
Article:
Khawaja, M and Jarvis, A (2025) Fermat's last theorem over Q(√2, (√3). Algebra & Number Theory, 19 (3). pp. 457-480. ISSN 1937-0652

https://doi.org/10.2140/ant.2025.19.457

Algebra & Number Theory

Volume 19
2025
No. 3

Fermat's last theorem over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

Maleeha Khawaja and Frazer Jarvis

msp

ALGEBRA AND NUMBER THEORY 19:3 (2025)
https://doi.org/10.2140/ant.2025.19.457

Fermat's last theorem over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$

Maleeha Khawaja and Frazer Jarvis

Dedicated to Iffat (Zaman) Khawaja
January 1936 – January 2022

In this paper, we begin the study of the Fermat equation $x^n + y^n = z^n$ over real biquadratic fields. In particular, we prove that there are no nontrivial solutions to the Fermat equation over $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ for $n \geq 4$.

1. Introduction

Since the groundbreaking work of Wiles [1995] on the resolution of the Fermat equation over $\mathbb{Q}$, the Fermat equation has been studied extensively over various number fields. Let K be a number field and let $n \geq 3$ be an integer. The Fermat equation over K with exponent n is the equation

$$x^n + y^n = z^n, \quad x, y, z \in K. \tag{1}$$

We say a solution (a, b, c) to (1) over K is trivial if $abc = 0$ and nontrivial otherwise.

Wiles' method of resolving (1) over $\mathbb{Q}$ became known as the modular approach. Thereafter, Jarvis and Meekin [2004] extended this method to prove that there are no nontrivial solutions to (1) over $\mathbb{Q}(\sqrt{2})$ for $n \geq 4$. This was followed by work of Freitas and Siksek [2015a; 2015b] who established a framework on how to resolve (1) (and more general Diophantine equations) over totally real number fields. Furthermore, Freitas and Siksek [2015b] proved that there are no nontrivial solutions to (1) over $\mathbb{Q}(\sqrt{d})$ for $n \geq 4$, where $3 \leq d \leq 23$, $d \neq 5, 17$ is a squarefree integer. When approaching real quadratic fields with a larger discriminant, they encountered the obstacle of demonstrating the irreducibility of certain Galois representations and eliminating the number of Hilbert newforms that arose as a result of level lowering. Michaud-Jacobs [2022] worked around these obstacles by studying quadratic points on certain modular curves and working directly with Hecke operators. He proved, for most squarefree d in the range $26 \leq d \leq 97$, that there are no nontrivial solutions to (1) over $\mathbb{Q}(\sqrt{d})$ for $n \geq 4$. Kraus [2019] provided a partial resolution of (1) over various totally real number fields of degrees ≤ 8. By a partial resolution we mean for all prime exponents $n = p > B_K$, where B_K is a constant depending only on K. For example if K is a real cubic field with discriminant 148, 404 or 564, or if K is the cyclic quartic field $\mathbb{Q}(\zeta_{16})^+$ then $B_K = 5$. It is a natural problem then to study (1) over real biquadratic fields. Freitas and Siksek [2015a] initiated the study of looking at (1) "asymptotically". As in [Freitas and Siksek 2015a], we say the

MSC2020: 11D41, 14G05, 14H52.
Keywords: Fermat equation, modularity, Galois representations, rational points, elliptic curves.

asymptotic Fermat's last theorem holds over K if there is a constant B_K such that there are no nontrivial solutions to (1) over K for primes $p > B_K$. Freitas, Kraus and Siksek [Freitas et al. 2020] studied the solutions to certain S-unit equations to prove that the asymptotic Fermat's last theorem holds for several infinite families of number fields — including some real biquadratic fields. In this paper, we will prove the following result and discuss some obstacles that arise over more general real biquadratic fields.

Theorem 1.1. *Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. There are no nontrivial solutions to (1) over K for $n \geq 4$.*

We give a brief outline of the paper. In Section 2, we apply and give a brief overview of the modular approach found in [Freitas and Siksek 2015a; 2015b]. In Section 3, we determine the conductor of the Frey curve using techniques outlined in [Freitas and Siksek 2015b], as well as Tate's algorithm [Silverman 1994, pp. 364–368]. In Section 4, we prove that $\bar{\rho}_{E,p}$ is irreducible for $p \geq 13$. For $p = 13$ and 17, we prove this by studying the explicit modular parametrisation. For $p \geq 19$, we use work of Derickx, Kamienny, Stein and Stoll [Derickx et al. 2023] and David [2011] to get a contradiction if $\bar{\rho}_{E,p}$ is reducible. In Section 6, we rule out solutions for certain small integer exponents. To treat $n = 9$ and $n = 6$, we study the hyperelliptic curves obtained from the Fermat curve of degree n. We also extend work of Mordell [1968] to determine all quartic points on the Fermat quartic lying in a quadratic extension of $\mathbb{Q}(\sqrt{2})$. In Section 7, we give a brief overview of some obstacles that arise when extending our method to more general real biquadratic fields. All supporting computations were performed in Magma; the scripts are available within the GitHub repository https://github.com/MaleehaKhawaja/Fermat.

2. The modular approach

Let K be a totally real field (until otherwise specified) and let $\mathcal{O}_K$ denote its ring of integers. Let $p \geq 5$ be a prime. Suppose (a, b, c) is a nontrivial solution to (1) over K with exponent p. The traditional Frey curve associated to (a, b, c) is given by

$$y^2 = x(x - a^p)(x + b^p).$$

Our Frey curve will be a quadratic twist of this elliptic curve by a well-chosen unit $\varepsilon \in \mathcal{O}_K^*$. We write

$$E = E_{a,b,c,\varepsilon} : y^2 = x(x - \varepsilon a^p)(x + \varepsilon b^p). \tag{2}$$

The reason for allowing twists by units is to reduce the number of possibilities for the conductor of the Frey curve. Write $\mathcal{N}_\varepsilon$ for the conductor of the Frey curve E above. We denote by $\bar{\rho}_{E,p}$ the mod p Galois representation associated to E.

The following theorem of Freitas and Siksek is formulated from the combination of the works of Fujiwara [2006], Jarvis [1999a; 1999b], and Rajaei [2001].

Theorem 2.1 [Freitas and Siksek 2015a, Theorem 7]. *Let K be a totally real field. Let $p \geq 5$ be a prime. Suppose $\mathbb{Q}(\zeta_p)^+ \not\subseteq K$. Let E be an elliptic curve over K with conductor $\mathcal{N}$. Suppose E is modular and $\bar{\rho}_{E,p}$ is irreducible. Denote by $\Delta_{\mathfrak{q}}$ the discriminant for a local minimal model of E at a prime ideal $\mathfrak{q}$*

of K. Let

$$\mathcal{M}_p := \prod_{\mathfrak{q} \| \mathcal{N}, p \mid v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})} \mathfrak{q}, \quad \mathcal{N}_p := \frac{\mathcal{N}}{M_p}.$$

Suppose the following conditions are satisfied for all prime ideals $\mathfrak{q} \mid p$:

(i) *E is semistable at $\mathfrak{q}$.*

(ii) *$p \mid v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$.*

(iii) *The ramification index satisfies $e(\mathfrak{q}/p) < p - 1$.*

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

We apply Theorem 2.1 to the Frey curve (2) in order to contradict the existence of the putative solution (a, b, c).

Several advances have been made in the direction of establishing the modularity of elliptic curves over totally real number fields. For example, the modularity of elliptic curves over real quadratic fields [Freitas et al. 2015] and totally real cubic fields [Derickx et al. 2020] has been established. Moreover, thanks to the following result of Box, we now know elliptic curves over most totally real quartic fields are modular.

Theorem 2.2 [Box 2022, Theorem 1.1]. *Let K be a totally real quartic field not containing $\sqrt{5}$. Every elliptic curve over K is modular.*

We turn to the question of how to show that conditions (i) and (ii) of Theorem 2.1 are satisfied. Let $\mathcal{H} = \mathrm{Cl}(K)/\mathrm{Cl}(K)^2$, where $\mathrm{Cl}(K)$ denotes the class group of K. We can assume, without loss of generality, that any nontrivial solution (a, b, c) to (1) is integral. By Lemma 3.3 of [Freitas and Siksek 2015b], a, b, c are coprime away from a small set of primes, i.e., $\gcd(a, b, c) = \mathfrak{m} \cdot \tau^2$ for some $\mathfrak{m} \in \mathcal{H}$ and odd prime ideal $\tau \neq \mathfrak{m}$. The following result addresses conditions (i) and (ii) above.

Lemma 2.3 [Freitas and Siksek 2015b, Lemma 3.3]. *Let K be a totally real field. Let S denote the set of primes of K above 2. Let $\mathfrak{q}$ be a prime ideal of K such that $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$. Then E is semistable at $\mathfrak{q}$ and $p \mid v_{\mathfrak{q}}(\Delta_{\mathfrak{q}})$.*

We remark that our Frey curve is a quadratic twist of the usual Frey curve by a unit and thus the set of primes dividing the conductor remains unchanged away from 2.

The Jacobian of the Fermat curve of degree 5, 7 or 11 has finitely many rational points. Since the divisor obtained from the formal sum of a point and its Galois conjugates gives a rational divisor, this allows the study of points on these Fermat curves over fields of low degree. Klassen and Tzermias [1997] have classified all points on the Fermat quintic defined over number fields of degree at most 6. Building on this work, Kraus [2018] has provided an algebraic description of the quartic points on the Fermat quintic. Tzermias [1998] has determined all points on the Fermat septic defined over number fields of degree at most 5. Gross and Rohrlich [1978] have determined all points on (1) with exponent $p = 11$ over fields of degree at most 5. We can thus suppose that $n = 4, 6, 9$, or $n = p \geq 13$ is a prime.

Throughout, unless otherwise specified, let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and let $\mathcal{O}_K$ denote its ring of integers. Let $p \geq 13$ be a prime. Suppose there is a nontrivial solution (a, b, c) to (1) over K with exponent p. Let E be the Frey curve (2) associated to this solution. By Theorem 2.2, E is modular. We note that K has class number 1 and thus $\mathfrak{m} = 1 \cdot \mathcal{O}_K$. Suppose $\mathfrak{q} \mid p$ is a prime ideal of K. By Lemma 2.3, assumptions (i) and (ii) of Theorem 2.1 are satisfied for $\mathfrak{q}$. In particular, E is semistable away from 2. Thus, in order to prove Theorem 1.1, it remains to

(1) determine the reduction type of E at $\mathfrak{P}$, where $\mathfrak{P}$ is the unique prime above 2,

(2) prove that $\bar{\rho}_{E,p}$ is irreducible for $p \geq 13$,

(3) eliminate the Hilbert newforms arising as a result of level lowering (Theorem 2.1),

(4) rule out solutions to (1) for $n = 4$, 6 and 9.

