

Algebra & Number Theory

Volume 10

2016

No. 6

Modular elliptic curves over
real abelian fields and the generalized
Fermat equation $x^{2\ell} + y^{2m} = z^p$

Samuele Anni and Samir Siksek



Modular elliptic curves over real abelian fields and the generalized Fermat equation $x^{2\ell} + y^{2m} = z^p$

Samuele Anni and Samir Siksek

Let K be a real abelian field of odd class number in which 5 is unramified. Let S_5 be the set of places of K above 5. Suppose for every nonempty proper subset $S \subset S_5$ there is a totally positive unit $u \in \mathcal{O}_K$ such that

$$\prod_{\mathfrak{q} \in S} \text{Norm}_{\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_5}(u \bmod \mathfrak{q}) \neq \bar{1}.$$

We prove that every semistable elliptic curve over K is modular, using a combination of several powerful modularity theorems and class field theory. We deduce that if K is a real abelian field of conductor $n < 100$, with $5 \nmid n$ and $n \neq 29, 87, 89$, then every semistable elliptic curve E over K is modular.

Let ℓ, m, p be prime, with $\ell, m \geq 5$ and $p \geq 3$. To a putative nontrivial primitive solution of the generalized Fermat equation $x^{2\ell} + y^{2m} = z^p$ we associate a Frey elliptic curve defined over $\mathbb{Q}(\zeta_p)^+$, and study its mod ℓ representation with the help of level lowering and our modularity result. We deduce the nonexistence of nontrivial primitive solutions if $p \leq 11$, or if $p = 13$ and $\ell, m \neq 7$.

1. Introduction

Let $p, q, r \in \mathbb{Z}_{\geq 2}$. The equation

$$x^p + y^q = z^r \tag{1}$$

is known as the *generalized Fermat equation* (or the *Fermat–Catalan equation*) with signature (p, q, r) . As in Fermat’s last theorem, one is interested in integer solutions x, y, z . Such a solution is called *nontrivial* if $xyz \neq 0$, and *primitive* if x, y, z are coprime. Let $\chi = p^{-1} + q^{-1} + r^{-1}$. The *generalized Fermat conjecture* [Darmon and Granville 1995; Darmon 1997], also known as the Tijdeman–Zagier

The authors are supported by EPSRC Programme Grant “LMF: *L*-Functions and Modular Forms” EP/K034383/1.

MSC2010: primary 11D41, 11F80; secondary 11G05, 11F41.

Keywords: elliptic curves, modularity, Galois representation, level lowering, irreducibility, generalized Fermat, Fermat–Catalan, Hilbert modular forms.

conjecture and as the Beal conjecture [Beukers 2012], is concerned with the case $\chi < 1$. It states that the only nontrivial primitive solutions to (1) with $\chi < 1$ are

$$\begin{aligned} 1 + 2^3 &= 3^2, & 2^5 + 7^2 &= 3^4, \\ 7^3 + 13^2 &= 2^9, & 2^7 + 17^3 &= 71^2, \\ 3^5 + 11^4 &= 122^2, & 1414^3 + 2213459^2 &= 65^7, \\ 17^7 + 76271^3 &= 21063928^2, & 9262^3 + 15312283^2 &= 113^7, \\ 43^8 + 96222^3 &= 30042907^2, & 33^8 + 1549034^2 &= 15613^3. \end{aligned}$$

The conjecture has been established for many signatures (p, q, r) , including several infinite families of signatures, starting with Fermat's last theorem (p, p, p) by Wiles [1995]; $(p, p, 2)$ and $(p, p, 3)$ by Darmon and Merel [1997]; $(2, 4, p)$ by Ellenberg [2004] and Bennett, Ellenberg and Ng [Bennett et al. 2010]; $(2p, 2p, 5)$ by Bennett [2006]; $(2, 6, p)$ by Bennett and Chen [2012]; and other signatures by other researchers. An excellent, exhaustive and up-to-date survey was recently compiled by Bennett, Chen, Dahmen and Yazdani [Bennett et al. 2015a], which also proves the generalized Fermat conjecture for several families of signatures, including $(2p, 4, 3)$.

The main Diophantine result of this paper is the following theorem.

Theorem 1.1. *Let $p = 3, 5, 7, 11$ or 13 . Let $\ell, m \geq 5$ be primes, and if $p = 13$ suppose moreover that $\ell, m \neq 7$. Then the only primitive solutions to*

$$x^{2\ell} + y^{2m} = z^p \tag{2}$$

are the trivial ones $(x, y, z) = (\pm 1, 0, 1)$ and $(0, \pm 1, 1)$.

If $\ell = 2, 3$ or $m = 2, 3$ then (2) has no nontrivial primitive solutions for prime $p \geq 3$; this follows from the aforementioned work on Fermat equations of signatures $(2, 4, p)$, $(2, 6, p)$ and $(2p, 4, 3)$.

Our approach is unusual in that it treats several bi-infinite families of signatures. We start with a descent argument (Section 4), inspired by the approach of Bennett [2006] for $x^{2n} + y^{2n} = z^5$ and that of Freitas [2015] for $x^r + y^r = z^p$ with certain small values of r . For $p = 3$ the descent argument allows us to quickly obtain a contradiction (Section 5) through results of Bennett and Skinner [2004]. The bulk of the paper is devoted to $5 \leq p \leq 13$. Our descent allows us to construct Frey curves (Sections 6 and 7) attached to (2) that are defined over the real cyclotomic field $K = \mathbb{Q}(\zeta + \zeta^{-1})$ where ζ is a p -th root of unity, or, for $p \equiv 1 \pmod{4}$, defined over the unique subfield K' of K of degree $\frac{1}{4}(p-1)$. These Frey curves are semistable over K , though not necessarily over K' .

In the remainder of the paper we study the mod ℓ representations of these Frey curves using modularity and level lowering. Several recent papers [Dieulefait and

Freitas 2013; Freitas and Siksek 2015a; 2015c; Freitas 2015; Bennett et al. 2015b] apply modularity and level lowering over totally real fields to study Diophantine problems. We need to refine many of the ideas in those papers, both because we are dealing with representations over number fields of relatively high degree, and because we are aiming for a “clean” result without any exceptions (the methods are much easier to apply for sufficiently large ℓ). We first establish modularity of the Frey curves by combining a modularity theorem for residually reducible representations due to Skinner and Wiles [1999] with a theorem of Thorne [2016] for residually dihedral representations, and implicitly applying modularity lifting theorems of Kisin [2009] and others for representations with “big image”. We use class field theory to glue together these great modularity theorems and produce our own theorem (proved in Section 2) that applies to our Frey curves, but which we expect to be of independent interest.

Theorem 1.2. *Let K be a real abelian number field. Write S_5 for the prime ideals \mathfrak{q} of K above 5. Suppose*

- (a) *5 is unramified in K ;*
- (b) *the class number of K is odd;*
- (c) *for each nonempty proper subset S of S_5 , there is some totally positive unit u of \mathcal{O}_K such that*

$$\prod_{\mathfrak{q} \in S} \text{Norm}_{\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_5}(u \bmod \mathfrak{q}) \neq \bar{1}. \tag{3}$$

Then every semistable elliptic curve E over K is modular.

Theorem 1.2 allows us to deduce the following corollary (also proved in Section 2).

Corollary 1.3. *Let K be a real abelian field of conductor $n < 100$ with $5 \nmid n$ and $n \neq 29, 87, 89$. Let E be a semistable elliptic curve over K . Then E is modular.*

To apply level lowering theorems to a modular mod ℓ representation, one must first show that this representation is irreducible. Let $G_K = \text{Gal}(\bar{K}/K)$. The mod ℓ representation that concerns us, denoted $\bar{\rho}_{E,\ell} : G_K \rightarrow \text{GL}_2(\mathbb{F}_\ell)$, is the one attached to the ℓ -torsion of our semistable Frey elliptic curve E defined over the field $K = \mathbb{Q}(\zeta + \zeta^{-1})$ of degree $\frac{1}{2}(p - 1)$. We exploit semistability of our Frey curve to show, with the help of class field theory, that if $\bar{\rho}_{E,\ell}$ is reducible then E or some ℓ -isogenous curve possesses nontrivial K -rational ℓ -torsion. Using famous results on torsion of elliptic curves over number fields of small degree due to Kamienny [1992], Parent [2000; 2003], and Derickx et al. [\geq 2016] and some computations of K -points on certain modular curves, we prove the required irreducibility result (Section 10).

The final step (Section 11) in the proof of Theorem 1.1 requires computations of certain Hilbert eigenforms over the fields K together with their eigenvalues at

primes of small norm. For these computations we have made use of the ‘‘Hilbert modular forms package’’ developed by Demb el e, Donnelly, Greenberg and Voight and available within the Magma computer algebra system [Bosma et al. 1997]. For the theory behind this package see [Demb el e and Voight 2013]. For $p \geq 17$, the required computations are beyond the capabilities of current software, though the strategy for proving Theorem 1.1 should be applicable to larger p once these computational limitations are overcome. In fact, at the end of Section 11, we heuristically argue that the larger the value of p is, the more likely that the argument used to complete the proof of Theorem 1.1 will succeed for that particular p . We content ourselves with proving the following theorem (Section 8).

Theorem 1.4. *Let p be an odd prime, and let $K = \mathbb{Q}(\zeta + \zeta^{-1})$ for $\zeta = \exp(2\pi i/p)$. Write \mathcal{O}_K for the ring of integers in K and \mathfrak{p} for the unique prime ideal above p . Suppose that there are no elliptic curves E/K with full 2-torsion and conductors $2\mathcal{O}_K, 2\mathfrak{p}$. Then there is an ineffective constant C_p (depending only on p) such that for all primes $\ell, m \geq C_p$, the only primitive solutions to (2) are the trivial ones $(x, y, z) = (\pm 1, 0, 1)$ and $(0, \pm 1, 1)$.*

If $p \equiv 1 \pmod{4}$ then let K' be the unique subfield of K of degree $\frac{1}{4}(p-1)$. Let \mathfrak{B} be the unique prime ideal of K' above p . Suppose that there are no elliptic curves E/K' with nontrivial 2-torsion and conductors $2\mathfrak{B}, 2\mathfrak{B}^2$. Then there is an ineffective constant C_p (depending only on p) such that for all primes $\ell, m \geq C_p$, the only primitive solutions to (2) are the trivial ones $(x, y, z) = (\pm 1, 0, 1)$ and $(0, \pm 1, 1)$.

The computations described in this paper were carried out using the computer algebra system Magma [Bosma et al. 1997]. The code and output is available from

<http://homepages.warwick.ac.uk/~maseap/progs/diophantine/>

2. Proof of Theorem 1.2 and Corollary 1.3

We need a result from class field theory. The following version is proved by Kraus [2007, Appendice A].

Proposition 2.1. *Let K be a number field, and q a rational prime that does not ramify in K . Denote the mod q cyclotomic character by $\chi_q : G_K \rightarrow \mathbb{F}_q^\times$. Write S_q for the set of primes \mathfrak{q} of K above q , and let S be a subset of S_q . Let $\varphi : G_K \rightarrow \mathbb{F}_q^\times$ be a character satisfying:*

- (a) φ is unramified outside S and the infinite places of K ;
- (b) $\varphi|_{I_{\mathfrak{q}}} = \chi_q|_{I_{\mathfrak{q}}}$ for all $\mathfrak{q} \in S$; here $I_{\mathfrak{q}}$ denotes the inertia subgroup of G_K at \mathfrak{q} .

Let $u \in \mathcal{O}_K$ be a unit that is positive in each real embedding of K . Then

$$\prod_{\mathfrak{q} \in S} \text{Norm}_{\mathbb{F}_{\mathfrak{q}}/\mathbb{F}_q}(u \bmod \mathfrak{q}) = \bar{1}.$$

Proof. For the reader’s convenience we give a sketch of Kraus’s elegant argument. Let L be the cyclic field extension of K cut out by the kernel of φ . Then we may view φ as a character $\text{Gal}(L/K) \rightarrow \mathbb{F}_q^\times$. Write M_K for the places of K . For $v \in M_K$, let $\Theta_v : K_v^* \rightarrow \text{Gal}(L/K)$ be the local Artin map. Let $u \in \mathcal{O}_K$ be a unit that is positive in each real embedding. We consider the values $\varphi(\Theta_v(u)) \in \mathbb{F}_q^\times$ as v ranges over M_K .

