } \; T_3 = [c_3 a_1 a_2],$$

where

(99)
$$c_1 = \max\{(\chi m L)^{2/3}, (2mL/a_1)^{1/2}\}, \; c_2 = \max\{2^{1/3}(mL)^{2/3}, (m/a_1)^{1/2}L\}$$

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

then conditions (i)-(v) are automatically satisfied. It remains to verify inequality (92).

To carry this out, we optimize numerically over values of ρ, L, m and χ as in [6] (full details are available there, by way of example, in case $q = 7$). Pari/GP code for carrying this out, due to Voutier, is available at

https://github.com/PV-314/lfl3-kit.

In each case, we obtain a sharpened upper bound upon the exponent n, provided inequality (93) holds. If, on the other hand, inequality (93) fails to be satisfied, from inequality (83) and our choices of S_1 and S_2, necessarily (**C3**) holds and we may rewrite Λ_2 as a linear form in two complex logarithms to which we can apply Theorem 11. In this case, we once again obtain a sharpened upper bound for n. Iterating this process leads to the upper bounds U_q given in (79). We observe that direct application of the new bounds from [32], with the corresponding Pari/GP code, substantially sharpens these bounds, though this is not especially important for our purposes. This completes the proof of Proposition 15.2.

Proof of Theorem 1. We now finish the proof of Theorem 1. By the remarks at the beginning of the current section, we are reduced to considering solutions (x, y, k) to (77), where q belongs to (78). Thanks to Propositions 14.1 and 15.2, we may suppose that the prime exponent n belongs to the range $1000 < n < U_q$ where U_q is given by (79).

Lemma 15.5. *Let (x, y, k) be a solution to (77) where q belongs to (78) and the exponent n is a prime belonging to the range $1000 < n < U_q$. Let $M = \mathbb{Q}(\sqrt{-q})$. Let h_q and α_q be as in Table 7, and choose i to be the unique integer $0 \leq i \leq h_q - 1$ satisfying $ni \equiv -2 \pmod{h_q}$. Write $n^* = (-ni - 2)/h_q$. Then, after possible changing the sign of x,*

$$(100) \qquad \frac{x + q^k\sqrt{-q}}{2} = \alpha_q^{n^*} \cdot \gamma^n,$$

where $\gamma \in \mathcal{O}_M$. Moreover, $\mathrm{Norm}(\gamma) = 2^{i-1}y$.

Proof. Recall that h_q is the class number of M, and that $\mathfrak{P}^{h_q} = \alpha_q \mathcal{O}_M$, where $\mathfrak{P}$ is one of the two prime ideals of $\mathcal{O}_M$ above 2. From (78), after possibly replacing x by $-x$,

$$\left(\frac{x + q^k\sqrt{-q}}{2} \right) \cdot \mathcal{O}_M = \mathfrak{P}^{-2} \cdot \mathfrak{A}^n,$$

where $\mathfrak{A}$ is an ideal of $\mathcal{O}_M$ of norm $y/2$. Now, for the values of q we are considering, the class group is cyclic and generated by $[\mathfrak{P}]$. Thus there is some $0 \leq i \leq h_q - 1$ such that $\mathfrak{P}^i \mathfrak{A}$ is principal. However,

$$\left(\frac{x + q^k\sqrt{-q}}{2} \right) \cdot \mathcal{O}_M = \mathfrak{P}^{-ni-2} \cdot (\mathfrak{P}^i \cdot \mathfrak{A})^n.$$

We deduce that $\mathfrak{P}^{-ni-2}$ is principal. As the class $[\mathfrak{P}]$ generates the class group, we infer that i is the unique integer $0 \leq i \leq h_q - 1$ satisfying $ni \equiv -2 \pmod{h_q}$. Write $n^* = (-ni - 2)/h_q$. As $\mathfrak{P}^{h_q} = \alpha_q$, we have $\mathfrak{P}^{-ni-2} = \alpha_q^{n^*} \cdot \mathcal{O}_M$. Hence

$$\frac{x + q^k\sqrt{-q}}{2} = \alpha_q^{n^*} \cdot \gamma^n,$$

where $\gamma \in \mathcal{O}_M$ is a generator for the principal ideal $\mathfrak{P}^i \mathfrak{A}$. We note that $\mathrm{Norm}(\gamma) = 2^{i-1}y$. $\qquad\square$

The following lemma, inspired by ideas of Kraus [26], provides a computational framework for showing that (77) has no solutions for a particular exponent n.

