On level-lowering for mod 2 representations.

Kevin Buzzard

Version of 1 Oct 1999.

Abstract.

The theory of "level-lowering" for mod l modular forms is now essentially complete when l is odd, thanks to work of Ribet and others. In the paper [T], Taylor explains how one might be able to attack new cases of Artin's conjecture if (amongst other things) Wiles' results on lifting of modular mod l Galois representations could be extended to the case $l = 2$. One ingredient necessary for such an extension is a level-lowering theorem valid in characteristic 2. In this paper we prove such a theorem, for most mod 2 Galois representations, using, for the most part, Ribet's ideas. In fact the results here, together with work of Dickinson, Shepherd-Barron and Taylor, enable new cases of Artin's conjecture to be established (see [BDST]).

§0. Introduction and notation.

Let l be a prime, and consider a continuous irreducible representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_l)$. Serre conjectured in [S2] that any such representation arose as the mod l representation associated to a modular form. Serre also gave a conjectural recipe for a level and a weight at which one might expect this form to arise. Let us refer to the conjecture that ρ arises from some modular form as the *weak Serre conjecture*. Furthermore, let us refer to to the conjecture that ρ arises from a form of Serre's predicted weight and level the *strong Serre conjecture*.

Although very little is known about the truth of these conjectures in general, for odd primes l the conjectures have, as a result of work of many people over the last 15 years, been proved to be equivalent. The case $l = 2$ has been more troublesome. If ρ is known to come from a modular form, then the statement that it comes from a form of Serre's predicted weight is known only modulo some unchecked compatibilities in the paper [G]. As for the level, again Serre's prediction was not known to be correct because a certain key intermediate result of Ribet was not known for $l = 2$. It is the purpose of this paper to establish this result, at least for a wide class of representations (those that "satisfy multiplicity one"), and hence to prove that Serre's conjectured level can be attained. We remark that the case where the image of ρ is dihedral has already been treated in many cases when $l = 2$, in [RT].

This paper has three sections. The first gives a proof that one can always remove 2 from the level of an absolutely irreducible modular mod 2 Galois representation, at the expense of increasing the weight. This result is already well known, as it can be deduced, for example, from the theory of 2-adic modular forms, but no elementary proof is in the literature. We give a simple proof in the style of [R3].

The second section seems to be new, but in fact most of the ideas in the proof were already known to the experts. The section was inspired by some lectures of Ribet, which he gave in October 1998 in Montreal as part of the CRM special year on number theory and arithmetic geometry. To explain what we prove in this section, let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be irreducible and modular, and suppose that ρ restricted to a decomposition group at 2 is not contained in the scalar matrices. Then ρ can be shown to occur in a certain Jacobian with "multiplicity one". Using this multiplicity one result and ideas of Ribet, one can prove a level-lowering result (Theorem 2.8), analogous to the known level-lowering results of Mazur and Ribet valid for mod l representations with $l > 2$ (see [R2]). We remark that in the case where the restriction of ρ to a decomposition group at 2 is contained in the scalars, the multiplicity one result alluded to above does not appear to be known, and indeed it is not clear whether one should expect it to be true. This remains an interesting open question.

In the third section we indicate how to deduce from these results the full level-lowering conjecture for the representations for which multiplicity one is known. This is standard and basically due to Carayol [C]. This level-lowering result can now be used with the results of [Dic] to prove a Wiles-like lifting theorem valid for many representations when $l = 2$, and hence (thanks to ideas of Taylor) to establish new examples of Artin's conjecture. See [T] for an overview, and [BDST] for more details.

I would like to express my gratitude to Richard Taylor, who motivated my interest in the problem, and also to Ken Ribet who, in his Montreal lectures, explained how to use primes q such that $\rho(\mathrm{Frob}_q)$ has

order 2 as "auxiliary primes". These primes can be used as a replacement for the primes q not congruent to 0 or 1 mod l in Ribet's original "switch" (the idea of using primes not congruent to 0 or 1 mod l has serious shortcomings when $l = 2$). The fact that these involutions can be used when $l = 2$ was discovered independently by Fujiwara. Ribet and Taylor also read preliminary versions of this manuscript and I am grateful for their comments. Finally I would like to thank Fred Diamond, who encouraged me to work on the problem and who made an off-the-cuff remark that turned out to be more useful than either of us could have imagined at the time.

Notation.

If Γ is a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$, and $k \geq 1$ is an integer, then let $S_k(\Gamma; \overline{\mathbb{Q}}_2)$ denote the space of cusp forms of weight k and level Γ with coefficients in $\overline{\mathbb{Q}}_2$. These forms can be thought of as certain sections of $\omega^{\otimes k}$ on the modular curve $X(\Gamma)$ corresponding to Γ, thought of as a variety over $\overline{\mathbb{Q}}_2$. Alternatively, if one fixes a field isomorphism $\overline{\mathbb{Q}}_2 \cong \mathbb{C}$, these forms can be thought of as classical cusp forms.

Let $\overline{\mathbb{Z}}_2$ denote the ring of integers in $\overline{\mathbb{Q}}_2$, and let λ denote the maximal ideal of $\overline{\mathbb{Z}}_2$. We say that two cusp forms are *congruent mod* λ if their q-expansions lie in $\overline{\mathbb{Z}}_2[[q]]$ and are congruent mod λ.

If $f \in S_k(\Gamma; \overline{\mathbb{Q}}_2)$ and $n \geq 1$, we write $a_n(f)$ for the coefficient of q^n in the q-expansion of f.

If $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ is irreducible, we say that ρ is *modular* if it is the mod 2 representation associated to some normalised eigenform $f \in S_k(\Gamma_1(N); \overline{\mathbb{Q}}_2)$. If we want to be precise, we say that ρ is *modular of weight k and level N*. Note that a representation can be modular of many weights and levels. If Γ is a group with $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$ and ρ arises as the mod 2 representation associated to some eigenform $f \in S_k(\Gamma; \overline{\mathbb{Q}}_2)$ then we say that ρ is *modular of level* Γ, or simply that ρ *arises from* Γ. Note that we are always asking that our eigenforms are characteristic 0 forms, and will be avoiding the phenomena of mod 2 forms sometimes not lifting to characteristic 0 when $k = 1$. In fact we will be staying away from weight 1 completely.