Suppose first that $v \in M_K$ is infinite. If v is complex then Θ_v is trivial and so certainly $\varphi(\Theta_v(u)) = \bar{1}$ in \mathbb{F}_q^\times . So suppose v is real. As u is positive in K_v , it is a local norm and hence in the kernel of Θ_v . Therefore $\varphi(\Theta_v(u)) = \bar{1}$.

Suppose next that $v \in M_K$ is finite. As $u \in \mathcal{O}_v^\times$, it follows from local reciprocity that $\Theta_v(u)$ belongs to the inertia subgroup $I_v \subseteq \text{Gal}(L/K)$. If $v \notin S$ then $\varphi(I_v) = 1$ by (a) and so $\varphi(\Theta_v(u)) = \bar{1}$. Thus suppose that $v = \mathfrak{q} \in S$. It follows from (b) that $\varphi(\Theta_{\mathfrak{q}}(u)) = \chi_{\mathfrak{q}}(\Theta_{\mathfrak{q}}(u))$. Through an explicit calculation, Kraus [2007, Appendice A, Proposition 1] shows that $\chi_{\mathfrak{q}}(\Theta_{\mathfrak{q}}(u)) = \text{Norm}_{\mathbb{F}_q/\mathbb{F}_q}(u \bmod \mathfrak{q})^{-1}$.

Finally, by global reciprocity, $\prod_{v \in M_K} \Theta_v(u) = 1$. Applying φ to this equality completes the proof. \square

We also make use of the following theorem of Thorne [2016, Theorem 1.1].

Theorem 2.2 (Thorne). *Let E be an elliptic curve over a totally real field K . Suppose 5 is not a square in K and that E has no 5-isogenies defined over K . Then E is modular.*

Thorne deduces this result by combining his beautiful modularity theorem for residually dihedral representations [Thorne 2016, Theorem 1.2], with [Freitas et al. 2015, Theorem 3]. The latter result is essentially a straightforward consequence of the powerful modularity lifting theorems for residual representations with “big image” due to Kisin [2009], Barnet-Lamb et al. [2012; 2013] and Breuil and Diamond [2014].

Finally we need the following modularity theorem for residually reducible representations due to Skinner and Wiles [1999, Theorem A].

Theorem 2.3 (Skinner and Wiles). *Let K be a real abelian number field. Let q be an odd prime, and*

$$\rho : G_K \rightarrow \text{GL}_2(\overline{\mathbb{Q}}_q)$$

be a continuous, irreducible representation, unramified away from a finite number of places of K . Suppose $\bar{\rho}$ is reducible and write $\bar{\rho}^{\text{ss}} = \psi_1 \oplus \psi_2$. Suppose further that

- (i) *the splitting field $K(\psi_1/\psi_2)$ of ψ_1/ψ_2 is abelian over \mathbb{Q} ;*
- (ii) *$(\psi_1/\psi_2)(\tau) = -1$ for each complex conjugation τ ;*
- (iii) *$(\psi_1/\psi_2)|_{D_{\mathfrak{q}}} \neq 1$ for each $\mathfrak{q} | q$;*

(iv) for all $q \mid q$,

$$\rho|_{D_q} \sim \begin{pmatrix} \phi_1^{(q)} \cdot \tilde{\psi}_1 & * \\ 0 & \phi_2^{(q)} \cdot \tilde{\psi}_2 \end{pmatrix}$$

with $\phi_2^{(q)}$ factoring through a pro- q extension of K_q and $\phi_2^{(q)}|_{I_q}$ having finite order, and where $\tilde{\psi}_i$ is a Teichmüller lift of ψ_i ;

(v) $\det(\rho) = \psi \chi_q^{k-1}$, where ψ is a character of finite order and $k \geq 2$ is an integer.

Then the representation ρ is associated to a Hilbert modular newform.

Proof of Theorem 1.2. As 5 is unramified in K , it certainly is not a square in K . If E has no 5-isogenies defined over K then the result follows from Thorne’s theorem. We may thus suppose that the mod 5 representation $\bar{\rho}$ of E is reducible, and write $\bar{\rho}^{\text{ss}} = \psi_1 \oplus \psi_2$. We verify hypotheses (i)–(v) in the theorem of Skinner and Wiles (with $q = 5$) to deduce the modularity of $\rho : G_K \rightarrow \text{Aut}(T_5(E)) \cong \text{GL}_2(\mathbb{Z}_5)$, where $T_5(E)$ is the 5-adic Tate module of E . If E has good supersingular reduction at some $q \mid 5$ then (as q is unramified) $\bar{\rho}|_{I_q}$ is irreducible [Serre 1972, Proposition 12], contradicting the reducibility of $\bar{\rho}$. It follows that E has good ordinary or multiplicative reduction at all $q \mid 5$. In particular, hypothesis (iv) holds with $\phi_i^{(q)} = 1$.

Now $\psi_1\psi_2 = \det(\rho) = \chi_5$ so hypothesis (v) holds with $\psi = 1$ and $k = 2$. Moreover, for each complex conjugation τ , we have

$$(\psi_1/\psi_2)(\tau) = \psi_1(\tau)\psi_2(\tau^{-1}) = \psi_1(\tau)\psi_2(\tau) = \chi_5(\tau) = -1,$$

so (ii) is satisfied. It follows from the fact that E has good ordinary or multiplicative reduction at all $q \mid 5$, that $(\bar{\rho}|_{I_q})^{\text{ss}} = \chi_5|_{I_q} \oplus 1$ and so ψ_1/ψ_2 is nontrivial when restricted to I_q (again as q is unramified in K); this proves (iii).

It remains to verify (i). Note that $\psi_1/\psi_2 = \chi_5/\psi_2^2$. Hence $K(\psi_1/\psi_2)$ is contained in the compositum of the fields $K(\zeta_5)$ and $K(\psi_2^2)$, and by symmetry also contained in the compositum of the fields $K(\zeta_5)$ and $K(\psi_1^2)$. It is sufficient to show that either $K(\psi_2^2) = K$ or $K(\psi_1^2) = K$. Note that $\psi_i^2 : G_K \rightarrow \mathbb{F}_5^\times$ are quadratic characters that are unramified at all archimedean places. We will show that one of them is everywhere unramified, and then the desired result follows from the assumption that the class number of K is odd. First note, by the semistability of E , that ψ_1 and ψ_2 are unramified at all finite primes $p \nmid 5$. Let S be the subset of $q \in S_5$ such that ψ_1 is unramified at q . By the above, we know that these are precisely the $q \in S_5$ such that $\psi_2|_{I_q} = \chi_5|_{I_q}$. By assumption (c) and Proposition 2.1, we have that either $S = \emptyset$ or $S = S_5$. If $S = \emptyset$ then ψ_2 is unramified at all $q \mid 5$, and if $S = S_5$ then ψ_1 is unramified at all $q \mid 5$. This completes the proof. \square

Proof of Corollary 1.3. Suppose first that $K = \mathbb{Q}(\zeta_n)^+$. If $n \equiv 2 \pmod{4}$ then $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{n/2})$, so we adopt the usual convention of supposing that $n \not\equiv 2 \pmod{4}$. We consider values $n < 100$ and impose the restriction $5 \nmid n$, which ensures that

condition (a) of Theorem 1.2 is satisfied. It is known [Miller 2014] that the class number h_n^+ of K is 1 for all $n < 100$. Thus condition (b) is also satisfied. Write E_n^+ for the group of units of K and C_n^+ for the subgroup of cyclotomic units. A result of Sinnott [1978] asserts that $[E_n^+ : C_n^+] = b \cdot h_n^+$, where b is an explicit constant that happens to be 1 for n with at most 3 distinct prime divisors, and so certainly for all n in our range. It follows that $E_n^+ = C_n^+$ for $n < 100$. Now let S_5 be as in the statement of Theorem 1.2. We wrote a simple Magma script which for each $n < 100$ satisfying $5 \nmid n$ and $n \not\equiv 2 \pmod{4}$ writes down a basis for the cyclotomic units C_n^+ and deduces a basis for the totally positive units. It then checks, for every nonempty proper subset of S_5 , if there is an element u of this basis of totally positive units that satisfies (3). We found this to be the case for all n under consideration except $n = 29, 87$ and 89 . The corollary follows from Theorem 1.2 for $K = \mathbb{Q}(\zeta_n)^+$ with n as in the statement of the corollary.

Now let K be a real abelian field with conductor n as in the statement of the corollary. Then $K \subseteq \mathbb{Q}(\zeta_n)^+$. As $\mathbb{Q}(\zeta_n)^+/K$ is cyclic, modularity of an elliptic curve E/K follows, by Langlands' cyclic base change theorem [Langlands 1980], from modularity of E over $\mathbb{Q}(\zeta_n)^+$, completing the proof of the corollary. \square

3. Cyclotomic preliminaries

Throughout p will be an odd prime. Let ζ be a primitive p -th root of unity, and $K = \mathbb{Q}(\zeta + \zeta^{-1})$ the maximal real subfield of $\mathbb{Q}(\zeta)$. We write

$$\theta_j = \zeta^j + \zeta^{-j} \in K, \quad j = 1, \dots, \frac{1}{2}(p-1).$$

Let \mathcal{O}_K be the ring of integers of K . Let \mathfrak{p} be the unique prime ideal of K above p . Then $p\mathcal{O}_K = \mathfrak{p}^{(p-1)/2}$.

Lemma 3.1. *For $j = 1, \dots, \frac{1}{2}(p-1)$, we have*

$$\theta_j \in \mathcal{O}_K^\times, \quad \theta_j + 2 \in \mathcal{O}_K^\times, \quad (\theta_j - 2)\mathcal{O}_K = \mathfrak{p}.$$

Moreover, $(\theta_j - \theta_k)\mathcal{O}_K = \mathfrak{p}$ for $1 \leq j < k \leq \frac{1}{2}(p-1)$.

Proof. Observe that $\theta_j = (\zeta^{2j} - \zeta^{-2j})/(\zeta^j - \zeta^{-j})$ and thus belongs to the group of cyclotomic units. Given j , let $j \equiv 2r \pmod{p}$. Then $\theta_j + 2 = \theta_r^2 \in \mathcal{O}_K^\times$.

For now, let $L = \mathbb{Q}(\zeta)$. Let \mathfrak{P} be the prime of \mathcal{O}_L above \mathfrak{p} . Then $\mathfrak{p}\mathcal{O}_L = \mathfrak{P}^2$. As is well-known, $\mathfrak{P} = (1 - \zeta^u)\mathcal{O}_L$ for $u = 1, 2, \dots, p-1$. Note that $\theta_j - 2 = (\zeta^r - \zeta^{-r})^2$, with $j \equiv 2r \pmod{p}$, from which we deduce that $(\theta_j - 2)\mathcal{O}_L = \mathfrak{P}^2 = \mathfrak{p}\mathcal{O}_L$, hence $(\theta_j - 2)\mathcal{O}_K = \mathfrak{p}$.

For the final part, $j \not\equiv \pm k \pmod{p}$. Thus there exist $u, v \not\equiv 0 \pmod{p}$ such that

$$u + v \equiv j, \quad u - v \equiv k \pmod{p}.$$

Then

$$(\zeta^u - \zeta^{-u})(\zeta^v - \zeta^{-v}) = \theta_j - \theta_k,$$

and so $(\theta_j - \theta_k)\mathcal{O}_L = \mathfrak{A}^2 = \mathfrak{p}\mathcal{O}_L$. This completes the proof. □

4. The descent

Now let $\ell, m \geq 5$ be prime, and let (x, y, z) be a nontrivial, primitive solution to (2). If $\ell = p$, then (2) can be rewritten as $z^p + (-x^2)^p = (y^m)^2$. Darmon and Merel [1997] have shown that the only primitive solutions to the generalized Fermat equation (1) with signature $(p, p, 2)$ are the trivial ones, giving us a contradiction. We shall henceforth suppose that $\ell \neq p$ and $m \neq p$.

