ESI **The Erwin Schrodinger International Institute for Mathematical Physics**
Boltzmanngasse 9
A-1090 Wien, Austria

Serre's modularity conjecture (I)

Chandrashekhar Khare
Jean-Pierre Wintenberger

Vienna, Preprint ESI 1891 (2007) February 12, 2007

Supported by the Austrian Federal Ministry of Education, Science and Culture
Available via http://www.esi.ac.at

SERRE'S MODULARITY CONJECTURE (I)

CHANDRASHEKHAR KHARE AND JEAN-PIERRE WINTENBERGER

Abstract. This paper is the first part of a work which proves Serre's modularity conjecture. We first prove the cases $p \neq 2$ and odd conductor, see Theorem 1.2, modulo Theorems 4.1 and 5.1. Theorems 4.1 and 5.1 are proven in the second part, see [13]. We then reduce the general case to a modularity statement for 2-adic lifts of modular mod 2 representations. This statement is now a theorem of Kisin [19].

AMS classification : 11R39

Contents

1. Introduction

Let $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$. Let $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ be a continuous, absolutely irreducible, two-dimensional, odd ($\det\bar{\rho}(c) = -1$ for c a complex conjugation), mod p representation, with $\mathbb{F}$ a finite field of characteristic p. We say that such a representation is of *Serre-type*, or S-type, for short.

We denote by $N(\bar{\rho})$ the (prime to p) Artin conductor of $\bar{\rho}$, and $k(\bar{\rho})$ the weight of $\bar{\rho}$ as defined in [26]. It is an important feature of the weight $k(\bar{\rho})$, for $p > 2$, that if $\overline{\chi}_p$ is the mod p cyclotomic character, then for some $i \in \mathbb{Z}$, $2 \leq k(\bar{\rho} \otimes \overline{\chi}_p{}^i) \leq p+1$. In the case of $p = 2$, the values of $k(\bar{\rho})$ can either be 2 or 4, with the former if and only if $\bar{\rho}$ is finite at 2.

We fix embeddings $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$ for all primes p hereafter, and when we say (a place above) p, we will mean the place induced by this embedding.

Serre has conjectured in [26] that such a $\bar{\rho}$ is *modular*, i.e., *arises from* (with respect to the fixed embedding $\iota_p : \overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}_p}$) a newform f of weight $k(\bar{\rho})$ and level $N(\bar{\rho})$. By *arises from* f we mean that there is an integral model $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$ of the p-adic representation ρ_f associated to f, such that $\bar{\rho}$ is isomorphic to the reduction of ρ modulo the maximal ideal of $\mathcal{O}$, and with $\mathcal{O}$ the ring of integers of a finite extension of $\mathbb{Q}_p$. In these circumstances we also say that $\bar{\rho}$ arises from $S_{k(\bar{\rho})}(\Gamma_1(N(\bar{\rho}))$.

1.1. **Main result.**

The case of the conjecture for conductor one, i.e., the *level one conjecture*, was proved in [14].

Theorem 1.1. *A $\bar{\rho}$ of S-type with $N(\bar{\rho}) = 1$ arises from $S_{k(\bar{\rho})}(\mathrm{SL}_2(\mathbb{Z}))$.*

This built on the ideas introduced in [12].

In this paper we first extend Theorem 1.1, and the methods of its proof, and prove the following theorem.

Theorem 1.2. *1. Let p be an odd prime. Then a $\bar{\rho}$ of S-type with $N(\bar{\rho})$ an odd integer arises from $S_{k(\bar{\rho})}(\Gamma_1(N(\bar{\rho})))$.*

2. Let $p = 2$. Then a $\bar{\rho}$ of S-type with $k(\bar{\rho}) = 2$ arises from $S_2(\Gamma_1(N(\bar{\rho})))$.

We note that Theorem 1.2(2) also completes the work that the qualitative form of Serre's conjecture implies the refined form by filling in a missing case in characteristic 2 (see [2] and [29]).

We reduce in Theorem 9.1 the general case of Serre's conjecture to a certain hypothesis (H) which is now a theorem of Kisin, see [19]. In Theorem 9.1, assuming (H), we first prove the case $p = 2, k(\bar{\rho}) = 4$, and then we deduce from it the case $p \neq 2$ and $N(\bar{\rho})$ even.

In this part we will prove Theorem 1.2 *modulo two lifting theorems*, Theorem 4.1 (closely related to Theorem 6.1 of [14]) and Theorem 5.1 (closely related to Theorem 5.1 of [14]) below, which we will only state here. Theorems 4.1 and 5.1 are proved in the second part, cf. [13].

1.2. **The nature of the proof of Theorem 1.2.** The proof of Theorem 1.2 can be viewed as a double induction on the complexity of $\bar{\rho}$ as measured by two parameters: (i) the number of prime divisors of the level $N(\bar{\rho})$, and (ii) the residue characteristic p of $\bar{\rho}$ (or, more or less equivalently, the weight $k(\bar{\rho})$). A *raising levels* argument (see Theorem 3.4) is used to reduce proving Theorem 1.2 to representations which are *locally good-dihedral*. The ideas used in the proofs of Theorems 3.2 and 3.1 are those of *weight reduction* of [14] (see Theorem 3.2), which then allows one to use the *killing ramification* idea of [12] restricted to weight 2 (see Theorem 3.1). Theorem 3.3, which is a corollary of Theorem 1.1, is used to get the induction started.

The main new ideas of this paper, as compared to [12] and [14], are as follows:

(i) The reduction of Serre's conjecture to proving it for *locally good-dihedral* $\bar{\rho}$. This is crucial as it allows us to avoid invoking any modularity lifting theorems in the *residually degenerate* cases (i.e., $\bar{\rho}|_{G_{\mathbb{Q}(\mu_p)}}$ reducible) beyond the use of such in the proof of Theorem 1.1, and which are due to Skinner-Wiles (see [27] and [28]).

(ii) The *weight cycles* used in the proof of Theorem 1.1 are completed so that they *start* at weight 2 (see Theorem 3.2).

(iii) This allows one to use the *killing ramification* idea of [12] in a way (see Theorem 3.1) so that the modularity lifting theorems needed here are in the weight 2 case, i.e., the results of Kisin in [17].

1.3. **A comparison to the approach of** [12]**.** The path we tread in the proof of our main theorem has many twists and turns (see diagram in Section 3) some of which could be straightened as modularity lifting techniques become more and more powerful. It might even be possible eventually to tread the very direct path outlined in Section 5 of [12].

The rather strong use made of various types of lifts (*congruences between Galois representations*) of a given residual representation is the main distinction between the approach here as well as in [14], and the approach sketched in Section 5 of [12]. The latter sought to prove Serre's conjecture using only minimal lifts and the compatible systems these live in.

The use of congruences between Galois representations, which allows one to be very conservative in the modularity lifting results used, we believe will be of help when proving modularity in other contexts. To be conservative in this matter seems like a virtue to us!

One of the subtleties in the approach we adopt here is that we make serious use of modularity lifting theorems for 2-adic lifts (see Theorem 4.1 (1)). As we believe that for the general case of Serre's conjecture, modularity lifting theorems for 2-adic lifts are unavoidable (see Theorem 9.1 and Hypothesis (H)), this seems fitting.

1.4. **Description of the paper.** In Section 2 we single out a class of $\bar{\rho}$ that we call *locally good-dihedral* (see Definition 2.1) which is easier for us to deal with. In Section 3 we reduce the proof of Theorem 1.2 to some auxiliary

theorems. In Sections 4 and 5 we state the Theorems 4.1 and 5.1 which are proved in [13]. In Section 6 we prove some easy lemmas needed for the proof of Theorem 1.2. In Section 7 some estimates on prime numbers are given that are needed for the proof of Theorem 3.2. The auxiliary theorems stated in Section 3 are proved in Section 8, modulo Theorems 4.1 and 5.1. In Section 9 we reduce the general case to a certain Hypothesis (H). In Section 10 we spell out a consequence of our main theorem for 2-dimensional, irreducible compatible systems of odd representations of $G_{\mathbb{Q}}$.