If $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i)) \to \overline{\mathbb{F}}_2^\times$ and $\rho = \mathrm{Ind}_{\mathbb{Q}(i)}^{\mathbb{Q}}(\chi)$ is the associated induced 2-dimensional representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, then, for brevity, we shall say that ρ is *induced from* $\mathbb{Q}(i)$.

Typically in this paper, N will denote an odd positive integer and M will denote an arbitrary positive integer.

§1. Removing 2 from the level.

In this section, we explain how to remove powers of 2 from the level of a modular representation. More precisely, let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be continuous and irreducible. The main result of this section is

Proposition 1.1. If N is odd and ρ is modular of level $2^n N$ for some $n \geq 0$, then ρ is modular of level N.

Remarks.

(1) Our method of proof is a minor modification of Theorem 2.1 of [R3], passing from group to group until we reach $\Gamma_1(N)$, and as in [R3], we lose all control of the weight during the proof.

(2) Note that all modular forms in our proof are characteristic 0 forms. We will invoke several times Lemme 6.11 of [DS], which enables us to prove that certain forms which are eigenforms mod λ are congruent to characteristic 0 eigenforms.

Proof.

By assumption, ρ arises from $\Gamma_1(2^n N)$. If $n = 0$ then we are done, so we may assume that $n \geq 1$. We now push through the proof of Theorem 2.1 of [R3] in this situation. It requires only minor modifications. First, a definition. If $a > 0$ is odd and χ is a character of $(\mathbb{Z}/2^n a\mathbb{Z})^\times$, then χ can be written as the product of a character χ_2 of conductor dividing 2^n and a character χ_2' of conductor dividing a. We refer to χ_2 as the 2-part of χ.

Step 1. ρ arises from $\Gamma_1(4N) \cap \Gamma_0(2^m)$ for some $m \geq 2$.

We are assuming that ρ arises from some form f_0 on $\Gamma_1(2^n N)$. Note that if $1 \leq n \leq 2$ then we can set $m = 2$ and we are already home, so let us assume that $n \geq 3$.

Let the character of f_0 be $\chi : (\mathbb{Z}/2^nN\mathbb{Z})^\times \to \overline{\mathbb{Q}}_2^\times$, and let χ_2 be the 2-part of this character, considered as a map $(\mathbb{Z}/2^n\mathbb{Z})^\times \to \overline{\mathbb{Q}}_2^\times$. It is an easy exercise to see that there is a character $\psi : (\mathbb{Z}/2^{n+1}\mathbb{Z})^\times \to \overline{\mathbb{Q}}_2^\times$ such that $\chi_2\psi^2$ is trivial on $1+4\mathbb{Z}$. Hence the twist $f_1 = f_0 \times \psi$ of f_0 is of the required form for some sufficiently large m (for example Proposition 3.64 of [Shim] implies that one may take $m = 2n+2$).

Step 2. ρ arises from $\Gamma_1(N) \cap \Gamma_0(2^m)$.

We know that ρ arises from f_1 of level $\Gamma_1(4N) \cap \Gamma_0(2^m)$. Say f_1 has weight k. By assumption we have $m \geq 2$. The 2-part of the character of f_1 factors through $(\mathbb{Z}/4\mathbb{Z})^\times$ and is hence either trivial, in which case we are done, or has order 2. In the latter case we multiply f_1 by the Eisenstein series

$$\begin{aligned} E &= \sum_{m,n \in \mathbb{Z}} q^{m^2+n^2} \\ &= 1 + 4(q + q^2 + q^4 + 2q^5 + \ldots) \end{aligned}$$

of weight 1, level 4 and non-trivial character. The product f_1E is a modular form of level $\Gamma_1(N) \cap \Gamma_0(2^m)$ and is congruent to f_1 mod λ. Using the Deligne-Serre lemma, we can find a characteristic 0 eigenform f_2 of level $\Gamma_1(N) \cap \Gamma_0(2^m)$ giving rise to ρ, finishing the proof of step 2.

Perhaps another approach, which would deal with steps 1 and 2 simultaneously, might be to try and find an appropriate Eisenstein series of character the inverse of f_0 and q-expansion congruent to 1 mod 2, then multiply f_0 by this Eisenstein series and apply the Deligne-Serre lemma to the product.

Step 3. ρ arises from $\Gamma_1(N) \cap \Gamma_0(2)$.

Ribet's argument in [R3] goes through unchanged in this situation so we merely sketch the details. We know that ρ arises from $\Gamma_1(N) \cap \Gamma_0(2^m)$ and we proceed by induction on m. It is a standard result that if $m \geq 2$ then the Hecke operator U_2 maps forms of level $\Gamma_1(N) \cap \Gamma_0(2^m)$ to forms of level $\Gamma_1(N) \cap \Gamma_0(2^{m-1})$, and applying U_2 to $\sigma((f_2)^2)$ where σ is an appropriate automorphism of $\overline{\mathbb{Q}}_2$, and then invoking the Deligne-Serre lemma, gives us the result by induction on m. Write f_3 for the form of level $\Gamma_1(N) \cap \Gamma_0(2)$ giving rise to ρ.

Step 4. ρ arises from $\Gamma_1(N)$.

Again Ribet's argument works with very few modifications, and so we merely sketch the argument, referring to [R3] for more details. Let $E_4 = 1 + 240(q + 9q^2 + 28q^3 + \ldots)$ denote the normalised weight 4 level 1 Eisenstein series. For a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with integer entries and positive determinant, and f a modular form of weight k, we define

$$f\left|\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = (ad-bc)^{k/2}(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right),\right.$$

and set

$$\begin{aligned} g = E_4(z) - 16E_4(2z) = E_4 - 4E_4\left|\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}\right. \\ = -15 + 240(q - 7q^2 + 28q^3 - \ldots). \end{aligned}$$

Let W be the matrix $\begin{pmatrix} 1+N & 1 \\ 2N & 2 \end{pmatrix} = \begin{pmatrix} \frac{1+N}{2} & 1 \\ N & 2 \end{pmatrix}\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ of determinant 2. Then an easy calculation shows that the q-expansion of $g|W$ is congruent to 0 mod 64.

