Fermat's last theorem over
some small real quadratic fields

Nuno Freitas and Samir Siksek

Fermat's last theorem over some small real quadratic fields

Nuno Freitas and Samir Siksek

Using modularity, level lowering, and explicit computations with Hilbert modular forms, Galois representations, and ray class groups, we show that for $3 \le d \le 23$, where $d \ne 5, 17$ and is squarefree, the Fermat equation $x^n + y^n = z^n$ has no nontrivial solutions over the quadratic field $\mathbb{Q}(\sqrt{d})$ for $n \ge 4$. Furthermore, we show that for $d = 17$, the same holds for prime exponents $n \equiv 3, 5 \pmod 8$.

1. Introduction

Interest in the Fermat equation

$$x^n + y^n = z^n \tag{1}$$

over various number fields goes back to the 19th and early 20th centuries, with the work of Maillet (1897) and Furtwängler (1910) [Dickson 1920, pages 758 and 768]. However, until the current work, the only number fields for which Fermat's last theorem has been proved are $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$. These proofs are respectively due to Wiles [1995] (as consequence of his ground-breaking proof of modularity of semistable elliptic curves over $\mathbb{Q}$) and to Jarvis and Meekin [2004]. The precise statements are that if $K = \mathbb{Q}$ and $n \ge 3$ or $K = \mathbb{Q}(\sqrt{2})$ and $n \ge 4$, then the only solutions to (1) in K are the trivial ones satisfying $xyz = 0$. In [Freitas and Siksek 2015], it is shown that for five-sixths of real quadratic fields K, there is a bound B_K such that for prime exponents $n \ge B_K$, the only solutions to the Fermat equation (1) over K are the trivial ones. This paper is concerned with proving Fermat's last theorem for several other real quadratic fields. Our main results are the following two theorems.

Theorem 1. *Let $3 \le d \le 23$ be squarefree with $d \ne 5, 17$. Then the Fermat equation (1) does not have any nontrivial solutions over $\mathbb{Q}(\sqrt{d})$ with exponent $n \ge 4$.*

Theorem 2. *The Fermat equation (1) has no nontrivial solutions over $\mathbb{Q}(\sqrt{17})$ for prime exponents $n \geq 5$ satisfying $n \equiv 3, 5 \pmod{8}$.*

Remark. For $n = 3$, equation (1) defines an elliptic curve having rank 0 over $\mathbb{Q}$; it does, however, have positive rank over some of the quadratic fields in the statement of Theorem 1. We therefore impose $n \geq 4$.

It is sufficient to prove Theorem 1 for exponents $n = 4, 6, 9$, and for prime exponents $n = p \geq 5$. In fact, all solutions to the Fermat equation in quadratic fields for $n = 4, 6, 9$ have been determined by Aigner [1934; 1957]. These are all defined over imaginary quadratic fields except for the trivial solutions. We may therefore restrict our attention to prime exponents $n = p \geq 5$.

Let $d \geq 2$ be a squarefree positive integer, and let $K = \mathbb{Q}(\sqrt{d})$, and write $\mathcal{O}_K$ for its ring of integers. By the *Fermat equation with exponent p over K*, we mean the equation

$$a^p + b^p + c^p = 0, \quad a, b, c \in \mathcal{O}_K. \tag{2}$$

A solution (a, b, c) is called *trivial* if $abc = 0$, otherwise it is *nontrivial*. For $p = 5, 7, 11$, all solutions of degree at most $(p-1)/2$ have been determined by Gross and Rohrlich [1978, Theorem 5]. It turns out that the only nontrivial quadratic solutions are permutations of $(1, \omega, \omega^2)$, where ω is a primitive cube root of unity. For $p = 13$, the same was shown to be true by Tzermias [2004]. We shall therefore henceforth assume that $p \geq 17$.

A brief overview of the method and difficulties. As in the proof of Fermat's last theorem over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$, let (a, b, c) be a nontrivial solution to the Fermat equation (2), and consider the Frey elliptic curve

$$E_{a,b,c} : Y^2 = X(X - a^p)(X + b^p). \tag{3}$$

Write $E = E_{a,b,c}$ and denote by $\bar{\rho}_{E,p}$ its mod p Galois representation. An essential fact to the proof of Fermat's last theorem over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$ is the modularity of the Frey curve. Modularity of elliptic curves over all real quadratic fields is now known (see [Freitas et al. 2014]). In particular, our Frey curve $E_{a,b,c}$ is modular over K. The proof of Fermat's last theorem over $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2})$ makes essential use of the fact that it is always possible to scale and permute the hypothetical nontrivial solution so that not only are a, b, c algebraic integers, but they are also coprime, and they satisfy additional 2-adic restrictions; over $\mathbb{Q}$, these are $a \equiv -1 \pmod 4$ and $2 \mid b$. In both cases, a suitable choice of scaling produces a semistable Frey curve $E_{a,b,c}$. Applying suitable level-lowering results to the modular Galois representation $\bar{\rho}_{E,p}$ shows that it arises from an eigenform of level 2 for $\mathbb{Q}$, and a Hilbert eigenform of level $\sqrt{2}$ for $\mathbb{Q}(\sqrt{2})$. There are no eigenforms at these levels, giving a contradiction and completing the proof for both fields.

It should be possible to carry out the same level lowering strategy over any real quadratic field K. To build on this and prove Fermat's last theorem over K there are, however, three principal difficulties:

(a) Verifying the irreducibility of $\bar{\rho}_{E,p}$; this is required for applying level lowering theorems.

(b) Computing the newforms at the levels predicted by conductor computations and level lowering; in general, these levels depend on the class and unit groups of K and are not of small norm.

(c) Dealing with the newforms found at these levels; in general, these spaces will be nonzero.

In [Freitas and Siksek 2015], it is shown that these difficulties disappear for $p > C_K$, where C_K is some inexplicit constant, for five-sixths of real quadratic fields K. In this paper, we show how to deal with (a), (b), (c) for the fields in the statement of Theorem 1. For $K = \mathbb{Q}(\sqrt{d})$ with $d = 5, 17$, our method for (c) fails. However, for $d = 17$, we are still able to prove Fermat's last theorem for half of exponents p using an argument of Halberstadt and Kraus [2002], yielding Theorem 2.

For $K = \mathbb{Q}$, it follows from Mazur's celebrated theorem on isogenies [1978] that $\bar{\rho}_{E,p}$ is irreducible for the Frey curve E and $p \geq 5$. The analogue of Mazur's theorem is not known for any other number field. However, Kraus shows that for K, a real quadratic field of class number 1, and E, a semistable elliptic curve over K, if $\bar{\rho}_{E,p}$ is reducible, then $p \leq 13$ or ramifies in K or $p \mid \text{Norm}_{K/\mathbb{Q}}(u^2 - 1)$, where u is a fundamental unit of K. It is possible to give corresponding bounds for p when the class group is nontrivial and E has some fixed set of additive primes (see for example [David 2012]), although these bounds are considerably worse. In Section 6, we overcome these difficulties for the fields in Theorem 1 through explicit class field theory computations. Without this, we would not have been able to deal with small exponents p.

Assuming modularity of the Frey curve, it should be possible to apply the same strategy to the Fermat equation over many totally real fields, although the computation of newforms for totally real fields with either large degree or large discriminant is likely to be impractical. In Section 9, we illustrate this by looking at $\mathbb{Q}(\sqrt{30})$ and $\mathbb{Q}(\sqrt{79})$. At the end of that section, we also include a comparison between the recipes of the current paper and those of [Freitas and Siksek 2015], illustrating the need for the improvements in the current work.

The computations in this paper were carried out on the computer algebra system Magma [Bosma et al. 1997]. In particular, we have used Magma's Hilbert modular forms package (for the theory see [Dembélé and Donnelly 2008] and [Dembélé and Voight 2013]) and class field theory package (due to C. Fieker).

Notational conventions. Throughout, p denotes an odd rational prime, and K a totally real number field, with ring of integers $\mathcal{O}_K$. We write S for the set of prime ideals in $\mathcal{O}_K$ dividing 2. For a nonzero ideal $\mathfrak{a}$ of $\mathcal{O}_K$, we denote by $[\mathfrak{a}]$ the class of $\mathfrak{a}$ in the class group $\mathrm{Cl}(K)$. For a nontrivial solution (a, b, c) to the Fermat equation (2), let

$$\mathcal{G}_{a,b,c} := a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K, \tag{4}$$

and let $[a, b, c]$ denote the class of $\mathcal{G}_{a,b,c}$ in $\mathrm{Cl}(K)$. We exploit the well-known fact (e.g., [Cassels and Fröhlich 1967, Theorem VIII.4]) that every ideal class contains infinitely many prime ideals. Let $r = \#(\mathrm{Cl}(K)/\mathrm{Cl}(K)^2)$. Let $\mathfrak{m}_1 = 1 \cdot \mathcal{O}_K$, and fix, once and for all, odd prime ideals $\mathfrak{m}_2, \ldots, \mathfrak{m}_r$ such that $[\mathfrak{m}_1], \ldots, [\mathfrak{m}_r]$ represent the cosets of $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2$. Let

$$\mathcal{H} = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}.$$

Let $G_K = \mathrm{Gal}(\overline{K}/K)$. For an elliptic curve E/K, we write

$$\bar{\rho}_{E,p} : G_K \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p) \tag{5}$$

for the representation of G_K on the p-torsion of E. For a Hilbert eigenform $\mathfrak{f}$ of parallel weight 2 over K, we let $\mathbb{Q}_{\mathfrak{f}}$ denote the field generated by its eigenvalues. In this situation, ϖ will denote a prime of $\mathbb{Q}_{\mathfrak{f}}$ above p; of course, if $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$, we write p instead of ϖ. All other primes we consider are primes of K. We reserve the symbol $\mathfrak{P}$ for primes belonging to S, and $\mathfrak{m}$ for primes belonging to $\mathcal{H}$. An arbitrary prime of K is denoted by $\mathfrak{q}$, and $G_{\mathfrak{q}}$ and $I_{\mathfrak{q}}$ are the decomposition and inertia subgroups of G_K at $\mathfrak{q}$.

