ON SERRE'S UNIFORMITY CONJECTURE FOR SEMISTABLE ELLIPTIC CURVES OVER TOTALLY REAL FIELDS

SAMUELE ANNI AND SAMIR SIKSEK

ABSTRACT. Let K be a totally real field, and let S be a finite set of non-archimedean places of K. It follows from the work of Merel, Momose and David that there is a constant $B_{K,S}$ so that if E is an elliptic curve defined over K, semistable outside S, then for all $p > B_{K,S}$, the representation $\overline{\rho}_{E,p}$ is irreducible. We combine this with modularity and level lowering to show the existence of an effectively computable constant $C_{K,S}$, and an effectively computable set of elliptic curves over K with CM $E_1, \dots, E_n$ such that the following holds. If E is an elliptic curve over K semistable outside S, and $p > C_{K,S}$ is prime, then either $\overline{\rho}_{E,p}$ is surjective, or $\overline{\rho}_{E,p} \sim \overline{\rho}_{E_i,p}$ for some $i = 1, \dots, n$.

1. Introduction

Let K be a number field. We write $G_K = \mathrm{Gal}(\overline{K}/K)$ for the absolute Galois group of K. For an elliptic curve E/K, we write $\overline{\rho}_{E,p}$ for the associated representation of G_K on the p-torsion of E:

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

We recall the following celebrated theorem of Serre.

Theorem 1 (Serre [26, Théorème 2])**.** *Let K be a number field and E an elliptic curve over K without CM. Then there is a constant $C_{E,K}$ such that for all $p > C_{E,K}$ the representation $\overline{\rho}_{E,p}$ is surjective.*

Serre's Uniformity Conjecture (originally formulated by Serre as a question [26, § 4.3] and [27]) asserts the existence of a constant C_K, depending only on K, such that if E is an elliptic curve over K without complex multiplication, and $p > C_K$ is a prime, then the representation $\overline{\rho}_{E,p}$ is surjective. Mazur [21] proved that $\overline{\rho}_{E,p}$ is irreducible for any prime $p > 163$ and elliptic curve E over $\mathbb{Q}$. Recently, Bilu, Parent and Rebolledo [3] proved, for $p \geq 11$, $p \neq 13$, and $E/\mathbb{Q}$ without complex multiplication, that the image of the representation is also not contained in the normalizer of a split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$.

No analogues of the above-mentioned theorems of Mazur and of Bilu, Parent and Rebolledo are known for elliptic curves over general number fields. The strongest

Date: April 12, 2016.
2010 *Mathematics Subject Classification.* Primary 11F80, Secondary 11G05, 11F41.
Key words and phrases. Elliptic curves, Serre's uniformity, modularity, Galois representation, level lowering, Hilbert modular forms.
The authors are supported by EPSRC Programme Grant 'LMF: L-Functions and Modular Forms' EP/K034383/1. The second-named author is also supported by an EPSRC Leadership Fellowship EP/G007268/1.

known result is Merel's Uniform Boundedness Theorem [22], which asserts the following: for $d \geq 1$, there is a constant B_d such that if E is an elliptic curve over a number field K of degree d, and $p > B_d$ is a prime, then $E(K)[p] = 0$. A number of irreducibility results are however known for semistable elliptic curves over number fields, whose proofs make essential use of Merel's Theorem. For example, Kraus [20, Appendix B] shows that if K is a number field that does not contain the Hilbert class field of an imaginary quadratic field, then there is a constant B_K such that for a prime $p > B_K$ and a semistable elliptic curve E/K, the representation $\overline{\rho}_{E,p}$ is irreducible.

