Canad. J. Math. Vol. **76** (1), 2024 pp. 18–38
http://dx.doi.org/10.4153/S0008414X22000633

Fermat's Last Theorem over $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{17})$

Imin Chen, Aisosa Efemwonkieke, and David Sun

Abstract. We prove Fermat's Last Theorem over $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{17})$ for prime exponents $p \geq 5$ in certain congruence classes modulo 48 by using a combination of the modular method and Brauer–Manin obstructions explicitly given by quadratic reciprocity constraints. The reciprocity constraint used to treat the case of $\mathbb{Q}(\sqrt{5})$ is a generalization to a real quadratic base field of the one used by Chen and Siksek. For the case of $\mathbb{Q}(\sqrt{17})$, this is insufficient, and we generalize a reciprocity constraint of Bennett, Chen, Dahmen, and Yazdani using Hilbert symbols from the rational field to certain real quadratic fields.

1 Introduction

The celebrated Fermat's Last Theorem was proven in [19, 22] by Taylor-Wiles and Wiles. Ever since then, it has been natural to attempt to use the same methods to tackle more general forms of the Fermat equation, particularly the still unresolved Beal conjecture [16].

Another direction has been to study the usual Fermat equation over number fields. For instance, Freitas and Siksek considered, in [10, 11], Fermat's Last Theorem over real quadratic fields. In particular, it is currently known that Fermat's Last Theorem is asymptotically true for $K = \mathbb{Q}(\sqrt{d})$ where $2 \leq d \leq 23$ square-free and $d \neq 5, 17$ and also on a subset of d which has density $5/6$ among square-free $d > 0$. For a given number field K, asymptotically true means that Fermat's Last Theorem is true for sufficiently large exponents. In a different vein, [6–8] establish more general criteria for proving the asymptotic Fermat's Last Theorem and apply these to a number of infinite families of number fields.

In this paper, we study Fermat's Last Theorem over K for $d = 5$ and $d = 17$, the first two notable cases where asymptotic results are not yet proved. These cases present difficulties within the framework of [11] due to a large number of solutions to the S-unit equation over K where S is the set of primes of K above 2. We circumvent these obstructions by showing that the reciprocity constraints in [1, 4] generalize to a real quadratic base field, allowing a complete resolution in certain congruence classes of

Received by the editors April 13, 2022; revised October 6, 2022; accepted November 7, 2022.
Published online on Cambridge Core November 21, 2022.
This work was supported by an NSERC Discovery Grant (I.C.) and NSERC USRA (A.E.).
AMS subject classification: **11D41, 11F80, 11F03.**
Keywords: Fermat equation over quadratic fields, Galois representations, Hilbert modular forms.

prime exponents p. In addition to [1, 4], we also mention [5, 14] where reciprocity constraints have been used to solve generalized Fermat equations.

Let K be a quadratic field, and let $\mathcal{O}_K$ be its ring of integers. Assume that K has class number one. We say that a solution (a,b,c) over $\mathcal{O}_K$, i.e., where $a,b,c \in \mathcal{O}_K$, to

$$x^p + y^p + z^p = 0 \tag{1.1}$$

is primitive if the ideal $(a,b,c) = \mathcal{O}_K$ and nontrivial if $abc \neq 0$.

Under the assumption that K has class number one, we note that any nonzero solution $(a,b,c) \in K^3$ to (1.1) can be scaled to a primitive solution over $\mathcal{O}_K$, and henceforth, when we refer to solutions over K, we mean that the solutions have been scaled to a primitive solution over $\mathcal{O}_K$. In the more general case that K does not have class number one, we refer the reader to [11].

Theorem 1.2 *There are no nontrivial primitive solutions over* $\mathbb{Q}(\sqrt{5})$ *to*

$$x^p + y^p + z^p = 0$$

for prime $p \geq 5$ *if* p *satisfies one of the following:*

(1) $p \equiv 5,7 \pmod 8$, *or*
(2) $p \equiv 19,41 \pmod{48}$.

The above theorem shows that Fermat's Last Theorem over $\mathbb{Q}(\sqrt{5})$ is true for a set of prime exponents with Dirichlet density $5/8$. In [15], Theorem 1.2 is proved for $5 \leq p < 10^7$, where we note that the small exponents in this range rely on [13]. The method used in [15] is to fix a prime exponent $p \geq 11$ and use an auxiliary prime $q = pk + 1$ with $k < p - 2$ and q split in K, and apply the modular method together with the local condition mod q on solutions to (1.1). In practice, it appears that most primes q of this form succeed in giving a proof for the fixed exponent p, but there is no currently known way to prove results of this type in general.

Theorem 1.3 *There are no nontrivial primitive solutions over* $\mathbb{Q}(\sqrt{17})$ *to*

$$x^p + y^p + z^p = 0$$

for prime $p \geq 5$ *if* p *satisfies one of the following:*

(1) $p \equiv 5,7 \pmod 8$, *or*
(2) $p \equiv 17 \pmod{24}$.

Remark 1.4 In [11], Theorem 1.3 is established for $p \equiv 3,5 \pmod 8$ using the symplectic method [12]. The above theorem and the result in [11] imply the corollary below, which shows that Fermat's Last Theorem over $K = \mathbb{Q}(\sqrt{17})$ is true for a set of prime exponents with Dirichlet density $7/8$.

Corollary 1.5 *There are no nontrivial primitive solutions over* $\mathbb{Q}(\sqrt{17})$ *to*

$$x^p + y^p + z^p = 0$$

for prime $p \geq 5$ *if* $p \not\equiv 1 \pmod{24}$.

The proofs of the above theorems are based on the modular method, which attaches a Frey elliptic curve E_0 defined over K to a putative nontrivial primitive solution.

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

One then considers the representation $\overline{\rho}_{E_0,p} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ on the p-torsion points of E_0, which, by virtue of being a Frey elliptic curve, has Artin conductor bounded independently of the solution and prime exponent p.

Using modularity and level lowering, one deduces that $\overline{\rho}_{E_0,p} \cong \overline{\rho}_{f,p}$, where $\overline{\rho}_{f,p} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ is the residual Galois representation attached to a Hilbert newform at the possible Artin conductors. For the cases considered in this paper, f has a coefficient field equal to the field of rational numbers.

Unlike the original Fermat's Last Theorem, the space of newforms with level equal to the possible Artin conductor is typically not zero. Hence, to achieve a contradiction, one needs additional methods. To accomplish this, we combine information from reciprocity constraints such as in [4] to obtain a contradiction for prime exponents in certain congruence classes. This succeeds for $\mathbb{Q}(\sqrt{5})$; however, the reciprocity constraint used in [4] is not strong enough to treat $\mathbb{Q}(\sqrt{17})$.

Using the approach in [1], valid over $\mathbb{Q}$, we prove a stronger reciprocity constraint, valid over certain real quadratic base fields, in terms of Hilbert symbols. This has an added advantage that the reciprocity law needed is simply the well-known reciprocity law for Hilbert symbols over a number field [21].

The programs and output transcripts for the computations needed in this paper are described and posted at [3].

2 Proof of Theorem 1.2

Let $K = \mathbb{Q}(\sqrt{5})$ and note that $\mathcal{O}_K$ has unique factorization. Suppose (a, b, c) is a nontrivial primitive solution over $\mathcal{O}_K$ to (1.1) for a prime $p \geq 5$. Normalize the solution (a, b, c) as in [15].

Let E_0 denote the Frey elliptic curve over K:

$$E_0 : Y^2 = X(X - a^p)(X + b^p). \tag{2.1}$$

Let $\mathfrak{P}$ be the unique prime of K above 2.

Proposition 2.2 *Assuming $p \geq 5$, the conductor of E_0 over K is given by*

$$N(E_0) = \mathfrak{P}^t \prod_{\mathfrak{q} \mid abc, \mathfrak{q} \neq \mathfrak{P}} \mathfrak{q},$$

where $t \in \{1, 2, 3\}$. Moreover, $t = 1$ if $2 \mid abc$ and $t \in \{2, 3\}$ if $2 \nmid abc$.

