GENERALIZED FERMAT EQUATIONS : A MISCELLANY

MICHAEL A. BENNETT, IMIN CHEN, SANDER R. DAHMEN AND SOROOSH YAZDANI

Abstract. This paper is devoted to the generalized Fermat equation $x^p + y^q = z^r$, where p, q and r are integers, and x, y and z are nonzero coprime integers. We begin by surveying the exponent triples (p, q, r), including a number of infinite families, for which the equation has been solved to date, detailing the techniques involved. In the remainder of the paper, we attempt to solve the remaining infinite families of generalized Fermat equations that appear amenable to current techniques. While the main tools we employ are based upon the modularity of Galois representations (as is indeed true with all previously solved infinite families), in a number of cases we are led via descent to appeal to a rather intricate combination of multi-Frey techniques.

Contents

Date: June 2014.

2010 *Mathematics Subject Classification.* Primary: 11D41, Secondary: 11D61, 11G05, 14G05.

Key words and phrases. Fermat equations, Galois representations, $\mathbb{Q}$-curves, multi-Frey techniques.

Research supported by NSERC. The third author is supported by an NWO-Veni grant.

1. Introduction

Since Wiles' [89] remarkable proof of Fermat's Last Theorem, a number of techniques have been developed for solving various generalized Fermat equations of the shape

$$a^p + b^q = c^r \quad \text{with} \quad \frac{1}{p} + \frac{1}{q} + \frac{1}{r} \leq 1, \tag{1}$$

where p, q and r are positive integers, and a, b and c are coprime integers. The *Euclidean* case, when $1/p + 1/q + 1/r = 1$, is well understood (see e.g. Proposition 6) and hence the main topic of interest is when $1/p+1/q+1/r < 1$, the *hyperbolic* case. The number of solutions (a, b, c) to such an equation is known to be finite, via work of Darmon and Granville [39], provided we fix the triple (p, q, r). It has, in fact, been conjectured that there are only finitely many nonzero coprime solutions to equation (1), even allowing the triples (p, q, r) to be variable (counting solutions corresponding to $1^p + 2^3 = 3^2$ just once). Perhaps the only solutions are those currently known; i.e. (a, b, c, p, q, r) coming from the solution to Catalan's equation $1^p + 2^3 = 3^2$, for $p \geq 6$, and from the following nine identities :

$$2^5 + 7^2 = 3^4, \quad 7^3 + 13^2 = 2^9, \quad 2^7 + 17^3 = 71^2, \quad 3^5 + 11^4 = 122^2, \quad 17^7 + 76271^3 = 21063928^2,$$
$$1414^3 + 2213459^2 = 65^7, \quad 9262^3 + 15312283^2 = 113^7, \quad 43^8 + 96222^3 = 30042907^2,$$
$$\text{and} \quad 33^8 + 1549034^2 = 15613^3.$$

Since all known solutions have $\min\{p, q, r\} \leq 2$, a similar formulation of the aforementioned conjecture, due to Beal (see [67]), is that there are no nontrivial solutions in coprime integers to (1), once we assume that $\min\{p, q, r\} \geq 3$. For references on the history of this problem, the reader is directed to the papers of Beukers [10], [11], Darmon and Granville [39], Mauldin [67] and Tijdeman [88], and, for more classical results along these lines, to the book of Dickson [41].

Our goals in this paper are two-fold. Firstly, we wish to treat the remaining cases of equation (1) which appear within reach of current technology (though, as a caveat, we will avoid discussion of exciting recent developments involving Hilbert modular forms [43], [47], [48], [49] in the interest of keeping our paper reasonably self-contained). Secondly, we wish to take this opportunity to document what, to the best of our knowledge, is the state-of-the-art for these problems. Regarding the former objective, we will prove the following two theorems :

Theorem 1. *Suppose that (p,q,r) are positive integers with $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$ and*

$$(p,q,r) \in \{(2,n,6),(2,2n,9),(2,2n,10),(2,2n,15),(3,3,2n),(3,6,n),(4,2n,3)\}$$

for some integer n. Then equation (1) has no solutions in coprime nonzero integers a,b and c.

Proof. These seven cases will be dealt with in Propositions 13, 19, 21, 22, 27, 9 and 23 respectively. □

Theorem 2. *Suppose that (p,q,r) are positive integers with $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$ and*

$$(p,q,r) = \begin{cases} (2m,2n,3), & n \equiv 3 \pmod 4, \quad m \geq 2, \quad \textit{or} \\ (2,4n,3), & n \equiv \pm 2 \pmod 5 \quad \textit{or} \quad n \equiv \pm 2, \pm 4 \pmod{13}. \end{cases}$$

Then the only solution to equation (1) in coprime nonzero integers a,b and c is with $(p,q,r,|a|,|b|,c) = (2,8,3,1549034,33,15613)$.

Proof. The first case will be treated in Proposition 18. The second is Proposition 24. □

Taking these results together with work of many other authors over the past twenty years or so, we currently know that equation (1) has only the known solutions for the following triples (p,q,r); in the first table, we list infinite families for which the desired results are known without additional conditions.

(p, q, r)	reference(s)
$(n, n, n), \ n \geq 3$	Wiles [89], Taylor-Wiles [87]
$(n, n, 2), \ n \geq 4$	Darmon-Merel [40], Poonen [71]
$(n, n, 3), \ n \geq 3$	Darmon-Merel [40], Poonen [71]
$(2n, 2n, 5), \ n \geq 2$	Bennett [1]
$(2, 4, n), \ n \geq 4$	Ellenberg [46], Bennett-Ellenberg-Ng [5], Bruin [17]
$(2, 6, n), \ n \geq 3$	Bennett-Chen [2], Bruin [17]
$(2, n, 4), \ n \geq 4$	immediate from Bennett-Skinner [8], Bruin [19]
$(2, n, 6), \ n \geq 3$	Theorem 1, Bruin [17]
$(3j, 3k, n), \ j, k \geq 2, n \geq 3$	immediate from Kraus [60]
$(3, 3, 2n), \ n \geq 2$	Theorem 1
$(3, 6, n), \ n \geq 2$	Theorem 1
$(2, 2n, k), \ n \geq 2, \ k \in \{9, 10, 15\}$	Theorem 1
$(4, 2n, 3), \ n \geq 2$	Theorem 1

(p, q, r)	reference(s)
$(3, 3, n)^*$	Chen-Siksek [26], Kraus [60], Bruin [18], Dahmen [30]
$(2, 2n, 3)^*$	Chen [23], Dahmen [30], [31], Siksek [81] [83]
$(2, 2n, 5)^*$	Chen [24]
$(2m, 2n, 3)^*$	Theorem 2
$(2, 4n, 3)^*$	Theorem 2
$(3, 3n, 2)^*$	Bennett-Chen-Dahmen-Yazdani [3]
$(2, 3, n), \ 6 \leq n \leq 9$	Poonen-Schaefer-Stoll [72], Bruin [17], [19], [20],
$(2, 3, n), \ n \in \{10, 15\}$	Brown [16], Siksek [83], Siksek-Stoll [85]
$(3, 4, 5)$	Siksek-Stoll [84]
$(5, 5, 7), \ (5, 5, 19), \ (7, 7, 5)$	Dahmen-Siksek [32]

The $(*)$ in the second table indicates that the result has been proven for a family of exponents of natural density one (but that there remain infinitely many prime exponents of positive Dirichlet density untreated). The following table provides the exact conditions that the exponents must satisfy.

(p,q,r)	n
$(3,3,n)$	$3 \leq n \leq 10^4$, or $n \equiv 2,3 \pmod 5$, $n \equiv 17,61 \pmod{78}$, $n \equiv 51,103,105 \pmod{106}$, or $n \equiv 43,49,61,79,97,151,157,169,187,205,259,265,277,295,313$ $367,373,385,403,421,475,481,493,511,529,583,601,619,637,$ $691,697,709,727,745,799,805,817,835,853,907,913,925,943,961,$ $1015,1021,1033,1051,1069,1123,1129,1141,1159,1177,1231,1237,$ $1249,1267,1285 \pmod{1296}$
$(2,2n,3)$	$3 \leq n \leq 10^7$ or $n \equiv -1 \pmod 6$
$(2m,2n,3)$	$m \geq 2$ and $n \equiv -1 \pmod 4$
$(2,4n,3)$	$n \equiv \pm 2 \pmod 5$ or $n \equiv \pm 2, \pm 4 \pmod{13}$
$(2,2n,5)$	$n \geq 17$ and $n \equiv 1 \pmod 4$ prime
$(3,3n,2)$	$n \equiv 1 \pmod 8$ prime.

Remark 3. *We do not list in these tables examples of equation (1) which can be solved under additional local conditions (such as, for example, the case $(p,q,r) = (5,5,n)$ with c even, treated in an unpublished note of Darmon and Kraus). We will also not provide information on generalized versions of (1) such as equations of the shape $Aa^p + Bb^q = Cc^r$, where A, B and C are integers whose prime factors lie in a fixed finite set. Regarding the latter, the reader is directed to* [25], [39], [44], [51], [61], [62], [69] *(for general signatures),* [58], [59] *(for signature (p,p,p)),* [7], [8], [29], [53], [54], [55] *(for signature $(p,p,2)$),* [9], [63] *(for signature $(p,p,3)$), and to* [6], [12], [13], [28], [42], [43] *and* [47] *(for various signatures of the shape (n,n,p) with n fixed).*

Remark 4. *In* [32]*, equation (1) with signatures $(5,5,11),(5,5,13)$ and $(7,7,11)$ is solved under the assumption of (a suitable version of) the Generalized Riemann Hypothesis. In each case, with sufficiently large computation, such a result can be made unconditional (and may, indeed, be so by the time one reads this).*

Remark 5. *Recent advances in proving modularity over totally real fields have enabled one to solve equations of the shape (1) over certain number fields. An early result along these lines is due to Jarvis and Meekin* [56]*, which proves such a result for signatures (n,n,n) over $\mathbb{Q}(\sqrt{2})$, while a striking recent paper of Freitas and Siksek* [49] *extends this to a positive proportion of all real quadratic fields.*

In each of the cases where equation (1) has been treated for an infinite family of exponents, the underlying techniques have been based upon the modularity of Galois representations. The limitations of this approach are unclear at this time, though work of Darmon and Granville (e.g. Proposition 4.2 of [39]; see also the discussion in [2]) suggests that restricting attention to Frey-Hellegouarch curves over $\mathbb{Q}$ (or, for that matter, to $\mathbb{Q}$-curves) might enable us to treat only signatures which can be related via descent to one of

$$(p, q, r) \in \{(n, n, n), (n, n, 2), (n, n, 3), (2, 3, n), (3, 3, n)\}. \tag{2}$$

Of course, as demonstrated by the striking work of Ellenberg [46] (and, to a lesser degree, by Theorems 1 and 2), there are some quite nontrivial cases of equations of the shape (1) which may be reduced to the study of the form $Aa^p + Bb^q = Cc^r$ for signatures (p, q, r) in (2). By way of example, if we wish to treat the equation $x^2 + y^4 = z^n$, we may, as in [46], factor the left-hand-side of this equation over $\mathbb{Q}(i)$ to conclude that both $y^2 + ix$ and $y^2 - ix$ are essentially n-th powers in $\mathbb{Q}(i)$. Adding $y^2 + ix$ to $y^2 - ix$ thus leads to an equation of signature $(n, n, 2)$.