Recall next the trace map from forms of level $\Gamma_1(N) \cap \Gamma_0(2)$ to forms of weight $\Gamma_1(N)$, defined by $f \mapsto \sum_{i=0}^2 f|\gamma_i$, where

$$\coprod_{i=0}^{2} (\Gamma_1(N) \cap \Gamma_0(2))\gamma_i = \Gamma_1(N).$$

Recall that we are assuming that ρ arises from some form f_3 of level $\Gamma_1(N) \cap \Gamma_0(2)$. By the method of section 3.2 of [S1], one can check that if j is sufficiently large then $\mathrm{Tr}(f_3 g^{2^j})$ is congruent to $f_3 g^{2^j}$ and hence to f_3

mod λ, and is on $\Gamma_1(N)$. Hence one more application of the Deligne-Serre lemma gives us an eigenform f_4 on $\Gamma_1(N)$ giving rise to ρ, thus completing the proof.

□

We end this section with some variants and strengthenings of this result, including known results on weight optimisation. Recall that a representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ is said to be *finite at 2* if ρ restricted to a decomposition group at 2 is the extension to $\overline{\mathbb{F}}_2$ of a representation coming from the generic fibre of a finite flat group scheme over $\mathbb{Z}_2$.

Lemma 1.2. Let N be an odd integer, and let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be an irreducible representation. Then ρ is modular of weight 2 and level $2N$ if and only if ρ is modular of weight 3 and level N.

Proof. The result follows from Proposition 8.18 of [G] if $N \geq 5$, and is clear if $N < 5$ because then there are no forms of level $2N$ and weight 2, nor of level N and weight 3. □

Proposition 1.3. If $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ is irreducible, and modular of level $2^n N$ for some odd integer N, then

(a) ρ is modular of some weight $2 \leq k \leq 3$ and level N,

(b) ρ is modular of weight 2 and level N if and only if ρ is finite at 2.

(c) If ρ is not finite at 2 then ρ is modular of weight 2 and level $2N$, and also of weight 3 and level N.

Proof.

(a) By Proposition 1.1, ρ is modular of level N and some weight. By Theorem 3.4 of [E1] one can deduce that ρ is modular of level N and weight at most 3 (note that the mod 2 cyclotomic character is trivial). Note that the definition of "modular" in [E1] is slightly weaker than our definition because Edixhoven uses Katz's definition of mod 2 modular forms and hence allows characteristic 2 forms which do not lift to characteristic 0. But, given a mod 2 modular form in the sense of Katz, giving rise to ρ and of weight at most 3, we can always multiply it by the Hasse invariant if necessary to make it have weight either 2 or 3, and then lift it by Lemma 1.9(1) and (2) of [E2] (which shows that the two definitions of a mod 2 cusp form are the same in weights 2 and 3).

(b) If ρ is finite at 2 then by (a) we may assume that ρ is modular of weight 3 and level N. Now applying Theorem 2.8 of [E1] shows that ρ is modular of weight 2 and level N. The converse is clear, because representations of weight 2 and level N are by construction finite at 2.

(c) If ρ is not finite at 2 then by (a) and (b) it must be modular of weight 3 and level N. Now apply Lemma 1.2. □

§2. Ribet's theorem in characteristic 2.

In this section we prove a characteristic 2 version of Ribet's level-lowering theorem, assuming a certain multiplicity one result. Fortunately this result is known in many cases, due to initial ideas of Mazur and extensions of these ideas. We begin by reviewing and slightly extending what is known about multiplicity one.

Let $M \geq 1$ be an integer. Let Γ be a group with $\Gamma_1(M) \subseteq \Gamma \subseteq \Gamma_0(M)$. Let $X(\Gamma)$ denote the associated compactified modular curve (viewed over the complexes) and let $J(\Gamma)$ denote its Jacobian. Let $\mathbb{T}$ be the Hecke algebra in $\mathrm{End}(J(\Gamma))$ generated (via Picard functoriality) by the Hecke operators T_n, $n \geq 1$ and the diamond operators $\langle d \rangle_M$ for $d \in (\mathbb{Z}/M\mathbb{Z})^\times$. Then $\mathbb{T}$ is a finite free $\mathbb{Z}$-module. Let $\mathbf{m}$ denote a maximal ideal of $\mathbb{T}$ containing 2.

Definition 2.1. With notation as above, we say that $\mathbf{m}$ *satisfies multiplicity one* if the finite group $J(\Gamma)[\mathbf{m}]$ has $\mathbb{T}/\mathbf{m}$-dimension 2.

Recall that one can associate to $\mathbf{m}$, as above, a semisimple Galois representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ (after choosing an embedding $\mathbb{T}/\mathbf{m} \to \overline{\mathbb{F}}_2$).

Now let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be an irreducible modular representation. We wish to define what it means for ρ to satisfy multiplicity one. It is convenient to break the definition up into two parts.

Definition 2.2—finite case. If ρ is finite at 2, then say that ρ *satisfies multiplicity one* if, for all *odd* M, and for all groups Γ with $\Gamma_1(M) \subseteq \Gamma \subseteq \Gamma_0(M)$, and $\mathbf{m}$ as above, such that $\rho_{\mathbf{m}} \cong \rho$ (after some choice of embedding $\mathbb{T}/\mathbf{m} \to \overline{\mathbb{F}}_2$), the ideal $\mathbf{m}$ satisfies multiplicity one.

Definition 2.2—non-finite case. If ρ is not finite at 2, then ρ can never arise as the mod 2 representation associated to a modular form of weight 2 and odd level. We say in this case that ρ *satisfies multiplicity one* if for all M divisible exactly once by 2, and for all $\mathbf{m}$ as above such that $\rho_{\mathbf{m}} \cong \rho$, the ideal $\mathbf{m}$ satisfies multiplicity one.

Note the restrictions on the M used in Definition 2.2. These restrictions are natural because of Proposition 1.3. We also remark that if ρ is irreducible, then to check that it satisfies multiplicity one we only have to check it for varying M and $\Gamma = \Gamma_1(M)$. This follows easily from the following lemma.

Lemma 2.3. If $\Gamma_1(M) \subseteq \Gamma \subseteq \Gamma_0(M)$ then $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on the kernel of the natural map $J(\Gamma) \to J_1(M)$ via an abelian quotient.

Proof. This is an immediate consequence of Proposition 6 of [LO] (and the discussion in §4.2 of [LO]). □

The author knows of no example of an irreducible modular representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ which does not satisfy multiplicity one. The following proposition shows that it is certainly is a common phenomenon.

Proposition 2.4. If $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ is irreducible and modular, and ρ restricted to a decomposition group at 2 is not contained within the scalar matrices, then ρ satisfies multiplicity one.

