PERFECT POWERS THAT ARE SUMS OF CONSECUTIVE CUBES

MICHAEL A. BENNETT, VANDITA PATEL, AND SAMIR SIKSEK

ABSTRACT. Euler noted the relation $6^3 = 3^3 + 4^3 + 5^3$ and asked for other instances of cubes that are sums of consecutive cubes. Similar problems have been studied by Cunningham, Catalan, Gennochi, Lucas, Pagliani, Cassels, Uchiyama, Stroeker and Zhongfeng Zhang. In particular Stroeker determined all squares that can be written as a sum of at most 50 consecutive cubes. We generalize Stroeker's work by determining all perfect powers that are sums of at most 50 consecutive cubes. Our methods include descent, linear forms in two logarithms, and Frey-Hellegouarch curves.

1. INTRODUCTION

Euler [6, art. 249], in his 1770 *Vollständige Anleitung zur Algebra*, notes the relation

$$6^3 = 3^3 + 4^3 + 5^3 \tag{1}$$

and asks for other instances of cubes that are sums of three consecutive cubes. Dickson's *History of the Theory of Numbers* gives an extensive survey of early work on the problem of cubes that are sums of consecutive cubes [5, pp. 582–585], and also squares that are sums of consecutive cubes [5, pp. 585–588] with contributions by illustrious names such as Cunningham, Catalan, Gennochi and Lucas. Both problems possess some parametric families of solutions; one such family was constructed by Pagliani [13] in 1829 :

$$\left(\frac{v^5 + v^3 - 2v}{6}\right)^3 = \sum_{i=1}^{v^3} \left(\frac{v^4 - 3v^3 - 2v^2 - 2}{6} + i\right)^3,$$

where the congruence restriction $v \equiv 2$ or $4 \pmod 6$ ensures integrality of the cubes. Pagliani uses this to answer a challenge, posed presumably by the editor Gergonne, of giving 1000 consecutive cubes whose sum is a cube. Of course, the problem of squares that are sums of consecutive cubes possesses the well-known parametric family of solutions

$$\left(\frac{d(d+1)}{2}\right)^2 = \sum_{i=1}^{d} i^3 = \sum_{i=0}^{d} i^3.$$

Date: July 29, 2016.

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

Key words and phrases. Exponential equation, Galois representation, Frey–Hellegouarch curve, modularity, level lowering, linear form in logarithms.

The first-named author is supported by NSERC. The second-named author is supported by an EPSRC studentship. The third-named author is supported by the EPSRC *LMF: L-Functions and Modular Forms* Programme Grant EP/K034383/1.

These questions have continued to be of intermittent interest throughout a period of over 200 years. For example, Lucas [10, page 92] states incorrectly that the only square expressible as a sum of three consecutive positive cubes is

$$6^2 = 1^3 + 2^3 + 3^3. \tag{2}$$

Both Cassels [4] and Uchiyama [19] determine the squares that can be written as sums of three consecutive cubes (without reference to Lucas) showing that the only solutions in addition to (2) are

$$0 = (-1)^3 + 0^3 + 1^3, \qquad 3^2 = 0^3 + 1^3 + 2^3, \qquad 204^2 = 23^3 + 24^3 + 25^3. \tag{3}$$

Lucas also states that the only square that is the sum of two consecutive positive cubes is $3^2 = 1^3 + 2^3$ and the only squares that are sums of 5 consecutive non-negative cubes are

$$10^2 = 0^3 + 1^3 + 2^3 + 3^3 + 4^3, \qquad 15^2 = 1^3 + 2^3 + 3^3 + 4^3 + 5^3,$$
$$315^2 = 25^3 + 26^3 + 27^3 + 28^3 + 29^3, \qquad 2170^2 = 96^3 + 97^3 + 98^3 + 99^3 + 100^3,$$
$$2940^2 = 118^3 + 119^3 + 120^3 + 121^3 + 122^3.$$

These two claims turn out to be correct as shown by Stroeker [18]. In modern language, the problem of which squares are expressible as the sum of d consecutive cubes, reduces for any given $d \geq 2$, to the determination of integral points on a genus 1 curve. Stroeker [18], using a (by now) standard method based on linear forms in elliptic logarithms, solves this problem for $2 \leq d \leq 50$.

The problem of expressing arbitrary perfect powers as a sum of d consecutive cubes with d small has received somewhat less attention, likely due to the fact that techniques for resolving such questions are of a much more recent vintage. Zhongfeng Zhang [21] showed that the only perfect powers that are sums of three consecutive cubes are precisely those already noted by Euler (1), Lucas (2) and Cassels (3). Zhang's approach is write the problem as

$$y^n = (x-1)^3 + x^3 + (x+1)^3 = 3x(x^2+2), \tag{4}$$

and apply a descent argument that reduces this to certain ternary equations that have already been solved in the literature.

In this paper, we extend Stroeker's aforementioned work, determining all perfect powers that are sums of d consecutive cubes, with $2 \leq d \leq 50$. This upper bound is somewhat arbitrary as our techniques extend to essentially any fixed values of d.

Theorem 1. *Let $2 \leq d \leq 50$. Let ℓ be a prime. The integral solutions to the equation*

$$(x+1)^3 + (x+2)^3 + \cdots + (x+d)^3 = y^\ell \tag{5}$$

with $x \geq 1$ are given in Table 1.

The restriction $x \geq 1$ imposed in the statement of Theorem 1 is merely to exclude a multitude of artificial solutions. Solutions with $x \leq 0$ can in fact be deduced easily, as we now explain :

(i) The value $x = 0$ gives the "trivial" solutions $(x, y, \ell) = (0, d(d+1)/2, 2)$, and no solutions for odd ℓ. Likewise the value $x = -1$ yields the trivial solutions $(x, y, \ell) = (-1, (d-1)d/2, 2)$ and no solutions for odd ℓ.

d	(x, y, ℓ)
2	
3	$(22, \pm 204, 2), (2, 6, 3)$
4	$(10, 20, 3)$
5	$(24, \pm 315, 2), (95, \pm 2170, 2), (117, \pm 2940, 2)$
6	
7	$(332, \pm 16296, 2)$
8	$(27, \pm 504, 2)$
9	$(715, \pm 57960, 2)$
10	
11	$(1314, \pm 159060, 2)$
12	$(13, \pm 312, 2)$
13	$(143, \pm 6630, 2), (2177, \pm 368004, 2)$
14	
15	$(24, \pm 720, 2), (3352, \pm 754320, 2), (57959, \pm 54052635, 2)$
16	
17	$(8, \pm 323, 2), (119, \pm 5984, 2), (4887, \pm 1412496, 2)$
18	$(152, \pm 8721, 2), (679, \pm 76653, 2)$
19	$(6830, \pm 2465820, 2)$
20	$(2, 40, 3), (14, 70, 3)$
21	$(13, \pm 588, 2), (143, \pm 8778, 2), (9229, \pm 4070220, 2)$
22	
23	$(12132, \pm 6418104, 2)$
24	
25	$(15587, \pm 9742200, 2), (5, 60, 3)$
26	
27	$(19642, \pm 14319396, 2)$
28	$(80, \pm 4914, 2)$
29	$(24345, \pm 20474580, 2)$
30	
31	$(29744, \pm 28584480, 2)$
32	$(68, \pm 4472, 2), (132, \pm 10296, 2), (495, \pm 65472, 2)$
33	$(32, \pm 2079, 2), (35887, \pm 39081504, 2)$
34	
35	$(224, \pm 22330, 2), (42822, \pm 52457580, 2)$
36	
37	$(50597, \pm 69267996, 2)$
38	
39	$(110, \pm 9360, 2), (59260, \pm 90135240, 2)$
40	$(3275, \pm 1196520, 2)$
41	$(68859, \pm 115752840, 2)$
42	$(63, \pm 5187, 2)$
43	$(79442, \pm 146889204, 2)$
44	
45	$(175, \pm 18810, 2), (91057, \pm 184391460, 2)$
46	
47	$(103752, \pm 229189296, 2)$
48	$(63, \pm 5880, 2), (409, \pm 62628, 2), (19880, \pm 19455744, 2), (60039, \pm 101985072, 2)$
49	$(117575, \pm 282298800, 2), (290, 1155, 3)$
50	$(1224, \pm 312375, 2)$

TABLE 1. The solutions to equation (5) with $2 \leq d \leq 50$, ℓ prime and $x \geq 1$.

