Bull. Aust. Math. Soc. **103** (2021), 38–49
doi:10.1017/S0004972720000441

INTEGERS REPRESENTED BY $x^4 - y^4$ REVISITED

MICHAEL A. BENNETT

(Received 12 March 2020; accepted 24 March 2020; first published online 20 May 2020)

Abstract

We sharpen earlier work of Dabrowski on near-perfect power values of the quartic form $x^4 - y^4$, through appeal to Frey curves of various signatures and related techniques.

2010 *Mathematics subject classification*: primary 11D41; secondary 11F33, 11F80, 11G05.

Keywords and phrases: Diophantine equations, Frey curves, modularity.

1. Introduction

The fact that the equation $x^4 - y^4 = z^2$ has no solutions in positive integers x, y and z was deduced centuries ago by Fermat, as an early application of the method of infinite descent. An analogous statement for the more general equation $x^4 - y^4 = z^n$, with $n \geq 2$ and $\gcd(x, y) = 1$, is of much more recent vintage, following work of Darmon [6], Darmon and Merel [8] and Ribet [17] (see also [3]).

Via similar techniques to [8] and [17], based essentially upon the modularity of Galois representations attached to (Frey) elliptic curves, Dabrowski [5] proved that the equation

$$x^4 - y^4 = 2^\alpha p^\beta z^n \tag{1.1}$$

has, for p a fixed prime with $p \neq 2^k \pm 1$ for k an integer, no solutions in coprime positive integers x, y and suitably large prime exponent n. Somewhat stronger results have been obtained in a number of papers, under the additional assumption that y is prime; see, for example, [1, 12, 18, 22].

Our first result sharpens the conclusions of [5].

Theorem 1.1. *If p is prime and α, β are nonnegative integers, then there exists an effectively computable constant $n_0 = n_0(p)$ such that (1.1) has no solutions in nonzero coprime integers x, y, z and prime $n \geq n_0$, unless $p = 2^{2^j} + 1$ for some integer $j \geq 1$ and* $xy \equiv 1 \bmod 2$.

The author was partially supported by a grant from NSERC.

An almost immediate corollary of this is the following result.

Corollary 1.2. *If p is prime with $p \neq 2^{2^j} + 1$ for any integer $j \geq 1$, then (1.1) has at most finitely many solutions in nonzero coprime integers x, y, z, nonnegative integers α, β and integer $n \geq 3$.*

We observe that the results of [5] fail to apply to Fermat and Mersenne primes (the latter a presumably infinite set), while Theorem 1.1 (and hence Corollary 1.2) is valid for all primes except Fermat primes (a set that is expected to contain only $p = 5, 17, 257$ and 65 537). For these excluded primes, we have a rather weaker conclusion; for simplicity, we restrict our statement to (1.1) with $\alpha = 0$ and $\beta = 1$.

Theorem 1.3. *If p is prime with $p = 2^{2^j} + 1$ for some integer $j \geq 3$, then there exists an effectively computable constant $n_0 = n_0(p)$ such that the equation*

$$x^4 - y^4 = pz^n \tag{1.2}$$

has no solutions in nonzero integers x, y, z and prime $n \geq n_0$ with either

$$\left(\frac{-10(2^{j-2} - 1)}{n}\right) = -1 \quad \text{or} \quad \left(\frac{-6(2^{j-1} - 3)}{n}\right) = \left(\frac{-6(2^{j-2} - 1)}{n}\right) = -1.$$

If $p \in \{5, 17\}$, (1.2) has no solutions in coprime positive integers x, y, z and prime $n > 5$.

Note that for $p = 257$, this eliminates large primes n in all but the following residue classes:

$$1, 7, 11, 49, 53, 59, 77, 103 \bmod 120.$$

For $p = 65\,537$, it excludes rather fewer primes.

It is worth observing that the obstruction to solving (1.2) for all suitably large prime n, if p is a Fermat prime, arises from the identity

$$(2^k + 1)^4 - (2^k - 1)^4 = (2^{2k} + 1)2^{k+3},$$

which provides a nontrivial solution to (1.2), if $p = 2^{2^j} + 1$, upon taking $k = 2^{j-1}$ (with $n = 7$ and $n = 11$, for $p = 257$ and $p = 65\,537$, respectively).