2. Level lowering

We need a level lowering result that plays the role of the Ribet step [1990] in the proof of Fermat's last theorem. The following theorem is deduced in [Freitas and Siksek 2015] from the work of Fujiwara [2006], Jarvis [2004] and Rajaei [2001].

Theorem 3. *Let K be a real quadratic field, and E/K an elliptic curve of conductor $\mathcal{N}$. Let p be a rational prime. For a prime ideal $\mathfrak{q}$ of K denote by $\Delta_{\mathfrak{q}}$ the discriminant of a local minimal model for E at $\mathfrak{q}$. Let*

$$\mathcal{M}_p := \prod_{\substack{\mathfrak{q} \mid \mathcal{N}, \\ p \mid v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})}} \mathfrak{q} \quad and \quad \mathcal{N}_p := \frac{\mathcal{N}}{\mathcal{M}_p}. \tag{6}$$

Suppose the following:

  (i) *Either $p \geq 5$, or $K = \mathbb{Q}(\sqrt{5})$ and $p \geq 7$.*

  (ii) *E is modular.*

  (iii) $\bar{\rho}_{E,p}$ is irreducible.

  (iv) E is semistable at all $\mathfrak{q} \mid p$.

  (v) $p \mid v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$ for all $\mathfrak{q} \mid p$.

Then, there is a Hilbert eigenform $\mathfrak{f}$ of parallel weight 2 that is new at level $\mathcal{N}_p$ and some prime ϖ of $\mathbb{Q}_{\mathfrak{f}}$ such that $\varpi \mid p$ and $\bar{\rho}_{E,p} \sim \bar{\rho}_{\mathfrak{f},\varpi}$.

3. Scaling and the odd part of the level

Let (a, b, c) be a nontrivial solution to the Fermat equation (2). Let $\mathcal{G}_{a,b,c}$ be as given in (4), which we think of as the greatest common divisor of a, b, c. An odd prime not dividing $\mathcal{G}_{a,b,c}$ is a prime of good or multiplicative reduction for $E_{a,b,c}$ and does not appear in the final level $\mathcal{N}_p$, as we see in due course. An odd prime dividing $\mathcal{G}_{a,b,c}$ exactly once is an additive prime and does appear in $\mathcal{N}_p$. To control $\mathcal{N}_p$, we need to control $\mathcal{G}_{a,b,c}$.

Scaling. We refer to page 878 for the notation.

Lemma 3.1. *Let (a, b, c) be a nontrivial solution to (2). There is a nontrivial integral solution (a', b', c') to (2) and some $\mathfrak{m} \in \mathcal{H}$ such that the following hold:*

  (i) *For some $\xi \in K^*$, we have $a' = \xi a$, $b' = \xi b$, $c' = \xi c$.*

  (ii) *$\mathcal{G}_{a',b',c'} = \mathfrak{m} \cdot \mathfrak{r}^2$, where $\mathfrak{r}$ is an odd prime ideal with $\mathfrak{r} \neq \mathfrak{m}$.*

  (iii) *$[a', b', c'] = [a, b, c]$.*

Proof. Recall that $\mathcal{H} = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_r\}$ and that $[\mathfrak{m}_1], \ldots, [\mathfrak{m}_r]$ represent the cosets of $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2$. Thus for some $\mathfrak{m} \in \mathcal{H}$, we have $[a, b, c] = [\mathfrak{m}] \cdot [\mathfrak{b}]^2$, where $\mathfrak{b}$ is a fractional ideal. Now every ideal class is represented by infinitely many prime ideals. Thus there is an odd prime ideal $\mathfrak{r} \neq \mathfrak{m}$ such that $[a, b, c] = [\mathfrak{m}] \cdot [\mathfrak{r}]^2$. It follows that $\mathfrak{m} \cdot \mathfrak{r}^2 = (\xi) \cdot \mathcal{G}_{a,b,c}$ for some $\xi \in K^*$. Let a', b', c' be as in (i). Note that

$$(a') = (\xi) \cdot (a) = \mathfrak{m} \cdot \mathfrak{r}^2 \cdot \mathcal{G}_{a,b,c}^{-1} \cdot (a),$$

which is an integral ideal since $\mathcal{G}_{a,b,c}$ (by its definition) divides a. Thus a' is in $\mathcal{O}_K$ and similarly so are b' and c'. For (ii) and (iii), note that

$$\mathcal{G}_{a',b',c'} = a'\mathcal{O}_K + b'\mathcal{O}_K + c'\mathcal{O}_K = (\xi) \cdot (a\mathcal{O}_K + b\mathcal{O}_K + c\mathcal{O}_K) = (\xi) \cdot \mathcal{G}_{a,b,c} = \mathfrak{m} \cdot \mathfrak{r}^2. \quad \square$$

Behaviour at odd primes. For $u, v, w \in \mathcal{O}_K$ such that $uvw \neq 0$ and $u + v + w = 0$, let

$$E : y^2 = x(x - u)(x + v). \tag{7}$$

The invariants c_4, c_6, Δ, j have their usual meanings and are given by

$$c_4 = 16(u^2 - vw) = 16(v^2 - wu) = 16(w^2 - uv),$$

$$c_6 = -32(u - v)(v - w)(w - u), \quad \Delta = 16u^2v^2w^2, \quad j = c_4^3/\Delta. \tag{8}$$

The following elementary lemma is a straightforward consequence of the properties of elliptic curves over local fields (e.g., [Silverman 1986, §VII.1 and §VII.5]).

Lemma 3.2. *With the above notation, let* $\mathfrak{q} \nmid 2$ *be a prime and let*

$$s = \min\{\upsilon_\mathfrak{q}(u), \upsilon_\mathfrak{q}(v), \upsilon_\mathfrak{q}(w)\}.$$

Write $E_{\min}$ *for a local minimal model at* $\mathfrak{q}$.

 (i) $E_{\min}$ *has good reduction at* $\mathfrak{q}$ *if and only if s is even and*

$$\upsilon_\mathfrak{q}(u) = \upsilon_\mathfrak{q}(v) = \upsilon_\mathfrak{q}(w). \tag{9}$$

 (ii) $E_{\min}$ *has multiplicative reduction at* $\mathfrak{q}$ *if and only if s is even and* (9) *fails to hold. In this case, the minimal discriminant* $\Delta_\mathfrak{q}$ *at* $\mathfrak{q}$ *satisfies*

$$\upsilon_\mathfrak{q}(\Delta_\mathfrak{q}) = 2\upsilon_\mathfrak{q}(u) + 2\upsilon_\mathfrak{q}(v) + 2\upsilon_\mathfrak{q}(w) - 6s.$$

 (iii) $E_{\min}$ *has additive potentially multiplicative reduction at* $\mathfrak{q}$ *if and only if s is odd and* (9) *fails to hold.*

 (iv) $E_{\min}$ *has additive potentially good reduction at* $\mathfrak{q}$ *if and only if s is odd and* (9) *holds. Moreover, E acquires good reduction over a quadratic extension of* $K_\mathfrak{q}$.

The odd part of the level. Let (a, b, c) be a nontrivial solution to the Fermat equation (2) with odd prime exponent p. Write E for the Frey curve in (3). Let $\mathcal{N}$ be the conductor of E and let $\mathcal{N}_p$ be as defined in (6). Recall that S is the set of prime ideals $\mathfrak{P}$ dividing 2. We define the *even parts* of $\mathcal{N}$ and $\mathcal{N}_p$ by

$$\mathcal{N}^{\text{even}} = \prod_{\mathfrak{P}\in S} \mathfrak{P}^{\upsilon_\mathfrak{P}(\mathcal{N})} \quad \text{and} \quad \mathcal{N}_p^{\text{even}} = \prod_{\mathfrak{P}\in S} \mathfrak{P}^{\upsilon_\mathfrak{P}(\mathcal{N}_p)}.$$

We define the *odd parts* of $\mathcal{N}$ and $\mathcal{N}_p$ by

$$\mathcal{N}^{\text{odd}} = \frac{\mathcal{N}}{\mathcal{N}^{\text{even}}} \quad \text{and} \quad \mathcal{N}_p^{\text{odd}} = \frac{\mathcal{N}}{\mathcal{N}_p^{\text{even}}}.$$

Lemma 3.3. *Let (a, b, c) be a nontrivial solution to the Fermat equation* (2) *with odd prime exponent p satisfying* $\mathcal{G}_{a,b,c} = \mathfrak{m} \cdot \mathfrak{r}^2$, *where* $\mathfrak{m} \in \mathcal{H}$, *and* $\mathfrak{r}$ *is an odd prime ideal such that* $\mathfrak{r} \neq \mathfrak{m}$. *Write E for the Frey curve in* (3). *Then at all* $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$, *the local minimal model $E_\mathfrak{q}$ is semistable and satisfies* $p \mid \upsilon_\mathfrak{q}(\Delta_\mathfrak{q})$. *Moreover,*

$$\mathcal{N}^{\text{odd}} = \mathfrak{m}^2 \cdot \mathfrak{r}^{0 \text{ or } 1} \cdot \prod_{\substack{\mathfrak{q} \mid abc \\ \mathfrak{q} \notin S \cup \{\mathfrak{m},\mathfrak{r}\}}} \mathfrak{q} \quad \text{and} \quad \mathcal{N}_p^{\text{odd}} = \mathfrak{m}^2. \tag{10}$$

Proof. Clearly, if $\mathfrak{q} \nmid 2abc$ then E has good reduction at $\mathfrak{q}$; hence $\mathfrak{q} \nmid \mathcal{N}, \mathcal{N}_p$. Note also that

$$\min\{\upsilon_{\mathfrak{r}(a^p)}, \upsilon_{\mathfrak{r}(b^p)}, \upsilon_{\mathfrak{r}(c^p)}\} = 2p.$$

By Lemma 3.2, E has good or multiplicative reduction at $\mathfrak{r}$, and in either case, $p \mid v_{\mathfrak{r}}(\Delta_{\mathfrak{r}})$, proving also the correctness of the exponents of $\mathfrak{r}$ in $\mathcal{N}$ and $\mathcal{N}_p$.