1.5. **Notation.** For F a field, $\mathbb{Q} \subset F \subset \overline{\mathbb{Q}}$, we write G_F for the Galois group of $\overline{\mathbb{Q}}/F$. For λ a prime/place of F, we mean by D_λ (resp., I_λ if λ is finite) a decomposition (resp., inertia) subgroup of G_F at λ. Recall that for each place p of $\mathbb{Q}$, we have fixed an embedding ι_p of $\overline{\mathbb{Q}}$ in its completions $\overline{\mathbb{Q}_p}$. Denote by χ_p the p-adic cyclotomic character, and ω_p the Teichmüller lift of the mod p cyclotomic character $\overline{\chi}_p$ (the latter being the reduction mod p of χ_p). By abuse of notation we also denote by ω_p the ℓ-adic character $\iota_\ell \iota_p^{-1}(\omega_p)$ for any prime ℓ: this should not cause confusion as from the context it will be clear where the character is valued. We also denote by $\omega_{p,2}$ a fundamental character of level 2 (valued in $\mathbb{F}_{p^2}^*$) of I_p: it factors through the unique quotient of I_p that is isomorphic to $\mathbb{F}_{p^2}^*$. We denote by the same symbol its Teichmüller lift, and also all its ℓ-adic incarnations $\iota_\ell \iota_p^{-1}(\omega_{p,2})$. For a number field F we denote the restriction of a character of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ to G_F by the same symbol. Mod p and p-adic representations of $G_{\mathbb{Q}}$ arising from newforms, or reducible mod p representations of $G_{\mathbb{Q}}$ which are odd, are said to be *modular*, another standard bit of terminology.

2. A crucial definition

Define the function $Q : \mathbb{N} \to \mathbb{N}$ such that $Q(1) = 1$, and for $n \geq 2$, $Q(n)$ is the largest prime that divides n.

Definition 2.1. *Let $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ be a continuous representation.*

We say that $q \neq p$ is a good dihedral prime for $\bar{\rho}$ if

(i) $\bar{\rho}|_{I_q}$ is of the form

$$\begin{pmatrix} \psi & 0 \\ 0 & \psi^q \end{pmatrix},$$

where ψ is a non-trivial character of I_q of order a power of an odd prime $t \neq q$, such that t divides $q+1$, and $t > \max(Q(\frac{N(\bar{\rho})}{q^2}), 5, p)$;

(ii) q is 1 mod 8, and 1 mod r for every prime $r \neq q$ such that $r \leq \max(Q(\frac{N(\bar{\rho})}{q^2}), p)$.

If there exists a good dihedral prime q for $\bar{\rho}$ we say that $\bar{\rho}$ is locally good-dihedral (for the prime q), or q-dihedral.

3. Proof of Theorem 1.2

In this section we state four theorems and derive Theorem 1.2 from them. The proofs of the theorems stated here, modulo Theorems 4.1 and 5.1, will be given in Section 8.

3.1. **Auxiliary theorems.** Consider the following hypotheses (for integers $r \geq 1$):

(L_r) All $\bar{\rho}$ of S-type which satisfy the following three conditions are modular: (a) $\bar{\rho}$ is locally good-dihedral; (b) $k(\bar{\rho}) = 2$ if $p = 2$; (c) $N(\bar{\rho})$ is odd and divisible by at most r primes.

(W_r) All $\bar{\rho}$ of S-type which satisfy the following three conditions are modular: (a) $\bar{\rho}$ is locally good-dihedral; (b) $k(\bar{\rho}) = 2$; (c) $N(\bar{\rho})$ is odd and divisible by at most r primes.

Theorems 3.1 and 3.2 exhibit relations between the (L_r)'s and (W_r)'s (besides the obvious one that (L_r) implies (W_r)!). Diagramatically the relations in Theorems 3.1 and 3.2 may be summarised as:

$$W_1 \Longrightarrow L_1$$
$$\searrow$$
$$W_2 \Longrightarrow L_2$$
$$\ldots$$
$$W_r \Longrightarrow L_r$$
$$\searrow$$
$$W_{r+1} \Longrightarrow L_{r+1}$$
$$\ldots$$

The following theorem is the idea of *killing ramification* of [12].

Theorem 3.1. *(killing ramification in weight 2) For a positive integer r, (L_r) implies (W_{r+1}).*

The following theorem is the idea of *weight reduction* of [14] (or *weight cycles* as they are called in [15]).

Theorem 3.2. *(reduction to weight 2) For a positive integer r, (W_r) implies (L_r).*

The following theorem is deduced from Corollary 1.2 of [14], and provides a starting point from which to apply Theorem 3.2 and 3.1.

Theorem 3.3. *The hypothesis (W_r) is true if $r = 1$.*

The following theorem uses an analog, for Galois representations, of a result for modular forms due to Carayol (see Section 5 of [4]) that is provided by Theorem 5.1 (4). It is used to reduce the proof of Theorem 1.2 to the proofs of Theorems 3.1, 3.2 and 3.3.

Theorem 3.4. *(raising levels)*

Assume the following hypothesis for a given integer $r \geq 0$:

(D_r) All $\bar{\rho}$ of S-type which satisfy the following three conditions are modular: (a) $\bar{\rho}$ is locally good-dihedral; (b) the residue characteristic of $\bar{\rho}$ is an odd prime; (c) $N(\bar{\rho})$ is not divisible by 2^{r+1}.

Then any $\bar{\rho}$ of S-type of residue characteristic p of conductor not divisible by 2^{r+1}, and with $k(\bar{\rho}) = 2$ if $p = 2$ and $r = 0$, is modular.

Remark: Note that by Theorem 3.4, (D_0) implies Serre's conjecture for $\bar{\rho}$ of S-type in odd characteristic with $N(\bar{\rho})$ odd, and for $\bar{\rho}$ of S-type in characteristic 2 with $k(\bar{\rho}) = 2$. Further (D_1) implies Serre's conjecture for $\bar{\rho}$ of S-type in characteristic 2, and for $\bar{\rho}$ of S-type in odd characteristic with $N(\bar{\rho})$ not divisible by 4.

3.2. **Proof of Theorem 1.2.** We will explain how hypothesis (D_0) follows from Theorems 3.1, 3.2 and 3.3. Then by Theorem 3.4, and the remark after it, we get Theorem 1.2.

Notice that hypothesis (D_0) will be satisfied if we prove (L_r) for each $r \geq 1$. We do this by induction on r.

(L_1): Theorem 3.3 fulfills the hypothesis (W_1) of Theorem 3.2. Thus Theorem 3.2 gives that (L_1) is true.

Induction step: Assume we have proved (L_r) for $r \geq 1$, and we want to prove (L_{r+1}). The hypothesis (L_r) implies the hypothesis (W_{r+1}) by Theorem 3.1. This by Theorem 3.2 yields (L_{r+1}).

4. Modularity lifting results

Consider $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ with $\mathbb{F}$ a finite field of characteristic p and $2 \leq k(\bar{\rho}) \leq p+1$ when $p > 2$. We assume that $\bar{\rho}$ has non-solvable image and is modular.

A continuous representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$, for $\mathcal{O}$ the ring of integers of a finite extension of $\mathbb{Q}_p$, is said to be a lift of $\bar{\rho}$ if the reduction of ρ modulo the maximal ideal of $\mathcal{O}$ is isomorphic to $\bar{\rho}$. We say that ρ is *odd* if $\det(\rho(c)) = -1$ for c a complex conjugation. If ρ is Hodge-Tate of weights $(k-1, 0)$ at p (for $k \in \mathbb{N}, k \geq 2$), we say that ρ is of weight k.

The proof of the following key technical result is postponed to the second part, cf. [13].

Theorem 4.1. *Consider $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ with $\mathbb{F}$ a finite field of characteristic p and $2 \leq k(\bar{\rho}) \leq p+1$ when $p > 2$. We assume that $\bar{\rho}$ has non-solvable image. We assume that $\bar{\rho}$ is modular.*

1. ($p = 2$) Let ρ be an odd lift of $\bar{\rho}$ to a 2-adic representation that is unramified outside a finite set of primes and is either Barsotti-Tate at 2,

or semistable of weight 2 at 2 with the latter case considered only when $k(\bar{\rho}) = 4$. Then ρ is modular.

