

ON SERRE'S CONJECTURE FOR MOD ℓ GALOIS REPRESENTATIONS OVER TOTALLY REAL FIELDS

KEVIN BUZZARD, FRED DIAMOND, AND FRAZER JARVIS

1. INTRODUCTION

Serre conjectured in [23] that if ℓ is prime and

$$\rho : G_{\mathbf{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_{\ell})$$

is a continuous, odd, irreducible representation, then ρ is *modular* in the sense that it arises as the reduction of an ℓ -adic representation associated to a Hecke eigenform in the space $S_k(\Gamma_1(N))$ of cusp forms of some weight k and level N . He goes on to formulate a refined conjecture which predicts the minimal weight and level of such an eigenform subject to the constraints $k \geq 2$ and $\ell \nmid N$. Through the work of Ribet [22], Gross [17], Coleman-Voloch [7] and others (see [10]), the equivalence between the conjecture and its refinement is known for $\ell > 2$, and also when $\ell = 2$ in many cases (see [4]). More recently, important work of Khare ([20]), following work of Khare and Wintenberger ([21]) shows that the conjecture is true in the case where ρ is unramified outside ℓ .

Suppose now that K is a totally real field. Let \mathcal{O} denote its ring of integers and let S_K be the set of embeddings of K in \mathbf{R} . Suppose that $\vec{k} \in \mathbf{Z}^{S_K}$ with all $k_{\tau} \geq 1$ and of the same parity, and that \mathfrak{n} is a non-zero ideal of \mathcal{O} . The space of Hilbert modular cusp forms of weight \vec{k} and level \mathfrak{n} , denoted $S_{\vec{k}}(U_1(\mathfrak{n}))$, is a finite-dimensional complex vector space equipped with an action of commuting Hecke operators $T_{\mathfrak{m}}$, indexed by the non-zero ideals \mathfrak{m} of \mathcal{O} . Fix once and for all embeddings $\overline{\mathbf{Q}} \rightarrow \mathbf{C}$ and $\overline{\mathbf{Q}} \rightarrow \overline{\mathbf{Q}}_{\ell}$, and let $0 \neq f \in S_{\vec{k}}(U_1(\mathfrak{n}))$ be an eigenform for all the $T_{\mathfrak{m}}$. A construction completed by Taylor in [24] associates to f an ℓ -adic representation

$$\rho_f : G_K \rightarrow \mathrm{GL}_2(\overline{\mathbf{Q}}_{\ell})$$

such that if \mathfrak{p} is a prime of \mathcal{O} not dividing $\ell\mathfrak{n}$, then ρ_f is unramified at \mathfrak{p} and $\mathrm{tr}\rho_f(\mathrm{Frob}_{\mathfrak{p}})$ is the eigenvalue of $T_{\mathfrak{p}}$ on f . Fixing an identification of the residue field of $\overline{\mathbf{Q}}_{\ell}$ with $\overline{\mathbf{F}}_{\ell}$, we obtain a representation

$$\overline{\rho}_f : G_K \rightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_{\ell})$$

defined as the semisimplification of the reduction of ρ_f . It is natural to expect the following generalization of Serre's Conjecture to hold:

Conjecture 1.1. *Suppose that $\rho : G_K \rightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_{\ell})$ is continuous, irreducible and totally odd. Then ρ is isomorphic to $\overline{\rho}_f$ for some Hilbert modular eigenform f .*

The aim of this paper is to formulate a refined conjecture over K along the lines of Serre's refinement for the case $K = \mathbf{Q}$, at least in the case where the prime ℓ is unramified in K . The main difficulty is in specifying the weight, where

we encounter several subtleties not present in Serre’s original work. Note first of all that there is no obvious notion of a minimal weight. Moreover the possible weights and level structures at primes over ℓ are intertwined, and, contrary to the case $K = \mathbf{Q}$, one does not always expect a representation as in Conjecture 1.1 to arise from a classical Hilbert modular form of level prime to ℓ . Indeed, the mod ℓ representation attached to such a form has determinant equal to the product of a finite order character unramified at ℓ and some power of the mod ℓ cyclotomic character, and it is not hard to construct a mod ℓ Galois representation whose determinant is not of this form. To deal with these issues, we introduce the notion of a *Serre weight*, namely an irreducible $\overline{\mathbf{F}}_\ell$ -representation σ of $\mathrm{GL}_2(\mathcal{O}/\ell)$, and define what it means for ρ to be modular of weight σ . Such a notion of weight is implicit in work of Khare [19] for classical modular forms and Ash and others [2], [1] in the context of GL_n over \mathbf{Q} . Our aim is to describe all possible Serre weights and level structures of forms giving rise to a representation ρ .

Our weight conjecture (Conjecture 3.12 below) then takes the form of a recipe for the set of weights σ for which ρ is modular. This recipe is given in terms of the local behavior of ρ at primes over ℓ . We show (Theorem 3.15) that Conjecture 3.12 can be deduced from known results on Serre’s Conjecture in the case $K = \mathbf{Q}$. It is supported for other fields by numerical evidence collected by one of the authors, Dembélé and Roberts [9] in the case $K = \mathbf{Q}(\sqrt{5})$, $\ell = 3$, and by theoretical evidence provided by results of another of us [18] on level lowering at ℓ and of Gee [16] on companion forms.

Loosely speaking, Conjecture 1.1 can be thought of in the context of a mod ℓ “Langlands’ philosophy”, with Conjecture 3.12 predicting a local-global compatibility at primes over ℓ . An interesting feature of the recipe for the weights is that if ℓ is inert in K and $\rho|_{G_{K_\ell}}$ is semisimple, then the set of weights that we associate to ρ are the Jordan–Hölder factors of the reduction of an *irreducible* irreducible $\overline{\mathbf{Q}}_\ell$ -representation of $\mathrm{GL}_2(\mathcal{O}/\ell)$. This is proved in [11], where it is further shown that this association establishes a natural correspondence between 2-dimensional Galois representations of a local field *in its residue characteristic* and representations of GL_2 of its residue field *in characteristic zero*.

This paper is structured as follows. In §2 we introduce the notion of a Serre weight, explain what it means for ρ to be modular of a given Serre weight, and relate this notion to the existence of Hilbert modular forms f such that $\rho \sim \bar{\rho}_f$. In §3 we formulate Conjecture 3.12 giving a recipe for the set of Serre weights for which ρ is modular. Finally, in §4 we use this recipe to formulate a refined conjecture over K (Conjecture 4.1) in the spirit of [12] and [19] which predicts all possible collections of local behavior of automorphic representations corresponding to forms of weight $(2, \dots, 2)$ giving rise to ρ .

Acknowledgements: NSF, RLT, Florian Herzig, Michael Schein

2. SERRE WEIGHTS

Suppose K is a totally real field and let \mathcal{O} denote its ring of integers. Let ℓ be a prime unramified in K and consider

$$G = \mathrm{GL}_2(\mathcal{O}/\ell\mathcal{O}) \cong \prod_{\mathfrak{p}|\ell} \mathrm{GL}_2(\mathcal{O}/\mathfrak{p}).$$

A *Serre weight* is an isomorphism class of irreducible $\overline{\mathbf{F}}_\ell$ -representations of G . These can be described explicitly as follows. For each prime \mathfrak{p} of K dividing ℓ , set $k_{\mathfrak{p}} = \mathcal{O}/\mathfrak{p}$, $f_{\mathfrak{p}} = [k_{\mathfrak{p}} : \mathbf{F}_\ell]$ and let $S_{\mathfrak{p}}$ be the set of embeddings $\tau : k_{\mathfrak{p}} \rightarrow \overline{\mathbf{F}}_\ell$. Then every irreducible $\overline{\mathbf{F}}_\ell$ -representation of $\mathrm{GL}_2(k_{\mathfrak{p}})$ is equivalent to one of the form

$$V_{\vec{a}, \vec{b}} = \bigotimes_{\tau \in S_{\mathfrak{p}}} (\det^{a_\tau} \otimes_{k_{\mathfrak{p}}} \mathrm{Sym}^{b_\tau - 1} k_{\mathfrak{p}}^2) \otimes_\tau \overline{\mathbf{F}}_\ell,$$

where $a_\tau, b_\tau \in \mathbf{Z}$ and $1 \leq b_\tau \leq \ell$ for each $\tau \in S_{\mathfrak{p}}$. Moreover we can assume that $0 \leq a_\tau \leq \ell - 1$ for each $\tau \in S_{\mathfrak{p}}$ and that $a_\tau < \ell - 1$ for some ℓ , in which case the resulting $(\ell^{f_{\mathfrak{p}}} - 1)\ell^{f_{\mathfrak{p}}}$ representations $V_{\vec{a}, \vec{b}}$ are also inequivalent. The irreducible representations of G are thus of the form $V = \otimes_{\{\mathfrak{p}|\ell\}} V_{\mathfrak{p}}$, where the tensor product is over $\overline{\mathbf{F}}_\ell$ and each $V_{\mathfrak{p}}$ is of the form $V_{\vec{a}, \vec{b}}$ for (\vec{a}, \vec{b}) as above.

Fix once and for all $\tau \in S_K$. Suppose that D is a quaternion algebra over K split at τ and at no other infinite places. Fix an isomorphism $D \otimes_{K, \tau} \mathbf{R} = M_2(\mathbf{R})$; this induces an isomorphism of $(D \otimes_\tau \mathbf{R})^\times$ with $\mathrm{GL}_2(\mathbf{R})$, which acts on $\mathfrak{H}^\pm := \mathbf{C} \setminus \mathbf{R}$ in the usual way. Consider K as a subfield of \mathbf{R} (and hence of \mathbf{C}) via the embedding τ . If \mathbf{A}_K^f denotes the finite adeles of K and U is an open compact subgroup of $(D \otimes_K \mathbf{A}_K^f)^\times$ then there is a Shimura curve Y_U over K , a smooth algebraic curve whose complex points (via $\tau : K \rightarrow \mathbf{C}$) are naturally identified with

$$D^\times \setminus \left((D \otimes_K \mathbf{A}_K^f)^\times \times \mathfrak{H}^\pm \right) / U$$

and such that Y_U is a canonical model for this space, in the sense of Deligne. A note for worriers: there is more than one convention for these canonical models. To fix ideas, we shall follow the conventions of Carayol in [5] and in particular our ‘‘Hodge structure’’ h will be that of section 0.1 of [5]. This corresponds to the choice $\epsilon = -1$ in the notation of [8]. See Section 3.3 of [8] for a discussion of the (few) differences between this choice and the other natural choice.