Recall that $\mathfrak{m} \in \mathcal{H}$ satisfies $\mathfrak{m} = 1 \cdot \mathcal{O}_K$, or $\mathfrak{m}$ is an odd prime ideal. In the former case, there is nothing to prove, so suppose that $\mathfrak{m}$ is an odd prime ideal. As E has full 2-torsion over K, the wild part of the conductor of E/K at $\mathfrak{m}$ vanishes (see [Silverman 1994, page 380]). Moreover,

$$\min\{v_{\mathfrak{m}}(a^p), v_{\mathfrak{m}}(b^p), v_{\mathfrak{m}}(c^p)\} = p.$$

By Lemma 3.2, E/K has additive reduction at $\mathfrak{m}$. Thus the exponent of $\mathfrak{m}$ in both $\mathcal{N}$ and $\mathcal{N}_p$ is 2.

Suppose that $\mathfrak{q} \mid abc$ and $\mathfrak{q} \notin S \cup \{\mathfrak{m}, \mathfrak{r}\}$. Since $\mathcal{G}_{a,b,c} = \mathfrak{m} \cdot \mathfrak{r}^2$, the prime $\mathfrak{q}$ divides precisely one of a, b, c. From (8), $\mathfrak{q} \nmid c_4$ so the model (3) is minimal and has multiplicative reduction at $\mathfrak{q}$, and $p \mid v_{\mathfrak{q}}(\Delta)$. By (6), we see that $\mathfrak{q} \nmid \mathcal{N}_p$. □

Corollary 3.4. *Let $2 \leq d \leq 23$ be squarefree and let $K = \mathbb{Q}(\sqrt{d})$. Let (a, b, c) be a nontrivial solution to the Fermat equation (2). We may scale (a, b, c) so that it remains integral, and*

$$\mathcal{G}_{a,b,c} = \mathfrak{m} \cdot \mathfrak{r}^2, \quad \mathcal{N}_p^{odd} = \mathfrak{m}^2,$$

where

(a) *if $d \neq 10, 15$ then $\mathfrak{m} = 1 \cdot \mathcal{O}_K$;*

(b) *if $d = 10$ then $\mathfrak{m} = 1 \cdot \mathcal{O}_K$ or $\mathfrak{m} = (3, 1 + \sqrt{10})$;*

(c) *if $d = 15$ then $\mathfrak{m} = 1 \cdot \mathcal{O}_K$ or $\mathfrak{m} = (3, \sqrt{15})$;*

and $\mathfrak{r}$ is an odd prime ideal such that $\mathfrak{r} \neq \mathfrak{m}$.

Proof. For $2 \leq d \leq 23$, where $d \neq 10, 15$ and is squarefree, we have $\mathrm{Cl}(K)$ is trivial and so $\mathcal{H} = \{1 \cdot \mathcal{O}_K\}$. For $d = 10$, we have $\mathrm{Cl}(K) = \{[1 \cdot \mathcal{O}_K], [(3, 1 + \sqrt{10})]\}$, and we choose $\mathcal{H} = \{1 \cdot \mathcal{O}_K, (3, 1 + \sqrt{10})\}$. For $d = 15$, we have $\mathrm{Cl}(K) = \{[1 \cdot \mathcal{O}_K], [(3, \sqrt{15})]\}$, and we choose $\mathcal{H} = \{1 \cdot \mathcal{O}_K, (3, \sqrt{15})\}$. The corollary follows immediately from Lemmas 3.1 and 3.3. □

4. Scaling by units and the even part of the level

In the previous section, we scaled (a, b, c) so that $\mathcal{G}_{a,b,c} = \mathfrak{m} \cdot \mathfrak{r}^2$, where $\mathfrak{m} \in \mathcal{H}$, and we computed the odd parts of the conductor $\mathcal{N}$ and level $\mathcal{N}_p$. Let $\mathcal{O}_K^*$ be the unit group of K. In this section, we study the effect on $\mathcal{N}$ and $\mathcal{N}_p$ of scaling (a, b, c) by units. Note that scaling (a, b, c) by units does not affect $\mathcal{G}_{a,b,c}$; it is plain from the proofs in the previous section that this leaves the odd parts of $\mathcal{N}$ and $\mathcal{N}_p$ unchanged. Applying an even permutation to (a, b, c) results in an isomorphic Frey curve, whereas applying an odd permutation replaces the Frey curve with its twist by -1, and so has the same effect as scaling (a, b, c) by -1.

Lemma 4.1. *Suppose K is a quadratic field and 2 is inert in $\mathcal{O}_K$. Let $\mathfrak{P} = 2\mathcal{O}_K$, and suppose $\mathfrak{P} \nmid abc$. Then after suitably permuting (a, b, c), we have $v_{\mathfrak{P}}(\mathcal{N}) = 4$. Moreover, E has potentially good reduction at $\mathfrak{P}$.*

Proof. We can write $K = \mathbb{Q}(\sqrt{d})$, where $d \equiv -3 \pmod 8$. Thus $\mathcal{O}_{\mathfrak{P}} = \mathbb{Z}_2[\omega]$, where $\omega^2 + \omega + 1 = 0$. The residue field of $\mathfrak{P}$ is $\mathbb{F}_2[\tilde{\omega}] \cong \mathbb{F}_4$. Write $A = a^p$, $B = b^p$, and $C = c^p$. Now $\mathfrak{P} \nmid ABC$ and $A + B + C = 0$. Then A, B, C are congruent modulo $\mathfrak{P}$ to 1, ω, ω^2 in some order. By rearranging, we may suppose that $C \equiv \omega^2 \pmod{\mathfrak{P}}$, and we will decide later on which of A, B are congruent to 1 and ω modulo $\mathfrak{P}$. Let E denote the Frey curve in (3). It follows from (8) that $v_{\mathfrak{P}}(\Delta) = 4$ and $v_{\mathfrak{P}}(c_4) \geq 5$. In particular, $v_{\mathfrak{P}}(j) \geq 11$, and so E has potentially good reduction at $\mathfrak{P}$. Furthermore, the Frey curve is minimal at $\mathfrak{P}$ and has additive reduction. We will follow the steps of Tate's algorithm as in [Silverman 1994, page 366]. Let $\tilde{E}$ denote the reduction of E modulo $\mathfrak{P}$. It is easy to check that the point $(\tilde{C}, \tilde{1})$ is singular on $\tilde{E}$. Now we shift the model E, replacing X by $X + C$ and Y by $Y + 1$, which has the effect of sending the point $(\tilde{C}, \tilde{1})$ on the special fibre to $(\tilde{0}, \tilde{0})$. Write $a_1, \ldots, a_6$ for the a-invariants of the resulting model. Then

$$a_6 = C^3 + (B - A)C^2 - ABC - 1.$$

By Step 3 of Tate's algorithm, we know that if $\mathfrak{P}^2 \nmid a_6$ then $v_{\mathfrak{P}}(\mathcal{N}) = v_{\mathfrak{P}}(\Delta) = 4$. Suppose $\mathfrak{P}^2 \mid a_6$. Now swapping A and B replaces a_6 by

$$a_6' = C^3 + (A - B)C^2 - ABC - 1.$$

Observe that $v_{\mathfrak{P}}(a_6' - a_6) = v_{\mathfrak{P}}(2(A - B)C^2) = 1$. Hence $\mathfrak{P}^2 \nmid a_6'$. Thus we may always permute A, B, C so that $v_{\mathfrak{P}}(\mathcal{N}) = 4$. □

Remark. Under the hypotheses of Lemma 4.1, it follows from Ogg's formula [Silverman 1994, Section IV.11] that the possible exponents of $\mathfrak{P}$ in the conductor are 2, 3, 4. Lemma 4.1 shows that we can always permute the solution so that the exponent of $\mathfrak{P}$ in the conductor is 4, avoiding having to compute newforms at the smaller levels. Unfortunately, we have found that it is not possible by permuting the solution to force the exponent to be smaller in general.

Lemma 4.2. *Suppose K is a quadratic field and let $\mathfrak{P} \in S$. Suppose (a, b, c) is a nontrivial solution to the Fermat equation, with $\mathfrak{P} \nmid \mathcal{G}_{a,b,c}$. The Frey curve E has potentially multiplicative reduction at $\mathfrak{P}$ if and only if*

(a) *either $f(\mathfrak{P}/2) = 1$ (i.e., 2 splits or ramifies in K),*

(b) *or $f(\mathfrak{P}/2) = 2$ (i.e., 2 is inert in K) and $\mathfrak{P} \mid abc$.*

Moreover, if the reduction at $\mathfrak{P}$ is multiplicative then $p \nmid v_{\mathfrak{P}}(\Delta_{\mathfrak{P}})$.

Proof. Suppose (a) or (b) holds. We claim that $\mathfrak{P} \mid abc$. If (b) holds, this is true by hypothesis. If (a) holds, then the residue field at $\mathfrak{P}$ is $\mathbb{F}_2$. It follows from $a^p + b^p + c^p = 0$ that $\mathfrak{P}$ divides at least one of a, b, c, establishing our claim. Moreover, as $\mathfrak{P} \nmid \mathcal{G}_{a,b,c}$, we see that $\mathfrak{P}$ divides precisely one of a, b, c. Let $t = \upsilon_{\mathfrak{P}}(abc) \geq 1$. By (8),

$$\upsilon_{\mathfrak{P}}(c_4) = 4\upsilon_{\mathfrak{P}}(2), \quad \upsilon_{\mathfrak{P}}(\Delta) = 4\upsilon_{\mathfrak{P}}(2) + 2pt.$$

Thus,

$$\upsilon_{\mathfrak{P}}(j) = 8\upsilon_{\mathfrak{P}}(2) - 2pt < 0 \tag{11}$$

as $p \geq 17$. Thus we have potentially multiplicative reduction at $\mathfrak{P}$. The converse follows from Lemma 4.1.