As we shall see, an admissible value for $n_0(p)$ is

$$n_0(p) = \left(\sqrt{8(p + 1)} + 1\right)^{2(p-1)}. \tag{1.3}$$

In practice, for reasonably small values of p, we can be much more precise. By way of example, we have the following result.

Theorem 1.4. *If p is prime with $2 \leq p < 50$, $p \neq 5, 17$, and α, β are nonnegative integers, then (1.1) has no solutions in coprime positive integers x, y, z and prime $n > 5$.*

We remark that with some work, one can treat the smaller exponents $n \in \{2, 3, 4, 5\}$, via Chabauty-type techniques and other means. Presumably, the only nontrivial solutions to (1.1) with $2 \le p < 257$ correspond to

$$\begin{gathered} n = 2 \text{ and either } p \equiv 5, 7 \bmod 8 \text{ or } p \in \{41, 137\}, \\ n = 4, p = 5, x = 3, y = 1, z = 2, \\ n = 5, p = 17, x = 5, y = 3, z = 2, \\ n = 4, p = 239, x = 120, y = 119, z = 13. \end{gathered}$$

We observe further that the restriction to coprime solutions to (1.1) is a necessary one. Indeed, if we fix any prime $p > 2$, then the identity

$$\left(\frac{p+1}{2}\right)^4 - \left(\frac{p-1}{2}\right)^4 = \left(\frac{p^2+1}{2}\right)p$$

leads to solutions to (1.2) for every $n \equiv 1 \bmod 4$, upon taking

$$x = \left(\frac{p+1}{2}\right)\left(\frac{p^2+1}{2}\right)^{(n-1)/4}, \quad y = \left(\frac{p-1}{2}\right)\left(\frac{p^2+1}{2}\right)^{(n-1)/4}, \quad z = \frac{p^2+1}{2}.$$

We proceed as follows. In Section 2, we use elementary factoring arguments to reduce the study of (1.1) to a number of ternary equations of signature (n, n, n) and $(n, n, 2)$, which we can treat through appeal to work of Kraus [10], Ivorra [9], and the author and Skinner [2]. This use of multiple Frey curves corresponding to different signatures has become quite common in the literature, and has typically been employed to rather less modest effect. Section 3 contains the proof of Theorem 1.3, which uses recent criteria for certain isomorphisms to be symplectic. In Section 4 we prove Theorem 1.4, which requires a somewhat more careful analysis of local properties of our Frey curves. Finally, in Section 5, we discuss the situation when, in (1.1), the exponent n is small, relative to the prime p. In such circumstances, things are rather less clear-cut than is the case for larger exponents.

2. Factoring and Frey curves

In this section we begin by proving Theorem 1.1 and Corollary 1.2. Suppose that $n \ge 2$ and that we have a solution to (1.1) in positive, coprime integers x, y and z, with α and β nonnegative integers such that $\beta \not\equiv 0 \bmod n$. Without loss of generality, $x > y$.

2.1. *xy* even. Assume first that xy is even (so that z is odd and $\alpha = 0$). Factoring, we have one of

$$\begin{cases} x - y = a^n \\ x + y = b^n \\ x^2 + y^2 = p^\beta c^n \end{cases}$$

or

$$\begin{cases} x \pm y = a^n \\ x \mp y = p^\beta b^n \\ x^2 + y^2 = c^n, \end{cases} \tag{2.1}$$

https://doi.org/10.1017/S0004972720000441 Published online by Cambridge University Press

for positive odd integers a, b and c. We thus find that either

$$a^{2n} + b^{2n} = 2p^\beta c^n \tag{2.2}$$

or

$$a^{2n} + p^{2\beta} b^{2n} = 2c^n. \tag{2.3}$$

Note that if $p \equiv -1 \bmod 4$, we are necessarily in cases (2.1) and (2.3).

