



On congruences between normalized eigenforms with different sign at a Steinberg prime

Luis Dieulefait and Eduardo Soto

Abstract. Let f be a newform of weight 2 on $\Gamma_0(N)$ with Fourier q -expansion $f(q) = q + \sum_{n \geq 2} a_n q^n$, where $\Gamma_0(N)$ denotes the group of invertible matrices with integer coefficients, upper triangular mod N . Let p be a prime dividing N once, $p \parallel N$, a Steinberg prime. Then, it is well known that $a_p \in \{1, -1\}$. We denote by K_f the field of coefficients of f . Let λ be a finite place in K_f not dividing $2p$ and assume that the mod λ Galois representation attached to f is irreducible. In this paper we will give necessary and sufficient conditions for the existence of another Hecke eigenform $f'(q) = q + \sum_{n \geq 2} a'_n q^n$ p -new of weight 2 on $\Gamma_0(N)$ and a finite place λ' of $K_{f'}$ such that $a_p = -a'_p$ and the Galois representations $\bar{\rho}_{f,\lambda}$ and $\bar{\rho}_{f',\lambda'}$ are isomorphic.

1. Introduction

Let $\bar{\mathbb{Q}}$ denote the algebraic closure of \mathbb{Q} in the field \mathbb{C} of complex numbers. Let f be a cusp Hecke eigenform of weight 2, level N and trivial nebentypus. We attach to f a sequence $\{a_n\}_{n \geq 1}$ of complex numbers consisting of the Fourier coefficients of f at infinity. We say that f is normalized if $a_1 = 1$. In this case $K_f = \mathbb{Q}(\{a_n\}_n) \subset \bar{\mathbb{Q}}$ and it is a number field. Let f, f' be normalized eigenforms of common weight 2, level N and N' respectively and trivial nebentypus. Consider the composite field $L = K_f \cdot K_{f'}$ in $\bar{\mathbb{Q}}$ and let \mathfrak{l} be a prime of L , $\ell\mathbb{Z} = \mathfrak{l} \cap \mathbb{Z}$. We will be interested in pairs of newforms f and f' for which

$$(1.1) \quad a_n \equiv a'_n \pmod{\mathfrak{l}} \quad \text{for every integer } n \text{ coprime to } \ell NN'.$$

The Fourier coefficients of a newform are completely determined by the a_p coefficients of prime subindex. It is easy to see then that (1.1) is equivalent to

$$(1.2) \quad a_p \equiv a'_p \pmod{\mathfrak{l}} \quad \text{for every prime } p \nmid \ell NN'.$$

Mathematics Subject Classification (2010): Primary 11F33; Secondary 11F80, 11G05.

Keywords: Galois representations, congruent modular forms, Steinberg prime.

Let $\lambda = \mathfrak{l} \cap \mathcal{O}_{K_f}$ and $\lambda' = \mathfrak{l} \cap \mathcal{O}_{K_{f'}}$ and assume that the residual Galois representations $\bar{\rho}_{f,\lambda}, \bar{\rho}_{f',\lambda'}$ attached to f and f' are irreducible. Then f, f' satisfy (1.1) if and only if $\bar{\rho}_{f,\lambda}$ and $\bar{\rho}_{f',\lambda'}$ are isomorphic. In general, it is not an easy problem to find for a given newform f another eigenform f' satisfying (1.1), neither proving the existence of such an eigenform f' . Ribet's level raising [6] and level lowering [7] theorems are very powerful in this context. In this article we will consider a newform f of weight 2 on $\Gamma_0(N)$ together with a prime $\lambda \nmid 2N$ of K_f and will give necessary and sufficient conditions for the existence of another eigenform f' of weight 2 on $\Gamma_0(N)$ and a prime λ' of $K_{f'}$ such that

- $\bar{\rho}_{f,\lambda}$ and $\bar{\rho}_{f',\lambda'}$ are isomorphic and
- $a_p = -a'_p$ for a prime p dividing N once and f' is p -new.

See [6] (Ribet 1990) for a definition of p -new, and theorem 4.4 for a precise statement of our result.