To complete the proof suppose that the reduction is multiplicative, and let c_4', c_6' and $\Delta' = \Delta_{\mathfrak{P}}$ be the corresponding invariants of a local minimal model. Now $\mathfrak{P} \nmid c_4'$, but $j' = (c_4')^3/\Delta'$. From (11), $p \nmid \upsilon_{\mathfrak{P}}(j)$, and hence $p \nmid \upsilon_{\mathfrak{P}}(\Delta_{\mathfrak{P}})$. $\square$

Lemma 4.3. *Let $K_{\mathfrak{P}}$ be a local field and E an elliptic curve over $K_{\mathfrak{P}}$ with potentially multiplicative reduction. Let c_4, c_6 be the usual c-invariants of E. Let $L = K_{\mathfrak{P}}(\sqrt{-c_6/c_4})$ and let $\Delta(L/K_{\mathfrak{P}})$ be the discriminant of this local extension. Then the conductor of $E/K_{\mathfrak{P}}$ is*

$$f(E/K_{\mathfrak{P}}) = \begin{cases} 1 & \text{if } \upsilon_{\mathfrak{P}}(\Delta(L/K_{\mathfrak{P}})) = 0, \\ 2\upsilon_{\mathfrak{P}}(\Delta(L/K_{\mathfrak{P}})) & \text{otherwise.} \end{cases}$$

Proof. Let E' be the quadratic twist of E by $-c_6/c_4$. Then E' is a Tate curve (see, for example, [Silverman 1994, Section V.5]). The lemma now follows from [Rohrlich 1994, Section 18]. $\square$

Lemma 4.4. *Let (a, b, c) be a nontrivial solution to the Fermat equation such that $\mathcal{G}_{a,b,c}$ is odd. Suppose 2 is either split or ramified in K, or that 2 is inert and $2 \mid abc$. Let*

$$\mathfrak{b} = \prod_{\mathfrak{P} \in S} \mathfrak{P}^{2\upsilon_{\mathfrak{P}}(2)+1},$$

and write

$$\Phi : \mathcal{O}_K^* \to (\mathcal{O}_K/\mathfrak{b})^*/((\mathcal{O}_K/\mathfrak{b})^*)^2$$

for the natural map. Choose a set $\lambda_1, \ldots, \lambda_k \in \mathcal{O}_K \setminus \mathfrak{b}$ that represent the elements of the cokernel of Φ. For $1 \leq i \leq k$, and for $\mathfrak{P} \in S$, let $\Delta_{\mathfrak{P}}^{(i)}$ be the discriminant of the local extension $K_{\mathfrak{P}}(\sqrt{\lambda_i})/K_{\mathfrak{P}}$, and let

$$\epsilon_{\mathfrak{P}}^{(i)} = \begin{cases} 1 & \text{if } \upsilon_{\mathfrak{P}}(\Delta_{\mathfrak{P}}^{(i)}) = 0, \\ 2\upsilon_{\mathfrak{P}}(\Delta_{\mathfrak{P}}^{(i)}) & \text{otherwise.} \end{cases}$$

Then we may scale (a, b, c) *by an element of* $\mathcal{O}_K^*$ *so that for some* i *and for every* $\mathfrak{P} \in S$, *we have* $v_{\mathfrak{P}}(\mathcal{N}) = \epsilon_{\mathfrak{P}}^{(i)}$.

Proof. Write $\mathcal{O} = \mathcal{O}_K$. By Lemma 4.2, we have potentially multiplicative reduction at $\mathfrak{P}$ for all the primes $\mathfrak{P} \in S$. Write c_4, c_6 for the usual c-invariants of the Frey curve E. Since $\mathcal{G}_{a,b,c}$ is odd but $\mathfrak{P} \mid abc$ for all $\mathfrak{P} \in S$, we have from (8) and the relation $a^p + b^p + c^p = 0$ that $v_{\mathfrak{P}}(c_4) = 4v_{\mathfrak{P}}(2)$ and $v_{\mathfrak{P}}(c_6) = 6v_{\mathfrak{P}}(2)$. Write $\gamma = -c_6/4c_4$. Then $\gamma \in \mathcal{O}_{\mathfrak{P}}^*$ for all $\mathfrak{P} \in S$, and

$$K_{\mathfrak{P}}(\sqrt{\gamma}) = K_{\mathfrak{P}}(\sqrt{-c_6/c_4}).$$

Now the exponent of $\mathfrak{P}$ in the conductor $\mathcal{N}$ of the Frey curve can be expressed by Lemma 4.3 in terms of the discriminant of the extension $K_{\mathfrak{P}}(\sqrt{\gamma})/K_{\mathfrak{P}}$.

We shall make use of the isomorphism

$$(\mathcal{O}/\mathfrak{b})^*/((\mathcal{O}/\mathfrak{b})^*)^2 \cong \prod_{\mathfrak{P} \in S} \mathcal{O}_{\mathfrak{P}}^*/(\mathcal{O}_{\mathfrak{P}}^*)^2,$$

which follows from the Chinese remainder theorem, and Hensel's lemma. Observe that scaling (a, b, c) by a unit $\eta \in \mathcal{O}_K^*$ scales γ by η^p. Now, as p is odd, it follows from the definition of Φ and the above isomorphism that we can scale (a, b, c) by some $\eta \in \mathcal{O}_K^*$ so that there is some $1 \leq i \leq k$ with $\gamma/\lambda_{\mathfrak{P}}^i$ a square in $\mathcal{O}_{\mathfrak{P}}$ for each $\mathfrak{P} \in S$. Therefore,

$$K_{\mathfrak{P}}(\sqrt{\gamma}) = K_{\mathfrak{P}}(\sqrt{\lambda_{\mathfrak{P}}^i}),$$

and the lemma follows from Lemma 4.3. $\qquad \square$

Remark. Let u be the fundamental unit of the real quadratic field K. Observe that if $\lambda \in \mathcal{O}_K \setminus \mathfrak{b}$ represents an element of the cokernel of Φ, then for every integer k, the same element of the cokernel is also represented by $\lambda' = \pm u^k \lambda$. The local extension $K_{\mathfrak{P}}(\sqrt{\lambda'})/K_{\mathfrak{P}}$ depends only on the choice of sign $\pm$ and the parity of k. To keep the even part of the level small, we replace each representative λ by whichever one of $\lambda, -\lambda, u\lambda, -u\lambda$ minimizes the norm of the even part of the level $\mathcal{N}_p$.

5. Possibilities for $\mathcal{N}_p$

Corollary 5.1. *Let* $2 \leq d \leq 23$ *be squarefree and let* $K = \mathbb{Q}(\sqrt{d})$. *Let* (a, b, c) *be a nontrivial solution to the Fermat equation* (2) *with odd prime exponent* p. *We may scale* (a, b, c) *so that it remains integral,* $\mathcal{G}_{a,b,c}$ *and* $\mathcal{N}_p^{\text{odd}}$ *are as in Corollary 3.4 and* $\mathcal{N}_p^{\text{even}} = \mathcal{N}^{\text{even}}$ *is as given in Table 1.*

Proof. The proof is a straightforward application of Lemma 4.1 and Lemma 4.4. When $\mathfrak{P} \mid abc$ (which includes all cases where 2 splits or ramifies), the third column of Table 1 lists our choices $\lambda_1, \ldots, \lambda_k$ of representatives for the cokernel of Φ as

in Lemma 4.4. In these cases, the even part of the conductor $\mathcal{N}^{\mathrm{even}}$ is given by Lemma 4.4. □

d	S	λs	$\mathcal{N}^{\mathrm{even}} = \mathcal{N}_{\mathfrak{p}}^{\mathrm{even}}$
2	$\mathfrak{P} = (\sqrt{2})$	$1, \quad -1 - 2\sqrt{2}$	$\mathfrak{P}$
3	$\mathfrak{P} = (1 + \sqrt{3})$	1 $-1 + 2\sqrt{3}$	$\mathfrak{P}$ $\mathfrak{P}^4$
5	$\mathfrak{P} = (2)$	$1, \quad -5 + 2\sqrt{5}$ $\mathfrak{P} \nmid abc$	$\mathfrak{P}$ $\mathfrak{P}^4$
6	$\mathfrak{P} = (-2 + \sqrt{6})$	1 $1 + \sqrt{6}$	$\mathfrak{P}$ $\mathfrak{P}^8$
7	$\mathfrak{P} = (3 + \sqrt{7})$	$1, \quad 21 - 8\sqrt{7}$ $-1 + 2\sqrt{7}, \quad -5 + 2\sqrt{7}$	$\mathfrak{P}$ $\mathfrak{P}^4$
10	$\mathfrak{P} = (2, \sqrt{10})$	$1, \quad 7 - 2\sqrt{10}$	$\mathfrak{P}$
11	$\mathfrak{P} = (3 + \sqrt{11})$	1 $-1 + 2\sqrt{11}$	$\mathfrak{P}$ $\mathfrak{P}^4$
13	$\mathfrak{P} = (2)$	$1, \quad -5 + 2\sqrt{13}$ $\mathfrak{P} \nmid abc$	$\mathfrak{P}$ $\mathfrak{P}^4$
14	$\mathfrak{P} = (4 + \sqrt{14})$	$1, \quad -3$ $1 + \sqrt{14}, \quad -3 + \sqrt{14}$	$\mathfrak{P}$ $\mathfrak{P}^8$
15	$\mathfrak{P} = (2, 1 + \sqrt{15})$	$1, \quad -15 + 4\sqrt{15}$ $-1 + 2\sqrt{15}, \quad 7 - 2\sqrt{15}$	$\mathfrak{P}$ $\mathfrak{P}^4$
17	$\mathfrak{P}_1 = \left(\frac{3+\sqrt{17}}{2}\right), \mathfrak{P}_2 = \left(\frac{3-\sqrt{17}}{2}\right)$	$1, 17-4\sqrt{17}, -9+2\sqrt{17}, -5+2\sqrt{17}$	$\mathfrak{P}_1 \cdot \mathfrak{P}_2$
19	$\mathfrak{P} = (13 + 3\sqrt{19})$	1 $-1 + 2\sqrt{19}$	$\mathfrak{P}$ $\mathfrak{P}^4$
21	$\mathfrak{P} = (2)$	$1, \quad -5 + 2\sqrt{21}$ $(7 - \sqrt{21})/2, \quad (3 + 3\sqrt{21})/2$ $\mathfrak{P} \nmid abc$	$\mathfrak{P}$ $\mathfrak{P}^4$ $\mathfrak{P}^4$
22	$\mathfrak{P} = (14 + 3\sqrt{22})$	1 $1 + \sqrt{22}$	$\mathfrak{P}$ $\mathfrak{P}^8$
23	$\mathfrak{P} = (5 + \sqrt{23})$	$1, \quad 115 + 24\sqrt{23}$ $-1 + 2\sqrt{23}, \quad -163 - 34\sqrt{23}$	$\mathfrak{P}$ $\mathfrak{P}^4$

Table 1. Quantities required for Corollary 5.1 and its proof.