For more general signatures, an ambitious program of Darmon [36], based upon the arithmetic of Frey-Hellegouarch abelian varieties, holds great promise for the future, though, in its full generality, perhaps not the near future.

By way of notation, in what follows, when we reference a *newform* f, we will always mean a cuspidal newform of weight 2 with respect to $\Gamma_0(N)$ for some positive integer N.This integer will be called the *level* of f.

2. The Euclidean Case

For convenience in the sequel, we will collect together a number of old results on the equation $a^p + b^q = c^r$ in the *Euclidean* case when $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 1$.

Proposition 6. *The equations*

$$a^2 + b^6 = c^3, \; a^2 + b^4 = c^4, \; a^4 + b^4 = c^2 \;\; \textit{and} \;\; a^3 + b^3 = c^3$$

have no solutions in coprime nonzero integers a, b and c. The only solutions to the equation $a^2+b^3 = c^6$ in coprime nonzero integers a, b and c are with $(|a|, b, |c|) = (3, -2, 1)$.

Proof. This is standard (and very classical). The equations correspond to the elliptic curves $E/\mathbb{Q}$ denoted by $144A1, 32A1, 64A1, 21A1$ and $36A1$ in Cremona's notation, respectively. Each of these curves is of rank 0 over $\mathbb{Q}$; checking the rational torsion points yields the desired result. □

3. Multi-Frey techniques

In [2], the first two authors applied *multi-Frey* techniques pioneered by Bugeaud, Mignotte and Siksek [22] to the generalized Fermat equation $a^2 + b^6 = c^n$. In this approach, information derived from one Frey-Hellegouarch curve (in this case, a $\mathbb{Q}$-curve specific to this equation) is combined with that coming from a second such curve (corresponding, in this situation, to the generalized Fermat equation $x^2 + y^3 = z^n$, with the additional constraint that y is square).

In this section, we will employ a similar strategy to treat two new families of generalized Fermat equations, the second of which is, in some sense, a "twisted" version of that considered in [2] (though with its own subtleties). A rather more substantial application of such techniques is published separately in [3], where we discuss the equation $a^3 + b^{3n} = c^2$.

3.1. **The equation $a^3 + b^6 = c^n$.** Here, we will combine information from Frey-Hellegouarch curves over $\mathbb{Q}$, corresponding to equation (1) for signatures $(2, 3, n)$ and $(3, 3, n)$. We begin by noting a result of Kraus [60] on (1) with $(p, q, r) = (3, 3, n)$.

Proposition 7 (Kraus)**.** *If a, b and c are nonzero, coprime integers for which*

$$a^3 + b^3 = c^n,$$

where $n \geq 3$ is an integer, then $c \equiv 3 \pmod 6$ and $v_2(ab) = 1$. Here $v_l(x)$ denotes the largest power of a prime l dividing a nonzero integer x.

Actually, Kraus proves this only for $n \geq 17$ a prime. The remaining cases of the above proposition follow from Proposition 6 and the results of [18] and [30], which yield that there are no nontrivial solutions to the equation above when $n \in \{3, 4, 5, 7, 11, 13\}$.

Remark 8. *Proposition 7 trivially implies that the equation*

$$a^{3j} + b^{3k} = c^n$$

has no solutions in coprime nonzero integers a, b and c, provided $n \geq 3$ and the integers j and k each exceed unity. The case with $n = 2$ remains, apparently, open.

Returning to the equation $a^3 + b^6 = c^n$, we may assume that $n > 163$ is prime, by appealing to work of Dahmen [30] (for $n \in \{5, 7, 11, 13\}$) and Kraus [60] (for primes n with $17 \leq n \leq 163$). The cases $n \in \{3, 4\}$ follow from Proposition 6 (alternatively, if $n \in \{4, 5\}$, one can also appeal to work of

Bruin [18]). Applying Proposition 7, we may suppose further that $c \equiv 3 \pmod 6$ and $v_2(a) = 1$. We begin by considering the Frey-Hellegouarch curve

$$F \;:\; Y^2 = X^3 + bX^2 + \frac{b^2+a}{3}X + \frac{b(b^2+a)}{9},$$

essentially a twist of the standard curve for signature $(2,3,n)$ (see page 530 of Darmon and Granville [39]). What underlies our argument here (and subsequently) is the fact that the discriminant of F satisfies

$$\Delta_F = -\frac{64}{27}\,(a^3+b^6) = -\frac{64}{27}\,c^n,$$

whereby $n \mid v_l(\Delta_F)$ for each prime $l > 3$ dividing c. Since $3 \mid c$, noting that $v_3(a^2 - ab^2 + b^4) \leq 1$, we thus have $v_3(a + b^2) \geq n - 1$. It follows, from a routine application of Tate's algorithm, that F has conductor $2^6 \cdot 3 \cdot \prod p$, where the product runs through primes $p > 3$ dividing c (the fact that 3 divides c ensures multiplicative reduction at 3).

Here and henceforth, for an elliptic curve $E/\mathbb{Q}$ and prime l, we denote by

$$\rho_l^E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_l)$$

the Galois representation induced from the natural action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the l-torsion points of E. Since $n > 163$, by work of Mazur et al (see e.g. [30, Theorem 22]), the representation ρ_n^F is irreducible. Appealing to modularity [15] and Ribet's level lowering [74], [76], it follows that the modular form attached to F is congruent, modulo n, to a modular form g of level $2^6 \cdot 3 = 192$. All such modular forms are integral and, in particular, have Fourier coefficients satisfying $a_7(g) \in \{0, \pm 4\}$.

Considering the curve F modulo 7, we find that either $7 \mid c$ or that $a_7(F) \equiv -b^3 \pmod 7$. In the first case, $a_7(g) \equiv \pm 8 \pmod n$, contradicting the fact that $n > 163$. If $7 \nmid bc$, then $a_7(F) \equiv \pm 1 \pmod 7$ and hence, by the Weil bounds, $a_7(F) = \pm 1$, which is incongruent modulo n to any of the choices for $a_7(g)$. We therefore conclude that $7 \mid b$.

We turn now to our second Frey-Hellegouarch curve, that corresponding to signature $(3,3,n)$. Following Kraus [60], we consider

$$E \;:\; Y^2 = X^3 + 3ab_1X + a^3 - b_1^3, \quad \text{where} \quad b_1 = b^2.$$

Arguing as in [60], the modular form attached to E is congruent modulo n to the unique modular form g' of level 72 which has $a_7(g') = 0$. Since $7 \mid b$, we find that $a_7(E) = \pm 4$, an immediate contradiction. We thus may conclude as follows.

Proposition 9. *If $n \geq 2$ is an integer, then the only solutions to the equation $a^3 + b^6 = c^n$ in nonzero coprime integers a, b and c are given by $(n, a, |b|, |c|) = (2, 2, 1, 3)$.*

3.2. **The equations** $a^2 \pm c^n = b^6$**.** We begin by noting that the cases with $n = 3$ follow from Proposition 6, while those with $n = 4$ were treated by Bruin [17] (Theorems 2 and 3). The desired result with $n = 7$ is immediate from [72]. We will thus suppose, without loss of generality, that there exist coprime nonzero integers a, b and c, with

$$a^2 + c^n = b^6, \quad \text{for } \ n = 5 \text{ or } n \geq 11 \text{ prime.} \tag{3}$$

We distinguish two cases depending upon the parity of c.

Assume first that c is odd. In the factorization $b^6 - a^2 = (b^3 - a)(b^3 + a)$, the factors on the right hand side must be odd and hence coprime. We deduce, therefore, the existence of nonzero integers A and B for which

$$b^3 - a = A^n \quad \text{and} \quad b^3 + a = B^n,$$

where $\gcd(b, A, B) = 1$. This leads immediately to the Diophantine equation

$$A^n + B^n = 2b^3,$$

which, by Theorem 1.5 of [9], has no coprime solutions for primes $n \geq 5$ and $|AB| > 1$. It follows that there are no nonzero coprime solutions to equation (3) with c odd.

Remark 10. *If we write the Frey-Hellegouarch curve used to prove Theorem 1.5 of* [9] *in terms of a and b, i.e. substitute $A^n = b^3 + a$, we are led to consider*

$$E \ : \ Y^2 + 6\, b\, XY + 4(b^3 + a)Y = X^3.$$

This model has the same c-invariants as, and hence is isomorphic to, the curve given by

$$Y^2 = X^3 - 3(5b^3 - 4a)bX + 2(11b^6 - 14b^3a + 2a^2). \tag{4}$$

On replacing a by $-ia$ in (4), one obtains the Frey-Hellegouarch $\mathbb{Q}$-curve used for the equation $a^2 + b^6 = c^n$ in [2].

Next, assume that c is even. In this case, we can of course proceed as previously, i.e. by factoring $b^6 - a^2$ as

$$b^3 \pm a = 2A^n \quad \text{and} \quad b^3 \mp a = 2^{n-1}B^n, \ \ \text{for } A, B \in \mathbb{Z},$$

reducing to a generalized Fermat equation

$$A^n + 2^{n-2}B^n = b^3, \tag{5}$$

and considering the Frey-Hellegouarch elliptic curve

$$E_1 \ : \ Y^2 + 3bXY + A^n Y = X^3.$$

This approach, as it transpires, again yields a curve isomorphic to (4). By Lemma 3.1 of [9], the Galois representation on the n-torsion points of E_1 is absolutely irreducible for $n \geq 5$, whereby we can apply the standard machinery based on modularity of Galois representations. If one proceeds in this direction, however, it turns out that one ends up dealing with (after level lowering, etc.) weight 2 cuspidal newforms of level 54; at this level, we are apparently unable to obtain the desired contradiction, at least for certain n. One fundamental reason why this level causes such problems is the fact that the curve (4), evaluated at $(a,b) = (3,1)$ or $(a,b) = (17,1)$, is itself, in each case, a curve of conductor 54.