(ii) For odd exponents ℓ, there is a symmetry between the solutions to (5) :
$$(x, y, \ell) \longleftrightarrow (-x - d - 1, -y, \ell).$$
This allows us to deduce, from Table 1 and (i), all solutions with $x \leq -d-1$.

(iii) The solutions with $-d \leq x \leq -2$ lead to non-negative solutions with smaller values of d through cancellation (and possibly applying the symmetry in (ii)).

Of course arbitrary perfect powers that are sums of at most 50 consecutive cubes can be deduced from our list of ℓ-th powers with ℓ prime.

A sum of d consecutive cubes can be written as
$$(x+1)^3+(x+2)^3+\cdots+(x+d)^3 = \left(dx + \frac{d(d+1)}{2}\right)\left(x^2 + (d+1)x + \frac{d(d+1)}{2}\right).$$
Thus, to prove Theorem 1, we need to solve the Diophantine equation
$$\left(dx + \frac{d(d+1)}{2}\right)\left(x^2 + (d+1)x + \frac{d(d+1)}{2}\right) = y^\ell, \tag{6}$$
with ℓ prime and $2 \leq d \leq 50$. We find it convenient to rewrite (6) as
$$d(2x + d + 1)\left(x^2 + (d+1)x + \frac{d(d+1)}{2}\right) = 2y^\ell. \tag{7}$$
We will use a descent argument together with the identity
$$4\left(x^2 + (d+1)x + \frac{d(d+1)}{2}\right) - (2x + d + 1)^2 = d^2 - 1. \tag{8}$$
to reduce (7) to a family of ternary equations. The main purpose of this paper is to highlight the degree to which such ternary equations can, through a combination of techniques including descent, lower bounds for linear forms in logarithms, and appeal to the modularity of Galois representations, be nowadays completely and explicitly solved.

We are grateful to the referee for careful reading of the paper and for suggesting several improvements.

2. Proof of Theorem 1 for $\ell = 2$

Although Theorem 1 with $\ell = 2$ follows from Stroeker's paper [18], we explain briefly how this can now be done with the help of an appropriate computer algebra package.

Let (x, y) be an integral solution to (6) with $\ell = 2$. Write $X = dx$, and $Y = dy$. Then (X, Y) is an integral point on the elliptic curve
$$E_d \ : \ Y^2 = \left(X + \frac{d^2 + d}{2}\right)\left(X^2 + (d^2 + d)X + \frac{d^4 + d^3}{2}\right).$$
Using the computer algebra package `Magma` [2], we determined the integral points on E_d for $2 \leq d \leq 50$. For this computation, `Magma` applies the standard linear forms in elliptic logarithms method [17, Chapter XIII], which is the same method used by Stroeker (though the implementation is independent). From this we immediately recover the original solutions (x, y) to (6) with $\ell = 2$, and the latter are found in our Table 1. We have checked that our solutions with $\ell = 2$ are precisely those given by Stroeker.

We shall henceforth restrict ourselves to $\ell \geq 3$.

3. Proof of Theorem 1 for $d = 2$

Our method for general d explained in later sections fails for $d = 2$. This is because of the presence of solutions $(x, y) = (-2, -1)$ and $(x, y) = (-1, 1)$ to (5) for all $\ell \geq 3$. In this section we treat the case $d = 2$ separately, reducing to Diophantine equations that have already been solved by Nagell.

We consider the equation (5) with $d = 2$. For convenience, let $z = x + 1$. The equation becomes $z^3 + (z+1)^3 = y^\ell$ which can be rewritten as

$$(2z+1)(z^2+z+1) = y^\ell. \tag{9}$$

Here y and z are integers and $\ell \geq 3$ is prime. Suppose first that $\ell = 3$. This equation here defines a genus 1 curve. We checked using `Magma` that it is isomorphic to the elliptic curve $Y^2 - 9Y = X^3 - 27$ with Cremona label `27A1`, and that it has Mordell–Weil group (over $\mathbb{Q}$) $\cong \mathbb{Z}/3\mathbb{Z}$. It follows that the only rational points on (9) with $\ell = 3$ are the three obvious ones : $(z, y) = (-1/2, 0)$, $(0, 1)$ and $(-1, -1)$. These yield the solutions $(x, y) = (-1, 1)$ and $(x, y) = (-2, -1)$ to (5).

We may thus suppose that $\ell \geq 5$ is prime. The resultant of the two factors on the left-hand side of (9) is 3 and, moreover, $9 \nmid (z^2 + z + 1)$. It follows that either

$$2z + 1 = y_1^\ell, \qquad z^2 + z + 1 = y_2^\ell, \qquad y = y_1 y_2$$

or

$$2z + 1 = 3^{\ell-1} y_1^n, \qquad z^2 + z + 1 = 3y_2^\ell, \qquad y = 3y_1 y_2.$$

Nagell [12] showed that the only integer solutions to the equation $X^2 + X + 1 = Y^n$ with $n \neq 3^k$ are the trivial ones with $X = -1$ or 0. Nagell [12] also solved the equation $X^2 + X + 1 = 3Y^n$ for $n > 2$ showing that the only solutions are again the trivial ones with $X = 1$. Working back, we see that the only solutions to (9) with $\ell \geq 5$ are $(z, y) = (0, 1)$ and $(-1, -1)$. These again give the solutions $(x, y) = (-1, 1)$ and $(-2, -1)$ to (5).

4. Descent for $\ell \geq 5$

Let $d \geq 3$. We consider equation (7) with exponent $\ell \geq 5$. The argument in this section will need modification for $\ell = 3$ which we carry out in Section 8. For a prime q we let

$$\mu_q = \mathrm{ord}_q(d^2 - 1) \quad \text{and} \quad \nu_q = \mathrm{ord}_q(d), \tag{10}$$

i.e. the largest power of q dividing $d^2 - 1$ and d, respectively. We associate to q a finite subset $T_q \subset \mathbb{Z}^2$ as follows.

- If $q \nmid d(d^2 - 1)$ then let $T_q = \{(0, 0)\}$.
- For $q = 2$ we define

$$T_2 = \begin{cases} \{(0, 1 - \nu_2)\} & \text{if } 2 \mid d \\ \{(1, 0),\ (\mu_2/2, 1 - \mu_2/2),\ (3 - \mu_2, \mu_2 - 2)\} & \text{if } 2 \nmid d \text{ and } 2 \mid \mu_2 \\ \{(1, 0),\ (3 - \mu_2, \mu_2 - 2)\} & \text{if } 2 \nmid d \text{ and } 2 \nmid \mu_2. \end{cases}$$

- For odd $q \mid d$, let

$$T_q = \{(-\nu_q, 0),\ (0, -\nu_q)\}.$$

- For odd $q \mid (d^2-1)$, let

$$T_q = \begin{cases} \{(0,0),\ (-\mu_q, \mu_q),\ (\mu_q/2, -\mu_q/2)\} & \text{if } 2 \mid \mu_q, \\ \{(0,0),\ (-\mu_q, \mu_q)\} & \text{if } 2 \nmid \mu_q. \end{cases}$$

We take $\mathcal{A}_d$ to be the set of pairs of positive rationals (α, β) such that

$$(\mathrm{ord}_q(\alpha), \mathrm{ord}_q(\beta)) \in T_q$$

for all primes q. It is clear that $\mathcal{A}_d$ is a finite set, which is, in practice, easy to write down for any value of d.