Lemma 15.6. *Let q belong to the list (78) and let $\beta_q = \overline{\alpha_q}/\alpha_q$. Let n be a prime belonging to the range $1000 < n < U_q$. Let E be the elliptic curve given in Table 6. Let $\ell \neq q$ be a prime satisfying the following three conditions.*

(I) $-q$ is a square modulo ℓ;
(II) $\ell = tn + 1$ for some positive integer t;
(III) $a_\ell(E)^2 \not\equiv 4 \pmod{n}$.

Let $\mathfrak{L}$ be one of the two prime ideals of $\mathcal{O}_M$ above ℓ, and write $\mathbb{F}_\mathfrak{L} = \mathcal{O}_M/\mathfrak{L} \cong \mathbb{F}_\ell$. Let $\beta \in \mathbb{F}_\mathfrak{L}$ satisfy $\beta \equiv \overline{\alpha_q}/\alpha_q \pmod{\mathfrak{L}}$. Choose g to be a cyclic generator for $\mathbb{F}_\mathfrak{L}^*$, set $h = g^n$, and define

$$\mathfrak{X}_{\ell,n} = \{\beta^{n^*} \cdot h^j \ : \ j = 0, 1, \ldots, t-1\} \subset \mathbb{F}_\mathfrak{L}.$$

For $\mathfrak{x} \in \mathfrak{X}_{\ell,n}$ let

$$E_\mathfrak{x} \ : \ Y^2 = X(X+1)(X+\mathfrak{x}).$$

Finally, define

$$\mathfrak{Y}_{\ell,n} = \{\mathfrak{x} \in \mathfrak{X} \ : \ a_\mathfrak{L}(E_\mathfrak{x})^2 \equiv a_\ell(E)^2 \pmod{n}\}.$$

If $\mathfrak{Y}_{\ell,n} = \emptyset$, then the equation (77) has no solutions.

Proof. Suppose that (x, y, k) is a solution to (77) for our particular pair (q, n). We change the sign of x if necessary so that (100) holds and let $x' = \pm x$ so that $x' \equiv 1 \pmod{4}$. By Lemma 15.1, we know that $\overline{\rho}_{G_{x',k},n} \sim \overline{\rho}_{E,n}$. Observe that $G_{x',k}$ is either the same elliptic curve as $G_{x,k}$ if $x' = x$, or it is a quadratic twist by -1 if $x' = -x$. Hence $a_\ell(G_{x,k}) = \pm a_\ell(G_{x',k})$ for any odd prime ℓ of good reduction for either (and hence both) elliptic curves. We let ℓ be a prime satisfying conditions (I), (II) and (III). From (III) and (II), we note that $a_\ell(E) \not\equiv \pm(\ell+1) \pmod{n}$. It follows from Lemma 7.1 that $\ell \nmid y$, and that $a_\ell(G_{x',k}) \equiv a_\ell(E) \pmod{n}$. Thus $a_\ell(G_{x,k})^2 \equiv a_\ell(E)^2 \pmod{n}$. By Lemma 15.5, identity (100) holds where $\mathrm{Norm}(\gamma) = 2^{i-1}y$. In particular, $\mathfrak{L}$ is disjoint from the support of γ and α_q. It follows from (100) that

$$\frac{x - q^k\sqrt{-q}}{x + q^k\sqrt{-q}} \;=\; \left(\frac{\overline{\alpha_q}}{\alpha_q}\right)^{n^*} \cdot \left(\frac{\overline{\gamma}}{\gamma}\right)^n.$$

As g is a generator of $\mathbb{F}_{\mathfrak{L}}^*$ which is cyclic of order $\ell - 1 = tn$, and as $h = g^n$, there is some $0 \le j \le t - 1$ such that $(\overline{\gamma}/\gamma)^n \equiv h^j \pmod{\mathfrak{L}}$. Hence

$$\frac{x - q^k\sqrt{-q}}{x + q^k\sqrt{-q}} \;\equiv\; \mathfrak{r} \pmod{\mathfrak{L}},$$

for some $\mathfrak{r} \in \mathfrak{X}_{\ell,n}$. The Frey–Hellegouarch curve $G_{x,k}$ defined in Lemma 15.1 can be rewritten as

$$Y^2 = X\left(X + 2(x - q^k\sqrt{-q})\right)\left(X + 2(x + q^k\sqrt{-q})\right)$$

and hence modulo $\mathfrak{L}$ is a quadratic twist of $E_{\mathfrak{r}}$. We deduce that $a_{\mathfrak{L}}(E_{\mathfrak{r}})^2 = a_\ell(G_{x,k})^2 \equiv a_\ell(E)^2 \pmod{n}$, whence $\mathfrak{r} \in \mathfrak{Y}_{\ell,n}$. This completes the proof. $\qquad\square$