If U' is a normal compact open subgroup of U , then the natural right action of U/U' on $Y_{U'}$ is defined over K . If $K = \mathbf{Q}$ and D is split, we let X_U denote the standard compactification of the modular curve Y_U ; otherwise we simply set $X_U = Y_U$. Then X_U is a smooth projective algebraic curve over K . Note that X_U , considered as a scheme over K , will be connected (see section 1.3 of [5]) but not in general geometrically connected. Note also that, with notation as above, the natural action of U/U' on $Y_{U'}$ extends to an action on $X_{U'}$.

If U is a compact open subgroup of $(D \otimes_K \mathbf{A}_K^f)^\times$ as above, then let $\mathrm{Pic}^0(X_U)$ denote the identity component of the relative Picard scheme of $X_U \rightarrow \mathrm{Spec}(K)$. If K_U denotes the global functions on X_U then K_U is a finite abelian extension of K , the curve X_U is geometrically connected when regarded as a scheme over $\mathrm{Spec}(K_U)$, and $\mathrm{Pic}^0(X_U)$ is canonically isomorphic to the restriction of scalars of the Jacobian of X_U/K_U . In particular, $\mathrm{Pic}^0(X_U)$ is an abelian variety over K .

If U again is as above, and if there is an isomorphism $D \otimes_{\mathbf{Q}} \mathbf{Q}_\ell \cong M_2(K \otimes \mathbf{Q}_\ell)$ such that U contains the pre-image of $\mathrm{GL}_2(\mathcal{O} \otimes \mathbf{Z}_\ell)$, then we say that U has *level prime to ℓ* . In this case, the natural map $U \rightarrow \mathrm{GL}_2(\mathcal{O}/\ell\mathcal{O}) = G$ is a surjection. Let U' denote its kernel. Then $U/U' = G$ acts naturally on the right on X_U and hence naturally on the left on $\mathrm{Pic}^0(X_U)$ and $\mathrm{Pic}^0(X_U)[\ell]$.

Definition 2.1. *Suppose that $\rho : G_K \rightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ is a continuous, irreducible, totally odd representation and V is a Serre weight. Then ρ is modular of weight*

V if there is a quaternion algebra D over K split at the primes above ℓ , at τ and no other infinite places of K , an open compact subgroup U of $(D \otimes_K \mathbf{A}_K^f)^\times$ of level prime to ℓ , such that (with notation as above) ρ is a sub- $\overline{\mathbf{F}}_\ell G_K$ -module of $(\text{Pic}^0(X_{U'})[\ell] \otimes V)^G$, where G acts diagonally on the tensor product, and G_K acts trivially on V .

We now relate this notion of modularity to the existence of Hilbert modular forms giving rise to ρ . First recall some background on Hilbert modular forms and Jacquet-Langlands...

Note that our chosen embeddings $\overline{\mathbf{Q}} \rightarrow \mathbf{C}$ and $\overline{\mathbf{Q}} \rightarrow \overline{\mathbf{Q}}_\ell$ and identification of the residue field of $\overline{\mathbf{Z}}_\ell$ with $\overline{\mathbf{F}}_\ell$ allow us to identify S_K with $\cup_{\mathfrak{p}|\ell} S_{\mathfrak{p}}$.

Proposition 2.2. *Suppose that $\vec{k} \in \mathbf{Z}^{S_K}$ with each $k_\tau \geq 2$ and of the same parity. Let $w = \max_{\tau \in S_K} \{k_\tau - 2\}$. Then $\rho \sim \bar{\rho}_f$ for some Hilbert modular eigenform of weight \vec{k} and level prime to ℓ if and only if ρ is modular of weight V for some Jordan-Holder constituent V of*

$$\bigotimes_{\mathfrak{p}|\ell} \bigotimes_{\tau \in S_{\mathfrak{p}}} \det^{-(k_\tau+w)/2} \text{Sym}^{k_\tau-2} k_{\mathfrak{p}}^2 \otimes_{\tau} \overline{\mathbf{F}}_\ell.$$

Proof. Sketch: Suppose ρ modular of weight V . For sufficiently small U define a lisse sheaf \mathcal{F}_V on X_U , a Jordan-Hölder constituent of $\mathcal{F}_{\vec{k}}/\ell\mathcal{F}_{\vec{k}}$ where $\mathcal{F}_{\vec{k}}$ is the ℓ -adic sheaf used by Carayol [6]. Check that the natural Galois/Hecke-equivariant maps

$$\begin{aligned} H_{\text{et}}^1(X_{U,\overline{K}}, \mathcal{F}_V) &\rightarrow (\text{Pic}^0(X_{U'})[\ell] \otimes V)^G \\ H_{\text{et}}^1(X_{U,\overline{K}}, \mathcal{F}_{\vec{k}})/\ell &\rightarrow H_{\text{et}}^1(X_{U,\overline{K}}, \mathcal{F}_{\vec{k}}/\ell) \end{aligned}$$

have Eisenstein kernel and cokernel as do obstructions to devissage. Let \mathfrak{m} be the usual maximal ideal in a Hecke algebra generated by good operators. Deduce that \mathfrak{m} is in the support of $H_{\text{et}}^1(X_{U,\overline{K}}, \mathcal{F}_{\vec{k}})$ and use Jacquet-Langlands to conclude that ρ is modular of weight \vec{k} . The argument works in reverse except that if $[K : \mathbf{Q}]$ is even, you have to combine Jacquet-Langlands with Taylor's level-raising result in [24] to switch to a quaternion algebra ramified at a finite place. \square

We can furthermore predict the local behavior at primes over ℓ of the automorphic representations of weight \vec{k} giving rise to ρ . Recall background on types...

Proposition 2.3. *Suppose that $\vec{k} \in \mathbf{Z}^{S_K}$ with each $k_\tau \geq 2$ and of the same parity. Let $w = \max_{\tau \in S_K} \{k_\tau - 2\}$. For each $\mathfrak{p}|\ell$, suppose that $\tau_{\mathfrak{p}} : U_{\mathfrak{p}} \rightarrow \text{Aut}_{\overline{\mathbf{Q}}_\ell} T_{\mathfrak{p}}$ is a type and let $\overline{T}_{\mathfrak{p}}$ be the semisimplification of the reduction of $\text{Ind}_{U_{\mathfrak{p}}}^{\text{GL}_2(K_{\mathfrak{p}})} \widehat{T}_{\mathfrak{p}}$, viewed as an $\overline{\mathbf{F}}_\ell[\text{GL}_2(k_{\mathfrak{p}})]$ -module. Then the following are equivalent:*

- $\rho \sim \bar{\rho}_\pi$ for some cuspidal holomorphic weight \vec{k} automorphic representations π of $\text{GL}_2(\mathbf{A}_K)$ such that $\pi_{\mathfrak{p}}$ has type $\tau_{\mathfrak{p}}$ for each $\mathfrak{p}|\ell$.
- ρ is modular of weight V for some Jordan-Holder constituent V of

$$\bigotimes_{\mathfrak{p}|\ell} \left(\overline{T}_{\mathfrak{p}} \otimes \bigotimes_{\tau \in S_{\mathfrak{p}}} \det^{-(k_\tau+w)/2} \text{Sym}^{k_\tau-2} k_{\mathfrak{p}}^2 \otimes_{\tau} \overline{\mathbf{F}}_\ell \right).$$

Proof. Essentially the same as preceding proposition, but need the following refinement of Taylor's level-raising result. \square

Lemma 2.4. *Suppose that $[K : \mathbf{Q}]$ is even and π is a cuspidal automorphic representation, holomorphic of weight \vec{k} . Then there is a prime \mathfrak{q} of K not dividing ℓ and cuspidal automorphic representation π' , holomorphic of weight \vec{k} , such that*

- $\bar{\rho}_\pi \sim \bar{\rho}_{\pi'}$;
- $\pi_{\mathfrak{q}}$ is an unramified special representation;
- $\pi_{\mathfrak{p}}$ is of the same type as $\pi'_{\mathfrak{p}}$ for each $\mathfrak{p}|\ell$.

Recall that for $K = \mathbf{Q}$, every modular ρ arises from a form of some level prime to ℓ and weight $k \geq 2$. Moreover, after twisting ρ , one may take the weight k satisfying $2 \leq k \leq \ell + 1$ (see [13]). This is false for larger K , at least if $[K : \mathbf{Q}]$ is even and ℓ is odd. (See [9] for examples with $K = \mathbf{Q}(\sqrt{5})$ and $\ell = 3$.) On the other hand, it is still the case that every modular ρ arises from a form of weight $(2, \dots, 2)$ and some level not necessarily prime to ℓ . Moreover, after twisting ρ , we can assume the form has level dividing $\mathfrak{n}\ell$ for some \mathfrak{n} prime to ℓ .

Corollary 2.5. *The following are equivalent:*

- (1) $\rho \sim \bar{\rho}_f$ for some Hilbert modular eigenform f ;
- (2) $\rho \sim \bar{\rho}_f$ for some Hilbert modular eigenform f of weight $(2, \dots, 2)$;
- (3) $\chi\rho \sim \bar{\rho}_f$ for some character χ and Hilbert modular eigenform f of weight $(2, \dots, 2)$ and level dividing $\mathfrak{n}\ell$ with \mathfrak{n} prime to ℓ .
- (4) ρ is modular of weight V for some Serre weight V .