3. Computing the lowered level

Write $\mathcal{N}_\varepsilon$ for the conductor of the Frey curve E above. We note that $2\mathcal{O}_K = \mathfrak{P}^4$ and $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$. Thus $\mathfrak{P}$ divides exactly one of a, b, c, since $\gcd(a, b, c) = 1$. Without loss of generality, we suppose $\mathfrak{P} \mid b$.

Lemma 3.1. *Suppose that either $p \geq 17$, or $p = 13$ and $\mathrm{ord}_{\mathfrak{P}}(b) \geq 2$. There is some $\varepsilon \in \mathcal{O}_K^*$ such that one of the following holds*:

(i) *Either E has multiplicative reduction at $\mathfrak{P}$, or*

(ii) *E has additive potentially multiplicative reduction at $\mathfrak{P}$ and $\mathrm{ord}_{\mathfrak{P}}(\mathcal{N}_\varepsilon) = 4$.*

Proof. Write c_4, c_6, Δ and j for the usual invariants attached to the model (2). A straightforward computation shows that

$$c_4 = \varepsilon^2 \cdot 16 \cdot (c^{2p} - a^p b^p), \quad \Delta = \varepsilon^6 \cdot 16 \cdot (abc)^{2p}, \quad j = c_4^3/\Delta.$$

We recall that $\mathfrak{P} \mid b$. Write $t = \mathrm{ord}_{\mathfrak{P}}(b)$. Then,

$$\mathrm{ord}_{\mathfrak{P}}(j) = 3\,\mathrm{ord}_{\mathfrak{P}}(c_4) - \mathrm{ord}_{\mathfrak{P}}(\Delta) = 32 - 2pt. \tag{3}$$

Under the assumptions of the lemma, we have $\mathrm{ord}_{\mathfrak{P}}(j) < 0$; thus we have potentially multiplicative reduction at $\mathfrak{P}$ (irrespective of the choice of ε).

The rest of the lemma is a consequence of [Freitas and Siksek 2015b, Lemma 4.4]. We give some of the details. Let

$$\mathfrak{b} = \mathfrak{P}^{2\,\mathrm{ord}_{\mathfrak{P}}(2)+1} = \mathfrak{P}^9.$$

Consider the natural map

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

By an explicit computation in Magma, we find that the image of Φ has index 2 in the codomain, and that $\lambda_1 = 1$ and $\lambda_2 = -1 + 2\mu$ are elements of $\mathcal{O}_K$ which represent the cokernel, where $\mu = \sqrt{2} + \sqrt{3}$. Let $n_i = \mathrm{ord}_{\mathfrak{P}}(\Delta(L_i/K))$, where $L_i = K(\sqrt{\lambda_i})$ and $\Delta(L_i/K)$ is the relative discriminant ideal for the

extension L_i/K. We find that $n_1 = 0$ and $n_2 = 2$. By the aforementioned lemma, there is a unit $\varepsilon \in \mathcal{O}_K^*$ such that $\mathrm{ord}_{\mathfrak{P}}(\mathcal{N}_\varepsilon) = 1$ or 4. □

In Lemma 3.1, we determined the conductor of the Frey curve E for all primes $p \geq 17$ and a suitable choice of $\varepsilon \in \mathcal{O}_K^*$. In particular, we prove that E either has multiplicative reduction or additive potentially multiplicative reduction at $\mathfrak{P}$. This proof fails for $p = 13$ in the case that $\mathrm{ord}_{\mathfrak{P}}(b) = 1$, and we treat this case separately in the rest of the section.

Lemma 3.2. *Suppose* $p = 13$ *and* $\mathrm{ord}_{\mathfrak{P}}(b) = 1$. *Then there is a unit* $\varepsilon \in \mathcal{O}_K^*$ *and* $\alpha \in \mathcal{O}_K$ *such that*

$$\mathfrak{P}^6 \mid (\varepsilon b^{13} - \varepsilon a^{13} - \alpha^2),$$

where $\mathfrak{P} \nmid \alpha$.

Proof. Let

$$\theta : \mathcal{O}_K^* \to U/U^2,$$

where $U = (\mathcal{O}_K/\mathfrak{P}^6)^*$. We checked that θ is surjective using a straightforward computation in Magma. Let $\beta = b^{13} - a^{13}$. Note that $\mathfrak{P} \nmid \beta$. As θ is surjective, there is some $\gamma \in \mathcal{O}_K^*$ such that $\theta(\gamma) = \beta U^2$. Thus $\beta \equiv \gamma\alpha^2 \pmod{\mathfrak{P}^6}$ for some $\alpha \in \mathcal{O}_K \setminus \mathfrak{P}$. Let $\varepsilon = \gamma^{-1} \in \mathcal{O}_K^*$. Then $\varepsilon\beta \equiv \alpha^2 \pmod{\mathfrak{P}^6}$, which proves the lemma. □

Let $\varepsilon \in \mathcal{O}_K^*$ be as in Lemma 3.2. We begin by working with the Frey curve

$$E_{13,\varepsilon} : y^2 = x(x - \varepsilon a^{13})(x + \varepsilon b^{13}). \tag{4}$$

We recall that, by Lemma 2.3, $E_{13,\varepsilon}$ is semistable away from $\mathfrak{P}$. Thus, in order to determine the conductor of $E_{13,\varepsilon}$, it remains to determine the reduction type of $E_{13,\varepsilon}$ at $\mathfrak{P}$.

Lemma 3.3. *Suppose* $\mathrm{ord}_{\mathfrak{P}}(b) = 1$. *The Frey curve* $E_{13,\varepsilon}$ *has additive potentially good reduction at* $\mathfrak{P}$. *Moreover*, $\mathrm{ord}_{\mathfrak{P}}(\mathcal{N}) = 5$, *where* $\mathcal{N}$ *is the conductor of* $E_{13,\varepsilon}$.

Proof. Let $\alpha \in \mathcal{O}_K$ be as in Lemma 3.2. Recall that K has class number 1, and therefore every ideal is principal. Let π be a generator for $\mathfrak{P}$. For example, we can take

$$\pi = \frac{\mu^3 + \mu^2 - 9\mu - 9}{4},$$

where $\mu = \sqrt{2} + \sqrt{3}$. We make the substitutions

$$x \mapsto \pi^6 x, \quad y \mapsto \alpha\pi^6 x + \pi^9 y.$$

This yields the model

$$W : y^2 + \frac{2\alpha}{\pi^3}xy = x^3 + \frac{(\varepsilon b^{13} - \varepsilon a^{13} - \alpha^2)}{\pi^6}x^2 - \frac{\varepsilon^2 a^{13} b^{13}}{\pi^{12}}x,$$

which is integral by Lemma 3.2 and has discriminant

$$\Delta(W) = \frac{\Delta(E_{13,\varepsilon})}{\pi^{36}} = \frac{16\varepsilon^6 a^{26} b^{26} c^{26}}{\pi^{36}}.$$

Note that $\mathrm{ord}_{\mathfrak{P}}(\Delta(W)) = 6$. Thus W is minimal at $\mathfrak{P}$. We use Tate's algorithm [Silverman 1994, pp. 364–368] to compute the valuation of the conductor for W. Let $a_1, \ldots, a_6$ be the usual a-invariants for W given in the above model, and let $b_2, \ldots, b_8$ be the corresponding b-invariants

$$b_2 = \frac{4\alpha^2}{\pi^6}, \quad b_4 = -\frac{2\varepsilon^2 a^{13} b^{13}}{\pi^{12}}, \quad b_6 = 0, \quad b_8 = -\frac{\varepsilon^4 a^{26} b^{26}}{\pi^{24}}.$$

In particular, $\mathfrak{P} \mid a_3$, a_4, b_2 and $\mathfrak{P}^2 \mid a_6$, and $\mathrm{ord}_{\mathfrak{P}}(b_8) = 2$. Thus, by Step 4 of Tate's algorithm, the reduction type for W at $\mathfrak{P}$ is III, and the valuation of the conductor at $\mathfrak{P}$ is

$$\mathrm{ord}_{\mathfrak{P}}(\mathcal{N}) = \mathrm{ord}_{\mathfrak{P}}(\Delta(W)) - 1 = 5. \qquad \square$$

4. Proving irreducibility of $\bar{\rho}_{E,p}$

We prove that $\bar{\rho}_{E,p}$ is irreducible for $p \geq 13$. In particular, we show that a possible consequence of $\bar{\rho}_{E,p}$ being reducible is that E has a K-rational point of order p. In this instance, by [Derickx et al. 2023, Theorem 1.2], we obtain a contradiction if $p \geq 19$. We thus treat the primes $p = 13$ and 17 separately.

Since the Frey curve E has full 2-torsion over K, it is sufficient to show that there are no noncuspidal K-rational points on one of the modular curves $X_0(p)$, $X_0(2p)$ or $X_0(4p)$. We find it convenient to work with the modular curves $X_0(26)$ and $X_0(34)$. In particular, we show that $X_0(26)(K) = X_0(26)(\mathbb{Q})$ and $X_0(34)(K) = X_0(34)(\mathbb{Q})$. All points in $X_0(26)(\mathbb{Q})$ and $X_0(34)(\mathbb{Q})$ are cuspidal, thus proving the irreducibility of $\bar{\rho}_{E,p}$ for $p = 13$ and 17.

4.1. $p = 13$. Using the explicit modular parametrisation, we prove that if $P \in X_0(26)(K)$ then either $P \in X_0(26)(\mathbb{Q}(\sqrt{3}))$ or $C(\mathbb{Q}(\sqrt{3}))$ is nonempty, where C is a genus 2 hyperelliptic curve. In the first case, by [Bruin and Najman 2015], $P \in X_0(26)(\mathbb{Q})$. In the second case, we show that $C(\mathbb{Q}(\sqrt{3}))$ is empty.

Lemma 4.1. *$\bar{\rho}_{E,13}$ is irreducible.*

Proof. We prove that $X_0(26)(K) = X_0(26)(\mathbb{Q})$. We work with the model

$$X_0(26) : y^2 = x^6 - 8x^5 + 8x^4 - 18x^3 + 8x^2 - 8x + 1 \tag{5}$$

given in Magma. Let

$$E' : y^2 + xy + y = x^3 - x^2 - 3x + 3.$$

Then E' is the elliptic curve with Cremona label `26b1`. Suppose $P = (a, b) \in X_0(26)(K)$. Note that if $a = 1$ then $b^2 = -16$, i.e., $P \notin X_0(26)(K)$. Suppose from now on that $a \neq 1$. Using Magma, we find the explicit parametrisation

$$\pi : X_0(26) \to E', \quad (a, b) \mapsto \left(-\frac{(a+1)^2}{(a-1)^2}, \frac{-2b + 2a(a-1)}{(a-1)^3} \right).$$

Let $L = \mathbb{Q}(\sqrt{3})$. We checked using Magma that $E'(K) = E'(L)$. It immediately follows that

$$\left(\frac{a+1}{a-1} \right)^2 \in L.$$

Let

$$\sigma : K \to K, \quad \sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(\sqrt{3}) = \sqrt{3}.$$

Then

$$\sigma\left(\frac{a+1}{a-1}\right) = \frac{a+1}{a-1} \quad \text{or} \quad \sigma\left(\frac{a+1}{a-1}\right) = -\frac{a+1}{a-1}.$$

Thus there are two cases to consider:

(1) $(a+1)/(a-1) \in L$.