As noted by Serre [21, Theorem 4], Mazur's Theorem cited above implies the following: if $E/\mathbb{Q}$ is a semistable elliptic curve without complex multiplication, then the representation $\overline{\rho}_{E,p}$ is surjective for any prime $p \geq 11$. To motivate our present work, it is appropriate to give a sketch of the argument. By Mazur's Theorem, we may suppose that $\overline{\rho}_{E,p}$ is irreducible. As $\mathbb{Q}$ has a real embedding, $\overline{\rho}_{E,p}$ is therefore absolutely irreducible (e.g. [25, Lemma 5]). If $\overline{\rho}_{E,p}$ is not surjective, then its image is contained in the normalizer N_{ns} of non-split Cartan subgroup C_{ns} or the normalizer N_{s} of a split Cartan subgroup C_{s}. In either case, the representation $\overline{\rho}_{E,p}$ induces a quadratic character $\psi : G_{\mathbb{Q}} \to N_*/C_* \cong \{\pm 1\}$. This character is unramified away from the archimedean and additive places. As E is semistable, we see that ψ is unramified away from ∞, and as the narrow class number of $\mathbb{Q}$ is 1, we have $\psi = 1$. It follows that the image of $\overline{\rho}_{E,p}$ is contained in C_{s} or C_{ns}. These groups are absolutely reducible, giving a contradiction. Over a number field K, the argument breaks down. First the narrow class number of K maybe greater than 1. Moreover, let L be the narrow class field of K. If the image of $\overline{\rho}_{E,p}$ is contained in the normalizer of a Cartan subgroup, then $\overline{\rho}_{E,p}(G_L)$ is contained in a Cartan subgroup: C_{s} or C_{ns}. If the former, then we can conclude the argument using (say) Kraus' result, provided L does not contain the Hilbert class field of an imaginary quadratic field. In the latter case, we do the same if L has some real embedding. It is clear, however, that the argument does not hold in general.

In this paper, we restrict ourselves to totally real fields K. This allows us to apply modularity and level lowering theorems to semistable elliptic curves E/K whose mod p image is contained in the normalizer of a Cartan subgroup.

Theorem 2. *Let K be a totally real field, and let S be a finite set of non-archimedean places of K. There are an effectively computable constant $C_{K,S}$, depending only on K and S, and a finite computable set $E_1, \ldots, E_n$ of elliptic curves over K with complex multiplication such that the following holds: if E is an elliptic curve over K semistable outside S, and $p > C_{K,S}$ is prime, then either $\overline{\rho}_{E,p}$ is surjective, or $\overline{\rho}_{E,p} \sim \overline{\rho}_{E_i,p}$ for some $i = 1, \ldots, n$.*

We would like to thank Fred Diamond, Nuno Freitas, James Newton and John Voight for helpful discussions. We would also thank the referee for the valuable suggestions and comments.

2. Irreducibility of mod p representations of elliptic curves

To deal with the Borel images we shall invoke the following theorem due to Freitas and Siksek [13], but is in fact a corollary of the ideas of David [8] and Momose [23] building on Merel's Uniform Boundedness Theorem [22].

Theorem 3 ([13, Theorem 1]). *Let K be a totally real Galois number field of degree d, with ring of integers $\mathcal{O}_K$ and Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$. Let $\mathfrak{S} = \{0, 12\}^G$, which we think of as the set of sequences of values 0, 12 indexed by $\tau \in G$. For $\mathbf{s} = (s_\tau) \in \mathfrak{S}$ and $\alpha \in K$, define the **twisted norm associated to** $\mathbf{s}$ by*

$$\mathcal{N}_{\mathbf{s}}(\alpha) = \prod_{\tau \in G} \tau(\alpha)^{s_\tau}.$$

Let $\epsilon_1, \dots, \epsilon_{d-1}$ be a basis for the unit group of K (modulo ± 1), and define

$$A_{\mathbf{s}} := \mathrm{Norm}\left(\gcd((\mathcal{N}_{\mathbf{s}}(\epsilon_1) - 1)\mathcal{O}_K, \dots, (\mathcal{N}_{\mathbf{s}}(\epsilon_{d-1}) - 1)\mathcal{O}_K)\right).$$

Let B be the least common multiple of the $A_{\mathbf{s}}$ taken over all $\mathbf{s} \neq (0)_{\tau \in G}$, $(12)_{\tau \in G}$. Then $B \neq 0$. Moreover, let $p \nmid B$ be a rational prime, unramified in K, such that $p \geq 17$ or $p = 11$. If E/K is an elliptic curve semistable at all $\upsilon \mid p$ and $\overline{\rho}_{E,p}$ is reducible then $p < (1 + 3^{6dh})$, where h is the class number of K.