Proof. Sketch: (3) \Rightarrow (2) \Rightarrow (1) is clear.

(1) \Rightarrow (4) clear from Proposition (and multiplication by Eisenstein series in the case of partial weight 1).

(4) \Rightarrow (3): Check that every $V_{\mathfrak{p}}$ is a Jordan-Hölder constituent of a tamely ramified principal series or special type (eg formulas in [11]). Proposition then shows ρ is modular of that type. Twist both sides to get conductor dividing ℓ . (Note that \mathfrak{n} might get bigger, unlike the $K = \mathbf{Q}$ case.) \square

For $\tau \in S_{\mathfrak{p}}$, we denote by ω_τ the fundamental character of $I_{K_{\mathfrak{p}}}$ defined by composing τ with the homomorphism $I_{K_{\mathfrak{p}}} \rightarrow k_{\mathfrak{p}}^\times$ gotten from local class field theory (with the convention that uniformizers correspond to geometric Frobenius elements). We then have the following compatibility among determinants, central characters and twists.

Corollary 2.6. (1) *If ρ is modular of weight V and V has central character $\otimes_{\mathfrak{p}|\ell} \prod_{\tau \in S_{\mathfrak{p}}} \tau^{c_\tau}$, then*

$$\det \rho|_{I_{K_{\mathfrak{p}}}} = \prod_{\tau \in S_{\mathfrak{p}}} \omega_\tau^{c_\tau+1}$$

for each $\mathfrak{p}|\ell$.

(2) *Let $\chi : G_K \rightarrow \bar{\mathbf{F}}_\ell^\times$ be such that $\chi|_{I_{K_{\mathfrak{p}}}} = \prod_{\tau \in S_{\mathfrak{p}}} \omega_\tau^{c_\tau}$ for each $\mathfrak{p}|\ell$. Then ρ is modular of weight V if and only if $\chi\rho$ is modular of weight $V \otimes V_\chi$, where*

$$V_\chi = \bigotimes_{\mathfrak{p}|\ell} \bigotimes_{\tau \in S_{\mathfrak{p}}} \det^{c_\tau} k_{\mathfrak{p}}^2 \otimes_\tau \bar{\mathbf{F}}_\ell.$$

3. THE WEIGHT CONJECTURE

Suppose that $\rho : G_K \rightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ is continuous, irreducible and totally odd. The aim of this section is to provide a conjectural recipe for the set of V such that ρ is modular of weight V .

For each prime \mathfrak{p} of K dividing ℓ , we will define a set of representations $W_{\mathfrak{p}}(\rho)$ of $\mathrm{GL}_2(k_{\mathfrak{p}})$ depending only on $\rho|_{I_{K_{\mathfrak{p}}}}$, and then define the conjectural weight set $W(\rho)$ as the set of Serre weights of the form $\otimes_{\overline{\mathbf{F}}_\ell} V_{\mathfrak{p}}$ with $V_{\mathfrak{p}} \in W_{\mathfrak{p}}(\rho)$.

We need some more notation before defining $W_{\mathfrak{p}}(\rho)$. With our prime \mathfrak{p} dividing ℓ fixed for now, we write simply k , f and S for $k_{\mathfrak{p}}$, $f_{\mathfrak{p}}$ and $S_{\mathfrak{p}}$. Fix an embedding $\overline{K} \rightarrow \overline{K}_{\mathfrak{p}}$ and identify $D = G_{K_{\mathfrak{p}}}$ and $I = I_{K_{\mathfrak{p}}}$ with subgroups of G_K . Let $K'_{\mathfrak{p}}$ the unramified quadratic extension of $K_{\mathfrak{p}}$ in $\overline{K}_{\mathfrak{p}}$ and let k' denote its residue field. We let S' denote the set of embeddings $k' \rightarrow \overline{\mathbf{F}}_\ell$, let $D' = G_{K'_{\mathfrak{p}}}$ and define a map $\pi : S' \rightarrow S$ by $\tau' \mapsto \tau'|_k$.

Suppose that $L \subset \overline{K}_{\mathfrak{p}}$ is a finite unramified extension of $K_{\mathfrak{p}}$ and σ is an embedding of its residue field $\mathcal{O}_L/\ell\mathcal{O}_L$ in $\overline{\mathbf{F}}_\ell^\times$. We denote by ω_σ the fundamental character of $I = I_L$ defined by composing σ with the homomorphism $I_L \rightarrow (\mathcal{O}_L/\ell\mathcal{O}_L)^\times$ gotten from local class field theory.

In defining $W_{\mathfrak{p}}(\rho)$, we treat separately the cases where $\rho|_D$ is irreducible and where it is reducible. If $\rho|_D$ is irreducible, we define $W_{\mathfrak{p}}(\rho)$ by the following rule:

$$(1) \quad V_{\vec{a}, \vec{b}} \in W_{\mathfrak{p}}(\rho) \iff \rho|_I \sim \prod_{\tau \in S} \omega_\tau^{a_\tau} \begin{pmatrix} \prod_{\tau' \in J} \omega_{\tau'}^{b_{\pi(\tau')}} & 0 \\ 0 & \prod_{\tau' \notin J} \omega_{\tau'}^{b_{\pi(\tau')}} \end{pmatrix}$$

for some $J \subset S'$ such that $\pi : J \xrightarrow{\sim} S$.

Since ρ is irreducible, there is a character $\xi : D' \rightarrow \overline{\mathbf{F}}_\ell^\times$ such that $\rho|_D \sim \mathrm{Ind}_{D'}^D \xi$. We define

$$W'(\xi) = \{ (V_{\vec{a}, \vec{b}}, J) \mid J \subset S', \pi : J \xrightarrow{\sim} S, \xi|_I = \prod_{\tau \in I} \omega_\tau^{a_\tau} \prod_{\tau' \in J} \omega_{\tau'}^{b_{\pi(\tau')}} \}.$$

Thus $W_{\mathfrak{p}}(\rho) = \{ V \mid (V, J) \in W'(\xi) \text{ for some } J \}$. (Note that replacing ξ by its conjugate under D/D' replaces J by its complement.) We shall see that the projection maps $W'(\xi) \rightarrow W_{\mathfrak{p}}(\rho)$ and $W'(\xi) \rightarrow \{ J \subset S' \mid \pi : J \xrightarrow{\sim} S \}$ are typically bijections, so that $|W_{\mathfrak{p}}(\rho)| = 2^f$.

We now choose an element of S' which we denote τ'_0 , and then let $\tau'_i = \tau'_0 \circ \mathrm{Frob}_\ell^i$ and $\tau_i = \pi(\tau'_i)$. Note that $S = \{ \tau_i \mid i \in \mathbf{Z}/f\mathbf{Z} \}$ and $S' = \{ \tau'_i \mid i \in \mathbf{Z}/2f\mathbf{Z} \}$. Letting $\omega = \omega_{\tau_0}$ and $\omega' = \omega_{\tau'_0}$, we have $\omega_{\tau_i} = \omega^{\ell^i}$, $\omega_{\tau'_i} = (\omega')^{\ell^i}$ and $\omega = (\omega')^{\ell^f + 1}$. Note that $\xi|_I = (\omega')^n$ for some $n \bmod \ell^{2f} - 1$, and since $\rho|_D$ is irreducible, n is not divisible by $\ell^f + 1$.

For $B \subset \{0, \dots, f-1\}$, let $J_B = \{ \tau'_i \mid i \in B \} \cup \{ \tau'_{f+i} \mid i \notin B \}$. If $a \in \mathbf{Z}/(\ell^f - 1)\mathbf{Z}$, $\vec{b} = (b_0, \dots, b_{f-1})$ with each $b_i \in \{1, \dots, \ell\}$ and $B \subset \{0, \dots, f-1\}$, let

$$n'_{\vec{a}, \vec{b}, B} = a(\ell^f + 1) + \sum_{i \in B} b_i \ell^i + \sum_{i \notin B} b_i \ell^{f+i} \bmod \ell^{2f} - 1.$$

Then $W'(\xi)$ is in bijection with the set of triples (a, \vec{b}, B) as above with $n \equiv n'_{\vec{a}, \vec{b}, B} \bmod \ell^{2f} - 1$. Now note for each $B \subset \{0, \dots, f-1\}$, there is a unique such

triple for each solution of

$$n \equiv \sum_{i \in B} b_i \ell^i - \sum_{i \notin B} b_i \ell^i \pmod{\ell^f + 1}.$$

with $b_0, \dots, b_{f-1} \in \{1, \dots, \ell\}$. But the values of $b_i \ell^i - \sum_{i \notin B} b_i \ell^i$ are the ℓ^f consecutive integers from $n'_B - \ell^f$ to $n'_B - 1$ where

$$n'_B = \sum_{i \in B} \ell^{i+1} - \sum_{i \notin B} \ell^i + 1,$$

so there is a solution as long as $n \not\equiv n'_B \pmod{\ell^f + 1}$ and this solution is unique. We have thus shown that $W'(\xi)$ is in bijection with the set of B such $n \not\equiv n'_B \pmod{\ell^f + 1}$; moreover the projection $W'(\xi) \rightarrow \{J \subset S' \mid \pi : J \xrightarrow{\sim} S\}$ is injective.

Note that if f is odd and B is either $\{0, 2, \dots, f-1\}$ or $B = \{1, 3, \dots, f-2\}$, then $n'_B \equiv 0 \pmod{\ell^f + 1}$. To see that the converse holds as well, observe that

$$-(\ell^f + 1) < -\ell \frac{\ell^{f-1} - 1}{\ell - 1} \leq n'_B \leq \frac{\ell^{f+1} - 1}{\ell - 1} < 2(\ell^f + 1).$$

Thus if $n'_B \equiv 0 \pmod{\ell^f + 1}$, then $n'_B = 0$ or $\ell^f + 1$. If $n'_B = 0$, then solving

$$\sum_{i \in B} \ell^{i+1} - \sum_{i \notin B} \ell^i + 1 \equiv 0 \pmod{\ell^r}$$

by induction on r , we find that f is odd and $B = \{1, 3, \dots, f-2\}$. Similarly if $n'_B = \ell^f + 1$, then f is odd and $B = \{0, 2, \dots, f-1\}$.