Clearly z is odd. By swapping in (2) the terms x^ℓ and y^m if necessary, we may suppose that $2 \mid x$. We factor the left-hand side over $\mathbb{Z}[i]$. It follows from our assumptions that the two factors $x^\ell + y^m i$ and $x^\ell - y^m i$ are coprime. There exist coprime rational integers a, b such that

$$x^\ell + y^m i = (a + bi)^p, \quad z = a^2 + b^2.$$

Then

$$\begin{aligned} x^\ell &= \frac{1}{2}((a + bi)^p + (a - bi)^p) \\ &= a \cdot \prod_{j=1}^{p-1} ((a + bi) + (a - bi)\zeta^j) \\ &= a \cdot \prod_{j=1}^{(p-1)/2} ((a + bi) + (a - bi)\zeta^j) \cdot ((a + bi) + (a - bi)\zeta^{-j}). \end{aligned}$$

In the last step we have paired up the complex conjugate factors. Multiplying out these pairs we obtain a factorization of x^ℓ over \mathcal{O}_K :

$$x^\ell = a \cdot \prod_{j=1}^{(p-1)/2} ((\theta_j + 2)a^2 + (\theta_j - 2)b^2). \tag{4}$$

To ease notation, write

$$\beta_j = (\theta_j + 2)a^2 + (\theta_j - 2)b^2, \quad j = 1, \dots, \frac{1}{2}(p - 1). \tag{5}$$

Lemma 4.1. *Write $n = v_2(x) \geq 1$.*

(i) *If $p \nmid x$ then*

$$a = 2^{\ell n} \alpha^\ell, \quad \beta_j \mathcal{O}_K = \mathfrak{b}_j^\ell,$$

where α is a rational integer and $\alpha \mathcal{O}_K, \mathfrak{b}_1, \dots, \mathfrak{b}_{(p-1)/2}$ are pairwise coprime ideals of \mathcal{O}_K , all of which are coprime to $2p$.

(ii) If $p \mid x$ then

$$a = 2^{\ell n} p^{\kappa \ell - 1} \alpha^\ell, \quad \beta_j \mathcal{O}_K = \mathfrak{p} \cdot \mathfrak{b}_j^\ell,$$

where $\kappa = v_p(x) \geq 1$, α is a rational integer and $\alpha \cdot \mathcal{O}_K, \mathfrak{b}_1, \dots, \mathfrak{b}_{(p-1)/2}$ are pairwise coprime ideals of \mathcal{O}_K , all of which are coprime to $2\mathfrak{p}$.

Proof. As $z = a^2 + b^2$ is odd, exactly one of a, b is even. Thus the β_j are coprime to $2\mathcal{O}_K$. We see from (4) that $2^{\ell n} \parallel a$, and hence that b is odd.

As a, b are coprime, it is clear that the greatest common divisor of $a\mathcal{O}_K$ and $\beta_j\mathcal{O}_K$ divides $(\theta_j - 2)\mathcal{O}_K = \mathfrak{p}$. Moreover, for $k \neq j$, the greatest common divisor of $\beta_j\mathcal{O}_K$ and $\beta_k\mathcal{O}_K$ divides

$$((\theta_j + 2)(\theta_k - 2) - (\theta_k + 2)(\theta_j - 2))\mathcal{O}_K = 4(\theta_k - \theta_j)\mathcal{O}_K = 4\mathfrak{p}.$$

However, β_j is odd, and so the greatest common divisor of $\beta_j\mathcal{O}_K$ and $\beta_k\mathcal{O}_K$ divides \mathfrak{p} . Now (i) follows immediately from (4). So suppose $p \mid x$. For (ii) we have to check that $\mathfrak{p} \parallel \beta_j$. However, since $(\theta_j - 2)\mathcal{O}_K = \mathfrak{p}$ and $\theta_j + 2 \in \mathcal{O}_K^\times$, reducing (4) modulo \mathfrak{p} shows that $a^p \equiv 0 \pmod{\mathfrak{p}}$, and hence that $p \mid a$. Since a, b are coprime, it follows that $v_p(\beta_j) = 1$. Now, from (4),

$$\frac{1}{2}(p-1)v_p(a) = v_p(a) = \ell v_p(x) - \sum_{j=1}^{(p-1)/2} v_p(\beta_j) = \frac{1}{2}(p-1)(\kappa \ell - 1),$$

giving the desired exponent of p in the factorization of a . □

5. Proof of Theorem 1.1 for $p = 3$

Suppose $p = 3$. Then $K = \mathbb{Q}$ and $\theta := \theta_1 = -1$. We treat first the case $3 \nmid x$. By Lemma 4.1,

$$a = 2^{\ell n} \alpha^\ell, \quad a^2 - 3b^2 = \gamma^\ell$$

for some coprime odd rational integers α and γ . We obtain the equation

$$2^{2\ell n} \alpha^{2\ell} - \gamma^\ell = 3b^2.$$

Bennett and Skinner [2004, Theorem 1] show that the equation $x^n + y^n = 3z^2$ has no solutions in coprime integers x, y, z for $n \geq 4$, giving us a contradiction.

We now treat $3 \mid x$. By Lemma 4.1,

$$a = 2^{\ell n} 3^{\kappa \ell - 1} \alpha^\ell, \quad a^2 - 3b^2 = 3\gamma^\ell$$

for coprime rational integers α, γ that are also coprime to 6. Thus

$$2^{2\ell n} 3^{2\kappa \ell - 3} \alpha^{2\ell} - \gamma^\ell = b^2.$$

Using the recipes of Bennett and Skinner [2004, Sections 2, 3], we can attach a Frey curve to such a triple (α, γ, b) whose mod ℓ representation arises from a classical newform of weight 2 and level 6. As there are no such newforms our contradiction is complete.

6. The Frey curve

We shall henceforth suppose $p \geq 5$. From now on, fix $1 \leq j, k \leq \frac{1}{2}(p - 1)$ with $j \neq k$. The expressions β_j, β_k are given by (5). For each such choice of (j, k) we shall construct a Frey curve. The idea is that the three expressions a^2, β_j, β_k are roughly ℓ -th powers (Lemma 4.1). Moreover they are linear combinations of a^2 and b^2 , and hence must be linearly dependent. Writing down this linear relation gives a Fermat equation (with coefficients) of signature (ℓ, ℓ, ℓ) . As in the work of Hellegouarch, Frey, Serre, Ribet, Kraus and many others, one can associate to such an equation a Frey elliptic curve whose mod ℓ representation has very little ramification. In what follows we take care to scale the expressions a^2, β_j, β_k appropriately so that the Frey curve is semistable.

Case I: $p \nmid x$. Let

$$u = \beta_j, \quad v = -\frac{(\theta_j - 2)}{(\theta_k - 2)}\beta_k, \quad w = \frac{4(\theta_j - \theta_k)}{(\theta_k - 2)} \cdot a^2. \tag{6}$$

Then $u + v + w = 0$. Moreover, by Lemmas 3.1 and 4.1,

$$u\mathcal{O}_K = \mathfrak{b}_j^\ell, \quad v\mathcal{O}_K = \mathfrak{b}_k^\ell, \quad w\mathcal{O}_K = 2^{2\ell n+2} \cdot \alpha^{2\ell} \mathcal{O}_K.$$

We let the Frey curve be

$$E = E_{j,k} : Y^2 = X(X - u)(X + v). \tag{7}$$

For a nonzero ideal \mathfrak{a} , we define its *radical*, denoted by $\text{Rad}(\mathfrak{a})$, to be the product of the distinct prime ideal factors of \mathfrak{a} .

Lemma 6.1. *Suppose $p \nmid x$. Let E be the Frey curve (7) where u, v, w are given by (6). The curve E is semistable, with multiplicative reduction at all primes above 2 and good reduction at \mathfrak{p} . It has minimal discriminant and conductor*

$$\mathcal{D}_{E/K} = 2^{4\ell n-4} \alpha^{4\ell} \mathfrak{b}_j^{2\ell} \mathfrak{b}_k^{2\ell}, \quad \mathcal{N}_{E/K} = 2 \cdot \text{Rad}(\alpha \mathfrak{b}_j \mathfrak{b}_k).$$

Proof. The invariants $c_4, c_6, \Delta, j(E)$ have their usual meanings and are given by

$$\begin{aligned} c_4 &= 16(u^2 - vw) = 16(v^2 - wu) = 16(w^2 - uv), \\ c_6 &= -32(u - v)(v - w)(w - u), \quad \Delta = 16u^2v^2w^2, \quad j(E) = c_4^3/\Delta. \end{aligned} \tag{8}$$

By Lemma 4.1, we have that $\alpha\mathcal{O}_K, \mathfrak{b}_j$ and \mathfrak{b}_k are pairwise coprime, and all coprime to $2p$. In particular $\mathfrak{p} \nmid \Delta$ and so E has good reduction at \mathfrak{p} . Moreover, c_4 and Δ are

coprime away from 2. Hence the model in (7) is already semistable away from 2. Recall that $2^\ell \mid a$ and $2 \nmid b$. Thus

$$u \equiv (\theta_j - 2)b^2 \pmod{2^{2\ell}}, \quad v \equiv -(\theta_j - 2)b^2 \pmod{2^{2\ell}}, \quad w \equiv 0 \pmod{2^{2\ell+2}}.$$

It is clear that $v_q(j) < 0$ for all $q \mid 2$. Thus E has potentially multiplicative reduction at all $q \mid 2$. Write $\gamma = -c_4/c_6$. To show that E has multiplicative reduction at q it is enough to show that $K_q(\sqrt{\gamma})/K_q$ is an unramified extension [Silverman 1994, Exercise V.5.11]. However,

$$\frac{1}{16}c_4 = (u^2 - vw) \equiv (\theta_j - 2)^2 \cdot b^4 \pmod{2^{2\ell}},$$

which shows that c_4 is a square in K_q . Moreover,

$$-\frac{1}{16}c_6 = 2(u - v)(v - w)(w - u) \equiv 4 \cdot (\theta_j - 2)^3 \cdot b^6 \pmod{2^{2\ell+1}}.$$

Thus $K_q(\sqrt{\gamma}) = K_q(\sqrt{\theta_j - 2})$. As before, letting r satisfy $2r \equiv j \pmod{p}$, we have $\theta_j - 2 = (\zeta^r - \zeta^{-r})^2$ and so $K_q(\sqrt{\gamma})$ is contained in the unramified extension $K_q(\zeta)$. Hence E has multiplicative reduction at $q \mid 2$.

Finally 2 is unramified in K , and so $v_q(c_4) = v_2(16) = 4$. It follows that $\mathcal{D}_{E/K} = (\Delta/2^{12}) \cdot \mathcal{O}_K$, as required. \square

Case II: $p \mid x$. Let

$$u = \frac{\beta_j}{(\theta_j - 2)}, \quad v = -\frac{\beta_k}{(\theta_k - 2)}, \quad w = \frac{4(\theta_j - \theta_k)}{(\theta_j - 2)(\theta_k - 2)} \cdot a^2. \tag{9}$$

Then, from Lemmas 3.1 and 4.1,

$$u\mathcal{O}_K = \mathfrak{b}_j^\ell, \quad v\mathcal{O}_K = \mathfrak{b}_k^\ell, \quad w\mathcal{O}_K = 2^{2\ell n+2} \cdot \mathfrak{p}^\delta \cdot \alpha^{2\ell} \mathcal{O}_K,$$

where

$$\delta = (\kappa\ell - 1)(p - 1) - 1. \tag{10}$$

Again $u + v + w = 0$ and the Frey curve is given by (7).

