Zeitschrift: Commentarii Mathematici Helvetici
Herausgeber: Schweizerische Mathematische Gesellschaft
Band: 93 (2018)
Heft: 2

Artikel: On the asymptotic Fermat's last theorem over number fields
Autor: engün, Mehmet Haluk / Siksek, Samir
DOI: https://doi.org/10.5169/seals-781067

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 21.01.2026

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Comment. Math. Helv. 93 (2018), 359–375
DOI 10.4171/CMH/437

Commentarii Mathematici Helvetici
© Swiss Mathematical Society

On the asymptotic Fermat's last theorem over number fields

Mehmet Haluk Şengün and Samir Siksek

Abstract. Let K be a number field, S be the set of primes of K above 2 and T the subset of primes above 2 having inertial degree 1. Suppose that $T \neq \emptyset$, and moreover, that for every solution (λ, μ) to the S-unit equation

$$\lambda + \mu = 1, \quad \lambda, \mu \in \mathcal{O}_S^\times,$$

there is some $\mathfrak{P} \in T$ such that $\max\{\upsilon_{\mathfrak{P}}(\lambda), \upsilon_{\mathfrak{P}}(\mu)\} \leq 4\upsilon_{\mathfrak{P}}(2)$. Assuming two deep but standard conjectures from the Langlands programme, we prove the asymptotic Fermat's last theorem over K: there is some B_K such that for all prime exponents $p > B_K$ the only solutions to $x^p + y^p + z^p = 0$ with $x, y, z \in K$ satisfy $xyz = 0$. We deduce that the asymptotic Fermat's last theorem holds for imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ with $-d \equiv 2, 3 \pmod 4$ squarefree.

Mathematics Subject Classification (2010). 11D41, 11F80.

Keywords. Fermat equation, Bianchi modular forms, Galois representations.

1. Introduction

Dickson, in his *History of the theory of numbers* [7, pp. 758 and 768], gives a survey of early work on the Fermat equation over number fields, with the earliest reference being to the work of Maillet (1897). Over a period of almost a century, number theorists have intermittently sought extensions of Kummer's cyclotomic approach to the setting of number fields. Perhaps the most satisfying work in that direction is that of Hao and Parry [12], who prove several results on the Fermat equation over quadratic fields subject to a regularity condition on the prime exponent p (as for $\mathbb{Q}$ one does not know how to prove that there are infinitely many regular primes).

In view of Wiles' remarkable proof of Fermat's last theorem, it is now more natural to attack the Fermat equation over number fields via Frey curves and modularity. Jarvis and Meekin [13] did just this, proving Fermat's last theorem over $\mathbb{Q}(\sqrt{2})$. They were followed by Freitas and Siksek [9] who proved Fermat's last theorem for various real quadratic fields of small discriminant. In another work, Freitas and Siksek [8] proved the asymptotic version of Fermat's last theorem (explained below)

for totally real fields satisfying some auxiliary conditions. Key to these successes is the extraordinary progress in modularity over totally real fields, due to the efforts of Barnett-Lamb, Breuil, Diamond, Gee, Geraghty, Kisin, Skinner, Taylor, Wiles, and others. Alas our understanding of modularity (or automorphy) in the setting of general number fields is largely conjectural. One can ask if it is possible to replicate the aforementioned successes for the Fermat equation over general number fields, by assuming standard conjectures. The purpose of this paper is to address this question, and to highlight additional challenges that arise in the general number field setting.

Let K be an algebraic number field. To keep this Introduction self-contained we relegate the precise statements of the two conjectures we assume to later sections, and now only briefly indicate what they are.

- Conjecture 3.1: this is a weak version of Serre's modularity conjecture ([11]) for odd, irreducible, continuous 2-dimensional mod p representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$ that are finite flat at every prime over p.
- Conjecture 4.1: this is a conjecture in the Langlands Programme (see [27]) which says that every weight 2 newform (for GL_2) over K with integer Hecke eigenvalues has an associated elliptic curve over K or a fake elliptic curve over K.

To state our main result, we need to set up some notation. Write $\mathbb{Z}_K$ for the ring of integers of K. Let S for the set of primes $\mathfrak{P}$ of $\mathbb{Z}_K$ above 2, and let T be the subset of $\mathfrak{P} \in S$ with inertial degree 1 (or equivalently with residue class field $\mathbb{F}_2$). We consider the Fermat equation

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

with $x, y, z \in K$ and prime exponent p. We say that a solution $(x, y, z) = (a, b, c) \in K^3$ is non-trivial if $abc \neq 0$.

Theorem 1.1. *Let K be a number field for which Conjectures 3.1 and 4.1 hold. Let S, T be as above and suppose $T \neq \emptyset$. Write $\mathcal{O}_S^\times$ for the set of S-units of K. Suppose that for every solution (λ, μ) to the S-unit equation*

$$\lambda + \mu = 1, \quad \lambda, \mu \in \mathcal{O}_S^\times. \tag{1.2}$$

there is some $\mathfrak{P} \in T$ that satisfies $\max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\} \leq 4\upsilon_{\mathfrak{P}}(2)$. Then the asymptotic Fermat's last theorem holds for K: there is some constant B_K such that the Fermat equation (1.1) *has no non-trivial solutions with prime exponent $p > B_K$.*

1.1. Differences from the totally real case. The reader comparing the statement of our Theorem 1.1 with that of Theorem 3 of Freitas and Siksek [8] may incorrectly (but understandably) presume that the proof is largely the same. In fact, in addition to making use of ideas in [8] we need to deal with following two additional challenges that do not arise in the totally real case.

(i) For a general number field K, Serre's modularity conjecture relates a representation $G_K \to \mathrm{GL}_2(\mathbb{F}_p)$, subject to certain conditions, to a mod p eigenform of weight 2 over K. If K is totally real, such a mod p eigenform lifts to a complex eigenform over K; this is not generally the case for a number field K with complex embeddings. We show that this difficulty is circumvented in our asymptotic Fermat setting where the prime exponent p is assumed to be sufficiently large. This step makes the constant B_K in Theorem 1.1 ineffective, in contrast to the totally real case. To make this effective we would need effective bounds for the size of torsion subgroups of integral cohomology groups associated to certain locally symmetric spaces (see Section 2.1).

(ii) If K has a real embedding, then a weight 2 complex eigenform over K with rational eigenvalues conjecturally corresponds to an elliptic curve over K. This is not true if K is totally complex; the eigenform does sometimes correspond to a fake elliptic curve. A careful study of images of inertia at primes $\mathfrak{P} \in T$ of the mod p representation of the Frey curve shows that they are incompatible with images of inertia for fake elliptic curves.

1.2. An octic example. We stress that S-unit equations have finitely many solutions and that there is a practical algorithm for determining these solutions; see for example [26]. Thus the criterion in Theorem 1.1 is algorithmically testable. To illustrate this, take $K = \mathbb{Q}(\zeta_{16})$ where ζ_{16} is a primitive 16th root of unity. Then K is a totally complex number field of degree 8. Let $\mathfrak{P} = (1 - \zeta_{16}) \cdot \mathbb{Z}_K$. Then $2\mathbb{Z}_K = \mathfrak{P}^8$. It follows that $S = T = \{\mathfrak{P}\}$. Smart [25, Section 5] determines the solutions to the S-unit equation (1.2) for this particular field and finds that there are precisely 795 solutions (λ, μ). It turns out that the largest possible value of $\max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\}$ is 22, which is smaller than $4\upsilon_{\mathfrak{P}}(2) = 32$. By Theorem 1.1, assuming Conjectures 3.1 and 4.1, the asymptotic Fermat's last theorem holds for K.