Proof. Let us first deal with the case where ρ is not finite at 2. Then for N odd, $M = 2N$, Γ and $\mathbf{m}$ as above, and $\mathbb{T}/\mathbf{m} \to \overline{\mathbb{F}}_2$, we would like to apply a version of the Main Theorem of [MR], which as it stands applies only when $\Gamma = \Gamma_0(2N)$. We indicate briefly how one adapts the proof so that it applies in our situation. Firstly, by Lemma 2.3 we are reduced to the case $\Gamma = \Gamma_1(2N) = \Gamma_1(N) \cap \Gamma_0(2)$. We would like to apply Proposition 18 of [MR], with R the subring of $\mathrm{End}(J(\Gamma))$ generated by T_n for n odd and the Atkin-Lehner operator $w = w_2$. It is well known that $w = -U_2$ on the space of 2-new forms of level $2N$, so the analogue of Proposition 20 of [MR] holds. To check the analogue of Proposition 22, the only part that is not an immediate generalisation of [MR] itself is the statement that a certain component group is Eisenstein (Axiom III in §9 of [MR]). But this component group is indeed Eisenstein, as is proved on pp. 672–673 of [R3]. Hence Proposition 18 of [MR] can be applied to deduce that multiplicity one holds in this case.

Now let us assume that ρ is finite at 2. Choose any M odd, set $\Gamma = \Gamma_1(M)$ (by Lemma 2.3 it suffices to treat this case), and say there exists $\mathbf{m}$, and $\mathbb{T}/\mathbf{m} \to \overline{\mathbb{F}}_2$, such that $\rho_{\mathbf{m}} \cong \rho$. Now in fact the proof of the Proposition can, for the most part, be extracted from [E1]. Note that Theorem 9.2 of [E1], parts (2) and (3), deals with every case apart from when ρ is unramified at 2 and $\rho(\mathrm{Frob}_2)$ is not diagonalisable. In this latter case, the exact sequence (9.2.1) of [E1] is not split and the arguments of [E1] still hold to prove the theorem in this case. □

We remark that the remaining irreducible case, where the representation restricted to a decomposition group at 2 lies in the scalar matrices, has caused some trouble in the theory of mod l modular forms. For example, Gross did not deal with such representations in his paper [G], and Wiles excluded them in his paper [W] when considering ordinary deformations. We shall also exclude them, because we do know know how to prove multiplicity one in this case (or indeed whether to expect it).

Another potential complication in the theory of mod 2 modular forms is that representations induced from a character of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i))$ can sometimes be hard to deal with. For example, Carayol's lemma must be modified slightly to deal with these representations, and their corresponding maximal ideals sometimes show up in the support of component groups of Néron models of Jacobians (see [R4] for more details of this phenomenon). We shall occasionally have to deal with these representations separately. For brevity, we shall refer to such representation as "induced from $\mathbb{Q}(i)$". These representations can in fact be dealt with by hand, and so we shall ignore them for the rest of this section and deal with them in §3.

Before we prove the main result of this section, we introduce a useful technical tool for dealing with representations that are not induced from $\mathbb{Q}(i)$.

Lemma 2.5. Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be an irreducible representation, not induced from $\mathbb{Q}(i)$. Then there is a prime $q > 3$ with $q \equiv 3 \bmod 4$, such that ρ is unramified at q and the trace of $\rho(\mathrm{Frob}_q)$ is non-zero.

Proof. Let $\omega : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to (\mathbb{Z}/4\mathbb{Z})^\times$ be the mod 4 cyclotomic character, and let G be the image of $\rho \oplus \omega$. Then G is a finite group. Let $H \triangleleft G$ be the kernel of ω. Note that for an unramified prime q, $\mathrm{Frob}_q \in H$ iff $q \equiv 1 \bmod 4$. We now divide into two cases.

Case 1. $\rho(H) = \rho(G)$. In this case, if the lemma were false, $\rho(G)$ would be contained within the matrices of trace zero. By assumption $\rho(G)$ is not contained within the upper triangular matrices. Hence there is some $g \in G$ such that $\rho(g) = \begin{pmatrix} a & b \\ c & a \end{pmatrix}$ with c non-zero. Now for any $\gamma \in G$, we have that $\rho(\gamma)$ and $\rho(g\gamma)$ must both have trace zero and hence $\rho(\gamma)$ must be of the form $\begin{pmatrix} d & \lambda e \\ e & d \end{pmatrix}$ with $\lambda = b/c$. Now an easy check shows that the image of ρ is abelian and hence ρ cannot be irreducible, a contradiction.

Case 2. $\rho(H) < \rho(G)$, a subgroup of index 2. In this case, any Sylow 2-subgroup of $\rho(G)$ must contain an element not in $\rho(H)$. Let $\rho(g)$ be such an element. Then $\rho(g)$ has order a power of two, at least two, and hence $\rho(g)$ has order exactly two because there are no elements of order 4 in $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$. Without loss of generality, $\rho(g) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Now if the lemma were false, then for all $h \in H$, $\rho(hg)$ would have trace zero and hence $\rho(h)$ would be a symmetric matrix. But any subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$ composed entirely of symmetric matrices must be abelian, because $XY = (XY)^t = Y^tX^t = YX$. Hence ρ restricted to H is reducible, and now by Frobenius reciprocity ρ is induced from a character of H. But H is precisely the image of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i))$, a contradiction. □

Corollary 2.6. Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be an irreducible representation, which is not induced from $\mathbb{Q}(i)$. Then there is a prime $q > 3$ such that ρ is unramified at q, having the following property: if M is any integer prime to q and $f \in S_2(\Gamma_1(Mq); \overline{\mathbb{Q}}_2)$ is a normalised eigenform giving rise to ρ, then there is a normalised eigenform $g \in S_2(\Gamma_1(M); \overline{\mathbb{Q}}_2)$ giving rise to ρ and such that $a_2(f)$ and $a_2(g)$ are congruent mod λ.