2. Galois representations mod λ attached to a normalized eigenform

From now on let us fix an odd prime ℓ and an immersion $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_\ell$. In particular, for every number field K we have fixed a prime λ over ℓ and a completion $K_\ell \subset \overline{\mathbb{Q}}_\ell$ of K with respect to λ . Let $\overline{\mathbb{F}}_\ell$ denote the residue field of the ring of integers of $\overline{\mathbb{Q}}_\ell$, which is indeed an algebraic closure of \mathbb{F}_ℓ . Let f be a normalized eigenform on $\Gamma_0(N)$ with q -expansion at infinity

$$f(z) = q + \sum_{n \geq 2} a_n q^n.$$

As in the introduction, K_f denotes the number field $\mathbb{Q}(\{a_n\}_n)$ of coefficients of f and by \mathcal{O}_f its ring of integers. Consider the ℓ -adic Galois representation attached to f by Deligne:

$$\rho_{f,\ell} : \text{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q}) \longrightarrow \text{GL}_2(K_{f,\ell}),$$

where $K_{f,\ell}$ denotes the completion of K_f with respect to (the fixed prime λ above) ℓ , and $\mathcal{O}_{f,\ell}$ denotes its ring of integers. Since $\text{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ is compact, one can (non-canonically) embed its image in $\text{GL}_2(\mathcal{O}_{f,\ell})$,

$$\iota : \text{Im } \rho_{f,\ell} \longrightarrow \text{GL}_2(\mathcal{O}_{f,\ell}).$$

Recall that $\mathcal{O}_{f,\ell}$ is a local ring whose residue field $\mathcal{O}_{f,\ell}/\mathfrak{m}_{f,\ell}$ is a finite extension of \mathbb{F}_ℓ contained in $\overline{\mathbb{F}}_\ell$. Reducing $\iota \circ \rho_{f,\ell} \bmod \mathfrak{m}_{f,\ell}$, we obtain the mod ℓ Galois representation

$$\bar{\rho}_{f,\ell} : \text{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q}) \longrightarrow \text{GL}_2(\mathcal{O}_{f,\ell}/\mathfrak{m}_{f,\ell}) \hookrightarrow \text{GL}_2(\overline{\mathbb{F}}_\ell)$$

attached to f (independent of ι up to semi-simplification), satisfying

$$\text{tr } \bar{\rho}_{f,\ell}(\text{Frob}_p) \equiv a_p \quad \det \bar{\rho}_{f,\ell}(\text{Frob}_p) \equiv p \pmod{\mathfrak{m}_{f,\ell}}$$

for every rational prime $p \nmid \ell N$.

3. Lowering and raising the levels

We state here Ribet’s theorems, they will be the main tools needed in the proof of our theorem. See [7] and [6] (theorem 1 and remarks in section 3) for the proofs.

Theorem 3.1 (Ribet’s level lowering theorem). *Let f be a newform of weight 2 on $\Gamma_0(N)$, let p be a prime dividing N once. Assume that $\ell \nmid 2p$ and that the mod ℓ Galois representation*

$$\bar{\rho}_{f,\ell} : \text{Gal}(\overline{\mathbb{Q}} | \mathbb{Q}) \longrightarrow \text{GL}_2(\overline{\mathbb{F}}_\ell)$$

is irreducible and unramified at p . If one or both of the following conditions hold,

- (1) $\ell \nmid N$,
- (2) $\bar{\rho}_{f,\ell}|_{G_{\mathbb{Q}(\zeta_\ell)}}$ *is irreducible,*

then there exists a newform f' of weight 2 on $\Gamma_0(M)$ for some M divisor of N/p such that $\bar{\rho}_{f',\ell}$ is isomorphic to $\bar{\rho}_{f,\ell}$.

Proof. By theorem 1.1 of [7], we may assume that $\bar{\rho}_{f,\ell}|_{G_{\mathbb{Q}(\zeta_\ell)}}$ is irreducible. We first prove the existence of a representation $\rho : \text{Gal}(\overline{\mathbb{Q}} | \mathbb{Q}) \rightarrow \text{GL}_2(\overline{\mathbb{Q}}_p)$ lifting $\bar{\rho}_{f,\ell}$ satisfying enough properties such that, if modular, it arises from a cusp eigenform of weight 2 on $\Gamma_0(N/p)$. We use some results of [8] §2, §7, and we follow the notation therein. Consider the lifting problem with:

- (i) Σ equal to the set of primes different from p at which $\rho_{f,\ell}$ is ramified and ℓ ,
- (ii) ψ trivial,
- (iii) type function t equal to the one attached to $\rho_{f,\ell}$,
- (iv) for each $q \in \Sigma$ the inertial type τ_q of $\rho_{f,\ell}|_{G_q}$.