(2) $(a+1)/(a-1) \in \sqrt{2} \cdot L$.

Case (1). In this case $a \in L$, and it immediately follows from the parametrisation of π that $b \in L$. Observe that $X_0(26)$ has infinitely many quadratic points of the form $(r, \sqrt{f(r)})$, where $r \in \mathbb{Q}$. Such points are called *nonexceptional* and all other quadratic points are called *exceptional*.

Case (1.1). If $a \in L \setminus \mathbb{Q}$ then P is an exceptional quadratic point on $X_0(26)$. Bruin and Najman [2015, Table 3] have given an explicit description of all quadratic points on $X_0(26)$. They find that all exceptional quadratic points are defined over $\mathbb{Q}(\sqrt{d})$ for $d = -1, -3, -11$ and -23.

Case (1.2). If $a \in \mathbb{Q}$ then $b^2 \in \mathbb{Q}$. Then P is a nonexceptional quadratic point on $X_0(26)$ defined over L. Moreover, P corresponds to a rational point on the quadratic twist of $X_0(26)$ over $\mathbb{Q}(\sqrt{3})$. We denote this quadratic twist by X_3. We checked using Magma that X_3 has no points defined over $\mathbb{Q}_3$. Thus $X_3(\mathbb{Q})$ is empty.

Case (2). In this case we have $(a+1)/(a-1) \in \sqrt{2} \cdot L$, i.e.,

$$\frac{a+1}{a-1} = \sqrt{2}\alpha \quad \text{for some } \alpha \in L. \tag{6}$$

Note the identity

$$\left(\frac{a+1}{a-1}\right)^2 - 1 = \frac{(a+1)^2 - (a-1)^2}{(a-1)^2} = \frac{4a}{(a-1)^2} = \frac{4a(a-1)}{(a-1)^3}. \tag{7}$$

From the parametrisation of π and (7), we see that

$$\frac{b}{(a-1)^3} \in L.$$

Note the identity

$$16\left(\frac{a^6 - 8a^5 + 8a^4 - 18a^3 + 8a^2 - 8a + 1}{(a-1)^6}\right) = -4\left(\frac{a+1}{a-1}\right)^6 - 3\left(\frac{a+1}{a-1}\right)^4 + 10\left(\frac{a+1}{a-1}\right)^2 + 13. \tag{8}$$

By combining (5) and (8), we obtain

$$\left(\frac{4b}{(a-1)^3}\right)^2 = -4\left(\frac{a+1}{a-1}\right)^6 - 3\left(\frac{a+1}{a-1}\right)^4 + 10\left(\frac{a+1}{a-1}\right)^2 + 13.$$

After making the substitutions $\beta = 4b/(a-1)^3$ and (6), we obtain

$$\beta^2 = -32\alpha^6 - 12\alpha^4 + 20\alpha^2 + 13.$$

Thus (α, β) is a L-rational point on the curve

$$C : y^2 = -32x^6 - 12x^4 + 20x^2 + 13.$$

Write $\mathcal{O}_L$ for the ring of integers of L. Then $13\mathcal{O}_L = \mathfrak{p}_1\mathfrak{p}_2$. We checked using Magma that there are no points on C defined over the completion of L at $\mathfrak{p}_1$. Thus $C(L)$ is empty. □

4.2. $p = 17$. Using the explicit modular parametrisation, we show that if $P \in X_0(34)(K)$ then either $P \in X_0(34)(\mathbb{Q}(\sqrt{2}))$ or $C(\mathbb{Q}(\sqrt{2}))$ is nonempty, where C is the quadratic twist of $X_0(34)$ over $\mathbb{Q}(\sqrt{3})$. In the first case, by [Ozman and Siksek 2019], $P \in X_0(34)(\mathbb{Q})$. In the second case, we show that $C(\mathbb{Q}(\sqrt{2}))$ is empty.

Lemma 4.2. *$\bar{\rho}_{E,17}$ is irreducible.*

Proof. We prove that $X_0(34)(K) = X_0(34)(\mathbb{Q})$. We work with the model

$$X_0(34) : x^4 - y^4 + x^3 + 3xy^2 - 2x^2 + x + 1 = 0 \tag{9}$$

given in Magma. Making the change of variables $x \mapsto x,\ y \mapsto y^2$ yields the curve

$$C' : x^4 - y^2 + x^3 + 3xy - 2x^2 + x + 1 = 0.$$

Since C' has genus 1, we can transform it to an elliptic curve:

$$C' \to E', \quad (x, y) \mapsto (2(x^2 - 2x + y),\ 4x(x^2 - 2x + y)), \tag{10}$$

where

$$E' : y^2 + xy + 2y = x^3 - 4x$$

is the elliptic curve with Cremona label `34a1`. We deduce the explicit modular parametrisation

$$\pi : X_0(34) \to E', \quad (x, y) \mapsto (2(x^2 - 2x + y^2),\ 4x(x^2 - 2x + y^2)).$$

Let $L = \mathbb{Q}(\sqrt{2})$. Using Magma we find that $E'(K) = E'(L)$. Suppose $P = (a, b) \in X_0(34)(K)$. Since

$$2(a^2 - 2a + b^2),\ 4a(a^2 - 2a + b^2) \in L,$$

it follows that either $a^2 - 2a + b^2 = 0$ or $a \in L$. Suppose the former is true, i.e.,

$$b^2 = 2a - a^2. \tag{11}$$

We substitute (11) into (9) to find that

$$2a^3 + a + 1 = 0$$

and $a \notin K$. Thus $a \in L$, and hence $b^2 \in L$. Either $b \in L$ or $b = \sqrt{3}\beta$ for some $\beta \in L$. If $b \in L$ then $P \in X_0(34)(L)$. Ozman and Siksek [2019] have determined the quadratic points on $X_0(34)$, and they found that there are no real quadratic points on $X_0(34)$. Thus $P \in X_0(34)(\mathbb{Q})$.

Suppose $b = \sqrt{3}\beta$ for some $\beta \in L$. Thus (a, β) is an L-rational point on the curve

$$C : x^4 - 9y^4 + x^3 + 9xy^2 - 2x^2 + x + 1 = 0,$$

where C is the quadratic twist of $X_0(34)$ over $\mathbb{Q}(\sqrt{3})$. Note that 3 is inert in L. We checked using Magma that there are no points on C defined over the completion of L at $3\mathcal{O}_L$. Thus $C(L)$ is empty. □

4.3. $p \geq 19$. We let $E = E_{a,b,c,\varepsilon}$, where $\varepsilon \in \mathcal{O}_K^*$ is chosen so that one of the two possibilities in Lemma 3.1 hold. Suppose $\bar{\rho}_{E,p}$ is reducible. Then

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

where θ and θ' are characters $G_K \to \mathbb{F}_p^*$. Recall that $\chi_p = \det(\bar{\rho}_{E,p}) = \theta\theta'$, where χ_p denotes the mod p cyclotomic character. We let $\mathcal{N}_\theta$ and $\mathcal{N}_{\theta'}$ denote the conductors of θ and θ', respectively. We shall require the following result of Freitas and Siksek.

Lemma 4.3 [Freitas and Siksek 2015b, Lemma 6.3]. *Let E be an elliptic curve defined over a number field K with conductor $\mathcal{N}$. Let $p \geq 5$ be a prime, and let $\mathfrak{q} \nmid p$ be a prime. Let θ and θ' be as above. If $\bar{\rho}_{E,p}$ is reducible then*

$$\operatorname{ord}_\mathfrak{q}(\mathcal{N}_\theta) = \operatorname{ord}_\mathfrak{q}(\mathcal{N}_{\theta'}) = \begin{cases} 0 & \text{if } E \text{ has good or multiplicative reduction at } \mathfrak{q}, \\ \frac{1}{2}\operatorname{ord}_\mathfrak{q}(\mathcal{N}) \in \mathbb{Z} & \text{if } E \text{ has additive reduction at } \mathfrak{q}. \end{cases}$$

Lemma 4.4. *Let $p \geq 19$. Then $\bar{\rho}_{E,p}$ is irreducible.*

Proof. Suppose $\bar{\rho}_{E,p}$ is reducible. Since p is unramified in K and E has good or multiplicative reduction at $\mathfrak{p} \mid p$, we have that, for any $\mathfrak{p} \mid p$, precisely one of θ, θ' is ramified at $\mathfrak{p}$; see [Kraus 1996, Lemma 1].

First suppose that either of θ, θ' is unramified at all $\mathfrak{p} \mid p$ (and thus the other is ramified at all $\mathfrak{p} \mid p$). We note that replacing E by a p-isogenous elliptic curve, if necessary, allows us to swap θ and θ'. Thus we may suppose that θ is unramified at all the primes above p, and hence θ is unramified away from $\mathfrak{P}$.

We shall use Lemma 4.3 to determine $\mathcal{N}_\theta$. Suppose we are in case (i) of Lemma 3.1 and E has multiplicative reduction at $\mathfrak{P}$. Then, by Lemma 4.3, we have $\operatorname{ord}_\mathfrak{P}(\mathcal{N}_{\theta'}) = \operatorname{ord}_\mathfrak{P}(\mathcal{N}_\theta) = 0$. Suppose now that we are in case (ii) of Lemma 3.1 and E has additive reduction at $\mathfrak{P}$. Then, by Lemma 4.3, we have

$$\operatorname{ord}_\mathfrak{P}(\mathcal{N}_\theta) = \operatorname{ord}_\mathfrak{p}(\mathcal{N}_{\theta'}) = \tfrac{1}{2}\operatorname{ord}_\mathfrak{P}(\mathcal{N}_\varepsilon) = 2.$$

Hence either $\mathcal{N}_\theta = 1$ or $\mathfrak{P}^2$. Let $\infty_1, \ldots, \infty_4$ denote the four real places of K. Then θ is a character for the ray class group of the modulus $\infty_1 \cdots \infty_4$ in the first case, and of the modulus $\mathfrak{P}^2 \cdot \infty_1 \cdots \infty_4$ in the second case. Using Magma we find that this ray class group is $\mathbb{Z}/2\mathbb{Z}$ in either case. Thus the order of θ divides 2, and θ is either trivial or a quadratic character. In the first case, when θ is trivial, E has a K-rational point of order p. In the second case, let E' be the quadratic twist of E by θ. Then

$$\bar{\rho}_{E',p} \sim \begin{pmatrix} \theta^2 & * \\ 0 & \theta\theta' \end{pmatrix} = \begin{pmatrix} 1 & * \\ 0 & \chi_p \end{pmatrix}.$$

Thus E' has a K-rational point of order p. In both cases, we obtain an elliptic curve with a point of order p defined over K (a quartic field). By [Derickx et al. 2023, Theorem 1.2], $p \leq 17$. We obtain a contradiction since $p \geq 19$.