Lemma 4.1. *Let (x, y) be a solution to (7) where $\ell \geq 5$ a prime. Then there are rationals y_1, y_2 and a pair $(\alpha, \beta) \in \mathcal{A}_d$ such that*

$$2x + d + 1 = \alpha y_1^{\ell}, \qquad x^2 + (d+1)x + \frac{d(d+1)}{2} = \beta y_2^{\ell}. \tag{11}$$

Moreover, if $3 \leq d \leq 50$ then y_1 and y_2 are integers.

Remark. The reader will observe that the definition of $\mathcal{A}_d$ is independent of ℓ. Thus, given d, the lemma provides us with a way of carrying out the descent uniformly for all $\ell \geq 5$.

Proof. Let us first assume the first part of the lemma and deduce the second. Using a short `Magma` script, we wrote down all possible pairs $(\alpha, \beta) \in \mathcal{A}_d$ for $3 \leq d \leq 50$ and checked that

$$\max\{\mathrm{ord}_q(\alpha),\ \mathrm{ord}_q(\beta)\} \leq 4$$

for all primes q. As x is an integer, we know from (11) that

$$\mathrm{ord}_q(\alpha) + \ell\, \mathrm{ord}_q(y_1) \geq 0 \quad \text{and} \quad \mathrm{ord}_q(\beta) + \ell\, \mathrm{ord}_q(y_2) \geq 0,$$

for all primes q. Since $\ell \geq 5$, it is clear that $\mathrm{ord}_q(y_1) \geq 0$ and $\mathrm{ord}_q(y_2) \geq 0$ for all primes q. This proves the second part of the lemma.

We now prove the first part of the lemma. For $2x + d + 1 = 0$ (which can only arise for odd values of d) we can take $y_1 = 0$, $y_2 = 1$,

$$\alpha = \frac{8}{d(d^2-1)} \quad \text{and} \quad \beta = \frac{d^2-1}{4}; \tag{12}$$

it is easy to check that this particular pair (α, β) belongs to $\mathcal{A}_d$. We shall henceforth suppose that $2x + d + 1 \neq 0$.

Claim: Let q be a prime and define

$$\epsilon = \mathrm{ord}_q(2x + d + 1) \quad \text{and} \quad \delta = \mathrm{ord}_q\left(x^2 + (d+1)x + \frac{d(d+1)}{2}\right).$$

Then $(\epsilon, \delta) \equiv (\epsilon', \delta') \pmod{\ell}$ for some $(\epsilon', \delta') \in T_q$.

To complete the proof of Lemma 4.1, it is clearly enough to prove this claim. From (7) and (8), the claim is certainly true if $q \nmid d(d^2-1)$, so we may suppose that $q \mid d(d^2-1)$. Observe that for any q, from (7),

$$\nu_q + \epsilon + \delta \equiv \mathrm{ord}_q(2) \pmod{\ell}. \tag{13}$$

Moreover, from (8),

$$\mu_q \geq \min(2\epsilon,\ \delta + 2\,\mathrm{ord}_q(2)) \qquad \text{with equality if } \ 2\epsilon \neq \delta + 2\,\mathrm{ord}_q(2). \tag{14}$$

We deal first with the case where $q = 2 \mid d$ (so that $\epsilon = 0$). By (13), we obtain that $(\epsilon, \delta) \equiv (0, 1 - \nu_2) \pmod{\ell}$, and, by definition, $T_2 = \{(0, 1 - \nu_2)\}$ establishing our claim. Next we suppose that $q = 2 \nmid d$ (in which case $\nu_2 = 0$):

- If $2\epsilon = \delta + 2$ then, from (13) and the fact that $\ell \geq 5$, we obtain $(\epsilon, \delta) \equiv (1, 0) \pmod{\ell}$.
- If $2\epsilon > \delta + 2$ then, from (14), we have $\mu_2 = \delta + 2$, so from (13) we obtain $(\epsilon, \delta) \equiv (3 - \mu_2, \mu_2 - 2) \pmod{\ell}$.
- If $2\epsilon < \delta + 2$ then, from (14), we have $\mu_2 = 2\epsilon$, so from (13) we obtain $(\epsilon, \delta) \equiv (\mu_2/2, 1 - \mu_2/2) \pmod{\ell}$.

Next, let us next consider odd $q \mid d$ (whereby we have that $\mu_q = 0$). From (14), it follows that either $\epsilon = 0$ or $\delta = 0$. From (13), we obtain $(\epsilon, \delta) \equiv (0, -\nu_q)$ or $(-\nu_q, 0) \pmod{\ell}$ as required.

Finally we consider odd $q \mid (d^2 - 1)$ (so $\nu_q = 0$):

- If $2\epsilon = \delta$ then, from (13) and the fact that $\ell \geq 5$, we obtain $(\epsilon, \delta) \equiv (0, 0) \pmod{\ell}$.
- If $2\epsilon > \delta$ then, from (14), we have $\mu_q = \delta$, so from (13) we obtain $(\epsilon, \delta) \equiv (-\mu_q, \mu_q) \pmod{\ell}$.
- If $2\epsilon < \delta$ then, from (14), we have $\mu_q = 2\epsilon$, so from (13) we obtain $(\epsilon, \delta) \equiv (\mu_q/2, -\mu_q/2) \pmod{\ell}$.

□

From (11) and (8), we deduce the following ternary equation

$$4\beta y_2^\ell - \alpha^2 y_1^{2\ell} = d^2 - 1. \tag{15}$$

We need to solve this for each possible $(\alpha, \beta) \in \mathcal{A}_d$ with $2 \leq d \leq 50$ and y_1, y_2 integers. Clearing denominators and dividing by the greatest common divisor of the coefficients we can rewrite this as

$$r y_2^\ell - s y_1^{2\ell} = t \tag{16}$$

where r, s, t are positive integers and $\gcd(r, s, t) = 1$.

5. Linear Forms in 2 logarithms

The descent step in the previous section transforms (7) into a family of ternary equations (15). In this section, we appeal to lower bounds for linear forms in logarithms to bound the exponent ℓ appearing in these equations. We will use a special case of Corollary 2 of Laurent [8] (with $m = 10$ in the notation of that paper) :

Proposition 5.1. *Let α_1 and α_2 be positive real, multiplicatively independent algebraic numbers and $\log \alpha_1$, $\log \alpha_2$ be any fixed determinations of their logarithms that are real and positive. Write $D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]$ and*

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

where b_1 and b_2 are positive integers and A_1 and A_2 are real numbers > 1 such that

$$\log A_i \geq \max\{h(\alpha_i), |\log \alpha_i|/D, 1/D\}, \qquad i = 1, 2.$$

Let $\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1$. Then

$$\log|\Lambda| \geq -25.2 D^4 \left(\max\{\log b' + 0.38, 10/D, 1\}\right)^2 \log A_1 \log A_2.$$

Here, we have defined, as usual, the *absolute logarithmic height* of an algebraic number α by

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

where a is the leading coefficient of the minimal polynomial of α and the $\alpha^{(i)}$ are the conjugates of α in $\mathbb{C}$.

In this section, we will assume that $3 \le d \le 50$. In the notation of the previous section, (α, β) will denote an element of $\mathcal{A}_d$ while (y_1, y_2) denotes an integral solution to (15). By definition of $\mathcal{A}_d$, the rationals α and β are both positive. It follows from (15) that $y_2 > 0$.

Lemma 5.2. *Let $\ell > 1000$. Suppose $|y_1|$, $y_2 \ge 2$ and $y_2 \ne y_1^2$. Let*

$$\alpha_1 = 4\beta/\alpha^2 \quad \text{and} \quad \alpha_2 = y_1^2/y_2. \tag{17}$$

Then α_1 and α_2 are positive and multiplicatively independent. Moreover, writing

$$\Lambda = \log\alpha_1 - \ell\log\alpha_2. \tag{18}$$

we have

$$0 < \Lambda < \frac{d^2-1}{\alpha^2 y_1^{2\ell}}. \tag{19}$$

Proof. By the observation preceding the statement of the lemma, we know that α_1 and α_2 are positive. From (15), (17), (18) and (19), we have

$$e^{\Lambda} - 1 = \frac{4\beta}{\alpha^2} \cdot \frac{y_2^{\ell}}{y_1^{2\ell}} - 1 = \frac{d^2-1}{\alpha^2 y_1^{2\ell}} > 0,$$

whence $\Lambda > 0$. The second part of the lemma thus follows from the inequality $e^{\Lambda} - 1 > \Lambda$.