It is, however, still possible to use this approach to rule out particular values of n, appealing to the method of Kraus [60] – we will do so for $n = 5$ and $n = 13$. In case $n = 5$, considering solutions modulo 31 to (5), we find that if $31 \nmid AB$, then necessarily $a_{31}(E_1) \in \{-7,-4,2,8\}$, whereby we have, for F_1 a weight 2 cuspidal newform of level 54, that $a_{31}(F_1) \equiv -7,-4,2,8 \pmod 5$ or $a_{31}(F_1) \equiv \pm 32 \pmod 5$. Since each such newform is one-dimensional with $a_{31}(F_1) = 5$, we arrive at a contradiction, from which we conclude that equation (3) has no nonzero coprime solutions with $n = 5$.

Similarly, if $n = 13$ and we consider solutions modulo 53 to (5), we find that $a_{53}(E_1) \in \{-6,3,12\}$ or E_1 has multiplicative reduction at 53. This implies that for F_1 a weight 2 cuspidal newform of level 54, we have $a_{53}(F_1) \equiv -6,3,12 \pmod{13}$ or $a_{53}(F_1) \equiv \pm 54 \pmod{13}$. On the other hand, for every such newform F_1, $a_{53}(F_1) = \pm 9$, a contradiction. Equation (3) thus has no nonzero coprime solutions with $n = 13$.

To treat the remaining values of n, we will employ a second Frey-Hellegouarch curve (that for the signature $(2,3,n)$). Specifically, to a potential solution (a,b,c) to (3) with $n \geq 11$ and $n \neq 13$ prime, we associate the curve given by the Weierstrass equation

$$E_2 \ : \ Y^2 = X^3 - 3b^2 X - 2a. \tag{6}$$

This model has discriminant $\Delta = 2^6 3^3 c^n$. Note that since c is even, both a and b are odd, whereby it is easy to show that $v_2(c_4) = 4, v_2(c_6) = 6$ and $v_2(\Delta) > 12$ (since $n > 6$). These conditions alone are not sufficient to ensure non-minimality of the model at 2 (in contrast to like conditions at an odd prime p). A standard application of Tate's algorithm, however, shows that for a short Weierstrass model satisfying these conditions either the given model or that obtained by replacing a_6 by $-a_6$ (i.e. twisting over $\mathbb{Q}(\sqrt{-1})$) is necessarily non-minimal. Without loss of generality, replacing a by

$-a$ if necessary, we may thus assume that E_2 is not minimal at 2. It follows that a minimal model for this curve has $v_2(c_4) = v_2(c_6) = 0$ and $v_2(\Delta) > 0$, whereby the conductor $N(E_2)$ of E_2 satisfies $v_2(N(E_2)) = 1$. If $3 \nmid c$, then $v_3(\Delta) \leq 3$ and so $v_3(N(E_2)) \leq 3$. If $3 \mid c$, then $v_3(c_4) = 2, v_3(c_6) = 3$ and $v_3(\Delta) > 6$ (since $n > 3$), which implies that the twist of E_2 over either of $\mathbb{Q}(\sqrt{\pm 3})$ has multiplicative reduction at 3, whereby $v_3(N(E_2)) = 2$. For any prime $p > 3$, we see that the model for E_2 is minimal at p. In particular $n \mid v_p(\Delta_{\min}(E_2))$ for primes $p > 3$. In conclusion,

$$N(E_2) = 2 \cdot 3^\alpha \prod_{p \mid c,\, p>3} p, \quad \alpha \leq 3.$$

In order to apply level lowering, it remains to establish the irreducibility of the representation $\rho_n^{E_2}$.

Lemma 11. *If $n \geq 11$, $n \neq 13$ is prime, then $\rho_n^{E_2}$ is irreducible.*

Proof. As is well-known (see e.g. [30, Theorem 22]) by the work of Mazur et al, $\rho_n^{E_2}$ is irreducible if $n = 11$ or $n \geq 17$, and $j(E_2)$ is not one of

$$-2^{15}, -11^2, -11 \cdot 131^3, \frac{-17 \cdot 373^3}{2^{17}}, \frac{-17^2 \cdot 101^3}{2}, -2^{15} \cdot 3^3, -7 \cdot 137^3 \cdot 2083^3,$$
$$-7 \cdot 11^3, -2^{18} \cdot 3^3 \cdot 5^3, -2^{15} \cdot 3^3 \cdot 5^3 \cdot 11^3, -2^{18} \cdot 3^3 \cdot 5^3 \cdot 23^3 \cdot 29^3.$$

Since $j(E_2) = 2^6 \cdot 3^3 b^6/c^n$, one quickly checks that none of these j-values leads to a solution of (3). $\square$

Remark 12. *We note that proving irreducibility of $\rho_n^{E_2}$ for $n = 5, 7, 13$ is reduced to studying the Diophantine equation $j(E_2) = j_n(x)$, where $j_n(x)$ is the j-map from $X_0(n)$ to $X(1)$. For example, when $n = 13$, this amounts (after introducing $y = a/b^3$) to finding rational points on a hyperelliptic curve of genus 3 that we can solve (with some work) using standard Chabauty-type techniques. The previous argument then shows that the Frey-Hellegouarch curve E_2 can be used as well to solve (5) for $n = 13$. We leave the details to the interested reader.*

Using Lemma 11, modularity [15] and level lowering [74], [76], we thus arrive at the fact that $\rho_n^{E_2}$ is modular of level $2 \cdot 3^\alpha$ with $\alpha \leq 3$ (and, as usual, with weight 2 and trivial character). At levels 2, 6 and 18, there are no newforms whatsoever, while at level 54 there are only rational newforms. It follows that there exists a newform f of level 54, with $\rho_n^{E_2} \simeq \rho_n^f$ (equivalently, an elliptic curve F_2 of conductor 54 with $\rho_n^{E_2} \simeq \rho_n^{F_2}$). If $5 \mid c$, then E_2 has multiplicative reduction at 5 and hence $a_5(f) \equiv \pm 6 \pmod{n}$. Since we are assuming that $n \geq 11$, and since $a_5(f) = \pm 3$, this leads to a contradiction. If $5 \nmid c$, then E_2 has good reduction at 5 and, considering all possible solutions of equation (3) modulo 5, we find that $a_5(E_2) \in \{\pm 4, \pm 1, 0\}$. Since $a_5(f) \equiv a_5(E_2) \pmod{n}$ and $n \geq 11$, the resulting contradiction finishes our proof. We have shown

Proposition 13. *The only solutions to the generalized Fermat equation*

$$a^2 + \delta\, c^n = b^6,$$

in coprime nonzero integers a, b and c, with $n \geq 3$ an integer and $\delta \in \{-1, 1\}$, are given by $(n, |a|, |b|, \delta c) = (3, 3, 1, -2)$ (i.e. the Catalan solutions).

Remark 14. *In the preceding proof, we saw that the possibilities for $a_p(f)$ and $a_p(E_2)$ are disjoint for $p = 5$. This does not appear to be the case for any prime $p > 5$ (and we cannot use either $p = 2$ or $p = 3$ in this fashion), so, insofar as there is ever luck involved in such a business, it appears that we have been rather lucky here.*

4. Covers of spherical equations

The *spherical* cases of the generalized Fermat equation $x^p + y^q = z^r$ are those with signature (p, q, r) satisfying $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} > 1$ (for integers p, q and r, each exceeding unity). To be precise, they are, up to reordering,

$$(p, q, r) \in \{(2, 3, 3), (2, 3, 4), (2, 4, 3), (2, 3, 5)\}$$

and $(p, q, r) = (2, 2, n)$ or $(2, n, 2)$, for some $n \geq 2$. In each case, the corresponding equations possess infinitely many coprime nonzero integer solutions, given by a finite set of 2-parameter families (see e.g. [10] and [45]). The explicit parameterizations (with proofs) can be found in Chapter 14 of Cohen [27]. We will have need of those for $(p, q, r) = (2, 2, 3), (2, 2, 5), (2, 4, 3)$ and $(3, 3, 2)$.

4.1. The equation $x^2 + y^2 = z^3$.

If x, y and z are coprime integer solutions to this equation, then we have (see page 466 of [27])

$$(x, y, z) = (s(s^2 - 3t^2), t(3s^2 - t^2), s^2 + t^2), \tag{7}$$

for coprime integers s and t, of opposite parity. We begin this subsection with some remarks on the Diophantine equation $a^2 + b^{2n} = c^3$. This particular family is treated in [23] and in [31], where, using techniques of Kraus [60] and Chen-Siksek [26], the following is proved.

Theorem 15 (Dahmen [31])**.** *If n is a positive integer satisfying $3 \leq n \leq 10^7$ or $n \equiv -1 \pmod 6$, then the Diophantine equation $a^2 + b^{2n} = c^3$ has no solutions in nonzero coprime integers a, b and c.*

Here we recall part of the proof of this theorem for completeness (and future use).

Proposition 16. *If a, b and c are nonzero coprime integers for which*

$$a^2 + b^{2n} = c^3,$$

where $n \geq 3$ is an integer, then $b \equiv 3 \pmod 6$.

Proof. We may suppose that $n \geq 7$ is prime, since for $n = 3, 4$ and 5 there are no solutions (see Proposition 6, [17] and [31]). From (7), if we have coprime integers a, b and c with $a^2 + b^{2n} = c^3$, there exist coprime integers s and t, of opposite parity, for which $b^n = t\,(3s^2 - t^2)$, and hence coprime integers B and C, and $\delta \in \{0, 1\}$, with

$$t = 3^{-\delta} B^n \quad \text{and} \quad 3s^2 - t^2 = 3^{\delta}\, C^n.$$

If $\delta = 0$ (this is the case when $3 \nmid b$), it follows that $C^n + B^{2n} = 3s^2$ which, via Theorem 1.1 of [8], implies $a = 0$ (and so $s = 0$). If, on the other hand, we have $\delta = 1$ (so that $3 \mid b$) and b (and hence t) even, then, writing $B = 3B_1$, we have that $C^n + 3^{2n-3} B_1^{2n} = s^2$, with B_1 even. Arguing as in [8], there thus exists a weight 2 cuspidal newform of level 6, an immediate contradiction. $\square$

Note that when $b \equiv 3 \pmod 6$ we are led to the Diophantine equation

$$C^n + \frac{1}{27} B^{2n} = A^2, \tag{8}$$

with A even and BC odd, and hence, via (say) the Frey-Hellegouarch curve (see e.g. [8])

$$E \;:\; Y^2 = X^3 + 2AX^2 + \frac{B^{2n}}{27} X, \tag{9}$$

to a cuspidal newform of level 96, which we are (presently) unable to rule out for certain n. However, arguing as in [26] and [31], we can resolve this case for a family of exponents n of natural density 1. We recall these techniques here.