2.2. *xy* odd. If, conversely, we suppose that xy is odd (so that either z is even or $\alpha \geq 4$), then either

$$\begin{cases} x \pm y = 2^\gamma a^n \\ x \mp y = 2b^n \\ x^2 + y^2 = 2p^\beta c^n \end{cases} \tag{2.4}$$

or

$$\begin{cases} x \pm y = 2^{\gamma_1} a^n \\ x \mp y = 2^{\gamma_2} p^\beta b^n \\ x^2 + y^2 = 2c^n, \end{cases}$$

where a, b and c are coprime, odd positive integers, and γ, γ_1 and γ_2 are suitably chosen integers with $\gamma \geq 2$, $\min\{\gamma_1, \gamma_2\} = 1$ and $\max\{\gamma_1, \gamma_2\} \geq 2$. We thus find that either

$$2^{2\gamma-2} a^{2n} + b^{2n} = p^\beta c^n \tag{2.5}$$

or

$$2^{2\gamma_1-2} a^{2n} + 2^{2\gamma_2-2} p^{2\beta} b^{2n} = c^n. \tag{2.6}$$

Once again, only the latter case can occur if $p \equiv -1 \bmod 4$. Our key result that eliminates the possibility of (1.1) having solutions when p is a Mersenne prime is the following proposition, a straightforward consequence of the observation that (2.6) defines ternary equations of both signatures (n, n, n) and $(n, n, 2)$.

Proposition 2.1. *If a, b, c, γ_1 and γ_2 are positive integers with*

$$\min\{\gamma_1, \gamma_2\} = 1 \quad \textit{and} \quad \max\{\gamma_1, \gamma_2\} \geq 2,$$

then (2.6) has no solutions in integers $n \geq 3$.

Proof. If $\gamma_1 = 1$, (2.6) can be rewritten as

$$a^{2n} - c^n = (2^{\gamma_2-1} p^\beta b^n)^2 \tag{2.7}$$

which has, by the main theorem of Darmon and Merel [8], no solutions in nonzero coprime integers for $n \geq 4$. If $n = 3$, any such solutions correspond to rational points

$$(X, Y) = \left(-\frac{c}{a^2}, \frac{2^{\gamma_2-1} p^\beta b^n}{a^3}\right)$$

on the elliptic curve $Y^2 = X^3 + 1$. This curve has rank 0 over $\mathbb{Q}$ and torsion subgroup of order 6, containing the point at infinity and those given by

$$(X, Y) \in \{(-1, 0), (0, -1), (0, 1), (2, -3), (2, 3)\}.$$

Since b and c are positive, it follows that (2.7) has no solutions in nonzero coprime a, b and c if $n \geq 3$.

If $\gamma_2 = 1$, (2.6) becomes

$$2^{2\gamma_1-2}a^{2n} - c^n = (p^\beta b^n)^2. \tag{2.8}$$

Since $\gamma_1 \geq 2$, this equation has, via [2, Theorem 1.2], no solutions in coprime integers a and c, provided $n \geq 7$ is prime. Further, it has no solutions modulo 4 for even n.

For $n \in \{3, 5\}$, solutions to (2.8) correspond to rational points (X, Y) with $X < 0$ and $Y > 0$ on the (hyper)elliptic curve $Y^2 = X^n + 2^{2k}$ for $0 \leq k \leq n-1$. If $n = 5$, by Mulholland [14, Theorem 5.1], no such points exist. If $n = 3$, each of the curves $Y^2 = X^3 + 2^{2k}$ has rank 0; once again the torsion points fail to correspond to nontrivial solutions to (2.8). □

An almost immediate consequence is the following result.

Corollary 2.2. *If x, y and z are coprime positive integers with x and y odd, then (1.1) has no solutions in prime $p \equiv -1 \bmod 4$, nonnegative integers α and β and integer $n \geq 3$.*

To complete the proof of Theorem 1.1, it remains, then, to treat (2.2), (2.3) and (2.5). We will show that for suitably large prime exponents n, the first two of these never have nontrivial solutions. We obtain a like conclusion for the third equation, unless p is a Fermat prime.

2.3. Ternary equations of signature (n, n, n). To solve (2.2), (2.3) and (2.5), we will begin by appealing to results on ternary equations of signature (n, n, n). In general, suppose we have a solution to an equation of the shape

$$A\alpha^n + B\beta^n = C\gamma^n,$$

in integers $A, B, C, \alpha, \beta, \gamma$, with $\gcd(A\alpha, B\beta) = 1$ and $n \geq 7$ prime. Without loss of generality, suppose further that