Proof. Choose q as in Lemma 2.5. Assume M and f are as in the statement of the Corollary. Say the character of f is $\chi_M\chi_q$, with χ_M of conductor dividing M and χ_q of conductor dividing q. Applying Lemma 2.2 of [D] with $m = q > 3$, we see that there is an eigenform f' of level Mq giving rise to ρ, with $a_2(f') \equiv a_2(f) \bmod \lambda$, and such that the character χ'_M of f' at M has odd order. Because f' has weight 2 we deduce that $\chi'_q(-1) = 1$. But $q \equiv 3 \bmod 4$ and hence χ'_q has odd order. Now $\det(\rho)$ is unramified at q and hence the mod 2 reduction of χ'_q is trivial. This means that χ'_q is trivial. So f' must either be old at q or unramified special. By Local Langlands, if f' is unramified special at q then ρ restricted to a decomposition group at q will have semisimplification isomorphic to the sum of two copies of an unramified character, contradicting the fact that $\mathrm{trace}(\rho(\mathrm{Frob}_q))$ is non-zero. Hence f' is old at q and we may let g be an eigenform of level M with $a_n(g) = a_n(f')$ for all n prime to q. This g works. □

Corollary 2.7 ("Carayol's Lemma"). Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be an irreducible representation which is not induced from $\mathbb{Q}(i)$. Assume that ρ comes from a characteristic 0 form f of weight 2, level M and character χ. Let ψ be a character of $(\mathbb{Z}/M\mathbb{Z})^\times$ such that $\psi(-1) = 1$ and such that ψ and χ are congruent mod λ. Then there is a characteristic 0 form g of weight 2, level M and character ψ giving rise to ρ. Moreover g can be chosen such that $a_2(g) \equiv a_2(f) \bmod \lambda$.

Proof. Choose a prime q as in Lemma 2.5. By Lemma 2.2 of [D] applied with $m = q$ there is a form f' of level Mq and character ψ at M with $a_2(f')$ congruent to $a_2(f)$. Now the character of f' at q must have odd order so, as in Corollary 2.6, f' must be old at q and the oldform at level M will do. □

The next theorem is the main theorem of this section.

Theorem 2.8.

Let M be a positive integer, and let p be a prime not dividing $2M$. Let $f \in S_2(\Gamma_1(M) \cap \Gamma_0(p); \overline{\mathbb{Q}}_2)$ be a normalised cuspidal eigenform. Assume that the associated mod 2 Galois representation ρ associated to f

is absolutely irreducible and satisfies multiplicity one. Assume furthermore that M is odd if ρ is finite at 2, and that 2 divides M exactly once if ρ is not finite at 2. Finally, assume that ρ is not induced from $\mathbb{Q}(i)$. Then there is a normalised eigenform $g \in S_2(\Gamma_1(M); \overline{\mathbb{Q}}_2)$ giving rise to ρ. Moreover, we may find such a g with the property that $a_2(g) \equiv a_2(f) \bmod \lambda$.

Remarks.

(a) Level-lowering results of this form were first proved by Mazur, Ribet and Diamond. The original proofs used a mod l multiplicity 1 principle which was later bypassed by Ribet. It is no doubt clear by now to the reader that our approach is based on the original multiplicity 1 method.

(b) In Ribet's original paper [R2] he also assumes $l > 2$ when he makes the choice of an auxiliary prime $q \neq l$ satisfying $q \not\equiv 1 \bmod l$. However, in a series of lectures in Montreal in the autumn of 1998, Ribet showed how one could modify his argument by instead using primes q such that $\rho(\mathrm{Frob}_q)$ was an involution. This is the approach that we shall use.

(c) In the case when ρ is irreducible and induced from $\mathbb{Q}(i)$ one can prove the theorem as well, by "brute force". Rather than explaining the details, we shall simply deal with these representations separately when we prove the general level-lowering theorem in §3.

Proof of Theorem 2.8. We use the notation of [R3] and [D], and refer to these papers for more details.

Firstly we reduce to the case $M \geq 5$. For, by assumption, ρ is not induced from $\mathbb{Q}(i)$, so if $M < 5$ we may choose a prime $q > 3$ as in Corollary 2.6 and then replace our form by an oldform of level Mqp. Applying Theorem 2.8 with M replaced by $Mq \geq 5$, we may deduce the existence of a form g of level Mq giving rise to ρ, and such that $a_2(f) \equiv a_2(g) \bmod \lambda$. But by Corollary 2.6 there will also be a form of level M giving rise to ρ, as required (in fact, we may now deduce that this situation can never occur, because there are no such forms when $M < 5$). So we can assume that $M \geq 5$.

Next some notation. For relatively prime integers a and b we denote by $\Gamma_1(a, b)$ the congruence subgroup $\Gamma_1(a) \cap \Gamma_0(b)$. We write $X_1(a, b)$ for the compactification of the moduli space over $\mathbb{Q}$ parameterising elliptic curves with a point of order a and a cyclic subgroup of order b. We write $J_1(a, b)$ for the Jacobian of $X_1(a, b)$. If $b = 1$ we denote these varieties by $X_1(a)$ and $J_1(a)$. Let T_n denote the Hecke correspondences acting on $X_1(a, b)$, and also, by Picard functoriality, as endomorphisms of $J_1(a, b)$. We do this primarily because this is the convention used in [D]. Note in particular the comments on p. 31 of [D]. Let $\mathbb{T}_{a,b}$ denote the Hecke algebra generated over $\mathbb{Z}$ by these Hecke operators, considered as a subring of $\mathrm{End}(J_1(a, b))$.

Write $\mathbb{T}$ for the Hecke algebra $\mathbb{T}_{M,p}$. The eigenform f induces a homomorphism of rings $\mathbb{T} \to \overline{\mathbb{F}}_2$. Because ρ satisfies multiplicity one, we see by definition that $J_1(M, p)[\mathbf{m}]$ has $\mathbb{T}/\mathbf{m}$-dimension two.

Firstly we deal with the cases treated by Mazur. Let us assume then that $\rho(\mathrm{Frob}_p)$ is not a scalar. Then Mazur's argument presented in [R2], generalised appropriately, shows the existence of g. We sketch the method. The Néron model $J_1(M, p)_{\mathbb{Z}_p}$ of $J_1(M, p)_{\mathbb{Q}_p}$ has well-understood reduction at p. The connected component J^0 of the special fibre $J_1(M, p)_{\mathbb{F}_p}$ is semi-abelian, and sits in an exact sequence

$$0 \to T \to J^0 \to J_1(M)^2_{\mathbb{F}_p} \to 0$$

where T is a torus over $\mathbb{F}_p$. The natural action of $\mathbb{T}$ on the middle term induces an action of $\mathbb{T}$ on the outer terms of this sequence, and we remark that for primes $q \neq p$ the action of T_q on $J_1(M)^2_{\mathbb{F}_p}$ is the natural diagonal action. The action of T_p is slightly more subtle but can be calculated explicitly, see for example p. 29 of [D]. Furthermore, the quotient $J_1(M, p)_{\mathbb{F}_p}/J^0$ is Eisenstein, as is proved on pp. 672–673 of [R3].