By proposition 2.6.1 in [8], t is definite. Since $\{\rho_{f,\ell}|_{G_q}\}_{q \in \Sigma}$ is a local solution to our lifting problem, theorem 7.2.1 in [8] says that there is a global solution ρ that is finitely ramified weight two. It is irreducible since $\bar{\rho}$ is irreducible, and odd since its determinant is the cyclotomic character. By theorem 1.1.4 in [8], ρ is modular, so it arises from a newform g of weight two. Comparing $\rho_{f,\ell}|_{G_q}$ and $\rho|_{G_q}$ at every q we have that g has level N/p and trivial nebentypus (since $\psi = 1$). \square

Theorem 3.2 (Ribet’s level raising theorem). *Let f be a normalized eigenform of weight 2 on $\Gamma_0(N)$ such that the mod ℓ Galois representation*

$$\bar{\rho}_{f,\ell} : \text{Gal}(\overline{\mathbb{Q}} | \mathbb{Q}) \longrightarrow \text{GL}_2(\overline{\mathbb{F}}_\ell)$$

is irreducible. Let $p \nmid \ell N$ be a prime satisfying

$$\text{tr } \bar{\rho}_{f,\ell}(Frob_p) \equiv (-1)^j(p + 1) \pmod{\ell}$$

for some $j \in \{0, 1\}$. Then there exists a normalized eigenform f' p -new of weight 2 on $\Gamma_0(pN)$ such that $\bar{\rho}_{f,\ell}$ is isomorphic to $\bar{\rho}_{f',\ell}$. Moreover, the p -th Fourier coefficient a'_p of f' equals $(-1)^j$. If $p + 1 \equiv 0 \pmod{\ell}$, then there are at least two such eigenforms f' : one for each coefficient $a'_p \in \{\pm 1\}$.

4. Local decomposition at Steinberg primes and proof of the theorem

In this article we consider newforms f of weight 2 on $\Gamma_0(N)$ and we work with primes p dividing N once. Recall that in this case the local type of (the automorphic form attached to) f at p is a twist of the Steinberg representation.

Definition 4.1. Let f be a normalized cusp Hecke eigenform of weight 2 level N and trivial nebentypus. We say that a prime p is a *Steinberg prime* of f if $p \parallel N$ and f is p -new.

Remark 4.2. With the hypothesis of definition 4.1, corollary 4.6.20 in [5] says that there is a unique newform g of weight 2 on $\Gamma_0(N')$ for some divisor N' of N , $p \mid N'$, such that f is in the old-space generated by g . Theorem 4.6.17 in [5] implies that $a_p(g) \in \{-1, 1\}$. Since f is normalized and $p \nmid N/N'$, it is easy to see that $a_p(f) = a_p(g)$.

Here we state a useful lemma related to the local behavior of the mod ℓ Galois representations at a Steinberg prime.

Lemma 4.3 (Langlands). *Let f be a cusp Hecke eigenform of weight 2, level N and trivial nebentypus. Let p be a Steinberg prime of f . Then one has that*

$$\bar{\rho}_{f,\ell}|_{D_p} \sim \begin{pmatrix} \bar{\chi} \cdot \bar{\varepsilon}_\ell & * \\ 0 & \bar{\chi} \end{pmatrix}$$

for every prime $\ell \neq p$, where $\bar{\chi}: D_p \rightarrow \mathbb{F}_\ell^*$ denotes the unramified character that maps Frob_p to $a_p(f)$, and $\bar{\varepsilon}_\ell$ denotes the mod ℓ cyclotomic character.