Fix $\mathfrak{p}_0$ a prime ideal of $\mathcal{O}_K$ above p. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. Then G acts transitively on the primes $\mathfrak{p} \mid p$. Let S be the set of $\tau \in G$ such that θ is ramified at $\tau(\mathfrak{p}_0)$. We know from above that S is a proper subset of G, i.e., $S \neq \varnothing$ and $S \neq G$. For a prime ideal $\mathfrak{q}$ of $\mathcal{O}_K$, we write $I_\mathfrak{q}$ for an inertia subgroup of G_K corresponding to $\mathfrak{q}$. Thus $\theta|_{I_\mathfrak{q}} = 1$ for all

$$\mathfrak{q} \notin \{\mathfrak{P}\} \cup \{\tau(\mathfrak{p}_0) : \tau \in S\}.$$

By Lemma 3.1, E has potentially multiplicative reduction at $\mathfrak{P}$. By the theory of the Tate curve [David 2011, Proposition 1.2], $\theta^2|_{I_\mathfrak{P}} = 1$. Let $\phi = \theta^2$. Then $\phi|_{I_\mathfrak{q}} = 1$ for all

$$\mathfrak{q} \notin \{\tau(\mathfrak{p}_0) : \tau \in S\}.$$

Recall that θ' is unramified at $\mathfrak{q} \in \{\tau(\mathfrak{p}_0) : \tau \in S\}$. Since $\theta\theta' = \chi_p$, we conclude that

$$\phi|_{I_\mathfrak{q}} = \begin{cases} \chi_p^2|_{I_\mathfrak{q}}, & \mathfrak{q} \in \{\tau(\mathfrak{p}_0) : \tau \in S\}, \\ 1 & \text{otherwise.} \end{cases} \tag{12}$$

Let $u \in \mathcal{O}_K^*$. We define the twisted norm of u attached to S to be

$$\mathfrak{N}_S(u) = \prod_{\tau \in S} (\tau(u))^2.$$

By the proof of [David 2011, Proposition 2.6], the existence of ϕ satisfying (12) ensures that

$$\mathfrak{p}_0 \mid (\mathfrak{N}_S(u) - 1).$$

Let $\mu = \sqrt{2} + \sqrt{3}$, and let

$$u_1 = \mu, \quad u_2 = \tfrac{1}{2}(-\mu^3 + 9\mu + 2), \quad u_3 = \tfrac{1}{4}(\mu^3 - \mu^2 - 9\mu + 5);$$

this is a basis for $\mathcal{O}_K^*/\{\pm 1\}$. Then $p \mid B_S$, where

$$B_S = \mathrm{Norm}\left(\sum_{i=1}^{3} (\mathfrak{N}_S(u_i) - 1) \cdot \mathcal{O}_K\right).$$

We used Magma to compute B_S for all nonempty proper subsets S of $G = \mathrm{Gal}(K/\mathbb{Q})$. In all cases we found that if $p \mid B_S$ then $p = 2$ or 3. Thus we obtain a contradiction. □

5. Eliminating Hilbert newforms

Let

$$\mathcal{N}_0 = \begin{cases} \mathfrak{P} & \text{if we are in case (i) of Lemma 3.1,} \\ \mathfrak{P}^4 & \text{if we are in case (ii) of Lemma 3.1,} \\ \mathfrak{P}^5 & \text{if } p = 13 \text{ and } \mathrm{ord}_\mathfrak{P}(b) = 1. \end{cases}$$

Applying level lowering (i.e., Theorem 2.1), we obtain

$$\bar{\rho}_{E,p} \sim \bar{\rho}_{\mathfrak{f},\mathfrak{p}},$$

where $\mathfrak{f}$ is a Hilbert newform of parallel weight 2 and level $\mathcal{N}_0$, and $\mathfrak{p}$ is some prime above p in $\mathbb{Q}_\mathfrak{f}$, the Hecke eigenvalue field of $\mathfrak{f}$. Using Magma we find that there are no newforms with parallel weight 2 and level $\mathfrak{P}$ or level $\mathfrak{P}^5$, obtaining a contradiction in these cases.

We thus suppose we are in case (ii) of Lemma 3.1. For the level $\mathfrak{P}^4$, we find that there are two newforms $\mathfrak{f}_1$ and $\mathfrak{f}_2$ and for both the corresponding Hecke eigenvalue field is $\mathbb{Q}$. Let E_1/K and E_2/K be the following elliptic curves:

$$E_1 : y^2 + (\mu+1)xy = x^3 + \tfrac{1}{4}(-\mu^3-\mu^2-3\mu+5)x^2 + \tfrac{1}{2}(-\mu^3-5\mu)x + \tfrac{1}{4}(\mu^3+7\mu^2-9\mu-3),$$
$$E_2 : y^2 + \tfrac{1}{4}(\mu^3+\mu^2+3\mu+3)y = x^3 + \tfrac{1}{2}(-\mu^2-1)x^2 + \mu^2 x + \tfrac{1}{4}(-3\mu^3-17\mu^2-\mu+1),$$

where $\mu = \sqrt{2}+\sqrt{3}$. These elliptic curves have conductors $\mathfrak{P}^4$ and were found using the Magma command EllipticCurveSearch. These are nonisogenous, as $a_\mathfrak{q}(E_1) = 6$ and $a_\mathfrak{q}(E_2) = -6$, where $3\mathcal{O}_K = \mathfrak{q}^2$. By the work of Box [2022], E_1 and E_2 are modular and thus correspond to the two Hilbert newforms $\mathfrak{f}_1$ and $\mathfrak{f}_2$ of parallel weight 2 and level $\mathfrak{P}^4$. Thus $\bar{\rho}_{E,p} \sim \bar{\rho}_{E_i,p}$, where $i = 1$ or 2. To obtain a contradiction, we shall use a standard image of inertia argument; see [Freitas and Siksek 2015a, Lemma 3.5].

Let j be the j-invariant of the Frey curve E. By (3) we have $\mathrm{ord}_\mathfrak{P}(j) < 0$ and $p \nmid \mathrm{ord}_\mathfrak{P}(j)$. Thus, $p \mid \#\bar{\rho}_{E,p}(I_\mathfrak{P})$ [Silverman 1994, Proposition 6.1, Chapter 5]. However, we find that E_1 and E_2 have j-invariants

$$j_1 = 0 \quad \text{and} \quad j_2 = -853632\mu^3 + 7682688\mu + 2417472,$$

respectively. As $\mathrm{ord}_\mathfrak{P}(j_i) \geq 0$, we have that E_1 and E_2 have potentially good reduction at $\mathfrak{P}$. It follows that $\#\bar{\rho}_{E_i,p}(I_\mathfrak{P}) \mid 24$ from [Kraus 1990, Introduction]. As $\bar{\rho}_{E,p} \sim \bar{\rho}_{E_i,p}$ for $i = 1$ or 2, we obtain $p \mid 24$ giving a contradiction.

6. Small integer exponents

We have thus far shown that there are no solutions to (1) over K for primes $p \geq 5$. In order to complete the proof of Theorem 1.1, it remains to rule out solutions to (1) for $n = 4, 6, 9$. We note in passing that there are nontrivial solutions to the Fermat cubic over $\mathbb{Q}(\sqrt{2})$; see [Jarvis and Meekin 2004, p. 184].

6.1. $n = 9$. We are very grateful to Samir Siksek for the lengthy discussions and ideas that resulted in this proof. We first convert the problem of finding K-points on the Fermat curve of degree 9 to finding the $\mathbb{Q}(\sqrt{3})$-points on a certain hyperelliptic curve C. We then study the Jacobian of C to show that $C(\mathbb{Q}(\sqrt{3})) = \{\infty\}$, where ∞ denotes the point at infinity on C.

Theorem 6.1. *There are no nontrivial solutions to (1) over K for $n = 9$.*

We find it convenient to let

$$F_9 : x^9 + y^9 + z^9 = 0.$$

That is, F_9 is the Fermat curve of degree 9. We recall that $2\mathcal{O}_K = \mathfrak{P}^4$ and that K has class number 1. We will prove that $F_9(K) = \{(1:-1:0), (1:0:-1), (0:1:-1)\}$, i.e, $F_9(K)$ consists only of trivial

solutions. Suppose $(\alpha : \beta : \gamma) \in F_9(K)$ is a nontrivial solution. We may suppose that $\alpha, \beta, \gamma \in \mathcal{O}_K$ and that they are coprime. We recall that $\mathcal{O}_K/\mathfrak{P} = \mathbb{F}_2$ and

$$F_9(\mathbb{F}_2) = \{(1:1:0), (1:0:1), (0:1:1)\}.$$

Hence, by permuting α, β, γ appropriately, we may suppose $(\alpha : \beta : \gamma) \equiv (1:1:0) \pmod{\mathfrak{P}}$. Thus

$$\mathfrak{P} \mid \gamma, \quad \mathfrak{P} \nmid \alpha\beta. \tag{13}$$

Observe

$$\gamma^{18} - (\alpha^9 - \beta^9)^2 = (\alpha^9 + \beta^9)^2 - (\alpha^9 - \beta^9)^2 = 4(\alpha\beta)^9.$$

After making the substitutions

$$u = \frac{\alpha\beta}{\gamma^2}, \quad v = \frac{\alpha^9 - \beta^9}{\gamma^9}, \tag{14}$$

we see that $Q_1 = (u, v) \in C_1(K)$, where

$$C_1 : y^2 = -4x^9 + 1.$$

Let

$$E_1 : y^2 = 4x^3 + 1.$$

This is an elliptic curve. Let

$$\pi_1 : C_1 \to E_1, \quad (x, y) \mapsto (-x^3, y).$$

The elliptic curve E_1 has minimal Weierstrass model

$$E_1' : z^2 + z = x^3,$$

which is obtained from E_1 by the substitution $y = 2z + 1$. This has Cremona label `27a3`. In particular, E_1' has good reduction away from 3. Let $R_1 = \pi_1(Q_1) = (-u^3, v) \in E_1(K)$. Then R_1 corresponds to the point

$$S_1 = \left(-u^3, \tfrac{1}{2}(v-1)\right) \in E_1'(K).$$

Let $\sigma : K \to K$ be the automorphism satisfying

$$\sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(\sqrt{3}) = \sqrt{3}.$$