4.2. **Quadratic Reciprocity.** In what follows, we will employ the Hilbert symbol instead of the Legendre symbol, to enable us to treat the prime 2 without modification of our arguments. Recall the (symmetric, multiplicative) Hilbert symbol $(\,,\,)_K : K^* \times K^* \to \{\pm 1\}$ defined by

$$(A, B)_K = \begin{cases} 1 & \text{if } z^2 = Ax^2 + By^2 \text{ has a nonzero solution in } K, \\ -1 & \text{otherwise.} \end{cases}$$

For concision, we let $(\,,\,)_p$, $(\,,\,)$ and $(\,,\,)_\infty$ denote $(\,,\,)_{\mathbb{Q}_p}$, $(\,,\,)_{\mathbb{Q}}$ and $(\,,\,)_{\mathbb{R}}$, respectively. Note that we have the reciprocity law

$$\prod_{p \leq \infty} (a, b)_p = 1, \tag{10}$$

valid for all nonzero rationals a and b. For an odd prime p, if $A = p^{\alpha}u$ and $B = p^{\beta}v$ with u and v p-adic units, we further have

$$(A,B)_p = (-1)^{\alpha\beta\frac{(p-1)}{2}} \left(\frac{u}{p}\right)^{\beta} \left(\frac{v}{p}\right)^{\alpha}. \tag{11}$$

In particular, for an odd prime p where $v_p(A)$ and $v_p(B)$ are even, it follows that $(A,B)_p = 1$. When $p = 2$, we have the following analogous formula : if we write $A = 2^{\alpha}u$ and $B = 2^{\beta}v$ with u and v 2-adic units, then

$$(A,B)_2 = (-1)^{\frac{u-1}{2}\frac{v-1}{2}+\alpha\frac{v^2-1}{8}+\beta\frac{u^2-1}{8}}.$$

Proposition 17. *Let r and s be nonzero rational numbers. Assume that $v_l(r) = 0$ for all $l \mid n$ and that the Diophantine equation*

$$A^2 - rB^{2n} = s(C^n - B^{2n})$$

has a solution in coprime nonzero integers A, B and C, with BC odd. Then

$$(r, s(C-B^2))_2 \prod_{\substack{v_p(r)\ odd \\ v_p(s)\ odd \\ 2<p<\infty}} (r, s(C-B^2))_p = 1$$

Proof. Let us begin by noting that, by the reciprocity law (10), we have

$$(r, s(C-B^2))_2 \prod_{\substack{v_p(r)\text{ odd}, \\ v_p(s)\text{ odd}, \\ 2<p<\infty}} (r, s(C-B^2))_p = (r, s(C-B^2))_\infty \prod_{\substack{v_p(r)\text{ even}, \\ v_p(s)\text{ odd}, \\ 2<p<\infty}} (r, s(C-B^2))_p. \tag{12}$$

Since we suppose

$$A^2 = rB^{2n} + s(C^n - B^{2n}) \cdot 1^2,$$

it follows that $(r, s(C^n - B^{2n}))_p = 1$, for all primes $p \leq \infty$. Therefore

$$(r, s(C-B^2))_p = (r, C^{n-1} + \cdots + B^{2n-2})_p.$$

Since $C^{n-1} + \cdots + B^{2n-2} > 0$, we also have $(r, s(C-B^2))_\infty = 1$. Now, assume that $v_p(r)$ is even for an odd prime p. If $v_p(s(C-B^2))$ is also even then, by equation (11), we have that $(r, s(C-B^2))_p = 1$. If $v_p(s(C-B^2))$ is odd, but $p \nmid n$ then $v_p(C^{n-1} + \cdots + B^{2n-2}) = 0$, which implies that

$$(r, s(C-B^2))_p = (r, C^{n-1} + \cdots + B^{2n-2})_p = 1.$$

When $p \mid n$ and $v_p(s(C-B^2))$ is odd, since we are assuming that r is a p-unit and since A, B and C are coprime, it follows that

$$A^2 \equiv rB^{2n} \pmod{p},$$

and hence $\left(\frac{r}{p}\right) = 1$. Appealing again to equation (11), we conclude that $(r, s(C - B^2))_p = 1$, as desired.

□

This proposition provides us with an extra constraint upon $C/B^2 \pmod r$ to which we can appeal, at least on occasion, to rule out exponents n in certain residue classes. If we suppose that we have a solution to equation (8) in integers A, B, C and n, with A even and BC odd, we can either add or subtract B^{2n} from both sides of the equation in order to apply the above proposition. Subtracting B^{2n} (this is the case treated in [31]), we obtain

$$A^2 - \frac{28}{27}B^{2n} = C^n - B^{2n}.$$

Here we have $r = \frac{28}{27}$ and $s = 1$, and, via Proposition 17 (supposing that $n \equiv -1 \pmod 6$ and appealing to [72] to treat the cases with $7 \mid n$), may conclude that

$$(28/27, C - B^2)_2 (28/27, C - B^2)_3 (28/27, C - B^2)_7 = 1.$$

Since $3 \mid B$, the quantity C^n is a perfect square modulo 3 and so $(28/27, C - B^2)_3 = 1$. Also, since $C^{n-1} + \cdots + B^{2n-2}$ is odd, we may compute that

$$(28/27, C - B^2)_2 = (28/27, C^n - B^{2n})_2 = 1.$$

If $7 \mid C - B^2$ then necessarily $7 \mid A$. It is easy to check from (9) that, in this case, $a_7(E) = 0$. On the other hand, each cuspidal newform f at level 96 has $a_7(f) = \pm 4$, whereby we have

$$0 = a_7(E) \not\equiv a_7(f) \pmod n,$$

an immediate contradiction. Therefore $7 \nmid C - B^2$, and so

$$1 = (28/27, C - B^2)_7 = \left(\frac{C - B^2}{7}\right). \tag{13}$$

On the other hand, since each elliptic curve $E/\mathbb{Q}$ of conductor 96 has $a_7(E) = \pm 4$, computing the corresponding Fourier coefficient for our Frey-Hellegouarch curve (9), we find that

$$A^2 \equiv B^{2n} \pmod 7 \ \ (\text{where } A \not\equiv 0 \pmod 7).$$

It follows from (8) that $(C/B^2)^n \equiv 2 \pmod 7$. Since $n \equiv -1 \pmod 6$, we therefore have $C/B^2 - 1 \equiv 3 \pmod 7$, contradicting (13). This proves the second part of Theorem 15.

Similarly, adding B^{2n} to both sides of equation (8), we have

$$A^2 + \frac{26}{27}B^{2n} = C^n + B^{2n} = -((-C)^n - B^{2n}),$$

where we suppose that $n \equiv 3 \pmod 4$ is prime (so that, via Theorem 15, $n \equiv 7 \pmod{12}$). We may thus apply Proposition 17 with $r = -26/27$ and $s = -1$ to conclude that

$$\prod_{p \mid 78} (-26/27, s((-C) - B^2))_p = \prod_{p \mid 78} (-78, C + B^2)_p = 1.$$

As before, we find that $(-78, C + B^2)_3 = 1$. Since each elliptic curve $E/\mathbb{Q}$ of conductor 96 has $a_{13}(E) = \pm 2$, we thus have, via (9),

$$\begin{cases} A \equiv \pm 1 \pmod{13}, \; B^{2n} \equiv 4, 9, 10 \text{ or } 12 \pmod{13}, \text{ or} \\ A \equiv \pm 2 \pmod{13}, \; B^{2n} \equiv 1, 3, 9 \text{ or } 10 \pmod{13}, \text{ or} \\ A \equiv \pm 3 \pmod{13}, \; B^{2n} \equiv 3, 4, 10 \text{ or } 12 \pmod{13}, \text{ or} \\ A \equiv \pm 4 \pmod{13}, \; B^{2n} \equiv 1, 4, 10 \text{ or } 12 \pmod{13}, \text{ or} \\ A \equiv \pm 5 \pmod{13}, \; B^{2n} \equiv 1, 3, 4 \text{ or } 9 \pmod{13}, \text{ or} \\ A \equiv \pm 6 \pmod{13}, \; B^{2n} \equiv 1, 3, 9 \text{ or } 12 \pmod{13}, \end{cases}$$

whereby $(C/B^2)^n \equiv 2, 3, 9$ or $11 \pmod{13}$ and hence from $n \equiv 7 \pmod{12}$, $C/B^2 \equiv 2, 3, 9$ or $11 \pmod{13}$. It follows that $(-78, C + B^2)_{13} = 1$, whereby $(-78, C + B^2)_2 = 1$. We also know that A is even, while BC is odd, whence $C + B^2 \equiv 2 \pmod 4$. It follows from $(-78, C + B^2)_2 = 1$ that $C/B^2 + 1 \equiv \pm 2 \pmod{16}$, and so $C/B^2 \equiv 1$ or $13 \pmod{16}$. If we now assume that $v_2(A) > 1$, then equation (8) implies that $C^n \equiv -3B^{2n} \pmod{16}$ (and so necessarily $C/B^2 \equiv 13 \pmod{16}$). Our assumption that $n \equiv 3 \pmod 4$ thus implies $(C/B^2)^n \equiv 5 \pmod{16}$, a contradiction. In conclusion, appealing to Proposition 6 in case $3 \mid n$, we have

Proposition 18. *If $n \equiv 3 \pmod 4$ and there exist nonzero coprime integers a, b and c for which $a^2 + b^{2n} = c^3$, then $v_2(a) = 1$. In particular, if $m \geq 2$ is an integer, then the equation $a^{2m} + b^{2n} = c^3$ has no solution in nonzero coprime integers a, b and c.*

4.2.1. $a^2 + b^{2n} = c^9$. The case $n = 2$ was handled previously by Bennett, Ellenberg and Ng [5], while the case $n = 3$ is well known (see Proposition 6). We may thereby suppose that $n \geq 5$ is prime. Applying Proposition 16 and (7), there thus exist coprime integers s and t, with s even and $t \equiv 3 \pmod 6$, for which

$$b^n = t\,(3s^2 - t^2) \quad \text{and} \quad c^3 = s^2 + t^2.$$

We can therefore find coprime $A, B \in \mathbb{Z}$ with $t = 3^{n-1} A^n$ and $3s^2 - t^2 = 3\,B^n$, whence

$$B^n + 4 \cdot 3^{2n-3} A^{2n} = c^3.$$

Via Lemma 3.4 of [9], for prime $n \geq 5$ this leads to a weight 2 cuspidal newform of level 6, a contradiction. We thus have

Proposition 19. *If n is an integer with $n \geq 2$, then the equation $a^2 + b^{2n} = c^9$ has no solutions in nonzero coprime integers a, b and c.*

4.3. **The equation $x^2 + y^2 = z^5$.** If x, y and z are coprime integers satisfying $x^2 + y^2 = z^5$, then (see page 466 of [27]) there exist coprime integers s and t, of opposite parity, with

$$(x, y, z) = (s(s^4 - 10s^2t^2 + 5t^4), t(5s^4 - 10s^2t^2 + t^4), s^2 + t^2). \tag{14}$$

The following result is implicit in [24]; we include a short proof for completeness.