$$A\alpha^n \equiv -1 \bmod 4 \quad \text{and} \quad B\beta^n \equiv 0 \bmod 2$$

and consider the elliptic curve

$$F : Y^2 = X(X - A\alpha^n)(X + B\beta^n).$$

If we denote by

$$\rho_n^F : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_n)$$

the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the n-torsion points $F[n]$, then, combining work of Wiles [21], Taylor and Wiles [20] and Ribet [16] (see Kraus [10, Théorème 1] for details), there necessarily exists a weight-2 cuspidal newform

$$f = q + \sum_{\ell \geq 2} c_\ell(f) q^\ell$$

https://doi.org/10.1017/S0004972720000441 Published online by Cambridge University Press

of level N, for

$$N = \begin{cases} \prod_{q|ABC} q & \text{if } \nu_2(ABC) = 4 \text{ and } \alpha\beta\gamma \equiv 1 \bmod 2, \\ 2^3 \prod_{q|ABC} q & \text{if } \nu_2(ABC) = 2 \text{ or } 3 \text{ and } \alpha\beta\gamma \equiv 1 \bmod 2, \\ 2^5 \prod_{q|ABC} q & \text{if } \nu_2(ABC) = 1 \text{ and } \alpha\beta\gamma \equiv 1 \bmod 2, \\ 2 \prod_{q|ABC} q & \text{otherwise,} \end{cases}$$

where each product is taken over odd primes q, with the property that if we write $K = K_f = \mathbb{Q}(c_2, c_3, \ldots)$, there exists some prime ideal $\mathfrak{n} \mid n$ with

$$a_\ell(F) \equiv c_\ell(f) \bmod \mathfrak{n} \quad \text{for all prime } \ell \nmid Nn\alpha\beta\gamma \tag{2.9}$$

and

$$\pm(\ell + 1) \equiv c_\ell(f) \bmod \mathfrak{n} \quad \text{for all prime } \ell \nmid Nn, \ell \mid \alpha\beta\gamma. \tag{2.10}$$

Here, for shorthand, we write $F \sim_n f$ and say that F *arises modulo* n *from* f.

Further, from Kraus [10, Théorème 1], we either have

$$n < \left(\left(\frac{N}{6} \prod_{\substack{l|N \\ l \text{ prime}}} \left(1 + \frac{1}{l}\right) \right)^{1/2} + 1 \right)^{2g_0^+(N)},$$

where $g_0^+(N)$ denotes the dimension of the space of cuspidal, weight-2, level-N newforms, or $K = \mathbb{Q}$ and $F \sim_n E$, for an elliptic curve $E/\mathbb{Q}$ of conductor N with full rational 2-torsion.

In the case of (2.2), (2.3) and (2.5), necessarily $N = 2^\kappa \cdot p$, where $\kappa \in \{0, 1, 3, 5\}$. To classify these p for which there exist elliptic curves of corresponding conductors and full rational 2-torsion, we turn to work of Ivorra [9].

PROPOSITION 2.3. *If $p > 2$ is prime, then there exists an elliptic curve $E/\mathbb{Q}$ with full rational 2-torsion and conductor $N = 2^\kappa \cdot p$ precisely when E is isogenous to*

$$E' : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

for a_i, p and κ as follows:

p	κ	$(a_1, a_2, a_3, a_4, a_6)$
3	3, 4, 5	$(0, \pm1, 0, 1, 0), (0, \pm1, 0, -2, 0)$
3	6	$(0, \pm1, 0, -4, \pm2), (0, \pm1, 0, 3, \pm3)$
5	3, 4, 6	$(0, 0, 0, -2, \pm1), (0, 0, 0, -8, \pm8)$
7	3, 4, 6	$(0, 0, 0, 1, \pm2), (0, 0, 0, 4, \pm16)$
17	0	$(1, -1, 1, -1, 0)$
$2^k - 1$	1	$(1, 2^{k-2}, 0, 2^{k-4}, 0), k \geq 5$
$2^k - 1$	4	$(0, -2^k - 2, 0, -2^k - 1, 0), k \geq 5$
$2^k + 1$	1	$(1, -2^{k-2}, 0, -2^{k-4}, 0), k \geq 8$
$2^k + 1$	4	$(0, 2^k + 2, 0, 2^k + 1, 0), k \geq 8.$

https://doi.org/10.1017/S0004972720000441 Published online by Cambridge University Press

For (2.2) and (2.3), we have $N = 2^5 \cdot p$ and hence, from Proposition 2.3, either $p = 3$ or, using the fact that $g_0^+(2^5 \cdot p) = p - 1$ (see Martin [13, Theorem 1]), it follows that $n < n_0(p)$, where this latter quantity is as defined in (1.3).