To finish the proof of Theorem 1, we wrote a `Magma` script which, for each q in (78) and each prime n in the interval $1000 < n < U_q$, found a prime ℓ satisfying conditions (I), (II) and (III), with, further, $\mathfrak{Y}_{\ell,n} = \emptyset$. The following table gives the approximate time taken for this computation, on a single processor.

q	Time	q	Time
7	115 hours	47	988 hours
23	450 hours	71	1058 hours
31	226 hours	79	1019 hours

As one may observe from our proofs, for a given q, the upper bound U_q upon n in equation (77), coming from bounds for linear forms in logarithms, depends strongly upon the class number of $\mathbb{Q}(\sqrt{-q})$. It is this dependence which makes extending Theorem 1 to larger values of q an expensive proposition, computationally.

16. Concluding remarks

There are quite a few additional Frey-Hellegouarch curves at our disposal, that might prove helpful in completing the solution of equation (5), for certain of our problematical values of q. A number of these arise from considering (5) as a special case of

$$x^2 - q^\delta z^\kappa = y^n,$$

where, say, $\kappa \in \{3, 4, 6\}$ and $0 \le \delta < \kappa$. In each case, the dimensions of the spaces of modular forms under consideration grow quickly, complicating matters. This is particularly true if $\kappa \in \{4, 6\}$, where our Frey-Hellegouarch curve will *a priori* be defined over $\mathbb{Q}(\sqrt{q})$, and so the relevant modular forms are Hilbert modular forms which are more challenging to compute than classical modular forms.

In case y is even in equation (5) (whence we are in the situation where our bounds coming from linear forms in logarithms are weaker), we can attach a Frey-Hellegouarch $\mathbb{Q}$-curve to a potential

solution (which at least corresponds to a classical modular form). To do this, write $M = \mathbb{Q}(\sqrt{q})$ and $\mathcal{O}_M$ for the ring of integers of M. Assuming that M has class number one (which is the case for, say, the remaining values $q \in \{41, 89, 97\}$), we have

$$\frac{x + q^k \sqrt{q}}{2} = \delta^r \gamma^{n-2} \alpha^n$$

for some $r \in \mathbb{Z}$ and $\alpha \in \mathcal{O}_M$. Here, δ is a fundamental unit for $\mathcal{O}_M$ and γ is a suitably chosen generator for one of the two prime ideals above 2 in M. From this equation,

$$q^k \sqrt{q} = \delta^r \gamma^{n-2} \alpha^n - \overline{\delta}^r \overline{\gamma}^{n-2} \overline{\alpha}^n.$$

Treating this as a ternary equation of signature $(n, n, 2)$, we can attach to such a solution a Frey–Hellegouarch $\mathbb{Q}$-curve; see for example [44, Section 6]. We will not pursue this here.

17. Acknowledgments

References

[1] S. A. Arif and F. S. Abu Muriefah. On the Diophantine equation $x^2 + q^{2k+1} = y^n$. *J. Number Theory*, 95(1):95–100, 2002.

[2] C. F. Barros. On the Lebesgue–Nagell equation and related subjects. University of Warwick PhD thesis, August 2010.

[3] M. Bauer and M. A. Bennett. Applications of the hypergeometric method to the generalized Ramanujan-Nagell equation. *Ramanujan J.*, 6(2):209–270, 2002.

[4] M. A. Bennett, J. S. Ellenberg, and N. C. Ng. The Diophantine equation $A^4 + 2^\delta B^2 = C^n$. *Int. J. Number Theory*, 6(2):311–338, 2010.

[5] M. A. Bennett, A. Gherga, V. Patel, and S. Siksek. Odd values of the Ramanujan tau function. *Math. Ann.*, 382(1-2):203–238, 2022.

[6] M. A. Bennett and S. Siksek. Differences between perfect powers : The Lebesgue–Nagell equation. to appear in Transactions of the AMS.

[7] M. A. Bennett and C. M. Skinner. Ternary Diophantine equations via Galois representations and modular forms. *Canad. J. Math.*, 56(1):23–54, 2004.

[8] A. Bérczes and I. Pink. On the Diophantine equation $x^2 + p^{2k} = y^n$. *Arch. Math. (Basel)*, 91(6):505–517, 2008.

[9] A. Bérczes and I. Pink. On the Diophantine equation $x^2 + d^{2l+1} = y^n$. *Glasg. Math. J.*, 54(2):415–428, 2012.

[10] Y. Bilu, G. Hanrot, and P. M. Voutier. Existence of primitive divisors of Lucas and Lehmer numbers. *J. Reine Angew. Math.*, 539:75–122, 2001. With an appendix by M. Mignotte.