Proposition 20. *If a, b and c are nonzero coprime integers for which*

$$a^2 + b^{2n} = c^5,$$

where $n \geq 2$ is an integer, then $b \equiv 1 \pmod 2$.

Proof. The cases $n = 2, 3$ and 5 are treated in [5], [2] and [71], respectively. We may thus suppose that $n \geq 7$ is prime. From (14), there are coprime integers s and t, of opposite parity, for which $b^n = t\,(5s^4 - 10s^2t^2 + t^2)$. There thus exist integers A and B, and $\delta \in \{0, 1\}$, with

$$t = 5^{-\delta} A^n \quad \text{and} \quad 5s^4 - 10s^2t^2 + t^4 = 5^\delta\, B^n.$$

It follows that

$$5^\delta\, B^n + 4 \cdot 5^{-4\delta} A^{4n} = 5(s^2 - t^2)^2. \tag{15}$$

If b is even (whereby the same is true of t and A) and $\delta = 1$, then again arguing as in [8], we deduce the existence of a weight 2 cuspidal newform of level 10, a contradiction. If, however, b is even and $\delta = 0$, the desired result is an immediate consequence of Theorem 1.2 of [8]. $\square$

4.3.1. *The equation $a^2 + b^{2n} = c^{10}$.* As noted earlier, we may suppose that $n \geq 7$ is prime and, from Proposition 20, that b is odd. Associated to such a solution, via the theory of Pythagorean triples, there thus exist coprime integers u and v, of opposite parity, with

$$b^n = u^2 - v^2 \quad \text{and} \quad c^5 = u^2 + v^2. \tag{16}$$

Hence, we may find integers A and B with

$$u - v = A^n \quad \text{and} \quad u + v = B^n.$$

From the second equation in (16) and from (14), there exist coprime integers s and t, of opposite parity, with

$$u - v = (s-t)\left(s^4 - 4s^3t - 14s^2t^2 - 4st^3 + t^4\right).$$

Since

$$(s-t)^4 - \left(s^4 - 4s^3t - 14s^2t^2 - 4st^3 + t^4\right) = 20s^2t^2,$$

it follows that $\gcd(s-t, s^4 - 4s^3t - 14s^2t^2 - 4st^3 + t^4) \mid 5$. Similarly, we have

$$u + v = (s+t)\left(s^4 + 4s^3t - 14s^2t^2 + 4st^3 + t^4\right)$$

where $\gcd(s+t, s^4+4s^3t-14s^2t^2+4st^3+t^4)$ also divides 5. Since s and t are coprime, we cannot have $s-t \equiv s+t \equiv 0 \pmod 5$ and so may conclude that at least one of $\gcd(s-t, s^4-4s^3t-14s^2t^2-4st^3+t^4)$ or $\gcd(s+t, s^4+4s^3t-14s^2t^2+4st^3+t^4)$ is equal to 1. There thus exist integers X and Y such that either $(X^n, Y^n) = (s-t, s^4-4s^3t-14s^2t^2-4st^3+t^4)$ or $(s+t, s^4+4s^3t-14s^2t^2+4st^3+t^4)$. In either case, $X^{4n} - Y^n = 5(2st)^2$ which, with Theorem 1.1 of [8], contradicts $st \neq 0$. In conclusion,

Proposition 21. *If n is an integer with $n \geq 2$, then the equation $a^2 + b^{2n} = c^{10}$ has no solutions in nonzero coprime integers a, b and c.*

4.3.2. *The equation $a^2 + b^{2n} = c^{15}$.* As before, we may suppose that $n \geq 7$ is prime. Using Proposition 16, we may also assume that $b \equiv 3 \pmod 6$. Appealing to our parametrizations for $x^2 + y^2 = z^5$ (i.e. equation (14)), we deduce the existence of a coprime pair of integers (s,t) for which

$$b^n = t\left(5s^4 - 10s^2t^2 + t^4\right) \quad \text{and} \quad c^3 = s^2 + t^2.$$

Since s and t are coprime, it follows that $5s^4 - 10s^2t^2 + t^4 \equiv \pm 1 \pmod 3$, whereby $3 \mid t$. There thus exist integers A and B, and $\delta \in \{0,1\}$ satisfying equation (15), with the additional constraint that $3 \mid A$. It follows that the corresponding Frey-Hellegouarch curve has multiplicative reduction at the prime 3, but level lowers to a weight 2 cuspidal newform of level $N = 40$ or 200 (depending on whether $\delta = 1$ or 0, respectively). This implies the existence of a form f at one of these levels with $a_3(f) \equiv \pm 4 \pmod n$. Since all such forms are one dimensional and have $a_3(f) \in \{0, \pm 2, \pm 3\}$, it follows that $n = 7$, contradicting the main result of [72]. We thus have

Proposition 22. *If n is an integer with $n \geq 2$, then the equation $a^2 + b^{2n} = c^{15}$ has no solutions in nonzero coprime integers a, b and c.*

4.4. **The equation $x^2 + y^4 = z^3$.** Coprime integer solutions to this equation satisfy one of (see pages 475–477 of [27])

$$\left\{ \begin{array}{l} x = 4ts\left(s^2 - 3t^2\right)\left(s^4 + 6s^2t^2 + 81t^4\right)\left(3s^4 + 2s^2t^2 + 3t^4\right) \\ y = \pm(s^2 + 3t^2)\left(s^4 - 18s^2t^2 + 9t^4\right) \\ z = (s^4 - 2t^2s^2 + 9t^4)(s^4 + 30t^2s^2 + 9t^4), \end{array} \right. \tag{17}$$

$$\left\{ \begin{array}{l} x = \pm(4s^4 + 3t^4)(16s^8 - 408t^4s^4 + 9t^8) \\ y = 6ts(4s^4 - 3t^4) \\ z = 16s^8 + 168t^4s^4 + 9t^8, \end{array} \right. \tag{18}$$

$$\left\{ \begin{array}{l} x = \pm(s^4 + 12t^4)(s^8 - 408t^4s^4 + 144t^8) \\ y = 6ts(s^4 - 12t^4) \\ z = s^8 + 168t^4s^4 + 144t^8, \end{array} \right. \tag{19}$$

or

$$\left\{ \begin{array}{ll} x = & \pm 2(s^4 + 2ts^3 + 6t^2s^2 + 2t^3s + t^4)\left(23s^8 - 16ts^7 - 172t^2s^6\right. \\ & \left. -112t^3s^5 - 22t^4s^4 - 112t^5s^3 - 172t^6s^2 - 16t^7s + 23t^8\right) \\ y = & 3(s-t)(s+t)(s^4 + 8ts^3 + 6t^2s^2 + 8t^3s + t^4) \\ z = & 13s^8 + 16ts^7 + 28t^2s^6 + 112t^3s^5 + 238t^4s^4 \\ & +112t^5s^3 + 28t^6s^2 + 16t^7s + 13t^8. \end{array} \right. \tag{20}$$

Here, s and t are coprime integers satisfying

$$\left\{ \begin{array}{l} s \not\equiv t \pmod 2 \text{ and } s \equiv \pm 1 \pmod 3, \text{ in case (17)}, \\ t \equiv 1 \pmod 2 \text{ and } s \equiv \pm 1 \pmod 3, \text{ in case (18)}, \\ s \equiv 1 \pmod 2 \text{ and } s \equiv \pm 1 \pmod 3, \text{ in case (19)}, \\ s \not\equiv t \pmod 2 \text{ and } s \not\equiv t \pmod 3, \text{ in case (20)}. \end{array} \right.$$

Since work of Ellenberg [46] (see also [5]) treats the case where z is an nth power (and more), we are interested in considering equations corresponding to $x = a^n$ or $y = b^n$. We begin with the former.

4.4.1. *The equation $a^{2n} + b^4 = c^3$.* The case $n = 2$ follows (essentially) from work of Lucas; see Section 5. We may thus suppose that $n \geq 3$. We appeal to the parametrizations (17) – (20), with $x = a^n$. In (17) and (20), we have a even, while, in (18) and (19), a is coprime to 3. Applying Proposition 16 leads to the desired conclusion :

Proposition 23. *If n is an integer with $n \geq 2$, then the equation $a^{2n} + b^4 = c^3$ has no solutions in nonzero coprime integers a, b and c.*

4.4.2. *The equation $a^2 + b^{4n} = c^3$.* For this equation, with $n \geq 2$ an integer, Proposition 16 implies that we are in case (20), i.e. that there exist integers s and t for which

$$b^n = 3(s-t)(s+t)(s^4 + 8s^3t + 6s^2t^2 + 8st^3 + t^4), \; s \not\equiv t \pmod 2, \; s \not\equiv t \pmod 3. \tag{21}$$

Assuming n is odd, we thus can find integers A, B and C with

$$s - t = A^n, \;\; s + t = \frac{1}{3}B^n \;\text{ and }\; s^4 + 8s^3t + 6s^2t^2 + 8st^3 + t^4 = C^n.$$

It follows that

$$A^{4n} - \frac{1}{27}B^{4n} = -2C^n, \tag{22}$$

with ABC odd and $3 \mid B$. There are (at least) three Frey-Hellegouarch curves we can attach to this Diophantine equation :

$$\begin{aligned} E_1 \,:\, Y^2 &= X(X - A^{4n})\left(X - \frac{B^{4n}}{27}\right), \\ E_2 \,:\, Y^2 &= X^3 + 2A^{2n}X^2 - 2C^nX, \\ E_3 \,:\, Y^2 &= X^3 - \frac{2B^{2n}}{27}X^2 + \frac{2C^n}{27}X. \end{aligned}$$

Although the solution $(A^{4n}, B^{4n}, C^n) = (1, 81, 1)$ does not persist for large n, it still appears to cause an obstruction to resolving this equation fully using current techniques : none of the E_i have complex multiplication, nor can we separate out this solution using images of inertia at 3 or other primes dividing the conductor. In terms of the original equation, the obstruction corresponds to the identity

$$(\pm 46)^2 + (\pm 3)^4 = 13^3.$$

Incidentally, this is the same obstructive solution which prevents a full resolution of $a^2 + b^{2n} = c^3$.