Proof. See [4] (Loeffler, Weinstein 2012), proposition 2.8; we follow the notation therein. The newform f is p -primitive since $p \parallel N$. Recall that Hecke correspondence (a modification of local Langlands correspondence) attaches to $\pi_{f,p} \simeq St \otimes \alpha$, for an unramified character α of \mathbb{Q}_p^* , a two dimensional Weil–Deligne representation that corresponds to a Galois representation $r : \text{Gal}(\bar{\mathbb{Q}}_p \mid \mathbb{Q}_p) \rightarrow \text{GL}_2(\bar{\mathbb{Q}}_\ell)$ of the form

$$r \sim \begin{pmatrix} \alpha \cdot \varepsilon_\ell & * \\ 0 & \alpha \end{pmatrix},$$

where we identify α with a character of $\text{Gal}(\bar{\mathbb{Q}}_p \mid \mathbb{Q}_p)$ via local class field theory. It is a theorem of Carayol [1] that $\rho_{f,\ell}|_{D_p}$ and r are isomorphic. □

Theorem 4.4 (Main result). *Let f be a newform of weight 2 on $\Gamma_0(N)$ and let p be a prime at which f is Steinberg. Let $\ell \nmid 2p$ be a prime. Assume either*

- (1) $\ell \nmid N$ and $\bar{\rho}_{f,\ell}$ is absolutely irreducible, or
- (2) $\bar{\rho}_{f,\ell}|_{G_{\mathbb{Q}(\zeta_\ell)}}$ is absolutely irreducible.

Then the following are equivalent:

(a) $\bar{\rho}_{f,\ell}$ is unramified at p and

$$p \equiv -1 \pmod{\ell}.$$

(b) There is a normalized eigenform f' p -new of weight 2 on $\Gamma_0(N)$ such that $\bar{\rho}_{f',\ell}$ is isomorphic to $\bar{\rho}_{f,\ell}$ and

$$a_p = -a'_p$$

where a_p (resp. a'_p) is the p -th Fourier coefficient of f (resp. f').

Proof. (b) \Rightarrow (a). Let us write $\bar{\rho} = \bar{\rho}_{f,\ell}$ and $\bar{\rho}' = \bar{\rho}_{f',\ell}$ for simplicity. Let $D_p \subseteq \text{Gal}(\overline{\mathbb{Q}} \mid \mathbb{Q})$ be a decomposition group of p . Since $\{a_p, a'_p\} = \{1, -1\}$, we may assume without loss of generality that $\bar{\rho}, \bar{\rho}'$ act locally at p as

$$\bar{\rho}|_{D_p} \sim \begin{pmatrix} \bar{\varepsilon}_\ell & * \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \bar{\rho}'|_{D_p} \sim \begin{pmatrix} \bar{\chi} \cdot \bar{\varepsilon}_\ell & * \\ 0 & \bar{\chi} \end{pmatrix},$$

due to lemma 4.3. Since $\bar{\rho}$ and $\bar{\rho}'$ are isomorphic so are their local behaviors. Thus, specializing at a Frobenius map,

$$\begin{pmatrix} p & * \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} -p & * \\ 0 & -1 \end{pmatrix} \pmod{\ell}.$$

Eigenvalues must coincide and $\ell > 2$, so

$$p \equiv -1 \pmod{\ell}.$$

To see that $\bar{\rho}$ is unramified at p , notice that

$$\bar{\chi} \bar{\varepsilon}_\ell \neq \bar{\varepsilon}_\ell.$$

Thus, $\bar{\rho}|_{D_p} \simeq \bar{\varepsilon}_\ell \oplus \bar{\chi} \bar{\varepsilon}_\ell$. Indeed, lemma 4.3 and the isomorphism $\bar{\rho} \simeq \bar{\rho}'$ say that $\bar{\rho}|_{D_p}$ has two 1-dimensional subrepresentations. Since the actions are different, they generate the whole space. Hence $\bar{\rho}$ is unramified at p .

(a) \Rightarrow (b). Ribet’s lowering level theorem applies to the modular representation $\bar{\rho}_{f,\ell}$ of level N . Thus, there exists a newform g of weight 2 on $\Gamma_0(M)$, for some $M \mid N/p$ such that $\bar{\rho}_{g,\ell} \sim \bar{\rho}_{f,\ell}$. Moreover, we have that

$$\text{tr} \bar{\rho}_{f,\ell}(\text{Frob}_p) \equiv a_p \cdot (p + 1) \equiv 0 \pmod{\ell},$$

by lemma 4.3. Now we can apply Ribet’s raising level theorem to $\bar{\rho}_{g,\ell}$ and there exists an eigenform f' p -new on $\Gamma_0(N)$ such that

$$\bar{\rho}_{f',\ell} \sim \bar{\rho}_{f,\ell}.$$

By §3, page 9, of [6], when both conditions

$$\text{tr} \bar{\rho}_{g,\ell}(\text{Frob}_p) \equiv \pm(p + 1) \pmod{\ell}$$

are satisfied Ribet’s proof allows us to choose the a_p coefficient of f' . We shall choose f' such that $a'_p = -a_p$ and the implication holds. \square

Remark 4.5. Let f be a newform satisfying (a). We expect that theorem 4.4 can be strengthened so that f' can be chosen to be a newform, not necessarily unique. This would follow from a stronger version of [6]. See section 5 for an example.