1.3. Imaginary quadratic fields. Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field, where d is a squarefree positive integer. If $-d \equiv 5 \pmod 8$ then 2 is inert in K and so $T = \emptyset$ and Theorem 1.1 does not apply. If $-d \equiv 1 \pmod 8$ then 2 splits in K and if $-d \equiv 2$ or $3 \pmod 4$ then it ramifies. Here we consider the particularly simple case of $-d \equiv 2$ or $3 \pmod 4$.

Theorem 1.2. *Let $K = \mathbb{Q}(\sqrt{-d})$ be an imaginary quadratic field with where d is a squarefree positive integer satisfying $-d \equiv 2$ or $3 \pmod 4$. Assume Conjectures 3.1 and 4.1. Then the asymptotic Fermat's last theorem holds for K.*

Proof. Note that $S = T = \{\mathfrak{P}\}$ where $\mathfrak{P}^2 = 2\mathbb{Z}_K$. Suppose first that $d > 2$. The assumptions ensure that the only units in K are ± 1. If $\mathfrak{P} = (a + b\sqrt{-d})$ is principal then $a^2 + db^2 = 2$ giving a contradiction. Thus $\mathfrak{P}$ is not principal. Hence if (λ, μ) is any solution to the S-unit equation (1.2) then $\lambda = \pm 2^r$, $\mu = \pm 2^s$ with $r, s \in \mathbb{Z}$. We quickly deduce that $(\lambda, \mu) = (2, -1)$ or $(-1, 2)$ or $(1/2, 1/2)$. In particular,

all solutions satisfy $\max\{|\upsilon_{\mathfrak{P}}(\lambda)|, |\upsilon_{\mathfrak{P}}(\mu)|\} \leq 4\upsilon_{\mathfrak{P}}(2)$. The proof is complete by Theorem 1.1 for $d > 2$. The cases $d = 1, 2$ are similar. □

It is straightforward, though somewhat lengthy, to adapt the method of [8, Sections 6–7] to deduce that the asymptotic Fermat's last theorem holds for 5/6 of imaginary quadratic fields, assuming Conjectures 3.1 and 4.1.

We are indebted to the referee for suggesting several corrections.

2. Eigenforms for GL_2 over number fields

In this section, we discuss modular forms, both complex and mod p, from a perspective that will be most useful for us. Let K be an algebraic number field with ring of integers $\mathbb{Z}_K$ and signature (r, s). Let $\widehat{\mathbb{Z}}_K$ be the finite adèles of $\mathbb{Z}_K$ and let $\mathbb{A}_K, \mathbb{A}_K^f$ denote the rings of adèles and of finite adèles of K, respectively. We let $\mathcal{H}_2^{\pm}$ denote the union of the upper and lower half planes and $\mathcal{H}_3$ denote the hyperbolic 3-space. Then $\mathrm{GL}_2(K)$ acts on $X = \left(\mathcal{H}_2^{\pm}\right)^r \times \mathcal{H}_3^s$ via the embedding

$$\mathrm{GL}_2(K) \hookrightarrow \mathrm{GL}_2(K \otimes \mathbb{R}) \simeq \mathrm{GL}_2(\mathbb{R})^r \times \mathrm{GL}_2(\mathbb{C})^s.$$

Fix an ideal $\mathfrak{N} \subseteq \mathbb{Z}_K$ and define the compact open subgroup

$$U_0(\mathfrak{N}) := \left\{\gamma \in \mathrm{GL}_2(\widehat{\mathbb{Z}}_K) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod \mathfrak{N}\right\}.$$

Consider the adelic locally symmetric space

$$Y_0(\mathfrak{N}) = \mathrm{GL}_2(K)\backslash\left(\left(\mathrm{GL}_2(\mathbb{A}_K^f)/U_0(\mathfrak{N})\right) \times X\right).$$

This space is a disjoint union of Riemannian $(2r + 3s)$-folds

$$Y_0(\mathfrak{N}) = \bigsqcup_{j=1}^{h} \Gamma_j \backslash X$$

where Γ_j are arithmetic subgroups of $\mathrm{GL}_2(K)$, with Γ_1 being the usual congruence subgroup $\Gamma_0(\mathfrak{N})$ of the modular group $\mathrm{GL}_2(\mathbb{Z}_K)$, and h is the class number of K.

For $i \in \{0, \ldots, 2r + 3s\}$, consider the ith cohomology group $H^i(Y_0(\mathfrak{N}), \mathbb{C})$. For every prime $\mathfrak{q}$ coprime to the level $\mathfrak{N}$, we can construct a linear endomorphism $T_{\mathfrak{q}}$ of $H^i(Y_0(\mathfrak{N}), \mathbb{C})$ (called a Hecke operator) and these operators commute with each other. We let $\mathbb{T}_{\mathbb{C}}^{(i)}(\mathfrak{N})$ denote the commutative $\mathbb{Z}$-algebra generated by these Hecke operators inside the endomorphism algebra of $H^i(Y_0(\mathfrak{N}), \mathbb{C})$.

For the purposes of this paper, a *(weight 2) complex eigenform f over K of degree i and level* $\mathfrak{N}$ is a ring homomorphism $\mathfrak{f}\colon \mathbb{T}_{\mathbb{C}}^{(i)}(\mathfrak{N}) \to \mathbb{C}$. Note that the values

of $\mathfrak{f}$ are algebraic integers and they generate a number field which we shall denote $\mathbb{Q}_{\mathfrak{f}}$. We shall call a complex eigenform *trivial* if we have $\mathfrak{f}(T_{\mathfrak{q}}) = \pm(\mathbf{N}\mathfrak{q} + 1)$ for all primes $\mathfrak{q}$ coprime to the level[1]. We call two complex eigenforms $\mathfrak{f}, \mathfrak{g}$ with possibly different degrees and levels *equivalent* if $\mathfrak{f}(T_{\mathfrak{q}}) = \mathfrak{g}(T_{\mathfrak{q}})$ for almost all prime ideals $\mathfrak{q}$ (notice that the two Hecke operators $T_{\mathfrak{q}}$ may live in different Hecke algebras). A complex eigenform, say of level $\mathfrak{N}$, is called *new* if it is not equivalent to one whose level is a proper divisor of $\mathfrak{N}$.

Now let p be a rational prime unramified in K and coprime to the level. The cohomology group $H^i(Y_0(\mathfrak{N}), \overline{\mathbb{F}}_p)$ also comes equipped with Hecke operators, still denoted $T_{\mathfrak{q}}$ (we only consider these for primes $\mathfrak{q}$ coprime to $p\mathfrak{N}$). We shall denote the corresponding algebra by $\mathbb{T}^{(i)}_{\overline{\mathbb{F}}_p}(\mathfrak{N})$. A *(weight 2)* mod p *eigenform* θ *over* K *of degree* i *and level* $\mathfrak{N}$ is a ring homomorphism

$$\theta\colon \mathbb{T}^{(i)}_{\overline{\mathbb{F}}_p}(\mathfrak{N}) \to \overline{\mathbb{F}}_p.$$

2.1. Lifting mod p eigenforms. We say that a mod p eigenform θ, say of level $\mathfrak{N}$, lifts to a complex eigenform if there is a complex eigenform $\mathfrak{f}$ of the same degree and level and a prime ideal $\mathfrak{p}$ of $\mathbb{Q}_{\mathfrak{f}}$ over p such that for every prime $\mathfrak{q}$ of K coprime to $p\mathfrak{N}$ we have $\theta(T_{\mathfrak{q}}) \equiv \mathfrak{f}(\overline{T_{\mathfrak{q}}}) \pmod{\mathfrak{p}}$.