2. ($p > 2$) Let ρ be a lift of $\bar{\rho}$ to a p-adic representation that is unramified outside a finite set of primes and is either (i) crystalline of weight k at p with $2 \leq k \leq p+1$, or (ii) potentially semistable at p of weight 2 (i.e., either up to twist semistable of weight 2, or potentially Barsotti-Tate (BT) at p). Then ρ is modular.

5. Lifting results

5.1. **Compatible systems of geometric representations.** Let $F \subset \overline{\mathbb{Q}}$ be a number field and let $\rho : G_F \to \mathrm{GL}_d(\overline{\mathbb{Q}_\ell})$ be a (continuous) Galois representation. We recall that it is called geometric if it is unramified outside a finite set of primes of F and its restrictions to the decomposition groups at primes above ℓ are potentially semi-stable ([8]). Such a representation defines for every prime q of F a representation of the Weil-Deligne group WD_q with values in $\mathrm{GL}_d(\overline{\mathbb{Q}_\ell})$, well defined up to conjugacy. For q of characteristic $\neq \ell$, this comes from the theory of Deligne-Grothendieck; for q of characteristic ℓ, this comes from the theory of Fontaine ([5], exp. 8 of [20], [8]).

For a number field E, we call an E-rational, 2-dimensional *strictly compatible system* of geometric representations (ρ_ι) of G_F the data of:
(i) for each prime ℓ and each embedding $\iota : E \hookrightarrow \overline{\mathbb{Q}_\ell}$, a continuous, semisimple geometric representation $G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}_\ell})$:
(ii) for all prime q of F, a F-semisimple (Frobenius semisimple) representation r_q of the Weil-Deligne group WD_q with values in $\mathrm{GL}_2(E)$ such that:

- a) r_q is unramified for all q outside a finite set,
- b) for each ℓ and each $\iota : E \hookrightarrow \overline{\mathbb{Q}_\ell}$, the Frobenius-semisimple Weil-Deligne parameter $\mathrm{WD}_q \to \mathrm{GL}_2(\overline{\mathbb{Q}_\ell})$ associated to $\rho_\iota|_{D_q}$ is conjugate to r_q (via the embedding $E \hookrightarrow \overline{\mathbb{Q}_\ell}$)).

(iii) there are two integers a, b, $a \geq b$, such that ρ_ι has Hodge-Tate weights (a, b).

The primes of F such that r_q is unramified are called the unramified primes of the compatible system. The restriction to $I_q \times \mathbb{G}_\mathrm{a}$ of r_q is called the inertial WD parameter at q. We refer to a, b, as the weights of the compatible system and when $a \geq 0, b = 0$ we say that ρ_ι is of weight $a + 1$. When $a \neq b$ we say that the compatible system is regular and otherwise irregular.

If we only impose (ii) b) for primes q not above ℓ, we shall say that the system is *compatible* .

When we say that for some number field E, an E-rational compatible system (ρ_ι) of 2-dimensional representations of $G_\mathbb{Q}$ lifts $\bar{\rho}$ we mean that the residual representation arising from ρ_{ι_p} is isomorphic to $\bar{\rho}$. We say that a compatible system (ρ_ι) is odd if ρ_ι is odd for every ι. For a prime ℓ we abuse notation and denote by ρ_ℓ the ℓ-adic representation ρ_ι for ι the chosen

embedding above ℓ. We say that a compatible system (ρ_ι) is *irreducible* if all the ρ_ι are irreducible.

When we say that $\rho := \rho_p$ is a minimal lift at q of the corresponding residual mod $p > 2$ representation $\bar{\rho}$, at primes q of characteristic $\ell \neq p$, we mean that the condition in Section 3 of [6] is satisfied. In particular, whenever $\bar{\rho}(I_q)$ is projectively not cyclic of order p, the reduction map $\rho(I_q) \to \bar{\rho}(I_q)$ is bijective. For $p = 2$ see section 3.3.1. of part 2. For every p, the restriction to inertia of the determinant of a minimal lift is the Teichmüller lift. When $\bar{\rho}(I_q)$ is projectively cyclic of order p, $\bar{\rho}_{|I_q}$ is of the shape :

$$\overline{\xi} \otimes \begin{pmatrix} 1 & \overline{\eta} \\ 0 & 1 \end{pmatrix},$$

$\overline{\eta}$ non trivial, and we ask that $\rho_{|I_q}$ isomorphic to:

$$\xi \otimes \begin{pmatrix} 1 & \eta \\ 0 & 1 \end{pmatrix},$$

with η a lift of $\overline{\eta}$ and ξ the Teichmüller lift of $\overline{\xi}$ (3.3.1. of [13]).

The proof of the following key technical result, close to Theorem 5.1 of [14], is postponed to the second part, cf. [13].

Theorem 5.1. *Consider a S-type representation $\bar{\rho}$ with $2 \leq k(\bar{\rho}) \leq p+1$ when $p > 2$, and assume that the image of $\bar{\rho}$ is not solvable.*

1. Assume $k(\bar{\rho}) = 2$ if $p = 2$. Then $\bar{\rho}$ lifts to an E-rational strictly compatible, irreducible, odd system (ρ_ι), such that the p-adic lift ρ_p of ρ is minimally ramified at all primes $\neq p$ and is crystalline of weight $k(\bar{\rho})$ at p.

2. $\bar{\rho}$ lifts to an E-rational strictly compatible, irreducible, odd system (ρ_ι), such that the p-adic lift ρ_p of $\bar{\rho}$ is of weight 2 and is minimally ramified at primes $\neq p$, and such that the inertial Weil-Deligne parameter of p is $(\omega_p^{k(\bar{\rho})-2} \oplus 1, 0)$ if $k(\bar{\rho}) \neq p+1$ when $p > 2$ and $k(\bar{\rho}) \neq 4$ when $p = 2$. In the case $p > 2, k(\bar{\rho}) = p+1$ or $p = 2$ and $k(\bar{\rho}) = 4$ it is of the form (id, N) with N a non-zero nilpotent matrix $\in \mathrm{GL}_2(\overline{\mathbb{Q}})$.

3. Assume $q||N(\bar{\rho})$ with q an odd prime such that $p|q-1$. Then $\bar{\rho}|_{I_q}$ is of the form

$$\begin{pmatrix} \overline{\chi} & * \\ 0 & 1 \end{pmatrix},$$

with $\overline{\chi}$ a character of I_q that factors through its quotient $(\mathbb{Z}/q\mathbb{Z})^*$. Let $\chi' = \omega_q^i$ $(0 < i \leq q-2)$ be any non-trivial $\overline{\mathbb{Z}}_p^*$-valued character of I_q that factors though $(\mathbb{Z}/q\mathbb{Z})^*$ and reduces to $\overline{\chi}$, and such that when $p = 2$, i is even.

There is an E-rational strictly compatible, irreducible, odd system (ρ_ι) that lifts $\bar{\rho}$, such that the p-adic lift ρ_p of $\bar{\rho}$ is minimally ramified at primes $\neq p, q$, and at p is either: (i) semistable of weight 2, or (ii) Barsotti-Tate over $\mathbb{Q}_p(\mu_p)$, and (iii) Barsotti-Tate at p if $k(\bar{\rho}) = 2$. Further $\rho_p|_{I_q}$ is of the form

$$\begin{pmatrix} \chi' & * \\ 0 & 1 \end{pmatrix}.$$

The residual representation $\bar{\rho}_q$, up to twisting by some power of $\overline{\chi}_q$, has Serre weight either $i+2$ or $q+1-i$.

4. Let $q \neq p$ be a prime and assume $\bar{\rho}|_{D_q}$ (up to unramified twist) is of the form

$$\begin{pmatrix} \overline{\chi}_p & * \\ 0 & 1 \end{pmatrix},$$

and assume that $p|q+1$. Let $\{\chi', \chi'^q\}$ be any pair of $\overline{\mathbb{Z}}_p^*$-valued characters of I_q of level 2 (i.e., that factors though $\mathbb{F}_{q^2}{}^*$, but not through $\mathbb{F}_q^*$) and which are of order a power of p. Thus we may write χ' as $\omega_{q,2}^i \omega_{q,2}^{qj}$ for some $0 \leq i < j \leq q-1$: we further assume that when $p=2$, $i+j$ is even.