For (2.5), we necessarily have $p \equiv 1 \bmod 4$ and $N \in \{p, 2p, 8p\}$, whence Proposition 2.3 implies $p = 5$ (and $N = 40$, $\gamma = 2$), $p = 17$ (and $N = 17$, $\gamma = 3$) or $p = 2^k + 1$ for $k \geq 8$ (whence $N = 2p$). This completes the proof of Theorem 1.1, for all $p > 3$.

To treat the case of (2.3) with $p = 3$, we will use a Frey curve of signature $(n, n, 2)$. Suppose that $n \geq 7$ is prime and consider the curve

$$E : Y^2 = X^3 + 2 \cdot 3^\beta b^n X^2 + 2 \cdot c^n X.$$

Appealing to [2, Proposition 4.3], we have $E \sim_n f$ where f is a weight-2 cuspidal newform f, with trivial character and level 128. All such forms have $K = \mathbb{Q}$ and $c_3(f) = \pm 2$, while, from $\beta > 0$, $a_3(E) = 0$, contradicting

$$a_3(E) \equiv c_3(f) \bmod n.$$

This completes the proof of Theorem 1.1. Corollary 1.2 is now almost immediate, since (1.1) has, for fixed exponent $n \geq 3$, at most finitely many coprime solutions x, y and z, via a result of Darmon and Granville [7] (which itself is a consequence of Faltings's theorem).

3. Applications of symplectic criteria

To prove Theorem 1.3, we begin by supposing that we have a solution to (1.2) in coprime integers x, y and z, where $n > 5$ is prime. We have either xy even, whereby $F \sim_n f$ for a newform of level $N = 32p$, or xy odd, so that, from (1.2), necessarily $\gamma \geq 5$ in (2.4), whence $F \sim_n f$ for a newform of level $N = 2p$. There are no newforms at level $N = 10$. A short Magma computation reveals that, for $p \in \{5, 17\}$,

$$c_3(f) \in \{\pm 2, \pm 2\sqrt{2}\}$$

if f has level 34 or 160, or if $N = 32 \cdot 17$ and $K_f = \mathbb{Q}$. Since our Frey curve E has full rational 2-torsion (whereby $a_\ell(E) \equiv \ell + 1 \bmod 4$ for primes ℓ of good reduction), it follows from (2.9) and (2.10) that

$$0, \pm 4 \equiv \pm 2, \pm 2\sqrt{2} \bmod n,$$

contradicting $n > 5$. For higher-dimensional forms at level $32 \cdot 17$, we have $c_3(f) = \theta$ where θ satisfies one of

$$\theta^2 - 2 = 0, \quad \theta^2 - 10 = 0 \quad \text{or} \quad \theta^3 \pm 2\theta^2 - 4\theta \mp 4 = 0.$$

Once again (2.9) and (2.10) contradict $n > 5$.

We may thus suppose that $p = 2^k + 1$ with $k = 2^j \geq 8$ and that we have a corresponding solution in integers a, b, c, γ and β to (2.5), with prime $n > n_0(p)$, $\beta = 1$ and $\gamma \equiv -2 \bmod n$. Define elliptic curves

$$E_p : Y^2 + XY = X^3 - 2^{k-2} X^2 - 2^{k-4} X$$

https://doi.org/10.1017/S0004972720000441 Published online by Cambridge University Press

and

$$F_p : Y^2 = X(X + pc^n)(X + 2^{2\gamma-2}a^{2n}).$$

Then, from [10, Théorème 1] and Proposition 2.3, by a slight abuse of notation, $F_p \sim_n E_p$, so that, in particular, the curves have isomorphic n-torsion modules $E_p[n]$ and $F_p[n]$. Since these curves have multiplicative reduction at 2 and p, the fact that $n > p$ allows us to apply Kraus and Oesterlé [11, Proposition 2] with $\ell \in \{2, p\}$ to conclude that $E_p[n]$ and $F_p[n]$ are symplectically isomorphic if and only if