A very intriguing aspect of the theory is that in general mod p eigenforms do not lift to complex ones. The obstruction to lifting is given by p-torsion in the integral cohomology as we now explain. The long exact sequence associated to the multiplication-by-p short exact sequence

$$0 \to \mathbb{Z} \xrightarrow{\cdot p} \mathbb{Z} \to \mathbb{F}_p \to 0$$

gives rise to the following short exact sequences

$$0 \to H^i(Y_0(\mathfrak{N}), \mathbb{Z}) \otimes \mathbb{F}_p \to H^i(Y_0(\mathfrak{N}), \mathbb{F}_p) \to H^{i+1}(Y_0(\mathfrak{N}), \mathbb{Z})[p] \to 0,$$

where $H^{i+1}(Y_0(\mathfrak{N}), \mathbb{Z})[p]$ denotes the p-torsion subgroup of $H^{i+1}(Y_0(\mathfrak{N}), \mathbb{Z})$. Hence we see that p-torsion of $H^{i+1}(Y_0(\mathfrak{N}), \mathbb{Z})$ vanishes if and only if the reduction map from $H^i(Y_0(\mathfrak{N}), \mathbb{Z})$ to $H^i(Y_0(\mathfrak{N}), \mathbb{F}_p)$ is surjective. Now, the existence of an eigenform (complex or mod p) is equivalent to the existence of a class in the corresponding cohomology group that is a simultaneous eigenvector for the Hecke operators such that its eigenvalues match the values of the eigenform. With this interpretation, we can utilize the lifting lemmas of Ash and Stevens [1, Section 1.2] and deduce that every mod p eigenform of degree i lifts to a complex one when $H^j(Y_0(\mathfrak{N}), \mathbb{Z})$ for $j = i, i+1$ have no p-torsion.

The integral cohomology groups $H^i(Y_0(\mathfrak{N}), \mathbb{Z})$ are well known to be finitely generated. Thus for a given level $\mathfrak{N}$, there are only finitely many primes p for which

[1]In the setting of GL_2, non-triviality amounts to cuspidality.

there is an i such that $H^i(Y_0(\mathfrak{N}), \mathbb{Z})[p]$ is non-trivial. We obtain the following easy corollary which is crucial for our paper.

Proposition 2.1. *There is a constant B, depending only on $\mathfrak{N}$, such that for any prime $p > B$, every* mod p *eigenform of level $\mathfrak{N}$ lifts to a complex one.*

3. Mod p Galois representations

We will be using the following very special case of Serre's modularity conjecture over number fields. This conjecture concerns the modularity of 2-dimensional mod p Galois representations. While it is easy to predict the level and the Nebentypus of the sought after mod p eigenform (Serre's original recipe [22] is still applicable), predicting all the possible weights (which actually is a completely local issue) is a very difficult task. A general weight recipe for GL_2 over number fields was given[2] by Buzzard, Diamond and Jarvis [3] (see also [2, Section 6] and [11]). However we shall not need the full strength of their conjecture; the mod p Galois representations that we shall encounter in this paper are of a very special type, namely finite flat at every prime over p, and for such representations it is well-known that (again going back to Serre's original work) we should expect the trivial Serre weight (which we called "weight 2" in this paper) among the possible weights. This is sufficient for our purposes.

Recall that for every real embedding $\sigma\colon K \hookrightarrow \mathbb{R}$ and every extension $\tau\colon \overline{K} \to \mathbb{C}$ of σ, we obtain a *complex conjugation* $\tau^{-1} \circ c \circ \tau \in G_K$, where $\langle c \rangle = \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. We say that $\overline{\rho}\colon G_K \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ is *odd* if the determinant of every complex conjugation is -1. If K is totally complex, we will regard $\overline{\rho}$ automatically as odd.

Conjecture 3.1. *Let $\overline{\rho}\colon G_K \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ be an odd, irreducible, continuous representation with Serre conductor $\mathfrak{N}$ (prime-to-p part of its Artin conductor) and trivial character (prime-to-p part of* $\det(\overline{\rho})$*). Assume that p is unramified in K and that $\overline{\rho}|_{G_{K_\mathfrak{p}}}$ arises from a finite-flat group scheme over $\mathbb{Z}_{K_\mathfrak{p}}$ for every prime $\mathfrak{p}|p$. Then there is a (weight 2)* mod p *eigenform θ over K of level $\mathfrak{N}$ such that for all primes $\mathfrak{q}$ coprime to $p\mathfrak{N}$, we have*

$$\mathrm{Tr}(\overline{\rho}(\mathrm{Frob}_\mathfrak{q})) = \theta(T_\mathfrak{q}).$$

4. Motives attached to complex eigenforms

Recall that a simple abelian surface A over K whose algebra $\mathrm{End}_K(A) \otimes_\mathbb{Z} \mathbb{Q}$ of K-endomorphisms is an indefinite division quaternion algebra D over $\mathbb{Q}$ is commonly

[2]Originally given for totally real fields but as the problem of weights is a local issue, their recipe applies to any number field.

called a *fake elliptic curve*. The field of definition of a fake elliptic curve is necessarily totally complex.

Let A/K be a fake elliptic curve and let p be a prime of good reduction for A. Consider the representation $\sigma_{A,p}\colon G_K \longrightarrow \mathrm{GL}_4(\mathbb{Z}_p)$ coming from the p-adic Tate module $T_p(A)$ of A. Let $\mathcal{O}$ denote $\mathrm{End}_K(A)$ viewed as an order in D. Assume that p splits D and denote $\mathcal{O} \otimes \mathbb{Z}_p$ by $\mathcal{O}_p$. Then $\mathcal{O}$ acts on $T_p(A)$ via endomorphisms and moreover $T_p(A) \simeq \mathcal{O}_p$ as a left $\mathcal{O}$ module. Consequently $\mathrm{Aut}_{\mathcal{O}_p}(T_p(A)) \cong \mathcal{O}_p^\times$, giving us a 2-dimensional representation.

$$\rho_{A,p}\colon G_K \longrightarrow \mathcal{O}_p^\times \simeq \mathrm{GL}_2(\mathbb{Z}_p). \tag{4.1}$$

By a theorem of Ohta [21], we have $\sigma_{A,p} \simeq \rho_{A,p} \oplus \rho_{A,p}$. It is the 2-dimensional representation $\rho_{A,p}$ that will be of interest to us.

The following is a very special case of a fundamental conjecture of the Langlands Programme [5,27] which asserts the existence of motives associated to cohomological automorphic representations.

Conjecture 4.1. *Let $\mathfrak{f}$ be a (weight 2) complex eigenform over K of level $\mathfrak{N}$ that is non-trivial and new. If K has some real place, then there exists an elliptic curve $E_\mathfrak{f}/K$, of conductor $\mathfrak{N}$, such that*

$$\#E_\mathfrak{f}(\mathbb{Z}_K/\mathfrak{q}) = 1 + \mathbf{N}\mathfrak{q} - \mathfrak{f}(T_\mathfrak{q}) \quad \textit{for all } \mathfrak{q} \nmid \mathfrak{N}. \tag{4.2}$$

If K is totally complex, then there exists either an elliptic curve $E_\mathfrak{f}$ of conductor $\mathfrak{N}$ satisfying (4.2) *or a fake elliptic curve $A_\mathfrak{f}/K$, of conductor $\mathfrak{N}^2$, such that*

$$\#A_\mathfrak{f}(\mathbb{Z}_K/\mathfrak{q}) = \big(1 + \mathbf{N}\mathfrak{q} - \mathfrak{f}(T_\mathfrak{q})\big)^2 \quad \textit{for all } \mathfrak{q} \nmid \mathfrak{N}. \tag{4.3}$$

Finally, we record a standard fact about fake elliptic curves that we shall crucially use later, see [14, Section 3].