5. An example

In this section we are going to give an example of mod 5 Galois representation to which our theorem applies. We will use many well-known properties of elliptic curves without proof.

Let ℓ be a prime, $n > 0$ an integer and E an elliptic curve over \mathbb{Q} . The ℓ^n -th torsion group $E[\ell^n]$ of E has a natural structure of free $\mathbb{Z}/\ell^n\mathbb{Z}$ -module of rank 2. The action of the Galois group $G = \text{Gal}(\overline{\mathbb{Q}} | \mathbb{Q})$ is compatible with the $\mathbb{Z}/\ell^n\mathbb{Z}$ -module structure of $E[\ell^n]$, so that $E[\ell^n]$ has a natural structure of $(\mathbb{Z}/\ell^n\mathbb{Z})[G]$ -module. That is, the action induces a group homomorphism

$$\bar{\rho}_{E,\ell^n} : \text{Gal}(\overline{\mathbb{Q}} | \mathbb{Q}) \longrightarrow \text{Aut}_{\mathbb{Z}/\ell^n\mathbb{Z}}(E[\ell^n]) \simeq \text{GL}_2(\mathbb{Z}/\ell^n\mathbb{Z})$$

where the isomorphism depends on the choice of a basis in $E[\ell^n]$. The case $n = 1$ is of special interest and is known as the mod ℓ Galois representation attached to E . The Tate module $\mathcal{T}_\ell E = \varprojlim E[\ell^n]$ of E at ℓ is a free \mathbb{Z}_ℓ -module of rank 2. The morphisms $\{\bar{\rho}_{E,\ell^n}\}$ induce a group morphism

$$\rho_{E,\ell} : \text{Gal}(\overline{\mathbb{Q}} | \mathbb{Q}) \longrightarrow \text{Aut}(\mathcal{T}_\ell E) \simeq \text{GL}_2(\mathbb{Z}_\ell)$$

known as the ℓ -adic Galois representation attached to E . The mod ℓ Galois representation $\bar{\rho}_{E,\ell}$ attached to E can be recovered from $\rho_{E,\ell}$ by taking reduction mod $\ell\mathbb{Z}_\ell$.

Well-known modularity theorems as Wiles, Taylor–Wiles and Breuil–Conrad–Diamond–Taylor state that such a ℓ -adic Galois representation is isomorphic to the Galois representation $\rho_{f_E,\ell}$ attached to some newform f_E of weight 2 on $\Gamma_0(N)$, for N equal to the conductor of E and $K_f = \mathbb{Q}$. Moreover, the p -th Fourier coefficient of f_E coincides with the c_p coefficient of E (defined below) for every prime p . In this section we will apply theorem 4.4 to the mod 5 Galois representation $\bar{\rho}_{E,5} \simeq \bar{\rho}_{f_E,5}$ attached to the following elliptic curve given by a (global minimal) Weierstrass equation:

$$E : ZY^2 + XYZ + YZ^2 = X^3 + X^2Z - 614XZ^2 - 5501Z^3.$$

Its discriminant is

$$\Delta = 2^5 \cdot 19^5 \cdot 37.$$

For every prime p , let \tilde{E}_p denote the curve obtained by reducing mod p a global minimal Weierstrass model of E . As usual, we consider the value

$$c_p = p + 1 - \#\tilde{E}_p$$

for every prime p . One can check that

$$\begin{cases} \tilde{E}_2 \text{ has a node whose tangent lines are defined over } \mathbb{F}_2, \\ \tilde{E}_p \text{ has a node whose tangent lines have slopes in } \mathbb{F}_{p^2} \setminus \mathbb{F}_p \text{ for } p \in \{19, 37\}, \\ \tilde{E}_p \text{ is an elliptic curve over } \mathbb{F}_p, \text{ otherwise.} \end{cases}$$

Thus E has conductor $N = 2 \cdot 19 \cdot 37 = 1406$, $c_2 = -c_{19} = -c_{37} = 1$ and there is a newform $f = q + \sum_{n \geq 2} a_n q^n$ of weight 2 on $\Gamma_0(1406)$ such that

- $\rho_{E,5}$ and $\rho_{f,5}$ are isomorphic.
- $c_p = a_p$ for every prime p .