We now show that if f is even, then the 2^f values of $n'_B \pmod{\ell^f + 1}$ are distinct. First note that

$$n'_B \equiv -1 + (\ell + 1) \sum_{i \in B^*} (-1)^i \ell^i \pmod{\ell^f + 1},$$

where $B^* = (\{0, 2, \dots, f-2\} \cap B) \cup (\{1, 3, \dots, f-1\} \setminus B)$. Thus $n'_{B_1} \equiv n'_{B_2} \pmod{\ell^f + 1}$ if and only if

$$\sum_{i \in B_1^*} (-1)^i \ell^i \equiv \sum_{i \in B_2^*} (-1)^i \ell^i \pmod{(\ell^f + 1)/d},$$

where $d = \gcd(\ell + 1, \ell^f + 1) \leq \ell - 1$. But these two sums differ by at most $(\ell^f - 1)/(\ell - 1) < (\ell^f + 1)/d$, so the above congruence holds if and only if equality holds, in which case $B_1^* = B_2^*$, so $B_1 = B_2$.

Next we show that if f and ℓ are odd, then the $2^f - 2$ non-zero values of $n'_B \pmod{\ell^f + 1}$ are distinct. In this case we have

$$n'_B \equiv (\ell + 1) \sum_{i \in B^*} (-1)^i \ell^i \pmod{\ell^f + 1},$$

where $B^* = (\{0, 2, \dots, f-1\} \cap B) \cup (\{1, 3, \dots, f-2\} \setminus B)$. Thus $n'_{B_1} \equiv n'_{B_2} \pmod{\ell^f + 1}$ if and only if

$$\sum_{i \in B_1^*} (-1)^i \ell^i \equiv \sum_{i \in B_2^*} (-1)^i \ell^i \pmod{(\ell^f + 1)/(\ell + 1)}.$$

But these two sums differ by at most $(\ell^f - 1)/(\ell - 1) < 2(\ell^f + 1)/(\ell + 1)$, so if the above congruence holds then either equality holds, in which case $B_1 = B_2$, or

$$\sum_{i \in B_2^*} (-1)^i \ell^i = \sum_{i \in B_1^*} (-1)^i \ell^i + \sum_{i=0}^{f-1} (-1)^i \ell^i,$$

exchanging B_1 and B_2 if necessary. Solving mod ℓ^r inductively on r , we see that the only possibility is that $B_1^* = \emptyset$ and $B_2^* = \{0, 1, \dots, f-1\}$, but these are precisely the cases where $n'_B \equiv 0 \pmod{\ell^f + 1}$.

Finally suppose that f is odd and $\ell = 2$. In this case we have

$$n'_B \equiv 3 \sum_{i \in B^*} (-1)^i 2^i \pmod{2^f + 1},$$

where $B^* = (\{0, 2, \dots, f-1\} \cap B) \cup (\{1, 3, \dots, f-2\} \setminus B)$. In particular $n'_B \equiv 0 \pmod{3}$. Moreover we have the inequality $|n'_{B_1} - n'_{B_2}| < 3(2^f + 1)$, showing that each congruence class mod $2^f + 1$ arises as n_B for at most 3 values of B . It follows that each of the $(2^f - 2)/3$ non-zero multiples of 3 mod $2^f + 1$ arises as n'_B for exactly 3 values of B .

We have thus proved the following propositions:

Proposition 3.1. *Suppose that ℓ is odd. If f is even, then the congruence classes mod $\ell^f + 1$ of the form*

$$-1 + (\ell + 1) \sum_{i \in B^*} (-1)^i \ell^i$$

are distinct and non-zero as B^ runs through all subsets of $\{0, 1, \dots, f-1\}$. If f is odd, then the congruence classes mod $\ell^f + 1$ of the form*

$$(\ell + 1) \sum_{i \in B^*} (-1)^i \ell^i$$

are distinct and non-zero as B^ runs through all non-empty proper subsets of $\{0, 1, \dots, f-1\}$. Letting A denote the set of such classes in each case, we have*

$$|W'(\xi)| = \begin{cases} 2^f, & \text{if } n \notin A, \\ 2^f - 1, & \text{if } n \in A. \end{cases}$$

Proposition 3.2. *Suppose that $\ell = 2$. Then*

$$|W'(\xi)| = \begin{cases} 2^f - 1, & \text{if } f \text{ is even,} \\ 2^f, & \text{if } f \text{ is odd and } 3 \nmid n, \\ 2^f - 3, & \text{if } f \text{ is odd and } 3|n. \end{cases}$$

Multiple B can occur with the same (a, \vec{b}) ; for example if $f = 3$ and $n = 1$, then $(0, (1, \ell, 1), \{0, 1\})$ and $(0, (1, \ell, 1), \{0, 2\})$ are both in $W'(\xi)$, so the map $W'(\xi) \rightarrow W_{\mathfrak{p}}(\rho)$ is not injective. (In this case in fact, $|W'(\xi)| = 8$, but $|W_{\mathfrak{p}}(\rho)| = 6$.)

Proposition 3.3. *The map $W'(\xi) \rightarrow W_{\mathfrak{p}}(\rho)$ fails to be injective if and only if $\ell^r n \equiv m \pmod{\ell^f + 1}$ for some integers r, m with $|m| \leq \ell(\ell^{f-2} - 1)/(\ell - 1)$.*

Proof. Suppose first that $W'(\xi) \rightarrow W_{\mathfrak{p}}(\rho)$ is not injective. This means that for some a, \vec{b} and $B_1 \neq B_2$, we have

$$(2) \quad n \equiv n'_{a, \vec{b}, B_1} \equiv n'_{a, \vec{b}, B_2} \pmod{\ell^{2f} - 1}.$$

First we note that B_2 cannot be the complement $\overline{B_1}$ of B_1 in $\{0, \dots, f-1\}$ since

$$n'_{a, \vec{b}, \overline{B_1}} \equiv \ell^f n'_{a, \vec{b}, B_1} \not\equiv n'_{a, \vec{b}, B_1} \pmod{\ell^{2f} - 1}$$

would imply $n \equiv 0 \pmod{\ell^f + 1}$, contradicting the irreducibility of $\rho|_D$. We thus have $J_2 \neq S' \setminus J_1$, where $J_1 = J_{B_1}$ and $J_2 = J_{B_2}$. We may therefore choose $t \in \mathbf{Z}/2f\mathbf{Z}$

so that $\tau'_{t-1} \in J_1 \setminus J_2$ and $\tau'_t \in J_1 \cap J_2$. We then have

$$\ell^{f-t}n \equiv n'_{a', \vec{b}', B'_1} \equiv n'_{a', \vec{b}', B'_2} \pmod{\ell^{2f} - 1},$$

where $a' \equiv \ell^{-t}a \pmod{\ell^f - 1}$, $b'_i = b_{i+t \bmod f}$ for $i \in \{0, \dots, f-1\}$ and B'_ν is such that $J_{B'_\nu} = J_\nu \circ \text{Frob}_\ell^{f-t}$ for $\nu = 1, 2$. Replacing n with $\ell^{f-t}n$, we may thus assume that $\tau'_{f-1} \in J_1 \setminus J_2$ and $\tau'_f \in J_1 \cap J_2$, or equivalently, $f-1 \in B_1 \setminus B_2$ and $0 \notin B_1 \cup B_2$.

Returning to the congruence (2), we have

$$\sum_{i \in B_1} b_i \ell^i + \ell^f \sum_{i \notin B_1} b_i \ell^i \equiv \sum_{i \in B_2} b_i \ell^i + \ell^f \sum_{i \notin B_2} b_i \ell^i \pmod{\ell^{2f} - 1},$$

or equivalently,

$$\sum_{i \in B_1 \setminus B_2} b_i \ell^i \equiv \sum_{i \in B_2 \setminus B_1} b_i \ell^i \pmod{\ell^f + 1}.$$

Since each sum is less than $2(\ell^f + 1)$, they must either be equal or differ by $\ell^f + 1$, and since $0 \notin B_1 \cup B_2$, each sum is divisible by ℓ , so in fact equality holds. Since $f-1 \in B_1 \setminus B_2$, we have

$$b_{f-1} \ell^{f-1} \leq \sum_{i \in B_1 \setminus B_2} b_i \ell^i = \sum_{i \in B_2 \setminus B_1} b_i \ell^i < \sum_{i=2}^{f-1} \ell^i < 2\ell^{f-1},$$

so $b_{f-1} = 1$. Moreover if $b_{f-2}, b_{f-3}, \dots, b_s$ are all less than ℓ , then we must have $b_{f-2} = b_{f-3} = \dots = b_s = \ell - 1$ and $f-2, f-3, \dots, s-1 \in B_2 \setminus B_1$, for if either fails, we find that

$$\sum_{i \in B_2 \setminus B_1} b_i \ell^i \leq (\ell - 1) \sum_{i=s}^{f-2} \ell^i + \sum_{i=2}^{s-1} \ell^i < \ell^{f-1}.$$

Since $0 \notin B_2 \setminus B_1$, we conclude that for some s with $0 < s < f-1$, we have $(b_s, b_{s+1}, \dots, b_{f-1}) = (\ell, \ell-1, \dots, \ell-1, 1)$ and $s, s+1, \dots, f-2 \in B_2 \setminus B_1$. It follows that

$$n \equiv \sum_{i \in B_1} b_i \ell^i - \sum_{i \notin B_1} b_i \ell^i \equiv \sum_{i \in B_1, i < s} b_i \ell^i - \sum_{i \notin B_1, i < s} b_i \ell^i \pmod{\ell^f + 1},$$

and this last difference has absolute value at most $\ell(\ell^{f-2} - 1)/(\ell - 1)$.