Proof See [15, Lemme 3]. ■

Proposition 2.3 *The representation $\overline{\rho}_{E_0,p} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ is irreducible if $p \geq 11$.*

Proof See [15, Proposition, p. 7]. ■

Proposition 2.4 *There is a Hilbert newform f of trivial character, parallel weight 2, and level $\mathfrak{P}^t$ such that $\overline{\rho}_{E_0,p} \simeq \overline{\rho}_{f,\mathfrak{p}}$.*

Proof The elliptic curve E_0 over K is modular by [9]. Using [10, Theorem 7], we obtain the desired statement. ■

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

The space of Hilbert newforms of trivial character, parallel weight 2, and level $\mathfrak{P}, \mathfrak{P}^2$ is zero, so these cases do not occur. In particular, we may now assume that

$$2 \nmid abc \tag{2.5}$$

and $t = 3$.

There is a unique Hilbert newform f of trivial character, parallel weight 2, and level $\mathfrak{P}^3$ which corresponds to an elliptic curve E over K. Hence, we have that

$$\overline{\rho}_{E_0,p} \simeq \overline{\rho}_{E,p} \tag{2.6}$$

by Proposition 2.4.

Lemma 2.7 *The elliptic curve E over K is given by*

$$E : Y^2 = X(X - (-8 + 4\sqrt{5}))(X + (9 - 4\sqrt{5})).$$

Proof The conductor of E over K is $\mathfrak{P}^3$. Since E is modular, it corresponds to the unique Hilbert newform f of trivial character, parallel weight 2, and level $\mathfrak{P}^3$. ■

Remark 2.8 In the last section, we explain how to determine the full list of solutions (a, b, c) to $a + b + c = 0$, up to multiplication by the square of a unit of $\mathcal{O}_K$, such that

$$E_{a,b,c} : Y^2 = X(X - a)(X + b)$$

gives rise to an elliptic curve in the same isogeny class of E over K. We remark that the 2-adic conditions on these (a, b, c) vary; in particular, there are some triples where $2 \nmid abc$. This implies that inertia arguments at 2 will fail as any solution which is 2-adically close to one of these triples (a, b, c) cannot be ruled out by inertia arguments at 2.

Let $L = K(\zeta_r)$ where ζ_r is a primitive rth root of unity. Using modularity arguments and Theorem 3.5 in the following cases involving values of r, we will prove Theorem 1.2.

(1) Case $r = 1$.

Let $k = \mathcal{O}_K/3\mathcal{O}_K \cong \mathbb{F}_9$, noting that $\#k^\times = 8$.
Let $\mathfrak{q}_3 = 3\mathcal{O}_K$ and $N(\mathfrak{q}_3) = 9$ be the norm of $\mathfrak{q}_3$.
If $abc = 0$ in k, then we obtain a bound on p by [15, p. 9]. In particular, if $p \neq 3$, then p divides

$$a_{\mathfrak{q}_3}(f) \pm (N(\mathfrak{q}_3) + 1) \neq 0, \tag{2.9}$$

which is nonzero by the Hasse bound

$$|a_{\mathfrak{q}_3}(f)| = |a_{\mathfrak{q}_3}(E)| \leq 2\sqrt{N(\mathfrak{q}_3)}. \tag{2.10}$$

If $a_{\mathfrak{q}_3}(E_0) \neq a_{\mathfrak{q}_3}(E)$, then we also obtain a bound on p by [15, p. 9]. In particular, if $p \neq 3$, then p divides

$$a_{\mathfrak{q}_3}(E_0) - a_{\mathfrak{q}_3}(E) \neq 0. \tag{2.11}$$

Thus, either we obtain a bound on p or we have that $a, b, c \in k^\times$ and $a_{\mathfrak{q}_3}(E_0) = a_{\mathfrak{q}_3}(E)$. The bound can be computed to be $p \in \{2, 3\}$.

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

Assume now that $a, b, c \in k^\times$ and $a_{\mathfrak{q}_3}(E_0) = a_{\mathfrak{q}_3}(E)$. Now, set

$$\varepsilon = a^p b^p c^{-2p} \text{ in } k. \tag{2.12}$$

Since $p^2 \equiv 1 \pmod 8$, we have that $\varepsilon^R = abc^{-2}$ in k where $R \equiv p \pmod 8$. Hence, the condition (3.6) becomes

$$\left(\frac{\varepsilon^R - 1}{3}\right)_K \neq -1, \tag{2.13}$$

for all permutations of a, b, c as (2.5) holds. Using Magma, we can check the set of triples $(a, b, c) \in (k^\times)^3$ which satisfy

$$a_{\mathfrak{q}_3}(E_0) = a_{\mathfrak{q}_3}(E),$$

and (2.13) for all permutations of a, b, c is empty if $p \equiv 5, 7 \pmod 8$.

(2) Case $r = 3$.

Let $k = \mathcal{O}_K/21\mathcal{O}_K \cong \mathbb{F}_9 \times \mathbb{F}_{49}$, noting that $\#k^\times = 384$. Let $\mathfrak{q}_3 = 3\mathcal{O}_K$ and $\mathfrak{q}_7 = 7\mathcal{O}_K$.

If $abc \notin k^\times$ or one of the following two conditions holds,

$$a_{\mathfrak{q}_3}(E_0) \neq a_{\mathfrak{q}_3}(E),$$
$$a_{\mathfrak{q}_7}(E_0) \neq a_{\mathfrak{q}_7}(E),$$

we obtain a bound on p similarly as in (2.9) and (2.11). This bound can be computed to be $p \in \{2, 3, 5\}$. The case $p = 5$ is covered by [15].

Assume from here on that $a, b, c \in k^\times$ and both

$$a_{\mathfrak{q}_3}(E_0) = a_{\mathfrak{q}_3}(E) \quad \text{and}$$
$$a_{\mathfrak{q}_7}(E_0) = a_{\mathfrak{q}_7}(E)$$

hold. Now set

$$\varepsilon = a^p b^p c^{-2p} \text{ in } k. \tag{2.14}$$

Let R^* be the least positive residue such that $p \equiv R^* \pmod{384}$, and let R be such that $RR^* \equiv 1 \pmod{384}$. Then we have that $\varepsilon^R = abc^{-2}$ in k. Hence, the condition (3.6), taking $\zeta_r' = \zeta_r^R$ since $r = 3$ divides 384, becomes

$$\left(\frac{\varepsilon^R - \zeta_r'}{1 - 4\zeta_r}\right)_K \neq -1, \tag{2.15}$$

for all permutations of a, b, c as (2.5) holds. Using Magma, we can check the set of triples $(a, b, c) \in (k^\times)^3$ which satisfy

$$a_{\mathfrak{q}_3}(E_0) = a_{\mathfrak{q}_3}(E),$$
$$a_{\mathfrak{q}_7}(E_0) = a_{\mathfrak{q}_7}(E),$$

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

and (2.15) for all permutations of a, b, c is empty if

$$p \equiv 7, 19, 29, 41, 55, 67, 77, 89, 103, 115, 125, 137, 151, 163, 173, 185,$$
$$199, 211, 221, 233, 247, 259, 269, 281, 295, 307, 317, 329, 343, 355, 365, 377 \pmod{384}.$$

It can be verified that the set of congruence condition above is equivalent to $p \equiv 7, 19, 29, 41 \pmod{48}$, noting that 48 divides 384.

This concludes the proof of Theorem 1.2.

Remark 2.16 In the proof of Theorem 1.2, we argued on a hypothetical solution (a, b, c) to $a^p + b^p + c^p = 0$ and applied constraints over the residue class ring k. However, since p is coprime to $\#k^\times$, we can check the modular and reciprocity constraints in terms of new variables $(a', b', c') = (a^p, b^p, c^p)$ in k^3. This remark also applies to Theorem 1.3.

Remark 2.17 For a given $r \geq 1$, let $K = \mathbb{Q}(\sqrt{d})$ and $L = \mathbb{Q}(\sqrt{d}, \zeta_r)$. Our method of obtaining results for the Fermat's Last Theorem over K requires us to check the reciprocity constraints for all 3-tuples $(a, b, c) \in k_r^3$ where k_r is the residue ring given by

$$k_r := \mathcal{O}_K / \mathfrak{N}_r$$

and $\mathfrak{N}_r := (1 - 4\zeta_r)\mathcal{O}_L \cap \mathcal{O}_K$. As we increase r, the size of the rational prime factors of $\mathrm{Norm}(1 - 4\zeta_r)$ grows rapidly, which leads to computational bottlenecks as then k_r is too large (implying that the number of R^* and triples $(a, b, c) \in k_r^3$ to consider are too numerous or the Hecke eigenvalue computation for the modular constraint is infeasible). We therefore restricted our search for results to $r \leq 10$.