Then there is an E-rational strictly compatible, irreducible, odd system (ρ_ι) that lifts $\bar{\rho}$, such that the p-adic, lift ρ_p of $\bar{\rho}$ is minimally ramified at primes $\neq p, q$ and at p is either: (i) semistable of weight 2, or (ii) Barsotti-Tate over $\mathbb{Q}_p(\mu_p)$, and (iii) Barsotti-Tate at p if $k(\bar{\rho}) = 2$. Further $\rho_p|_{I_q}$ is of the form

$$\begin{pmatrix} \chi' & * \\ 0 & \chi'^q \end{pmatrix}.$$

If q is odd, the residual representation $\bar{\rho}_q$, up to twisting by some power of $\overline{\chi}_q$, has Serre weight either $q+1-(j-i)$ or $j-i$ when $j > i+1$, and q when $j = i+1$.

Remark: The computation of the weights of the residual representations in Theorem 5.1 (3) and (4) is done by Savitt in Corollary 6.15 (1) and (2) of [25]. The conditions of parity when $p=2$ garantee that the lift ρ is odd.

6. Some utilitarian lemmas

We recall Dickson's theorem (see [10], II.8.27): for any prime p a finite subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}_p})$ that acts irreducibly on $\overline{\mathbb{F}_p}^2$ has projective image that is either isomorphic to a dihedral group, A_4, S_4, A_5, $\mathrm{PSL}_2(\mathbb{F}')$ or $\mathrm{PGL}_2(\mathbb{F}')$ for $\mathbb{F}'$ a finite subfield of $\overline{\mathbb{F}_p}$. Note also that $\mathrm{PSL}_2(\mathbb{F}')$ is a simple (non-abelian) group as soon as $|\mathbb{F}'| \geq 4$. Although the lemma below, which refines the above statement for $p=2$, is also a part of Dickson's theorem it is often not stated as such, and we give the easy proof. (We thank Serre for some correspondence about this.)

Lemma 6.1. *Let G be a finite, solvable subgroup of $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$ which acts irreducibly on $\overline{\mathbb{F}}_2{}^2$. Then the projective image of G is dihedral.*

Proof. By Dickson's theorem, the projective image of G is isomorphic to a dihedral group, A_4 or S_4. The possibility of S_4 can be ruled out as any element in $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$ of order a power of 2 is forced to be of order 1 or 2. The possibility of A_4 can be ruled out by using the facts that A_4 has a normal subgroup of order 4, and that a Sylow 2-subgroup of $\mathrm{GL}_2(\mathbb{F})$ for $\mathbb{F}$ a finite field of characteristic 2 is given by the unipotent matrices. This forces a G with projective image A_4 to be conjugate to a subgroup of the upper

triangular matrices of $\mathrm{GL}_2(\overline{\mathbb{F}}_2)$. This contradicts the hypothesis that G acts irreducibly on $\overline{\mathbb{F}}_2{}^2$. □

Lemma 6.2. *(i) Let $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ be an S-type representation with solvable image. Then $\bar{\rho}$ is modular, and in fact arises from $S_{k(\bar{\rho})}(\Gamma_1(N(\bar{\rho})))$.*

(ii) If $\bar{\rho}$ is of S-type, $p \geq 3$, $2 \leq k(\bar{\rho}) \leq p+1$, and $\bar{\rho}|_{G_{\mathbb{Q}(\mu_p)}}$ is reducible, then $\bar{\rho}$ has weight either $\frac{p+1}{2}$ or $\frac{p+3}{2}$.

Proof. (i) If $p > 2$ this is a consequence of the Langlands-Tunnell theorem (see Theorem 4 of [16]). If $p = 2$ we only have to consider the case when the projective image of $\bar{\rho}$ is dihedral by Lemma 6.1. The dihedral case follows from the method of proof of Proposition 10 of [26]: see [22], where this is alluded to as the "trick of Serre", or Lemma 2 of [29]. For $p = 2$, it follows from Theorem 1 of [29] that $\bar{\rho}$ arises from $S_{k(\bar{\rho})}(\Gamma_1(N(\bar{\rho})))$.

(ii) As $p > 2$ the projectivisation $\bar{\rho}_{\mathrm{proj}}$ of the representation $\bar{\rho}$ is tamely ramified at p, and thus $\bar{\rho}_{\mathrm{proj}}(I_p)$ is cyclic. As the quadratic subfield of $\mathbb{Q}(\mu_p)$ is ramified at p, $\bar{\rho}_{\mathrm{proj}}(I_p)$ is of order 2. From this the result follows by the definition of $k(\bar{\rho})$ in Section 2 of [26].

□

Remark: Just as in [14], it should be possible with greater care to avoid using Lemma 6.2 in the proof of Theorem 1.2 except in the case when $\bar{\rho}$ has (projectively) dihedral image.

Lemma 6.3. *Let $\bar{\rho}$ be a locally good-dihedral representation (for a prime q).*

(i) The image of $\bar{\rho}$ is not solvable.

(ii) Let (ρ_ι) be any strictly compatible system lifting of $\bar{\rho}$ such that the ramified primes of the compatible system are contained in the prime divisors of $N(\bar{\rho})p$ and $\rho_p|_{D_q}$ is a minimal lift of $\bar{\rho}|_{D_q}$. Then for any prime $r \leq \max(Q(\frac{N(\bar{\rho})}{q^2}), p)$, any mod r representation $\bar{\rho}_r$ that arises from (ρ_ι) is locally good-dihedral (for the prime q) and hence has non-solvable image (which is projectively not isomorphic to A_5).

Proof. Part (ii) follows from strict compatibility, part (i) and the following observation. Let $a \geq 1$ be an integer, let $t \neq 2$ and r be distinct primes. Let $D_{2t^a} \subset \mathrm{PGL}_2(\overline{\mathbb{Q}_r})$ be the dihedral group of order $2t^a$ which we may assume to be a subgroup of $\mathrm{PGL}_2(\overline{\mathcal{O}})$ with $\overline{\mathcal{O}}$ the valuation ring of $\overline{\mathbb{Q}}_r$. Then the reduction map is bijective on D_{2t^a}.

Let us prove (i). By definition $\bar{\rho}|_{I_q}$ is of the form

$$\begin{pmatrix} \psi & 0 \\ 0 & \psi^q \end{pmatrix},$$

where ψ is a character of I_q of order a power of a prime $t|q+1$, and t is bigger than $\max(r, p, 5)$ where $r \neq q$ ranges over primes that divide $N(\bar{\rho})$. As t does not divide $q-1$, $\bar{\rho}|_{D_q}$ is irreducible, and hence so is $\bar{\rho}$. As $t > 5$, we see that the projective image cannot be A_5.

We see that if the image of $\bar{\rho}$ is solvable, as $t > 5$, then by Dickson's theorem the projective image of $\bar{\rho}$ is dihedral. Note that the primes s different from q at which $\bar{\rho}$ is ramified are such that q is 1 mod s (and 1 mod 8 if $s = 2$). Suppose $\bar{\rho}$ is induced from G_K with K a quadratic extension of $\mathbb{Q}$. Then K is unramified outside the primes that are ramified in $\bar{\rho}$. Thus the prime q either splits in K or is ramified in K: both possibilities lead to a contradiction. If q splits in K, this contradicts the fact that $\bar{\rho}|_{D_q}$ is irreducible. If K is ramified at q we again get a contradiction as t is odd. □

7. Estimates on primes

In the arguments below we need to check, that for each prime $p \geq 5$, there is a prime $P > p$ (for instance the next prime after p) and either

(i) an odd prime power divisor $\ell^r || (P-1)$ so that

$$\frac{P}{p} \leq \frac{2m+1}{m+1} - (\frac{m}{m+1})(\frac{1}{p}) \tag{1}$$

where we have set $\ell^r = 2m+1$ with $m \geq 1$, or

(ii) $2^r || (P-1)$ (with $r \geq 4$) so that

$$\frac{P}{p} \leq \frac{2^r}{2^{r-1}+2} - (\frac{2^{r-1}-2}{2^{r-1}+2})(\frac{1}{p}). \tag{2}$$

This can be checked as in [14] using the estimates on primes of [23] as follows:

We check this by hand for $p \leq 31$. From [23] one deduces (see [14]) that for $p > 31$, $\frac{P}{p} \leq \frac{3}{2} - (\frac{1}{30}) = 1.4\overline{6}$. This establishes (1) and (2) above as $\frac{2m+1}{m+1}$ and $\frac{2^r}{2^{r-1}+2}$ are $\geq \frac{3}{2}$ and $\frac{m}{m+1}$ and $\frac{2^{r-1}-2}{2^{r-1}+2}$ are ≤ 1 (for $m \geq 1, r \geq 4$).