Conversely suppose that $\ell^r n \equiv m \pmod{\ell^f + 1}$ for some i, m with $|m| \leq \ell(\ell^{f-2} - 1)/(\ell - 1)$. Replacing r by $r + f$ if necessary, we may assume $m > 0$ and then

$$\frac{\ell^s - 1}{\ell - 1} \leq m \leq \ell \cdot \frac{\ell^s - 1}{\ell - 1}$$

for some s with $0 < s < f-1$. We can then write

$$\ell^r n \equiv a(\ell^f + 1) + \sum_{i=0}^{s-1} b_i \ell^i \pmod{\ell^{2f} - 1}$$

for some $a \in \mathbf{Z}/(\ell^f - 1)\mathbf{Z}$ and $b_0, b_1, \dots, b_{s-1} \in \{1, \dots, \ell\}$. We then have

$$\ell^r n \equiv n_{a, \vec{b}, B_1} \equiv n_{a, \vec{b}, B_2} \pmod{\ell^{2f} - 1},$$

where $\vec{b} = (b_0, b_1, \dots, b_{s-1}, \ell, \ell-1, \dots, \ell-1, 1)$, $B_1 = \{0, 1, \dots, f-2\}$ and $B_2 = \{0, 1, \dots, s-1, f-1\}$. We conclude that

$$n \equiv n'_{a', \vec{b}', B'_1} \equiv n'_{a', \vec{b}', B'_2} \pmod{\ell^{2f} - 1},$$

where $a' \equiv \ell^{-r}a \pmod{\ell^f - 1}$, $b'_i = b_{i+r} \pmod{\ell^f}$ for $i \in \{0, \dots, f-1\}$ and B'_ν is such that $J_{B'_\nu} = J_{B_\nu} \circ \text{Frob}_\ell^{-r}$ for $\nu = 1, 2$. \square

Now suppose $\rho|_{G_{K_p}}$ is reducible, write $\rho|_{G_{K_p}} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$ and c_ρ denote the corresponding class in $H^1(K_p, \chi_1\chi_2^{-1})$. Consider now the set of pairs

$$W'(\chi_1, \chi_2) = \{ (V_{\vec{a}, \vec{b}}, J) \mid J \subset S, \chi_1|_{I_{K_p}} = \prod_{\tau \in S} \omega_\tau^{a_\tau} \prod_{\tau \in J} \omega_\tau^{b_\tau}, \chi_2|_{I_{K_p}} = \prod_{\tau \in S} \omega_\tau^{a_\tau} \prod_{\tau \notin J} \omega_\tau^{b_\tau} \}.$$

(Note that interchanging χ_1 and χ_2 replaces J by its complement.) We shall see that the projection map $\pi_2 : W'(\chi_1, \chi_2) \rightarrow \{J \subset S\}$ is typically a bijection, so that $|W'(\chi_1, \chi_2)| = 2^f$. However $W_p(\rho)$ will be defined below as a subset of $\pi_1(W'(\chi_1, \chi_2))$ depending on c_ρ .

We now analyze the set $W'(\chi_1, \chi_2)$ in a manner analagous to the irreducible case. We write $\chi_\nu = \omega^{n_\nu}$ with $n_\nu \in \mathbf{Z}/(\ell^f - 1)\mathbf{Z}$ for $\nu = 1, 2$, and we let $n = n_1 - n_2$. If $a \in \mathbf{Z}/(\ell^f - 1)\mathbf{Z}$, $\vec{b} = (b_0, \dots, b_{f-1})$ with each $b_i \in \{1, \dots, \ell\}$ and $B \subset \{0, \dots, f-1\}$, let

$$n_{a, \vec{b}, B} = a + \sum_{i \in B} b_i \ell^i \pmod{\ell^f - 1}.$$

Then $W'(\chi_1, \chi_2)$ is in bijection with the set of triples (a, \vec{b}, B) as above with $n_1 \equiv n'_{a, \vec{b}, B} \pmod{\ell^f - 1}$ and $n_2 \equiv n'_{a, \vec{b}, \bar{B}} \pmod{\ell^f - 1}$ where \bar{B} is the complement of B in $\{0, \dots, f-1\}$. Note that for each $B \subset \{0, \dots, f-1\}$ there is a unique such triple for each solution of

$$n \equiv \sum_{i \in B} b_i \ell^i - \sum_{i \notin B} b_i \ell^i \pmod{\ell^f - 1}.$$

with $b_0, \dots, b_{f-1} \in \{1, \dots, \ell\}$. But the values of $b_i \ell^i - \sum_{i \notin B} b_i \ell^i$ are the ℓ^f consecutive integers from $n_B + 1 - \ell^f$ to n_B where

$$n_B = \sum_{i \in B} \ell^{i+1} - \sum_{i \notin B} \ell^i,$$

so there is a unique solution if $n \not\equiv n_B \pmod{\ell^f - 1}$ and two solutions if $n \equiv n_B \pmod{\ell^f - 1}$. In particular the projection $W'(\chi_1, \chi_2) \rightarrow \{J \subset S\}$ is surjective and $|W'(\chi_1, \chi_2)| = 2^f + |\{B \mid n \equiv n_B \pmod{\ell^f - 1}\}|$.

We now show that if f is odd, then the 2^f values of $n_B \pmod{\ell^f - 1}$ are distinct, unless $\ell = 2$ or 3 , in which case $n_{\{0, \dots, f-1\}} \equiv n_\emptyset \pmod{\ell^f - 1}$ and the rest are distinct. First note that

$$n_B \equiv -1 + (\ell + 1) \sum_{i \in B^*} (-1)^i \ell^i \pmod{\ell^f - 1},$$

where $B^* = (\{0, 2, \dots, f-1\} \cap B) \cup (\{1, 3, \dots, f-2\} \setminus B)$. Thus $n_{B_1} \equiv n_{B_2} \pmod{\ell^f - 1}$ if and only if

$$\sum_{i \in B_1^*} (-1)^i \ell^i \equiv \sum_{i \in B_2^*} (-1)^i \ell^i \pmod{(\ell^f - 1)/d},$$

where $d = \gcd(\ell + 1, \ell^f - 1)$. If $\ell > 3$, then $d = 2$ and the two sums differ by at most $(\ell^f - 1)/(\ell - 1) < (\ell^f + 1)/d$, so the above congruence holds if and only if equality holds, in which case $B_1^* = B_2^*$, so $B_1 = B_2$. If $\ell = 2$ or 3 , then $d = \ell - 1$, but the two sums differ by $(\ell^f - 1)/(\ell - 1)$ only when one of B_1 or B_2 is $\{0, \dots, f-1\}$ and the other is empty.

Now consider the case where f is even and $\ell > 3$. We then have

$$n_B \equiv (\ell + 1) \sum_{i \in B^*} (-1)^i \ell^i \pmod{\ell^f - 1},$$

where $B^* = (\{0, 2, \dots, f-2\} \cap B) \cup (\{1, 3, \dots, f-1\} \setminus B)$. Thus $n_{B_1} \equiv n_{B_2} \pmod{\ell^f - 1}$ if and only if

$$\sum_{i \in B_1^*} (-1)^i \ell^i \equiv \sum_{i \in B_2^*} (-1)^i \ell^i \pmod{(\ell^f - 1)/(\ell + 1)}.$$

But these two sums differ by at most $(\ell^f - 1)/(\ell - 1)$, which is less than $2(\ell^f - 1)/(\ell + 1)$. So if the above congruence holds then either equality holds, in which case $B_1 = B_2$, or

$$\sum_{i \in B_2^*} (-1)^i \ell^i = \sum_{i \in B_1^*} (-1)^i \ell^i + \sum_{i=0}^{f-1} (-1)^i \ell^i,$$

exchanging B_1 and B_2 if necessary. Solving $\pmod{\ell^r}$ inductively on r , we see that the only possibility is that $B_1^* = \emptyset$ and $B_2^* = \{0, 1, \dots, f-1\}$, in which case $n_{B_\nu} \equiv 0 \pmod{\ell^f - 1}$.

If f is even and $\ell = 3$, then the situation is the same, except that we have $(\ell^f - 1)/(\ell - 1) = 2(\ell^f - 1)/(\ell + 1)$, so in addition to the possibilities that arose for $\ell > 3$, we have

$$n_{\{0, \dots, f-1\}} \equiv n_\emptyset \equiv (\ell^f - 1)/2 \pmod{\ell^f - 1}$$

as for odd f .

Finally suppose that f is even and $\ell = 2$. In this case we have

$$n_B \equiv 3 \sum_{i \in B^*} (-1)^i 2^i \pmod{2^f - 1},$$

where $B^* = (\{0, 2, \dots, f-1\} \cap B) \cup (\{1, 3, \dots, f-2\} \setminus B)$. In particular $n_B \equiv 0 \pmod{3}$. Moreover we have $|n_{B_1} - n_{B_2}| \leq 3(2^f - 1)$ with equality possible only when one of B_1 or B_2 is $\{0, \dots, f-1\}$ and the other is empty, in which case $n_{B_\nu} \equiv 0 \pmod{2^f - 1}$. Thus each non-zero congruence class $\pmod{2^f - 1}$ arises as n_B for at most 3 values of B , while 0 arises for at most 4. It follows that each of the $(2^f - 4)/3$ non-zero multiples of 3 $\pmod{2^f - 1}$ arises as n_B for exactly 3 values of B , while 0 arises for exactly 4 values.