We note that the fixed field of σ is $L = \mathbb{Q}(\sqrt{3})$. Thus $S_1 + S_1^\sigma \in E_1'(L)$. We checked using Magma that E_1' has rank 0 over L, and indeed

$$E_1'(L) = \{\mathcal{O}, (0,0), (0,-1)\} \cong \mathbb{Z}/3\mathbb{Z}. \tag{15}$$

Thus $S_1 + S_1^\sigma$ is one of these three points. However, $\mathrm{ord}_{\mathfrak{P}}(u) < 0$ by (13) and (14). It follows that

$$S_1 \equiv \mathcal{O} \pmod{\mathfrak{P}}.$$

Hence

$$S_1^\sigma \equiv \mathcal{O}^\sigma = \mathcal{O} \pmod{\mathfrak{P}^\sigma}.$$

However, $\mathfrak{P}$ is a totally ramified prime, so $\mathfrak{P}^\sigma = \mathfrak{P}$. Thus $S_1^\sigma \equiv \mathcal{O} \pmod{\mathfrak{P}}$, and

$$S_1 + S_1^\sigma \equiv \mathcal{O} \pmod{\mathfrak{P}}.$$

By (15) and the injectivity of torsion upon reduction modulo primes of good reduction (see [Katz 1981, Appendix]), we conclude that

$$S_1 + S_1^\sigma = \mathcal{O}.$$

Hence

$$R_1 + R_1^\sigma = \mathcal{O}.$$

Hence

$$(-u^3)^\sigma = -u^3, \quad v^\sigma = -v.$$

As the only cube root of 1 in K is 1, we have $u^\sigma = u$ and so $u \in L$. Moreover, $v^2 = -4u^9 + 1 \in L$ and $v^\sigma = -v$, so $v = w/\sqrt{2}$, where $w \in L$. Hence $(u, w) \in C(L)$, where

$$C : y^2 = 2(-4x^9 + 1).$$

Lemma 6.2. $C(L) = \{\infty\}$.

Since $u = \alpha\beta/\gamma^2$, Theorem 6.1 follows from Lemma 6.2. We now prove Lemma 6.2 by studying $J(\mathbb{Q})$, where J is the Jacobian of C.

Proof. Let

$$E : y^2 = x^3 + 2,$$

which is the elliptic curve with Cremona label `1728a1`. Let

$$\pi : C \to E, \quad (x, y) \mapsto (-2x^3, y). \tag{16}$$

Using Magma we find that E has zero torsion and rank 1 over $\mathbb{Q}$ and that, in fact,

$$E(\mathbb{Q}) = \mathbb{Z} \cdot (-1, 1).$$

We write $\mathrm{Pic}^0(E)$ for the group of rational degree 0 divisors on $E/\mathbb{Q}$ modulo linear equivalence and $\mathrm{Pic}^0(C)$ for the group of rational degree 0 divisors on $C/\mathbb{Q}$ modulo linear equivalence. We recall the standard isomorphism [Silverman 2009, Proposition III.3.4]

$$E(\mathbb{Q}) \cong \mathrm{Pic}^0(E), \quad P \mapsto [P - \infty], \tag{17}$$

where $[D]$ denotes the linear equivalence class of a divisor D. Thus

$$\mathrm{Pic}^0(E) = \mathbb{Z} \cdot \mathcal{Q}, \quad \mathcal{Q} = [(-1, 1) - \infty].$$

We also recall the standard isomorphism $J(\mathbb{Q}) \cong \mathrm{Pic}^0(C)$, and we will represent elements of the Mordell–Weil group $J(\mathbb{Q})$ as elements of $\mathrm{Pic}^0(C)$. Using Magma we find that J has good reduction away from the primes 2 and 3. Moreover, a straightforward calculation in Magma returns

$$J(\mathbb{F}_5) \cong \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/126\mathbb{Z}, \quad J(\mathbb{F}_{13}) \cong \mathbb{Z}/42997\mathbb{Z}.$$

As these two groups have coprime orders, we conclude that J has trivial torsion over $\mathbb{Q}$. Moreover, using Magma, we find that J has 2-Selmer rank 1 over $\mathbb{Q}$, so J has rank at most 1 over $\mathbb{Q}$. The morphism π in (16) has degree 3 and induces homomorphisms (see [Silverman 2009, Section II.3])

$$\pi_* : \mathrm{Pic}^0(C) \to \mathrm{Pic}^0(E), \quad \left[\sum a_i P_i\right] \mapsto \left[\sum a_i \pi(P_i)\right]$$

and

$$\pi^* : \mathrm{Pic}^0(E) \to \mathrm{Pic}^0(C), \quad \left[\sum b_j Q_j\right] \mapsto \left[\sum b_j \sum_{P \in \pi^{-1}(Q_j)} e_\pi(P) \cdot P\right],$$

where $e_\pi(P)$ denotes the ramification degree of π at P.

Let

$$\mathcal{P} = \pi^*(\mathcal{Q}) = [(1/\sqrt[3]{2}, 1) + (\omega/\sqrt[3]{2}, 1) + (\omega^2/\sqrt[3]{2}, 1) - 3\infty] \in \mathrm{Pic}^0(C) \cong J(\mathbb{Q}),$$

where ω is a primitive cube root of 1. The point $\mathcal{P}$ has infinite order on $J(\mathbb{Q})$. Thus J has rank exactly 1 over $\mathbb{Q}$ and no torsion. Therefore $J(\mathbb{Q}) = \mathbb{Z} \cdot \mathcal{P}'$ for some $\mathcal{P}' \in J(\mathbb{Q}) = \mathrm{Pic}^0(C)$. Hence

$$\mathcal{P} = k\mathcal{P}',$$

where k is a nonzero integer. Applying π_* to both sides, we obtain

$$k\pi_*(\mathcal{P}') = \pi_*(\mathcal{P}) = 3\mathcal{Q}.$$

However, $\pi_*(\mathcal{P}') \in \mathrm{Pic}^0(E) = \mathbb{Z}\mathcal{Q}$, so

$$\pi_*(\mathcal{P}') = \ell \cdot \mathcal{Q}$$

for some $\ell \in \mathbb{Z}$. Hence $k\ell = 3$, so $k = \pm 1$ or ± 3. Using Magma we checked that the image of $\mathcal{P}$ under the composition

$$J(\mathbb{Q}) \to J(\mathbb{F}_5) \to J(\mathbb{F}_5)/3J(\mathbb{F}_5)$$

is nonzero. Thus $k \neq \pm 3$, so $k = \pm 1$; hence

$$J(\mathbb{Q}) = \mathrm{Pic}^0(C) = \mathbb{Z} \cdot \mathcal{P}.$$

Suppose $P \in C(L)$. Let $\tau : L \to L$ be the nontrivial automorphism. Then $[P + P^\tau - 2\infty] \in \mathrm{Pic}^0(C)$. Thus

$$[P + P^\tau - 2\infty] = n \cdot \mathcal{P} = n \cdot \pi^*(\mathcal{Q}) = \pi^*(n \cdot \mathcal{Q})$$

for some integer n. We claim that $n = 0$. Suppose otherwise; then $n \cdot \mathcal{Q} \in \mathrm{Pic}^0(E) \setminus \{0\}$ and by the isomorphism in (17) we have $n \cdot \mathcal{Q} = [Q - \infty]$, where $Q \in E(\mathbb{Q}) \setminus \{\mathcal{O}\}$. Write $Q = (a, b) \in E(\mathbb{Q})$ with $a, b \in \mathbb{Q}$. Then

$$[P + P^\tau - 2\infty] = \pi^*([(a, b) - \infty]) = [D - 3\infty],$$

where

$$D = P_1 + P_2 + P_3, \quad P_j = (-\omega^{j-1}\sqrt[3]{a/2}, b), \quad j = 1, 2, 3.$$

Hence

$$D \sim D', \quad D' = P + P^\tau + \infty,$$

where $\sim$ denotes linear equivalence on C. Write $|D|$ for the complete linear system of effective divisors of C linearly equivalent to D. Let $r(D) = \dim|D|$. Note that $D' \in |D|$ and $D' \neq D$; therefore $r(D) \geq 1$. By Riemann–Roch [Arbarello et al. 1985, p. 13],

$$r(D) - i(D) = \deg(D) - g = -1,$$

where $i(D) \geq 0$ is the so-called index of speciality of D and $g = 4$ is the genus of C. It follows that $i(D) > 0$ and therefore that D is a special divisor. By Clifford's theorem [Hartshorne 1977, Theorem IV.5.4],

$$r(D) \leq \tfrac{1}{2}\deg(D) = \tfrac{3}{2}.$$

Hence $r(D) = 1$. Thus the complete linear system $|D|$ is a g^1_3. As C is hyperelliptic, by [Arbarello et al. 1985, p. 13], $|D| = g^1_2 + p$, where p is a fixed base point of the linear system. In particular, every divisor in $|D|$ is the sum of p and two points interchanged by the hyperelliptic involution. We apply this to D itself. Thus two of the points P_1, P_2, P_3 are interchanged by the hyperelliptic involution. However, they all have the same y-coordinate b, so $b = 0$. But $(a, b) \in E(\mathbb{Q})$, so $a \in \mathbb{Q}$ and $a^3 = -2$, giving a contradiction. Hence $n = 0$, and so

$$P + P^\tau \sim 2\infty.$$

Thus P and P^τ are interchanged by the hyperelliptic involution. We recall that we want to show that $P = \infty$. Suppose otherwise. Then we can write $P = (c, d)$, where $c, d \in L$ and $c^\tau = c$, $d^\tau = -d$. Thus $c \in \mathbb{Q}$ and $d = e/\sqrt{3}$ with $e \in \mathbb{Q}$. Thus $P' = (c, e) \in C'(\mathbb{Q})$, where

$$C' : y^2 = 6(-4x^9 + 1).$$

Let J' be the Jacobian of C' and

$$E' : y^2 = 6(4x^3 + 1).$$

Using Magma, we find that $E'(\mathbb{Q}) = \mathbb{Z} \cdot \left(\frac{1}{2}, 3\right)$. Let $\mathcal{Q}' = \left[\left(\frac{1}{2}, 3\right) - \infty\right] \in \mathrm{Pic}^0(E')$, so $\mathrm{Pic}^0(E') = \mathbb{Z} \cdot \mathcal{Q}$. Let

$$\pi' : C' \to E', \quad (x, y) \mapsto (-x^3, y).$$

Using Magma, we find that J' has trivial torsion and 2-Selmer rank 1, and, following the same steps as before, we show that $J'(\mathbb{Q}) = \mathrm{Pic}^0(C) = \mathbb{Z} \cdot \mathcal{P}'$, where $\mathcal{P}' = (\pi')^*(\mathcal{Q})$. Now $[P' - \infty]$ equals $n\mathcal{P}'$, where n is an integer, and must be nonzero as $P' \neq \infty$. Let $(f, g) = n \cdot \left(\frac{1}{2}, 3\right) \in E'(\mathbb{Q}) \setminus \{\mathcal{O}\}$. As before, we find that

$$P' + 2\infty \sim P'_1 + P'_2 + P'_3, \quad P'_j = (-\omega^{j-1} \cdot \sqrt[3]{f}, g).$$

Continuing as before, it follows that $g = 0$, so $f^3 = -\frac{1}{4}$, contradicting $f \in \mathbb{Q}$. We can thus conclude that if $P \in C(L)$ then $P = \infty$. This completes the proof of Lemma 6.2 and therefore Theorem 6.1. $\square$

6.2. $n = 6$. We show that a K-point on the Fermat curve of degree 6 induces a K-point P on a certain hyperelliptic curve C. Let E be the elliptic curve obtained by taking the quotient of C by a certain automorphism of C. We find that $E(K) = E(\mathbb{Q}) = \mathbb{Z}$ and use this to show that P is defined over a quadratic subfield of K. This leads to the search of $\mathbb{Q}$-rational points on the twists of C over the quadratic subfields of K.