$$\left(\frac{\nu_\ell(\Delta(E_p))/\nu_\ell(\Delta(F_p))}{n}\right) = 1,$$

where $\nu_\ell(\Delta(E_p))$ and $\nu_\ell(\Delta(F_p))$ denote the exponents of ℓ occurring in the prime factorisations of the minimal discriminants of E_p and F_p, respectively. Since these minimal discriminants satisfy

$$\Delta(E_p) = 2^{2k-8}p^2 \quad \text{and} \quad \Delta(F_p) = 2^{4\gamma-12}p^2(a^2b^2c)^{2n},$$

taking $\ell = p$ implies that E_p and F_p are necessarily symplectically isomorphic and hence we have a contradiction from the choice of $\ell = 2$, whenever

$$\left(\frac{(2k-8)(\gamma-3)}{n}\right) = -1.$$

Since $\gamma \equiv -2 \bmod n$ and $k = 2^j$ for $j \geq 3$, this is equivalent to

$$\left(\frac{-10(2^{j-2}-1)}{n}\right) = -1.$$

Let us next view (2.5) as one of signature $(n, n, 2)$ (by considering b^{2n} as $(b^n)^2$), and write

$$G_p : Y^2 + XY = X^3 + \left(\frac{\pm b^n - 1}{4}\right)X^2 - 2^{2\gamma-8}a^{2n}X,$$

with minimal discriminant

$$\Delta(G_p) = 2^{4\gamma-16}p(a^4b^2)^n.$$

From Ivorra [9, Théorème 1], we find that $G_p \sim_n E_p$, where E_p is either

$$E_{p,1} : Y^2 + XY = X^3 - 2^{k-6}X$$

or

$$E_{p,2} : Y^2 + XY = X^3 + 2^{k-3}X^2 + 2^{2k-8}X.$$

Note that G_p does not (necessarily) have full rational 2-torsion. For these curves, we have minimal discriminants

$$\Delta(E_{p,1}) = 2^{2k-12}p \quad \text{and} \quad \Delta(E_{p,2}) = 2^{4k-16}p.$$

https://doi.org/10.1017/S0004972720000441 Published online by Cambridge University Press

Once again applying Kraus and Oesterlé [11, Proposition 2] with $\ell \in \{2, p\}$, we reach a contradiction provided

$$\left(\frac{(2k-12)(\gamma-4)}{n}\right) = -1 \quad \text{and} \quad G_p \sim_n E_{p,1}$$

or

$$\left(\frac{(k-4)(\gamma-4)}{n}\right) = -1 \quad \text{and} \quad G_p \sim_n E_{p,2}.$$

From $\gamma \equiv -2 \bmod n$ and $k = 2^j$ for $j \geq 3$, these are equivalent to

$$\left(\frac{-6(2^{j-1}-3)}{n}\right) = -1 \quad \text{and} \quad G_p \sim_n E_{p,1}$$

and

$$\left(\frac{-6(2^{j-2}-1)}{n}\right) = -1 \quad \text{and} \quad G_p \sim_n E_{p,2}.$$

This completes the proof of Theorem 1.3.

4. Proof of Theorem 1.4

From the arguments leading to Theorem 1.1 and Proposition 2.1, we are left to treat (2.2), (2.3) and (2.5) with prime p satisfying $7 \leq p < 50$, $p \neq 17$, and exponents $n \geq 7$ prime and bounded above by $n_0(p)$. Arguing as previously, and applying (2.9) and (2.10), there necessarily exist a weight-2, cuspidal newform f of level $N = 2p$ or $N = 32p$, and an ideal $\mathfrak{n} \mid n$ in K_f, such that, for every odd prime $\ell \nmid np$,

$$c_\ell(F) \equiv \kappa \bmod \mathfrak{n},$$

where either $\kappa = \pm(\ell + 1)$ or

$$|\kappa| < 2\sqrt{\ell} \quad \text{and} \quad \kappa \equiv \ell + 1 \bmod 4.$$