3. Modularity

Let K be a totally real number field, and let E be an elliptic curve over K. Recall that E is **modular** if there exists a Hilbert cuspidal eigenform $\mathfrak{f}$ over K of parallel weight 2, with rational Hecke eigenvalues, such that the Hasse–Weil L-function of E is equal to the Hecke L-function of $\mathfrak{f}$. It is conjectured that all elliptic curves over totally real fields are modular, and, recently, modularity has been proved for elliptic curves over real quadratic fields, see [15].

For what follows, we need a suitable modularity lifting theorem. The following such theorem is derived in [15] as a relatively straightforward consequence of a deep theorem of Breuil and Diamond [5, Théorème 3.2.2], which builds on the work of Kisin [19], Gee [17], and Barnet-Lamb, Gee and Geraghty [1], [2].

Theorem 4 ([15, Theorem 2]). *Let E be an elliptic curve over a totally real number field K, and let $p \neq 2$ be a rational prime. Suppose $\overline{\rho}_{E,p}$ is modular in the following sense: $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ for some Hilbert cuspidal eigenform over K of parallel weight 2, where $\varpi \mid p$. Suppose moreover that $\overline{\rho}_{E,p}(G_{K(\zeta_p)})$ is absolutely irreducible. Then E is modular.*

Proposition 3.1. *Let K be a totally real field. Let $p \geq 7$ be a prime that is unramified in K. Suppose that E is semistable at some prime υ of K above p, and that moreover $\overline{\rho}_{E,p}$ is irreducible but not surjective. Then E is modular.*

Proof. Write $G := \overline{\rho}_{E,p}(G_K)$. As $\upsilon \mid p$ is unramified, we have $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$, and so $\det \overline{\rho}_{E,p} = \chi : G_K \to \mathbb{F}_p^*$ is surjective, where χ is the mod p cyclotomic character. By assumption $\overline{\rho}_{E,p}$ is irreducible but not surjective, and so G does not contain $\mathrm{SL}_2(\mathbb{F}_p)$. It follows [26, §2] that G is contained in the normalizer of a Cartan subgroup, or its projectivization $\mathbb{P}G := G/(G \cap \mathbb{F}_p^*)$ is isomorphic to A_4, S_4 or A_5. In particular, G does not contain elements of order p.

Write $I_\upsilon \subset G_K$ for the inertia subgroup at υ. As E is semistable at υ and υ is an unramified prime, we have (using [26, §1.11, §1.12] and the fact that G does not contain elements of order p):

$$\overline{\rho}_{E,p}|_{I_\upsilon} \sim \begin{pmatrix} \chi & 0 \\ 0 & 1 \end{pmatrix} \qquad \text{or} \qquad \overline{\rho}_{E,p}|_{I_\upsilon} \otimes_{\mathbb{F}_p} \mathbb{F}_{p^2} \sim \begin{pmatrix} \omega & 0 \\ 0 & \omega^p \end{pmatrix}; \tag{1}$$

here ω is a level 2 fundamental character $I_\upsilon \to \mathbb{F}_{p^2}^*$. More precisely, if E has good ordinary or multiplicative reduction at υ then we are in the first case of (1), and if E has good supersingular reduction at υ then we are in the second case. We observe from (1) that $\mathbb{P}G$ contains an element of order $p-1$ or $p+1$. Since $p \geq 7$, we see that $\mathbb{P}G$ is not isomorphic to A_4, S_4 and A_5. It follows that G is contained in the normalizer N_* of a Cartan subgroup C_*. The representation $\overline{\rho}_{E,p}$ is irreducible, and as K is totally real, $\overline{\rho}_{E,p}$ must be absolutely irreducible (e.g. [25, Lemma 5]). Thus the image G is contained in N_* but not in C_*.

Now, as $\overline{\rho}_{E,p}$ has solvable image, we can view it as a totally odd irreducible Artin representation. By a standard argument (c.f. [10, Proof of Lemma 4.2]), we have $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$, for some Hilbert modular form $\mathfrak{f}$ over K, of parallel weight 2, and $\varpi \mid p$.