Theorem 6.3. *There are no nontrivial solutions to (1) over K for $n = 6$.*

Proof. We find it convenient to let

$$F_6 : x^6 + y^6 = z^6.$$

That is, F_6 is the Fermat curve of degree 6. We will prove that

$$F_6(K) = \{(0 : -1 : 1), (-1 : 0 : 1), (0 : 1 : 1), (1 : 0 : 1)\},$$

i.e., $F_6(K)$ consists only of trivial solutions. Suppose $(\alpha : \beta : \gamma) \in F_6(K)$ is a nontrivial solution. We can assume without loss of generality that α, β, γ are integral and coprime. Similar to the proof of Theorem 6.1, observe

$$\gamma^{12} - (\alpha^6 - \beta^6)^2 = (\alpha^6 + \beta^6)^2 - (\alpha^6 - \beta^6)^2 = 4(\alpha\beta)^6.$$

Let

$$a = \frac{\alpha\beta}{\gamma^2}, \quad b = \frac{\alpha^6 - \beta^6}{\gamma^6}.$$

Then $P = (a, b) \in C(K)$, where

$$C : y^2 = -4x^6 + 1.$$

Let

$$E : y^2 = x^3 - 4.$$

This is the elliptic curve with Cremona label `432b1`. Let

$$\pi : C \to E, \quad (x, y) \mapsto \left(\frac{1}{x^2}, \frac{y}{x^3}\right), \quad (0, \pm 1) \mapsto 0_E.$$

We checked using Magma that E has rank 1 over K (and $\mathbb{Q}$) and that

$$E(K) = E(\mathbb{Q}) \cong \mathbb{Z}.$$

Since $\pi(P) \in E(\mathbb{Q})$, it follows that $a^2 \in \mathbb{Q}$ and hence $b^2 \in \mathbb{Q}$. If $a = 0$ then it's clear that $(\alpha : \beta : \gamma)$ is a trivial solution. Observe that a and b are necessarily defined over the same quadratic subfield of K since

$$\frac{b}{a} \in \mathbb{Q}.$$

Either $a \in \mathbb{Q}$ and hence $b \in \mathbb{Q}$, or

$$a = \frac{a'}{\sqrt{d}}, \quad b = \frac{b'}{\sqrt{d}}, \qquad \text{for } d \in \{2, 3, 6\}, \quad a', b' \in \mathbb{Q}.$$

If $a, b \in \mathbb{Q}$ then $P \in C(\mathbb{Q})$. The Jacobian of C has rank 1 over $\mathbb{Q}$. Using the Chabauty implementation in Magma, we find that

$$C(\mathbb{Q}) = \{(0, \pm 1)\},$$

and it immediately follows that $(\alpha : \beta : \gamma)$ is a trivial solution. Thus, $(a', b'd) \in C_d(\mathbb{Q})$ where

$$C_d : y^2 = -4x^6 + d^3,$$

where $d \in \{2, 3, 6\}$. Suppose $d = 3$ or 6. We checked using Magma that there are no points on C_d defined over $\mathbb{Q}_2$. Thus $C_3(\mathbb{Q}) = C_6(\mathbb{Q}) = \varnothing$. It remains to determine $C_2(\mathbb{Q})$. We will work with the model

$$C_2 : y^2 = -x^6 + 2. \tag{18}$$

We note that the curve C_2 has genus 2 and the rank of the Jacobian of C_2 over $\mathbb{Q}$ is 2. Thus, we are unable to determine $C_2(\mathbb{Q})$ using Chabauty. Instead, we used the elliptic curve Chabauty method of [Bruin 2003] to do so as we now demonstrate.

Let $\theta = \sqrt[6]{2}$, and note that θ is a root of the hyperelliptic polynomial for C_2 given in (18). Let $L = \mathbb{Q}(\theta)$. Consider the map

$$\varphi : C_2(\mathbb{Q}) \to L^*/(L^*)^2, \quad (x, y) \to (x - \theta) \cdot (L^*)^2.$$

The method of two-cover descent, due to Bruin and Stoll [2009], uses sieving information to determine a small finite set containing the image of φ. This is implemented in Magma, and applying it we find that

$$\varphi(C_2(\mathbb{Q})) \subseteq \{(1 + \theta) \cdot (L^*)^2, (1 - \theta) \cdot (L^*)^2\}.$$

Thus, for a rational point $(x, y) \in C_2(\mathbb{Q})$, we have

$$x - \theta = (1 \pm \theta)\beta^2 \tag{19}$$

with $\beta \in L^*$. Now let $F = \mathbb{Q}(\sqrt[3]{2})$, and note that $x^2 - \sqrt[3]{2} = \mathrm{Norm}_{L/F}(x - \theta)$. Observe that

$$\mathrm{Norm}_{L/F}(1 \pm \theta) = (1 - \theta)(1 + \theta) = 1 - \sqrt[3]{2}.$$

Taking norms in (19) gives

$$x^2 - \sqrt[3]{2} = (1 - \sqrt[3]{2})w^2, \quad w = \mathrm{Norm}_{L/F}(\beta) \in F^*.$$

Note the factorisation

$$C_2 : y^2 = -x^6 + 2 = -(x^2 - \sqrt[3]{2})(x^4 + \sqrt[3]{2}x^2 + \sqrt[3]{2}^2).$$

Thus, for $(x, y) \in C_2(\mathbb{Q})$, we have

$$x^4 + \sqrt[3]{2}x^2 + \sqrt[3]{2}^2 = \frac{-y^2}{x^2 - \sqrt[3]{2}} = \frac{-1}{(1 - \sqrt[3]{2})} \cdot \frac{y^2}{w^2}.$$

Let $\epsilon = -1/(1 - \sqrt[3]{2}) = 1 + \sqrt[3]{2} + \sqrt[3]{2}^2 \in F^*$ and $z = y/w \in F^*$. Then, for $(x, y) \in C_2(\mathbb{Q})$, we have

$$x^4 + \sqrt[3]{2}x^2 + \sqrt[3]{2}^2 = \epsilon z^2. \tag{20}$$

Let

$$X = \epsilon x^2 \quad \text{and} \quad Y = \epsilon^2 xz. \tag{21}$$

Then $(X, Y) \in E_2(F)$, where E_2/F is the elliptic curve

$$E_2 : Y^2 = X^3 + \epsilon\sqrt[3]{2}X^2 + \epsilon^2\sqrt[3]{2}^2 X.$$

Using Magma, we found that the Mordell–Weil group is given by

$$E_2(F) = (\mathbb{Z}/2\mathbb{Z}) \cdot (0, 0) \oplus \mathbb{Z} \cdot (1 + \sqrt[3]{2} + \sqrt[3]{2}^2, 5 + 4\sqrt[3]{2} + 3\sqrt[3]{2}^2).$$

We are interested in points $(X, Y) \in E_2(F)$ which satisfy (21), where $(x, y) \in C_2(\mathbb{Q})$. In particular, to determine $C_2(\mathbb{Q})$, it is enough to find all points $Q = (X, Y) \in E_2(F)$ such that $f(Q) \in \mathbb{Q}$, where $f(X, Y) = X/\epsilon$. The elliptic curve Chabauty method of [Bruin 2003] is one that can sometimes be used to provably determine all F-points Q on an elliptic curve E defined over a number field F such that $f(Q) \in \mathbb{Q}$ for a given nonconstant function $f \in F(E)$, provided the degree $[F : \mathbb{Q}]$ exceeds the rank of E over F. In our situation, the degree is $[F : \mathbb{Q}] = 3$ and the rank of E over F is 1. We applied the implementation of the elliptic curve Chabauty method available in Magma to our E_2/F and f. This succeeded in showing that the only $(X, Y) \in E_2(F)$ with $X/\varepsilon \in \mathbb{Q}$ are

$$(X, Y) = (0, 0), \quad (1 + \sqrt[3]{2} + \sqrt[3]{2}^2, 5 + 4\sqrt[3]{2} + 3\sqrt[3]{2}^2), \quad (1 + \sqrt[3]{2} + \sqrt[3]{2}^2, -5 - 4\sqrt[3]{2} - 3\sqrt[3]{2}^2).$$

Thus $X = 0$ or ϵ, and hence if $(x, y) \in C_2(\mathbb{Q})$ then $x = 0$ or ± 1. It immediately follows that

$$C_2(\mathbb{Q}) = \{(\pm 1, \pm 1)\}.$$

Thus, $(a', b') \in \{(\pm 1, \pm 1)\}$ and if $P = (a, b) \in C(K)$ then $P \in \{(\pm 1/\sqrt{2}, \pm 1/\sqrt{2})\}$. Recall that

$$b = \frac{\alpha^6 - \beta^6}{\gamma^6},$$

where $(\alpha : \beta : \gamma) \in F_6(K)$. It immediately follows that $\frac{1}{2}(b + 1)$ is a square in K. For each b, we check using Magma that $\frac{1}{2}(b + 1)$ is not a square in K. We have reached a contradiction. □

6.3. $n = 4$. Quadratic points on the Fermat quartic have been studied by Aigner [1934], Faddeev [1960] and Mordell [1968]. Mordell starts with the knowledge that there are no nontrivial points on the Fermat quartic over $\mathbb{Q}$ and studies points over all quadratic fields. We generalise his method, observing that we can also classify points over quadratic extensions of certain quadratic fields. More precisely, if L is any field for which there are no points on the Fermat quartic, and if the two elliptic curves with Cremona labels `32a1` and `64a1` have rank 0 over L, then we give a procedure to write down all the points on the Fermat quartic over quadratic extensions of L.