We have thus proved the following propositions:

Proposition 3.4. *Suppose that $\ell > 3$. If f is odd, then the congruence classes $\pmod{\ell^f - 1}$ of the form*

$$-1 + (\ell + 1) \sum_{i \in B^*} (-1)^i \ell^i$$

are distinct and non-zero as B^ runs through all subsets of $\{0, 1, \dots, f-1\}$. If f is even, then the congruence classes $\pmod{\ell^f - 1}$ of the form*

$$(\ell + 1) \sum_{i \in B^*} (-1)^i \ell^i$$

are distinct and non-zero as B^* runs through all non-empty proper subsets of $\{0, 1, \dots, f-1\}$. Letting A denote the set of such classes in each case, we have

$$|W'(\chi_1, \chi_2)| = \begin{cases} 2^f + 2, & \text{if } n = 0 \text{ and } f \text{ is even,} \\ 2^f + 1, & \text{if } n \in A, \\ 2^f, & \text{otherwise.} \end{cases}$$

Proposition 3.5. *Suppose that $\ell = 3$. If f is odd, then the congruence classes mod $3^f - 1$ of the form*

$$-1 + 4 \sum_{i \in B^*} (-1)^i 3^i$$

are distinct and non-zero mod $(\ell^f - 1)/2$ as B^* runs through all subsets of $\{0, 1, \dots, f-1\}$ other than $\{0, 2, \dots, f-1\}$ and $\{1, 3, \dots, f-2\}$. If f is even, then the congruence classes mod $3^f - 1$ of the form

$$4 \sum_{i \in B^*} (-1)^i 3^i$$

are distinct and non-zero mod $(3^f - 1)/2$ as B^* runs through all non-empty proper subsets of $\{0, 1, \dots, f-1\}$ other than $\{0, 2, \dots, f-2\}$ and $\{1, 3, \dots, f-1\}$. Letting A denote the set of such classes in each case, we have

$$|W'(\chi_1, \chi_2)| = \begin{cases} 2^f + 2, & \text{if } n = 0 \text{ and } f \text{ is even, or } n = (\ell^f - 1)/2 \\ 2^f + 1, & \text{if } n \in A, \\ 2^f, & \text{otherwise.} \end{cases}$$

Proposition 3.6. *Suppose that $\ell = 2$. Then*

$$|W'(\chi_1, \chi_2)| = \begin{cases} 2^f + 4, & \text{if } n = 0 \text{ and } f \text{ is even,} \\ 2^f + 3, & \text{if } n \neq 0, 3|n \text{ and } f \text{ is even,} \\ 2^f + 2, & \text{if } n = 0 \text{ and } f \text{ is odd,} \\ 2^f + 1, & \text{if } n \neq 0 \text{ and } f \text{ is odd,} \\ 2^f, & \text{if } 3 \nmid n \text{ and } f \text{ is even.} \end{cases}$$

As in the irreducible case, multiple B can occur with the same (a, \vec{b}) .

Proposition 3.7. *The map $W'(\chi_1, \chi_2) \rightarrow W_p(\rho)$ fails to be injective if and only if $\ell^r n \equiv m \pmod{\ell^f - 1}$ for some integers r, m with $|m| \leq \ell(\ell^{f-2} - 1)/(\ell - 1)$.*

Proof. Suppose first that $W'(\chi_1, \chi_2) \rightarrow W_p(\rho)$ is not injective. This means that for some a, \vec{b} and $B_1 \neq B_2$, we have

$$n_1 \equiv n_{a, \vec{b}, B_1} \equiv n_{a, \vec{b}, B_2} \pmod{\ell^f - 1}.$$

We can assume $n \not\equiv 0 \pmod{\ell^f - 1}$, which implies that B_2 is not the complement of B_1 . We can then assume $f-1 \in B_1 \setminus B_2$ and $0 \notin (B_1 \setminus B_2) \cup (B_2 \setminus B_1)$ after multiplying n by a power of ℓ as in the irreducible case. The rest of the argument is then exactly as in the irreducible case, except that

$$\sum_{i \in B_1 \setminus B_2} b_i \ell^i - \sum_{i \in B_2 \setminus B_1} b_i \ell^i = 2(\ell^f - 1)$$

is possible if $\ell = 2$, but this forces $n \equiv 0 \pmod{\ell^f - 1}$. □

For each pair $\alpha = (V_{\bar{a}, \bar{b}}, J) \in W'(\chi_1, \chi_2)$ we shall define below a subspace $L_\alpha \subset H^1(K_{\mathfrak{p}}, \overline{\mathbf{F}}_\ell(\chi_1 \chi_2^{-1}))$ of dimension $|J| + \delta$, where $\delta = 0$ except in certain cases where $\chi_1 \chi_2^{-1}$ is trivial or cyclotomic. We then define $W_{\mathfrak{p}}(\rho)$ by the following rule:

$$V_{\bar{a}, \bar{b}} \in W_{\mathfrak{p}}(\rho) \text{ if and only if } c_\rho \in L_\alpha \text{ for some } \alpha = (V_{\bar{a}, \bar{b}}, J) \in W'(\chi_1, \chi_2).$$

Before defining the subspace L_α , we recall some facts about crystalline representations. Recall that a character $\psi : D \rightarrow \overline{\mathbf{Q}}_\ell^\times$ is crystalline if and only the filtered ϕ -module $D_{\text{crys}}(\psi) = (B_{\text{crys}} \otimes_{\mathbf{Q}_\ell} \overline{\mathbf{Q}}_\ell(\psi))^D$ is free of rank one over $K_{\mathfrak{p}} \otimes_{\mathbf{Q}_\ell} \overline{\mathbf{Q}}_\ell$.

For each $\tau \in S$, let $e_\tau : K_{\mathfrak{p}} \otimes_{\mathbf{Q}_\ell} \overline{\mathbf{Q}}_\ell \rightarrow \overline{\mathbf{Q}}_\ell$ denote the projection defined by $a \otimes b \mapsto \tilde{\tau}(a)b$ where $\tilde{\tau}$ is the embedding $K_{\mathfrak{p}} \rightarrow \overline{\mathbf{Q}}_\ell$ reducing to τ , and let $e_\tau D_{\text{crys}}(\psi)$ denote the filtered $\overline{\mathbf{Q}}_\ell$ -vector space $D_{\text{crys}}(\psi) \otimes_{K \otimes_{\mathbf{Q}_\ell, \tau} \overline{\mathbf{Q}}_\ell} \overline{\mathbf{Q}}_\ell$.

Lemma 3.8. *Suppose that ψ is a crystalline character and for each $\tau \in S$, m_τ is the integer such that $\text{gr}^{-m_\tau} e_\tau D_{\text{crys}}(\psi) \neq 0$. Then $\overline{\psi}|_I = \prod_{\tau \in S} \omega_\tau^{m_\tau}$.*

Proof. Such crystalline characters satisfying the first condition correspond to (weakly) admissible filtered ϕ -modules with the specified filtration. These exist, and any two such differ by an unramified twist. Taking tensor products, the lemma reduces to the case where $m_\tau = 1$ or 0 according to whether or not $\tau = \tau_0$. The result in this case follows for example from Theorems 5.3 and 8.4 of [15]. \square

Recall that $\alpha = (V_{\bar{a}, \bar{b}}, J) \in W'(\chi_1, \chi_2)$ if and only if

$$\chi_1|_{I_{K_{\mathfrak{p}}}} = \prod_{\tau \in S} \omega_\tau^{a_\tau} \prod_{\tau \in J} \omega_\tau^{b_\tau}, \quad \chi_2|_{I_{K_{\mathfrak{p}}}} = \prod_{\tau \in S} \omega_\tau^{a_\tau} \prod_{\tau \notin J} \omega_\tau^{b_\tau}.$$

Lemma 3.9. *Suppose that $\alpha = (V_{\bar{a}, \bar{b}}, J) \in W'(\chi_1, \chi_2)$. Let $m_{\tau, \alpha} = b_\tau$ or $-b_\tau$ according to whether or not $\tau \in J$. Then there is a unique lift χ_α of $\chi_1 \chi_2^{-1}$ with the following properties:*

- χ_α is crystalline with $\text{gr}^{-m_\tau} e_\tau D_{\text{crys}}(\chi_{i, \alpha}) \neq 0$ for each $\tau \in S$;
- if $g \in D^{\text{ab}}$ corresponds via local class field theory to ℓ , then $\chi_\alpha(g)$ is the Teichmüller lift of $\chi_1 \chi_2^{-1}(g)$.

Proof. Let ψ be a character satisfying the first condition. The preceding lemma shows that the reduction of ψ is an unramified twist of $\chi_1 \chi_2^{-1}$. Let $\chi_\alpha = \delta \psi$, where $\delta(g) = \tilde{\chi}_1 \tilde{\chi}_2^{-1}(g) \psi^{-1}(g)$. \square

Recall that if $\psi : G_{K_{\mathfrak{p}}} \rightarrow \overline{\mathbf{Q}}_\ell^\times$ is a crystalline representation, then Bloch and Kato define a subspace $H_f^1(K_{\mathfrak{p}}, \overline{\mathbf{Q}}_\ell(\psi))$ corresponding to those extensions of topological $\overline{\mathbf{Q}}_\ell G_{K_{\mathfrak{p}}}$ -modules

$$0 \rightarrow \overline{\mathbf{Q}}_\ell(\psi) \rightarrow E \rightarrow \overline{\mathbf{Q}}_\ell \rightarrow 0$$

which are crystalline. By Corollary 3.8.4 of [3] for example, we have

$$\dim H_f^1(K_{\mathfrak{p}}, \overline{\mathbf{Q}}_\ell(\psi)) = \dim H^0(K_{\mathfrak{p}}, \overline{\mathbf{Q}}_\ell(\psi)) + \dim D_{\text{crys}}(\psi) - \dim \text{Fil}^0 D_{\text{crys}}(\psi)$$

where the dimensions are over $\overline{\mathbf{Q}}_\ell$. Applying this for $\psi = \chi_\alpha$ for $\alpha = (V_{\bar{a}, \bar{b}}, J) \in W'(\chi_1, \chi_2)$, we see that $\dim H_f^1(K_{\mathfrak{p}}, \overline{\mathbf{Q}}_\ell(\chi_\alpha)) = |J|$. We then define $H_f^1(K_{\mathfrak{p}}, \overline{\mathbf{Z}}_\ell(\chi_\alpha))$ as the preimage of $H_f^1(K_{\mathfrak{p}}, \overline{\mathbf{Q}}_\ell(\chi_\alpha))$ under the natural map

$$H^1(K_{\mathfrak{p}}, \overline{\mathbf{Z}}_\ell(\chi_\alpha)) \rightarrow H^1(K_{\mathfrak{p}}, \overline{\mathbf{Q}}_\ell(\chi_\alpha))$$

and L'_α as the image of $H_f^1(K_{\mathfrak{p}}, \overline{\mathbf{Z}}_\ell(\chi_\alpha))$ under the natural map

$$H^1(K_{\mathfrak{p}}, \overline{\mathbf{Z}}_\ell(\chi_\alpha)) \rightarrow H^1(K_{\mathfrak{p}}, \overline{\mathbf{F}}_\ell(\chi_1\chi_2^{-1})).$$