Lemma 6.2. *Suppose $p \mid x$. Let E be the Frey curve (7) where u, v, w are given by (9). The curve E is semistable, with multiplicative reduction at \mathfrak{p} and at all primes above 2. It has minimal discriminant and conductor*

$$\mathcal{D}_{E/K} = 2^{4\ell n-4} \mathfrak{p}^{2\delta} \alpha^{4\ell} \mathfrak{b}_j^{2\ell} \mathfrak{b}_k^{2\ell}, \quad \mathcal{N}_{E/K} = 2\mathfrak{p} \cdot \text{Rad}(\alpha \mathfrak{b}_j \mathfrak{b}_k).$$

Proof. The proof is an easy modification of the proof of Lemma 6.1. \square

7. A closer look at the Frey curve for $p \equiv 1 \pmod{4}$

In this section we suppose that $p \equiv 1 \pmod{4}$. The Galois group of $K = \mathbb{Q}(\zeta + \zeta^{-1})$ is cyclic of order $\frac{1}{2}(p - 1)$. Thus the field $K = \mathbb{Q}(\zeta + \zeta^{-1})$ has a unique involution $\tau \in \text{Gal}(K/\mathbb{Q})$, and we let K' be the subfield of degree $\frac{1}{4}(p - 1)$ that is fixed by

this involution. In the previous section we let $1 \leq j, k \leq \frac{1}{2}(p-1)$ with $j \neq k$. In this section we shall impose the further condition that $\tau(\theta_j) = \theta_k$. Now a glance at the definition (7) of the Frey curve E and the formulae (9) for u and v in the case $p \mid x$ shows that the curve E is in fact defined over K' . This is not true in the case $p \nmid x$, but we can take a twist of the Frey curve so that it is defined over K' .

Case I: $p \nmid x$. Let

$$u' = (\theta_k - 2)\beta_j, \quad v' = -(\theta_j - 2)\beta_k, \quad w' = 4(\theta_j - \theta_k) \cdot a^2, \quad (11)$$

and let

$$E' : Y^2 = X(X - u')(X + v').$$

Clearly the coefficients of E' are invariant under τ , and so E' is defined over K' . Moreover, E'/K is the quadratic twist of E/K by $(\theta_k - 2)$. Let \mathfrak{B} be the unique prime of K' above p . Let

$$\mathfrak{b}_{j,k} = \text{Norm}_{K/K'}(\mathfrak{b}_j) = \text{Norm}_{K/K'}(\mathfrak{b}_k).$$

It follows from Lemma 4.1 that the $\mathcal{O}_{K'}$ -ideal $\mathfrak{b}_{j,k}$ is coprime to α and to $2p$. An easy calculation leads us to the following lemma.

Lemma 7.1. *Suppose $p \nmid x$. Let E'/K' be the above Frey elliptic curve. Then E' is semistable away from \mathfrak{B} , with minimal discriminant and conductor*

$$\mathcal{D}_{E'/K'} = 2^{4\ell n - 4} \mathfrak{B}^3 \alpha^{4\ell} \mathfrak{b}_{j,k}^{2\ell}, \quad \mathcal{N}_{E'/K'} = 2 \cdot \mathfrak{B}^2 \cdot \text{Rad}(\alpha \mathfrak{b}_{j,k}).$$

Case II: $p \mid x$. Another straightforward computation yields the following lemma.

Lemma 7.2. *Suppose $p \mid x$. Let $E' = E$ be the Frey curve in Lemma 6.2. Then E' is defined over K' . The curve E'/K' is semistable with minimal discriminant and conductor*

$$\mathcal{D}_{E'/K'} = 2^{4\ell n - 4} \mathfrak{B}^\delta \alpha^{4\ell} \mathfrak{b}_{j,k}^{2\ell}, \quad \mathcal{N}_{E'/K'} = 2 \cdot \mathfrak{B} \cdot \text{Rad}(\alpha \mathfrak{b}_{j,k}),$$

where δ is given by (10).

Remark. Clearly E has full 2-torsion over K . The curve E' has a point of order 2 over K' , but not necessarily full 2-torsion.

8. Proof of Theorem 1.4

Lemma 8.1. *Let p be an odd prime. There is an ineffective constant $C_p^{(1)}$ depending on p such that for odd primes $\ell, m \geq C_p^{(1)}$ and any nontrivial primitive solution (x, y, z) of (2), the Frey curve E/K as in Section 6 is modular. If $p \equiv 1 \pmod{4}$ then under the same assumptions, the Frey curve E'/K' as in Section 7 is modular.*

Proof. Freitas et al. [2015] show that for any totally real field K there are at most finitely many nonmodular j -invariants. Let j_1, \dots, j_r be the values of these j -invariants. Let \mathfrak{q} be a prime of K above 2. By Lemmas 6.1 and 6.2, we have $v_{\mathfrak{q}}(j(E)) = -(4\ell n - 4)$ with $n \geq 1$. Thus for ℓ, m sufficiently large we have $v_{\mathfrak{q}}(j(E)) < v_{\mathfrak{q}}(j_i)$ for $i = 1, \dots, r$, completing the proof. \square

Remarks. • The argument in [Freitas et al. 2015] relies on Faltings’ theorem (finiteness of the number of rational points on a curve of genus ≥ 2) to deduce finiteness of the list of possibly nonmodular j -invariants. It is for this reason that the constant $C_p^{(1)}$ (and hence the constant C_p in Theorem 1.4) is ineffective.

- In the above argument, it seems that it is enough to suppose that ℓ is sufficiently large without an assumption on m . However, in Section 4 we swapped the terms $x^{2\ell}$ and y^{2m} in (2) if needed to ensure that x is even. Thus in the above argument we need to suppose that both ℓ and m are sufficiently large.

We shall make use of the following result due to Freitas and Siksek [2015b, Theorem 2]. It is a variant of results proved by Kraus [2007] and by David [2012]. All these build on the celebrated uniform boundedness theorem of Merel [1996].

Theorem 8.2. *Let K be a totally real field. There is an effectively computable constant C_K such that for a prime $\ell > C_K$, and for an elliptic curve E/K semistable at all $\lambda \mid \ell$, the mod ℓ representation $\bar{\rho}_{E,\ell} : G_K \rightarrow \text{GL}_2(\mathbb{F}_{\ell})$ is irreducible.*

In [Freitas and Siksek 2015b, Theorem 2] it is assumed that K is Galois as well as totally real. Theorem 8.2 follows immediately on replacing K with its Galois closure.

Lemma 8.3. *Let E/K be the Frey curve given in Section 6. Suppose $\bar{\rho}_{E,\ell}$ is irreducible and E is modular. Then $\bar{\rho}_{E,\ell} \sim \bar{\rho}_{\mathfrak{f},\lambda}$ for some Hilbert cuspidal eigenform \mathfrak{f} over K of parallel weight 2 that is new at level \mathcal{N}_{ℓ} , where*

$$\mathcal{N}_{\ell} = \begin{cases} 2\mathcal{O}_K & \text{if } p \nmid x, \\ 2\mathfrak{p} & \text{if } p \mid x. \end{cases}$$

Here $\lambda \mid \ell$ is a prime of $\mathbb{Q}_{\mathfrak{f}}$, the field generated over \mathbb{Q} by the eigenvalues of \mathfrak{f} .

If $p \equiv 1 \pmod{4}$, let E'/K' be the Frey curve given in Section 7. Suppose $\bar{\rho}_{E',\ell}$ is irreducible and E is modular. Then $\bar{\rho}_{E',\ell} \sim \bar{\rho}_{\mathfrak{f},\lambda}$ for some Hilbert cuspidal eigenform \mathfrak{f} over K of parallel weight 2 that is new at level \mathcal{N}'_{ℓ} , where

$$\mathcal{N}'_{\ell} = \begin{cases} 2\mathfrak{B}^2 & \text{if } p \nmid x, \\ 2\mathfrak{B} & \text{if } p \mid x. \end{cases}$$

Proof. This is immediate from Lemmas 6.1, 6.2, 7.1 and 7.2, and a standard level lowering recipe derived in [Freitas and Siksek 2015a, Section 2.3] from the work of Jarvis, Fujiwara and Rajaei. Alternatively, one could use modern modularity lifting

theorems which integrate level lowering with modularity lifting, as for example in [Breuil and Diamond 2014]. □

Proof of Theorem 1.4. Let $K = \mathbb{Q}(\zeta + \zeta^{-1})$ and E be the Frey curve constructed in Section 6. Let $C_p^{(1)}$ be the constant in Lemma 8.1, and $C_p^{(2)} = C_K$ be the constant in Theorem 8.2. Let $C_p = \max(C_p^{(1)}, C_p^{(2)})$. Suppose that $\ell, m \geq C_p$. Then $\bar{\rho}_{E,\ell}$ is irreducible and modular, and it follows from Lemma 8.3 that $\bar{\rho}_{E,\ell} \sim \bar{\rho}_{f,\lambda}$ for some Hilbert eigenform over K of parallel weight 2 that is new at level \mathcal{N}_ℓ , where $\mathcal{N}_\ell = 2\mathcal{O}_K$ or $2\mathfrak{p}$. Now a standard argument (see [Bennett and Skinner 2004, Section 4], [Kraus 1997, Section 3] or [Siksek 2012, Section 9]) shows that, after enlarging C_p by an effective amount, we may suppose that the field of eigenvalues of f is \mathbb{Q} . Observe that the level \mathcal{N}_ℓ is nonsquarefull (meaning there is a prime q at which the level has valuation 1). As the level is nonsquarefull and the field of eigenvalues is \mathbb{Q} , the eigenform f is known to correspond to some elliptic curve E_1/K of conductor \mathcal{N}_ℓ [Blasius 2004], and $\bar{\rho}_{E,\ell} \sim \bar{\rho}_{E_1,\ell}$. Finally, and again by standard arguments (see one of the references a few lines above), we may enlarge C_p by an effective constant so that the isomorphism $\bar{\rho}_{E,\ell} \sim \bar{\rho}_{E_1,\ell}$ forces E_1 to either have full 2-torsion, or to be isogenous to an elliptic curve E_2/K that has full 2-torsion. This contradicts the hypothesis of Theorem 1.4 that there are no such elliptic curves with conductor $2\mathcal{O}_K, 2\mathfrak{p}$, and completes the proof of the first part of the theorem. The proof of the second part is similar, and makes use of the Frey curve E'/K' . □

9. Modularity of the Frey curve for $5 \leq p \leq 13$

Lemma 9.1. *If $p = 5, 7, 11$ or 13 then the Frey curve E/K in Section 6 is modular. If $p = 5, 13$ then the Frey curve E'/K' in Section 7 is modular.*

Proof. Recall that E is defined over $K = \mathbb{Q}(\zeta + \zeta^{-1})$, where ζ is a primitive p -th root of unity. If $p = 5$ then $K = \mathbb{Q}(\sqrt{5})$, and modularity of elliptic curves over real quadratic fields was recently established by Freitas et al. [2015].

For $p = 7, 11, 13$, the prime 5 is unramified in K , the class number of K is 1 and condition (c) of Theorem 1.2 is easily verified. Thus E is modular.

For $p = 13$, the curves E and E' are at worst quadratic twists over K , and K/K' is quadratic. The modularity of E'/K' follows from the modularity of E/K and the cyclic base change theorem of [Langlands 1980]. For $p = 5$ we could use the same argument, or more simply note that $K' = \mathbb{Q}$, and conclude by the modularity theorem over the rationals [Breuil et al. 2001]. □

10. Irreducibility of $\bar{\rho}_{E,\ell}$ for $5 \leq p \leq 13$

We let E be the Frey curve as in Section 6, and $p = 5, 7, 11, 13$. To apply Lemma 8.3 we need to prove the irreducibility of $\bar{\rho}_{E,\ell}$ for $\ell \geq 5$; equivalently, we need to show

that E does not have an ℓ -isogeny for $\ell \geq 5$. Alas, there is not yet a uniform boundness theorem for isogenies. The papers [Kraus 2007; David 2012; Freitas and Siksek 2015b] do give effective bounds C_K such that for $\ell > C_K$ the representation $\bar{\rho}_{E,\ell}$ is irreducible, however these bounds are too large for our present purpose. We refine the arguments in those papers, making use of the fact that the curve E is semistable, and the number fields $K = \mathbb{Q}(\zeta + \zeta^{-1})$ all have narrow class number 1. Before doing this, we relate, for $p = 5$ and 13, the representations $\bar{\rho}_{E,\ell}$ and $\bar{\rho}_{E',\ell}$, where E' is the Frey curve in Section 7.