Let us assume for a contradiction that no form g exists. We know that $J_1(M, p)[\mathbf{m}]$ is a non-zero finite group scheme over $\mathbb{Q}$, whose associated Galois representation is isomorphic to $\mathrm{Hom}(\rho, \mu_2)$ (we remark that we do not actually need multiplicity one for this part of the argument but shall use it for simplicity). Let V denote the finite étale group scheme $J_1(M, p)_{\mathbb{Q}_p}[\mathbf{m}]$. Then $V(\overline{\mathbb{Q}}_p) \cong (\mathbb{T}/\mathbf{m})^2$ as a $\mathbb{T}/\mathbf{m}$-module, and the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ on $V(\overline{\mathbb{Q}}_p)$ is unramified, with Frob_p not acting as an element of $\mathbb{T}/\mathbf{m}$.

By an appropriate generalisation of Lemma 2 of [ST], we see that the reduction map $J_1(M, p)(\overline{\mathbb{Q}}_p)[\mathbf{m}] \to J_1(M, p)(\overline{\mathbb{F}}_p)[\mathbf{m}]$ is an isomorphism which commutes with the action of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. Hence $J_1(M, p)_{\mathbb{F}_p}[\mathbf{m}]$ is a finite étale group scheme whose $\overline{\mathbb{F}}_p$-points are a free $\mathbb{T}/\mathbf{m}$-module of rank 2, and on which Frob_p acts in a $\mathbb{T}/\mathbf{m}$-linear way but not as an element of $\mathbb{T}/\mathbf{m}$.

Because $J_1(M,p)_{\mathbb{F}_p}/J^0$ is Eisenstein we see that $J^0(\overline{\mathbb{F}}_p)[\mathbf{m}] = J_1(M,p)(\overline{\mathbb{F}}_p)[\mathbf{m}]$. We are assuming that g does not exist, hence $J_1(M)^2(\overline{\mathbb{F}}_p)[\mathbf{m}] = 0$ and so $J_1(M,p)_{\mathbb{F}_p}(\overline{\mathbb{F}}_p)[\mathbf{m}] = T(\overline{\mathbb{F}}_p)[\mathbf{m}]$. But Frob_p acts on $T(\overline{\mathbb{F}}_p)[\mathbf{m}]$ as T_p, that is, as an element of $\mathbb{T}/\mathbf{m}$, and hence Frob_p acts on $V(\overline{\mathbb{Q}}_p)$ as an element of $\mathbb{T}/\mathbf{m}$, a contradiction.

We now deal with the case where $\rho(\mathrm{Frob}_p)$ is a scalar. By assumption, ρ is absolutely irreducible. If the image G of ρ had odd order then the mod 2 representation theory of G would be "the same" as the characteristic 0 representation theory of G and in particular the degree of any absolutely irreducible representation of G would divide the order of G. This would contradict the fact that G had odd order. Hence the order of G is even and there is a prime $q \nmid 2Mp$ such that $\rho(\mathrm{Frob}_q)$ has order 2. All elements of order 2 in $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$ have trace 0 and hence we are in a position to apply a well-known level raising result of Ribet (c.f. [R1], which proves this result in the Γ_0 case, but the proof generalises easily (using Lemma 2.3)) to deduce the existence of a q-new form $f' \in S_2(\Gamma_1(M) \cap \Gamma_0(pq); \overline{\mathbb{Q}}_2)$ giving rise to ρ. Note that although the statement of the level-raising theorem does not usually include the property that $a_2(f) \equiv a_2(f') \bmod \lambda$, this is contained in the proof.

Now if there were a form g' of level $\Gamma_1(M,q)$ giving rise to ρ and such that $a_2(g') \equiv a_2(f') \bmod \lambda$ then we are home because we are reduced to the case treated by Mazur, so we may assume that this is not the case. In particular, we may assume that f' is pq-new. We now use an adaptation of Ribet's "switch" and get a contradiction.

Let B be the quaternion algebra over $\mathbb{Q}$ with discriminant pq. Let $X_1^B(M)_{\mathbb{Q}}$ denote the Shimura curve over $\mathbb{Q}$ parameterising false elliptic curves equipped with a false point of order M (see [R2] or [B]). Write $J_1^B(M)_{\mathbb{Q}}$ for the Jacobian of this curve. Let Y_p denote the character group of the torus associated to the mod p reduction of the Néron model of $J_1^B(M)_{\mathbb{Q}_p}$, and similarly let Y_q denote the character group of the torus at q. Let the character group of the torus associated to the mod p reduction of $J_1(M,pq)_{\mathbb{Q}_p}$ be denoted L_p, and similarly let L_q be the analogous character group at q. Let the character group at p of $J_1(M,p)^2$ be X_p, and let X_q denote the character group of $J_1(M,q)^2$ at q.

We now write $\mathbb{T}'$ for the ring $\mathbb{T}_{M,pq}$, and let $\mathbf{m}'$ denote the kernel of the map $\mathbb{T}' \to \overline{\mathbb{F}}_2$ induced by f'. It is explained in §3 of [D] that $J_1^B(M)$ has a natural action of $\mathbb{T}'$. By assumption, ρ is pq-new at level $\Gamma_1(M,pq)$, so $J_1^B(M)[\mathbf{m}']$ is non-zero. By [BLR] we deduce that the Galois representation associated to $J_1^B(M)[\mathbf{m}']$ is a direct sum of copies of $\mathrm{Hom}(\rho,\mu_2)$ and hence has $\mathbb{T}'/\mathbf{m}'$-dimension 2μ for some integer $\mu > 0$. Furthermore, $J_1^B(M)[\mathbf{m}']$ is unramified at both p and q.

We now use Ribet's exact sequence (see p. 29 of [D])

$$0 \to Y_p \to L_q \to X_q \to 0$$

(where all of these modules have the $\mathbb{T}'$-actions described in [D]). Now our assumptions on ρ imply that $(X_q)_{\mathbf{m}'} = 0$ and we deduce that $(Y_p)_{\mathbf{m}'} \cong (L_q)_{\mathbf{m}'}$.