We then let $L_\alpha = L'_\alpha$ except in two cases:

- if $\chi_1\chi_2^{-1}$ is the cyclotomic character, $\vec{b} = (\ell, \dots, \ell)$ and $J = S$, then we let $L_\alpha = H^1(K_{\mathfrak{p}}, \overline{\mathbf{F}}_\ell(\chi_1\chi_2^{-1}))$;
- if $\chi_1\chi_2^{-1}$ is the trivial character and $J \neq S$, then we let $L_\alpha = L'_\alpha + L_{\text{ur}}$, where L_{ur} is the one-dimensional space of unramified classes in $H^1(K_{\mathfrak{p}}, \overline{\mathbf{F}}_\ell)$.

Lemma 3.10. *If $\alpha = (V_{\vec{a}, \vec{b}}, J) \in W'(\chi_1, \chi_2)$, then $\dim L_\alpha = |J|$ except in the following cases:*

- (1) *if $\chi_1\chi_2^{-1}$ is cyclotomic, $\vec{b} = (\ell, \dots, \ell)$, $J = S$ and $\ell > 2$, then $\dim L_\alpha = |J| + 1$;*
- (2) *if $\chi_1\chi_2^{-1}$ is trivial and $\ell > 2$, then $\dim L_\alpha = |J| + 1$ or $|J| + 2$ according to whether or not $L_{\text{ur}} \subset L'_\alpha$;*
- (3) *if $\chi_1\chi_2^{-1}$ is trivial (or equivalently, cyclotomic) and $\ell = 2$, then $\dim L_\alpha = |J| + 1$ unless either $L_{\text{ur}} \not\subset L'_\alpha$ or $\vec{b} = (\ell, \dots, \ell)$ and $J = S$, in which case $\dim L_\alpha = |J| + 2$.*

Proof. Note first that $H_f^1(K_{\mathfrak{p}}, \overline{\mathbf{Z}}_\ell(\chi_\alpha))$ contains $H^1(K_{\mathfrak{p}}, \overline{\mathbf{Z}}_\ell(\chi_\alpha))_{\text{tor}}$ and that the quotient is free of rank $|J| = \dim H_f^1(K_{\mathfrak{p}}, \overline{\mathbf{Q}}_\ell(\chi_\alpha))$. Therefore the natural map

$$H_f^1(K_{\mathfrak{p}}, \overline{\mathbf{Z}}_\ell(\chi_\alpha)) \otimes_{\overline{\mathbf{Z}}_\ell} \overline{\mathbf{F}}_\ell \rightarrow H^1(K_{\mathfrak{p}}, \overline{\mathbf{Z}}_\ell(\chi_\alpha)) \otimes_{\overline{\mathbf{Z}}_\ell} \overline{\mathbf{F}}_\ell \rightarrow H^1(K_{\mathfrak{p}}, \overline{\mathbf{F}}_\ell(\chi_1\chi_2^{-1}))$$

is injective and its image L'_α has dimension $|J|$, unless $\chi_1\chi_2^{-1}$ is trivial, in which case the dimension is $|J| + 1$. The lemma is now immediate from the definition of L_α and, in the cyclotomic $J = S$ case, the local Euler characteristic formula. \square

If $\rho|_{G_{K_{\mathfrak{p}}}} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$ and c_ρ is the corresponding class in $H^1(K_{\mathfrak{p}}, \overline{\mathbf{F}}_\ell(\chi_1\chi_2^{-1}))$, we now define

$$(3) \quad W_{\mathfrak{p}}(\rho) = \{ V \mid c_\rho \in L_\alpha \text{ for some } \alpha = (V, J) \in W'(\chi_1, \chi_2) \}.$$

Note that if $\rho|_{G_{K_{\mathfrak{p}}}} \sim \chi_1 \oplus \chi_2$, or equivalently $c_\rho = 0$, then $W_{\mathfrak{p}}(\rho) = \pi_1(W'(\chi_1, \chi_2))$ is independent of the choice of ordering of χ_1 and χ_2 . Note also in this case that $|W_{\mathfrak{p}}(\rho)| \sim 2^f$ as in the irreducible case (1). (We remark that it is shown in [11] that in the cases where $\rho|_{G_{K_{\mathfrak{p}}}}$ is semisimple, the set $W_{\mathfrak{p}}(\rho)$ is related to the set of Jordan-Hölder constituents of the reduction of a corresponding irreducible characteristic zero of $\text{GL}_2(k)$.)

The set $W_{\mathfrak{p}}(\rho)$ was defined in terms of the restriction of ρ to $G_{K_{\mathfrak{p}}}$. We now check that it is in fact non-empty and depends only on the restriction to inertia.

Proposition 3.11. *If $\rho : G_K \rightarrow \text{GL}_2(\overline{\mathbf{F}}_\ell)$ is continuous, irreducible and totally odd, then $W_{\mathfrak{p}}(\rho)$ is non-empty and depends only on $\rho|_{I_{K_{\mathfrak{p}}}}$.*

Proof. We first prove that $W_{\mathfrak{p}}(\rho) \neq \emptyset$. If $\rho|_{G_{K_{\mathfrak{p}}}}$ is irreducible, then it is induced from a character ξ , and Propositions 3.1 and 3.2 show that $W'(\xi)$ is non-empty, and hence so is $W_{\mathfrak{p}}(\rho)$. (Note that if $\ell^f = 2$, then n is not divisible by 3.) If $\rho|_{G_{K_{\mathfrak{p}}}}$ is reducible, then it is of the form $\begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$, and we showed that the projection map $W'(\chi_1, \chi_2) \rightarrow \{J \subset S\}$ is surjective. In particular, there is an

element $\alpha = (V_{\vec{a}, \vec{b}}, S) \in W'(\chi_1, \chi_2)$. Moreover if $\chi_1 \chi_2^{-1}$ is cyclotomic, we may choose $\vec{b} = (\ell, \dots, \ell)$, so that in all cases $L_\alpha = H^1(K_{\mathfrak{p}}, \overline{\mathbf{F}}_\ell(\chi_1 \chi_2^{-1}))$ by Lemma 3.10 and the local Euler characteristic formula. It follows that $c_\rho \in L_\alpha$ and $V_{\vec{a}, \vec{b}} \in W_{\mathfrak{p}}(\rho)$.

For the dependence only on inertia, first note that the irreducibility of $\rho|_{G_{K_{\mathfrak{p}}}}$ is determined by $\rho|_{I_{K_{\mathfrak{p}}}}$. In the case that $\rho|_{G_{K_{\mathfrak{p}}}}$ is irreducible, $W_{\mathfrak{p}}(\rho)$ is determined by $W'(\xi)$, which depends only on $\xi|_{I_{K_{\mathfrak{p}}}}$, which in turn depends only on $\rho|_{I_{K_{\mathfrak{p}}}}$.

Suppose now that $\rho|_{G_{K_{\mathfrak{p}}}}$ is reducible and $\rho' : G_K \rightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ is such that $\rho|_{I_{K_{\mathfrak{p}}}} \sim \rho'|_{I_{K_{\mathfrak{p}}}}$. Changing bases, we may assume $\rho|_{G_{K_{\mathfrak{p}}}} = \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$ and $\rho|_{I_{K_{\mathfrak{p}}}} = \rho'|_{I_{K_{\mathfrak{p}}}}$. Note that the function $G_{K_{\mathfrak{p}}}/I_{K_{\mathfrak{p}}} \rightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ defined by $g \mapsto \rho'(g)\rho(g)^{-1}$ takes values in $Z(\rho(I_{K_{\mathfrak{p}}}))$. We divide the proof into cases according to the possible centralizers.

Suppose first that $\chi_1 \chi_2^{-1}$ is ramified and c_ρ has non-trivial restriction to $I_{K_{\mathfrak{p}}}$. In this case $\rho|_{I_{K_{\mathfrak{p}}}}$ is indecomposable and has centralizer consisting only of the scalar matrices. It follows that $\rho' = \psi\rho$ for some unramified character $\psi : G_{K_{\mathfrak{p}}} \rightarrow \overline{\mathbf{F}}_\ell^\times$. Since $W'(\chi_1, \chi_2)$ depends only on the restriction of χ_1 and χ_2 to $I_{K_{\mathfrak{p}}}$, we have $W'(\psi\chi_1, \psi\chi_2) = W'(\chi_1, \chi_2)$. Moreover the subspaces L_α of $H^1(K_{\mathfrak{p}}, \overline{\mathbf{F}}_\ell(\chi_1 \chi_2^{-1}))$ do not change if ρ is replaced by an unramified twist, nor does the class c_ρ . It follows that $W_{\mathfrak{p}}(\rho') = W_{\mathfrak{p}}(\rho)$.