Note that, if $K_f = \mathbb{Q}$, we can actually obtain these congruences in the case $\ell = n$ as well. A relatively short computation in Magma using admissible $\ell < 100$ contradicts our assumption that $n \geq 7$ in almost all cases. In fact, if $N = 2p$ (where we may restrict attention to $p \equiv 1 \bmod 4$ and (2.5)), we are left to treat only one form f of level $2p$ for $(p, n) = (13, 7)$, and only one form of level $32p$ for $(p, n) = (43, 11)$. For these pairs (p, n), we will work somewhat more carefully. If we have a solution to (2.5) with $(p, n) = (13, 7)$, then the obstruction to reaching our desired conclusion corresponds to an elliptic curve E (that is, $K_f = \mathbb{Q}$), denoted 26b in Cremona's tables, for which

$$a_\ell(E) \equiv \ell + 1 \bmod 7$$

for all odd primes $\ell \neq 13$. We may thus suppose, in particular, that our solution to (2.5) has the property that $3 \mid abc$. Since c divides a sum of two coprime squares, necessarily $3 \mid a$ or $3 \mid b$. Treating (2.5) as having signature $(7, 7, 2)$ (by considering $2^{2\gamma-2}a^{14}$ or b^{14} as squares if $3 \mid a$ or $3 \mid b$, respectively) and appealing to [2], we construct a Frey curve

F with $F \sim_7 f$ for a form of level $2^7 \cdot 13$ if $3 \mid a$ and level $2 \cdot 13$ if $3 \mid b$, and, in either case, $a_3(F) = 0$. We check via Magma that this, in every case, contradicts (2.9).

To complete the proof of Theorem 1.4, it remains to handle the case of (2.3) with $(p, n) = (43, 11)$. Considering $43^{2\beta} b^{2n}$ as a square, as previously we may construct an $(11, 11, 2)$ Frey curve F, this time with $a_{43}(F) = 0$ and $F \sim_{11} f$ for a newform of level 128, so that $0 \equiv \pm 6 \bmod 11$. This contradiction finishes our proof.

5. A few comments

The fact that our techniques enable us to show that (1.1) has no coprime solutions only when the prime exponent n is suitably large as a function of p is not entirely an artefact of our approach. Indeed, it is not difficult, given $n > 2$, to construct what are likely infinite sets of primes p for which even the more restrictive (1.2) has nontrivial solutions.

By way of example, if k is a positive integer and $a > b$ are odd positive integers, then, setting

$$x = \frac{a^{2^k} + b^{2^k}}{2} \quad \text{and} \quad y = \frac{a^{2^k} - b^{2^k}}{2},$$

we have

$$x^4 - y^4 = (ab)^{2^k} F_k(a, b),$$

where

$$F_k(a, b) = \frac{a^{2^{k+1}} + b^{2^{k+1}}}{2}.$$

Since the polynomial $x^{2^{k+1}} + 1$ is irreducible, our expectation is that $F_k(a, b)$ will take on prime values infinitely often.

If $n > 3$ is prime, we may set

$$x = 2^{n-3} a^n + b^n \quad \text{and} \quad y = 2^{n-3} a^n - b^n,$$

so that

$$x^4 - y^4 = (2^{2n-6} a^{2n} + b^{2n})\,(2ab)^n.$$

We note that the polynomial $x^{2n} + 2^{2n-6}$ is irreducible for all primes $n > 3$ (but not for $n = 3$), via a classical result of Capelli [4], and hence we once again expect that the form $2^{2n-6} a^{2n} + b^{2n}$ is prime infinitely often. It is worth mentioning that, despite this expectation, the smallest primes constructed here can be quite large. If, for example, we take $n = 19$, the smallest prime for which we find a solution to (1.2) via this approach is given by

$$p = 3\,740\,434\,668\,995\,905\,047\,343\,202\,488\,519\,402\,432\,937.$$

Finally, if $n = 3$, we set

$$x = \frac{a^3 + b^3}{2} \quad \text{and} \quad y = \frac{a^3 - b^3}{2},$$

https://doi.org/10.1017/S0004972720000441 Published online by Cambridge University Press

where

$$a = s^3 - 3st^2 - 3s^2t + t^3$$

and

$$b = s^3 + 3s^2t - 3st^2 - t^3,$$

for s and t coprime integers of opposite parity. From this,

$$x^4 - y^4 = G(s,t)(ab(s^2+t^2))^3,$$

where $G(s,t)$ is equal to

$$s^{12} + 114s^{10}t^2 - 705s^8t^4 + 1436s^6t^6 - 705s^4t^8 + 114s^2t^{10} + t^{12},$$

an irreducible form. Once again, we expect that $G(s,t)$ is prime infinitely often.