Lemma 10.1. *Suppose $p = 5$ or 13. Let τ be the unique involution of K , and K' the subfield fixed by it. Let j and k satisfy $\tau(\theta_j) = \theta_k$. Let E/K be the Frey elliptic curve in Section 6 and E'/K' the Frey curve in Section 7, associated to this pair (j, k) . Then $\bar{\rho}_{E,\ell}$ is irreducible as a representation of G_K if and only if $\bar{\rho}_{E',\ell}$ is irreducible as a representation of $G_{K'}$.*

Proof. Note that K/K' is a quadratic extension and E/K is a quadratic twist of E'/K . Thus $\bar{\rho}_{E,\ell}$ is a twist of $\bar{\rho}_{E',\ell}|_{G_K}$ by a quadratic character. If $\bar{\rho}_{E',\ell}$ is reducible as a representation of $G_{K'}$ then certainly $\bar{\rho}_{E,\ell}$ is reducible as a representation of G_K .

Conversely, suppose $\bar{\rho}_{E',\ell}(G_{K'})$ is irreducible. We would like to show that $\bar{\rho}_{E,\ell}(G_K)$ is irreducible. It is enough to show that $\bar{\rho}_{E',\ell}(G_K)$ is irreducible. Let $q \mid 2$ be a prime of K' . Then $v_q(j(E')) = 4 - 4\ell n$, which is negative but not divisible by ℓ . Thus $\bar{\rho}_{E',\ell}(G_{K'})$ contains an element of order ℓ [Silverman 1994, Proposition V.6.1]. By Dickson’s classification [Swinnerton-Dyer 1973] of subgroups of $GL_2(\mathbb{F}_\ell)$ we see that $\bar{\rho}_{E',\ell}(G_{K'})$ must contain $SL_2(\mathbb{F}_\ell)$. The latter is a simple group, and must therefore be contained in $\bar{\rho}_{E',\ell}(G_K)$. This completes the proof. \square

Lemma 10.2. *Suppose $\bar{\rho}_{E,\ell}$ is reducible. Then E/K either has nontrivial ℓ -torsion, or is ℓ -isogenous to an elliptic curve defined over K that has nontrivial ℓ -torsion.*

Proof. Suppose $\bar{\rho}_{E,\ell}$ is reducible, and write

$$\bar{\rho}_{E,\ell} \sim \begin{pmatrix} \psi_1 & * \\ 0 & \psi_2 \end{pmatrix}.$$

We show that either ψ_1 or ψ_2 is trivial. It follows in the former case that E has nontrivial ℓ -torsion, and in the latter case that the K -isogenous curve $E/\text{Ker}(\psi_1)$ has nontrivial ℓ -torsion.

As K has narrow class number 1 for $p = 5, 7, 11, 13$, it is sufficient to show that one of ψ_1, ψ_2 is unramified at all finite places. As E is semistable, the characters ψ_1 and ψ_2 are unramified away from ℓ and the infinite places. Let S_ℓ be the set of primes $\lambda \mid \ell$ of K . Let $S \subset S_\ell$ for the set of $\lambda \in S_\ell$ such that ψ_1 is ramified at λ . Then ψ_2 is ramified exactly at the primes $S \setminus S_\ell$ (see proof of Theorem 1.2).

Moreover, $\psi_1|_{I_\lambda} = \chi_\ell|_{I_\lambda}$ for all $\lambda \in S$, and $\psi_2|_{I_\lambda} = \chi_\ell|_{I_\lambda}$ for all $\lambda \in S_\ell \setminus S$. It is enough to show that either S is empty or $S_\ell \setminus S$ is empty.

Suppose S is a nonempty proper subset of S_ℓ . Fix $\lambda \in S$ and let

$$D = D_\lambda \subset G = \text{Gal}(K/\mathbb{Q})$$

be the decomposition group of λ ; by definition $\lambda^\sigma = \lambda$ for all $\sigma \in D_\lambda$. As K/\mathbb{Q} is abelian and Galois, $D_{\lambda'} = D$ for all $\lambda' \in S_\ell$, and G/D acts transitively and freely on S_ℓ . Fix a set T of coset representatives for G/D . Then there is a subset $T' \subset T$ such that

$$S = \{\lambda^{\tau^{-1}} : \tau \in T'\}, \quad S_\ell \setminus S = \{\lambda^{\tau^{-1}} : \tau \in T \setminus T'\}.$$

As S is a nonempty proper subset of S_ℓ , we have that T' is a nonempty proper subset of T . Now, by Proposition 2.1, for any totally positive unit u of \mathcal{O}_K ,

$$\prod_{\tau \in T'} \text{Norm}_{\mathbb{F}_\lambda/\mathbb{F}_\ell}(u + \lambda^{\tau^{-1}}) = \bar{1}.$$

But

$$\begin{aligned} \text{Norm}_{\mathbb{F}_\lambda/\mathbb{F}_\ell}(u + \lambda^{\tau^{-1}}) &= \prod_{\sigma \in D} (u + \lambda^{\tau^{-1}})^\sigma \\ &= \prod_{\sigma \in D} (u^\sigma + \lambda^{\tau^{-1}}) \\ &= \left(\prod_{\sigma \in D} (u^{\sigma\tau} + \lambda) \right)^{\tau^{-1}} \\ &= \prod_{\sigma \in D} (u^{\sigma\tau} + \lambda) \quad (\text{as this expression belongs to } \mathbb{F}_\ell). \end{aligned}$$

Let

$$B_{T',D}(u) = \text{Norm}_{K/\mathbb{Q}} \left(\left(\prod_{\tau \in T', \sigma \in D} u^{\sigma\tau} \right) - 1 \right).$$

It follows that $\ell \mid B_{T',D}(u)$. Now let u_1, \dots, u_d be a system of totally positive units. Then ℓ divides

$$B_{T',D}(u_1, \dots, u_d) = \text{gcd}(B_{T',D}(u_1), \dots, B_{T',D}(u_d)).$$

To sum up, if the lemma is false for ℓ , then there is some subgroup D of G and some nonempty proper subset T' of G/D such that ℓ divides $B_{T',D}(u_1, \dots, u_d)$.

The proof of the lemma is completed by a computation that we now describe. For each of $p = 5, 7, 11, 13$ we fix a basis u_1, \dots, u_d for the system of totally positive units of \mathcal{O}_K . We run through the subgroups D of $G = \text{Gal}(K/\mathbb{Q})$. For each subgroup D we fix a set of coset representatives T , and run through the nonempty proper subsets T' of T , computing $B_{T',D}(u_1, \dots, u_d)$. We found that for $p = 5, 7$

the possible values for $B_{T',D}(u_1, \dots, u_d)$ are all 1; for $p = 11$ they are 1 and 23; and for $p = 13$ they are 1, 5^2 and 3^5 . Thus the proof is complete for $p = 5, 7$ and it remains to deal with $(p, \ell) = (11, 23), (13, 5)$. For each of these possibilities we run through the nonempty proper $S \subset S_\ell$ and check that there is some totally positive unit u such that $\prod_{\lambda \in S} \text{Norm}(u + \lambda) \neq \bar{1}$. This completes the proof. \square

Suppose $\bar{\rho}_{E,\ell}$ is reducible. It follows from Lemma 10.2 that there is an elliptic curve E_1/K (which is either E or ℓ -isogenous to E) such that $E_1(K)$ has a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\ell\mathbb{Z}$. Such an elliptic curve is isogenous¹ to an elliptic curve E_2/K with a K -rational cyclic subgroup isomorphic to $\mathbb{Z}/4\ell\mathbb{Z}$. Thus we obtain a noncuspidal K -point on the curves

$$X_0(\ell), X_1(\ell), X_0(2\ell), X_1(2\ell), X_0(4\ell), X_1(2, 2\ell).$$

To achieve a contradiction it is enough to show that there are no noncuspidal K -points on one of these curves. For small values of ℓ , we find Magma’s “small modular curves package”, as well as Magma’s functionality for computing Mordell–Weil groups of elliptic curves over number fields, invaluable. Four of the modular curves of interest to us happen to be elliptic curves. The aforementioned Magma package gives the following models:

$$X_0(20) : y^2 = x^3 + x^2 + 4x + 4 \quad (\text{Cremona label } 20a1), \quad (12)$$

$$X_0(14) : y^2 + xy + y = x^3 + 4x - 6 \quad (\text{Cremona label } 14a1), \quad (13)$$

$$X_0(11) : y^2 + y = x^3 - x^2 - 10x - 20 \quad (\text{Cremona label } 11a1), \quad (14)$$

$$X_0(19) : y^2 + y = x^3 + x^2 - 9x - 15 \quad (\text{Cremona label } 19a1). \quad (15)$$

Lemma 10.3. *Let $p = 5$. Then $\bar{\rho}_{E,\ell}$ is irreducible. Moreover, $\bar{\rho}_{E',\ell}$ is irreducible.*

Proof. Suppose $\bar{\rho}_{E,\ell}$ is reducible. By the above there is an elliptic curve E_2 over the quadratic field $K = \mathbb{Q}(\sqrt{5})$, with a K -rational subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\ell\mathbb{Z}$. From classification of torsion subgroups of elliptic curves over quadratic fields [Kamienny 1992] we deduce that $\ell \leq 5$. However we are assuming throughout that $\ell \geq 5$ and $\ell \neq p$. This gives a contradiction as $p = 5$. Thus $\bar{\rho}_{E,\ell}$ is irreducible. The irreducibility of $\bar{\rho}_{E',\ell}$ follows from Lemma 10.1. \square

Lemma 10.4. *Let $p = 7$. Then $\bar{\rho}_{E,\ell}$ is irreducible.*

¹At the suggestion of one of the referees we prove this statement. Let $P_1, P_2 \in E_1(K)$ be independent points of order 2. Let Q be a solution to the equation $2X = P_1$. Then Q has order 4 and the complete set of solutions is $\{Q, Q + P_2, 3Q, 3Q + P_2\}$, which is Galois-stable. Let $E_2 = E_1/\langle P_2 \rangle$ and let $\phi : E_1 \rightarrow E_2$ be the induced isogeny. As $\text{Ker}(\phi) \cap \langle Q \rangle = 0$, we see that $Q' = Q + \langle P_2 \rangle$ has order 4. Moreover, the set $\{Q', 3Q'\}$ is Galois-stable, so $\langle Q' \rangle$ is a K -rational cyclic subgroup of order 4 on E_2 . The point of order ℓ on E_1 survives the isogeny, and so E_2 has a K -rational cyclic subgroup of order 4ℓ .

Proof. In this case K is a cubic field. By the classification of cyclic ℓ -torsion on elliptic curves over cubic fields [Parent 2000; 2003], we know $\ell \leq 13$. Since $\ell \neq p$, we need only deal with the case $\ell = 5, 11, 13$. To eliminate $\ell = 5$ and $\ell = 11$ we computed the K -points on the modular curves $X_0(20)$ and $X_0(11)$. These both have rank 0 and their K -points are in fact defined over \mathbb{Q} . The \mathbb{Q} -points of $X_0(20)$ are cuspidal thus $\ell \neq 5$. The three noncuspidal \mathbb{Q} -points on $X_0(11)$ all have integral j -invariants. As our curve E has multiplicative reduction at $2\mathcal{O}_K$, it follows that $\ell \neq 11$.

We suppose $\ell = 13$. We now apply [Bruin and Najman 2016, Theorem 1]. That theorem gives a useful and practical criterion for ruling out the existence of torsion subgroups $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ on elliptic curves over a given number field K (the remarks at the end of Section 2 of [Bruin and Najman 2016] are useful when applying that theorem). The theorem involves making certain choices and we indicate them briefly; in the notation of the theorem, we take $A = \mathbb{Z}/26\mathbb{Z}$, $L = \mathbb{Q}$, $m = 1$, $n = 26$, $X = X' = X_1(26)$, $p = \mathfrak{p}_0 = 7$. To apply the theorem we need the fact that the gonality of $X_1(26)$ is 6 [Derickx and van Hoeij 2014], and that its Jacobian has Mordell–Weil rank 0 over \mathbb{Q} [Bruin and Najman 2016, page 11]. We merely check that conditions (i)–(vi) of [Bruin and Najman 2016, Theorem 1] are satisfied, and conclude that there are no elliptic curves over K with a subgroup isomorphic to $\mathbb{Z}/26\mathbb{Z}$. This completes the proof. \square

Lemma 10.5. *Let $p = 11$. Then $\bar{\rho}_{E,\ell}$ is irreducible.*

Proof. Now K has degree 5. By the classification of cyclic ℓ -torsion on elliptic curves over quintic fields [Derickx et al. \geq 2016] we know that $\ell \leq 19$. As $\ell \neq p$ we need to deal with $\ell = 5, 7, 13, 17, 19$.