Theorem 4.2. *Let A/K be a fake elliptic curve. Then A has potential good reduction everywhere. More precisely, let $\mathfrak{q}$ be a prime of K and consider $A/K_\mathfrak{q}$. There is totally ramified extension $K'/K_\mathfrak{q}$ of degree dividing* 24 *such that A/K' has good reduction.*

5. The Frey curve and the associated mod p Galois representation

For an elliptic curve E over a number field K and a rational prime p we write

$$\overline{\rho}_{E,p}\colon G_K \to \mathrm{Aut}(E[p]) \cong \mathrm{GL}_2(\mathbb{F}_p)$$

for the representation induced by the action of G_K on the p-torsion $E[p]$. We make repeated use of the following lemma.

Lemma 5.1. *Let E be an elliptic curve over K with j-invariant j. Let $p \geq 5$ be a rational prime and write $\overline{\rho} = \overline{\rho}_{E,p}$. Let $\mathfrak{q} \nmid p$ be a prime of K.*

(i) *If $v_{\mathfrak{q}}(j) \geq 0$ (i.e. E has potentially good reduction at $\mathfrak{q}$) then $\#\overline{\rho}(I_{\mathfrak{q}}) \mid 24$.*

(ii) *Suppose $v_{\mathfrak{q}}(j) < 0$ (i.e. E has potentially multiplicative reduction at $\mathfrak{q}$).*

- *If $p \nmid v_{\mathfrak{q}}(j)$ then $\#\overline{\rho}(I_{\mathfrak{q}}) = p$ or $2p$.*
- *If $p \mid v_{\mathfrak{q}}(j)$ then $\#\overline{\rho}(I_{\mathfrak{q}}) = 1$ or 2.*

Proof. For (i) see [16, Introduction]. For (ii) we suppose first that E has split multiplicative reduction at $\mathfrak{q}$. As $\mathfrak{q} \nmid p$ and E is semistable at $\mathfrak{q}$, inertia at $\mathfrak{q}$ acts unipotently on $E[p]$, and thus $\#\overline{\rho}(I_{\mathfrak{q}}) \mid p$. From the theory of the Tate curve [24, Proposition V.6.1], we know that $p \mid \#\overline{\rho}(I_{\mathfrak{q}})$ if and only if $p \nmid v_{\mathfrak{q}}(j)$. This proves (ii) if E has split multiplicative reduction. Suppose now that E has potentially multiplicative reduction. Then E is a quadratic twist of an elliptic curve E' with split multiplicative reduction. Thus $\overline{\rho} = \phi \otimes \overline{\rho'}$, where $\overline{\rho'} = \overline{\rho}_{E',p}$ and ϕ is a quadratic character. Part (ii) follows. □

Let S and T be as in the Introduction. We suppose once and for all that $T \neq \emptyset$. Let p be an odd prime, and let $(a, b, c) \in K^3$ be a non-trivial solution to the Fermat equation (1.1). We scale the solution (a, b, c) so that it is integral. As the class number might not be 1, we cannot suppose that a, b, c are coprime. However, following [8], we may suppose that the ideal generated by a, b, c belongs to a finite set as we now explain. For a non-zero ideal $\mathfrak{a}$ of $\mathbb{Z}_K$, we denote by $[\mathfrak{a}]$ the class of $\mathfrak{a}$ in the class group $\mathrm{Cl}(K)$. Let

$$\mathcal{G}_{a,b,c} := a\mathbb{Z}_K + b\mathbb{Z}_K + c\mathbb{Z}_K \tag{5.1}$$

and let $[a, b, c]$ denote the class of $\mathcal{G}_{a,b,c}$ in $\mathrm{Cl}(K)$. We exploit the well-known fact (e.g. [4, Theorem VIII.4]) that every ideal class contains infinitely many prime ideals. Let $\mathfrak{c}_1, \ldots, \mathfrak{c}_h$ be the ideal classes of K. For each class $\mathfrak{c}_i$, we choose (and fix) a prime ideal $\mathfrak{m}_i \nmid 2$ of smallest possible norm representing $\mathfrak{c}_i$. The set $\mathcal{H}$ denotes our fixed choice of odd prime ideals representing the class group: $\mathcal{H} = \{\mathfrak{m}_1, \ldots, \mathfrak{m}_h\}$. By [8, Lemma 3.2], we may scale (a, b, c) so that it remains integral, but $\mathcal{G}_{a,b,c} \in \mathcal{H}$. We shall henceforth suppose $\mathcal{G}_{a,b,c} = \mathfrak{m} \in \mathcal{H}$. Associated to (a, b, c) is the Frey curve

$$E = E_{a,b,c} : Y^2 = X(X - a^p)(X + b^p). \tag{5.2}$$

We write $\overline{\rho} = \overline{\rho}_{E,p}$.

The following is Lemma 3.7 of [8], but as it is crucial to everything that follows we include a proof here.

Lemma 5.2. *Let $\mathfrak{P} \in T$ and suppose $p > 4v_{\mathfrak{P}}(2)$. Then*

(i) *E has potentially multiplicative reduction at $\mathfrak{P}$;*

(ii) *$p \mid \#\overline{\rho}(I_{\mathfrak{P}})$ where $I_{\mathfrak{P}}$ denotes the inertia subgroup of G_K at $\mathfrak{P}$.*

Proof. Since $\mathcal{G}_{a,b,c} = \mathfrak{m} \nmid 2$, we know $\mathfrak{P}$ divides at most one of a, b, c. By definition of T, the residue field of $\mathfrak{P}$ is $\mathbb{F}_2$. If $\mathfrak{P} \nmid abc$ then

$$0 = a^p + b^p + c^p \equiv 1 + 1 + 1 \pmod{\mathfrak{P}},$$

giving a contradiction. We see that $\mathfrak{P}$ divides precisely one of a, b, c. We permute a, b, c so that $\mathfrak{P} \mid b$; such a permutation corresponds to twisting E by ± 1, and so does not affect j. Now the expression for j in terms of a, b, c is

$$j = 2^8 \cdot \frac{(b^{2p} - a^p c^p)^3}{a^{2p} b^{2p} c^{2p}}. \tag{5.3}$$

It follows that $\upsilon_{\mathfrak{P}}(j) = 8\upsilon_{\mathfrak{P}}(2) - 2p\upsilon_{\mathfrak{P}}(b)$. As $p > 4\upsilon_{\mathfrak{P}}(2)$ we have that $\upsilon_{\mathfrak{P}}(j) < 0$ and so E has potentially multiplicative reduction at $\mathfrak{P}$. Moreover, $p \nmid \upsilon_{\mathfrak{P}}(j)$. The lemma follows from Lemma 5.1. □

Lemma 5.3. *Suppose $p \geq 5$ and $\mathfrak{m} \nmid p$. Then $\#\overline{\rho}(I_{\mathfrak{m}}) \mid 24$.*