For later reference we note that it follows from (1) that

$$p+1 \geq \frac{m+1}{2m+1}(P-1) + 2 = (P+1) - \frac{m}{2m+1}(P-1), \tag{3}$$

and it follows from (2) that

$$p+1 \geq \frac{2^{r-1}+2}{2^r}(P-1) + 2 \geq (P+1) - \frac{1}{2}(P-1). \tag{4}$$

Remark : It is proven in [14] that in fact one can always find P such that (i) holds (for example P the smallest non Fermat prime $> p$).

8. Proofs of the auxiliary theorems

8.1. **Proof of Theorem 3.1.** Assume (L_r).

Consider $\bar{\rho}$ of S-type which is locally good-dihedral for a prime q, with $k(\bar{\rho}) = 2$, and such that $N(\bar{\rho})$ is odd and at most divisible by $r+1$ primes. Choose a prime $s \neq q$ that divides $N(\bar{\rho})$.

By Theorem 5.1 (1) construct a compatible lift (ρ_ι) and consider ρ_s. Then $\bar{\rho}_s$ is a S-type representation, is q-dihedral and hence has non-solvable image (by Lemma 6.3 (ii)) , and $N(\bar{\rho}_s)$ is divisible by at most r primes: the prime

divisors of $N(\bar{\rho}_s)$ are a subset of the set of the prime divisors of the prime-to-s part of $N(\bar{\rho})$. Thus by (L_r) we know $\bar{\rho}_s$ is modular, and then by Theorem 4.1 we are done.

8.2. **Proof of Theorem 3.2.** Assume (W_r). Then we have to prove that any $\bar{\rho}$ of S-type which is locally good-dihedral (for a prime q), such that p is odd, $N(\bar{\rho})$ is odd, and divisible by at most r primes, is modular.

We do this by induction on the prime p as in the paper [14].

We first do the case $p = 3$ and $p = 5$ as the arguments in these cases are a little different from the general inductive step of the proof.

Mod 3: Consider $\bar{\rho}$ of S-type which is locally good-dihedral (for a prime q), $k(\bar{\rho}) \leq 4$ in residue characteristic 3, $N(\bar{\rho})$ is odd, and at most divisible by r primes. Using Theorem 5.1 (2) lift it to a compatible system (ρ_ι) and consider ρ_2. The residual representation $\bar{\rho}_2$ is q-dihedral and hence has non-solvable image (see Lemma 6.3), $k(\bar{\rho}_2) = 2$ and $N(\bar{\rho}_2)$ is divisible by at most at $r + 1$ primes, the primes dividing $N(\bar{\rho})$ and 3. If $\bar{\rho}_2$ is unramified at 3, $N(\bar{\rho}_2)$ is divisible by at most r primes, and then $\bar{\rho}_2$ is modular by (W_r). Theorem 4.1 yields that (ρ_ι) is modular and hence $\bar{\rho}$ is modular in this case.

Otherwise, note that $\bar{\rho}_2|_{I_3}$ is unipotent, as $\overline{\chi_3}$ is of order 2. Thus $\bar{\rho}_2|_{D_3}$ (up to unramified twist) is of the form

$$\begin{pmatrix} \overline{\chi}_2 & * \\ 0 & 1 \end{pmatrix}.$$

Thus we may use Theorem 5.1 (4) to lift $\bar{\rho}_2$ to an odd compatible system (ρ'_ι), choosing $\chi' = \omega_{3,2}^2$. Consider ρ'_3 and the residual representation $\bar{\rho}'_3$ which by Lemma 6.3 is q-dihedral and hence has non-solvable image. By Theorem 5.1 (4), a twist of $\bar{\rho}'_3$ has weight 2, and $N(\bar{\rho}'_3)$ is odd and divisible by at most r primes. Thus $\bar{\rho}'_3$ is modular by (W_r), and we are done by applying Theorem 4.1.

Mod 5: Consider $\bar{\rho}$ of S-type which is locally good-dihedral (for a prime q), in residue characteristic 5, $N(\bar{\rho})$ is odd, $k(\bar{\rho}) \leq 6$, and at most divisible by r primes. Using Theorem 5.1 (2) lift it to a compatible system (ρ_ι) and consider ρ_2. The residual representation $\bar{\rho}_2$ is q-dihedral and hence has non-solvable image (see Lemma 6.3), $k(\bar{\rho}_2) = 2$ and $N(\bar{\rho}_2)$ is divisible by at most $r+1$ primes. If $\bar{\rho}_2$ is unramified at 5, $N(\bar{\rho}_2)$ is divisible by at most r primes, and then $\bar{\rho}_2$ is modular by (W_r). Theorem 4.1 yields that (ρ_ι) is modular and hence $\bar{\rho}$ is modular.

Otherwise we use Theorem 5.1 (3) to lift $\bar{\rho}_2$ to an odd compatible system (ρ'_ι), choosing $\chi' = \omega_5^2$. Consider ρ'_5 and the residual representation $\bar{\rho}'_5$: by Lemma 6.3, $\bar{\rho}'_5$ is q-dihedral and has non-solvable image. By Theorem 5.1 (3) (after twisting by a suitable power of $\overline{\chi}_5$) $\bar{\rho}'_5$ has weight 4. The conductor $N(\bar{\rho}'_5)$ is odd and divisible by at most r primes. It will be enough to prove that $\bar{\rho}'_5$ is modular, as then Theorem 4.1 yields that (ρ'_ι) is modular. The compatible systems (ρ_ι) and (ρ'_ι) are linked at 2 (we have $\overline{\rho_2} \simeq \overline{\rho'_2}$).

Another application of Theorem 4.1 yields that (ρ_ι) is modular, and hence $\bar\rho$ is modular.

It remains to prove that $\bar\rho'_5$ is modular. There are 2 cases:

(i) either 3 divides $N(\bar\rho'_5)$, or

(ii) 3 does not divide $N(\bar\rho'_5)$.

In the case of (i) we use Theorem 5.1 (2) to get a compatible lift (ρ''_ι) of $\bar\rho'_5$ and then observe that $N(\bar\rho''_3)$ is odd and is divisible by at most r primes: note that the set of primes that divide the odd integer $N(\bar\rho''_3)$ is a subset of the set of prime divisors of the prime-to-3 part of $5N(\bar\rho'_5)$. As we know the modularity of such a $\bar\rho''_3$ (which is again q-dihedral) by the earlier step, we may apply Theorem 4.1 to conclude that the compatible system (ρ''_ι) is modular, and hence that $\bar\rho'_5$ is modular.

In the case of (ii) we use Theorem 5.1 (1) to get a compatible lift (ρ''_ι) of $\bar\rho'_5$ which is of weight 4. We know the modularity of $\bar\rho''_3$ by the earlier step: in this case the set of primes that divide the odd integer $N(\bar\rho''_3)$ is a subset of the set of prime divisors of $N(\bar\rho'_5)$. Then we may apply Theorem 4.1 to conclude that (ρ''_ι) is modular (note that $k(\rho''_3) = 4 \leq 3+1$). Hence $\bar\rho'_5$ is modular.