Remark 2.18 We describe more specifically how Remark 2.17 applies to $d = 5$: if $r = 2$, then $(1 - 4\zeta_2)\mathcal{O}_L = (\sqrt{5}\mathcal{O}_L)^2$ so that

$$\left(\frac{ab - c^2\zeta_r'}{5}\right)_L = \left(\frac{ab - c^2\zeta_r'}{\sqrt{5}}\right)_L \left(\frac{ab - c^2\zeta_r'}{\sqrt{5}}\right)_L = 1 \neq -1 \tag{2.19}$$

for any $(a, b, c) \in k_r^3$; that is, we obtain a trivial reciprocity constraint. For $r = 4, 5, 6, 10$, every possible choice of R^* had a triple $(a, b, c) \in k_r^3$ which passed all of the imposed constraints, implying negative results for these r's. For $r = 8$, the Hecke eigenvalue computation for the modular constraint was not feasible. For $r = 7, 9$, the size of k_r was unfeasible ($\#k_r > 17 \times 10^6$). However, there were choices of R^* such that sampling many $(a, b, c) \in k_r^3$ at random for that R^* did not yield a triple (a, b, c) which passed all of the imposed constraints. It thus remains possible that the imposed constraints are in principle sufficient to give a positive result for some R^*'s for $r = 7, 9$, but the method is infeasible computationally in its present form because $\#k_r$ is too large.

3 Reciprocity constraints

In this section, we will prove the reciprocity constraint, which is used in the proof of Theorem 1.2. For this, we will use the following form of quadratic reciprocity over number fields and a corollary, both of which are taken from [4].

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

Let L be a number field with ring of integers $\mathcal{O}_L$. For an element or ideal of $\mathcal{O}_L$, we say that it is odd if it is coprime to $2\mathcal{O}_L$.

Theorem 3.1 *Suppose L is a number field with r real embeddings. We write $\operatorname{sgn}_i(\alpha)$ for the sign of the image of α under the ith real embedding. Let $\alpha, \lambda \in \mathcal{O}_L$ be integers with α odd and α and λ coprime. Decompose $\lambda\mathcal{O}_L = \mathfrak{L}\mathfrak{N}$ where $\mathfrak{N}$ is an odd ideal in $\mathcal{O}_L$ and $\mathfrak{L}$ is even. Suppose that α is a quadratic residue modulo $4\mathfrak{L}$. Then*

$$\left(\frac{\lambda}{\alpha}\right)_L \left(\frac{\alpha}{\mathfrak{N}}\right)_L = (-1)^{\sigma},$$

where $\left(\frac{\alpha}{\mathfrak{N}}\right)_L$ is the Jacobi symbol in L and

$$\sigma = \sum_{i=1}^{r} \frac{\operatorname{sgn}_i(\alpha) - 1}{2} \frac{\operatorname{sgn}_i(\lambda) - 1}{2}.$$

For the definition of Jacobi symbol $\left(\frac{\lambda}{\mathfrak{N}}\right)_L$ over a number field L, see [4] or [17, Definition 8.2]. Furthermore, for $\alpha \in \mathcal{O}_L$, $\left(\frac{\lambda}{\alpha}\right)_L := \left(\frac{\lambda}{\alpha\mathcal{O}_L}\right)_L$.

Corollary 3.2 *Let α, λ be algebraic integers in the number field L with α odd. Suppose that $\alpha \equiv \varepsilon^2 \pmod{4\lambda}$ for some algebraic integer ε in L. In addition, suppose that α is positive in every real embedding of L. Then*

$$\left(\frac{\lambda}{\alpha}\right)_L \neq -1.$$

Proof If α and λ are not coprime, the above symbol is zero. Otherwise, we are in the case where we can apply Theorem 3.1 in the case where $\mathfrak{L} = \lambda\mathcal{O}_L$ and $\mathfrak{N} = \mathcal{O}_L$. In this case, $\sigma = 0$ since α is positive in every real embedding, and $\left(\frac{\alpha}{\mathcal{O}_L}\right)_L = 1$, so that $\left(\frac{\lambda}{\alpha}\right)_L = 1$. ∎

We also require the following lemmas.

Lemma 3.3 *If $x, y \in \mathbb{R}$ satisfy $x^n + y^n = 1$ for $n \in \mathbb{N}$, then $xy < 1$.*

Proof For all real x, we have that $x^{2n} - x^n + 1 > 0$. This implies that $x^n(1 - x^n) < 1$. If $xy \geq 1$, then we would have that $x^n y^n = x^n(1 - x^n) \geq 1$, a contradiction. Hence, we conclude $xy < 1$. ∎

Lemma 3.4 *If (a, b, c) is a primitive nontrivial solution to Fermat's equation over K for some odd prime $p > 2$, then $ab - c^2$ is negative in every real embedding of K.*

Proof Let ρ be any real embedding of K. Since (a, b, c) is a primitive solution to the Fermat equation, $(\rho(a), \rho(b), \rho(c))$ is also a primitive solution. Thus, if (a, b, c) is such a triple, then

$$\left(\frac{\rho(a)}{-\rho(c)}\right)^p + \left(\frac{\rho(b)}{-\rho(c)}\right)^p = 1.$$

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

Now, we employ Lemma 3.3 to deduce

$$\frac{\rho(a)\rho(b)}{\rho(c)^2} < 1,$$

which gives $\rho(ab - c^2) = \rho(a)(b) - \rho(c)^2 < 0$. ■

We now state and prove the reciprocity constraint.

Theorem 3.5 *Let K be a number field, and let ζ_r be a primitive rth root of unity where $(r,p) = 1$. If $r = 1$, assume further that K has an even number of real embeddings. Let $L = K(\zeta_r)$ and write $\zeta_r = \zeta_r'^{p}$ where ζ_r' is a primitive rth root of unity.*

If (a,b,c) is a primitive solution over $\mathcal{O}_K$ to

$$a^p + b^p + c^p = 0$$

and c is coprime to $2\mathcal{O}_K$, then

$$\left(\frac{ab - c^2\zeta_r'}{1 - 4\zeta_r}\right)_L \neq -1. \tag{3.6}$$

In particular, if abc is coprime to $2\mathcal{O}_K$, then (3.6) holds for all permutations of a, b, c.

Proof By assumption, c is coprime to $2\mathcal{O}_K$. We employ the identity

$$(a^p - b^p)^2 = -4(ab)^p + c^{2p}.$$

Subtracting both sides of this identity by $c^{2p}(1 - 4\zeta_r)$, we get

$$\begin{aligned}(a^p - b^p)^2 - c^{2p}(1 - 4\zeta_r) &= -4\left((ab)^p - \zeta_r c^{2p}\right)\\ &= -4(ab - c^2\zeta_r')h,\end{aligned} \tag{3.7}$$

where

$$h = (ab)^{p-1} + \zeta_r' c^2 (ab)^{p-2} + \cdots + \zeta_r'^{(p-1)} c^{2(p-1)}.$$

Let $\alpha = 1 - 4\zeta_r$ and $\lambda = ab - c^2\zeta_r'$. We first show that c is invertible modulo $4\lambda = 4(ab - c^2\zeta_r')$. To this end, let $\mathfrak{P}$ be a prime in $\mathcal{O}_L$ dividing c. We show that $\mathfrak{P}$ does not divide 4λ. Indeed, suppose this were the case. Then $\mathfrak{P}$ divides 4λ and so either divides $4\mathcal{O}_L$ or divides λ. Note that $\mathfrak{P}$ cannot divide $4\mathcal{O}_L$, for then $\mathfrak{P}$ divides $2\mathcal{O}_L$ and thus $c \in \mathfrak{P} \cap \mathcal{O}_K$, contradicting that c is coprime to $2\mathcal{O}_K$. Hence, $\mathfrak{P} \mid \lambda$. Then we have that

$$ab = \lambda + c^2\zeta_r' \in \mathfrak{P}$$

and so either a or b is in $\mathfrak{P}$. However,

$$a^p + b^p + c^p = 0,$$

so $\mathfrak{P}$ divides a, b, and c. We have assumed that a, b, c are coprime in $\mathcal{O}_K$. Let r_1, r_2, r_3 be such that

$$r_1 a + r_2 b + r_3 c = 1.$$

Then we get the contradiction that $1 \in \mathfrak{P}$.