Proof. As $\mathcal{G}_{a,b,c} = \mathfrak{m}$ we know that $\upsilon_{\mathfrak{m}}(a)$, $\upsilon_{\mathfrak{m}}(b)$, $\upsilon_{\mathfrak{m}}(c)$ are all positive. Moreover, as $a^p + b^p + c^p = 0$, we have that at least two of $\upsilon_{\mathfrak{m}}(a)$, $\upsilon_{\mathfrak{m}}(b)$, $\upsilon_{\mathfrak{m}}(c)$ are equal. Permuting a, b, c (which twists E by ± 1 and so does not affect the image of inertia at $\mathfrak{m} \nmid 2$) we may suppose

$$\upsilon_{\mathfrak{m}}(a) = \upsilon_{\mathfrak{m}}(c) = k, \quad \upsilon_{\mathfrak{m}}(b) = k + t,$$

where $k \geq 1$ and $t \geq 0$. If $t = 0$ then from (5.3) we have $\upsilon_{\mathfrak{m}}(j) \geq 0$ and so the lemma follows from Lemma 5.1. Thus suppose that $t \geq 1$. Then $\upsilon_{\mathfrak{m}}(j) = -2pt$ and so by Lemma 5.1 we have $\overline{\rho}(I_{\mathfrak{m}}) = 1$ or 2, completing the proof. □

Lemma 5.4. *The Frey curve E is semistable away from $S \cup \{\mathfrak{m}\}$, where $\mathfrak{m} = \mathcal{G}_{a,b,c}$. Suppose $p \geq 5$ and not divisible by any $\mathfrak{q} \in S \cup \{\mathfrak{m}\}$. The determinant of $\overline{\rho}$ is the* mod *p cyclotomic character. Its Serre conductor $\mathfrak{N}$ is supported on $S \cup \{\mathfrak{m}\}$ and belongs to a finite set that depends only on the field K. The representation $\overline{\rho}$ is odd (in the sense of Section 3) and is finite flat at every $\mathfrak{q}$ over p.*

Proof. The statement about the determinant is a well-known consequence of the theory of the Weil pairing on $E[p]$. This immediately implies oddness. Let $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$ be a prime of K. Let c_4 and Δ denote the usual invariants of the model E given in (5.2). These are given by the formulae

$$c_4 = 2^4(b^{2p} - a^p c^p), \quad \Delta = 2^4 a^{2p} b^{2p} c^{2p}.$$

It follows from $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$ (together with the relation $a^p + b^p + c^p = 0$) that $\mathfrak{q}$ cannot divide both c_4 and Δ. Thus the given model is minimal, and E is semistable at $\mathfrak{q}$. Moreover, $p \mid \upsilon_{\mathfrak{q}}(\Delta)$. It follows (c.f. [22]) that $\overline{\rho}$ is unramified at $\mathfrak{q}$ if $\mathfrak{q} \nmid p$ and finite flat at $\mathfrak{q}$ if $\mathfrak{q} \mid p$. It remains to show that the set of possible Serre conductors $\mathfrak{N}$

is finite. These can only be divisible by primes $\mathfrak{q} \in S \cup \{\mathfrak{m}\}$. Moreover, $\mathfrak{N}$ divides the conductor N of E, thus $\upsilon_{\mathfrak{q}}(\mathfrak{N}) \leq \upsilon_{\mathfrak{q}}(N) \leq 2 + 3\upsilon_{\mathfrak{q}}(3) + 6\upsilon_{\mathfrak{q}}(2)$ by [24, Theorem IV.10.4]. It follows that the list of possible Serre conductors is finite. Moreover as $\mathfrak{m} \in \mathcal{H}$ and the set $\mathcal{H}$ depends only on K, this list of Serre conductors depends only on K. □

6. Surjectivity of $\overline{\rho}$

To apply Conjecture 3.1 to the mod p representation $\overline{\rho}$ of the Frey curve E, we need to show that $\overline{\rho}$ is absolutely irreducible. We have been unable to find a theorem in the literature that immediately implies this. However, guided by the work of Momose [20], Kraus [18] and David [6] (all relying on Merel's uniform boundedness theorem [19]), we prove the following result which is sufficient for our purpose.

Proposition 6.1. *Let L be a Galois number field and let $\mathfrak{q}$ be a prime of L. There is a constant $B_{L,\mathfrak{q}}$ such that the following is true. Let $p > B_{L,\mathfrak{q}}$ be a rational prime. Let E/L be an elliptic curve that is semistable at all $\mathfrak{p} \mid p$ and having potentially multiplicative reduction at $\mathfrak{q}$. Then $\overline{\rho}_{E,p}$ is irreducible.*

Before proving Proposition 6.1 we apply it to the Frey curve.

Corollary 6.2. *Let K be a number field, and suppose (in the notation of the Introduction) that $T \neq \emptyset$. There is a constant C_K such that if $p > C_K$ and $(a, b, c) \in \mathbb{Z}_K^3$ is a non-trivial solution to the Fermat equation with exponent p, and scaled so that $\mathcal{G}_{a,b,c} \in \mathcal{H}$, then $\overline{\rho}_{E,p}$ is surjective, where E is the Frey curve given in* (5.2).

Proof. We know from Lemma 5.2 that E has potentially multiplicative reduction at $\mathfrak{P} \in T$. Moreover, from the proof of Lemma 5.4, we know that E is semistable away from the primes above 2 and those contained in $\mathcal{H}$. Let L be the Galois closure of K, and let $\mathfrak{q}$ be a prime of L above $\mathfrak{P}$. Applying Proposition 6.1 we see that there is a constant $B_{L,\mathfrak{q}}$ such that for $p > B_{L,\mathfrak{q}}$ we have that $\overline{\rho}_{E,p}(G_L)$ is irreducible. Now $\mathfrak{q} \mid \mathfrak{P} \mid 2$ and so $B_{L,\mathfrak{q}}$ depends only on K and we denote it by C_K. We enlarge C_K if needed so that for $C_K > 4\upsilon_{\mathfrak{P}}(2)$. It follows from Lemma 5.2 that the image of $\overline{\rho}_{E,p}$ contains an element of order p. Any subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ that contains an element of order p is either reducible or contains $\mathrm{SL}_2(\mathbb{F}_p)$. It follows for $p > C_K$ that the image in fact contains $\mathrm{SL}_2(\mathbb{F}_p)$. Moreover, again enlarging C_K if necessary, we may suppose that $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$ for $p > C_K$. Thus $\chi_p = \det(\overline{\rho}_{E,p})$ is surjective, completing the proof. □

6.1. Proof of Proposition 6.1. Suppose $\overline{\rho}_{E,p}$ is reducible. Thus,

$$\overline{\rho}_{E,p} \sim \begin{pmatrix} \lambda & * \\ 0 & \lambda' \end{pmatrix}, \tag{6.1}$$

where λ, $\lambda' \colon G_L \to \mathbb{F}_p^*$ are characters, and $\lambda\lambda' = \det(\overline{\rho}_{E,p}) = \chi_p$ is the mod p cyclotomic character. We suppose from now on that p is unramified in L and that E is semistable at all $\mathfrak{p} \mid p$.

Lemma 6.3. *Write $\sigma_{\mathfrak{q}} \in G_L$ for a Frobenius element at $\mathfrak{q}$. Then $\lambda^2(\sigma_{\mathfrak{q}})$, $\lambda'^2(\sigma_{\mathfrak{q}})$ are (up to reordering) congruent to* 1, $\mathrm{Norm}(\mathfrak{q})^2$ *modulo p.*

Proof. Write $D_{\mathfrak{q}}$ for the decomposition subgroup at $\mathfrak{q}$. As E has potentially multiplicative reduction at $\mathfrak{q}$, we know that $\overline{\rho}_{E,p}|_{D_{\mathfrak{q}}}$ is up to semisimplification equal to $\phi \oplus \phi \cdot \chi_p$, where ϕ is at worst a quadratic character. The lemma follows since $\chi_p(\sigma_{\mathfrak{q}}) \equiv \mathrm{Norm}(\mathfrak{q}) \pmod{p}$. □

From (6.1), there is a non-zero $P \in E[p]$ such that $\sigma(P) = \lambda(\sigma)P$ for $\sigma \in G_K$. Replacing E by p-isogenous $E/\langle P\rangle$ results in swapping the two characters λ, λ' in (6.1). This allows us to suppose from now on that $\lambda^2(\sigma_{\mathfrak{q}}) \equiv 1 \pmod{p}$.