It remains to show the multiplicative independence of α_1 and α_2, so suppose, for a contradiction, that they are are multiplicatively dependent. Thus there exist coprime positive integers u and v such that $\alpha_1^u = \alpha_2^v$. If $\alpha_1 = 1$ then $\alpha_2 = 1$ so that $y_2 = y_1^2$ contradicting the hypotheses of the lemma. Thus $\alpha_1 \ne 1$. Defining

$$g = \gcd\{\mathrm{ord}_p(\alpha_1) \,:\, p \text{ prime}\},$$

as $\alpha_1 \ne 1$, we necessarily have $g \ne 0$. Clearly $v \mid g$. However, from (18),

$$\Lambda = (\log\alpha_1)\left(1 - \ell\frac{\log\alpha_2}{\log\alpha_1}\right) = (\log\alpha_1)\left(1 - \ell\frac{u}{v}\right) = |\log\alpha_1| \cdot \left|1 - \ell\frac{u}{v}\right|.$$

From (19), we have

$$0 < \left|1 - \ell\frac{u}{v}\right| < \frac{d^2-1}{|\log\alpha_1| \cdot \alpha^2 y_1^{2\ell}}.$$

Now the non-zero rational $1 - \ell u/v$ has denominator dividing v and hence dividing g. Thus,

$$\frac{1}{g} \le \left|1 - \ell\frac{u}{v}\right|.$$

Since $|y_1| \ge 2$, it follows that

$$4^{\ell} \le y_1^{2\ell} < \frac{(d^2-1)g}{|\log\alpha_1| \cdot \alpha^2},$$

and so

$$\ell < \log\left(\frac{(d^2-1)g}{|\log\alpha_1|\cdot\alpha^2}\right)/\log 4\,.$$

We wrote a simple `Magma` script that computes this bound on ℓ for the values of d in the range $3 \le d \le 50$ and the possible pairs $(\alpha,\beta) \in \mathcal{A}_d$ with corresponding $\alpha_1 = 4\beta/\alpha^2 \ne 1$. We found that the largest possible value for the right-hand side of the inequality is $19.09\ldots$ corresponding to $d = 50$ and $(\alpha,\beta) = (1/62475, 2499)$. As $\ell > 1000$, we have a contradiction by a wide margin.

In fact, we found only one pair (α,β) for which $\alpha_1 = 1$. This arises when $d = 8$ and $(\alpha,\beta) = (1, 1/4)$. □

Lemma 5.3. *Let $A_2 = \max\{y_1^2, y_2\}$. Under the notation and assumptions of the previous lemma,*

$$1 \;\le\; \frac{\log A_2}{\log y_1^2} \;\le\; 1.03.$$

Proof. It is sufficient to show that $\log y_2/\log y_1^2 \le 1.03$. From (17), (18) and (19), we have

$$\log\alpha_1 - \ell(\log y_1^2 - \log y_2) \;<\; \frac{d^2-1}{\alpha^2\cdot 4^\ell}$$

where we have used the assumption $|y_1| \ge 2$. It follows that

$$\begin{aligned}\frac{\log y_2}{\log y_1^2} &< 1 + \frac{1}{\ell\log y_1^2}\left(-\log\alpha_1 + \frac{(d^2-1)}{\alpha^2\cdot 4^\ell}\right)\\ &\le 1 + \frac{1}{\ell\log y_1^2}\left(|\log\alpha_1| + \frac{(d^2-1)}{\alpha^2\cdot 4^\ell}\right)\\ &< 1 + \frac{1}{1000\log 4}\left(|\log\alpha_1| + \frac{(d^2-1)}{\alpha^2\cdot 4^{1000}}\right),\end{aligned}$$

using the assumptions $\ell > 1000$ and $|y_1| \ge 2$. We wrote a `Magma` script that computed this upper bound for $\log y_1^2/\log y_2$ for all $3 \le d \le 50$ and $(\alpha,\beta) \in \mathcal{A}_d$. The largest value of the upper bound we obtained was $1.02257\ldots$, again corresponding to $d = 50$ and $(\alpha,\beta) = (1/62475, 2499)$. This completes the proof. □

We continue under the assumptions of Lemma 5.2, applying Proposition 5.1 to obtain a bound for the exponent ℓ. We let

$$A_1 = \max\{H(\alpha_1),\, e\},$$

where $H(u/v)$, for coprime integers u, v (with v non-zero) is simply $\max\{|u|, |v|\}$. Let A_2 be as in Lemma 5.3. We see, thanks to Lemma 5.2, that the hypotheses of Proposition 5.1 are satisfied for our choices of α_1, α_2, A_1, A_2 with $D = 1$. We write

$$b' = \frac{1}{\log A_2} + \frac{\ell}{\log A_1} > \frac{1000}{\log A_1}$$

as $\ell > 1000$. We checked that the smallest possible value for $1000/\log A_1$ for $3 \le d \le 50$ and $(\alpha,\beta) \in \mathcal{A}_d$ is $31.95\cdots$ arising from the choice $d = 50$ and $(\alpha,\beta) = (1/62475, 2499)$. From Proposition 5.1,

$$-\log|\Lambda| < 25.2\log A_1\cdot\log A_2\cdot(\log b')^2 \le 25.2\log A_1\cdot\log A_2\cdot\log^2\left(\frac{\ell}{\log A_1} + \frac{1}{\log 4}\right),$$

where we have used the fact that $A_2 \geq y_1^2 \geq 4$. Combining this with (19), we have

$$\ell \log y_1^2 \ < \ \log\left(\frac{d^2-1}{\alpha^2}\right) + 25.2 \log A_1 \cdot \log A_2 \cdot \log^2\left(\frac{\ell}{\log A_1} + \frac{1}{\log 4}\right).$$

Next we divide by $\log y_1^2$, making use of the fact that $\log A_2/\log y_1^2 < 1.03$ and also that $|y_1| \geq 2$, to obtain

$$\ell \ < \ \frac{1}{\log 4}\log\left(\frac{d^2-1}{\alpha^2}\right) + 26 \log A_1 \cdot \log^2\left(\frac{\ell}{\log A_1} + \frac{1}{\log 4}\right).$$

The only remaining variable in this inequality is ℓ. It is a straightforward exercise in calculus to deduce a bound on ℓ for any d, α and β. In fact the largest bound on ℓ we obtain for d in our range is $\ell < 2,648,167$. We summarize the results of this section in the following lemma.

Lemma 5.4. *Let $3 \leq d \leq 50$ and $(\alpha, \beta) \in \mathcal{A}_d$. Let (y_1, y_2) be an integral solution to (15) with $|y_1|$, $y_2 \geq 2$ and $y_2 \neq y_1^2$. Then $\ell < 3 \times 10^6$.*

5.1. **Proof of Theorem 1: bounding ℓ.** We have dealt with the cases $\ell = 2$ and $d = 2$ in Sections 2 and 3 respectively, and so $\ell \geq 3$ and $3 \leq d \leq 50$. We will deal with $\ell = 3$ in Section 8, so suppose $\ell \geq 5$. Lemma 4.1 provides a finite set $\mathcal{A}_d$ of pairs (α, β) such that for every solution (x, y) of (7) there is a pair $(\alpha, \beta) \in \mathcal{A}_d$ and integers (y_1, y_2) satisfying (11), (15) and (16). Lemma 5.4 tells us that $\ell < 3 \times 10^6$ provided the $|y_1|$, $y_2 > 2$ and $y_2 \neq y_1^2$. It is easy to determine (y_1, y_2) for which these conditions fail. Indeed, instead of (15) consider the equivalent (16) with integral coefficients. If $y_2 = y_1^2$ then (16) reduces to $(r-s)y_1^{2\ell} = t$ which allows us to easily determine the corresponding solutions, and similarly for $y_2 = 1$, and for $y_1 \in \{-1, 0, 1\}$. We determined all the solutions (y_1, y_2) where the hypotheses fail for $3 \leq d \leq 50$ and checked that none of these leads to a solution to (7) with $x \geq 1$ integral (for the purpose of proving Theorem 1, we are only interested in $x \geq 1$). Thus we may suppose that the hypotheses of Lemma 5.4 hold and conclude that $\ell < 3 \times 10^6$.