The elliptic curves $X_0(20)$, $X_0(14)$ and $X_0(19)$ have rank 0 over K and this allows us to quickly eliminate $\ell = 5, 7, 19$.

Suppose $\ell = 13$. We again apply [Bruin and Najman 2016, Theorem 1], with choices $A = \mathbb{Z}/26\mathbb{Z}$, $L = \mathbb{Q}$, $m = 1$, $n = 26$, $X = X' = X_1(26)$, $p = \mathfrak{p}_0 = 11$ (with Mordell–Weil and gonality information as in the proof of Lemma 10.4). This shows that there are no elliptic curves over K with a subgroup isomorphic to $\mathbb{Z}/26\mathbb{Z}$, allowing us to eliminate $\ell = 13$.

Suppose $\ell = 17$. We apply the same theorem with choices $A = \mathbb{Z}/34\mathbb{Z}$, $L = \mathbb{Q}$, $m = 1$, $n = 34$, $X = X' = X_1(34)$, $p = \mathfrak{p}_0 = 11$. For this we need the fact that X has gonality 10 [Derickx and van Hoeij 2014] and that the rank of $J_1(34)$ over \mathbb{Q} is 0 [Bruin and Najman 2016, page 11]. Applying the theorem shows that there are no elliptic curves over K with a subgroup isomorphic to $\mathbb{Z}/34\mathbb{Z}$. This completes the proof. \square

It remains to deal with $p = 13$. Unfortunately the field K in this case is sextic, and the known bound [Derickx et al. \geq 2016] for cyclic ℓ -torsion over sextic fields is $\ell \leq 37$, and we have been unable to deal with the cases $\ell = 37$ directly over the sextic field. We therefore proceed a little differently. We are in fact most interested

in showing the irreducibility of $\bar{\rho}_{E',\ell}$, where E' is the Frey curve defined over the degree 3 subfield K' .

Lemma 10.6. *Let $p = 13$. Then $\bar{\rho}_{E',\ell}$ is irreducible.*

Proof. Suppose $\bar{\rho}_{E',\ell}$ is reducible. We treat the cases $13 \mid x$ and $13 \nmid x$ separately. Suppose first that $13 \mid x$. Then the curve E' over the field K' is semistable (Lemma 7.2). It is now straightforward to adapt the proof of Lemma 10.2 to show that E' has nontrivial ℓ -torsion, or is ℓ -isogenous to an elliptic curve with nontrivial ℓ -torsion. Thus there is an elliptic curve over K' with a point of exact order 2ℓ . Now K' is cubic, so by [Parent 2000; 2003] we have $\ell \leq 13$. As $\ell \neq p$, it remains to deal with the cases $\ell = 5, 7, 11$. The elliptic curves $X_0(14)$ and $X_0(11)$ have rank zero over K' , and in fact their K' -points are the same as their \mathbb{Q} -points. This easily allows us to eliminate $\ell = 7$ and $\ell = 11$ as before. The curve $X_0(10)$ has genus 0 so we need a different approach, and we leave this case to the end of the proof (recall that E' does not necessarily have full 2-torsion over K').

Now suppose that $13 \nmid x$. Here E'/K' is not semistable. As we have assumed that $\bar{\rho}_{E',\ell}$ is reducible, we have that $\bar{\rho}_{E,\ell}$ is reducible (Lemma 10.1). Now we may apply Lemma 10.2 to deduce the existence of E_1/K (which is E or ℓ -isogenous to it) that has a subgroup isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\ell\mathbb{Z}$. As before, let \mathfrak{p} be the unique prime of K above 13. By Lemma 6.1 the Frey curve E has good reduction at \mathfrak{p} . As $\mathfrak{p} \nmid 2\ell$, we know from injectivity of torsion that $4\ell \mid \#E(\mathbb{F}_{\mathfrak{p}})$. But $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_{13}$. By the Hasse–Weil bounds,

$$\ell \leq (\sqrt{13} + 1)^2/4 \approx 5.3.$$

Thus $\ell = 5$.

It remains to deal with the case $\ell = 5$ for both $13 \mid x$ and $13 \nmid x$. In both cases we obtain a K -point on $X = X_0(20)$ whose image in $X_0(10)$ is a K' -point. We would like to compute $X(K)$. This computation proved beyond Magma’s capability. However, $K = K'(\sqrt{13})$. Thus the rank of $X(K)$ is the sum of the ranks of $X(K')$ and of $X'(K')$, where X' is the quadratic twist of X by 13. Computing the ranks of $X(K')$ and $X'(K')$ turns out to be a task within the capabilities of Magma, and we find that they are respectively 0 and 1. Thus $X(K)$ has rank 1. With a little more work we find that

$$X(K) = \frac{\mathbb{Z}}{6\mathbb{Z}} \cdot (4, 10) + \mathbb{Z} \cdot (3, 2\sqrt{13}).$$

Thus $X(K) = X(\mathbb{Q}(\sqrt{13}))$. It follows that the j -invariant of E' must belong to $\mathbb{Q}(\sqrt{13})$. But the j -invariant belongs to K' too, and so belongs to $\mathbb{Q}(\sqrt{13}) \cap K' = \mathbb{Q}$.

Let the rational integers a, b be as in Sections 4 and 6. Recall that b is odd, and that $v_2(a) = 5n$, where $n > 0$. Write $a = 2^{5n}a'$, where a' is odd. We know that $v_2(j(E)) = -(20n - 4)$. The prime 2 is inert in K' . An explicit calculation,

making use of the fact that $a' \equiv b \equiv 1 \pmod{2}$, shows that

$$2^{20n-4} j(E) \equiv \frac{\theta_j^2 \theta_k^2}{(\theta_j - \theta_k)^2} \pmod{2}.$$

Computing this residue for the possible values of j and k , we check that it does not belong to \mathbb{F}_2 , giving us a contradiction. \square

11. Proof of Theorem 1.1

In Section 5 we proved Theorem 1.1 for $p = 3$. In this section we deal with the values $p = 5, 7, 11, 13$. Let $\ell, m \geq 5$ be primes. Suppose (x, y, z) is a primitive nontrivial solution to (2). Without loss of generality, $2 \mid x$. We let $K = \mathbb{Q}(\zeta + \zeta^{-1})$ where $\zeta = \exp(2\pi i/p)$. For $p = 13$ we also let K' be the unique subfield of K of degree 3. Let E be the Frey curve attached to this solution (x, y, z) defined in Section 6, where we take $j = 1$ and $k = 2$. For $p = 13$ we also work with the Frey curve E' defined in Section 7, where we take $j = 1$ and $k = 5$ (these choices satisfy the condition $\tau(\theta_j) = \theta_k$, where τ is unique involution on K). By Lemma 9.1 these elliptic curves are modular. Moreover, by the results of Section 10 the representation $\bar{\rho}_{E,\ell}$ is irreducible for $p = 5, 7, 11, 13$, and the representation $\bar{\rho}_{E',\ell}$ is irreducible for $p = 13$. Let \mathcal{K} be the number field K unless $p = 13$ and $13 \mid x$, in which case we take $\mathcal{K} = K'$. Also let \mathcal{E} be the Frey curve E unless $p = 13$ and $13 \mid x$, in which we take \mathcal{E} to be E' . By Lemma 8.3 there is a Hilbert cuspidal eigenform f over \mathcal{K} of parallel weight 2 and level \mathcal{N} as given in Table 1, such that $\bar{\rho}_{\mathcal{E},\ell} \sim \bar{\rho}_{f,\lambda}$, where $\lambda \mid \ell$ is a prime of \mathbb{Q}_f , the field generated by the Hecke eigenvalues of f .

Using the Magma ‘‘Hilbert modular forms’’ package we compute the possible Hilbert newforms at these levels. The information is summarized in Table 1.

As shown in the table, there are no newforms at the relevant levels for $p = 5$, completing the contradiction for this case.²

We now explain how we complete the contradiction for the remaining cases. Suppose \mathfrak{q} a prime of \mathcal{K} such that $\mathfrak{q} \nmid 2p\ell$. In particular, \mathfrak{q} does not divide the level of f , and \mathcal{E} has good or multiplicative reduction at \mathfrak{q} . Write $\sigma_{\mathfrak{q}}$ for a Frobenius element of $G_{\mathcal{K}}$ at \mathfrak{q} . Comparing the traces of $\bar{\rho}_{\mathcal{E},\ell}(\sigma_{\mathfrak{q}})$ and $\bar{\rho}_{f,\lambda}(\sigma_{\mathfrak{q}})$ we obtain

- (i) if \mathcal{E} has good reduction at \mathfrak{q} then $a_{\mathfrak{q}}(\mathcal{E}) \equiv a_{\mathfrak{q}}(f) \pmod{\lambda}$;
- (ii) if \mathcal{E} has split multiplicative reduction at \mathfrak{q} then $\text{Norm}(\mathfrak{q}) + 1 \equiv a_{\mathfrak{q}}(f) \pmod{\lambda}$;
- (iii) if \mathcal{E} has nonsplit multiplicative reduction at \mathfrak{q} then $-(\text{Norm}(\mathfrak{q}) + 1) \equiv a_{\mathfrak{q}}(f) \pmod{\lambda}$.

²We point out in passing that for $p = 5$ we could have also worked with the Frey curve E'/\mathbb{Q} . In that case the Hilbert newforms f are actually classical newforms of weight 2 and levels 2 and 50. There are no such newforms of level 2, but there are two newforms of level 50 corresponding to the elliptic curve isogeny classes 50a and 50b. These would require further work to eliminate.

p	case	field \mathcal{K}	Frey curve \mathcal{E}	level \mathcal{N}	eigenforms \mathfrak{f}	$[\mathbb{Q}_{\mathfrak{f}} : \mathbb{Q}]$
5	$5 \nmid x$	K	E	$2\mathcal{O}_K$	–	–
	$5 \mid x$	K	E	$2\mathfrak{p}$	–	–
7	$7 \nmid x$	K	E	$2\mathcal{O}_K$	–	–
	$7 \mid x$	K	E	$2\mathfrak{p}$	\mathfrak{f}_1	1
11	$11 \nmid x$	K	E	$2\mathcal{O}_K$	\mathfrak{f}_2	2
	$11 \mid x$	K	E	$2\mathfrak{p}$	$\mathfrak{f}_3, \mathfrak{f}_4$	5
13	$13 \nmid x$	K	E	$2\mathcal{O}_K$	$\mathfrak{f}_5, \mathfrak{f}_6$	1
					\mathfrak{f}_7	2
					\mathfrak{f}_8	3
	$13 \mid x$	K'	E'	$2\mathfrak{B}$	$\mathfrak{f}_9, \mathfrak{f}_{10}$ $\mathfrak{f}_{11}, \mathfrak{f}_{12}$	1 3

Table 1. Frey curve and Hilbert eigenform information. Here \mathfrak{p} is the unique prime of K above p , and \mathfrak{B} is the unique prime of K' above p .