6. Irreducibility

We begin with a proposition that gathers some well-known facts in the literature.

Proposition 6.1. *Let E be an elliptic curve over a number field K and let p be a rational prime.*

(i) *If $\mathfrak{q} \nmid p$ and is a prime of good or multiplicative reduction then*

$$\bar{\rho}_{E,p}|_{I_\mathfrak{q}} \sim \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}.$$

(ii) *If $\mathfrak{p} \mid p$ and is a prime of good ordinary reduction, or of multiplicative reduction, then*

$$\bar{\rho}_{E,p}|_{I_\mathfrak{p}} \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix},$$

where χ is the mod p cyclotomic character.

(iii) *If $\mathfrak{p} \mid p$ and is a prime of good supersingular reduction with ramification degree e, then either*

$$\bar{\rho}_{E,p}|_{I_\mathfrak{p}} \sim \begin{pmatrix} \psi_2^e & 0 \\ 0 & \psi_2^{pe} \end{pmatrix}, \tag{12}$$

where $\psi_2 : I_\mathfrak{p} \to \mathbb{F}_{p^2}^*$ is a level 2 fundamental character, or

$$\bar{\rho}_{E,p}|_{I_\mathfrak{p}} \sim \begin{pmatrix} \psi_1^f & 0 \\ 0 & \psi_1^{e-f} \end{pmatrix}, \tag{13}$$

where $\psi_1 : I_\mathfrak{p} \to \mathbb{F}_p^*$ is the level 1 fundamental character, and f is some integer satisfying $0 < f < e$.

Proof. See [Serre 1972, §1.11, 1.12] and the proof of [Kraus 1996, Lemma 1]. $\square$

Corollary 6.2. *Let E be an elliptic curve over a quadratic field K. Let p be a rational prime. Suppose $\bar{\rho}_{E,p}$ is reducible and E has supersingular reduction at some $\mathfrak{p}$ dividing p. Then $(p) = \mathfrak{p}^2$, and*

$$\bar{\rho}_{E,p}|_{I_\mathfrak{p}} \sim \begin{pmatrix} \psi_1 & 0 \\ 0 & \psi_1 \end{pmatrix}.$$

Proof. Write e for the ramification degree of $\mathfrak{p}$. As K is quadratic, $e = 1$ or 2. We apply part (iii) of Proposition 6.1. Suppose first that $\bar{\rho}_{E,p}|_{I_\mathfrak{p}}$ is given by (12). Now the characters ψ_2 and ψ_2^2 are not $\mathbb{F}_p$-valued, contradicting the reducibility of $\bar{\rho}_{E,p}$.

It follows that $\bar{\rho}_{E,p}|_{I_\mathfrak{p}}$ is given by (13), where f is an integer satisfying the inequality $1 < f < e$. Thus $e = 2$ and $f = 1$, completing the proof. $\square$

Lemma 6.3. *Let E be an elliptic curve over a number field K of conductor $\mathcal{N}$ and let $p \geq 5$ be a rational prime. Suppose $\bar{\rho}_{E,p}$ is reducible and write*

$$\bar{\rho}_{E,p} \sim \begin{pmatrix} \theta & * \\ 0 & \theta' \end{pmatrix}, \tag{14}$$

where $\theta, \theta' : G_K \to \mathbb{F}_p^*$ are characters. Write $\mathcal{N}_\theta$ and $\mathcal{N}_{\theta'}$ for the respective conductors of these characters. Let $\mathfrak{q}$ be a prime of K with $\mathfrak{q} \nmid p$.

(a) *If E has good or multiplicative reduction at $\mathfrak{q}$ then $\upsilon_{\mathfrak{q}}(\mathcal{N}_\theta) = \upsilon_{\mathfrak{q}}(\mathcal{N}'_\theta) = 0$.*

(b) *If E has additive reduction at $\mathfrak{q}$ then $\upsilon_{\mathfrak{q}}(\mathcal{N})$ is even and*

$$\upsilon_{\mathfrak{q}}(\mathcal{N}_\theta) = \upsilon_{\mathfrak{q}}(\mathcal{N}_{\theta'}) = \tfrac{1}{2} \upsilon_{\mathfrak{q}}(\mathcal{N}).$$

Proof. If E has good or multiplicative reduction at $\mathfrak{q}$ then, by Proposition 6.1(i), the characters θ, θ' are unramified at $\mathfrak{q}$. This immediately implies (a).

Suppose now that E has additive reduction at $\mathfrak{q}$. Recall that $\theta = \chi/\theta'$, where $\chi : G_K \to \mathbb{F}_p^*$ is the mod p cyclotomic character. As χ is unramified away from p, and therefore unramified at $\mathfrak{q}$, we see that $\upsilon_{\mathfrak{q}}(\mathcal{N}_\theta) = \upsilon_{\mathfrak{q}}(\mathcal{N}_{\theta'})$.

Suppose that $\upsilon_{\mathfrak{q}}(\mathcal{N}_\theta) = \upsilon_{\mathfrak{q}}(\mathcal{N}_{\theta'}) = 0$; we will deduce a contradiction. Then $\theta|_{I_{\mathfrak{q}}} = \theta'|_{I_{\mathfrak{q}}} = 1$. It follows that $\bar{\rho}_{E,p}(I_{\mathfrak{q}})$ has order 1 or p. Suppose first that E has potentially good reduction at $\mathfrak{q}$. Then (see [Kraus 1990, Introduction]), the order of $\bar{\rho}_{E,p}(I_{\mathfrak{q}})$ divides 24, and moreover is equal to 1 if and only if E has good reduction at $\mathfrak{q}$. As $p \geq 5$, we have a contradiction. We may therefore suppose that E has potentially multiplicative reduction. It then follows from the theory of the Tate curve [Silverman 1994, Proposition V.6.1] that $\#\bar{\rho}_{E,p}(I_{\mathfrak{q}}) = 1$ or 2. Again as $p \geq 5$, we have that $\bar{\rho}_{E,p}(I_{\mathfrak{q}}) = 1$ and so E has multiplicative reduction at $\mathfrak{q}$. This contradicts the fact that E has additive reduction at $\mathfrak{q}$.

Thus $\upsilon_{\mathfrak{q}}(\mathcal{N}_\theta) = \upsilon_{\mathfrak{q}}(\mathcal{N}_{\theta'}) = 1 + t$, where $t \geq 0$ is the wild part of these conductors of the characters at $\mathfrak{q}$. As E has additive reduction at $\mathfrak{q}$, we can write $\upsilon_{\mathfrak{q}}(\mathcal{N}) = 2 + \delta$, where δ is the wild part of conductor of E at $\mathfrak{q}$. To prove (b), it is sufficient to show that $\delta = 2t$. Let $I_{\mathfrak{q}}^w$ be the wild inertia subgroup at $\mathfrak{q}$. As $I_{\mathfrak{q}}^w$ is a pro-q group, where q is the rational prime below $\mathfrak{q}$, and as $p \neq q$, we have

$$\bar{\rho}_{E,p}|_{I_{\mathfrak{q}}^w} \sim \begin{pmatrix} \theta|_{I_{\mathfrak{q}}^w} & 0 \\ 0 & \theta'|_{I_{\mathfrak{q}}^w} \end{pmatrix}.$$

Now the relation $\delta = 2t$ follows straightforwardly from the formula [Silverman 1994, page 380] for the wild part of the conductor of E at $\mathfrak{q}$. $\qquad\square$

Suppose E is as in Lemma 6.3. Observe that $\mathrm{Ker}\,\theta$ is a K-rational subgroup of $E[p]$ of order p. Thus $E' = E/\mathrm{Ker}\,\theta$ is a p-isogenous elliptic curve defined

over K. It is straightforward to show that

$$\bar{\rho}_{E',p} \sim \begin{pmatrix} \theta' & * \\ 0 & \theta \end{pmatrix}.$$

Thus by replacing E with a p-isogenous elliptic curve, we may swap θ and θ' in (14) as we please.

Lemma 6.4. *Let $p \geq 17$, and let $2 \leq d \leq 23$ be squarefree. Let $K = \mathbb{Q}(\sqrt{d})$. Let (a, b, c) be a nontrivial solution to the Fermat equation (2) scaled as in Corollary 5.1. Then $\bar{\rho}_{E,p}$ is irreducible.*

Proof. Suppose that $\bar{\rho}_{E,p}$ is reducible. As E has nontrivial 2-torsion, it gives rise to a K-point on $X_0(2p)$. The quadratic points on $X_0(34)$ have been determined by Ozman [≥ 2015]. These are all defined over $\mathbb{Q}(i)$, $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-15})$. Thus we suppose $p \geq 19$.

Let θ, θ', $\mathcal{N}_\theta$, $\mathcal{N}_{\theta'}$ be as in Lemma 6.3.

We shall first complete the proof under the assumption that p is coprime to either $\mathcal{N}_\theta$ or $\mathcal{N}_{\theta'}$. After swapping θ and θ', we can assume that p is coprime to $\mathcal{N}_\theta$. It follows from Lemma 6.3 that $\mathcal{N}_\theta$ is the square root of the additive part of the conductor $\mathcal{N}$. From Lemma 3.3, we know that the odd additive part is $\mathfrak{m}^2$ where the possibilities for $\mathfrak{m}$ are as in Corollary 3.4. The even additive part of $\mathcal{N}$ can be deduced from Table 1. For the cases where 2 is inert and $2 \nmid abc$, the even part of the conductor is $\mathcal{N}^{\text{even}} = (2)^4$ (after appropriate scaling of (a, b, c)) by Lemma 4.1.