By Theorem 15, we may assume that every prime divisor l of n exceeds 10^6, which implies that $\rho_l^{E_i}$ is, in each case, irreducible. Applying level lowering results, we find that the modular form attached to E_i is congruent to a modular form f_i of weight 2 and level N_i, where

$$N_i = \begin{cases} 96 & i = 1, \\ 384 & i = 2, \\ 1152 & i = 3. \end{cases}$$

The latter two conductor calculations can be found in [8] and the former in [59]. Since $l > 10^6$, all the f_i's with noninteger coefficients can be ruled out, after a short computation. This implies that there is an elliptic curve F_i with conductor N_i such that $\rho_l^{F_i} \simeq \rho_l^{E_i}$. Furthermore, E_i must have good reduction at primes $5 \leq p \leq 53$ (again after a short calculation using the fact that $l > 10^6$).

Adding $2B^{4n}$ to both sides of equation (22), we have

$$A^{4n} + \frac{53}{27}B^{4n} = 2(-C^n + B^{4n})$$

and hence, via Proposition 17,

$$(-53/27, 2(-C + B^4))_2(-53/27, 2(-C + B^4))_3(-53/27, 2(-C + B^4))_{53} = 1.$$

Since $-2C^n \equiv A^{4n} \pmod 3$, we have $(-53/27, 2(-C + B^4))_3 = 1$. Also, since $-53/27 \equiv 1 \pmod 8$, it is a perfect square in $\mathbb{Q}_2$, which implies that $(-53/27, 2(-C + B^4))_2 = 1$. Therefore

$$(-53/27, 2(-C + B^4))_{53} = 1,$$

i.e. $-C/B^4 + 1$ is a quadratic nonresidue modulo 53. Since all the elliptic curves F_1 of conductor 96 have $a_{53}(F_1) = 10$ (whereby, from $l > 10^6$, $a_{53}(E_1) = 10$), if follows that $(A^4/B^4)^n \equiv 36 \pmod{53}$. Therefore

$$(-C/B^4)^n \equiv 17 \pmod{53}.$$

If $n \equiv \pm 9, \pm 11, \pm 15, \pm 17 \pmod{52}$ then $(-C/B^4)^n = (\alpha - 1)^n \not\equiv 17 \pmod{53}$ for any choice of quadratic nonresidue α. It follows that if $n \equiv \pm 2, \pm 4 \pmod{13}$, equation (22) has no solution with ABC odd and $3 \mid B$.

Similarly, if we subtract $2B^{2n}$ from both sides of equation (22), we obtain

$$A^{4n} - \frac{55}{27}B^{4n} = 2(-C^n - B^{4n}).$$

Proposition 17 thus implies

$$(55/27, 2(-C - B^4))_2 \, (55/27, 2(-C - B^4))_3 \, (55/27, 2(-C - B^4))_5 \, (55/27, 2(-C - B^4))_{11} = 1.$$

As before we have $(55/27, 2(-C - B^4))_3 = 1$ and since $55/27 \equiv 1 \pmod 4$ and $C^{n-1} + \cdots + B^{4n-4}$ is odd, also $(55/27, C^{n-1} + \cdots + B^{4n-4})_2 = (55/27, 2(-C - B^4))_2 = 1$. Similarly, since $(A^4/B^4)^n \equiv 1 \pmod 5$, it follows that $(-C/B^4)^n \equiv -1 \pmod 5$, whereby, since n is odd, $-C/B^4 \equiv -1 \pmod 5$. Therefore $(55/27, 2(-C-B^4))_5 = 1$, which implies $(55/27, 2(-C-B^4))_{11} = 1$. In particular $-C/B^4 \equiv \lambda \pmod{11}$ where

$$\lambda \in \{0, 1, 3, 7, 8, 9\}. \tag{23}$$

We can rule out $\lambda = 0$ and 1 since we are assuming that $11 \nmid ABC$. To treat the other cases, we will apply the Chen-Siksek method to the curves E_2 and E_3. We first show that $a_{11}(E_2) = -4$.

Notice that considering all possible solutions to equation (22) modulo 13, necessarily $a_{13}(E_2) = -6$ (since we assume that $13 \nmid ABC$). Observe also that E_2 has nonsplit multiplicative reduction at 3. Therefore

$$\rho_n^{E_2}|_{G_3} \simeq \rho_n^{F_2}|_{G_3} \simeq \begin{pmatrix} \chi\epsilon & * \\ 0 & \epsilon \end{pmatrix}$$

where χ is the cyclotomic character and $\epsilon : G_3 \to \mathbb{F}_n^*$ is the unique unramified quadratic character (see, for example, [38]). It follows that F_2 must have nonsplit multiplicative reduction at 3 and hence F_2 must be isogenous to the elliptic curve $384D$ in the Cremona's database. In particular,we have $a_{11}(E_2) = -4$ and so

$$\frac{A^{2n}}{B^{2n}} \equiv 1, 5 \pmod{11}.$$

When $A^{2n}/B^{2n} \equiv 1 \pmod{11}$, we find, by direct computation, that $a_{11}(E_3) = 0$, contradicting the fact that $a_{11}(E) \in \{\pm 2, \pm 4\}$ for every elliptic curve $E/\mathbb{Q}$ of conductor 1152. Therefore, we necessarily have

$$\frac{A^{2n}}{B^{2n}} \equiv 5 \pmod{11} \implies \left(\frac{-C}{B^4}\right)^n \equiv 8 \pmod{11},$$

whereby $\lambda^n \equiv 8 \pmod{11}$. A quick calculation shows, however, that for $n \equiv \pm 3 \pmod{10}$, this contradicts (23). Collecting all this together, we conclude as follows (noting the solution coming from $(p, q, r) = (2, 8, 3)$; see Bruin [17]).

Proposition 24. *If n is a positive integer with either $n \equiv \pm 2 \pmod 5$ or $n \equiv \pm 2, \pm 4 \pmod{13}$, then the equation $a^2 + b^{4n} = c^3$ has only the solution $(a, b, c, n) = (1549034, 33, 15613, 2)$ in positive coprime integers a, b and c.*

Remark 25. *The table of results regarding equation (1) given on page 490 of Cohen [27] lists the case of signature $(2, 4n, 3)$ as solved, citing work of the first two authors. This is due to an over-optimistic communication of the first author to Professor Cohen. We regret any inconvenience or confusion caused by this mistake.*

Remark 26. *Regarding the Diophantine equation (22) as an equation of signature $(2, 4, n)$, we can attach the Frey-Hellegouarch $\mathbb{Q}$-curves*

$$E_4 \ : \ Y^2 = X^3 + 4B^n X^2 + 2(B^{2n} + 3\sqrt{3}A^{2n})X$$

and

$$E_5 \ : \ Y^2 = X^3 + 4A^n X^2 + 2\left(A^{2n} + \frac{1}{3\sqrt{3}} B^{2n}\right) X.$$

One further Frey-Hellegouarch $\mathbb{Q}$-curve can be derived as follows. Defining

$$U = (A^{4n} + B^{4n}/27)/2 = 2(s^4 + 2s^3t + 6s^2t^2 + 2st^3 + t^4)$$

we have

$$U^2 - \frac{1}{27} A^{4n} B^{4n} = C^{2n}.$$

Considering this as an equation of signature $(n, n, 2)$ turns out to give us the Frey-Hellegouarch curve E_1 again. Writing $V = A^n B^n/3$ and $W = C^2$, we arrive at the generalized Fermat equation of signature $(2, 4, n)$

$$U^2 - 3V^4 = W^n$$

in nonzero coprime integers U, V and W, with $3 \mid V$ and $v_2(U) = 1$. As before, we can associate a $\mathbb{Q}$-curve to this equation.

Although the solution $(A^{4n}, B^{4n}, C^n) = (1, 81, 1)$ does not satisfy our desired 3-adic properties, it still apparently forms an obstruction using current techniques, here and for all Frey-Hellegouarch curves we have considered, to solving this equation in full generality.

4.5. **The equation $x^3 + y^3 = z^2$.** From [27] (pages 467 – 470), the coprime integer solutions to this equation satisfy one of

$$\left\{\begin{array}{l} x = s(s+2t)(s^2 - 2ts + 4t^2) \\ y = -4t(s-t)(s^2 + ts + t^2) \\ z = \pm(s^2 - 2ts - 2t^2)(s^4 + 2ts^3 + 6t^2s^2 - 4t^3s + 4t^4), \end{array}\right. \tag{24}$$

$$\left\{\begin{array}{l} x = s^4 - 4ts^3 - 6t^2s^2 - 4t^3s + t^4 \\ y = 2(s^4 + 2ts^3 + 2t^3s + t^4) \\ z = 3(s-t)(s+t)(s^4 + 2s^3t + 6s^2t^2 + 2st^3 + t^4), \end{array}\right. \tag{25}$$

or

$$\left\{\begin{array}{l} x = -3s^4 + 6t^2s^2 + t^4 \\ y = 3s^4 + 6t^2s^2 - t^4 \\ z = 6st(3s^4 + t^4). \end{array}\right. \tag{26}$$

Here, the parametrizations are up to exchange of x and y, and s and t are coprime integers with

$$\begin{cases} s \equiv 1 \pmod 2 \text{ and } s \not\equiv t \pmod 3, & \text{in case (24)}, \\ s \not\equiv t \pmod 2 \text{ and } s \not\equiv t \pmod 3, & \text{in case (25)}, \\ s \not\equiv t \pmod 2 \text{ and } t \not\equiv 0 \pmod 3, & \text{in case (26)}. \end{cases}$$

4.5.1. *The equation $a^3 + b^3 = c^{2n}$.* The cases $n \in \{2, 3, 5\}$ follow from [18] and Proposition 6. We may thus suppose that $n \geq 7$ is prime. Since Proposition 7 implies $c \equiv 3 \pmod 6$, it follows that

$$c^n = 3(s-t)(s+t)(s^4 + 2s^3t + 6s^2t^2 + 2st^3 + t^4),$$

for s and t coprime integers with $s \not\equiv t \pmod 2$ and $s \not\equiv t \pmod 3$. There thus exist integers A, B and C with

$$s - t = A^n, \quad s + t = 3^{n-1} B^n \quad \text{and} \quad s^4 + 2s^3t + 6s^2t^2 + 2st^3 + t^4 = C^n,$$

whereby

$$A^{4n} + 3^{4n-3} B^{4n} = 4\, C^n,$$

which we rewrite as

$$4\, C^n - A^{4n} = 3 \left(3^{2n-2}\, B^{2n}\right)^2.$$

Applying Theorem 1.2 of [8] to this last equation, we may conclude, for $n \geq 7$ prime, that either $ABC = 0$ or $3^{2n-2}\, B^{2n} = \pm 1$, in either case a contradiction. We thus have

Proposition 27. *If n is an integer with $n \geq 2$, then the equation $a^3 + b^3 = c^{2n}$ has no solutions in nonzero coprime integers a, b and c.*

4.5.2. *The equation $a^3 + b^{3n} = c^2$.* The techniques involved in this case require some of the most elaborate combination of ingredients to date, including $\mathbb{Q}$-curves and delicate multi-Frey and image of inertia arguments. For this reason, we have chosen to publish this separately in [3]. Our main result there is as follows.