Because ρ satisfies multiplicity one, we know that $J_1(M,pq)[\mathbf{m}']$ has $\mathbb{T}'/\mathbf{m}'$-dimension 2. If we write $J_1(M,pq)_{\mathbb{Z}_q}$ for the Néron model of $J_1(M,pq)_{\mathbb{Q}_q}$, then again by a mild generalisation of Lemma 2 of [ST], we see that $J_1(M,pq)(\overline{\mathbb{Q}}_q)[\mathbf{m}'] = J_1(M,pq)_{\mathbb{F}_q}(\overline{\mathbb{F}}_q)[\mathbf{m}']$.

Now let T' denote the toric part of the connected component of the special fibre of the Néron model over $\mathbb{Z}_q$ of $J_1(M,pq)_{\mathbb{Q}_q}$. Then Frob_q acts as T_q on $T'(\overline{\mathbb{F}}_q)[\mathbf{m}']$, which can be considered as a $\mathbb{T}'/\mathbf{m}'$-subspace of $J_1(M,pq)(\overline{\mathbb{F}}_q)[\mathbf{m}']$. But Frob_q acts as an involution on this space, which has $\mathbb{T}'/\mathbf{m}'$-dimension 2, and hence any subspace where Frob_q acts as an element of $\mathbb{T}'/\mathbf{m}'$ must have $\mathbb{T}'/\mathbf{m}'$-dimension at most 1. We deduce that the $\mathbb{T}'/\mathbf{m}'$-dimension of $T'(\overline{\mathbb{F}}_q)[\mathbf{m}']$ is at most 1. We may identify $T'(\overline{\mathbb{F}}_q)$ with $\mathrm{Hom}(L_q, \overline{\mathbb{F}}_q^\times)$ and deduce that the $\mathbb{T}'/\mathbf{m}'$-dimension of $L_q/\mathbf{m}'L_q$ is at most 1.

Conversely, looking at $J_1^B(M)[\mathbf{m}']$ in characteristic p, we see the following. Firstly, the component group does not involve $\mathbf{m}'$, because of the existence of a map from $X_q/\mathbf{m}'X_q$ to this group (see p. 30 of [D]) whose kernel and cokernel are Eisenstein, and the fact that $X_q/\mathbf{m}'X_q = 0$. Hence if G_p is the torus of $J_1^B(M)$ at p, similar arguments to those above show that the $\mathbb{T}'/\mathbf{m}'$-dimension of $G_p(\overline{\mathbb{F}}_p)[\mathbf{m}']$ must be at least 2, and hence the $\mathbb{T}'/\mathbf{m}'$-dimension of $Y_p/\mathbf{m}'Y_p$ is at least 2.

Finally, we know already that $Y_p/\mathbf{m}'Y_p \cong L_q/\mathbf{m}'L_q$, a contradiction. This completes the proof. □

In §7 of [R3], Ribet gives a similar argument to prove, by contradiction, a level-lowering theorem valid for $l > 2$. Ribet shows that if the theorem were false then, for certain positive integers λ and μ, we have

$2\mu \leq \lambda$ and $2\lambda \leq 2\mu$, and deduces a contradiction, proving the theorem without assuming multiplicity one. Using this terminology we could summarise our argument thus: Ribet's proof that $2\lambda \leq 2\mu$ assumes $l > 2$ (when he shows that the sequence (7.10) in [R3] splits) and so does not seem to generalise, but his proof that $2\mu \leq \lambda$ works, and in our case we have $\lambda = 1$ (by multiplicity one) and $\mu \geq 1$, the contradiction we require.

§3. Level-lowering for $l = 2$.

The goal of this section is to put everything together.

Theorem 3.1.

Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be irreducible and modular, coming from a normalised cuspidal eigenform $f \in S_2(\Gamma_1(M); \overline{\mathbb{Q}}_2)$ for some integer M. Assume that ρ satisfies multiplicity one and is not induced from $\mathbb{Q}(i)$. Let N be the conductor of ρ (by definition prime to 2). Then there is a normalised eigenform $g \in S_2(\Gamma_1(N'); \overline{\mathbb{Q}}_2)$ giving rise to ρ, where $N' = N$ if ρ is finite at 2, and $N' = 2N$ otherwise. Furthermore, if M is odd, we may assume that $a_2(f) \equiv a_2(g) \bmod \lambda$.

Remarks.

(a) Recall from Proposition 2.4 that the multiplicity one assumption is only a mild one.

(b) We avoid completely the delicate question of whether or not ρ arises from a weight 1 form. This is for several reasons—firstly we have only been considering characteristic 0 forms and have not been using Katz's definition of mod 2 modular forms. Secondly, there is currently a gap in the literature concerning the proof of the companion forms theorem in this case—the paper [G] on companion forms assumes some unchecked compatibilities and the paper [CV] assumes $l > 2$.

Proof. The methods here are essentially that of [C]. In fact it is well known that Theorem 2.8 removes the only obstruction to proving this theorem. We briefly sketch the details.

By Proposition 1.3, we may assume that M is odd if ρ is finite at 2, and M is divisible exactly once by 2 if ρ is not finite at 2. Now recall that Carayol has proved in [C] that N divides M, and hence N' divides M. Moreover, Carayol has classified the cases where there can exist an odd prime p dividing M/N'. For any such prime p we will construct, following Carayol, a form of level M/p whilst preserving $a_2 \bmod \lambda$, and this will prove the theorem by induction.

Recall from Section 2.2 of [C] that there are 4 possible cases where degeneration may occur, classified according to the the local component π_p of the automorphic representation π associated to the form of level M:

(i) π_p is principal series associated to two characters μ and ν, where μ is tamely ramified with unramified reduction,

(ii) π_p is an unramified special representation,

(iii) π_p is a twist of the special representation by a character μ which is tamely ramified and has unramified reduction,

(iv) π_p is supercuspidal, induced from a character ξ of the unramified extension of $\mathbb{Q}_p$, and ξ is tamely ramified with unramified reduction.

We must deal with these four cases. Case (ii) is precisely the case dealt with by Theorem 2.8.

We subdivide case (i) into two subcases. Firstly ν could be unramified, in which case we can use Carayol's lemma to replace our form by a form for which π_p is an unramified twist of the special representation and we have reduced ourselves to case (ii). Secondly ν could be ramified, in which case twisting by a finite order character of conductor p which agrees with the inverse of μ on tame inertia decreases the level by a factor of at least p whilst preserving a_2. So this deals with case (i).