By Theorem 4, in order to show that E is modular it is sufficient to show that $\overline{\rho}_{E,p}(G_{K(\zeta_p)})$ is absolutely irreducible. Suppose otherwise. It follows [15, Lemma 4.2] that $G^+ := G \cap \mathrm{GL}_2^+(\mathbb{F}_p)$ is absolutely reducible, where $\mathrm{GL}_2^+(\mathbb{F}_p)$ is the subgroup of $\mathrm{GL}_2(\mathbb{F}_p)$ consisting of matrices with square determinant. Suppose E has good ordinary or multiplicative reduction at υ and so we are in the first case of (1). Let g be a generator of $\mathbb{F}_p^*$. Then, with a suitable choice of basis for $E[p]$, the image G contains all matrices of the form $A_r := \left(\begin{smallmatrix} g^r & 0 \\ 0 & 1 \end{smallmatrix}\right)$; these share the eigenvectors $\mathbf{u} = \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$, $\mathbf{v} = \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$. As G is absolutely irreducible, it must contain some matrix B whose eigenvectors $\neq \mathbf{u}$, $\mathbf{v}$. It follows that G^+ contains the pair of matrices A_2, BA_s, where $s = 0$ or 1 according to whether $\det(B)$ is a square or non-square. It is easy to check that these do not have common eigenvectors, contradicting the absolute reducibility of G^+. If E has good supersingular reduction at υ then we are in the second case of (1). It is now easy to check, similarly to the above, that G^+ is absolutely irreducible, giving a contradiction. This completes the proof. □

4. Level lowering

In this section, K is a totally real field, and S a finite set of non-archimedean primes of K. Moreover, $p \geq 7$ is a rational prime that is unramified in K such that $\upsilon \notin S$ for all $\upsilon \mid p$.

Lemma 4.1. *Let E be an elliptic curve defined over K that is semistable outside S. Suppose that $\overline{\rho}_{E,p}$ is irreducible but not surjective. Then*

(i) $\overline{\rho}_{E,p}$ is unramified at all $\mu \notin S$, $\mu \nmid p$;
(ii) $\overline{\rho}_{E,p}$ is finite at all $\upsilon \mid p$.

Proof. Let $\upsilon \mid p$. We would like to prove (ii), which is certainly true if E has good reduction at υ. By hypothesis, E is semistable at υ, and so we may assume that E has multiplicative reduction at υ. Write $G_\upsilon \subset G_K$ for the decomposition group at υ. By the proof of Proposition 3.1, we know that $G = \overline{\rho}_{E,p}(G_K)$ does not contain any elements of order p. It immediately follows that $\overline{\rho}_{E,p}|_{G_\upsilon}$ is "peu ramifié", proving (ii).

Let μ be a non-archimedean prime of K, not in S, and not above p. Then E is semistable at μ, and so the inertia subgroup $I_\mu \subset G_K$ acts unipotently on $E[p]$. As G does not contain elements of order p, we have $\overline{\rho}_{E,p}(I_\mu) = 1$, proving (i). □

Now let

$$\mathcal{M} = \prod_{\mathfrak{l} \in S} \mathfrak{l}^{2+6\,\upsilon_{\mathfrak{l}}(2)+3\,\upsilon_{\mathfrak{l}}(3)}.$$

Lemma 4.2. *Assume the hypotheses of Lemma 4.1. Then there exists a Hilbert eigenform* $\mathfrak{f}$ *over* K *of parallel weight* 2 *and level dividing* $\mathcal{M}$ *such that* $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ *where* $\varpi \mid p$ *is a prime of* $\mathbb{Q}_{\mathfrak{f}}$*, the field generated by the eigenvalues of* $\mathfrak{f}$*.*

Proof. Let $\mathcal{N}$ be the conductor of E. The additive part of $\mathcal{N}$ divides $\mathcal{M}$ (e.g. [28, Theorem IV.10.4]). By Proposition 3.1 and Theorem 4, there is a Hilbert eigenform $\mathfrak{f}_0$ over K, with rational eigenvalues, level $\mathcal{N}$ and parallel weight 2 such that $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f}_0,p}$. By Lemma 4.1, we have $\overline{\rho}_{\mathfrak{f}_0,p}$ is finite at all $v \mid p$, and unramified at all $\mu \nmid \mathcal{M}$. Applying level lowering theorems due Fujiwara [16], Jarvis [18] and Rajaei [24], we may remove these primes from the level (without changing the weight); the argument is practically identical to that in [14, Theorem 7], and so we omit the details. □

Remark. Chen [6] observes that if E is an elliptic curve over $\mathbb{Q}$, and $\overline{\rho}_{E,p}$ has image contained in the normalizer of a Cartan subgroup, then p is a congruence prime for the newform attached to E. Our Lemma 4.2 encompasses Chen's observation.