Let $q \nmid 2p\ell$ be a rational prime and let

$$\mathcal{A}_q = \{(\eta, \mu) : 0 \leq \eta, \mu \leq q - 1, (\eta, \mu) \neq (0, 0)\}.$$

For $(\eta, \mu) \in \mathcal{A}_q$ let

$$u(\eta, \mu) = \begin{cases} (\theta_j + 2)\eta^2 + (\theta_j - 2)\mu^2 & \text{if } p \nmid x, \\ \frac{1}{(\theta_j - 2)}((\theta_j + 2)\eta^2 + (\theta_j - 2)\mu^2) & \text{if } p \mid x, \end{cases}$$

$$v(\eta, \mu) = \begin{cases} -\frac{(\theta_k - 2)}{(\theta_k - 2)}((\theta_k + 2)\eta^2 + (\theta_k - 2)\mu^2) & \text{if } p \nmid x, \\ -\frac{1}{(\theta_k - 2)}((\theta_k + 2)\eta^2 + (\theta_k - 2)\mu^2) & \text{if } p \mid x. \end{cases}$$

Write

$$E_{(\eta, \mu)} : Y^2 = X(X - u(\eta, \mu))(X + v(\eta, \mu)).$$

Let $\Delta(\eta, \mu)$, $c_4(\eta, \mu)$ and $c_6(\eta, \mu)$ be the usual invariants of this model. Let $\gamma(\eta, \mu) = -c_4(\eta, \mu)/c_6(\eta, \mu)$. Let (a, b) be as in Section 4. As $\gcd(a, b) = 1$, we have $(a, b) \equiv (\eta, \mu) \pmod{q}$ for some $(\eta, \mu) \in \mathcal{A}_q$. In particular, $(a, b) \equiv (\eta, \mu) \pmod{q}$ for all primes $q \mid q$ of \mathcal{K} . From the definitions of the Frey curves E and E' in Sections 6 and 7 we see that \mathcal{E} has good reduction at q if and only if

$q \nmid \Delta(\eta, \mu)$, and in this case $a_q(\mathcal{E}) = a_q(E_{(\eta, \mu)})$. Let

$$B_q(\mathfrak{f}, \eta, \mu) = \begin{cases} a_q(E_{(\eta, \mu)}) - a_q(\mathfrak{f}) & \text{if } q \nmid \Delta(\eta, \mu), \\ \text{Norm}(\mathfrak{q}) + 1 - a_q(\mathfrak{f}) & \text{if } q \mid \Delta(\eta, \mu) \text{ and } \overline{\gamma(\eta, \mu)} \in (\mathbb{F}_q^*)^2, \\ \text{Norm}(\mathfrak{q}) + 1 + a_q(\mathfrak{f}) & \text{if } q \mid \Delta(\eta, \mu) \text{ and } \overline{\gamma(\eta, \mu)} \notin (\mathbb{F}_q^*)^2. \end{cases}$$

From (i)–(iii) above we see that $\lambda \mid B_q(\mathfrak{f}, \eta, \mu)$. Now let

$$B_q(\mathfrak{f}, \eta, \mu) = \sum_{\mathfrak{q} \mid q} B_{\mathfrak{q}}(\mathfrak{f}, \eta, \mu) \cdot \mathcal{O}_{\mathfrak{f}},$$

where $\mathcal{O}_{\mathfrak{f}}$ is the ring of integers of $\mathbb{Q}_{\mathfrak{f}}$. Since $(a, b) \equiv (\eta, \mu) \pmod{\mathfrak{q}}$ for all $\mathfrak{q} \mid q$, we have that $\lambda \mid B_q(\mathfrak{f}, \eta, \mu)$. Now (η, μ) is some unknown element of \mathcal{A}_q . Let

$$B'_q(\mathfrak{f}) = \prod_{(\eta, \mu) \in \mathcal{A}_q} B_q(\mathfrak{f}, \eta, \mu).$$

Then $\lambda \mid B'_q(\mathfrak{f})$. Previously, we have supposed that $q \nmid 2p\ell$. This is inconvenient as ℓ is unknown. Now we simply suppose $q \nmid 2p$, and let $B_q(\mathfrak{f}) = qB'_q(\mathfrak{f})$. Then, since $\lambda \mid \ell$, we certainly have that $\lambda \mid B_q(\mathfrak{f})$ regardless of whether $q = \ell$ or not.

Finally, if $S = \{q_1, q_2, \dots, q_r\}$ is a set of rational primes with $q_i \nmid 2p$, then λ divides the $\mathcal{O}_{\mathfrak{f}}$ -ideal $\sum_{i=1}^r B_{q_i}(\mathfrak{f})$, and thus ℓ divides $B_S(\mathfrak{f}) = \text{Norm}(\sum_{i=1}^r B_{q_i}(\mathfrak{f}))$. Table 2 gives our choices for the set S and the corresponding value of $B_S(\mathfrak{f})$ for each of the eigenforms $\mathfrak{f}_1, \dots, \mathfrak{f}_{12}$ appearing in Table 1. Recalling that $\ell \geq 5$ and $\ell \neq p$ gives a contradiction unless $p = 13$ and $\ell = 7$. This completes the proof of Theorem 1.1. □

The reader may be wondering whether we can eliminate the case $p = 13$ and $\ell = 7$ by enlarging our set S ; here we need only concern ourselves with forms \mathfrak{f}_9 and \mathfrak{f}_{11} . Consider $(\eta, \mu) = (0, 1)$, which belongs to \mathcal{A}_q for any q . The corresponding Weierstrass model $E_{(0,1)}$ is singular with a split note. It follows that

$$B_q(\mathfrak{f}, 0, 1) = \text{Norm}(\mathfrak{q}) + 1 - a_q(\mathfrak{f}).$$

Note that if λ is a prime of $\mathbb{Q}_{\mathfrak{f}}$ that divides $\text{Norm}(\mathfrak{q}) + 1 - a_q(\mathfrak{f})$ for all $q \nmid 26$, then ℓ will divide $B_S(\mathfrak{f})$ for any set S where $\lambda \mid \ell$. This appears to be the case with $\ell = 7$ for \mathfrak{f}_{11} , and we now show that it is indeed the case for \mathfrak{f}_9 . Let F be the elliptic curve with Cremona label 26b1:

$$F : y^2 + xy + y = x^3 - x^2 - 3x + 3,$$

which has conductor $2\mathfrak{B}$ as an elliptic curve over \mathcal{K} . As \mathcal{K}/\mathbb{Q} is cyclic, we know that F is modular over \mathcal{K} and hence corresponds to a Hilbert modular form of parallel weight 2 and level $2\mathfrak{B}$, and by comparing eigenvalues we can show that it in fact corresponds to \mathfrak{f}_9 . Now the point $(1, 0)$ on F has order 7. It follows that $7 \mid \#E(\mathbb{F}_q) = \text{Norm}(\mathfrak{q}) + 1 - a_q(\mathfrak{f})$ for all $q \nmid 26$, showing that for \mathfrak{f}_9 we can never

p	case	S	eigenform f	$B_S(f)$
7	$7 \mid x$	{3}	f_1	$2^8 \times 3^5 \times 7^6$
11	$11 \nmid x$	{23, 43}	f_2	1
	$11 \mid x$	{23, 43}	f_3 f_4	1 1
13	$13 \nmid x$	{79, 103}	f_5	$2^{6240} \times 3^{312}$
			f_6	$2^{12792} \times 3^{234}$
			f_7	$2^{10608} \times 3^{624}$
			f_8	$2^{18720} \times 3^{936}$
	$13 \mid x$	{3, 5, 31, 47}	f_9	7^2
			f_{10} f_{11} f_{12}	3^7 7^6 1

Table 2. Our choice of set of primes S and the value of $B_S(f)$ for each of the eigenforms in Table 1.

eliminate $\ell = 7$ by enlarging the set S . We can still complete the contradiction in this case as follows. Note that $\bar{\rho}_{f_9,7} \sim \bar{\rho}_{F,7}$ which is reducible. As $\bar{\rho}_{E,7}$ is irreducible we have $\bar{\rho}_{E,7} \not\sim \bar{\rho}_{f_9,7}$, completing the contradiction for $f = f_9$. We strongly suspect that reducibility of $\bar{\rho}_{f_{11},\lambda}$ (where λ is the unique prime above 7 of $\mathbb{Q}_{f_{11}}$), but we are unable to prove it.

Remark. We now explain why we believe that the above strategy will succeed in proving that (2) has no nontrivial primitive solutions, or at least in bounding the exponent ℓ , for larger values of p provided the eigenforms f at the relevant levels can be computed. The usual obstruction to bounding the exponent (see [Siksek 2012, Section 9]) comes from eigenforms f that correspond to elliptic curves with a torsion structure that matches the Frey curve \mathcal{E} . Let f be such an eigenform. Let $q \nmid 2p$ be a rational prime and q_1, \dots, q_r be the primes of \mathcal{K} above q . Note that $\text{Norm}(q_1) = \dots = \text{Norm}(q_r) = q^{d/r}$, where $d = [\mathcal{K} : \mathbb{Q}]$. We would like to estimate the “probability” that $B_q(f)$ is nonzero. Observe that if $B_q(f)$ is nonzero, then we obtain a bound for ℓ . Examining the definitions above shows that the ideal $B_q(f)$ is 0 if and only if there is some $(\eta, \mu) \in \mathcal{A}_q$ such that $a_q(E_{(\eta,\mu)}) = a_q(f)$ for $q = q_1, q_2, \dots, q_r$. Treating $a_q(E_{(\eta,\mu)})$ as a random variable belonging to the Hasse interval $[-2q^{d/2r}, 2q^{d/2r}]$, we see that the “probability” that $a_q(E_{(\eta,\mu)}) = a_q(f)$ is roughly $c/q^{d/2r}$, with $c = \frac{1}{4}$.

We can be a little more sophisticated and take account of the fact that the torsion structures coincide, and that these impose congruence restrictions on both

traces. In that case we should take $c = 1$ if \mathcal{E} has full 2-torsion (i.e., \mathcal{E} is the Frey curve E) and take $c = \frac{1}{2}$ if \mathcal{E} has just one nontrivial point of order 2 (i.e., $\mathcal{E} = E'$ and $p \equiv 1 \pmod{4}$). Thus the “probability” that $a_q(E_{(\eta,\mu)}) = a_q(f)$ for all $q \mid q$ simultaneously is roughly $c^r/q^{d/2}$. Since $B_q(f) = q \prod_{(\eta,\mu) \in \mathcal{A}_q} B_q(f, \eta, \mu)$, it follows that the “probability” \mathbb{P}_q (say) that $B_q(f)$ is nonzero satisfies

$$\mathbb{P}_q \sim \left(1 - \frac{c^r}{q^{d/2}}\right)^{q^2-1}.$$

For q large, we have $(1 - c^r/q^{d/2})^{q^{d/2}} \approx e^{-c^r}$. For $d \geq 5$, from the above estimates, we expect that $\mathbb{P}_q \rightarrow 1$ as $q \rightarrow \infty$. Thus we certainly expect our strategy to succeed in bounding the exponent ℓ .

Acknowledgments

We are grateful to the three referees for their careful reading of the paper and for suggesting many improvements. We are indebted to Lassina Dembélé, Steve Donnelly, Marc Masdeu and Jack Thorne for stimulating conversations.

References

- [Barnet-Lamb et al. 2012] T. Barnet-Lamb, T. Gee, and D. Geraghty, “Congruences between Hilbert modular forms: constructing ordinary lifts”, *Duke Math. J.* **161**:8 (2012), 1521–1580. MR Zbl
- [Barnet-Lamb et al. 2013] T. Barnet-Lamb, T. Gee, and D. Geraghty, “Congruences between Hilbert modular forms: constructing ordinary lifts, II”, *Math. Res. Lett.* **20**:1 (2013), 67–72. MR Zbl
- [Bennett 2006] M. A. Bennett, “The equation $x^{2n} + y^{2n} = z^5$ ”, *J. Théor. Nombres Bordeaux* **18**:2 (2006), 315–321. MR Zbl
- [Bennett and Chen 2012] M. A. Bennett and I. Chen, “Multi-Frey \mathbb{Q} -curves and the Diophantine equation $a^2 + b^6 = c^n$ ”, *Algebra Number Theory* **6**:4 (2012), 707–730. MR Zbl
- [Bennett and Skinner 2004] M. A. Bennett and C. M. Skinner, “Ternary Diophantine equations via Galois representations and modular forms”, *Canad. J. Math.* **56**:1 (2004), 23–54. MR Zbl
- [Bennett et al. 2010] M. A. Bennett, J. S. Ellenberg, and N. C. Ng, “The Diophantine equation $A^4 + 2^\delta B^2 = C^n$ ”, *Int. J. Number Theory* **6**:2 (2010), 311–338. MR Zbl
- [Bennett et al. 2015a] M. A. Bennett, I. Chen, S. R. Dahmen, and S. Yazdani, “Generalized Fermat equations: a miscellany”, *Int. J. Number Theory* **11**:1 (2015), 1–28. MR Zbl
- [Bennett et al. 2015b] M. A. Bennett, S. R. Dahmen, M. Mignotte, and S. Siksek, “Shifted powers in binary recurrence sequences”, *Math. Proc. Cambridge Philos. Soc.* **158**:2 (2015), 305–329. MR
- [Beukers 2012] F. Beukers, “The generalized Fermat equation”, pp. 119–149 in *Explicit methods in number theory*, Panor. Synthèses **36**, Soc. Math. France, Paris, 2012. MR Zbl
- [Blasius 2004] D. Blasius, “Elliptic curves, Hilbert modular forms, and the Hodge conjecture”, pp. 83–103 in *Contributions to automorphic forms, geometry, and number theory*, edited by H. Hida et al., Johns Hopkins University Press, Baltimore, 2004. MR Zbl
- [Bosma et al. 1997] W. Bosma, J. Cannon, and C. Playoust, “The Magma algebra system. I. The user language”, *J. Symbolic Comput.* **24**:3-4 (1997), 235–265. MR Zbl