The inductive step: Our inductive assumption is that all $\bar\rho$ of S-type which are locally good-dihedral, in residue characteristic $\leq p$, for p a prime with $p \geq 5$, such that $N(\bar\rho)$ is odd, and at most divisible by r primes are modular. Let P be the next prime after p. We will prove modularity of all $\bar\rho$ of S-type which are good-dihedral (for a prime q), in residue characteristic P, such that $N(\bar\rho)$ is odd, and at most divisible by r primes.

Consider $\bar\rho$ of S-type which is locally good-dihedral (for a prime q), in residue characteristic P, $N(\bar\rho)$ is odd, $k(\bar\rho) \leq P+1$ and at most divisible by r primes. Choose a prime divisior $\ell^r || (P-1)$ that satisfies one of the estimates (1) or (2) of Section 7. Using Theorem 5.1 (2) lift it to a compatible system (ρ_ι) and consider ρ_ℓ. The residual representation $\bar\rho_\ell$ is q-dihedral and hence has non-solvable image (see Lemma 6.3), and $N(\bar\rho_\ell)$ is odd and divisible by at most $r+1$ primes. If $\bar\rho_\ell$ is unramified at P, $N(\bar\rho_\ell)$ is divisible by at most r primes, and then $\bar\rho_\ell$ is modular by our inductive assumption as $\ell \leq p$. Theorem 4.1 yields that (ρ_ι) is modular and hence $\bar\rho$ is modular.

Otherwise we use Theorem 5.1 (3) to lift $\bar\rho_\ell$ to an odd compatible system (ρ'_ι), choosing $\chi' = \omega_P^i$ with $i \in [\frac{m}{2m+1}(P-1), \frac{m+1}{2m+1}(P-1)]$ when $\ell > 2$, and an even $i \in [\frac{1}{2}(P-1), \frac{2^{r-1}+2}{2^r}(P-1)]$ when $\ell = 2$. Consider ρ'_P and the residual representation $\bar\rho'_P$. By choice of i, the estimates (3) and (4) of Section 7, and Theorem 5.1 (3), we deduce that (after twisting by a suitable power of $\overline{\chi}_P$) $k(\bar\rho'_P) \leq p+1$, and is q-dihedral and hence has non-solvable image, and the conductor $N(\bar\rho'_P)$ is odd and divisible by at most r primes. (Note that if $\ell | N(\bar\rho'_P)$, then $\ell | N(\bar\rho)$.) It will be enough to prove that $\bar\rho'_P$ is modular, as then Theorem 4.1 yields that (ρ'_ι) is modular. The compatible systems (ρ_ι) and (ρ'_ι) are linked at ℓ, and another application of Theorem 4.1 yields that (ρ_ι) is modular, and hence $\bar\rho$ is modular.

It remains to prove that $\bar{\rho}'_P$ is modular. There are 2 cases:
(i) either p divides $N(\bar{\rho}'_P)$, or
(ii) p does not divide $N(\bar{\rho}'_P)$.

In the case of (i) we use Theorem 5.1 (2) to get a compatible lift (ρ''_ι) of $\bar{\rho}'_P$ and then observe that $N(\bar{\rho}''_p)$ is odd and divisible by at most r primes: note that the set of primes that divide $N(\bar{\rho}''_p)$ is a subset of the set of prime divisors of the prime-to-p part of $PN(\bar{\rho}'_P)$. As we inductively know the modularity of such a $\bar{\rho}''_p$ (which is again q-dihedral), we may apply Theorem 4.1 to conclude that the compatible system (ρ''_ι) is modular, and hence that $\bar{\rho}'_P$ is modular.

In the case of (ii) we use Theorem 5.1 (1) to get a compatible lift (ρ''_ι) of $\bar{\rho}'_P$. We inductively know the modularity of $\bar{\rho}''_p$: in this case the set of primes that divide the odd integer $N(\bar{\rho}''_p)$ is a subset of the set of prime divisors of $N(\bar{\rho}'_P)$. Then we may apply Theorem 4.1 to conclude that (ρ''_ι) is modular, and hence that $\bar{\rho}'_P$ is modular.

Remarks:

1. It seems possible with greater care to avoid in the general inductive step of the proof of Theorem 3.2 the use of $\ell = 2$. It is also possible to present the general inductive step slightly differently by at the outset dividing into 2 cases: (i) $\bar{\rho}$ is ramified at some prime $< P$, (ii) $\bar{\rho}$ is unramified at all primes $< P$.

2. As seen above all the residual representations considered in the proofs of Theorem 3.1 and 3.2 are locally good-dihedral which avoids problems of residual degeneracy. Also, starting with a q-dihedral $\bar{\rho}$ in characteristic P, that is ramified at a set of primes S, the proof needs to consider residual representations in characteristic at most $\max_{\ell \in S \setminus \{q\}}(P, \ell)$. This is what motivates our Definition 2.1.

8.3. **Proof of Theorem 3.3.** Theorem 3.3 follows from Corollary 8.1 (i) below, which in turn follows from Corollary 8.1 (ii). The latter (in the case $p > 2$) is Corollary 1.2 of [14].

Corollary 8.1. *(i) If $\bar{\rho}$ is an irreducible, odd, 2-dimensional, mod p representation of $G_{\mathbb{Q}}$ with $k(\bar{\rho}) = 2$, $N(\bar{\rho}) = q$, with q an odd prime, then it arises from $S_2(\Gamma_1(q))$.*

(ii) If $\bar{\rho}$ is an irreducible, odd, 2-dimensional, mod p representation of $G_{\mathbb{Q}}$ with $k(\bar{\rho}) = 2$, unramified outside p and another odd prime q, tamely ramified at q, such that the order of $\bar{\rho}(I_q)$ is the power of an odd prime $t > 5$, then $\bar{\rho}$ arises from $S_2(\Gamma_1(q^2))$.

Proof. The first statement is exactly Corollary 1.2 of [14], except that we also use Theorem 5.1 (1) in the case when $p = 2$.

We reduce the second statement to the first. We may assume that $t \neq p$, as otherwise this is covered by the first statement. Also as $\bar{\rho}$ is tamely

ramified at q, we deduce that $t \neq q$. We may also assume that $\mathrm{im}(\bar{\rho})$ is not solvable as otherwise we are done by Lemma 6.2.

Using Theorem 5.1 (1) we construct a compatible system lift (ρ_ι) of $\bar{\rho}$. Thus ρ_p unramified outside $\{p, q\}$, is Barsotti-Tate at p, $|\rho_p(I_q)| = |\bar{\rho}_p(I_q)|$.

If the reduction $\bar{\rho}_t$ of an integral model of ρ_t is reducible, or unramified at q (which implies reducibility by the proof in [12] of the level 1 weight 2 case of Serre's conjecture), then we are done by applying the modularity lifting theorems of [27], which allow us to conclude that ρ_t is modular, hence (ρ_ι) is modular and hence so is $\bar{\rho}$.

If $\bar{\rho}_t$ is irreducible and ramified at q, then part (i) implies that the representation is modular (as in fact the ramification will be unipotent at q), and then by modularity lifting results in [31], [30], we again conclude that ρ_t is modular, hence (ρ_ι) is modular and hence so is $\bar{\rho}$. The lifting theorems apply as one easily checks that $\bar{\rho}_t|_{\mathbb{Q}(\mu_t)}$ is irreducible using that $k(\bar{\rho}_t) = 2$ and $t > 5$ (see Lemma 6.2 (ii)).

□

8.4. **Proof of Theorem 3.4.** Consider $\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F})$ of S-type, $\mathbb{F}$ a finite field of characteristic p, with $k(\bar{\rho}) = 2$ if $p = 2$ and $r = 0$, and of conductor not divisible by 2^{r+1}.

Let S be the primes other than p at which $\bar{\rho}$ is ramified. We may assume that $\bar{\rho}$ has non-solvable image.

Using Theorem 5.1 (2), construct a compatible system (ρ_λ) that lifts $\bar{\rho}$. If there is a $p' \notin S \cup \{p\}$ and $p' > 5$ at which the mod p' representation $\bar{\rho}_{p'}$ has solvable image we are done after using Lemma 6.2 and then applying the modularity lifting theorems in [27] if $\mathrm{im}(\bar{\rho}_{p'})$ is reducible, or the ones in [31] in the irreducible case. Note that for $p' \notin S \cup \{p\}$, $p' > 5$, $\bar{\rho}_{p'}$ cannot be irreducible and induced from the quadratic subfield of $\mathbb{Q}(\mu_{p'})$ (as $k(\bar{\rho}_{p'}) = 2$ and $p' > 5$: see Lemma 6.2 (ii)).