If $n = 2$, it is a pleasant exercise in elementary number theory to prove the following result.

Proposition 5.1. *If p is prime, the equation*

$$x^4 - y^4 = pz^2 \tag{5.1}$$

has infinitely many solutions in coprime, nonzero integers x, y and z if p is a congruent number, and no such solutions if p is a noncongruent number.

In particular, from work of Nagell [15] and Stephens [19], (5.1) has no nonzero solutions for $p \equiv 3 \bmod 8$, and infinitely many nontrivial solutions whenever $p \equiv 5, 7 \bmod 8$; the case $p \equiv 1 \bmod 8$ is more subtle, since, for example, 17 is noncongruent and 41 is congruent.

References

[1] A. Bajolet, B. Dupuy, F. Luca and A. Togbé, 'On the Diophantine equation $x^4 - q^4 = py^r$', *Publ. Math. Debrecen* **79** (2011), 269–282.

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

[3] Z. Cao, 'The Diophantine equations $x^4 - y^4 = z^p$ and $x^4 - 1 = dy^q$', *C. R. Math. Rep. Acad. Sci. Canada* **21** (1999), 23–27.

[4] A. Capelli, 'Sulla riduttibilità della funzione $x^n - A$ in un campo qualunque di razionalità', *Math. Ann.* **54** (1901), 602–603.

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

[6] H. Darmon, 'The equation $x^4 - y^4 = z^p$', *C. R. Math. Rep. Acad. Sci. Canada.* **15**(6) (1993), 286–290.

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

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

[9] W. Ivorra, 'Courbes elliptiques sur $\mathbb{Q}$, ayant un point d'ordre 2 rationnel sur $\mathbb{Q}$, de conducteur $2^N p$' (in French) [Elliptic curves over $\mathbb{Q}$ with a rational point of order 2 over $\mathbb{Q}$ and conductor $2^N p$]', *Dissertationes Math. (Rozprawy Mat.)* **429** (2004).

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

https://doi.org/10.1017/S0004972720000441 Published online by Cambridge University Press

[11] A. Kraus and J. Oesterlé, 'Sur une question de B. Mazur', *Math. Ann.* **293** (1992), 259–275.
[12] F. Luca and A. Togbé, 'On the Diophantine equation $x^4 - q^4 = py^3$', *Rocky Mountain J. Math.* **40** (2010), 995–1008.
[13] G. Martin, 'Dimensions of the spaces of cuspforms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$', *J. Number Theory* **112** (2005), 298–331.
[14] J. Mulholland, '*Elliptic Curves with Rational 2-torsion and Related Ternary Diophantine Equations*', PhD Thesis, The University of British Columbia (Canada), 2006.
[15] T. Nagell, 'L'analyse indéterminée de degré supérieur', in: *Mémorial des sciences mathématiques,* Vol. 39 (Gauthier-Villars, Paris, 1929).
[16] K. Ribet, 'On modular representations of Gal($\overline{\mathbb{Q}}/\mathbb{Q}$) arising from modular forms', *Invent. Math.* **100** (1990), 431–476.
[17] K. Ribet, 'On the equation $a^p + 2^\alpha b^p + c^p = 0$', *Acta Arith.* **79**(1) (1997), 7–16.
[18] D. Savin, 'On the Diophantine equation $x^4 - q^4 = py^5$', *Ital. J. Pure Appl. Math.* **26** (2009), 103–108.
[19] N. M. Stephens, 'Congruence properties of congruent numbers', *Bull. Lond. Math. Soc.* **7** (1975), 182–184.
[20] R. L. Taylor and A. Wiles, 'Ring theoretic properties of certain Hecke algebras', *Ann. Math.* **141** (1995), 553–572.
[21] A. Wiles, 'Modular elliptic curves and Fermat's Last Theorem', *Ann. of Math. (2)* **141**(3) (1995), 443–551.
[22] L. Yanyan, 'On the diophantine equation $x^4 - q^4 = py^n$', *Expo. Math.* **30** (2013), 196–203.

MICHAEL A. BENNETT, Department of Mathematics,
University of British Columbia, Vancouver, BC, Canada V6T 1Z2
e-mail: bennett@math.ubc.ca