Thus for each d, we have a small list of possibilities for $\mathcal{N}_\theta$. Let ∞_1 and ∞_2 be the two real places of K. It follows that θ is a character of the ray class group for the modulus $\mathcal{N}_\theta \infty_1 \infty_2$. Using Magma, we computed this ray class group in all cases and found it to be one of the following groups:

$$0, \quad \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}.$$

The order of θ divides the exponent of the group, and so it is 1, 2 or 4. If θ has order 1, then E has a point of order p over K. The possibilities for p-torsion over quadratic fields have been determined by Kamienny, Kenku and Momose (see [Kamienny 1992, Theorem 3.1]) and their results imply that $p \leq 13$, giving a contradiction. If θ has order 2, then E has a point of order p over a quadratic extension L/K. The field L has degree 4 over $\mathbb{Q}$. The possibilities for p-torsion over quartic fields have been determined by Derickx, Kamienny, Stein and Stoll [Derickx et al. ≥ 2015] and their results imply that $p \leq 17$, again giving a contradiction. Suppose θ has order 4. Let L be the unique quadratic extension of K cut out by θ^2. Now $\phi = \theta|_{G_L}$ is a quadratic character. Twisting E/L by ϕ gives an elliptic curve defined over L with a point of order p. As before, $p \leq 17$. This completes the proof if p is coprime to either $\mathcal{N}_\theta$ or $\mathcal{N}_{\theta'}$.

From now on we assume that neither $\mathcal{N}_\theta$ nor $\mathcal{N}_{\theta'}$ is coprime to p. Observe that E is semistable at all $\mathfrak{p} \mid p$. We shall divide into cases according to whether p is inert, splits or is ramified in K.

(a) Suppose first that p is inert in K. It follows from Corollary 6.2 that E cannot have good supersingular reduction at $\mathfrak{p} = (p)$. Thus E has either good ordinary or multiplicative reduction at $\mathfrak{p}$. By Proposition 6.1(ii), we see that one of θ, θ' is unramified at $\mathfrak{p}$. It follows that one of $\mathcal{N}_\theta, \mathcal{N}_{\theta'}$ is coprime to p, giving a contradiction.

(b) Suppose now that p ramifies in K. This means that $d = p$ and d is either 19 or 23. Let $\mathfrak{p}$ be the unique prime above p in K. If E has good ordinary or multiplicative reduction at $\mathfrak{p}$ then we obtain a contradiction as in (a). Thus suppose E has good supersingular reduction at $\mathfrak{p}$. We will now apply Proposition 6.5 below to show this cannot happen. The field $K = \mathbb{Q}(\sqrt{d})$ has a prime $\mathfrak{P}$ dividing 2 with residue field $\mathbb{F}_2$, and so by Lemma 4.2, this is a prime of potentially multiplicative reduction for E. In the notation of Proposition 6.5, $\sqrt{\mathcal{A}} = (1)$ or $\mathfrak{P}^2$. In all cases, the ray class group of modulus $\sqrt{\mathcal{A}}\infty_1\infty_2$ is $\mathbb{Z}/2\mathbb{Z}$, and the proposition implies that $4 = \mathrm{Norm}(\mathfrak{P})^2 \equiv 1 \pmod{p}$. As $p = 19$ or 23, we have a contradiction and so E cannot be supersingular at $\mathfrak{P}$.

(c) Suppose p splits as $\mathfrak{p}\mathfrak{p}'$. The primes $\mathfrak{p}, \mathfrak{p}'$ are unramified, and again we deduce that E has either good ordinary or multiplicative reduction at these. By Proposition 6.1(ii), we have that precisely one of θ, θ' is ramified at $\mathfrak{p}$ and precisely one of them is ramified at $\mathfrak{p}'$. If θ is unramified at both $\mathfrak{p}, \mathfrak{p}'$ then we have a contradiction, and likewise if θ' is unramified at both $\mathfrak{p}, \mathfrak{p}'$. We can assume $\mathfrak{p} \mid \mathcal{N}_\theta$, $\mathfrak{p} \nmid \mathcal{N}_{\theta'}$ and $\mathfrak{p}' \nmid \mathcal{N}_\theta$, $\mathfrak{p}' \mid \mathcal{N}_{\theta'}$. Thus, by Proposition 6.1(ii), $\theta|_{I_\mathfrak{p}} = \chi|_{I_\mathfrak{p}}$ and $\theta'|_{I_{\mathfrak{p}'}} = \chi|_{I_{\mathfrak{p}'}}$. We shall write down a small integer $n > 0$ such that θ^n is unramified away from $\mathfrak{p}$. If $\mathfrak{q} \nmid p$ is a prime of potentially multiplicative reduction then θ^2 is unramified at $\mathfrak{q}$. Furthermore, for our Frey curve E, the only odd additive prime is $\mathfrak{q} = \mathfrak{m}$, and Lemma 3.2(iv) implies that $\#\bar{\rho}_{E,p}(I_\mathfrak{q}) = 2$, and so θ^2 is unramified at $\mathfrak{q}$. We are left with primes $\mathfrak{q}$, with $\mathfrak{q} \mid 2$, of potentially good reduction. These only arise for $d = 5, 13, 21$, and in these cases $v_\mathfrak{q}(\Delta_\mathfrak{q}) = 4$. It follows from [Kraus 1990, Theorem 3] that $\bar{\rho}_{E,p}(I_\mathfrak{q})$ is either cyclic of order 3, 6 or isomorphic to $\mathrm{SL}_2(\mathbb{F}_3)$ and so has order 24. The last case cannot occur, as $\mathrm{SL}_2(\mathbb{F}_3)$ is nonabelian, and any nonabelian reducible subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ has an element of order p. It follows that θ^6 is unramified at $\mathfrak{q}$. Letting $n = 6$ for $d = 5, 13, 21$, and $n = 2$ for other values of d, we conclude that the character θ^n is unramified away from $\mathfrak{p}$, and that $\theta^n|_{I_\mathfrak{p}} = \chi^n|_{I_\mathfrak{p}}$. Let u be a generator of the subgroup of totally positive units in $\mathcal{O}_K^*$. It follows (see [Kraus 1996, page 249]) that $p \mid \mathrm{Norm}(u^n - 1)$. We computed the factorization of $\mathrm{Norm}(u^n - 1)$ for our values of d and found that none are divisible by primes $p \geq 19$, except when $d = p = 19$ or $d = p = 23$. However, in these cases p ramifies in the field $K = \mathbb{Q}(\sqrt{d})$, and so are covered by case (b). $\qquad\square$

Proposition 6.5. *Let $d = p \geq 5$ be a prime and $\mathfrak{p}$ be the unique prime in $K = \mathbb{Q}(\sqrt{d})$ above p. Let E/K be an elliptic curve and denote by $\mathcal{A}$ the additive part of its conductor. Suppose that E has good supersingular reduction at $\mathfrak{p}$ and potentially multiplicative reduction at some prime $\mathfrak{q}_0 \neq \mathfrak{p}$. Suppose further that $\bar{\rho}_{E,p}$ is reducible. Therefore, $\mathcal{A}$ is a square and we let n be the exponent of the ray class group for the modulus $\sqrt{\mathcal{A}}\infty_1\infty_2$. Then, $\mathrm{Norm}(\mathfrak{q}_0)^n \equiv 1 \pmod{p}$.*

Proof. Suppose $\bar{\rho}_{E,p}$ is reducible and let θ, θ' be as in the proof of Lemma 6.4. Write $\epsilon = \theta/\theta'$. By Corollary 6.2, the character ϵ is unramified at $\mathfrak{p}$; it is here that we use the assumption that E has good supersingular reduction at $\mathfrak{p}$. Moreover, as $\epsilon = \theta^2/\chi$, where χ is the cyclotomic character, it follows that for $\mathfrak{q}$, an additive prime with $\mathfrak{q} \nmid p$,

$$\upsilon_{\mathfrak{q}}(\mathcal{N}_\epsilon) \leq \upsilon_{\mathfrak{q}}(\mathcal{N}_\theta) = \tfrac{1}{2}\upsilon_{\mathfrak{q}}(\mathcal{A}).$$

Therefore, the exponent of the ray class group of modulus $\mathcal{N}_\epsilon\infty_1\infty_2$ is a divisor of n. Thus $\epsilon^n = 1$. Let $\sigma_{\mathfrak{q}_0}$ be the Frobenius element of G_K at $\mathfrak{q}_0$. Since $\mathfrak{q}_0$ is of potentially multiplicative reduction the possible pairs of eigenvalues of $\bar{\rho}_{E,p}(\sigma_{\mathfrak{q}_0})$ are $(1, \mathrm{Norm}(\mathfrak{q}_0))$ or $(-1, -\mathrm{Norm}(\mathfrak{q}_0))$ and they correspond to the values of $\theta(\sigma_{\mathfrak{q}_0})$ and $\theta'(\sigma_{\mathfrak{q}_0})$ up to reordering. Thus,

$$1 = \epsilon^n(\sigma_{\mathfrak{q}_0}) = \theta(\sigma_{\mathfrak{q}_0})^n/\theta'(\sigma_{\mathfrak{q}_0})^n \equiv \mathrm{Norm}(\mathfrak{q}_0)^{\pm n} \pmod{p}. \qquad \square$$

7. Proof of Theorem 1

For now let $2 \leq d \leq 23$ be squarefree, and let $K = \mathbb{Q}(\sqrt{d})$. We would like to show that the equation $x^n + y^n = z^n$ has only trivial solutions in K for $n \geq 4$, although as we will see in due course, our proof strategy fails for $d = 5$ and $d = 17$. As in the introduction, we reduce to showing that the Fermat equation (2) has no nontrivial solutions (a, b, c) in $\mathcal{O}_K$ with prime exponent $p \geq 17$. Now suppose (a, b, c) is a nontrivial solution with $p \geq 17$, and scale this as in Corollary 5.1. Let $E = E_{a,b,c}$ be the Frey curve given by (3), and let $\bar{\rho}_{E,p}$ be its mod p representation. We know from Lemma 6.4 that $\bar{\rho}_{E,p}$ is irreducible. We now apply Theorem 3 to deduce that there is a cuspidal Hilbert newform $\mathfrak{f}$ over K of weight $(2, 2)$ and level $\mathcal{N}_p$ (one of the levels predicted by Corollary 5.1) such that $\bar{\rho}_{E,p} \sim \bar{\rho}_{\mathfrak{f},\varpi}$ for some prime $\varpi \mid p$ of $\mathbb{Q}_{\mathfrak{f}}$.