Lemma 6.4. *The character λ^{12} is unramified away from the primes above p. Let $\mathfrak{p} \mid p$ be a prime of K. Then*

$$\lambda^{12}|_{I_{\mathfrak{p}}} = \left(\chi_p|_{I_{\mathfrak{p}}}\right)^{s_{\mathfrak{p}}},$$

where $s_{\mathfrak{p}} \in \{0, 12\}$.

Proof. The first part of the lemma is Proposition 1.4 and 1.5 of [6]. The second part is derived in [10, Proposition 2.1] from results found in [6]. □

Now let $G = \mathrm{Gal}(L/\mathbb{Q})$. As $L/\mathbb{Q}$ is Galois, G acts transitively on the primes $\mathfrak{p} \mid p$. Write $\mathfrak{p}_0 \mid p$. For $\tau \in G$ we write $s_\tau \in \{0, 12\}$ for the integer $s_{\mathfrak{p}}$ associated to $\mathfrak{p} = \tau^{-1}(\mathfrak{p}_0)$ in Lemma 6.4.

Lemma 6.5 (David [6, Proposition 2.6]). *Let $\alpha \in L$ be non-zero. Suppose $\upsilon_{\mathfrak{p}}(\alpha) = 0$ for all $\mathfrak{p} \mid p$. Then*

$$\prod_{\tau \in G} \tau(\alpha)^{s_\tau} \equiv \prod \left(\lambda^{12}(\sigma_{\mathfrak{r}})\right)^{\upsilon_{\mathfrak{r}}(\alpha)} \pmod{\mathfrak{p}_0},$$

where the product on the right-hand side is taken over all prime $\mathfrak{r}$ in the support of α.

We now choose a positive integer r so that $\mathfrak{q}^r$ is principal and write $\alpha\mathbb{Z}_L = \mathfrak{q}^r$. Since $\lambda^{12}(\sigma_{\mathfrak{q}}) = 1$ we see that

$$\prod_{\tau \in G} \tau(\alpha)^{s_\tau} \equiv 1 \pmod{\mathfrak{p}_0}.$$

The left-hand side belongs to a finite set $\mathcal{A}$ that depends only on L and $\mathfrak{q}$, since $s_\tau = 0$ or 12 for any $\tau \in G$. Moreover, if we denote the left-hand side by β then p divides $\mathrm{Norm}(\mathfrak{p}_0)$ which in turn divides $\mathrm{Norm}(\beta - 1)$. We choose $B_{L,\mathfrak{q}} > \mathrm{Norm}(\beta - 1)$ for all $\beta \in \mathcal{A}$ with $\beta \neq 1$. Then for $p > B_{L,\mathfrak{q}}$ we deduce that $\beta = 1$. Thus $s_\tau = 0$

for all $\tau \in G$. It follows from Lemma 6.4 that the character λ^{12} is unramified at all places of L. Hence there is an extension M/L of degree $12 \cdot h_L$ where h_L is the class number of L such that $\lambda|_{G_M} = 1$. It follows from (6.1) that E has a point of order p over M. Finally applying Merel's uniform boundedness theorem [19], shows that p is bounded by a constant that depends only on the degree $[M : \mathbb{Q}] = 12 \cdot h_L \cdot [L : \mathbb{Q}]$ completing the proof.

7. Applying the conjectures

This section is devoted to the proof of the following proposition.

Proposition 7.1. *Let K be a number field. Assume Conjectures 3.1 and 4.1. Suppose, in the notation of Section 5, that $T \neq \emptyset$. Then there is a constant B_K depending only on K such that the following holds. Let $(a, b, c) \in \mathbb{Z}_K^3$ being a non-trivial solution to the Fermat equation with exponent $p > B_K$, and we suppose that it is scaled so that $\mathcal{G}_{a,b,c} = \mathfrak{m} \in \mathcal{H}$. Let E/K be the associated Frey curve defined in (5.2). Then there is an elliptic curve E'/K such that the following hold:*

(i) *E' has good reduction away from $S \cup \{\mathfrak{m}\}$, and potentially good reduction away from S.*

(ii) *E' has full 2-torsion.*

(iii) $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$.

(iv) *for $\mathfrak{P} \in T$ we have $\upsilon_{\mathfrak{P}}(j') < 0$ where j' is the j-invariant of E'.*

Assume the hypotheses of the proposition. We suppose that p is suitably large, and so by Corollary 6.2, the representation $\overline{\rho}_{E,p}$ is surjective. We now apply Conjecture 3.1 and deduce the existence of a weight 2 mod p eigenform θ over K of level $\mathfrak{N}$, with $\mathfrak{N}$ as in Lemma 5.4, such that for all primes $\mathfrak{q}$ coprime to $p\mathfrak{N}$, we have

$$\mathrm{Tr}\left(\overline{\rho}_{E,p}(\mathrm{Frob}_{\mathfrak{q}})\right) = \theta(T_{\mathfrak{q}}).$$

Since there are only finitely many possible levels $\mathfrak{N}$, see Lemma 5.4, we can take p large enough to guarantee that, see Proposition 2.1, for any level $\mathfrak{N}$, there will be a weight 2 complex eigenform $\mathfrak{f}$ with level $\mathfrak{N}$ that is a lift of θ. Observe that the list of such eigenforms $\mathfrak{f}$ is finite and depends only on K (and not on p or the solution (a, b, c)). Thus every constant that depends later of these eigenforms depends only on K.

Next we show that if p is sufficiently large then $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$. The idea here is due to Mazur, though apparently unpublished. It can be found in [23, Section 9].

Lemma 7.2. *Suppose $\mathbb{Q}_{\mathfrak{f}} \neq \mathbb{Q}$. There is a constant $C_{\mathfrak{f}}$ depending only on $\mathfrak{f}$ such that $p < C_{\mathfrak{f}}$.*

Proof. Choose and fix a prime $\mathfrak{q}$ of K such that $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$ and $\mathfrak{f}(T_\mathfrak{q}) \notin \mathbb{Q}$. If $\mathfrak{q} \mid p$ then $p \mid \mathrm{Norm}(\mathfrak{q})$ and so p is bounded. Thus we may suppose that $\mathfrak{q} \nmid p$. Now E has either good or multiplicative reduction at $\mathfrak{q}$ (since E is semistable away from the primes in $S \cup \{\mathfrak{m}\}$). Note that

$$\mathrm{Tr}\left(\overline{\rho}_{E,p}(\mathrm{Frob}_\mathfrak{q})\right) = \begin{cases} \pm\big(\mathrm{Norm}(\mathfrak{q}) + 1\big) & \text{if } E \text{ has multiplicative reduction at } \mathfrak{q}, \\ a_\mathfrak{q}(E) & \text{if } E \text{ has good reduction at } \mathfrak{q}. \end{cases}$$

In particular, this trace belongs to a finite list of rational integers that depends only on $\mathfrak{q}$. However, there is prime ideal $\mathfrak{p}$ of $\mathbb{Q}_\mathfrak{f}$ over p such that

$$\mathrm{Tr}\left(\overline{\rho}_{E,p}(\mathrm{Frob}_\mathfrak{q})\right) \equiv \mathfrak{f}(T_\mathfrak{q}) \pmod{\mathfrak{p}}.$$

As $\mathfrak{f}(T_\mathfrak{q}) \notin \mathbb{Q}$, the difference between the two sides is non-zero and belongs to a finite set. As $\mathfrak{p} \mid p$, the norm of the difference is divisible by p. This gives an upper bound on p that depends only on $\mathfrak{f}$. □

Note that if $\mathbb{Q}_\mathfrak{f} = \mathbb{Q}$ then the above argument fails as the difference might be zero.