6. A Criterion for the non-existence of solutions

In Section 4, we reduced the problem of solving equation (7) (for $3 \leq d \leq 50$ and prime exponents $\ell \geq 5$) to the resolution of a number of equations of the form (16). In Section 5, we showed that the exponent ℓ is necessarily bounded by 3×10^6. In this section, we will provide a criterion for the non-existence of solutions to (16), given r, s, t and ℓ.

Lemma 6.1. *Let $\ell \geq 3$ be prime. Let r, s and t be positive integers satisfying $\gcd(r, s, t) = 1$. Let $q = 2k\ell + 1$ be a prime that does not divide r. Define*

$$\mu(\ell, q) = \{\eta^{2\ell} \ : \ \eta \in \mathbb{F}_q\} = \{0\} \cup \{\zeta \in \mathbb{F}_q^* \ : \ \zeta^k = 1\} \tag{20}$$

and

$$B(\ell, q) = \left\{\zeta \in \mu(\ell, q) \ : \ ((s\zeta + t)/r)^{2k} \in \{0, 1\}\right\}.$$

If $B(\ell, q) = \emptyset$, then equation (16) does not have integral solutions.

Proof. Suppose $B(\ell, q) = \emptyset$. Let (y_1, y_2) be a solution to (16). Let $\zeta = \overline{y_1}^{2\ell} \in \mu(\ell, q)$. From (16) we have

$$(s\zeta + t)/r \equiv y_2^{\ell} \pmod{q}.$$

Thus

$$((s\zeta+t)/r)^{2k} \equiv y_2^{q-1} \equiv 0 \text{ or } 1 \pmod{q}.$$

This shows that $\zeta \in B(\ell, q)$ giving a contradiction. □

Remark. We now provide a heuristic explanation why Lemma 6.1 should succeed in proving the non-existence of solutions to (16) provided there are no solutions, particularly if ℓ is large. Observe that $\#\mu(\ell, q) = k+1$. For $\zeta \in \mu(\ell, q)$, the element $((s\zeta+t)/r)^{2k} \in \mathbb{F}_q$ is either 0 or an ℓ-th root of unity. Thus the "probability" that it belongs to $\{0, 1\}$ is $2/(\ell+1)$. It follows that the "expected size" of $B(\ell, q)$ is $2(k+1)/(\ell+1) \approx 2q/\ell^2$. For large ℓ we expect to find a prime $q = 2k\ell+1$ such that $2q/\ell^2$ is tiny and so we likewise expect that $\#B(\ell, q) = 0$.

6.1. **Proof of Theorem 1: applying the criterion.** We wrote a `Magma` script which, for each $3 \le d \le 50$, and each $(\alpha, \beta) \in \mathcal{A}_d$ (and corresponding triple of coefficients (r, s, t)), and every prime $5 \le \ell < 3 \times 10^6$, systematically searches for a prime $q = (2k\ell+1) \nmid r$ with $k \le 1000$ such that $B(\ell, q) = \emptyset$. If it finds such a q then by Lemma 6.1 we know that (15) has no solutions, and thus there are no solutions to (7) that give rise to the pair (α, β) via Lemma 4.1. The entire time for the computation was roughly 3 hours on a 2500MHz AMD Opteron. The criterion systematically failed for all exponents $5 \le \ell < 3 \times 10^6$ whenever $4\beta = d^2 - 1$ (equivalently the coefficients of (16) satisfy $r = t$). This failure is unsurprising as equations (15) and (16) have the obvious solution $(y_1, y_2) = (0, 1)$. In all cases where $4\beta \ne d^2 - 1$, the criterion succeeded for all values of ℓ except for a handful of small values. There were a total of 224 quintuples (d, ℓ, r, s, t) with $r \ne t$ for which the criterion fails. The largest value of ℓ in cases $r \ne t$ for which the criterion fails is $\ell = 19$ with $d = 27$, $\alpha = 1/7$, $\beta = 14/27$, and corresponding $r = 2744$, $s = 27$, $t = 963144$.

At this point, to complete the proof of Theorem 1, we thus require another method to handle (16) when $r = t$, and also some new techniques to solve this equation when $r \ne t$, for the remaining small ℓ. The first question is addressed in Section 7, and the second in Section 9.

7. Frey-Hellegouarch Curve for the case $r = t$

In practice, we have found that Lemma 6.1 will eliminate all elements $(\alpha, \beta) \in \mathcal{A}_d$ for any given sufficiently large ℓ except when $\beta = (d^2-1)/4$ (which is equivalent to $r = t$). In this case, equation (15) has the solution $(y_1, y_2) = (0, 1)$ which causes the criterion of Lemma 6.1 fails; for this situation, we would like to show that $(y_1, y_2) = (0, 1)$ is in fact the only solution. In this section, we will thus focus on (15) for $\beta = (d^2-1)/4$, and continue to suppose that $\ell \ge 5$ is prime. It follows from the definition of $\mathcal{A}_d$ that $\alpha = 8/d(d^2-1)$, and moreover that this pair $(\alpha, \beta) = (8/d(d^2-1), (d^2-1)/4)$ arises exactly when either $\mathrm{ord}_2(d) = 0$ or 3. We can rewrite (15) as

$$y_2^\ell - \frac{64}{d^2(d^2-1)^3} \cdot y_1^{2\ell} = 1. \tag{21}$$

We note from (11) that y_1 is even if $\mathrm{ord}_2(d) = 0$ and y_1 is odd if $\mathrm{ord}_2(d) = 3$. By the conclusion of Lemma 4.1, we know that y_1, y_2 are integers. It follows from (21)

that $S \mid y_1$ where

$$\begin{cases} S = \mathrm{Rad}\left(d(d^2-1)\right) & \text{if } \mathrm{ord}_2(d) = 0, \\ S = \mathrm{Rad}_2\left(d(d^2-1)\right)\right) & \text{if } \mathrm{ord}_2(d) = 3. \end{cases}$$

Let $y_1 = Sy_3$. Then, from (21),

$$y_2^\ell - Ty_3^{2\ell} = 1 \tag{22}$$

where

$$T = \frac{64S^{2\ell}}{d^2(d^2-1)^3}.$$

In addition to the assumption $\ell \geq 5$, let us further suppose that

$$2\ell > \mathrm{ord}_q(d^2(d^2-1)^3) \tag{23}$$

for all odd primes q. If $\mathrm{ord}_2(d) = 0$, we will also assume that

$$2\ell \geq 3\,\mathrm{ord}_2(d^2-1) - 1. \tag{24}$$

From assumptions (23) and (24), it follows that T is an integer and that $\mathrm{Rad}(T) = S$. If $\mathrm{ord}_2(d) = 0$, then $2^5 \mid T$. If, however, $\mathrm{ord}_2(d) = 3$, then $\mathrm{ord}_2(T) = 0$ and $2 \nmid y_3 \mid y_1$ so that $2 \mid y_2$. We would like to show that all solutions to (21) satisfy $y_1 = 0$, so suppose $y_1 \neq 0$ (which implies $y_3 \neq 0$). Clearly $y_2 \neq 0$. We associate our solution (y_2, y_3) to the Frey–Hellegouarch curve

$$\begin{cases} E \ : \ Y^2 = X(X+1)(X - Ty_3^{2\ell}) & \text{if } \mathrm{ord}_2(d) = 0, \\ E \ : \ Y^2 = X(X+1)(X + y_2^\ell) & \text{if } \mathrm{ord}_2(d) = 3. \end{cases}$$