Thus we may choose $p' > 5$ that is congruent to 1 modulo 4, with p' larger than all the primes in $S \cup \{p\}$, and such that $\bar{\rho}_{p'} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}')$ has non-solvable image with $\mathbb{F}'$ a finite field of characteristic p'.

We have the following general lemma:

Lemma 8.2. *Let p be a prime that is congruent to 1 modulo 4, and $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F})$ a representation of S-type, with $\mathbb{F}$ a finite field of characteristic p. Assume that $\mathrm{im}(\bar{\rho})$ is not solvable. Denote by $\bar{\rho}_{\mathrm{proj}}$ the projectivisation of $\bar{\rho}$, and $c \in G_{\mathbb{Q}}$ a complex conjugation. There is a set of primes $\{q\}$ of positive density that are unramified in $\bar{\rho}$ such that:*

(i) $\bar{\rho}_{\mathrm{proj}}(\mathrm{Frob}_q)$ is the conjugacy class of $\bar{\rho}_{\mathrm{proj}}(c)$,

(i) q is congruent to 1 modulo all primes $\leq p-1$ and is 1 modulo 8,

(iii) q is -1 mod p.

Proof. By Dickson's theorem, and as $\bar{\rho}$ has non-solvable image, the image of $\bar{\rho}_{\mathrm{proj}}$ is conjugate to either $\mathrm{PSL}_2(\mathbb{F}'')$ or $\mathrm{PGL}_2(\mathbb{F}'')$ for some subfield $\mathbb{F}''$ of $\mathbb{F}$, with $|\mathbb{F}''| \geq 4$, or is isomorphic to A_5. When the image is conjugate to

$\mathrm{PGL}_2(\mathbb{F}'')$, note that as p is congruent to 1 mod 4, $\bar{\rho}_{\mathrm{proj}}(c)$ is inside $\mathrm{PSL}_2(\mathbb{F}'')$. As $\mathrm{PSL}_2(\mathbb{F}'')$ (for $|\mathbb{F}''| \geq 4$) and A_5 are simple (and non-cyclic), and as p is congruent to 1 modulo 4, we may appeal to the Cebotarev density theorem as follows. We choose q satisfying the following conditions : $q \equiv 1 \mathrm{mod}(8)$, $\overline{\chi_\ell}(\mathrm{Frob}_q) = 1$ for ℓ odd $< p$, $\overline{\chi_p}(\mathrm{Frob}_q) = -1$, and $\bar{\rho}_{\mathrm{proj}}(\mathrm{Frob}_q)$ conjugate to $\bar{\rho}_{\mathrm{proj}}(c)$. We explain why the conditions are compatible. Let L be the intersection of the field defined by the kernel of $\bar{\rho}_{\mathrm{proj}}$ and the cyclotomic field generated by μ_8, μ_ℓ for ℓ odd $< p$ and μ_p. The degree of L over $\mathbb{Q}$ is either 1 or 2. If it is of degree 1, the compatibilty is clear. If L is quadratic, the image of $\bar{\rho}_{\mathrm{proj}}$ is $\mathrm{PGL}_2(\mathbb{F}'')$, and the first three conditions, as well as the fourth, impose that q is split in L ; it is also the case for the fourth condition, because as p is 1 mod 4, -1 is a square mod p. This proves the lemma.

□

Apply Lemma 8.2 to our $\bar{\rho}_{p'}$, and choose a prime q as in the lemma. Next one uses Theorem 5.1 (4) to lift $\bar{\rho}_{p'}$ to a compatible system (ρ'_λ) such that $\rho_{p'}|_{I_q}$ is of the shape there for some χ' a p'-adic character of I_q level 2 and order a power of p'. Let s be the largest prime $< p'$: consider ρ'_s, and the corresponding residual representation $\bar{\rho}'_s$. Note that $s > 2$, $\bar{\rho}'_s$ is good-dihedral (for the prime q), and $N(\bar{\rho}'_s)$ is not divisible by 2^{r+1}. Thus, by hypothesis (D_r), $\bar{\rho}'_s$ is modular and we know by Lemma 6.3 that $\bar{\rho}'_s$ has non-solvable image. Hence by Theorem 4.1 the compatible system (ρ'_λ) is modular. Observe that the compatible systems (ρ_λ) and (ρ'_λ) are linked at $\bar{\rho}_{p'}$. Applying Theorem 4.1 again we conclude that that (ρ_λ) is modular, and hence $\bar{\rho}$ is modular, proving the theorem.

9. The general case

Consider the following hypothesis:

Hypothesis (H): *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathcal{O})$ be a continuous, odd, irreducible, p-adic representation, such that:*

(i) the residual representation $\bar{\rho}$ has non-solvable image, and $\bar{\rho}$ is modular;

(ii) ρ is unramified outside a finite set of primes, is of weight 2 and potentially crystalline at p.

Then ρ is modular.

We show using essentially all the results and methods of this paper:

Theorem 9.1. *Assume Hypothesis (H). Then Serre's conjecture is true.*

Proof. We will prove (D_r) for all non-negative integers r, thus proving Serre's conjecture (under (H)) by Theorem 3.4.

We begin by proving (D_1) and Serre's conjecture in residue characteristic 2. By Theorem 3.4 it is enough to prove (D_1). Thus we wish to show that a $\bar{\rho}$ of S-type in odd residue characteristic p, which is locally good-dihedral, and with $N(\bar{\rho})$ not divisible by 4, is modular.

The argument we give for this is analogous to that given for going from residue characteristic 3 to residue characteristic 2 in the proof of Theorem 3.2 except that the roles of 2 and 3 are reversed. Using Theorem 5.1 (2), construct a compatible system lift (ρ_λ) of $\bar\rho$ such that ρ_p is a minimal weight 2 lift. Consider $\bar\rho_3$. This has non-solvable image by Lemma 6.3, and if it is unramified at 2 we are done by applying Theorem 1.2 and Theorem 4.1. If $\bar\rho_3$ is ramified at 2, then $\bar\rho_3(I_2)$ is unipotent and thus $\bar\rho_3(D_2)$ is up to unramified twist of the form

$$\begin{pmatrix} \overline{\chi}_3 & * \\ 0 & 1 \end{pmatrix}.$$

Consider the two 3-adic characters χ', χ'^2 of I_2 of order 3, and using Theorem 5.1 (4), construct a compatible system lift (ρ'_λ) of $\bar\rho$ such that in particular $\rho'_3(I_2)$ has the form

$$\begin{pmatrix} \chi' & * \\ 0 & \chi'^2 \end{pmatrix}.$$

Note that the WD parameter of ρ'_3 at 2 is of the form $(\tau, 0)$ with τ irreducible. Consider $\bar\rho'_2$. We claim that $k(\bar\rho'_2) = 2$. If so we would be done by Theorem 1.2(ii) and Hypothesis (H), as we know by Lemma 6.3 that $\bar\rho'_2$ has non-solvable image, and by Theorem 5.1 (4) that ρ'_2 is potentially semistable of weight 2 at 2.

To prove the claim (we give this *ad hoc* argument as the reference [25] does not consider the case $p = 2$), note that if $k(\bar\rho'_2) = 4$, then it is très ramifiée and thus for a finite extension K of $\mathbb{Q}_2$ of odd ramification index, $\bar\rho'_2(G_K)$ cannot be finite flat. On the other hand we do know by Theorem 5.1(2) that we may take a finite extension K of $\mathbb{Q}_2$ of ramification index 3 (= order of χ'), such that $\bar\rho'_2(G_K)$ is finite flat which is plainly a contradiction thus proving the claim. (We can take K for instance to be the field cut out by χ' over the quadratic unramified extension of $\mathbb{Q}_2$.)