By supposing that p is sufficiently large, we may henceforth suppose that $\mathbb{Q}_\mathfrak{f} = \mathbb{Q}$. The fact that $\overline{\rho}_{E,p}$ is irreducible implies that $\mathfrak{f}$ is non-trivial. If $\mathfrak{f}$ is not new, we replace it with an equivalent new eigenform that is of smaller level. Thus we can assume that $\mathfrak{f}$ is new and has level $\mathfrak{N}'$ dividing $\mathfrak{N}$. By Conjecture 4.1, $\mathfrak{f}$ either has an associated elliptic curve $E_\mathfrak{f}/K$ of conductor $\mathfrak{N}'$, or has an associated fake elliptic curve $A_\mathfrak{f}/K$ of conductor $\mathfrak{N}'^2$.

Lemma 7.3. *If $p > 24$ then $\mathfrak{f}$ has an associated elliptic curve $E_\mathfrak{f}$.*

Proof. This is another point where we make use of our assumption $T \neq \emptyset$. Let $\mathfrak{P} \in T$. We know from Lemma 5.2 that $p \mid \#\overline{\rho}_{E,p}(I_\mathfrak{P})$. If $\mathfrak{f}$ corresponds to a fake elliptic curve $A_\mathfrak{f}$, then it follows from Theorem 4.2 that $\#\overline{\rho}_{A_\mathfrak{f},p}(I_\mathfrak{P}) \leq 24$ where $\rho_{A_\mathfrak{f},p}$ is the 2-dimensional representation defined in (4.1). As $\overline{\rho}_{E,p} \sim \overline{\rho}_{A_\mathfrak{f},p}$ we have a contradiction. □

We may henceforth suppose that $\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p}$ where $E' = E_\mathfrak{f}$ is an elliptic curve of conductor $\mathfrak{N}'$ dividing $\mathfrak{N}$.

Lemma 7.4. *If E' does not have full 2-torsion, and is not 2-isogenous to an elliptic curve with full 2-torsion, then $p \leq C_{E'}$.*

Proof. By Lemma 7.5 (below) there infinitely many primes $\mathfrak{q}$ such that $\#E'(\mathbb{F}_\mathfrak{q}) \not\equiv 0 \pmod 4$. Fix such a prime $\mathfrak{q} \notin S \cup \{\mathfrak{m}\}$. Now if $\mathfrak{q}$ is a prime of good reduction for E, then $\#E(\mathbb{F}_\mathfrak{q}) \equiv E'(\mathbb{F}_\mathfrak{q}) \pmod p$. Note that $\#E(\mathbb{F}_\mathfrak{q})$ is divisible by 4 as the Frey curve E has full 2-torsion. Thus the difference $\#E(\mathbb{F}_\mathfrak{q}) - \#E'(\mathbb{F}_\mathfrak{q})$, which is divisible by p, is non-zero. Moreover, this difference belongs to a finite set depending on $\mathfrak{q}$,

and so p is bounded. We may therefore suppose that E has multiplicative reduction at $\mathfrak{q}$. In this case, comparing traces of Frobenius at $\mathfrak{q}$ we have

$$\pm\big(\mathrm{Norm}(\mathfrak{q}) + 1\big) \equiv a_{\mathfrak{q}}(E') \pmod{p}.$$

Again the difference is non-zero and depends only on $\mathfrak{q}$, giving a bound for p. □

If E' is 2-isogenous to an elliptic curve E'' then (as $p \neq 2$) then the isogeny induces an isomorphism $E'[p] \cong E''[p]$ of Galois modules. Thus,

$$\overline{\rho}_{E,p} \sim \overline{\rho}_{E',p} \sim \overline{\rho}_{E'',p}.$$

Hence we may, after possibly replacing E' by E'', suppose that E' has full 2-torsion. To complete the proof the proposition, we need to show that E' has potentially good reduction at $\mathfrak{m}$, and that $\upsilon_{\mathfrak{P}}(j') < 0$ for $\mathfrak{P} \in T$. Recall by Lemmas 5.2 and 5.3 that $p \mid \#\overline{\rho}_{E,p}(I_{\mathfrak{P}})$ for $\mathfrak{P} \in T$, and that $\#\overline{\rho}_{E,p}(I_{\mathfrak{m}}) \leq 24$. As $\#\overline{\rho}_{E,p}(I_{\mathfrak{P}}) = \#\overline{\rho}_{E',p}(I_{\mathfrak{P}})$ we deduce from Lemma 5.1 that $\upsilon_{\mathfrak{P}}(j') < 0$ for $\mathfrak{P} \in T$. Finally if E' has potentially multiplicative reduction at $\mathfrak{m}$ then for every $p > |\upsilon_{\mathfrak{m}}(j')|$ we have, by Lemma 5.1, that $p \mid \#\overline{\rho}_{E',p}(I_{\mathfrak{m}})$, giving a contradiction for large p.

7.1. 2-torsion of elliptic curves. To complete the proof Lemma 7.4 we need the following result which is stated as a fact in [17, Section 3]. We are grateful to Nicolas Billerey for pointing out that this is a special case of a theorem of Katz [15].

Lemma 7.5. *Let E be an elliptic curve over a number field K. Suppose that $4 \mid \#E(\mathbb{F}_{\mathfrak{q}})$ for all primes $\mathfrak{q}$ of sufficiently large norm. Then either E has full 2-torsion, or it is 2-isogenous to some elliptic curve E' having full 2-torsion.*

Proof. By [15, Theorem 2] there is an elliptic curve E'/K isogenous to E such that $4 \mid \#E'(K)_{\mathrm{tors}}$. If E' has full 2-torsion then we are finished. Otherwise E' has some K-point P of order 4. The points of order 2 on E' are $2P$, Q, R (say) where Q and R are Galois conjugates, related by $R = Q + 2P$. The points of order 2 on the 2-isogenous curve $E'/\langle 2P\rangle$ are $P + \langle 2P\rangle$, $Q + \langle 2P\rangle = R + \langle 2P\rangle$ and $P + Q + \langle 2P\rangle$. These are clearly individually fixed by the action of G_K. □

8. Proof of Theorem 1.1

We apply Proposition 7.1 which yields an elliptic curve E'/K with full 2-torsion and potentially good reduction outside S whose j-invariant j' satisfies $\upsilon_{\mathfrak{P}}(j') < 0$ for all $\mathfrak{P} \in T$. Write

$$E' : Y^2 = X(X - e_1)(X - e_2)$$

with $e_1, e_2 \in \mathbb{Z}_K$. Let $\lambda = e_1/e_2$. Let λ' be any of the following six expressions (which are known as the λ-invariants of E'):

$$\lambda, \quad 1/\lambda, \quad 1-\lambda, \quad 1/(1-\lambda), \quad \lambda/(\lambda-1), \quad (\lambda-1)/\lambda.$$

Then

$$j' = 2^8 \cdot \frac{(\lambda'^2 - \lambda' + 1)^3}{\lambda'^2(1-\lambda')^2}. \tag{8.1}$$