Let us see now that $\bar{\rho}_{f,5}$ satisfies the hypothesis of the theorem 4.4 for $p = 19$. Since

$$\begin{aligned} E_3 &= \{[x : y : z] \in \mathbb{P}_{\mathbb{F}_3}^2 : zy^2 + xyz + yz^2 = x^3 + x^2z + xz^2 + z^3\} \\ &= \{[0 : 1 : 0], [2 : 0 : 1]\}, \end{aligned}$$

then $c_3 = 2$ and the characteristic polynomial of $\bar{\rho}_{f,5}(\text{Frob}_3)$ is congruent to

$$P(X) = X^2 - 2X + 3 \pmod{5}.$$

Since the discriminant of $P(X)$ is $2 \pmod{5}$ and 2 is not a square in \mathbb{F}_5 , then $P(X)$ is irreducible over \mathbb{F}_5 . In particular $\bar{\rho}_{f,5} : \text{Gal}(\mathbb{Q} | \mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_5)$ is irreducible. It is well known that such a representation is irreducible if and only if it is absolutely irreducible, thus $\bar{\rho}_{f,5}$ is absolutely irreducible. Indeed, $\bar{\rho}_{f,5}$ is odd and hence its image contains a matrix E with eigenvalues $\{\pm 1\}$. Say $\bar{\rho}_{f,5}(c) = E$. If $\bar{\rho}_{f,5}$ is not absolutely irreducible, $\bar{\rho}_{f,5}$ is conjugate over \mathbb{F}_5 to a representation of the form

$$\bar{r} = \begin{pmatrix} \theta_1 & * \\ 0 & \theta_2 \end{pmatrix}$$

for some characters θ_1, θ_2 . Take $\epsilon := \theta_1(c) \in \{\pm 1\}$. By changing coordinates over \mathbb{F}_5 , we may assume that

$$\bar{\rho}_{f,5}(c) = \begin{pmatrix} \epsilon & 0 \\ 0 & -\epsilon \end{pmatrix}.$$

By comparing \bar{r} and $\bar{\rho}_{f,5}$ at c , it follows that the conjugation matrix is upper triangular and hence that $\bar{\rho}_{f,5}$ is upper triangular over \mathbb{F}_5 .

On the other hand, it is well known (see [2] proposition 2.12) that for a prime $p \neq \ell$ dividing once the conductor of an elliptic curve E , $\bar{\rho}_{E,\ell}$ is unramified at p if and only if $\ell \mid v_p(\Delta)$. Since $v_{19}(\Delta) = 5$, $\bar{\rho}_{f,5}$ is also unramified at 19. Hence theorem 4.4 applies to $\bar{\rho}_{E,5}$, and there exists another eigenform f' of weight 2 on $\Gamma_0(1406)$ such that $\bar{\rho}_{f',\ell}$ is isomorphic to $\bar{\rho}_{E,5}$. Thus,

$$c_p \equiv a_p \pmod{\mathfrak{m}_{f',\ell}} \text{ for every } p \nmid 1406 \cdot 5,$$

and the 19th Fourier coefficient a'_{19} of f' satisfies

$$a'_{19} = -c_{19} = 1.$$

In this example we can find an elliptic curve E' of conductor 1406 such that its corresponding newform f' satisfies part (b) of theorem 4.4. In order to find E' , we have assumed that f' can be chosen to be a newform, see remark 4.5. Assuming that f' is newform, we can determine a'_2 and a'_{37} of f' as follows. If $a'_2 = -c_2$, theorem 4.4 applies with $\ell = 5$ and $p = 2$, so we conclude that $2 \equiv -1 \pmod{5}$.