Theorem 28. [3] *If n is prime with $n \equiv 1 \pmod 8$, then the equation $a^3 + b^{3n} = c^2$ has no solutions in coprime nonzero integers a, b and c, apart form those given by $(a, b, c) = (2, 1, \pm 3)$.*

4.6. **Other spherical equations.** Solutions to the generalized Fermat equation with *icosahedral* signature $(2, 3, 5)$ correspond to 27 parametrized families, in each case with parametrizing forms of degrees $30, 20$ and 12 (see e.g. [45]). We are unable to apply the techniques of this paper to derive much information of value in this situation (but see [4]).

5. Historical notes on the equations $a^4 \pm b^4 = c^3$

In [40], it is proved that the generalized Fermat equation (1) with $(p,q,r) = (n,n,3)$, has no coprime, nonzero integer solutions a, b and c, provided $n \geq 7$ is prime (and assuming the modularity of elliptic curves over $\mathbb{Q}$ with conductor divisible by 27, now a well known theorem [15]). To show the nonexistence of solutions for all integers $n \geq 3$, it suffices, in addition, to treat the cases $n = 3, 4$ and 5; the first of these is classical and was (essentially) solved by Euler (see Proposition 6), while the last was handled by Poonen in [71]. The case $n = 4$ is attributed in [40] and [71], citing [41, p. 630], to the French mathematician Édouard Lucas (1842–1891), in particular to [64] and [65, Chapitre III].

In these two papers, as well as in other work of Lucas [52, pp. 282–288], there does not appear to be, however, any explicit mention of the equation

$$a^4 + b^4 = c^3, \quad a, b, c \in \mathbb{Z}, \quad abc \neq 0, \quad \gcd(a,b,c) = 1. \tag{27}$$

In this section, we will attempt to indicate why, despite this, the aforementioned attributions are in fact correct. It is worth mentioning that the equations $a^4 \pm b^4 = c^3$ are also explicitly solved in Cohen [27] (as Proposition 14.6.6).

5.1. **Reduction to elliptic generalized Fermat equations.** First of all, it is quite elementary to reduce the nonexistence of solutions to (27) (or, analogously, the equation $a^4 - b^4 = c^3$; in the sequel, we will not discuss this latter equation further) to the nonexistence of solutions to certain elliptic generalized Fermat equations of signature $(4,4,2)$. To carry this out, we note that a solution in integers a, b and c to (27) implies, via (7) (and changing the sign of t), the existence of nonzero coprime integers s and t for which

$$a^2 = s(s^2 - 3t^2) \tag{28}$$

$$b^2 = t(t^2 - 3s^2) \tag{29}$$

(and $c = s^2 + t^2$). Without loss of generality, we assume that $3 \nmid s$. Then $\gcd(s, s^2 - 3t^2) = 1$ and, from (28), we have

$$s = \epsilon_1 \alpha^2 \tag{30}$$

$$s^2 - 3t^2 = \epsilon_1 \beta^2 \tag{31}$$

for some nonzero integers α, β and $\epsilon_1 \in \{\pm 1\}$. Using $\gcd(t, t^2 - 3s^2) \in \{1, 3\}$ and (29), we have

$$t = \epsilon_2 \gamma^2 \tag{32}$$

$$t^2 - 3s^2 = \epsilon_2 \delta^2 \tag{33}$$

for nonzero integers γ, δ and $\epsilon_2 \in \{\pm 1, \pm 3\}$. Examining (31) or (33) modulo 4, shows that $\epsilon_1, \epsilon_2 \not\equiv -1 \pmod 4$. Considering these equations simultaneously modulo 8, now shows that $\epsilon_2 \neq 1$. It follows that we have

$$\epsilon_1 = 1 \quad \text{and} \quad \epsilon_2 = -3.$$

Substituting (30) and (32) in equation (31) now yields

$$\alpha^4 - 27\gamma^4 = \beta^2, \tag{34}$$

while substituting (30) and (32) in (33) yields

$$\alpha^4 - 3\gamma^4 = \delta^2. \tag{35}$$

5.2. **Relation to work of Lucas.** In the the preceding subsection, we showed that in order to prove that there are no solutions to (27), it suffices to demonstrate that one of the Diophantine equations (34) or (35) does not have solutions in nonzero integers. In [64, Chapitre I] and [65, Chapitre III], Lucas studied the Diophantine equation $Ax^4 + By^4 = Cz^2$ in unknown integers x, y, z, using Fermat's method of descent. Here, A, B and C are integers whose prime divisors are contained in $\{2, 3\}$. His chief concern, however, was not with explicitly showing that a given equation of this shape has no nontrivial solutions, but rather in describing nontrivial solutions in the cases where they exist. In [64, Chapitre I, §X] a description of all the equations $Ax^4 + By^4 = Cz^2$ as above that do have nontrivial solutions is recorded, together with a reference to the explicit solutions. For the other equations $Ax^4 + By^4 = Cz^2$, including (34) and (35), it is simply stated that there are no nontrivial solutions, without explicit proof of this fact. In these references, however, Lucas clearly demonstrates his mastery of Fermat's method of descent and one can check that this method indeed applies immediately to prove the nonexistence of nontrivial solutions in these cases. This provides convincing evidence that Lucas had proofs for his claims that there are no nontrivial solutions to (34) and (35), amongst others (which he failed to record, apparently as he considered these cases to be lacking in interest!).

6. Future work

A problem of serious difficulty that likely awaits fundamentally new techniques is that of solving equation (1) for, say, fixed r and infinite, unbounded families p and q, with $\gcd(p, q) = 1$. A truly spectacular result at this stage would be to solve an infinite family where p, q and r are pairwise coprime. Indeed, solving a single new equation of this form will likely cost considerable effort using current techniques.

A limitation of the modular method at present is that the possible exponents (p, q, r) must relate to a moduli space of elliptic curves (or more generally, abelian varieties of GL_2-type). For general (p, q, r), this is not the case. When this precondition holds, the modular method can be viewed as a technique for reducing the problem of resolving (1) to that of studying certain rational points on these moduli spaces through Galois representations. The inability to carry out the modular method in such a situation relates to a lack of sufficiently strong methods for effectively bounding these rational points (i.e. Mazur's method fails or has not been developed). We note however that irreducibility is typically easier to prove because the Frey-Hellegouarch curves encountered will have semi-stable reduction away from small primes – this allows Dieulefait and Freitas [43], and Freitas [47], for instance, to prove irreducibility without resort to a Mazur-type result (essentially, via modifications of a method of Serre [78, p. 314, Corollaire 2] which predates and is used in Mazur [66]).

For general (p, q, r), Darmon [36] constructs Frey-Hellegouarch abelian varieties of GL_2-type over a totally real field and established modularity in some cases; the analogous modular curves are, in general, quotients of the complex upper half plane by non-arithmetic Fuchsian groups.

The ABC conjecture implies that there are only finitely many solutions to (1) in coprime integers once $\min\{p, q, r\} \geq 3$. In addition, an effective version of the ABC conjecture would imply an effective bound on the size of the solutions, though this effectivity needs to be within computational range to allow a complete quantitative resolution of (1).

7. Acknowledgments

The authors would like to thank the anonymous referee for numerous suggestions that improved the readability of this paper.

References

[1] M. Bennett. The equation $x^{2n} + y^{2n} = z^5$, *J. Théor. Nombres Bordeaux* 18 (2006), no. 2, 315–321.

[2] M. Bennett and I. Chen, Multi-Frey $\mathbb{Q}$-curves and the Diophantine equation $a^2 + b^6 = c^n$, *Algebra Number Theory* 6 (2012), no. 4, 707–730.

[3] M. Bennett, I. Chen, S. Dahmen and S. Yazdani, On the equation $a^3 + b^{3n} = c^2$, *Acta Arith.*, to appear.

[4] M. Bennett and S. Dahmen. Klein forms and the generalized superelliptic equation, *Ann. of Math.* 77 (2013), 171–239.

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

[6] M. Bennett, F. Luca and J. Mulholland. Twisted extensions of the cubic case of Fermat's last theorem, Ann. Sci. Math. Québec 35 (2011), 1–15.

[7] M. Bennett and J. Mulholland. On the Diophantine equation $x^n + y^n = 2^\alpha p z^2$, C. R. Math. Acad. Sci. Soc. R. Can. 28 (2006), 6–11.

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

[9] M. Bennett, V. Vatsal and S. Yazdani. Ternary Diophantine equations of signature $(p, p, 3)$, *Compositio Math.* 140 (2004), 1399–1416.

[10] F. Beukers. The Diophantine equation $Ax^p + By^q = Cz^r$, *Duke Math. J.* 91 (1998), 61–88.

[11] F. Beukers. The generalized Fermat equation, see : `http://www.staff.science.uu.nl/~beuke106/Fermatlectures.pdf`

[12] N. Billerey. Équations de Fermat de type $(5, 5, p)$, *Bull. Austral. Math. Soc.* 76 (2007), 161–194.

[13] N. Billerey and L.V. Dieulefait. Solving Fermat-type equations $x^5 + y^5 = dz^p$, *Math. Comp.* 79 (2010), 535–544.

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

[15] C. Breuil, B. Conrad, F. Diamond and R. Taylor, On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.*14 No. 4 (2001), 843–939.

[16] D. Brown. Primitive Integral Solutions to $x^2 + y^3 = z^{10}$, Int. Math. Res. Not. IMRN 2012 (2012), 423–436.

[17] N. Bruin. The Diophantine equations $x^2 \pm y^4 = \pm z^6$ and $x^2 + y^8 = z^3$, *Compositio Math.* 118 (1999), 305–321.

[18] N. Bruin. On powers as sums of two cubes, In *Algorithmic Number Theory* (Leiden, 2000), Lecture Notes in Comput. Sci., vol 1838, Springer, Berlin, 2000, pp. 169–184.

[19] N. Bruin. Chabauty methods using elliptic curves, *J. Reine Angew. Math.* 562 (2003), 27–49.

[20] N. Bruin. The primitive solutions to $x^3 + y^9 = z^2$, *J. Number Theory* 111 (2005), no. 1, 179–189.

[21] Y. Bugeaud, F. Luca, M. Mignotte and S. Siksek. Almost powers in the Lucas sequences, *J. Théor. Nombres Bordeaux* 20 (2008), 555–600.

[22] Y. Bugeaud, M. Mignotte and S. Siksek. A multi-Frey approach to some multi-parameter families of Diophantine equations, *Canad. J. Math.* 60 (2008), 491–519.

[23] I. Chen. On the equation $s^2 + y^{2p} = \alpha^3$, *Math. Comp.* 77 (2008), 1223–1227.