5. Proof of Theorem 2

Assume the hypotheses of Theorem 2: in particular, let E be an elliptic curve semistable outside S. With the help of Theorem 3, we know that there is an effectively computable constant $C_{K,S}$ such that if $p > C_{K,S}$ then p is unramified in K, all the primes $v \mid p$ satisfy $v \notin S$, and $\overline{\rho}_{E,p}$ is irreducible. Suppose $\overline{\rho}_{E,p}$ is not surjective. We now apply Lemma 4.2 to deduce that $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ for some cuspidal Hilbert eigenform of parallel weight 2 and level dividing $\mathcal{M}$. There are certainly only finitely many such eigenforms. We would like to increase $C_{K,S}$ by an effectively computable amount so that the conclusion of Theorem 2 holds. Crucial to the effectivity is the existence of an algorithm [9] for determining the eigenforms $\mathfrak{f}$ of a given weight and level, as well as their Hecke eigenvalues at given primes, and the fields generated by these eigenvalues. We will eliminate all such eigenforms $\mathfrak{f}$ with $\mathbb{Q}_{\mathfrak{f}} \neq \mathbb{Q}$, where $\mathbb{Q}_{\mathfrak{f}}$ is the field generated by the eigenvalues of $\mathfrak{f}$. So suppose that $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},\varpi}$ where $\mathbb{Q}_{\mathfrak{f}} \neq \mathbb{Q}$. Let $\mathfrak{l}$ be the prime ideal of smallest possible norm such that $\mathfrak{l} \notin S$ and $a_{\mathfrak{l}}(\mathfrak{f}) \notin \mathbb{Q}$. If $\mathfrak{l} \mid p$, then $p \mid \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{l})$ and so we obtain a contradiction by supposing that $C_{K,S} > \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{l})$. We may therefore suppose that $\mathfrak{l} \nmid p$. Comparing the traces of the images of Frobenius at $\mathfrak{l}$ in the representations $\overline{\rho}_{E,p}$ and $\overline{\rho}_{\mathfrak{f},\varpi}$ we have either $a_{\mathfrak{l}}(\mathfrak{f}) \equiv a_{\mathfrak{l}}(E) \pmod{\varpi}$ if E has good reduction at $\mathfrak{l}$, or $a_{\mathfrak{l}}(\mathfrak{f}) \equiv \pm(\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{l}) + 1) \pmod{\varpi}$ if E has multiplicative reduction at $\mathfrak{l}$. In the former case, by the Hasse–Weil bounds, p divides

$$\prod_{|t| \leq B} \mathrm{Norm}_{\mathbb{Q}_{\mathfrak{f}}/\mathbb{Q}}(a_{\mathfrak{l}}(\mathfrak{f}) - t), \qquad B = 2(\mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{l}))^{1/2}.$$

As $a_{\mathfrak{l}}(\mathfrak{f}) \notin \mathbb{Q}$, all the terms in the product are non-zero, and so this gives a bound on p. By taking $C_{K,S}$ larger than this product we obtain a contradiction. If E has multiplicative reduction at $\mathfrak{l}$, then p divides

$$\mathrm{Norm}_{\mathbb{Q}_{\mathfrak{f}}/\mathbb{Q}}(a_{\mathfrak{l}}(\mathfrak{f}) - \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{l}) - 1) \cdot \mathrm{Norm}_{\mathbb{Q}_{\mathfrak{f}}/\mathbb{Q}}(a_{\mathfrak{l}}(\mathfrak{f}) + \mathrm{Norm}_{K/\mathbb{Q}}(\mathfrak{l}) + 1)$$

and again we obtain a contradiction by taking $C_{K,S}$ larger than this product. Thus we are reduced to finitely many forms $\mathfrak{f}$ satisfying $\mathbb{Q}_{\mathfrak{f}} = \mathbb{Q}$.

So far we proved that there are an effectively computable constant $C_{K,S}$ and a finite computable set $\mathfrak{f}_1, \ldots, \mathfrak{f}_n$ of Hilbert eigenforms over K of parallel weight 2 with $\mathbb{Q}$-rational eigenvalues such that the following holds: if E is an elliptic curve over K semistable outside S, and $p > C_{K,S}$ is prime, then either $\overline{\rho}_{E,p}$ is surjective, or $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f}_i,p}$ for some $i = 1, \dots, n$.