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

In light of this, let $\varepsilon \in \mathcal{O}_L$ be such that the image of ε in $\mathcal{O}_L/(4(ab - c^2\zeta_r'))$ is

$$c^{-p}(a^p - b^p) \pmod{4(ab - c^2\zeta_r')}.$$

We see that α is odd, for if $\mathfrak{P}$ divides both α and $2\mathcal{O}_L$, then $\mathfrak{P}$ divides 1, a contradiction. Then, from (3.7),

$$\alpha \equiv \varepsilon^2 \pmod{4\lambda}.$$

Since L has no real embeddings if $r > 2$, Corollary 3.2 gives the result in this case.

If $r = 2$, we have that $\alpha = 5$ is positive in every real embedding of $L = K$ because $\mathbb{Q}$ is fixed. Corollary 3.2 then gives the result in this case.

From Theorem 3.1, we have that

$$\left(\frac{ab - c^2}{-3}\right)_K = (-1)^\sigma.$$

We are under the assumption that K has an even number of real embeddings $2t$ so that

$$\sigma = \sum_{i=1}^{2t} \frac{\operatorname{sgn}_i(-3) - 1}{2} \frac{\operatorname{sgn}_i(ab - c^2) - 1}{2}.$$

We see that $\operatorname{sgn}_i(-3) = -1$ for all i. Lemma 3.4 gives that $ab - c^2$ is totally negative and so $\operatorname{sgn}_i(ab - c^2) = -1$ for all i and hence we conclude $\sigma = 2t$ is even. This gives the result for $r = 1$. ∎

4 Proof of Theorem 1.3

Let $K = \mathbb{Q}(\sqrt{17})$, and let $\mathcal{O}_K$ be its ring of integer, which has unique factorization. The prime 2 splits in K as $2\mathcal{O}_K = \mathfrak{P}_1\mathfrak{P}_2$ for prime ideals $\mathfrak{P}_1$ and $\mathfrak{P}_2$ of K. Suppose (a, b, c) is a nontrivial primitive solution over $\mathcal{O}_K$ to (1.1), and let E_0 denote the Frey elliptic curve over K:

$$E_0 : Y^2 = X(X - a^p)(X + b^p). \tag{4.1}$$

Proposition 4.2 *Assume $p \geq 5$. Up to scaling (a, b, c) by a unit in $\mathcal{O}_K$, the conductor of E_0 over K is given by*

$$N(E_0) = \mathfrak{P}_1\mathfrak{P}_2 \prod_{\mathfrak{q} \mid abc, \mathfrak{q} \nmid \mathfrak{P}_1\mathfrak{P}_2} \mathfrak{q}.$$

Proof See [11, Corollary 5.1]. We note the fact that $\mathcal{O}_K$ has unique factorization means that there is no need to consider the extraneous prime $\mathfrak{r}$ in [11]. ∎

We may assume that

$$2 \mid abc, \tag{4.3}$$

since $a^p + b^p + c^p = 0$ implies that one of a^p, b^p, c^p is 0 in the residue fields of $\mathfrak{P}_1$ and $\mathfrak{P}_2$.

By the arguments in [11, p. 2], we need only prove Theorem 1.3 for $p \geq 17$, which we now assume.

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

Proposition 4.4 *The Galois representation* $\overline{\rho}_{E_0,p} : G_K \to \mathrm{GL}_2(\mathbb{F}_p)$ *is irreducible if* $p \geq 17$.

Proof See [11, Lemma 6.1, p. 9]. ∎

Proposition 4.5 *There is a Hilbert newform f of trivial character, parallel weight 2, and level $\mathfrak{P}_1\mathfrak{P}_2$ such that* $\overline{\rho}_{E_0,p} \simeq \overline{\rho}_{f,\mathfrak{p}}$.

Proof The elliptic curve E_0 over K is modular by [9]. Using [10, Theorem 7], we obtain the desired statement. ∎

There is a unique Hilbert newform f of trivial character, parallel weight 2, and level $\mathfrak{P}_1\mathfrak{P}_2$, and this corresponds to an elliptic curve E over K.

Lemma 4.6 *The elliptic curve E over K is given by*

$$E : Y^2 = X(X - (4 - \sqrt{17}))\left(X + \frac{-13 + 5\sqrt{17}}{2}\right).$$

Proof See [11, p. 13]. The conductor of E over K is $2\mathcal{O}_K$. Since E is modular, it corresponds to the unique Hilbert newform f of trivial character, parallel weight 2, and level $2\mathcal{O}_K$. ∎

Hence, we have that

$$\overline{\rho}_{E_0,p} \simeq \overline{\rho}_{E,p} \tag{4.7}$$

by Proposition 4.5.

Proof of Theorem 1.3 Let $L = K(\zeta_r)$ where ζ_r is a primitive rth root of unity. We give two proofs in the cases $r = 1$, $r = 2$, and $r = 3$.

(1) Case $r = 1$.

Let $k = \mathcal{O}_K/3\mathcal{O}_K \cong \mathbb{F}_9$, noting that $\#k^\times = 8$. Let $\mathfrak{q}_3 = 3\mathcal{O}_K$.

If $abc \notin k^\times$ or $a_{\mathfrak{q}_3}(E_0) \not\equiv a_{\mathfrak{q}_3}(E)$, then we obtain a bound on p similarly as in (2.9) and (2.11). This bound can be computed to be $p \in \{2, 3\}$.

Assume from here on that $a, b, c \in k^\times$ and $a_{\mathfrak{q}_3}(E_0) = a_{\mathfrak{q}_3}(E)$ holds. For $a, b, c \in k^\times$, we set

$$\varepsilon = a^p b^p c^{-2p} \text{ in } k. \tag{4.8}$$

Since $p^2 \equiv 1 \pmod 8$, we have that $\varepsilon^R = abc^{-2}$ in k where $R \equiv p \pmod 8$. Hence, the condition (5.22) becomes

$$\left(\frac{\varepsilon^R - 1}{3}\right)_K \not\equiv -1, \tag{4.9}$$

for all permutations of a, b, c as (4.3) holds. We note that (5.20) holds as if not, by the left-hand side of (5.10), we would have that $\sqrt{-3} \in K$.

Using Magma, we can check the set of triples $(a, b, c) \in (k^\times)^3$ which satisfy

$$a_{\mathfrak{q}_3}(E_0) = a_{\mathfrak{q}_3}(E),$$

and (4.11) for all permutations of a, b, c is empty if $p \equiv 5, 7 \pmod 8$.

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

(2) Case $r = 2$.

Let $k = \mathcal{O}_K/5\mathcal{O}_K \cong \mathbb{F}_{25}$, noting that $\#k^\times = 24$. Let $\mathfrak{q}_5 = 5\mathcal{O}_K$.

If $abc \notin k^\times$ or $a_{\mathfrak{q}_5}(E_0) \neq a_{\mathfrak{q}_5}(E)$, then we obtain a bound on p similarly as in (2.9) and (2.11). This bound can be computed to be $p \in \{2, 3, 5, 7\}$.

Assume from here on that $a, b, c \in k^\times$ and $a_{\mathfrak{q}_5}(E_0) = a_{\mathfrak{q}_5}(E)$ holds. For $a, b, c \in k^\times$, we set

$$\varepsilon = a^p b^p c^{-2p} \text{ in } k. \tag{4.10}$$

Since $p^2 \equiv 1 \pmod{24}$, we have that $\varepsilon^R = abc^{-2}$ in k where $R \equiv p \pmod{24}$. Hence, the condition (5.22) becomes

$$\left(\frac{\varepsilon^R - 1}{5}\right)_K \neq -1, \tag{4.11}$$

for all permutations of a, b, c as (4.3) holds. We note that (5.20) holds as if not, by the left-hand side of (5.10), we would have that $\sqrt{5} \in K$.

Using Magma, we can check the set of triples $(a, b, c) \in (k^\times)^3$ which satisfy

$$a_{\mathfrak{q}_5}(E_0) = a_{\mathfrak{q}_5}(E),$$

and (4.11) for all permutations of a, b, c is empty if $p \equiv 13, 17, 19, 23 \pmod{24}$.