[11] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. volume 24, pages 235–265. 1997. Computational algebra and number theory (London, 1993).

[12] C. Breuil, B. Conrad, F. Diamond, and R. Taylor. On the modularity of elliptic curves over **Q**: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939, 2001.

[13] Y. Bugeaud. On the Diophantine equation $x^2 - p^m = \pm y^n$. *Acta Arith.*, 80(3):213–223, 1997.

[14] Y. Bugeaud and M. Laurent. Minoration effective de la distance p-adique entre puissances de nombres algébriques. *J. Number Theory*, 61(2):311–342, 1996.

[15] Y. Bugeaud, M. Mignotte, and S. Siksek. Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue-Nagell equation. *Compos. Math.*, 142(1):31–62, 2006.

[16] R. D. Carmichael. On the numerical factors of the arithmetic forms $\alpha^n \pm \beta^n$. *Ann. of Math. (2)*, 15(1-4):49–70, 1913/14.

[17] J. H. E. Cohn. The Diophantine equation $x^4 - Dy^2 = 1$. II. *Acta Arith.*, 78(4):401–403, 1997.

[18] J. H. E. Cohn. The Diophantine equation $x^n = Dy^2 + 1$. *Acta Arith.*, 106(1):73–83, 2003.

[19] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, second edition, 1997.

[20] A. Gherga and S. Siksek. Efficient resolution of Thue-Mahler equations. https://arxiv.org/abs/2207.14492.

[21] E. Halberstadt and A. Kraus. Courbes de Fermat: résultats et problèmes. *J. Reine Angew. Math.*, 548:167–234, 2002.

[22] 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(4):327–338, 2003.

[23] W. Ivorra and A. Kraus. Quelques résultats sur les équations $ax^p + by^p = cz^2$. *Canad. J. Math.*, 58(1):115–153, 2006.

[24] A. Koutsianas. An application of the modular method and the symplectic argument to a Lebesgue-Nagell equation. *Mathematika*, 66(1):230–244, 2020.

[25] A. Kraus. Majorations effectives pour l'équation de Fermat généralisée. *Canad. J. Math.*, 49(6):1139–1161, 1997.

[26] A. Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experiment. Math.*, 7(1):1–13, 1998.

[27] A. Kraus and J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293(2):259–275, 1992.

[28] M. Laurent. Linear forms in two logarithms and interpolation determinants. II. *Acta Arith.*, 133(4):325–348, 2008.

[29] 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(6):125–180, 2000.

[30] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[31] M. Mignotte. A kit on linear forms in three logarithms. `http://www-irma.u-strasbg.fr/~bugeaud/travaux/kit.ps`, 2008.

[32] M. Mignotte and P. Voutier (with an appendix by M. Laurent) A kit for linear forms in three logarithms. https://arxiv.org/pdf/2205.08899.pdf, 2022.

[33] P. Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine Angew. Math.*, 572:167–195, 2004.

[34] A. Pethő, H. G. Zimmer, J. Gebel, and E. Herrmann. Computing all S-integral points on elliptic curves. *Math. Proc. Cambridge Philos. Soc.*, 127(3):383–402, 1999.

[35] S. S. Pillai, On $a^x - b^y = c$, *J. Indian Math. Soc. (N.S.)* , 1936, 2, 119–122.

[36] K. A. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100(2):431–476, 1990.

[37] K. A. Ribet. On the equation $a^p + 2^\alpha b^p + c^p = 0$. *Acta Arith.*, 79(1):7–16, 1997.

[38] J.-P. Serre. Divisibilité de certaines fonctions arithmétiques. In *Séminaire Delange-Pisot-Poitou, 16e année (1974/75), Théorie des nombres, Fasc. 1, Exp. No. 20*, page 28. 1975.

[39] S. Siksek. On the Diophantine equation $x^2 = y^p + 2^k z^p$. *J. Théor. Nombres Bordeaux*, 15(3):839–846, 2003.

[40] S. Siksek. The modular approach to Diophantine equations. In *Explicit methods in number theory*, volume 36 of *Panor. Synthèses*, pages 151–179. Soc. Math. France, Paris, 2012.

[41] N. P. Smart. *The algorithmic resolution of Diophantine equations*, volume 41 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1998.

[42] W. Stein. *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells.

[43] M. Stoll and J. E. Cremona. On the reduction theory of binary forms. *J. Reine Angew. Math.*, 565:79–99, 2003.

[44] J. M. van Langen. On the sum of fourth powers in arithmetic progression. *Int. J. Number Theory*, 17(1):191–221, 2021.

[45] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

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