[24] I. Chen. On the equation $a^2 + b^{2p} = c^5$, *Acta Arith.* 143 (2010), 345–375.

[25] I. Chen. On the equation $a^2 - 2b^6 = c^p$, *LMS J. Comput. Math.* 15 (2012), no. 1, 158–171.

[26] I. Chen and S. Siksek. Perfect powers expressible as sums of two cubes, *J. Algebra* 322 (2009), 638–656.

[27] H. Cohen. Number Theory, Vol. II : Analytic and Modern Tools, Springer-Verlag, GTM 240, 2007.

[28] A. Dabrowski. On integers represented by $x^4 - y^4$, *Bull. Austral. Math. Soc.* 76 (2007), 133–136.

[29] A. Dabrowski. On a class of generalized Fermat equations, *Bull. Austral. Math. Soc.* 82 (2010), 505–510.

[30] S. Dahmen. Classical and modular methods applied to Diophantine equations, PhD thesis, University of Utrecht, 2008. Permanently available at
`http://igitur-archive.library.uu.nl/dissertations/2008-0820-200949/UUindex.html`

[31] S. Dahmen. A refined modular approach to the Diophantine equation $x^2 + y^{2n} = z^3$, *Int. J. Number Theory* 7 (2011), no. 5, 1303–1316.

[32] S. Dahmen and S. Siksek, Perfect powers expressible as sums of two fifth or seventh powers, *Acta Arith.*, to appear.

[33] H. Darmon. On the equations $x^n + y^n = z^2$ and $x^n + y^n = z^3$, *Duke IMRN* 72 (1993), 263–274.

[34] H. Darmon. The equation $x^4 - y^4 = z^p$, *C.R. Math. Rep. Acad. Sci. Canada* 15 (1993), 286–290.

[35] H. Darmon. Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation, *C.R. Math. Rep. Acad. Sci. Canada* 19 (1997), 3–14.

[36] H. Darmon. Rigid local systems, Hilbert modular forms, and Fermat's Last Theorem, *Duke. Math. J.* 102 (2000), 413–449.

[37] H. Darmon. A fourteenth lecture on Fermat's last theorem. Number theory, 103–115, CRM Proc. Lecture Notes, 36, Amer. Math. Soc., Providence, RI, 2004.

[38] H. Darmon, F. Diamond and R. Taylor. Fermat's Last Theorem, In *Elliptic curves, modular forms & Fermat's Last Theorem (Hong Kong, 1993)*, pages 2–140. International Press, 1997.

[39] H. Darmon and A. Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$, *Bull. London Math. Soc.* 27 (1995), 513–543.

[40] H. Darmon and L. Merel. Winding quotients and some variants of Fermat's Last Theorem, *J. Reine Angew. Math.* 490 (1997), 81–100.

[41] L.E. Dickson, History of the theory of numbers, Vol. II: Diophantine analysis, Chelsea Publishing Co., New York, 1971.

[42] L.V. Dieulefait and N. Freitas. The Fermat-type equations $x^5 + y^5 = 2z^p$ and $x^5 + y^5 = 3z^p$ solved via $\mathbb{Q}$-curves, *Math. Comp.*, 83 (2014), 917–933.

[43] L.V. Dieulefait and N. Freitas. Fermat-type equations of signature $(13, 13, p)$ via Hilbert cuspforms, *Math. Ann.* 357 (2013), 987–1004.

[44] L.V. Dieulefait and J.J. Urroz. Solving Fermat-type equations $x^4 + dy^2 = z^p$ via modular $\mathbb{Q}$-curves over polyquadratic fields, *J. Reine Angew. Math*, 633 (2009), 183-195.

[45] J. Edwards. A complete solution to $X^2 + Y^3 + Z^5 = 0$, *J. Reine Angew. Math.* 571 (2004), 213–236.

[46] J. Ellenberg. Galois representations attached to $\mathbb{Q}$-curves and the generalized Fermat equation $A^4 + B^2 = C^p$, *Amer. J. Math.* 126 (2004), 763–787.

[47] N. Freitas. Recipes to Fermat-type equations of the form $x^r + y^r = Cz^p$, `arXiv:1203.3371 [math.NT]`.

[48] N. Freitas, B. Le Hung and S. Siksek, Elliptic curves over real quadratic fields are modular, `arXiv:1310.7088 [math.NT]`.

[49] N. Freitas and S. Siksek, Modularity and the Fermat equation over totally real fields, `arXiv:1307.3162 [math.NT]`.

[50] N. Freitas and S. Siksek, Criteria for the irreducibility of mod p representations of Frey curves, *J. Théor. Nombres Bordeaux*, to appear.

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

[52] D. Harkin, On the mathematical work of Francois-Édouard-Anatole Lucas, *Enseignement Math.* (2) 3 1957, 276–288.

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

[54] W. Ivorra. Sur les courbes hyperelliptiques cyclotomiques et les équations $x^p - y^p = cz^2$, *Dissertationes Math.* 444 (2007), 46pp.

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

[56] F. jarvis and P. Meekin. The Fermat equation over $\mathbb{Q}(\sqrt{2})$, *J. Number Th.* 109 (2004), 182–196.

[57] A. Kraus. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive, *Manuscripta Math.* 69 (1990), 353–385.

[58] A. Kraus. Sur les équations $a^p + b^p + 15c^p = 0$ et $a^p + 3b^p + 5c^p = 0$, *C. R. Acad. Sci. Par. Sér. I Math.* 322 (1996), 809–812.

[59] A. Kraus. Majorations effectives pour l'équation de Fermat généralisée, *Canad. J. Math.* **49** (1997), no. 6, 1139–1161.

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

[61] A. Kraus. On the equation $x^p + y^q = z^r$: a survey, *Ramanujan J.* 3 (1999), 315–333.

[62] A. Kraus. Une question sur les équations $x^m - y^m = Rz^n$, *Compositio Math.* 132 (2002), 1–26.

[63] K. Krawciow. On generalized Fermat equations of signature $(p, p, 3)$, *Colloq. Math.* 123 (2011), 49–52.

[64] É. Lucas, *Recherches sur l'analyse indéterminée et l'arithmètique de Diophante*, extrait du Bulletin de la Société d'émulation du Département de l'Allier, 12, 1873, 441–532; Moulins, 1873, imprimerie de C. Desrosiers. Online at `http://edouardlucas.free.fr/pdf/oeuvres/diophante.pdf`

[65] É. Lucas, *Recherches sur plusieurs ouvrages de Léonard de Pise et sur diverses questions d'arithmétique supérieure*, extrait du Bullettino di Bibliografia e di Sioria delle Scienze matematiche e fisiche, 10, 1877, 129–193 and 239–293; Rome, 1877, imprimerie des sciences mathématiques et physiques. Online at `http://edouardlucas.free.fr/pdf/oeuvres/Leonard_de_Pise.pdf`

[66] B. Mazur. Rational isogenies of prime degree, *Invent. Math.* 44 (1978), no. 2, 129–162.

[67] R. Mauldin. A generalization of Fermat's Last Theorem: the Beal conjecture and prize problem, *Notices Amer. Math. Soc.* 44 (1997), 1436–1437.

[68] F. Momose. Rational points on the modular curves $X_{\mathrm{split}}(p)$, *Compositio Math.* 52 (1984), no. 1, 115–137.

[69] L. Merel. Arithmetic of elliptic curves and diophantine equations, *J. Théor. Nombres Bordeaux* 11 (1999), 173–200.

[70] J. Milne. On the arithmetic of abelian varieties, *Invent. Math.* 17 (1972), 177–190.

[71] B. Poonen. Some Diophantine equations of the form $x^n + y^n = z^m$, *Acta Arith.* 86 (1998), 193–205.

[72] B. Poonen, E. Schaefer and M. Stoll. Twists of $X(7)$ and primitive solutions to $x^2 + y^3 = z^7$, *Duke Math. J.* 137 (2007), 103–158.

[73] J. Quer. $\mathbb{Q}$-curves and abelian varieties of GL_2-type, *Proc. London Math. Soc.* 81(2000), 285–317.

[74] K. Ribet. On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, *Invent. Math.* 100 (1990), 431–476.

[75] K. Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms, In *Algebra and Topology 1992*, Korea Adv. Inst. Sci. Tech., 53–79, 1992.

[76] K. Ribet. Report on mod l representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, in Motives, Proc. Symp. Pure Math. **55**:2 (1994), 639–676.

[77] K. Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms, In *Algebra and Topology 1992*, Korea Adv. Inst. Sci. Tech., 53–79, 1992.

[78] J.-P. Serre. Propriétés galoisiennes des points d'order fini des courbes elliptiques, *Invent. Math.* 15 (1972), 259-331.

[79] J.-P. Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Duke Math. J.* 54 (1987), 179–230.

[80] J.H. Silverman. *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag, 1994.

[81] S. Siksek. Correspondence with second author, 2008.

[82] S. Siksek. Diophantine equations after Fermat's Last Theorem, *J. Théor. Nombres Bordeaux* 21 (2009), no. 2, 425–436.

[83] S. Siksek. Explicit Chabauty over number fields, *Algebra Number Theory* 7 (2013), issue 4, 765–793.

[84] S. Siksek and M. Stoll, Partial descent on hyperelliptic curves and the generalized Fermat equation $x^3+y^4+z^5=0$, *Bull. London Math. Soc.* 44 (2012), 151–166.

[85] S. Siksek and M. Stoll, The generalized Fermat equation $x^2+y^3=z^{15}$, `arXiv:1309.4421 [math.NT]`.

[86] K. Takeuchi. Commensurability classes of arithmetic triangle groups, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.* 24 (1977), 201–212.

[87] R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* 141 (1995), 553–572.

[88] R. Tijdeman. Diophantine equations and diophantine approximations, *Number theory and applications (Banff, AB, 1988)*, Kluwer Acad. Publ., Dordrecht, 1989, 215–243.

[89] A. Wiles. Modular elliptic curves and Fermat's Last Theorem, *Ann. of Math* 141 (1995), 443–551.

Michael A. Bennett, Department of Mathematics, University of British Columbia, Vancouver, British Columbia, V6T 1Z2, CANADA

E-mail address: `bennett@math.ubc.ca`

Imin Chen, Department of Mathematics, Simon Fraser University, Burnaby, British Columbia, CANADA

E-mail address: `ichen@math.sfu.ca`

Sander R. Dahmen, Department of Mathematics, VU University Amsterdam, De Boelelaan 1081a, 1081 HV Amsterdam, The Netherlands,

E-mail address: `s.r.dahmen@vu.nl`

Soroosh Yazdani, Department of Mathematics and Computer Science, University of Lethbridge, Lethbridge, Alberta, T1K 3M4, CANADA

E-mail address: `soroosh.yazdani@uleth.ca`