(3) Case $r = 3$.

Let $k = \mathcal{O}_K/21\mathcal{O}_K \cong \mathbb{F}_9 \times \mathbb{F}_{49}$, noting that $\#k^\times = 384$. Let $\mathfrak{q}_3 = 3\mathcal{O}_K$ and $\mathfrak{q}_7 = 7\mathcal{O}_K$.

If $abc \notin k^\times$ or one of the following two conditions holds,

$$a_{\mathfrak{q}_3}(E_0) \neq a_{\mathfrak{q}_3}(E),$$
$$a_{\mathfrak{q}_7}(E_0) \neq a_{\mathfrak{q}_7}(E),$$

we obtain a bound on p similarly as in (2.9) and (2.11). This bound can be computed to be $p \in \{2, 3, 5, 7\}$.

Assume from here on that $a, b, c \in k^\times$ and both

$$a_{\mathfrak{q}_3}(E_0) = a_{\mathfrak{q}_3}(E) \quad \text{and}$$
$$a_{\mathfrak{q}_7}(E_0) = a_{\mathfrak{q}_7}(E)$$

hold. For $a, b, c \in k^\times$, we set

$$\varepsilon = a^p b^p c^{-2p} \text{ in } k. \tag{4.12}$$

Let R^* be the least positive residue such that $p \equiv R^* \pmod{384}$, and let R be such that $RR^* \equiv 1 \pmod{384}$. Then we have that $\varepsilon^R = abc^{-2}$ in k. Hence, the condition (5.22), taking $\zeta_r' = \zeta_r^R$ since $r = 3$ divides 384, becomes

$$\left(\frac{\varepsilon^R - \zeta_r'}{1 - 4\zeta_r}\right)_K \neq -1, \tag{4.13}$$

for all permutations of a, b, c as (4.3) holds. We note that the hypothesis (5.20) holds as K is totally real.

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

Using Magma, we can check the set of triples $(a,b,c) \in (k^\times)^3$ which satisfy

$$a_{\mathfrak{q}_3}(E_0) = a_{\mathfrak{q}_3}(E),$$
$$a_{\mathfrak{q}_7}(E_0) = a_{\mathfrak{q}_7}(E),$$

and (4.13) for all permutations of a, b, c is empty if

$$p \equiv 5,7,13,23,29,31,37,47,53,55,61,71,77,79,85,95,101,103,$$
$$109,119,125,127,133,143,149,151,157,167,173,175,181,191,197,199,205,$$
$$215,221,223,229,239,245,247,253,263,269,271,277,287,293,295,301,$$
$$311,317,319,325,335,341,343,349,359,365,367,373,383 \pmod{384}.$$

It can be verified that the congruence condition above is equivalent to $p \equiv 5,7,13,23 \pmod{24}$, noting that 24 divides 384. Finally, the congruence $p \equiv 5,7,13,23 \pmod{24}$ is equivalent to $p \equiv 5,7 \pmod 8$ for prime $p \geq 5$. ∎

Remark 4.14 We describe more specifically how Remark 2.17 applies to $d = 17$: if $r = 4$, we have that $(1-\zeta_4)\mathcal{O}_L = (\sqrt{17}\mathcal{O}_L)^2$, so in a similar way as in (2.19), we obtain a trivial reciprocity constraint. For $r = 6, 8$, every possible choice of R^* had a triple $(a,b,c) \in k_r^3$ which passed all of the imposed constraints, implying a negative result. For $r = 5,7,9,10$, the sizes of the k_r's were too large ($\#k_r > 4 \times 10^4$). For $r = 5,7,9,10$, there were choices of R^* such that sampling many $(a,b,c) \in k_r^3$ at random for that R^* did not yield a triple (a,b,c) which passed all of the imposed constraints. It thus remains possible that the imposed constraints are in principle sufficient to give a positive result for some R^*'s for $r = 5,7,9,10$, but the method is infeasible computationally in its present form because $\#k_r$ is too large.

5 Reciprocity constraints using the Hilbert symbol

In this section, we use Hilbert symbols to prove a strengthened reciprocity constraint which does not have a condition on c.

Definition 5.1 For a global field L, we define the *Hilbert symbol* $(\cdot,\cdot)_L : L^\times \times L^\times \to \{-1,1\}$ as

$$(a,b)_L := \begin{cases} 1, & \text{if } z^2 = ax^2 + by^2 \text{ has a nontrivial solution in } L, \\ -1, & \text{otherwise.} \end{cases} \tag{5.2}$$

Let S_L denote the set of normalized places of L and partition them into

$$S_L^\infty = \{v \in S_L : v \mid \infty\},$$
$$S_L^{\text{even}} = \{v \in S_L : v \mid 2\},$$
$$S_L^{\text{odd}} = \{v \in S_L : v \nmid 2\}.$$

For a place $v \in S_L$ of L, we denote $(\alpha,\beta)_v := (\alpha,\beta)_{L_v}$, where L_v is the completion of L at v. Let π_v be a uniformizer for L_v, let $\mathcal{O}_v$ be the ring of integers of L_v, and let $\mathbb{F}_v$ be the residue field of L_v.

We will state a few useful properties of the Hilbert symbol for later use.

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

Lemma 5.3 *The Hilbert symbol defines a nondegenerate symmetric bimultiplicative pairing.*

Proof See [21, Lemma 12.4.6]. ∎

Lemma 5.4 *Let $a, b \in L^\times$. Then the following hold:*

(1) $(ac^2, bd^2)_L = (a, b)_L$ *for all* $c, d \in L^\times$.
(2) $(b, a)_L = (a, b)_L$.
(3) $(a, b)_L = (a, -ab)_L = (b, -ab)_L$.
(4) $(1, a)_L = (a, -a)_L = 1$.
(5) *If* $a \neq 1$, *then* $(a, 1-a) = 1$.
(6) *If* $\sigma \in \mathrm{Aut}(L)$, *then* $(a, b)_L = (\sigma(a), \sigma(b))_L$.

Proof See [21, Lemma 12.4.3]. ∎

Lemma 5.5 (Reciprocity law) *Let L be a number field, and let S_L be the set of places of L. Then, for any $\alpha, \beta \in L^*$, we have that*

$$\prod_{v\in S_L} (\alpha, \beta)_v = 1. \tag{5.6}$$

Proof See [21, Corollary 14.6.2]. ∎

Lemma 5.7 *With notation as above, let $q = \#\mathbb{F}_v$ be odd. Write $a = a_0\pi_v^{v(a)}$ and $b = b_0\pi_v^{v(b)}$. Then we have that*

$$(a, b)_v = (-1)^{v(a)v(b)(q-1)/2}\left(\frac{a_0}{\pi_v}\right)^{v(b)}\left(\frac{b_0}{\pi_v}\right)^{v(a)}. \tag{5.8}$$

Proof See [21, equation (12.4.10)]. ∎

We now move on to the theorem that enables us to tackle the reciprocity constraint on the primitive solutions over $\mathbb{Q}(\sqrt{17})$. The following is a generalization of [1, Proposition 17].

Theorem 5.9 *Let L be a number field containing a primitive rth root of unity ζ_r such that $(r, n) = 1$ where $n \in \mathbb{N}$. Assume $s, t \in \mathcal{O}_L$, $v(t) = 0$ for all $v \in S_L$ such that $v(n) > 0$, and $v(s) > 0$ only for places $v \in \mathrm{S}_\mathrm{L}^{\mathrm{even}}$. Furthermore, suppose we have the following identity:*

$$A^2 - tB^{2n} = s(C^n - \zeta_r B^{2n}) \neq 0 \tag{5.10}$$

for coprime $A, B, C \in \mathcal{O}_L$ and write $\zeta_r = \zeta_r'^{\,n}$ where ζ_r' is a primitive rth root of unity.