The condition $y_2 y_3 \neq 0$ ensures that the given Weierstrass model is smooth. We apply the recipes of Kraus [7] which build on modularity of elliptic curves due to Wiles, Breuil, Conrad, Diamond and Taylor [20], [3], on Ribet's level lowering theorem [14], and on Mazur's theorem [11]. The recipes of Kraus are also reproduced in [15, Section 14.1]. In the notation of that reference, $E \sim_\ell f$ where f is a weight 2 newform of level

$$N = \begin{cases} S & \text{if } \mathrm{ord}_2(d) = 0 \\ 2S & \text{if } \mathrm{ord}_2(d) = 3. \end{cases}$$

If f is irrational (i.e. the Fourier coefficients of f do not all lie in $\mathbb{Q}$) then we can obtain a sharp bound for ℓ as we now explain. Let K be the number field generated by the coefficients of f. For a prime $q \nmid N$, write $a_q(f) \in \mathcal{O}_K$ for the q-th coefficient of f. Let

$$H_q = \{a \in \mathbb{Z} \cap [-2\sqrt{q}, 2\sqrt{q}] \ : \ q + 1 - a \equiv 0 \pmod 4\}.$$

Let

$$B_q(f) = q \cdot \mathrm{Norm}_{K/\mathbb{Q}}((q+1)^2 - a_q(f)^2) \cdot \prod_{a \in H_q} \mathrm{Norm}_{K/\mathbb{Q}}(a - a_q(f)).$$

If $E \sim_\ell f$ then by [15, Proposition 9.1], $\ell \mid B_q(f)$. As f is irrational, there is a positive density of primes $q \nmid N$ such that $a_q(f) \notin \mathbb{Q}$, and so $B_q(f) \neq 0$. This means that we obtain a bound for f, which is practice is quite small. We can usually improve on this bound by choosing a set of primes $\mathcal{Q} = \{q_1, \ldots, q_n\}$ all not dividing N and letting

$$B_{\mathcal{Q}}(f) = \gcd(B_q(f) \ : \ q \in \mathcal{Q}).$$

If $E \sim_\ell f$ then $\ell \mid B_{\mathcal{Q}}(f)$.

Lemma 7.1. *Let $3 \le d \le 50$ with $\mathrm{ord}_2(d) = 0$ or 3. Suppose $\ell \ge 5$ is a prime that satisfies* (23) *for all odd primes q. If $\mathrm{ord}_2(d) = 0$, suppose ℓ also satisfies* (24)*. Let N be as above. Suppose for each irrational newform of weight 2 and level N there is a set of primes $\mathcal{Q}$ not dividing N such that $\ell \nmid B_{\mathcal{Q}}(f)$. Suppose for every elliptic curve F of conductor N there is a prime $q = 2k\ell + 1$, $q \nmid N$, such that*

(i) $B(\ell, q) = \{\overline{0}\}$, where $B(\ell, q)$ is as in the statement of Lemma 6.1;
(ii) $\ell \nmid (a_q(F)^2 - 4)$.

Then

- *if $\mathrm{ord}_2(d) = 3$ then* (7) *has no solutions with $(\alpha, \beta) = (8/d(d^2-1), (d^2-1)/2)$ in Lemma 4.1;*
- *if $\mathrm{ord}_2(d) = 0$ then the only solution to* (7) *with $(\alpha, \beta) = (8/d(d^2-1), (d^2-1)/2)$ in Lemma 4.1 satisfies $x = -(d+1)/2$.*

Proof. The conclusion of the lemma is immediate if $y_1 = 0$ in (11). Let us thus suppose that $y_1 \neq 0$ and attempt to deduce a contradiction. From the above discussion, there is a newform f of level N such that $E \sim_\ell f$, where E is the Frey–Hellegouarch curve. If f is irrational then $\ell \mid B_{\mathcal{Q}}(f)$, which contradicts the hypotheses of the lemma. Thus f is rational and so f corresponds to an elliptic curve $F/\mathbb{Q}$ of conductor N. Thus $E \sim_\ell F$.

Suppose (i). By the proof of Lemma 6.1 we have that $q \mid y_1$. Thus $q \mid y_3$. It follows that E has multiplicative reduction at q. Thus $(q+1) \equiv \pm a_q(F) \pmod{\ell}$. As $q \equiv 1 \pmod{\ell}$ we obtain $4 \equiv a_q(F)^2 \pmod{\ell}$. This contradicts (ii) and completes the proof. □

Remark. In this section, we are concerned with equation (15) with $4\beta = d^2 - 1$, or equivalently equation (16) with $r = t$. These have the solution $(y_1, y_2) = (0, 1)$. It follows from the proof of Lemma 6.1 that $\overline{0} \in B(\ell, q)$ (for any suitable q) and thus $B(\ell, q) \neq \emptyset$. However, in this case, the heuristic remark following the proof of Lemma 6.1 leads us to expect $B(\ell, q) = \{\overline{0}\}$ for sufficiently large ℓ (and suitable q).

7.1. **Proof of Theorem 1: the case $r = t$.** We wrote a `Magma` script which, for each $3 \le d \le 50$ with $\mathrm{ord}_2(d) = 0$ or 3, computes the newforms of weight 2, level N. Our script take $\mathcal{Q}$ to be set of primes < 100 that do not divide N, and computes $B_{\mathcal{Q}}(f)$ for each irrational eigenform f at level N. These unsurprisingly are all non-zero. For every prime $5 \le \ell < 3 \times 10^6$ that does not divide any of the $B_{\mathcal{Q}}(f)$, and satisfies inequality (23), and also inequality (24) if $\mathrm{ord}_2(d) = 0$, and for every isogeny class of elliptic curves F of conductor N, the script systematically searches for a prime $q = (2k\ell + 1) \nmid r$ with $k \le 1000$ such that conditions (i) and (ii) of Lemma 7.1 hold. If it finds such a q we know that there are no solutions to (7) that give rise to the pair $(\alpha, \beta) = (8/d(d^2-1), (d^2-1)/2)$ via Lemma 7.1. The entire time for the computation was roughly 2.5 hours on a 2500MHz AMD Opteron. In all cases the criterion succeeded for all values of ℓ except for a handful of small values. There were a total of 53 quintuples (d, ℓ, r, s, t) with $r = t$ for which either ℓ does not satisfy the inequalities (23), (24), or it divides $B_{\mathcal{Q}}(f)$ for some irrational eigenform, or for which the script did not find a suitable q that satisfies (i), (ii). The largest value of ℓ among the 53 quintuples is $\ell = 19$: with $d = 37$, $r = t = 54762310872$, $s = 1$, and with $d = 40$, $r = t = 102208119975$, $s = 1$.

8. Descent for $\ell = 3$

In this section we modify the approach of Section 4 to deal with equation (7) with exponent $\ell = 3$.

For an integer m, we denote by $[m]$ the element in $\{0, 1, 2\}$ such that $m \equiv [m] \pmod 3$. For a prime q we let μ_q and ν_q be as in (10). For each prime q, we define a finite subset $T_q \subset \{(m, n) : m, n \in \{0, 1, 2\}\}$.

- If $q \nmid d(d^2 - 1)$ then let $T_q = \{(0, 0)\}$.
- For $q = 2$ we let

$$T_2 = \begin{cases} \{(0, [1 - \nu_2])\} & \text{if } 2 \mid d \\ \{(1, 0),\ (0, 1),\ (2, 2)\} & \text{if } 2 \nmid d \text{ and } \mu_2 \geq 4. \\ \{(1, 0),\ (0, 1)\} & \text{if } 2 \nmid d \text{ and } \mu_2 = 3. \end{cases}$$

- For odd $q \mid d$, let

$$T_q = \{([-\nu_q],\ 0),\ (0,\ [-\nu_q])\}.$$

- For odd $q \mid (d^2 - 1)$, let

$$T_q = \begin{cases} \{(0, 0),\ (1, 2),\ (2, 1)\} & \text{if } \mu_q \geq 2 \\ \{(0, 0),\ (2, 1)\} & \text{if } \mu_q = 1. \end{cases}$$

Let $\mathcal{A}_d$ be the set of pairs of positive integers (α, β) such that $(\mathrm{ord}_q(\alpha), \mathrm{ord}_q(\beta)) \in T_q$ for all primes q.