In an earlier version of this paper, we conjectured that there are no points on the Fermat quartic over any real biquadratic field. We thank Pedro José Cazorla Garcia for pointing out to us that the point $(\sqrt{3}, 2, \sqrt{5})$ lies on the Fermat quartic over $\mathbb{Q}(\sqrt{3}, \sqrt{5})$.

After the completion of this work, we were made aware that Ishitsuka, Ito and Ohshita [Ishitsuka et al. 2020, Theorem 7.3] have previously determined all points on the Fermat quartic lying in a quadratic extension of $\mathbb{Q}(\zeta_8)$. We thank the authors for making us aware of this. Since $\mathbb{Q}(\sqrt{2})$ is contained in $\mathbb{Q}(\zeta_8)$, this is indeed stronger than the statement of Theorem 6.4. We note that the authors of [Ishitsuka et al. 2020] study the Jacobian of the Fermat quartic over $\mathbb{Q}(\zeta_8)$ and that the proof of Theorem 6.4, extending work of Mordell [1968], makes use of a different strategy.

Theorem 6.4. *The points on the Fermat quartic lying in quadratic extensions of* $\mathbb{Q}(\sqrt{2})$ *lie in one of* $\mathbb{Q}(\sqrt{2},i)$, $\mathbb{Q}(\sqrt{2},\sqrt{-7})$, $\mathbb{Q}(\sqrt[4]{2})$ *or* $\mathbb{Q}(\sqrt[4]{2}i)$.

Proof. Let $L=\mathbb{Q}(\sqrt{2})$, and let K be a quadratic extension of L. We will determine all points on the Fermat quartic $F_4: x^4+y^4=1$ in K, using the same strategy as Mordell (where, of course, Mordell works with a quadratic extension K of $L=\mathbb{Q}$). Let $t=(1-x^2)/y^2$, so that $x^2+ty^2=1$. This gives a parametrisation

$$x^2=\frac{1-t^2}{1+t^2},\quad y^2=\frac{2t}{1+t^2}.$$

We point out that if $x, y\in K$ then $x^2, y^2\in K$ and therefore so is t.

Suppose first that $t\in L$. Then $x^2, y^2\in L$. In order for x and y to lie in the same quadratic extension K of L, either $x\in L$, $y\in L$ or $x/y\in L$. This means that one of

$$\frac{1-t^2}{1+t^2},\quad \frac{2t}{1+t^2}\quad\text{or}\quad \frac{2t}{1-t^2}$$

is a square in L. Equivalently, $(1-t^2)(1+t^2)$, $2t(1+t^2)$ or $2t(1-t^2)$ is a square in L. These correspond to L-rational points of one of the curves

$$u^2=(1-t^2)(1+t^2),\quad u^2=2t(1+t^2),\quad u^2=2t(1-t^2).$$

Both of the first two possibilities are isomorphic to $E_1: y^2=x^3+4x$ (the elliptic curve with Cremona label `32a1`) via the maps

$$(t,u)\mapsto\left(\frac{2t+2}{1-t},\frac{u}{(1-t)^2}\right)\quad\text{and}\quad (t,u)\mapsto(2t,2u),$$

respectively, and the third to $E_2: y^2=x^3-4x$ (the elliptic curve with Cremona label `64a1`) via the map $(t,u)\mapsto(-2t,2u)$. We checked, using Magma, that E_1 and E_2 have rank 0 over L. We first consider E_1 and find

$$E_1(L)=E_1(\mathbb{Q})=\{\mathcal{O},(0,0),(2,\pm4)\}.$$

We find that these points correspond on the first curve to $t=\pm1$ and $t=0$, and on the second to $t=0$, $t=1$ and $t=\infty$. These values of t correspond to

$$(x^2,y^2)=\{(1,0),(-1,0),(0,1),(0,-1)\},$$

corresponding to points on F_4 defined over $\mathbb{Q}$ or $\mathbb{Q}(i)$. Similarly,

$$E_2(L) = \{\mathcal{O},\ (0,0),\ (\pm 2, 0)\} \cup \{(2+2\sqrt{2},\ \pm(4+4\sqrt{2}),\ (2-2\sqrt{2},\ \pm(4-4\sqrt{2})\},$$

and the rational points correspond to $t = \pm 1$ and $t = 0$, and the point at infinity to $t = \infty$, as before. The points in $E(L) \setminus E(\mathbb{Q})$ correspond to $t = -1 \pm \sqrt{2}$, and these give

$$(x^2, y^2) \in \left\{ \left(\frac{1}{\sqrt{2}}, \frac{1}{\sqrt{2}} \right), \left(-\frac{1}{\sqrt{2}}, -\frac{1}{\sqrt{2}} \right) \right\},$$

corresponding to points on F_4 defined over $\mathbb{Q}(\sqrt[4]{2})$ or $\mathbb{Q}(\sqrt[4]{2}i)$.

We now suppose $t \in K,\ t \notin L$. We write $F(t) = t^2 + \beta t + \gamma$ for the minimal polynomial of t over L, so $\beta, \gamma \in L$. We let $A = (1+t^2)xy$ and $B = (1+t^2)y$, so that

$$A^2 = 2t(1-t^2), \quad B^2 = 2t(1+t^2).$$

Since $A^2, B^2 \in K$ and $K = L(t)$, we can write

$$A = \lambda + \mu t, \quad B = \lambda' + \mu' t, \quad \lambda, \mu, \lambda', \mu' \in L.$$

Comparing the two expressions for A yields

$$(\lambda + \mu t)^2 = 2t(1-t^2).$$

In particular, the equation

$$(\lambda + \mu z)^2 - 2z(1-z^2) = 0$$

has a root $z = t$. As the equation is defined over L, we see the left-hand side is divisible by the minimal polynomial $F(z)$, and, as this is a cubic, we have

$$(\lambda + \mu z)^2 - 2z(1-z^2) = F(z)(\rho + \sigma z), \tag{M1}$$

a factorisation over L (so $\rho, \sigma \in L$). Then $z = -\rho/\sigma$ is a solution to the left-hand side of (M1) defined over L. In particular, we have a solution with $z \in L$ to

$$Y^2 = 2z(1-z^2) = -2z^3 + 2z,$$

where $Y = \lambda + \mu z \in L$. Thus we get an L-point on the elliptic curve $Y^2 = -2X^3 + 2X$, which is isomorphic to the elliptic curve E_2, and the points in $E_2(L)$ correspond to $z = \pm 1,\ z = 0$ and $z = -1 \pm \sqrt{2}$. In exactly the same way, looking at B^2, we will get a solution over L to

$$(\lambda' + \mu' z)^2 - 2z(1+z^2) = F(z)(\rho' + \sigma' z), \tag{M2}$$

and therefore a solution over L to $Y^2 = 2z(1+z^2)$, which is isomorphic to E_1. The points in $E_2(L)$ correspond to $z = 0$ and $z = 1$.

We will now consider all these cases, as in Mordell. We write (z_1, z_2) for the situation where (M1) is solved by z_1 and (M2) is solved by z_2. We remark that these calculations are quite involved, and we therefore omit some details.

Case 1. $(-1, 1)$ This is Mordell's case (VI). If $z_1 = -1$ is a root of the left-hand side of (M1) then $\lambda + \mu = 0$ and, since -1 must then be a root of the right-hand side of (M1), it follows that $\rho + \sigma = 0$. Similarly, if $z_1 = 1$ is a root of the left-hand side of (M2) then $\lambda' + \mu' = 2$, $\rho' + \sigma' = 0$. Equation (M1) is

$$\lambda^2(1+z) - 2z(1-z) = \rho F(z)$$

(after dividing by $1 - z$). We can rewrite the left-hand side of (M2) as $(2 - \mu' + \mu' z)^2 - 2z - 2z^3 = \rho'(1-z)F(z)$. Thus, after dividing by $1 - z$, we get

$$\text{(M2)} : 2(z^2 + z + 2) - 4\mu' + \mu'^2(1-z) = \rho' F(z).$$

Both (M1) and (M2) have the same coefficient of z^2, so $\rho = \rho'$. Comparing constant terms and z terms:

$$\lambda^2 = (2-\mu')^2, \quad \lambda^2 - 2 = 2 - \mu'^2,$$

so either $(\lambda, \mu') = (0, 2)$ or $(\lambda, \mu') = (\pm 2, 0)$. In the first case, (M1) becomes $-2z(1-z) = \rho \cdot F(z)$, but this contradicts the irreducibility of $F(z)$. In the second case,

$$\text{(M1)} : \rho F(z) = 4(1+z) - 2z(1-z) = 2(z^2 + z + 2),$$

so $F(z) = z^2 + z + 2$. Thus, $t = \frac{1}{2}(-1 \pm \sqrt{-7})$ and $K = L(\sqrt{-7})$.

Case 2. $(-1, 0)$ This is Mordell's case (III). In order for $z = -1$ to be a root of the left-hand side of (M1), we need $(\lambda - \mu)^2 = 0$. So $\lambda - \mu = 0$. Similarly, for $z = 0$ to be a root of the left-hand side of (M2), we need $\lambda' = 0$. Then for the left-hand side of (M1) to have -1 as a root, the same will be true of the right-hand side, so $\rho - \sigma = 0$. Equation (M1) is then divisible by $(1 + z)$, and dividing through, we get

$$\text{(M1)} : \lambda^2(1+z) - 2z(1-z) = \rho \cdot F(z).$$

We rewrite this as

$$\text{(M1)} : 2z^2 + (\lambda^2 - 2)z + \lambda^2 = \rho \cdot F(z).$$

In order for $z = 0$ to be a root of the left-hand side of (M2), it must be that $\lambda' = 0$, and thus

$$\text{(M2)} : -2z^2 + \mu'^2 z - 2 = \sigma' F(z).$$

The right-hand sides of (M1) and (M2) differ by a constant, and upon comparing the z^2 coefficients on the left-hand sides, we see that they differ by a factor of -1. Then comparing the constant term, we get $\lambda^2 = 2$. Thus $\lambda = \mu = \pm\sqrt{2}$. The coefficient of z in the first equation is $\lambda^2 - 2$, and the coefficient of z in the second is μ'^2, so $\mu' = 0$. Then $Y = \lambda' + \mu' t = 0$. But $Y^2 = 2t(1 + t^2)$, so this means that $t = 0$, contradicting $t \notin L$, or $(1 + t^2)$ in which case $t = i$ and $K = L(i)$.

For the remaining pairs (z_1, z_2), in each case, after performing a similar analysis, we reach a contradiction to the fact $\lambda, \mu, \lambda', \mu' \in L$, and thus no solutions are found in these cases. □

This completes the proof of Theorem 1.1.

7. More general real biquadratic fields

We give examples of obstacles that arise in generalising the proof of Theorem 1.1 to more general real biquadratic fields. As in the proof of Theorem 1.1, we apply level lowering (Theorem 2.1) to the Frey curve (2) for $p \geq 17$ and $E_{13,\epsilon}$ for $p = 13$.