Then we have that

(5.11)
$$\prod_{v\in S_L^\infty} (t, s(C - \zeta_r' B^2))_v \prod_{v\in \mathrm{S}_\mathrm{L}^{\mathrm{even}}} (t, s(C - \zeta_r' B^2))_v \prod_{v\in \mathrm{S}_\mathrm{L}^{\mathrm{odd}}, \mathrm{v(t)\ odd}} (t, s(C - \zeta_r' B^2))_v = 1.$$

Proof The hypotheses imply that $s, t, (C^n - \zeta_r B^{2n})$ are nonzero, and hence also $(C - \zeta_r' B^2) \neq 0$, so the Hilbert symbols used below are well defined. Note that

$$(t, s(C^n - \zeta_r B^{2n}))_v = 1$$

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

for all $v \in S_L$ because

$$A^2 = tB^{2n} + s(C^n - \zeta_r B^{2n}) \cdot 1^2.$$

Using the fact that $\zeta_r = \zeta_r'^n$ and the factorization

$$\begin{aligned} C^n - \zeta_r B^{2n} &= C^n - (\zeta_r' B^2)^n \\ &= (C - \zeta_r' B^2)(C^{n-1} + C^{n-2}\zeta_r' B^2 + \cdots + (\zeta_r' B^2)^{n-1}), \end{aligned} \tag{5.12}$$

we see that

$$(t, s(C - \zeta_r' B^2))_v = (t, C^{n-1} + C^{n-2}\zeta_r' B^2 + \cdots + (\zeta_r' B^2)^{n-1})_v, \tag{5.13}$$

using Lemma 5.3.

Let $\beta = s(C - \zeta_r' B^2)$. By (5.6), we have that

$$\prod_{v \in S_L^\infty} (t,\beta)_v \prod_{v \in S_L^{\text{even}}} (t,\beta)_v \prod_{v \in S_L^{\text{odd}}, v(t) \text{ odd}} (t,\beta)_v = \prod_{v \in S_L^{\text{odd}}, v(t) \text{ even}} (t,\beta)_v. \tag{5.14}$$

Thus, it suffices to show that $(t,\beta)_v = 1$ when $v \in S_L^{\text{odd}}$ and $v(t)$ is even.

Suppose $v \in S_L^{\text{odd}}$ and $v(t)$ is even. By (5.8), $(t,\beta)_v = 1$ when $v(\beta)$ is even. So suppose that $v(\beta)$ is odd.

If $v(n) > 0$, then we have that $v(t) = 0$ by assumption. As $v(\beta)$ is odd, we deduce from (5.10) and (5.12) that

$$v(A^2 - tB^{2n}) = v(s(C^n - \zeta_r B^{2n})) \geq v(\beta) > 0,$$

so that

$$A^2 \equiv tB^{2n} \pmod{\pi_v}. \tag{5.15}$$

Since A, B, C are coprime, by (5.10), we deduce that A and B are coprime, as $v(A), v(B) > 0$ implies $v(sC^n) > 0$. Since $v(s) = 0$, we see that $v(C) > 0$, contradicting A, B, C being coprime. Hence, if $v(B) > 0$, then by (5.15) we obtain that $v(A) > 0$, contradicting A, B being coprime. Thus, $v(B) = 0$ and B is a v-adic unit. From (5.15), we deduce that

$$(AB^{-n})^2 \equiv t \pmod{\pi_v},$$

and hence

$$\left(\frac{t}{\pi_v}\right) = 1,$$

using also that $v(t) = 0$. Using Lemma 5.7, this leads to $(t,\beta) = 1$.

If $v(n) = 0$, then since $v(\beta)$ is odd and $v(s) = 0$, we firstly have that

$$v(C - \zeta_r' B^2) = v(\beta) > 0. \tag{5.16}$$

We have that $v(C) = 0$ for if $v(C) > 0$, then by (5.16) $v(B) > 0$ and hence by (5.10) $v(A) > 0$, contradicting that A, B, C are coprime. It follows that

$$C^{n-1} + \cdots + (\zeta_r' B^2)^{n-1} \equiv nC^{n-1} \pmod{\pi_v},$$

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

which from the conditions $v(n) = v(C) = 0$ imply that

$$v(C^{n-1} + \cdots + (\zeta_r' B^2)^{n-1}) = 0.$$

Since $v(t)$ is even, using Lemma 5.7, it follows that $(t, C^{n-1} + \cdots + (\zeta_r' B^2)^{n-1})_v = 1$. Hence, by (5.13), we obtain

$$(t, \beta)_v = (t, C^{n-1} + \cdots + (\zeta_r' B^2)^{n-1})_v = 1,$$

as desired. ■

Remark 5.17 In our application, $L = K(\zeta_r)$, $n = p$, $t = 1 - 4\zeta_r$, $s = 4$, $C = ab$, $B = c$, $A = a^p - b^p$, and we have the identity (5.10) because of (3.7). Here, $v(s) > 0$ only for places $v \in S_L^{\text{even}}$ and A, B, C are coprime. Finally, we require (p) to be coprime to $(t) = (1 - 4\zeta_r)$ to ensure the hypothesis $v(t) = 0$ for all $v \in S_L$ such that $v(n) > 0$.

We need a few more lemmas to aid the proof of our reciprocity constraint.

Lemma 5.18 *Let L be a number field containing a primitive rth root of unity ζ_r, and L is unramified at 2. Let v be a place of L above 2. Then $(1 - 4\zeta_r, b)_v = 1$ for any $b \in L$ with $v(b) = 0$.*

Proof The proof in [18, Theorem 1, Chapter III, Section 1.2] for the case $L = \mathbb{Q}$ and $\alpha = \beta = 0$ can be adapted to prove this lemma.

If u and b are elements in $L_v^\times$ with $u \equiv 1 \pmod 8$, then we first show that

$$(u, b)_v = 1,$$

where the Hilbert symbol is taken in L_v. Indeed, if $u \equiv 1 \pmod 8$, then since

$$v(1^2 - u) \geqslant 3 > 2 = 2v(2(1)),$$

applying Hensel's lemma to $f(x) = x^2 - u$, we see that u is a square in L_v, say $u = a^2$. Hence,

$$a^2 = u(1)^2 + b(0)^2,$$

so $(u, b)_v = 1$.

Now, let k_v be the residue field of L_v, and let $u = 1 - 4\zeta_r$. Since $k_v^\times$ is odd, we can solve the equation $bx^2 = \zeta_r$ in $k_v^\times$ for $x \in k_v^\times$. Then $u(1)^2 + b(2x)^2 \equiv 1 \pmod 8$ and hence $u(1)^2 + b(2x)^2 = a^2$ for some $a \in L_v$ by the argument above. It follows then that $(u, b)_v = (1 - 4\zeta_r, b) = 1$. ■

The following is a strengthened version of Theorem 3.5, now with no condition on c being coprime to $2\mathcal{O}_K$.

Theorem 5.19 *Let K be a number field, and let $L = K(\zeta_r)$ where ζ_r be a primitive rth root of unity such that $(r, p) = 1$. If $r = 1$, assume further that K has an even number of real embeddings.*

Suppose L is unramified at 2, K is totally split at 2, (p) is coprime to $(1 - 4\zeta_r)$, and write $\zeta_r = \zeta_r'^p$ where ζ_r' is a primitive rth root of unity.

If (a, b, c) is a primitive solution over $\mathcal{O}_K$ to

$$a^p + b^p + c^p = 0$$

such that

$$(ab)^p - \zeta_r c^{2p} \neq 0, \tag{5.20}$$

then one has

$$\left(\frac{ab - c^2\zeta_r'}{1-4\zeta_r}\right)_L \neq -1, \tag{5.21}$$

for all permutations of a, b, c.