- [Breuil and Diamond 2014] C. Breuil and F. Diamond, “Formes modulaires de Hilbert modulo p et valeurs d’extensions entre caractères galoisiens”, *Ann. Sci. Éc. Norm. Supér. (4)* **47**:5 (2014), 905–974. MR Zbl
- [Breuil et al. 2001] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, “On the modularity of elliptic curves over \mathbb{Q} : wild 3-adic exercises”, *J. Amer. Math. Soc.* **14**:4 (2001), 843–939. MR Zbl
- [Bruin and Najman 2016] P. Bruin and F. Najman, “A criterion to rule out torsion groups for elliptic curves over number fields”, *Res. Number Theory* **2** (2016), Art. 3, 13. MR Zbl
- [Darmon 1997] H. Darmon, “Faltings plus epsilon, Wiles plus epsilon, and the generalized Fermat equation”, *C. R. Math. Rep. Acad. Sci. Canada* **19**:1 (1997), 3–14. MR Zbl
- [Darmon and Granville 1995] H. Darmon and A. Granville, “On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$ ”, *Bull. London Math. Soc.* **27**:6 (1995), 513–543. MR Zbl
- [Darmon and Merel 1997] H. Darmon and L. Merel, “Winding quotients and some variants of Fermat’s last theorem”, *J. Reine Angew. Math.* **490** (1997), 81–100. MR Zbl
- [David 2012] A. David, “Caractère d’isogénie et critères d’irréductibilité”, preprint, 2012. arXiv
- [Dembélé and Voight 2013] L. Dembélé and J. Voight, “Explicit methods for Hilbert modular forms”, pp. 135–198 in *Elliptic curves, Hilbert modular forms and Galois deformations* (CRM Barcelona), edited by H. Darmon et al., Birkhäuser/Springer, Basel, 2013. MR Zbl
- [Derickx and van Hoeij 2014] M. Derickx and M. van Hoeij, “Gonality of the modular curve $X_1(N)$ ”, *J. Algebra* **417** (2014), 52–71. MR Zbl
- [Derickx et al. \geq 2016] M. Derickx, S. Kamienny, W. Stein, and M. Stoll, “Torsion points on elliptic curves over number fields of small degree”, in preparation.
- [Dieulefait and Freitas 2013] L. Dieulefait and N. Freitas, “Fermat-type equations of signature $(13, 13, p)$ via Hilbert cuspforms”, *Math. Ann.* **357**:3 (2013), 987–1004. MR Zbl
- [Ellenberg 2004] J. S. Ellenberg, “Galois representations attached to \mathbb{Q} -curves and the generalized Fermat equation $A^4 + B^2 = C^p$ ”, *Amer. J. Math.* **126**:4 (2004), 763–787. MR Zbl
- [Freitas 2015] N. Freitas, “Recipes to Fermat-type equations of the form $x^r + y^r = Cz^p$ ”, *Math. Z.* **279**:3 (2015), 605–639. MR Zbl
- [Freitas and Siksek 2015a] N. Freitas and S. Siksek, “The asymptotic Fermat’s last theorem for five-sixths of real quadratic fields”, *Compos. Math.* **151**:8 (2015), 1395–1415. MR Zbl
- [Freitas and Siksek 2015b] N. Freitas and S. Siksek, “Criteria for irreducibility of mod p representations of Frey curves”, *J. Théor. Nombres Bordeaux* **27**:1 (2015), 67–76. MR Zbl
- [Freitas and Siksek 2015c] N. Freitas and S. Siksek, “Fermat’s last theorem over some small real quadratic fields”, *Algebra Number Theory* **9**:4 (2015), 875–895. MR Zbl
- [Freitas et al. 2015] N. Freitas, B. V. Le Hung, and S. Siksek, “Elliptic curves over real quadratic fields are modular”, *Invent. Math.* **201**:1 (2015), 159–206. MR Zbl
- [Kamienny 1992] S. Kamienny, “Torsion points on elliptic curves and q -coefficients of modular forms”, *Invent. Math.* **109**:2 (1992), 221–229. MR Zbl
- [Kisin 2009] M. Kisin, “Moduli of finite flat group schemes, and modularity”, *Ann. of Math. (2)* **170**:3 (2009), 1085–1180. MR Zbl
- [Kraus 1997] A. Kraus, “Majorations effectives pour l’équation de Fermat généralisée”, *Canad. J. Math.* **49**:6 (1997), 1139–1161. MR Zbl
- [Kraus 2007] A. Kraus, “Courbes elliptiques semi-stables sur les corps de nombres”, *Int. J. Number Theory* **3**:4 (2007), 611–633. MR Zbl
- [Langlands 1980] R. P. Langlands, *Base change for $GL(2)$* , Annals of Mathematics Studies **96**, Princeton University Press, 1980. MR Zbl

- [Merel 1996] L. Merel, “Bornes pour la torsion des courbes elliptiques sur les corps de nombres”, *Invent. Math.* **124**:1-3 (1996), 437–449. MR Zbl
- [Miller 2014] J. C. Miller, “Class numbers of real cyclotomic fields of composite conductor”, *LMS J. Comput. Math.* **17**:suppl. A (2014), 404–417. MR Zbl
- [Parent 2000] P. Parent, “Torsion des courbes elliptiques sur les corps cubiques”, *Ann. Inst. Fourier (Grenoble)* **50**:3 (2000), 723–749. MR Zbl
- [Parent 2003] P. Parent, “No 17-torsion on elliptic curves over cubic number fields”, *J. Théor. Nombres Bordeaux* **15**:3 (2003), 831–838. MR Zbl
- [Serre 1972] J.-P. Serre, “Propriétés galoisiennes des points d’ordre fini des courbes elliptiques”, *Invent. Math.* **15**:4 (1972), 259–331. MR Zbl
- [Siksek 2012] S. Siksek, “The modular approach to Diophantine equations”, pp. 151–179 in *Explicit methods in number theory*, Panor. Synthèses **36**, Soc. Math. France, Paris, 2012. MR Zbl
- [Silverman 1994] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics **151**, Springer, New York, 1994. MR Zbl
- [Sinnott 1978] W. Sinnott, “On the Stickelberger ideal and the circular units of a cyclotomic field”, *Ann. of Math. (2)* **108**:1 (1978), 107–134. MR Zbl
- [Skinner and Wiles 1999] C. M. Skinner and A. J. Wiles, “Residually reducible representations and modular forms”, *Inst. Hautes Études Sci. Publ. Math.* **89** (1999), 5–126. MR Zbl
- [Swinnerton-Dyer 1973] H. P. F. Swinnerton-Dyer, “On l -adic representations and congruences for coefficients of modular forms”, pp. 1–55. Lecture Notes in Math., Vol. 350 in *Modular functions of one variable, III* (Antwerp, 1972), edited by W. Kuyk and J.-P. Serre, Springer, Berlin, 1973. MR Zbl
- [Thorne 2016] J. A. Thorne, “Automorphy of some residually dihedral Galois representations”, *Math. Ann.* **364**:1 (2016), 589–648. MR Zbl
- [Wiles 1995] A. Wiles, “Modular elliptic curves and Fermat’s last theorem”, *Ann. of Math. (2)* **141**:3 (1995), 443–551. MR Zbl

Communicated by Joseph H. Silverman

Received 2015-06-09

Revised 2016-03-22

Accepted 2016-06-22

samuele.anni@gmail.com

*Mathematics Institute, University of Warwick,
Coventry CV4 7AL, United Kingdom*

samir.siksek@gmail.com

*Mathematics Institute, University of Warwick,
Coventry CV4 7AL, United Kingdom*

Algebra & Number Theory

msp.org/ant

EDITORS

MANAGING EDITOR

Bjorn Poonen
Massachusetts Institute of Technology
Cambridge, USA

EDITORIAL BOARD CHAIR

David Eisenbud
University of California
Berkeley, USA

BOARD OF EDITORS

Dave Benson	University of Aberdeen, Scotland	Susan Montgomery	University of Southern California, USA
Richard E. Borcherds	University of California, Berkeley, USA	Shigefumi Mori	RIMS, Kyoto University, Japan
John H. Coates	University of Cambridge, UK	Raman Parimala	Emory University, USA
J-L. Colliot-Thélène	CNRS, Université Paris-Sud, France	Jonathan Pila	University of Oxford, UK
Brian D. Conrad	Stanford University, USA	Anand Pillay	University of Notre Dame, USA
Hélène Esnault	Freie Universität Berlin, Germany	Victor Reiner	University of Minnesota, USA
Hubert Flenner	Ruhr-Universität, Germany	Peter Sarnak	Princeton University, USA
Sergey Fomin	University of Michigan, USA	Joseph H. Silverman	Brown University, USA
Edward Frenkel	University of California, Berkeley, USA	Michael Singer	North Carolina State University, USA
Andrew Granville	Université de Montréal, Canada	Vasudevan Srinivas	Tata Inst. of Fund. Research, India
Joseph Gubeladze	San Francisco State University, USA	J. Toby Stafford	University of Michigan, USA
Roger Heath-Brown	Oxford University, UK	Ravi Vakil	Stanford University, USA
Craig Huneke	University of Virginia, USA	Michel van den Bergh	Hasselt University, Belgium
Kiran S. Kedlaya	Univ. of California, San Diego, USA	Marie-France Vignéras	Université Paris VII, France
János Kollár	Princeton University, USA	Kei-Ichi Watanabe	Nihon University, Japan
Yuri Manin	Northwestern University, USA	Efim Zelmanov	University of California, San Diego, USA
Philippe Michel	École Polytechnique Fédérale de Lausanne	Shou-Wu Zhang	Princeton University, USA

PRODUCTION

production@msp.org
Silvio Levy, Scientific Editor


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

The subscription price for 2016 is US \$290/year for the electronic version, and \$485/year (+\$55, if shipping outside the US) for print and electronic. Subscriptions, requests for back issues and changes of subscribers address should be sent to MSP.

Algebra & Number Theory (ISSN 1944-7833 electronic, 1937-0652 printed) at Mathematical Sciences Publishers, 798 Evans Hall #3840, c/o University of California, Berkeley, CA 94720-3840 is published continuously online. Periodical rate postage paid at Berkeley, CA 94704, and additional mailing offices.

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

PUBLISHED BY

 **mathematical sciences publishers**
nonprofit scientific publishing

<http://msp.org/>

© 2016 Mathematical Sciences Publishers

Algebra & Number Theory

Volume 10 No. 6 2016

Modular elliptic curves over real abelian fields and the generalized Fermat equation $x^{2\ell} + y^{2m} = z^p$	1147
SAMUELE ANNI and SAMIR SIKSEK	
Geometry and stability of tautological bundles on Hilbert schemes of points	1173
DAVID STAPLETON	
Anabelian geometry and descent obstructions on moduli spaces	1191
STEFAN PATRIKIS, JOSÉ FELIPE VOLOCH and YURI G. ZARHIN	
On the local Tamagawa number conjecture for Tate motives over tamely ramified fields	1221
JAY DAIGLE and MATTHIAS FLACH	
Heegner divisors in generalized Jacobians and traces of singular moduli	1277
JAN HENDRIK BRUINIER and YINGKUN LI	
On 2-dimensional 2-adic Galois representations of local and global fields	1301
VYTAUTAS PAŠKŪNAS	
A probabilistic Tits alternative and probabilistic identities	1359
MICHAEL LARSEN and ANER SHALEV	



1937-0652(2016)10:6;1-J