7.1. $K = \mathbb{Q}(\sqrt{2}, \sqrt{5})$. In order to apply level lowering (Theorem 2.1), one needs to demonstrate the modularity of the Frey curve over K. It has not yet been proven that elliptic curves over totally real quartic fields containing $\sqrt{5}$ are modular; see [Box 2022, Section 7.1] for a discussion concerning this problem. We remark however that establishing the modularity of the Frey curve over this particular field K may be possible through the use of [Freitas et al. 2015, Theorem 7].

7.2. $K = \mathbb{Q}(\sqrt{2}, \sqrt{7})$. Write $\mathcal{O}_K$ for the ring of integers of K. A straightforward computation in Magma returns that K has class number 1 and $2\mathcal{O}_K = \mathfrak{P}^4$. A straightforward generalisation of Lemmas 3.1, 3.2 and 3.3 returns that the lowered level is $\mathfrak{P}^t$, where $t = 1, 5, 8$ or 16. In particular, the dimension of Hilbert newforms of parallel weight 2 and level $\mathfrak{P}^{16}$ is 40960, making the elimination step currently computationally infeasible in this case.

7.3. $K = \mathbb{Q}(\sqrt{2}, \sqrt{11})$. Write $\mathcal{O}_K$ for the ring of integers of K. A straightforward computation in Magma returns that K has class number 1 and $2\mathcal{O}_K = \mathfrak{P}^4$. By a direct generalisation of the techniques outlined in Section 4, it is straightforward to see that $\bar{\rho}_{E,p}$ is irreducible for $p \geq 13$.

A straightforward generalisation of Lemmas 3.1, 3.2 and 3.3 returns that the lowered level is $\mathfrak{P}^t$, where $t = 1, 4$ or 5. As is true for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, there are no Hilbert newforms of parallel weight 2 and level $\mathfrak{P}$ over K. There are 44 Hilbert newforms of parallel weight 2 and level $\mathfrak{P}^4$ and 76 Hilbert newforms of parallel weight 2 and level $\mathfrak{P}^5$ over K. In order to get a contradiction, we make use of the standard method of eliminating newforms given by the following lemma.

Lemma 7.1 [Freitas and Siksek 2015b, Lemma 7.1]. *Let K be a totally real field, and let $p \geq 5$ be a prime. Let E be an elliptic curve over K of conductor $\mathcal{N}$, and let $\mathfrak{f}$ be a newform of parallel weight 2 and level $\mathcal{N}_p$. Let t be a positive integer satisfying $t \mid \#E(K)_{\mathrm{tors}}$. Let $\mathfrak{q} \nmid t\mathcal{N}_p$ be a prime ideal of $\mathcal{O}_K$, and let*

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

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

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

We briefly explain how to apply Lemma 7.1. Namely let

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

where T is a small set of primes $\mathfrak{q} \nmid t\mathcal{N}_p$. Let $C_\mathfrak{f} = \mathrm{Norm}_{\mathbb{Q}_\mathfrak{f}/\mathbb{Q}}(B_\mathfrak{f})$. Then Lemma 7.1 asserts that $p \mid C_\mathfrak{f}$. We wrote a short program to implement Lemma 7.1 in Magma with $\mathcal{N}_p = \mathfrak{P}^4$ or $\mathfrak{P}^5$, with $t = 4$ and T

equal to the set of prime ideals $\mathfrak{q} \neq \mathfrak{P}$ of K with norm less than 90. From this implementation, we found that if $\bar{\rho}_{E,p} \sim \bar{\rho}_{\mathfrak{f},\varpi}$, where E is our Frey curve and $\mathfrak{f}$ is a newform of level $\mathcal{N}_p$, then $p = 2$ or 3.

We remark that the proofs of Theorems 6.1 and 6.3 do not readily generalise to K. In combination with the remarks made in Section 2, this leads to the following result.

Theorem 7.2. *Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{11})$. There are no nontrivial solutions to (1) over K for all primes $n \geq 5$.*

Acknowledgements

We would like to thank Samir Siksek for several useful and enlightening discussions, particularly with regard to the contents of Section 4 and the proof of Theorem 6.1. We would also like to thank Philippe Michaud-Jacobs, Jeremy Rouse and Michael Stoll for helpful correspondence, and Pedro José Cazorla Garcia for a careful reading of an earlier version of this paper. We would like to thank the authors, Yasuhiro Ishitsuka, Tetsushi Ito and Tatsuya Ohshita, of [Ishitsuka et al. 2020] for making us aware of their work determining all points on the Fermat quartic lying in a quadratic extension of $\mathbb{Q}(\zeta_8)$. We would like to thank the referees for their careful reading of the paper as well as the invaluable comments and suggestions they provided. Khawaja thanks the University of Sheffield for their financial support via a doctoral training partnership scholarship (ESPRC grant no EP/T517835/1).

References

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

[Arbarello et al. 1985] E. Arbarello, M. Cornalba, P. A. Griffiths, and J. Harris, *Geometry of algebraic curves, I*, Grundl. Math. Wissen. **267**, Springer, 1985. MR Zbl

[Box 2022] J. Box, "Elliptic curves over totally real quartic fields not containing $\sqrt{5}$ are modular", *Trans. Amer. Math. Soc.* **375**:5 (2022), 3129–3172. MR Zbl

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

[Bruin and Najman 2015] P. Bruin and F. Najman, "Hyperelliptic modular curves $X_0(n)$ and isogenies of elliptic curves over quadratic fields", *LMS J. Comput. Math.* **18**:1 (2015), 578–602. MR Zbl

[Bruin and Stoll 2009] N. Bruin and M. Stoll, "Two-cover descent on hyperelliptic curves", *Math. Comp.* **78**:268 (2009), 2347–2370. MR Zbl

[David 2011] A. David, "Caractère d'isogénie et critères d'irréductibilité", preprint, 2011. arXiv 1103.3892

[Derickx et al. 2020] M. Derickx, F. Najman, and S. Siksek, "Elliptic curves over totally real cubic fields are modular", *Algebra Number Theory* **14**:7 (2020), 1791–1800. MR Zbl

[Derickx et al. 2023] M. Derickx, S. Kamienny, W. Stein, and M. Stoll, "Torsion points on elliptic curves over number fields of small degree", *Algebra Number Theory* **17**:2 (2023), 267–308. MR Zbl

[Faddeev 1960] D. K. Faddeev, "Group of divisor classes on the curve defined by the equation $x^4 + y^4 = 1$", *Soviet Math. Dokl.* **1** (1960), 1149–1151. Zbl

[Freitas and Siksek 2015a] N. Freitas and S. Siksek, "The asymptotic Fermat's last theorem for five-sixths of real quadratic fields", *Compos. Math.* **151**:8 (2015), 1395–1415. MR Zbl

[Freitas and Siksek 2015b] N. Freitas and S. Siksek, "Fermat's last theorem over some small real quadratic fields", *Algebra Number Theory* **9**:4 (2015), 875–895. MR Zbl

[Freitas et al. 2015] N. Freitas, B. V. Le Hung, and S. Siksek, "Elliptic curves over real quadratic fields are modular", *Invent. Math.* **201**:1 (2015), 159–206. MR Zbl

[Freitas et al. 2020] N. Freitas, A. Kraus, and S. Siksek, "Class field theory, Diophantine analysis and the asymptotic Fermat's last theorem", *Adv. Math.* **363** (2020), art. id. 106964. MR Zbl

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

[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 Zbl

[Hartshorne 1977] R. Hartshorne, *Algebraic geometry*, Grad. Texts in Math. **52**, Springer, 1977. MR Zbl

[Ishitsuka et al. 2020] Y. Ishitsuka, T. Ito, and T. Ohshita, "Explicit calculation of the mod 4 Galois representation associated with the Fermat quartic", *Int. J. Number Theory* **16**:4 (2020), 881–905. MR Zbl

[Jarvis 1999a] F. Jarvis, "Level lowering for modular mod l representations over totally real fields", *Math. Ann.* **313**:1 (1999), 141–160. MR Zbl

[Jarvis 1999b] F. Jarvis, "Mazur's principle for totally real fields of odd degree", *Compos. Math.* **116**:1 (1999), 39–79. MR Zbl

[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 Zbl

[Katz 1981] N. M. Katz, "Galois properties of torsion points on abelian varieties", *Invent. Math.* **62**:3 (1981), 481–502. MR Zbl

[Klassen and Tzermias 1997] M. Klassen and P. Tzermias, "Algebraic points of low degree on the Fermat quintic", *Acta Arith.* **82**:4 (1997), 393–401. MR Zbl

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

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

[Kraus 2018] A. Kraus, "Quartic points on the Fermat quintic", *Ann. Math. Blaise Pascal* **25**:1 (2018), 199–205. MR Zbl

[Kraus 2019] A. Kraus, "Le théorème de Fermat sur certains corps de nombres totalement réels", *Algebra Number Theory* **13**:2 (2019), 301–332. MR Zbl

[Michaud-Jacobs 2022] P. Michaud-Jacobs, "Fermat's last theorem and modular curves over real quadratic fields", *Acta Arith.* **203**:4 (2022), 319–351. MR Zbl

[Mordell 1968] L. J. Mordell, "The Diophantine equation $x^4 + y^4 = 1$ in algebraic number fields", *Acta Arith.* **14** (1968), 347–355. MR Zbl

[Ozman and Siksek 2019] E. Ozman and S. Siksek, "Quadratic points on modular curves", *Math. Comp.* **88**:319 (2019), 2461–2484. MR Zbl

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

[Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Grad. Texts in Math. **151**, Springer, 1994. MR Zbl

[Silverman 2009] J. H. Silverman, *The arithmetic of elliptic curves*, 2nd ed., Grad. Texts in Math. **106**, Springer, 2009. MR Zbl

[Tzermias 1998] P. Tzermias, "Algebraic points of low degree on the Fermat curve of degree seven", *Manuscripta Math.* **97**:4 (1998), 483–488. MR Zbl

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

Communicated by Bjorn Poonen
Received 2022-12-26 Revised 2024-03-14 Accepted 2024-04-29

maleehakhawaja@hotmail.com *School of Mathematics and Statistics, University of Sheffield, Sheffield, United Kingdom*

a.f.jarvis@sheffield.ac.uk *School of Mathematics and Statistics, University of Sheffield, Sheffield, United Kingdom*

Algebra & Number Theory

msp.org/ant

See inside back cover or msp.org/ant for submission instructions.

The subscription price for 2025 is US $565/year for the electronic version, and $820/year (+$70, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscriber address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online.

ANT peer review and production are managed by EditFLOW® from MSP.

PUBLISHED BY

mathematical sciences publishers

nonprofit scientific publishing

http://msp.org/

Algebra & Number Theory

Volume 19 No. 3 2025