Proof We may assume that $ab - c^2\zeta_r'$ and $1-4\zeta_r$ are coprime, or else we are already done as we would have

$$\left(\frac{ab - c^2\zeta_r'}{1-4\zeta_r}\right)_L = 0.$$

Since $1-4\zeta_r$ is coprime to $2\mathcal{O}_L$, we have from the definition of Jacobi (see, for instance, [17, Definition 8.2]) symbol that

$$\left(\frac{ab - c^2\zeta_r'}{1-4\zeta_r}\right)_L = \prod_{v \in S_L^{\mathrm{odd}}, v(1-4\zeta_r) \text{ odd}} \left(\frac{ab - c^2\zeta_r'}{\pi_v}\right)^{v(1-4\zeta_r)}. \tag{5.22}$$

We note that the product is by definition over the $v \in S_L^{\mathrm{odd}}$, but only the terms with $v(1-4\zeta_r)$ odd can be −1. Using Lemma 5.7, we see that

$$\left(\frac{ab - c^2\zeta_r'}{\pi_v}\right)^{v(1-4\zeta_r)} = (1-4\zeta_r, ab - c^2\zeta_r')_v$$

if $v \in S_L^{\mathrm{odd}}$, $v(1-4\zeta_r)$ is odd, and $v(ab - c^2\zeta_r') = 0$. Hence, we obtain that

$$\left(\frac{ab - c^2\zeta_r'}{1-4\zeta_r}\right)_L = \prod_{v \in S_L^{\mathrm{odd}}, v(1-4\zeta_r) \text{ odd}} (1-4\zeta_r, ab - c^2\zeta_r')_v. \tag{5.23}$$

As (a, b, c) is primitive, for any $v \in S_L^{\mathrm{even}}$, two of the elements a, b, c are units in $\mathcal{O}_{L,v}$ and the remaining element has positive valuation, since $a, b, c \in \mathcal{O}_K$ and K is totally split at 2. This implies that

$$ab - c^2\zeta_r'$$

is coprime to $2\mathcal{O}_L$. By Lemma 5.18, it follows that

$$(1-4\zeta_r, ab - c^2\zeta_r')_v = 1$$

for all $v \in S_L^{\mathrm{even}}$ as we are assuming L is unramified at 2.

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

If $r \geq 3$, then L is totally complex and we have that $(1-4\zeta_r, ab - c^2\zeta_r')_v = 1$ for all $v \in S_L^\infty$.

If $r = 2$, then $L = K$ and $1 - 4\zeta_r = 5$ is positive in every real embedding of L. Thus, $(1-4\zeta_r, ab - c^2\zeta_r')_v = 1$ for all $v \in S_L^\infty$.

If $r = 1$, then $L = K$ is a number field with an even number of real embeddings by hypothesis. Thus, using Lemma 3.4, we obtain that

$$\prod_{v \in S_K^\infty} (-3, ab - c^2)_v = 1$$

as the Hilbert symbols which are -1 occur in total an even number of times in the above product.

Thus, in all cases for r, using Theorem 5.9, we see that the third product in (5.11) is 1, which implies that

$$\left(\frac{ab - c^2\zeta_r'}{1 - 4\zeta_r}\right)_L = 1.$$

The hypothesis (5.20) ensures that the quantity in (5.10) is nonzero. ∎

Remark 5.24 The constraint in (5.11) of Theorem 5.9 is an example of a Brauer–Manin obstruction. Let $\mathcal{A}$ be the Azumaya algebra given by the Hilbert symbol $(t, s(C - \zeta_r' B^2))$ on the variety defined by (5.10), subject to A, B, C coprime and $C^n - \zeta_r B^{2n} \neq 0$. Then (5.14), which is used in the proof of (5.11), corresponds to the condition

$$\sum_v \mathrm{inv}_v \mathcal{A}(x_v) = 0$$

of the first formula in the introduction of [2].

6 Essential obstructive S-unit solutions

Let $K = \mathbb{Q}(\sqrt{5})$ or $K = \mathbb{Q}(\sqrt{17})$, and let S be the set of places of K above 2.

Suppose $(a, b, c) \in \mathcal{O}_K^3$ is a nontrivial primitive solution to (1.1) with $p = 1$, that is,

$$a + b + c = 0. \tag{6.1}$$

If the Frey curve

$$E_{a,b,c} : y^2 = x(x-a)(x+b)$$

is an elliptic curve over K with conductor $N = 8\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{5})$ and conductor $N = 2\mathcal{O}_K$ for $K = \mathbb{Q}(\sqrt{17})$, then the triple (a, b, c) poses an obstruction to solving (1.1) over K using the modular method. We call such a triple (a, b, c) an (essential) obstructive solution to (1.1). Given such a triple (a, b, c), multiplication by the square of a unit in $\mathcal{O}_K$ produces another such triple with $E_{a,b,c}$ in the same isomorphism class over K, and thus it is natural to consider obstructive solutions (a, b, c) up to multiplication by the square of a unit in $\mathcal{O}_K$.

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

If (a, b, c) is an obstructive solution to (1.1), it can be seen that division by any one of $-a, -b, -c$ in (6.1) gives a solution to the S-unit equation

$$U + V = 1, \tag{6.2}$$

where U, V are S-units in K. Conversely, given a solution (U, V) to the S-unit equation, we can form a triple from the six orderings of $U, V, -1$ and scale by an element of K^* to produce a primitive solution $(a, b, c) \in \mathcal{O}_K^3$ to (6.1). However, the possible triples (a, b, c) which arise need not be obstructive solutions, so not all solutions to the S-unit equation (6.2) are relevant as obstructions to the modular method.

In this section, we give methods to list the obstructive solutions (a, b, c) to (1.1). This serves two purposes: first, it gives a more detailed description of the obstructions to solving Fermat's Last Theorem over these quadratic fields, and second it gives a double check on the computations used to prove the main results of this paper.

One method to list the obstructive solutions (a, b, c) to (1.1) would be to compute the solutions to the S-unit equation (6.2) for K. This can be done in a few minutes in `SageMath`. However, a direct computation of solutions to the S-unit equation for $\mathbb{Q}(\sqrt{17})$ using SageMath is slow and does not appear to terminate in any reasonable amount of time.

We explain now an alternate method of determining obstructive solutions (a, b, c) to (1.1) using known lists of elliptic curves over K with conductor N [20].

First, recall that if we have two elliptic curves E_1 and E_2 over K, given in the following form,

$$E_1 : y_1^2 = f_1(x_1),$$
$$E_2 : y_2^2 = f_2(x_2),$$

where $f_i \in \mathcal{O}_K[x]$ are monic of degree 3, then E_1 is isomorphic to E_2 over K if and only if there exist $u, \beta \in \mathcal{O}_K$ and a change of variables

$$y_2 = u^3 y_2, \tag{6.3}$$

$$x_2 = u^2 x_1 + \beta, \tag{6.4}$$

$$\Delta(E_2) = u^{12} \Delta(E_1). \tag{6.5}$$

Suppose (a, b, c) is an obstructive solution to (1.1). Then the elliptic curve

$$E_0 = E_{a,b,c} : y^2 = x(x - a)(x + b) \tag{6.6}$$

satisfies

$$E_0 \cong_K E$$

for some elliptic curve E defined over K of conductor equal to N. Due to primitivity of (a, b, c), (6.6) is semistable at primes $\mathfrak{q}$ of K coprime to $2\mathcal{O}_K$, and hence already a local minimal Weierstrass model at such $\mathfrak{q}$. Since $E_0 \cong_K E$ and E_0 has full 2-torsion over K, it follows that E also has full 2-torsion over K.

Put E into global minimal Weierstrass form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + x_4x + a_6. \tag{6.7}$$

By completing the square, we may transform to a model for E of the form

$$E : y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3), \tag{6.8}$$

where $f \in \mathcal{O}_K[x]$ is monic of degree 3, and this model is a local minimal Weierstrass model at all primes $\mathfrak{q}$ of K coprime to $2\mathcal{O}_K$.

Using (6.5), we deduce that u is an S-unit in $\mathcal{O}_K$ by definition of local minimal Weierstrass model (i.e., a Weierstrass model over $\mathcal{O}_{K_\mathfrak{q}}$ whose discriminant has minimal valuation). Furthermore, by $E_0 \cong_K E$ and (6.4), there is some permutation of e_1, e_2, e_3 such that

$$\begin{aligned} u^2e_1 + \beta &= 0, \\ u^2e_2 + \beta &= a, \\ u^2e_3 + \beta &= -b, \end{aligned}$$

or equivalently

$$a = u^2(e_2 - e_1), \tag{6.9}$$

$$b = -u^2(e_3 - e_1). \tag{6.10}$$

Conversely, given an elliptic curve E over K of conductor N and full 2-torsion over K, we can produce an obstructive solution $(a, b, c) := (a, b, -a - b)$ if and only if there is an S-unit u of K such that a and b are coprime in (6.9) and (6.10). A triple (a, b, c) produced from E is unique up to multiplication by the square of a unit in $\mathcal{O}_K$ (and up to a choice of labeling of $e_1, e_2, e_3 \in K$).

We have determined the list of obstructive solutions for both $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(\sqrt{17})$, which can be found in the electronic resources for this paper [3]. For those congruence classes of exponents p where we obtain a result, all obstructive solutions are eliminated by the reciprocity constraints. For those congruence classes of exponents p where we do not obtain a result, there is some obstructive solution that is not eliminated by the reciprocity constraints.