Lemma 8.1. *Let (x, y) be a solution to (7) where $\ell = 3$ a prime. Then there are integers y_1, y_2 and a pair $(\alpha, \beta) \in \mathcal{A}_d$ such that (11) holds.*

Proof. The proof is an easy adaptation of the proof of Lemma 4.1. We omit the details. □

8.1. **Proof of Theorem 1: descent for $\ell = 3$.** From this lemma and (8) we reduce the resolution of (7) with $\ell = 3$ to solving a number of equations of the form (15). These can be transformed by clearing denominators and dividing by the greatest common divisor of the coefficients into equations of the form (16) where r, s, t are positive integers and $\gcd(r, s, t) = 1$. An implementation of above procedure leaves us with 942 quintuples (d, ℓ, r, s, t) with $\ell = 3$.

We emphasize in passing the difference between the approach of Section 4 and that of this section; the former gives the same set of triples (r, s, t) for all exponents $\ell \geq 5$, whereas the latter gives a possibly different set of triples (r, s, t) for $\ell = 3$.

9. Completing the proof of Theorem 1

Looking back at 6.1, 7.1 and 8.1 we see that, to complete the proof of Theorem 1, we need to solve $224 + 53 + 942 = 1219$ equations of the form (16) with r, s and t positive integers and $\gcd(r, s, t) = 1$. In the second column of Table 2 we give a breakdown of these equations according to the exponent ℓ. In what follows we look at three methods of eliminating or solving these equations.

Exponent ℓ	original number of equations (16) with exponent ℓ	number surviving after local solubility tests	number surviving after further descent
3	942	393	223
5	179	63	3
7	77	35	0
11	10	7	0
13	5	4	0
17	3	2	0
19	3	3	0
Total	1219	507	226

TABLE 2. In Sections 6.1, 7.1 and 8.1 we have reduced the proof of Theorem 1 to the resolution of 1219 equations of the form (16). The first second column gives a breakdown of this number according to the exponent ℓ. The third column gives the number of these equations surviving the local solubility tests of Section 9.1, and the fourth column gives the number that also survive the further descent of Section 9.2.

9.1. **Local Solubility.** Recall that $\gcd(r,s,t)=1$ in (16). Write $g=\mathrm{Rad}(\gcd(r,t))$ and suppose that $g>1$. Then $g \mid y_1$, and we can write $y_1=gy_1'$, and thus

$$ry_2^\ell - sg^{2\ell}{y_1'}^{2\ell} = t.$$

Now we may remove a factor of g from the coefficients to obtain

$$r'{y_2}^\ell - s'{y_1'}^{2\ell} = t',$$

where $t'=t/g<t$. Likewise, if $h=\gcd(s,t)>1$, we obtain an equation

$$r'{y_2'}^\ell - s'{y_1}^{2\ell} = t',$$

Likewise where $t'=t/h<t$. We apply these operations repeatedly until we arrive at an equation of the form

$$R\rho^\ell - S\sigma^{2\ell} = T \tag{25}$$

where R, S, T are pairwise coprime. A necessary condition for the existence of solutions is that for any odd prime $q \mid R$, the residue $-ST$ modulo q is a square. Besides this simple test we check for local solubility at the primes dividing R, S, T, and the primes $q \le 19$. We subjected all of the 1219 equations to these local solubility tests. These have allowed us to eliminate 712 equations, leaving 507 equations. A breakdown of these according to the exponent ℓ is given in the third column of Table 2.

9.2. **A Further Descent.** If local solubility fails to rule out solutions then we carry out a descent to do so. Specifically, let

$$S' = \prod_{\mathrm{ord}_q(S) \text{ is odd}} q.$$

Thus $SS' = v^2$. Write $RS' = u$ and $TS' = mn^2$ with m squarefree. We may now rewrite (25) as

$$(v\sigma^\ell + n\sqrt{-m})(v\sigma^\ell - n\sqrt{-m}) = u\rho^\ell.$$

Let $K = \mathbb{Q}(\sqrt{-m})$ and $\mathcal{O}$ be its ring of integers. Let $\mathfrak{S}$ be the prime ideals of $\mathcal{O}$ that divide u or $2n\sqrt{-m}$. Clearly $(v\sigma^\ell + n\sqrt{-m})K^{*\ell}$ belongs to the "ℓ-Selmer group"

$$K(\mathfrak{S}, \ell) = \{\epsilon \in K^*/K^{*\ell} \, : \, \mathrm{ord}_{\mathcal{P}}(\epsilon) \equiv 0 \pmod{\ell} \text{ for all } \mathcal{P} \notin \mathfrak{S}\}.$$

This is an $\mathbb{F}_\ell$-vector space of finite dimension and, for a given ℓ, easy to compute from class group and unit group information (see [16, Proof of Proposition VIII.1.6]). Let

$$\mathcal{E} = \{\epsilon \in K(\mathfrak{S}, \ell) \, : \, \mathrm{Norm}(\epsilon)/u \in \mathbb{Q}^{*\ell}\}.$$

It follows that

$$v\sigma^\ell + n\sqrt{-m} = \epsilon\eta^\ell, \tag{26}$$

where $\eta \in K^*$ and $\epsilon \in \mathcal{E}$.

Lemma 9.1. *Let $\mathfrak{q}$ be a prime ideal of K. Suppose one of the following holds:*

(i) $\mathrm{ord}_{\mathfrak{q}}(v)$, $\mathrm{ord}_{\mathfrak{q}}(n\sqrt{-m})$, $\mathrm{ord}_{\mathfrak{q}}(\epsilon)$ *are pairwise distinct modulo ℓ;*
(ii) $\mathrm{ord}_{\mathfrak{q}}(2v)$, $\mathrm{ord}_{\mathfrak{q}}(\epsilon)$, $\mathrm{ord}_{\mathfrak{q}}(\overline{\epsilon})$ *are pairwise distinct modulo ℓ;*
(iii) $\mathrm{ord}_{\mathfrak{q}}(2n\sqrt{-m})$, $\mathrm{ord}_{\mathfrak{q}}(\epsilon)$, $\mathrm{ord}_{\mathfrak{q}}(\overline{\epsilon})$ *are pairwise distinct modulo ℓ.*

Then there is no $\sigma \in \mathbb{Z}$ and $\eta \in K$ satisfying (26).

Proof. Suppose (i) holds. Then the three terms in (26) have pairwise distinct valuations, so (26) is impossible $\mathfrak{q}$-adically. If (ii) or (iii), then we apply the same idea to

$$2v\sigma^\ell = \epsilon\,\eta^\ell + \overline{\epsilon}\,\overline{\eta}^\ell, \qquad 2n\sqrt{-m} = \epsilon\,\eta^\ell - \overline{\epsilon}\,\overline{\eta}^\ell,$$

which follow from (26), and its conjugate equation. □

Lemma 9.2. *Let $q = 2k\ell + 1$ be a prime. Suppose $q\mathcal{O} = \mathfrak{q}_1\mathfrak{q}_2$ where $\mathfrak{q}_1$, $\mathfrak{q}_2$ are distinct, and such that* $\mathrm{ord}_{\mathfrak{q}_j}(\epsilon) = 0$ *for $j = 1, 2$. Let*

$$\chi(\ell, q) = \{\eta^\ell \, : \, \eta \in \mathbb{F}_q\}.$$

Let

$$C(\ell, q) = \{\zeta \in \chi(\ell, q) \, : \, ((v\zeta + n\sqrt{-m})/\epsilon)^{2k} \equiv 0 \text{ or } 1 \pmod{\mathfrak{q}_j} \text{ for } j = 1, 2\}.$$

Suppose $C(\ell, q) = \emptyset$. Then there is no $\sigma \in \mathbb{Z}$ and $\eta \in K$ satisfying (26).