Case (iii) is also dealt with by twisting by a character of 2-power order.

Case (iv) is a little more subtle. One way of treating it, as sketched in [D], is to switch to the quaternion algebra ramified at p, via the Jacquet-Langlands theorem. Now the proof of the analogue of Carayol's lemma in Theorem 9 of [DT] goes through and then we can use the Jacquet-Langlands theorem to switch back to a form of level dividing M/p. Alternatively there is a slightly more convoluted argument involving raising the

level by another prime, then applying an indefinite quaternion algebra version of Carayol's result. We leave the reader to fill in the details of this last approach.

This deals with all four cases and hence proves the theorem. □

Although Theorem 3.1 is the form of the main theorem that is used in [BDST], we note that in fact one can prove the following rather cleaner result using these methods:

Theorem 3.2. Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_2)$ be irreducible and modular. Assume that ρ satisfies multiplicity one. Set $k = 2$ if ρ is finite at 2, and $k = 3$ otherwise. Let N be the conductor of ρ. Then there is a normalised eigenform $g \in S_k(\Gamma_1(N); \overline{\mathbb{Q}}_2)$ giving rise to ρ.

Remark. If furthermore ρ is not induced from $\mathbb{Q}(i)$ and ρ is finite at 2 then one can use Corollary 2.7 to deduce that g can be chosen with character equal to that predicted by Serre. If ρ is not finite at 2 then Serre initially defined the weight k_ρ associated to ρ to be 4, because in his initial paper he wanted the character of the form giving rise to ρ to have odd order and hence the weight of the form had to be even. Serre slightly modified his conjecture later on, but the remarks above explain why the second case of Remark 4.4 of [E1] occurs—Serre could not initially predict $k = 3$ in this case.

Proof. Firstly we deal with the case where ρ is induced from a character of $\mathbb{Q}(i)$. In this case, one can lift this character to a character $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i)) \to \overline{\mathbb{Q}}_2^\times$ with odd order. The resulting induced representation $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{Q}}_2)$ is known to be modular, coming from a classical weight 1 cusp form of level $4N$. Now by Proposition 1.3, one can find a form of level N and the correct weight. Note that no subtle level-lowering results are necessary in this situation.

If ρ is not induced from $\mathbb{Q}(i)$ then by Proposition 1.3(c), ρ is modular of weight 2 and some level. Now by Theorem 3.1, ρ is modular of level N' and weight 2, where $N' = N$ if ρ is finite and $2N$ if not. Finally we apply Lemma 1.2 to deduce the result we require. □

References.

[B] K. Buzzard, *Integral models of certain Shimura curves*, Duke Math. J. 87 (1997), 591–612.

[BDST] K. Buzzard, M. Dickinson, N. Shepherd-Barron and R. Taylor, *On icosahedral Artin representations*, preprint.

[BLR] N. Boston, H. Lenstra and K. Ribet, *Quotients of group rings arising from two-dimensional representations*, C.R.A.S. Paris, Série I, 312 (1991), pp. 323–328.

[C] H. Carayol, *Sur les représentations galoisiennes modulo l attachées aux formes modulaires*, Duke Math. J. 59 (1989), pp. 785–801.

[CV] R.F. Coleman and J.F. Voloch, *Companion forms and Kodaira-Spencer theory*, Invent. Math. 110 (1992), pp. 263–281.

[CY] *Elliptic curves, Modular Forms and Fermat's Last Theorem*, eds J. Coates and S. T. Yau, International Press, Cambridge, pp. 22–37 (1995).

[D] F. Diamond, *The refined conjecture of Serre*, in [CY].

[DT] F. Diamond and R. Taylor, *Lifting modular mod l representations*, Duke Math. J. 74 (1994), 253–269.

[Dic] M. Dickinson, *On the modularity of certain 2-adic Galois representations*, in preparation.

[DS] P. Deligne and J.-P. Serre, *Formes modulaires de poids 1*, Ann. Sci. Ec. Norm. Sup. (4) 7, 507–530 (1974).

[E1] B. Edixhoven, *The weight in Serre's conjectures on modular forms*, Invent. Math. 109 (1992), 563–594.

[E2] S.J. Edixhoven, *Serre's conjecture*, pp. 209–242 of *Modular Forms and Fermat's Last Theorem*, eds. G.Cornell, J. H. Silverman and G. Stevens, Springer 1997.

[G] B.H. Gross, *A tameness criterion for Galois representations associated to modular forms (mod p)*, Duke Math. J. 61 (1990), 445–517

[LO] S. Ling and J. Oesterlé, *The Shimura subgroup of $J_0(N)$*, pp. 171–203 of Astérisque 196–197 (1991).

[MR] B. Mazur and K. Ribet, *Two-dimensional representations in the arithmetic of modular curves*, pp. 215–255 of Astérisque 196–197 (1991).

[R1] K. Ribet, *Raising the levels of modular representations*, Séminaire de Théorie des Nombres, Paris 1987–88, Progress in Mathematics, Volume 81.

[R2] K. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *arising from modular forms*, Invent. Math. 100, 431–476 (1990).

[R3] K. Ribet, *Report on mod l representations of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, in Motives, Proc. Symp. Pure Math. 55:2 (1994), 639–676.

[R4] K. Ribet, *Irreducible Galois representations arising from component groups of jacobians*, pp. 131–147 of [CY].

[RT] D. Rohrlich and J. Tunnell, *An elementary case of Serre's conjecture*, Olga Taussky-Todd memorial issue, Pacific J. Math. (1997), 299–309.

[S1] J.-P. Serre, *Formes modulaires et fonctions zêta p-adiques*, Lecture Notes in Mathematics Volume 350, pp. 191–268.

[S2] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987), 179–230.

[Shim] G. Shimura, *Introduction to the arithmetic theory of automorphic functions.* Princeton University Press, reprinted 1994.

[ST] J.-P. Serre and J. Tate, *Good reduction of abelian varieties*, Annals of Mathematics (2) 88 (1968), pp. 492–517.

[T] R. Taylor, *Icosahedral Galois representations*, Pacific J. Math., Special Issue in memory of Olga Taussky-Todd, pp. 337–347 (1997).

[W] A. Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Annals of Math. 142, 443–551 (1995).