We end by illustrating the two methods for listing the obstructive solutions (a, b, c) to (1.1) for $K = \mathbb{Q}(\sqrt{5})$. The first method starts with the solutions (U, V) to the S-unit equation (6.2):

$$\begin{aligned} &(2, -1), \left(\frac{-\sqrt{5}+1}{4}, \frac{\sqrt{5}+3}{4}\right), \left(\frac{-\sqrt{5}-1}{2}, \frac{\sqrt{5}+3}{2}\right), \left(\frac{\sqrt{5}+2}{4}, \frac{-\sqrt{5}+2}{4}\right), \\ &(4\sqrt{5}-8, -4\sqrt{5}+9), \left(\frac{-\sqrt{5}+1}{2}, \frac{\sqrt{5}+1}{2}\right), (-4\sqrt{5}-8, 4\sqrt{5}+9), \end{aligned} \tag{6.11}$$

$$\left(\frac{-\sqrt{5}+3}{2},\frac{\sqrt{5}-1}{2}\right),\left(-\sqrt{5}-2,\sqrt{5}+3\right),\left(-\sqrt{5}-1,\sqrt{5}+2\right),\left(\frac{\sqrt{5}+1}{4},\frac{-\sqrt{5}+3}{4}\right),$$
$$\left(-\sqrt{5}+2,\sqrt{5}-1\right),\left(-\sqrt{5}+3,\sqrt{5}-2\right),\left(\frac{1}{2},\frac{1}{2}\right),$$

as computed by SageMath and listed up to permutation of U, V.

For triples $(a,b,c),(u,v,w)\in K^3$, we write $(a,b,c)\sim(u,v,w)$ if (a,b,c) is a nonzero scalar multiple of a permutation of (u,v,w). Consider the set

$$\mathfrak{S}=\{(a,b,c)\in\mathcal{O}_K^3:(a,b,c)\sim(U,V,-1),(U,V)\text{ is an }S\text{-unit solution,}\\ \text{and }(a,b,c)\text{ is primitive}\}.$$

The obstructive solutions to (1.1) are the triples $(a,b,c)\in\mathfrak{S}$ such that the conductor of $E_{a,b,c}$ is $8\mathcal{O}_K$. As we consider obstructive solutions up to equivalence by multiplication by the square of a unit in $\mathcal{O}_K$, the set $\mathfrak{S}$ is finite up to this equivalence and representatives can be computed from (11).

In the second method, we consider each of the elliptic curves E over K with conductor $8\mathcal{O}_K$ and produce if possible an obstructive solution (a,b,c) from it using the process described in the previous paragraphs.

Both methods give the same list up to equivalence by multiplication by the square of a unit in $\mathcal{O}_K$. In all, there are 12 obstructive solutions to (1.1) over $K=\mathbb{Q}(\sqrt{5})$, up to equivalence by multiplication by the square of a unit in $\mathcal{O}_K$:

$$\begin{aligned}(6.12)\qquad &\left(-1,-4\sqrt{5}-8,4\sqrt{5}+9\right),\left(4\sqrt{5}+8,1,-4\sqrt{5}-9\right),\\ &\left(-1,\frac{\sqrt{5}+3}{2},\frac{-\sqrt{5}-1}{2}\right),\left(1,\frac{-\sqrt{5}+1}{2},\frac{\sqrt{5}-3}{2}\right),\\ &\left(\frac{-3\sqrt{5}-7}{2},2\sqrt{5}+2,\frac{-\sqrt{5}+3}{2}\right),\left(\frac{-\sqrt{5}-1}{2},-1,\frac{\sqrt{5}+3}{2}\right),\\ &\left(\frac{\sqrt{5}+1}{2},\frac{-\sqrt{5}-3}{2},1\right),\left(4\sqrt{5}+9,-1,-4\sqrt{5}-8\right),\\ &\left(-4\sqrt{5}+8,1,4\sqrt{5}-9\right),\left(1,-4\sqrt{5}-9,4\sqrt{5}+8\right),\\ &\left(\frac{-\sqrt{5}+3}{2},\frac{\sqrt{5}-1}{2},-1\right),\left(\frac{-\sqrt{5}-3}{2},1,\frac{\sqrt{5}+1}{2}\right).\end{aligned}$$

Acknowledgment We would like to thank Alain Kraus for helpful comments and improvements on an earlier version of this paper, and Nuno Freitas and Samir Siksek for useful comments about the problems studied in this paper.

References

[1] M. A. Bennett, I. Chen, S. R. Dahmen, and S. Yazdani, *Generalized Fermat equations: a miscellany*. Int. J. Number Theory **11**(2015), no. 1, 1–28.

[2] M. Bright, *Efficient evaluation of the Brauer–Manin obstruction*. Math. Proc. Cambridge Philos. Soc. **142**(2007), no. 1, 13–23.

[3] I. Chen, A. Efemwonkieke, and D. Sun, Supporting files for this paper. https://iminchen.org

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press

[4] I. Chen and S. Siksek, *Perfect powers expressible as sums of two cubes*. J. Algebra **322**(2019), 638–655.

[5] H. Deconinck, *The generalized Fermat equation over totally real number fields*. Ph.D. thesis, University of Warwick, 2016.

[6] N. Freitas, A. Kraus, and S. Siksek, *Class field theory, Diophantine analysis and the asymptotic Fermat's Last Theorem*. Adv. Math. **363**(2020), Article no. 106964, 37 pp.

[7] N. Freitas, A. Kraus, and S. Siksek, *On asymptotic Fermat over $\mathbb{Z}_p$ -extensions of $\mathbb{Q}$*. Algebra Number Theory **14**(2020), no. 9, 2571–2574.

[8] N. Freitas, A. Kraus, and S. Siksek, *Local criteria for the unit equation and the asymptotic Fermat's Last Theorem*. Proc. Natl. Acad. Sci. USA **118**(2021), no. 12, Article no. 2026449118, 5 pp.

[9] N. Freitas, B. V. LeHung, and S. Siksek, *Elliptic curves over real quadratic fields are modular*. Invent. Math. **201**(2015), no. 1, 159–206.

[10] N. Freitas and S. Siksek, *The asymptotic Fermat's Last Theorem for five-sixths of real quadratic fields*. Compos. Math. **151**(2015), no. 8, 1395–1415.

[11] N. Freitas and S. Siksek, *Fermat's Last Theorem over some small real quadratic fields*. Algebra Number Theory **9**(2015), no. 4, 875–895.

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

[13] F. H. Hao and C. J. Parry, *The Fermat equation over quadratic fields*. J. Number Theory **19**(1984), no. 1, 115–130.

[14] M. Ibrahim, *Modular and reciprocity approaches to a family of Diophantine equations*. Ph.D. thesis, University of Warwick, 2009.

[15] A. Kraus, *Sur le théorème de Fermat sur $\mathbb{Q}(\sqrt{5})$. Ann. Math. Qué.* **39**(2015), no. 1, 49–59.

[16] R. D. Mauldin, *A generalization of Fermat's Last Theorem: the Beal conjecture and prize problem*. Notices Amer. Math. Soc. **44**(1997), no. 11, 1436–1437.

[17] J. Neukirch, *Algebraic number theory*, Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 322, Springer, Berlin, 1999, translated from the 1992 German original and with a note by Norbert Schappacher, with a foreword by G. Harder.

[18] J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics, 7, Springer, New York–Heidelberg, 1973, translated from the French.

[19] R. Taylor and A. Wiles, *Ring-theoretic properties of certain Hecke algebras*. Ann. of Math. (2) **141**(1995), no. 3, 553–572.

[20] The LMFDB Collaboration, *The L-functions and modular forms database*, 2022. http://www.lmfdb.org.

[21] J. Voight, *Quaternion algebras*, Graduate Texts in Mathematics, 288, Springer, Cham, 2021.

[22] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*. Ann. of Math. (2) **141**(1995), no. 3, 443–551.

Department of Mathematics, Simon Fraser University Burnaby, BC V5A 1S6, Canada
e-mail: ichen@sfu.ca aisosa_efemwonkieke@sfu.ca david_sun_2@sfu.ca

https://doi.org/10.4153/S0008414X22000633 Published online by Cambridge University Press