Hence, $a'_2 \neq -c_2$. Since $a'_2 \in \{\pm 1\}$, then $a'_2 = c_2 = 1$. Similarly, one can prove that $a'_{37} = c_{37} = -1$. There are three newforms (up to conjugation) with this configuration of signs $(a'_2, a'_{19}, a'_{37}) = (1, 1, -1)$ out of sixteen newforms of weight 2 on $\Gamma_0(1406)$. One of those (the only one satisfying $a'_3 \equiv c_3 \pmod{\mathfrak{m}_{f',5}}$) corresponds to the elliptic curve E' given by a global minimal Weierstrass equation

$$E' : Y^2Z + XYZ + YZ^2 = X^3 - X^2Z - 1191XZ^2 + 507615Z^3.$$

One can check that its conductor is $N = 1406$ and that $c'_2 = c'_{19} = -c'_{37} = 1$. We will use Sturm's bound (see theorem 9.18 in Stein's book [9]) in order to prove that E' corresponds to an eigenform f' as in theorem 4.4. Notice that

$$c'_{19} = 19 + 1 - \#\tilde{E}' = 1 = -c_{19}.$$

Hence, Sturm's result does not apply to the pair $(f_E, f_{E'})$. After twisting both modular forms $f_E, f_{E'}$ by the quadratic character ψ of conductor 19, we get two cusp forms $f_E^\psi, f_{E'}^\psi$ of weight 2 on $\Gamma_0(1406 \cdot 19)$. Sturm's bound for cusp forms of weight 2 on $\Gamma_0(1406 \cdot 19)$ is 7218.38, and one can check computationally that

$$(5.1) \quad \psi(p) c_p \equiv \psi(p) c'_p \pmod{5}$$

for every prime $p < 7219$. Hence, Sturm's result applies to $(f_E^\psi, f_{E'}^\psi)$ and (5.1) is true for every p . Thus

$$c_p \equiv c'_p \pmod{5}$$

for every prime p for which $\psi(p) \neq 0$, i.e., for every prime $p \neq 19$.

Remark 5.1. Take again $\ell = 5$, $p = 19$. Similarly one can check that at level 741 there is an elliptic curve (Cremona's labeling 741b) satisfying theorem 4.4 a). Notice that there exists no elliptic curve of conductor 741 corresponding to an f' as in theorem 4.4 b). However, it does exist a newform f on $\Gamma_0(741)$ and weight 2 satisfying theorem 4.4 b), it satisfies $[K_f : \mathbb{Q}] = 4$.

Acknowledgments. The authors are grateful to K. Ribet for providing so much valuable feedback. The second author wants to thank X. Guitart and S. Anni for many stimulating conversations, and N. Billerey for helpful comments.

References

- [1] CARAYOL, H.: Sur les représentations ℓ -adiques associées aux formes modulaires de Hilbert. *Ann. Sci. École Norm. Sup. (4)* **19** (1986), no. 3, 409–468.
- [2] DARMON, H., DIAMOND, F. AND TAYLOR, R.: *Fermat's last theorem. Elliptic curves, modular forms and Fermat's last theorem*. Int. Press, Cambridge, MA, 1997.
- [3] LANGLANDS, R. P.: Modular forms and ℓ -adic representations. In *Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, 361–500. Lecture Notes in Math. 349, Springer, Berlin, 1973.

- [4] LOEFFLER, D. AND WEINSTEIN, J.: On the computation of local components of a newform. *Math. Comp.* **81** (2012), no. 278, 1179–1200.
- [5] MIYAKE, T.: *Modular forms*. Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2006.
- [6] RIBET, K. A.: Raising the levels of modular representations. In *Séminaire de Théorie des Nombres (Paris 1987–88)*, 259–271. Progr. Math. 81, Birkhäuser, Boston, MA, 1990.
- [7] RIBET, K. A.: On modular representations of $\text{Gal}(\bar{Q}/Q)$ arising from modular forms. *Invent. Math.* **100** (1990), no. 2, 431–476.
- [8] SNOWDEN, A.: On two dimensional weight two odd representations of totally real fields. Preprint, [arXiv:0905.4266](https://arxiv.org/abs/0905.4266), 2009.
- [9] STEIN, W.: *Modular forms, a computational approach*. Graduate Studies in Mathematics 79, American Mathematical Society, Providence, RI, 2007.

Received November 11, 2015; revised December 7, 2016.

LUIS DIEULEFAIT: Departament de Matemàtiques i Informàtica, Universitat de Barcelona, Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain.

E-mail: ldieulefait@ub.edu

EDUARDO SOTO: Departament de Matemàtiques i Informàtica, Universitat de Barcelona, Gran Via de les Corts Catalanes 585, 08007 Barcelona, Spain.

E-mail: eduard.soto@ub.edu