Lemma 7.1. *Let $\mathfrak{q} \nmid \mathcal{N}_p$ be a prime of K, and let*

$$\mathcal{A} = \{a \in \mathbb{Z} : |a| \leq 2\sqrt{\mathrm{Norm}(\mathfrak{q})}, \ \mathrm{Norm}(\mathfrak{q}) + 1 - a \equiv 0 \pmod{4}\}.$$

If $\bar{\rho}_{E,p} \sim \bar{\rho}_{\mathfrak{f},\varpi}$ then ϖ divides the principal ideal

$$B_{\mathfrak{f},\mathfrak{q}} = \mathrm{Norm}(\mathfrak{q})\big((\mathrm{Norm}(\mathfrak{q}) + 1)^2 - a_{\mathfrak{q}}(\mathfrak{f})^2\big) \prod_{a \in \mathcal{A}} (a - a_{\mathfrak{q}}(\mathfrak{f})) \cdot \mathcal{O}_{\mathbb{Q}_{\mathfrak{f}}}.$$

Proof. If $\mathfrak{q} \mid p$, then $\mathrm{Norm}(\mathfrak{q})$ is a power of p. Since $\varpi \mid p$, we have ϖ divides $B_{\mathfrak{f},\mathfrak{q}}$. Thus we may suppose $\mathfrak{q} \nmid p$. By assumption $\mathfrak{q} \nmid \mathcal{N}_p$. From the definition of $\mathcal{N}_p$

in (6), the prime $\mathfrak{q}$ is of good or multiplicative reduction for E. If $\mathfrak{q}$ is a prime of good reduction for E, then $a_\mathfrak{q}(E) \equiv a_\mathfrak{q}(\mathfrak{f}) \pmod{\varpi}$. By the Hasse–Weil bounds, we know that $|a_\mathfrak{q}(E)| \leq 2\sqrt{\mathrm{Norm}(\mathfrak{q})}$. Moreover, as E has full 2-torsion (and $\mathfrak{q} \nmid 2$, as $\mathfrak{q} \nmid \mathcal{N}_p$), we have $4 \mid \#E(\mathbb{F}_\mathfrak{q})$. Thus $a_\mathfrak{q}(E) \in \mathcal{A}$ and so $\varpi \mid B_{\mathfrak{f},\mathfrak{q}}$. Finally, suppose $\mathfrak{q}$ is a prime of multiplicative reduction for $\mathcal{N}_p$. Then, comparing the traces of the images of Frobenius at $\mathfrak{q}$ under $\bar\rho_{E,p}$ and $\bar\rho_{\mathfrak{f},\varpi}$, we have

$$\pm(\mathrm{Norm}(\mathfrak{q}) + 1) \equiv a_\mathfrak{q}(\mathfrak{f}) \pmod{\varpi}.$$

It follows that ϖ divides $B_{\mathfrak{f},\mathfrak{q}}$ in this case too. ☐

Using Magma we computed the newforms $\mathfrak{f}$ at the predicted levels, the fields $\mathbb{Q}_\mathfrak{f}$, and eigenvalues $a_\mathfrak{q}(\mathfrak{f})$ at primes $\mathfrak{q}$ of K small norm. We computed for each $\mathfrak{f}$ at level $\mathcal{N}_p$, the ideal

$$B_\mathfrak{f} := \sum_{\mathfrak{q} \in T} B_{\mathfrak{f},\mathfrak{q}}, \tag{15}$$

where T is the set of prime ideals $\mathfrak{q}$ of K, with $\mathfrak{q} \nmid \mathcal{N}_p$ and with norm less than 60 (this turns out to be sufficient for our purpose). Let $C_\mathfrak{f} := \mathrm{Norm}_{\mathbb{Q}_\mathfrak{f}/\mathbb{Q}}(B_\mathfrak{f})$. If $\bar\rho_{E,p} \sim \bar\rho_{\mathfrak{f},\varpi}$ then by the above lemma, $\varpi \mid B_\mathfrak{f}$ and so $p \mid C_\mathfrak{f}$. Hence, the isomorphism $\bar\rho_{E,p} \sim \bar\rho_{\mathfrak{f},\varpi}$ is impossible if $p \nmid C_\mathfrak{f}$. Thus, the newforms satisfying $C_\mathfrak{f} = 0$ are the problematic ones. We computed $C_\mathfrak{f}$ for all newforms $\mathfrak{f}$ at the predicted levels, and found only three fields where $C_\mathfrak{f} = 0$ for some $\mathfrak{f}$. All the others produced values of $C_\mathfrak{f}$ that are not divisible by primes $p \geq 17$. Thus to complete the proof, we have to deal with the cases where $C_\mathfrak{f} = 0$; these are as follows:

(i) $K = \mathbb{Q}(\sqrt{3})$, $\mathcal{N}_p = (1 + \sqrt{3})^4$. Here $\mathfrak{f}$ is the unique newform at level $\mathcal{N}_p$. It satisfies $\mathbb{Q}_\mathfrak{f} = \mathbb{Q}$ and corresponds to the elliptic curve

$$E' : y^2 = x(x + 1)(x + 8 + 4\sqrt{3})$$

   of conductor $(1 + \sqrt{3})^4$.

(ii) $K = \mathbb{Q}(\sqrt{5})$, $\mathcal{N}_p = (2)^4$. There are three newforms at level $\mathcal{N}_p$, and all three satisfy $\mathbb{Q}_\mathfrak{f} = \mathbb{Q}$. For all three newforms, $C_\mathfrak{f} = 0$.

(iii) $K = \mathbb{Q}(\sqrt{17})$, $\mathcal{N}_p = (2)$. Here $\mathfrak{f}$ is the unique newform at level $\mathcal{N}_p$. It satisfies $\mathbb{Q}_\mathfrak{f} = \mathbb{Q}$ and corresponds to the elliptic curve

$$W : y^2 = x(x - 4 + \sqrt{17})\left(x + \frac{-13 + 5\sqrt{17}}{2}\right)$$

   of conductor (2).

Indeed, the remaining eigenforms $\mathfrak{f}$ correspond to elliptic curves with full 2-torsion. It is easy to see from the definitions that $B_{\mathfrak{f},\mathfrak{q}} = 0$ for such an eigenform. It follows that it is futile to enlarge the set T in (15).

Since $d \neq 5, 17$ in the statement of Theorem 1, we only have to complete the proof for $d = 3$. To do this, we must discard the isomorphism $\bar{\rho}_{E,p} \sim \bar{\rho}_{E',p}$, where E' is given in (i) above. The elliptic curve E' has j-invariant $j' = 54000$ and so potentially good reduction at $\mathfrak{P} = (1 + \sqrt{3})$; in particular [Kraus 1990], the order of $\bar{\rho}_{E',p}(I_{\mathfrak{P}})$ is 1, 2, 3, 4, 6, 8 or 24. On the other hand, the Frey curve E has potentially multiplicative reduction, and $p \nmid \upsilon_{\mathfrak{P}}(j)$. By the theory of the Tate curve [Silverman 1994, Proposition V.6.1], we have $p \mid \bar{\rho}_{E',p}(I_{\mathfrak{P}})$, giving a contradiction as $p \geq 17$.

8. Proof of Theorem 2

To complete the proof of Theorem 2, it remains to discard the isomorphism $\bar{\rho}_{E,p} \sim \bar{\rho}_{W,p}$, where W is given in (iii) above. We apply Lemma 1.6 of [Halberstadt and Kraus 2002] — this is proved for $K = \mathbb{Q}$, but the proof for K, a general number field, is identical. Let $\mathfrak{P}_1$, $\mathfrak{P}_2$ be as in Table 1 for $d = 17$. The curve E has multiplicative reduction at $\mathfrak{P}_i$, and the valuations of the minimal discriminants are $-8 + 2pt_i$, where t_1, t_2 are positive integers. The curve W has conductor $(2) = \mathfrak{P}_1 \mathfrak{P}_2$ and its minimal discriminant Δ_W satisfies $\upsilon_{\mathfrak{P}_1}(\Delta_W) = 4$ and $\upsilon_{\mathfrak{P}_2}(\Delta_W) = 2$. The quantity

$$\frac{\upsilon_{\mathfrak{P}_1}(\Delta_E)\upsilon_{\mathfrak{P}_2}(\Delta_E)}{\upsilon_{\mathfrak{P}_1}(\Delta_W)\upsilon_{\mathfrak{P}_2}(\Delta_W)} = \frac{(-8 + 2pt_1)(-8 + 2pt_2)}{4 \cdot 2} \equiv 8 \pmod{p}$$

is a square modulo p if and only if $p \equiv 1, 7 \pmod 8$. It follows from [Halberstadt and Kraus 2002, Lemma 1.6] that $\bar{\rho}_{E,p} \sim \bar{\rho}_{W,p}$ cannot hold if $p \equiv 3, 5 \pmod 8$, concluding the proof.

9. Computational remarks

In the introduction, we indicated that the above strategy can be applied over other totally real fields (assuming the modularity of the Frey curve). However, the computation of newforms will often be impractical, particularly if the levels predicted by level lowering have large norm. These levels depend crucially on a choice of odd prime ideal representatives $\mathcal{H}$ for $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2$. In this section, we illustrate these computational issues by looking at $K = \mathbb{Q}(\sqrt{30})$ and $K = \mathbb{Q}(\sqrt{79})$.