Next we have to show that the surviving forms $\mathfrak{f}$ have CM, possibly after enlarging $C_{K,S}$ by an effective amount. In fact, by a theorem of Dimitrov ([12, Theorem 2.1], [11, § 3]), if $\mathfrak{f}$ does not have CM, there is a constant $B_{\mathfrak{f}}$ such that for $p > B_{\mathfrak{f}}$ and $\varpi \mid p$, the image of $\overline{\rho}_{\mathfrak{f},\varpi}$ contains a conjugate of $\mathrm{SL}_2(\mathbb{F}_p)$. It is however unclear to us as to whether Dimitrov's proof can be made effective, and so we proceed in a more elementary manner.

By the proof of Proposition 3.1 the image of $\overline{\rho}_{E,p}$ is dihedral, and so there is a quadratic character ψ such that $\overline{\rho}_{E,p} \sim \overline{\rho}_{E,p} \otimes \psi$. It is immediate from Lemma 4.1 that ψ is unramified away from S, the archimedean primes, and the primes $\upsilon \mid p$. Suppose $\upsilon \mid p$. Comparing the restriction of the representation to the inertia subgroup at υ, displayed in (1), and the restriction of the twisted representation by ψ, it is easy to deduce that the quadratic character ψ is unramified at υ. Hence, its conductor divides $\prod_{\mathfrak{l} \in S} \mathfrak{l}^{1+2\,\upsilon_{\mathfrak{l}}(2)}$ and so ψ belongs to a finite effectively computable set of characters.

Suppose $\overline{\rho}_{E,p} \sim \overline{\rho}_{\mathfrak{f},p}$ where now $\mathfrak{f}$ has rational eigenvalues. Let $\mathfrak{g} = \mathfrak{f} \otimes \psi$. If $\mathfrak{g} = \mathfrak{f}$ then $\mathfrak{f}$ has CM as desired. Thus we may suppose $\mathfrak{g} \neq \mathfrak{f} \otimes \psi$. Let $\mathfrak{l}$ be the prime ideal of K of smallest possible norm so that $\mathfrak{l} \notin S$ and $a_{\mathfrak{l}}(\mathfrak{f}) \neq a_{\mathfrak{l}}(\mathfrak{g})$. As before, if $\mathfrak{l} \mid p$ or if E has multiplicative reduction at $\mathfrak{l}$, then we obtain a bound on p. We therefore suppose that $\mathfrak{l} \nmid p$ and E has good reduction at $\mathfrak{l}$. From the relations $\overline{\rho}_{E,p} \sim \overline{\rho}_{E,p} \otimes \psi$ and $\mathfrak{g} = \mathfrak{f} \otimes \psi$ we have $a_{\mathfrak{l}}(\mathfrak{f}) \equiv a_{\mathfrak{l}}(\mathfrak{g}) \pmod{p}$. As $a_{\mathfrak{l}}(\mathfrak{f}) \neq a_{\mathfrak{l}}(\mathfrak{g})$ we obtain a bound on p.

Now as the surviving forms $\mathfrak{f}_i$ are CM Hilbert eigenforms over K of parallel weight 2 with $\mathbb{Q}$-rational eigenvalues. As explained in [4, § 2.2], they correspond to CM elliptic curves E_i over K. The conductors of E_i are the levels of $\mathfrak{f}_i$. As there is an effective algorithm to determine elliptic curves of a given conductor (c.f. [7]), the proof is complete.

References

[1] T. Barnet-Lamb, T. Gee and D. Geraghty, *Congruences between Hilbert modular forms: constructing ordinary lifts*, Duke Math. Journal **161** (2012), 1521–1580.

[2] T. Barnet-Lamb, T. Gee and D. Geraghty, *Congruences between Hilbert modular forms: constructing ordinary lifts II*, Mathematical Research Letters **20** (2013), 81–86.

[3] Yu. Bilu, P. Parent, M. Rebolledo, *Rational points on* $X_0^+(p^r)$, Ann. Inst. Fourier, to appear; `arXiv:1104.4641`.