Proof. The proof is a straightforward modification of the proof of Lemma 6.1. □

We have found Lemmata 9.1 and 9.2 useful in eliminating many, and often all, $\epsilon \in \mathcal{E}$. Of course if they succeed in eliminating all $\epsilon \in \mathcal{E}$ then we know that (25) has no solutions, and so the same would be true for (16). Of course, when $r = t$, equation (16) always has a solution, namely $(y_1, y_2) = (0, 1)$. For $r = t$, the reduction process in 9.1 leads to equation (25) with $R = T = 1$. The solution $(y_1, y_2) = (0, 1)$ to (16) corresponds to the solution $(\rho, \sigma) = (1, 0)$ in (25). It follows from (26) that $n\sqrt{-m}K^{*\ell} \in \mathcal{E}$. Naturally, Lemma 9.1 and Lemma 9.2 do not eliminate the case $\epsilon = n\sqrt{-m}$ since equation (26) has the solution with $\sigma = 0$ and $\eta = 1$. In this case, our interest is in showing that this is the only solution.

Lemma 9.3. *Suppose*

(i) $\mathrm{ord}_{\mathfrak{q}}(n\sqrt{-m}) < \ell$ *for all prime ideals* $\mathfrak{q}$ *of* $\mathcal{O}$*;*
(ii) the polynomial $X^\ell + (d-X)^\ell - 2$ *has no roots in* $\mathcal{O}$ *for* $d = 1, -1, -2$*;*
(iii) the only root of the polynomial $X^\ell + (2-X)^\ell - 2$ *in* $\mathcal{O}$ *is* $X = 1$*.*

Then, for $\epsilon = n\sqrt{-m}$*, the only solution to* (26) *with* $\sigma \in \mathbb{Z}$ *and* $\eta \in K$ *is* $\sigma = 0$ *and* $\eta = 1$*.*

Proof. Let $\epsilon = n\sqrt{-m}$ and suppose $\sigma \in \mathbb{Z}$ and $\eta \in K$ is a solution to (26). Note that the left-hand side of (26) belongs to $\mathcal{O}$, and from (i), we deduce that $\eta \in \mathcal{O}$. Now substracting (26) from its conjugate and dividing by $n\sqrt{-m}$ leads to the equation

$$\eta^\ell + \overline{\eta}^\ell = 2.$$

We deduce that the rational integer $\eta + \overline{\eta}$ divides 2 and hence $\eta + \overline{\eta} = d$ where $d = \pm 1, \pm 2$. Thus η is a root of $X^\ell + (d-X)^\ell - 2$ for one of these values of d. By (ii), (iii) it follows that $d = 2$ and $\eta = 1$. From (26) we see that $\sigma = 0$. □

For each of the 507 equations (16) that survive the local solubility tests in Section 9.1, we computed the set $\mathcal{E}$ and applied the criteria in Lemma 9.1 and Lemma 9.2 (the latter with $k \leq 1000$) to eliminate as many of the $\epsilon \in \mathcal{E}$ as possible. If the two lemmata succeed in eliminating all possible values of ϵ then (25) has no solutions, and therefore equation (16) does not have solutions either. If they succeeded in eliminating all but one value $\epsilon \in \mathcal{E}$, and that value is $n\sqrt{-m}$, then we checked the conditions of Lemma 9.3 which if satisfied allow us to conclude that $\sigma = 0$ and therefore $y_1 = 0$. Recall that Theorem 1 is concerned with (7) with $x \geq 1$. If $y_1 = 0$ then $x = -(d+1)/2$ (via (11)) and so we can eliminate (r, s, t) if Lemmata 9.1, 9.2 and 9.3 allow us to conclude that $\sigma = 0$. Using this method, we managed to eliminate 281 of the 507 equations (16), leaving just 226 equations. In Table 2 we provide a breakdown of these according to the the exponent ℓ.

9.3. **A Thue Approach.** Finally, writing $\tau = \sigma^2$ in (25) we obtain the (binomial) Thue equation

$$R\rho^\ell - S\tau^\ell = T.$$

We solved the remaining 226 equations using the the Thue equation solver in `Magma`. The theory behind this Thue equation solver is discussed in [17, Chapter VII]. As we see from Table 2, we are left with the problem of solving 223 Thue equations of degree 3, and three Thue equations of degree 5. Working backwards from these solutions, we obtained precisely six solutions to (7) with $x \geq 1$. These are

$$3^3 + 4^3 + 5^3 = 6^3, \qquad 11^3 + 12^3 + 13^3 + 14^3 = 20^3,$$
$$3^3 + 4^3 + 5^3 + \cdots + 22^3 = 40^3,$$
$$15^3 + 16^3 + 17^3 + \cdots + 34^3 = 70^3,$$
$$6^3 + 7^3 + 8^3 + \cdots + 30^3 = 60^3,$$
$$291^3 + 292^3 + 293^3 + \cdots + 229^3 = 1115^3.$$

Noting that these solutions are in Table 1, this completes the proof of Theorem 1.

References

[1] K. Belabas, F. Beukers, P. Gaudry, H. Lenstra, W. McCallum, B. Poonen, S. Siksek, M. Stoll, M. Watkins, *Explicit Methods in Number Theory: Rational Points and Diophantine Equations*, Panoramas et synthèses **36**, Société Mathématique de France, Paris, 2012.

[2] W. Bosma, J. Cannon and C. Playoust, *The Magma Algebra System I: The User Language*, J. Symb. Comp. **24** (1997), 235–265. (See also `http://magma.maths.usyd.edu.au/magma/`)
[3] C. Breuil, B. Conrad, F. Diamond and R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), 843–939.
[4] J. W. S. Cassels, *A Diophantine equation*, Glasgow Math. Journal **27** (1985), 11–88.
[5] L. E. Dickson, *History of the theory of numbers*, volume II, Chelsea, New York, 1971.
[6] L. Euler, *Vollständige Anleitung zur Algebra*, volume 2, St. Petersburg, 1770.
[7] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Canad. J. Math. **49** (1997), 1139–1161.
[8] M. Laurent, *Linear forms in two logarithms and interpolation determinants. II*, Acta Arith. **133** (2008), 325–348.
[9] W. Ljunggren, *Noen Setninger om ubestemte likninger av formen* $(x^n-1)/(x-1) = y^q$, Norsk. Mat. Tidsskr. **25** (1943), 17–20.
[10] E. Lucas, *Researches sur l'analyse indéterminée et l'arithmétique de Diophante*, Moulin, 1873.
[11] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. 44 (1978), 129–162.
[12] T. Nagell, *Des équations indéterminées* $x^2 + x + 1 = y^n$ *et* $x^2 + x + 1 = 3y^n$ Norsk Mat. Forenings Skr. **1** (1921), no. 2, 14 pages.
[13] C. Pagliani, *Solution du problème d'analyse indéterminée énoncé à la pag. 212 du présent volume*, Annales de Mathématiques pures et appliquées **20** (1829-1830), 382–384.
[14] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), 431–476.
[15] S. Siksek, *The modular approach to Diophantine equations*, pages 151–179 of [1].
[16] J. H. Silverman, *Arithmetic of Elliptic Curves*, second edition, Graduate Texts in Mathematics **106** Springer-Verlag, New York, 2008.
[17] N. P. Smart, *The Algorithmic Resolution of Diophantine Equations*, London Mathematical Society Student Texts **41**, Cambridge University Press, 1997.
[18] R. J. Stroeker, *On the sum of consecutive cubes being a square*, Compositio Mathematica **97** (1995), 295–307.
[19] S. Uchiyama, *On a Diophantine equation*, Proc. Japan Acad. Ser. A Math. Sci. **55** (1979), no. 9, 367–369.
[20] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. **141** (1995), 443–551.
[21] Z. Zhang, *On the Diophantine equation* $(x-1)^k + x^k + (x+1)^k = y^n$, Publ. Math. Debrecen **85** (2014), 93–100.

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

Mathematics Institute, University of Warwick, Coventry CV4 7AL, United Kingdom
E-mail address: `vandita.patel@warwick.ac.uk`

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