Let $K = \mathbb{Q}(\sqrt{30})$. Here $\mathrm{Cl}(K)$ has order 2, and we can take $\mathcal{H} = \{1 \cdot \mathcal{O}_K, \mathfrak{m}\}$, where $\mathfrak{m}$ is the unique prime above 3. By computations similar to those leading to Corollary 5.1, we obtain four possible levels $\mathcal{N}_p$. One of these is $\mathcal{N}_p = \mathfrak{P}^8 \cdot \mathfrak{m}^2$, where $\mathfrak{P}$ is the unique prime above 2. The dimension of the space of cusp forms of level $\mathcal{N}_p$ is 26108, making the computation of newforms infeasible with the current Magma implementation.

Let $K = \mathbb{Q}(\sqrt{79})$. Here $\mathrm{Cl}(K)$ has order 3, and thus $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2$ is trivial; this is the smallest real quadratic field for which $\mathrm{Cl}(K)$ and $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2$ differ. By definition, $\mathcal{H} = \{1 \cdot \mathcal{O}_K\}$. We can show by variants of the arguments in Section 6 that $\bar{\rho}_{E,p}$ is irreducible for $p \geq 17$. Moreover the predicted levels $\mathcal{N}_p$ are $\mathfrak{P}$ and $\mathfrak{P}^4$, where $\mathfrak{P} \mid 2$. The dimensions of the corresponding spaces of cusp forms are 156 and 1077 respectively. Here it feasible to compute the newforms, and similar arguments to those in Section 7 allow us to deduce the following.

Theorem 4. *The Fermat equation* (1) *has only trivial solutions over* $K = \mathbb{Q}(\sqrt{79})$ *for* $n \geq 4$.

In [Freitas and Siksek 2015], the reader will also find recipes for the possible levels $\mathcal{N}_p$. The objectives of [loc. cit.] are theoretical and there is no need to make the levels $\mathcal{N}_p$ particularly small. The purpose of the following remarks is to illustrate the value of Sections 3 and 4 of the current paper, where a finer analysis of the levels and the effect of scaling the solution is carried out. In [loc. cit.], the set $\mathcal{H}$ is taken to be representatives of $\mathrm{Cl}(K)$ rather than representatives for $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2$. For the fields K appearing in Theorem 1, all class groups are either trivial or cyclic of order 2. Therefore there is no difference between $\mathrm{Cl}(K)$ and $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2$. For these fields, the main improvement of the current paper lies in Section 4 which radically reduces the possibilities for the even part of the level. However, to extend the computations to other fields, the distinction between $\mathrm{Cl}(K)$ and $\mathrm{Cl}(K)/\mathrm{Cl}(K)^2$ becomes crucial. For example, for $K = \mathbb{Q}(\sqrt{79})$, a set of odd representatives for $\mathrm{Cl}(K)$ is $\{1 \cdot \mathcal{O}_K, \mathfrak{m}_1, \mathfrak{m}_2\}$, where $\mathfrak{m}_1 \mathfrak{m}_2 = 3 \cdot \mathcal{O}_K$. Following the recipe in [loc. cit.], the odd part of the level will be $1 \cdot \mathcal{O}_K$, $\mathfrak{m}_1^2$ or $\mathfrak{m}_2^2$. Thus the possibilities for $\mathcal{N}_p$ include $\mathfrak{P}^4 \cdot \mathfrak{m}_1^2$. The dimension of the space of cusp forms for this level is 12090, which makes the computation of newforms impractical. Finally, we point out that the even part of the level given by the recipe in [loc. cit.] can be as large as $\mathfrak{P}^{10}$. Even if the odd part of the level is taken to be trivial, the dimension of the space of cusp forms of level $\mathfrak{P}^{10}$ is 64596, which again is too large. It is clear that the refinements of Sections 3 and 4 are required for $K = \mathbb{Q}(\sqrt{79})$, and will be needed if the computations of the current paper are to be extended to other totally real fields.

References

[Aigner 1934] A. Aigner, "Uber die Möglichkeit von $x^4 + y^4 = z^4$ in quadratischen Körpern", *Jahresber. Dtsch. Math.-Ver.* **43** (1934), 226–229. Zbl 0008.29502

[Aigner 1957] A. Aigner, "Die Unmöglichkeit von $x^6 + y^6 = z^6$ und $x^9 + y^9 = z^9$ in quadratischen Körpern", *Monatsh. Math.* **61** (1957), 147–150. MR 19,120e Zbl 0079.06502

[Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, "The Magma algebra system I: the user language", *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR 1484478 Zbl 0898.68039

[Cassels and Fröhlich 1967] J. W. S. Cassels and A. Fröhlich (editors), *Algebraic number theory*, Academic Press, London, 1967. MR 35 #6500 Zbl 0153.07403

[David 2012] A. David, "Caractère d'isogénie et critères d'irréductibilité", preprint, 2012. arXiv 1103.3892v2

[Dembélé and Donnelly 2008] L. Dembélé and S. Donnelly, "Computing Hilbert modular forms over fields with nontrivial class group", pp. 371–386 in *Algorithmic number theory*, edited by A. J. van der Poorten and A. Stein, Lecture Notes in Comput. Sci. **5011**, Springer, Berlin, 2008. MR 2010d:11149 Zbl 1232.11128

[Dembélé and Voight 2013] L. Dembélé and J. Voight, "Explicit methods for Hilbert modular forms", pp. 135–198 in *Elliptic curves, Hilbert modular forms and Galois deformations*, edited by H. Darmon et al., Springer, Basel, 2013. MR 3184337 Zbl 1276.11004

[Derickx et al. ≥ 2015] M. Derickx, S. Kamienny, W. Stein, and M. Stoll, "Torsion points on elliptic curves over number fields", in preparation.

[Dickson 1920] L. E. Dickson, *History of the theory of numbers, Volume II: Diophantine analysis*, Carnegie Institution of Washington, 1920. Zbl 47.0100.04

[Freitas and Siksek 2015] N. Freitas and S. Siksek, "The asymptotic Fermat's last theorem for five-sixths of real quadratic fields", *Compos. Math.* (online publication May 2015).

[Freitas et al. 2014] N. Freitas, B. Le Hung, and S. Siksek, "Elliptic curves over real quadratic fields are modular", *Invent. Math.* (online publication November 2014).

[Fujiwara 2006] K. Fujiwara, "Level optimisation in the totally real case", preprint, 2006. arXiv math/0602586v1

[Gross and Rohrlich 1978] B. H. Gross and D. E. Rohrlich, "Some results on the Mordell–Weil group of the Jacobian of the Fermat curve", *Invent. Math.* **44**:3 (1978), 201–224. MR 58 #10911 Zbl 0369.14011

[Halberstadt and Kraus 2002] E. Halberstadt and A. Kraus, "Courbes de Fermat: résultats et problèmes", *J. Reine Angew. Math.* **548** (2002), 167–234. MR 2003h:11068 Zbl 1125.11038

[Jarvis 2004] F. Jarvis, "Correspondences on Shimura curves and Mazur's principle at p", *Pacific J. Math.* **213**:2 (2004), 267–280. MR 2004m:11066 Zbl 1073.11030

[Jarvis and Meekin 2004] F. Jarvis and P. Meekin, "The Fermat equation over $\mathbb{Q}(\sqrt{2})$", *J. Number Theory* **109**:1 (2004), 182–196. MR 2005g:11045 Zbl 1078.11019

[Kamienny 1992] S. Kamienny, "Torsion points on elliptic curves and q-coefficients of modular forms", *Invent. Math.* **109**:2 (1992), 221–229. MR 93h:11054 Zbl 0773.14016

[Kraus 1990] A. Kraus, "Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive", *Manuscripta Math.* **69**:4 (1990), 353–385. MR 91j:11045 Zbl 0792.14014

[Kraus 1996] A. Kraus, "Courbes elliptiques semi-stables et corps quadratiques", *J. Number Theory* **60**:2 (1996), 245–253. MR 97e:11065 Zbl 0865.11050

[Mazur 1978] B. Mazur, "Rational isogenies of prime degree", *Invent. Math.* **44**:2 (1978), 129–162. MR 80h:14022 Zbl 0386.14009

[Ozman ≥ 2015] E. Ozman, "Quadratic points on non-hyperelliptic modular curves", in preparation.

[Rajaei 2001] A. Rajaei, "On the levels of mod l Hilbert modular forms", *J. Reine Angew. Math.* **537** (2001), 33–65. MR 2002i:11041 Zbl 0982.11023

[Ribet 1990] K. A. Ribet, "On modular representations of Gal($\overline{\mathbf{Q}}/\mathbf{Q}$) arising from modular forms", *Invent. Math.* **100**:2 (1990), 431–476. MR 91g:11066 Zbl 0773.11039

[Rohrlich 1994] D. E. Rohrlich, "Elliptic curves and the Weil–Deligne group", pp. 125–157 in *Elliptic curves and related topics*, edited by H. Kisilevsky and M. R. Murty, CRM Proc. Lecture Notes **4**, Amer. Math. Soc., Providence, RI, 1994. MR 95a:11054 Zbl 0852.14008

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331. MR 52 #8126 Zbl 0235.14012

[Silverman 1986] J. H. Silverman, *The arithmetic of elliptic curves*, Graduate Texts in Mathematics **106**, Springer, New York, 1986. MR 87g:11070 Zbl 0585.14026

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, New York, 1994. MR 96b:11074 Zbl 0911.14015

[Tzermias 2004] P. Tzermias, "Low-degree points on Hurwitz–Klein curves", *Trans. Amer. Math. Soc.* **356**:3 (2004), 939–951. MR 2004j:11061 Zbl 1116.14017

[Wiles 1995] A. Wiles, "Modular elliptic curves and Fermat's last theorem", *Ann. of Math.* (2) **141**:3 (1995), 443–551. MR 96d:11071 Zbl 0823.11029

nunobfreitas@gmail.com   *Mathematisches Institut, Universität Bayreuth, 95440 Bayreuth, Germany*

samir.siksek@gmail.com   *Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom*

Algebra & Number Theory

Algebra & Number Theory

Volume 9   No. 4   2015