Having proved Serre's conjecture in residue characteristic 2 and (D_1), we deduce from this (D_r) for all integers $r > 1$. Thus we wish to show that a $\bar\rho$ of S-type in odd residue characteristic p, which is good-dihedral, and with $N(\bar\rho)$ not divisible by 2^{r+1}, is modular. As we have proved (D_1), we may assume that $\bar\rho(I_2)$ does not have, up to a twist, unipotent image. Using Theorem 5.1 (2), construct a compatible system lift (ρ_λ) of $\bar\rho$ such that ρ_p is a minimal weight 2 lift. Consider $\bar\rho_2$. This has non-solvable image by Lemma 6.3, and we know it is modular, and by Theorem 5.1 (2) that ρ_2 is potentially crystalline of weight 2 at 2. Thus we are done by applying Hypothesis (H).

□

10. Modularity of compatible systems

We formulate the following corollary of Serre's conjecture (Theorem 1.2 and 9.1 of this paper, and Theorem 0.1 and Corollary 0.2 of [19]). For the definition of compatible systems and their regularity, see Section 5. The

proof is similar to the arguments in Sections 4.7 and 4.8 of [26], but we also use the argument of [11].

Theorem 10.1. *(i) A (2-dimensional) regular compatible system that is irreducible and odd arises up to twist from a newform of weight* ≥ 2.

(ii) An (2-dimensional) irregular compatible system that is irreducible and odd arises up to twist from a newform of weight 1.

Proof. We only sketch the proof.

In both cases it is easy to see that $\bar{\rho}_\lambda$ is irreducible for almost all λ using the fact that the conductor of ρ_λ is bounded independently of λ and the Hodge-Tate weights of ρ_λ are fixed.

After twisting we may assume that the Hodge-Tate numbers (a, b) of the compatible system are such that $b = 0$ and $a \geq 0$.

In the case of (i), when $a > 0$, we see that Theorem 1.2 applies to $\bar{\rho}_\lambda$ for infinitely many λ and that these arise from a fixed newform $f \in S_k(\Gamma_1(N))$ for some fixed integers $k = a + 1, N$. This proves (i).

In the case of (ii), when $a = b = 0$, by a theorem of Sen and Fontaine for all but finitely many λ, ρ_λ is unramified at $\ell(\lambda)$, where $\ell(\lambda)$ is the residue characteristic of the residue field arising from λ. Then arguing as in [11], which uses the results of Gross and Coleman-Voloch, [9] and [3] (see also 3.4 of [7]), we conclude from Theorem 1.2, that $\bar{\rho}_\lambda$ for almost all λ arise from the space $S_1(\Gamma_1(N))$ of classical forms of weight 1 and level N with N independent of λ. This proves (ii). □

Part (ii) implies Artin's conjecture for odd irreducible 2-dimensional representations of $G_{\mathbb{Q}}$, but is not implied by it: thus we rederive by a different method Theorem A of [1]. Part (i) combined with Faltings' isogeny theorem yields modularity of abelian varieties of GL_2-type over $\mathbb{Q}$: see Theorem 4.4 of [21].

11. Acknowledgements

We thank Florian Herzig and Ravi Ramakrishna for their helpful comments on the manuscript, and especially David Savitt for his detailed comments that were extremely useful. We owe to Savitt the suggestion that we index the hypotheses (D_r) in Theorem 3.4.

References

[1] K. Buzzard, M. Dickinson, N. Shepherd-Barron and R. Taylor. On icosahedral Artin representations. Duke Math. J. 109 (2001), no. 2, 283–318.

[2] Kevin Buzzard. On level-lowering for mod 2 representations. Math. Res. Lett. 7 (2000), no. 1, 95–110.

[3] Robert Coleman and José Felipe Voloch Companion forms and Kodaira-Spencer theory. Invent. Math. 110 (1992), no. 2, 263–281.

[4] Henri Carayol. Sur les représentations galoisiennes modulo ℓ attachées aux formes modulaires. Duke Math. J. 59 (1989), no. 3, 785–801.

[5] Deligne, P. Les constantes des équations fonctionnelles des fonctions L. Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, 1972) : 501–597. Lecture Notes in Math., Vol. 349. Springer, Berlin 1973.
[6] Fred Diamond. An extension of Wiles' results. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 475–489. Springer, New York, 1997.
[7] Bas Edixhoven. The weight in Serre's conjectures on modular forms. *Invent. Math.*. 109 (1992), no. 3, 563–594.
[8] Jean-Marc Fontaine and Barry Mazur. Geometric Galois representations. In *Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993)*, Ser. Number Theory, I, pages 41–78. Internat. Press, Cambridge, MA, 1995.
[9] Benedict Gross. A tameness criterion for Galois representations associated to modular forms (mod p). Duke Math. J. 61 (1990), no. 2, 445–517.
[10] Bertram Huppert. Endliche Gruppen I. Springer-Verlag, 1967.
[11] Chandrashekhar Khare. Remarks on mod p forms of weight one. Internat. Math. Res. Notices 1997, no. 3, 127–133. (Corrigendum: IMRN 1999, no. 18, pg. 1029.)
[12] Chandrashekhar Khare and Jean-Pierre Wintenberger. On Serre's reciprocity conjecture for 2-dimensional mod p representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. preprint.
[13] Chandrashekhar Khare and Jean-Pierre Wintenberger. Serre's modularity conjecture (II). preprint.
[14] Chandrashekhar Khare. Serre's modularity conjecture : The level one case. *Duke Mathematical Journal*, 134(3):557–589, 2006.
[15] Chandrashekhar Khare. Serre's modularity conjecture: a survey of the level one case. to appear in proccedings of the LMS conference on L-functions and Galois representations (Durham 2004), eds. Buzzard, Burns, Nekovar.
[16] Hyunsuk Moon and Yuichiro Taguchi. Refinement of Tate's discriminant bound and non-existence theorems for mod p Galois representations. Doc. Math. 2003, Extra Vol.(Kazuya Kato's fiftieth birthday), 641–654 (electronic).
[17] Mark Kisin. Moduli of finite flat group schemes, and modularity. *preprint* (2004).
[18] Mark Kisin. Potentially semi-stable deformation rings. *preprint* (2006).
[19] Mark Kisin. Modularity of 2-adic Barsotti-Tate representations. *preprint*, 2007.
[20] *Périodes p-adiques*. Société Mathématique de France, Paris, 1994. Papers from the seminar held in Bures-sur-Yvette, 1988, Astérisque No. 223 (1994).
[21] Kenneth Ribet. Abelian varieties over $\mathbb{Q}$ and modular forms. Algebra and topology 1992 (Taejuon), 53–79, Korea Adv. Inst. Sci. Tech., Taejuon, 1992.
[22] David Rohrlich and Jerrold Tunnell. An elementary case of Serre's conjecture. Pacific J. of Math., Olga-Taussky-Todd Memorial issue, 1997, 299 –309.
[23] J. Barkley Rosser and Lowell Schoenfeld. Approximate formulas for some functions of prime numbers. Illinois J. Math. 6 (1962), 64–94.
[24] Takeshi Saito. Modular forms and p-adic Hodge theory. preprint.
[25] David Savitt. On a Conjecture of Conrad, Diamond, and Taylor. Duke Mathematical Journal 128 (2005), no. 1, 141-197.
[26] Jean-Pierre Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.
[27] Chistopher Skinner and Andrew Wiles. Residually reducible representations and modular forms. *Inst. Hautes Études Sci. Publ. Math.*, (89):5–126 (2000), 1999.
[28] Christopher Skinner and Andrew Wiles. Nearly ordinary deformations of irreducible residual representations. *Ann. Fac. Sci. Toulouse Math. (6)*, 10(1):185–215, 2001.
[29] Gabor Wiese. Dihedral Galois representations and Katz modular forms. Documenta Mathematica, Vol. 9 (2004), 123–133.
[30] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.
[31] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

E-mail address: shekhar@math.utah.edu

Department of Mathematics, 155 South 1400 East, Room 233, Salt Lake City, UT 84112-0090, U.S.A.

E-mail address: wintenb@math.u-strasbg.fr

Université Louis Pasteur, Département de Mathématique, 7, rue René Descartes, 67084, Strasbourg Cedex, France