[4] Don Blasius, *Elliptic curves, Hilbert modular forms, and the Hodge conjecture*, pages 83-103 in: H. Hida, D. Ramakrishnan and F. Shahidi, *Contributions to automorphic forms, geometry, and number theory*, Johns Hopkins University Press, 2004.

[5] C. Breuil and F. Diamond, *Formes modulaires de Hilbert modulo p et valeurs d'extensions galoisiennes*, Annales Scientifiques de l'École Normale Supérieure, to appear.

[6] I. Chen, *Surjectivity of mod* ℓ *representations attached to elliptic curves and congruence primes*, Canadian Math. Bull. **45** (2002), no. 3, 337–348.

[7] J. Cremona and M. Lingham, *Finding all elliptic curves with good reduction outside a given set of primes*, Experimental Mathematics **16** (2007), 303–312.

[8] A. David, *Caractère d'isogénie et critères d'irréductibilité*, `arXiv:1103.3892v2`.

[9] L. Dembélé and J. Voight, *Explicit methods for Hilbert modular forms*, pages 135–198 in: L. Berger, G. Böckle, L. Dembélé, M. Dimitrov, T. Dokchitser, J. Voight, *Elliptic curves, Hilbert modular forms and Galois deformations*, Advanced Courses in Mathematics-CRM Barcelona, Springer Basel, 2013.

[10] L. Dieulefait and N. Freitas, *Fermat-type equations of signature* $(13, 13, p)$ *via Hilbert cuspforms*, Math. Ann. **357** (2013), no. 3, 987–1004.

[11] M. Dimitrov, *Galois representations modulo p and cohomology of Hilbert modular varieties*, Ann. Sci. Ecole Norm. Sup. **38** (2005), 505–551.

[12] M. Dimitrov, *Arithmetic aspects of Hilbert modular forms and varieties*, pages 119–134 in: L. Berger, G. Böckle, L. Dembélé, M. Dimitrov, T. Dokchitser, J. Voight, *Elliptic curves, Hilbert modular forms and Galois deformations*, Advanced Courses in Mathematics-CRM Barcelona, Springer Basel, 2013..

[13] N. Freitas and S. Siksek, *Criteria for irreducibility of mod p representations of Frey curves*, to appear in the Journal de Théorie des Nombres de Bordeaux.

[14] N. Freitas and S. Siksek, *An Asymptotic Fermat's Last Theorem for Five-Sixths of Real Quadratic Fields*, to appear in Compositio Mathematica.

[15] N. Freitas, B. V. Le Hung and S. Siksek, *Elliptic curves over real quadratic fields are modular*, to appear in Inventiones Mathematicae.

[16] K. Fujiwara, *Level optimisation in the totally real case*, `arXiv:0602586v1`.

[17] T. Gee, *Automorphic lifts of prescribed types*, Mathematische Annalen **350** (2011), 107–144.

[18] F. Jarvis *Correspondences on Shimura curves and Mazur's principle at p*, Pacific J. Math. **213** (2004), no. 2, 267–280.

[19] M. Kisin, *Moduli of finite flat group schemes, and modularity*, Annals of Math. **170** (2009), no. 3, 1085–1180.

[20] A. Kraus, *Courbes elliptiques semi-stables sur les corps de nombres*, International Journal of Number Theory **3** (2007), 611–633.

[21] B. Mazur, *Rational isogenies of prime degree*, Invent. Math. **44** (1978), 129–162.

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

[23] F. Momose, *Isogenies of prime degree over number fields*, Compositio Mathematica **97** (1995), 329–348.

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

[25] K. Rubin, *Modularity of mod* 5 *representations*, pages 463–474 in: G. Cornell, J. H. Silverman and G. Stevens, *Modular Forms and Fermat's Last Theorem*, Springer–Verlag, 1997..

[26] J.-P. Serre, *Properiétés galoisiennes des points d'ordre fini des courbes elliptiques*, Inventiones Math. **15** (1972), 259–331.

[27] J.-P. Serre, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Ètudes Sci. Publ. Math. 54 (1981), 123–201.

[28] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, GTM 151, Springer, 1994.

Mathematics Institute, University of Warwick, Coventry, CV4 7AL, United Kingdom
E-mail address: `samuele.anni@gmail.com`
E-mail address: `samir.siksek@gmail.com`