Let $\mathfrak{q} \notin S$ be a prime of K. As E' has potentially good reduction at $\mathfrak{q}$, we know that $v_{\mathfrak{q}}(j') \geq 0$. Thus λ' is the root of a degree six monic polynomial with coefficients that are $\mathfrak{q}$-integral. It immediately follows that $v_{\mathfrak{q}}(\lambda') \geq 0$. This is true for both $\lambda' = \lambda$ and $\lambda' = 1/\lambda$, thus $\lambda \in \mathcal{O}_S^\times$. Moreover, letting $\mu = 1 - \lambda$ we see that $\mu \in \mathcal{O}_S^\times$, hence (λ, μ) is a solution to the the S-unit equation (1.2). Suppose, as in the statement of the theorem, that for every such solution (λ, μ) there some $\mathfrak{P} \in T$ such that

$$t := \max\left\{|v_{\mathfrak{P}}(\lambda)|, |v_{\mathfrak{P}}(\mu)|\right\} \leq v_{\mathfrak{P}}(2).$$

If $t = 0$ then it follows from (8.1) with $\lambda' = \lambda$ that $v_{\mathfrak{P}}(j') > 0$ giving a contradiction. Thus $t > 0$. Now the relation $\lambda + \mu = 1$ forces either

$$v_{\mathfrak{P}}(\lambda) = v_{\mathfrak{P}}(\mu) = -t,$$

or

$$v_{\mathfrak{P}}(\lambda) = 0 \quad \text{and} \quad v_{\mathfrak{P}}(\mu) = t,$$

or

$$v_{\mathfrak{P}}(\lambda) = t \quad \text{and} \quad v_{\mathfrak{P}}(\mu) = 0.$$

Thus

$$v_{\mathfrak{P}}(\lambda\mu) = -2t < 0 \quad \text{or} \quad v_{\mathfrak{P}}(\lambda\mu) = t > 0.$$

But

$$j' = 2^8 \cdot (1 - \lambda\mu)^3 \cdot (\lambda\mu)^{-2},$$

which shows, either way, that $v_{\mathfrak{P}}(j') = 8v_{\mathfrak{P}}(2) - 2t \geq 0$ giving a contradiction. This completes the proof.

References

[1] A. Ash and G. Stevens, Cohomology of arithmetic groups and congruences between systems of Hecke eigenvalues, *J. Reine Angew. Math.*, **365** (1986), 192–220. Zbl 0596.10026 MR 826158

[2] N. Bergeron and A. Venkatesh. The asymptotic growth of torsion homology for arithmetic groups, *J. Inst. Math. Jussieu*, **12** (2013), no. 2, 391–447. Zbl 1266.22013 MR 3028790

[3] K. Buzzard, F. Diamond, and F. Jarvis, On Serre's conjecture for mod ℓ Galois representations over totally real fields, *Duke Math. J.*, **55** (2010), no. 1, 105–161. Zbl 1227.11070 MR 2730374

[4] J. W. S. Cassels and A. Fröhlich (eds.), *Algebraic number theory. Proceedings of the instructional conference held at the University of Sussex, Brighton, 1965*, Academic Press, 1967. MR 911121

[5] L. Clozel, Motifs et formes automorphes: applications du Principe de Fonctorialité, in *Automorphic forms, Shimura varieties, and L-functions (Ann Arbor, Mi, 1988). Vol. I*, 77–159, Perspect. Math. Boston, 10, MA: Academic Press, 1990. Zbl 0705.11029 MR 1044819

[6] A. David, Caractère d'isogénie et critéres d'irréductibilité, 2012. arXiv:1103.3892v2

[7] L. E. Dickson, *History of the theory of numbers, Vol. II*, Chelsea, New York, 1971. Zbl 1214.11002 MR 245500

[8] N. Freitas and S. Siksek, An asymptotic Fermat's last theorem for five-sixths of real quadratic fields, *Compositio Mathematica*, **151** (2015), 1395–1415. Zbl 06484393 MR 3383161

[9] N. Freitas and S. Siksek, Fermat's last theorem for some small real quadratic fields, *Algebra & Number Theory*, **9** (2015), 875–895. Zbl 06442354 MR 3352822

[10] N. Freitas and S. Siksek, Criteria for irreducibility of mod p representations of Frey curves, *J. Théor. Nombres Bordeaux*, **27** (2015), no. 1, 67–76. Zbl 06554398 MR 3346965

[11] T. Gee, F. Herzig, and D. Savitt, General Serre weight conjectures, 2017. arXiv:1509.02527v2

[12] F. H. Hao and C. J. Parry, The Fermat equation over quadratic fields, *J. Number Theory*, **19** (1984), no. 1, 115–130. Zbl 0538.10015 MR 751168

[13] F. Jarvis and P. Meekin, The Fermat equation over $\mathbb{Q}(\sqrt{2})$, *J. Number Theory*, **109** (2004), 182–196. Zbl 1078.11019 MR 2098483

[14] B. Jordan, Points on Shimura curves rational over number fields, *J. Reine Angew. Math.*, **371** (1986), 92–114. Zbl 0587.14018 MR 859321

[15] N. M. Katz, Galois properties of torsion points on abelian varieties, *Invent. Math.*, **62** (1981), 481–502. Zbl 0471.14023 MR 604840

[16] A. Kraus, Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive, *Manuscripta Math.*, **69** (1990), no. 4, 353–385. Zbl 0792.14014 MR 1080288

[17] A. Kraus, Majorations effectives pour l'équation de Fermat généralisée, *Canad. J. Math.*, **49** (1997), no. 6, 1139–1161. Zbl 0908.11017 MR 1611640

[18] A. Kraus, Courbes elliptiques semi-stables sur les corps de nombres, *Int. J. Number Theory*, **3** (2007), 611–633. Zbl 1145.11043 MR 2371778

[19] L. Merel, Bornes pour la torsion des courbes elliptiques sur les corps de nombres, *Invent. Math.*, **124** (1996), 437–449. Zbl 0936.11037 MR 1369424

[20] F. Momose, Isogenies of prime degree over number fields, *Compositio Mathematica*, **97** (1995), 329–348. Zbl 1044.11582 MR 1353278

[21] M. Ohta, On ℓ-adic representations of Galois groups obtained from certain two-dimensional abelian varieties, *J. Fac. Sci. Univ. Tokyo Sect. IA Math.*, **21** (1974), 299–308. Zbl 0317.14019 MR 419368

[22] J.-P. Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *Duke Math. J.*, **54** (1987), 179–230. Zbl 0641.10026 MR 885783

[23] S. Siksek, The modular approach to Diophantine equations, in *Explicit methods in number theory*, 151–179, Panor. Synthèses, 36, Soc. Math. France, Paris, 2012. Zbl 1343.11042 MR 3098134

[24] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, 151, Springer, 1994. Zbl 0911.14015 MR 1312368

[25] N. P. Smart, Determining the small solutions to S-unit equations, *Math. Comp.*, **68** (1999), 1687–1699. Zbl 0935.11053 MR 1653990

[26] N. P. Smart, *The algorithmic resolution of Diophantine equations*, London Mathematical Society Student Texts, 41, Cambridge University Press, Cambridge, 1998. Zbl 0907.11001 MR 1689189

[27] R. Taylor, Representations of Galois groups associated to modular forms, in *Proceedings of the International Congress of Mathematicians (Zürich, 1994). Vol. 1, 2*, 435–442, Basel, Birkhäuser, 1995. Zbl 0864.11022 MR 1403943

Received September 18, 2016

M. H. Şengün, School of Mathematics and Statistics, University of Sheffield,
Sheffield S3 7RH, UK
E-mail: m.sengun@sheffield.ac.uk

S. Siksek, Mathematics Institute, University of Warwick,
Coventry CV4 7AL, UK
E-mail: samir.siksek@gmail.com