Next suppose that $\chi_1 \chi_2^{-1}$ is ramified and c_ρ has trivial restriction to $I_{K_{\mathfrak{p}}}$. Then in fact $c_\rho = 0$, so we may assume $\rho|_{G_{K_{\mathfrak{p}}}} = \begin{pmatrix} \chi_1 & 0 \\ 0 & \chi_2 \end{pmatrix}$. In this case the centralizer of $\rho(I_{K_{\mathfrak{p}}})$ consists of the diagonal matrices. It follows that $\rho'|_{G_{K_{\mathfrak{p}}}} = \begin{pmatrix} \psi_1 \chi_1 & 0 \\ 0 & \psi_2 \chi_2 \end{pmatrix}$ for some unramified characters ψ_1 and ψ_2 . Moreover we have $c_{\rho'} = 0$ and $W'(\psi_1 \chi_1, \psi_2 \chi_2) = W'(\chi_1, \chi_2)$, so $W_{\mathfrak{p}}(\rho') = W_{\mathfrak{p}}(\rho)$.

Next suppose that $\chi_1 \chi_2^{-1}$ is unramified and c_ρ has non-trivial restriction to $I_{K_{\mathfrak{p}}}$. In this case we have

$$Z(\rho(I_{K_{\mathfrak{p}}})) = \left\{ \begin{pmatrix} x & xy \\ 0 & x \end{pmatrix} \mid x \in \overline{\mathbf{F}}_\ell^\times, y \in \overline{\mathbf{F}}_\ell \right\},$$

so if $g \in G_{K_{\mathfrak{p}}}$, then

$$\rho'(g) = \begin{pmatrix} 1 & \mu(g) \\ 0 & 1 \end{pmatrix} \psi(g)\rho(g)$$

for some unramified character ψ and cocycle $\mu : G_{K_{\mathfrak{p}}}/I_{K_{\mathfrak{p}}} \rightarrow \overline{\mathbf{F}}_\ell(\chi_1 \chi_2^{-1})$. It follows that if $\chi_1 \neq \chi_2$, then $c_{\rho'} = c_\rho$ in $H^1(K_{\mathfrak{p}}, \overline{\mathbf{F}}_\ell(\chi_1 \chi_2^{-1}))$, and if $\chi_1 = \chi_2$, then $c_{\rho'} - c_\rho \in L_{\mathrm{ur}}$. Since the spaces L_α are the same for ρ and ρ' and contain L_{ur} if $\chi_1 = \chi_2$, we conclude that $W_{\mathfrak{p}}(\rho') = W_{\mathfrak{p}}(\rho)$.

Finally suppose that $\chi_1 \chi_2^{-1}$ is unramified and c_ρ has trivial restriction to $I_{K_{\mathfrak{p}}}$, so

$$\rho'(g) = \rho(g) = \begin{pmatrix} \chi_1(g) & 0 \\ 0 & \chi_1(g) \end{pmatrix}$$

for $g \in I_{K_{\mathfrak{p}}}$. Note that $c_\rho = 0$ unless $\chi_1 = \chi_2$, in which case $c_\rho \in L_{\mathrm{ur}}$, and similarly for $c_{\rho'}$. It follows that $W_{\mathfrak{p}}(\rho') = \pi_1(W'(\chi'_1, \chi'_2)) = \pi_1(W'(\chi_1, \chi_2)) = W_{\mathfrak{p}}(\rho)$. \square

We are now ready to state the weight conjecture. Recall that $W(\rho)$ is defined as the set of representations of $\prod_{\mathfrak{p}|\ell} \mathrm{GL}_2(k_{\mathfrak{p}})$ of the form $\otimes_{\overline{\mathbf{F}}_\ell} V_{\mathfrak{p}}$ with each $V_{\mathfrak{p}} \in$

$W_{\mathfrak{p}}(\rho)$. By the preceding proposition $W(\rho)$ is non-empty and depends only on the restrictions of ρ to inertia groups at primes over ℓ .

Conjecture 3.12. *If $\rho : G_K \rightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ is modular, then*

$$W(\rho) = \{ V \mid \rho \text{ is modular of weight } V \}.$$

We now check compatibility of the conjectural weight set with twists and determinants.

Proposition 3.13. *Suppose that $\rho : G_K \rightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ is continuous, irreducible and totally odd.*

- (1) *Let $\chi : G_K \rightarrow \overline{\mathbf{F}}_\ell^\times$ be such that $\chi|_{I_{K_{\mathfrak{p}}}} = \prod_{\tau \in S_{\mathfrak{p}}} \omega_\tau^{c_\tau}$ for each $\mathfrak{p}|\ell$. Then $V \in W(\rho)$ if and only if $V \otimes V_\chi \in W(\chi\rho)$, where*

$$V_\chi = \otimes_{\mathfrak{p}|\ell} \otimes_{\tau \in S_{\mathfrak{p}}} \det^{c_\tau} k_{\mathfrak{p}}^2 \otimes_{\tau} \overline{\mathbf{F}}_\ell.$$

- (2) *If $V \in W(\rho)$ and V has central character $\otimes_{\mathfrak{p}|\ell} \prod_{\tau \in S_{\mathfrak{p}}} \tau^{c_\tau}$, then $\det \rho|_{I_{K_{\mathfrak{p}}}} = \prod_{\tau \in S_{\mathfrak{p}}} \omega_\tau^{c_\tau+1}$ for each $\mathfrak{p}|\ell$.*

Proof. To prove the first assertion it suffices to show that $V \in W_{\mathfrak{p}}(\rho)$ if and only if $V \otimes V_{\chi_{\mathfrak{p}}} \in W_{\mathfrak{p}}(\chi\rho)$ where $\chi_{\mathfrak{p}} = \chi|_{G_{K_{\mathfrak{p}}}}$ and $V_{\chi_{\mathfrak{p}}} = \otimes_{\tau \in S_{\mathfrak{p}}} \det^{c_\tau} k_{\mathfrak{p}}^2 \otimes_{\tau} \overline{\mathbf{F}}_\ell$. If $\rho|_{G_{K_{\mathfrak{p}}}} \sim \mathrm{Ind}_{D'}^D \xi$ is irreducible, then $(V, J) \in W'(\xi)$ if and only if $(V \otimes V_{\chi_{\mathfrak{p}}}, J) \in W'(\xi\chi_{\mathfrak{p}})$, yielding the assertion in this case. If $\rho|_{G_{K_{\mathfrak{p}}}} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$ is reducible, then $\alpha = (V, J) \in W'(\chi_1, \chi_2)$ if and only if $\alpha' = (V \otimes V_{\chi_{\mathfrak{p}}}, J) \in W'(\chi_1\chi_{\mathfrak{p}}, \chi_2\chi_{\mathfrak{p}})$. Moreover, since $V_{\vec{a}, \vec{b}} \otimes V_{\chi_{\mathfrak{p}}}$ is of the form $V_{\vec{a}', \vec{b}'}$, we see that $\chi_\alpha = \chi_{\alpha'}$, so $L_\alpha = L'_{\alpha'} \subset H^1(K_{\mathfrak{p}}, \overline{\mathbf{F}}_\ell(\chi_1\chi_2^{-1}))$. Since also $c_\rho = c_{\chi\rho}$, we get the assertion in this case as well.

To prove the second assertion, we can again work locally at primes $\mathfrak{p}|\ell$. Writing $V = \otimes_{\mathfrak{p}|\ell} V_{\mathfrak{p}}$, we have $V_{\mathfrak{p}} \in W_{\mathfrak{p}}(\rho)$ for each $\mathfrak{p}|\ell$. If $V_{\mathfrak{p}} = V_{\vec{a}, \vec{b}}$, this gives $\det \rho|_{I_{K_{\mathfrak{p}}}} = \prod_{\tau \in S_{\mathfrak{p}}} \omega_\tau^{2a_\tau + b_\tau}$. Since $V_{\vec{a}, \vec{b}}$ has central character $\prod_{\tau \in S_{\mathfrak{p}}} \tau^{2a_\tau + b_\tau - 1}$, we have

$$\sum_{i=0}^{f_{\mathfrak{p}}-1} c_{\tau_i} \ell^i \equiv \sum_{i=0}^{f_{\mathfrak{p}}-1} (2a_{\tau_i} + b_{\tau_i} - 1) \ell^i \pmod{(\ell^{f_{\mathfrak{p}}} - 1)}.$$

Adding $\sum_{i=0}^{f_{\mathfrak{p}}-1} \ell^i$ to each side of the congruence, we deduce that $\prod_{\tau \in S_{\mathfrak{p}}} \omega_\tau^{c_\tau+1} = \prod_{\tau \in S_{\mathfrak{p}}} \omega_\tau^{2a_\tau + b_\tau}$. \square

Combining the first part of the proposition with that of Proposition 3.13, we deduce the following:

Corollary 3.14. *Suppose that $\rho : G_K \rightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ is continuous, irreducible and totally odd and $\chi : G_K \rightarrow \overline{\mathbf{F}}_\ell^\times$ is a character. Then Conjecture 3.12 holds for ρ if and only if it holds for $\chi\rho$.*

In the case $K = \mathbf{Q}$ follows from known results on Serre's Conjecture (cf. [19], [2]).

Theorem 3.15. *Conjecture 3.12 holds if $K = \mathbf{Q}$.*

Proof. Replacing ρ by a twist, we can assume $\rho|_{I_\ell}$ has the form $\begin{pmatrix} \omega_2^b & 0 \\ 0 & \omega_2^{\ell b} \end{pmatrix}$ or $\begin{pmatrix} \omega^b & * \\ 0 & 1 \end{pmatrix}$ for some b with $1 \leq b \leq \ell - 1$. In the second case we write $\rho|_{G_{\mathbf{Q}_\ell}} \sim \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$. We shall also use ω to denote the cyclotomic character on $G_{\mathbf{Q}}$ or $G_{\mathbf{Q}_\ell}$.

In the first case we find that $W(\rho) = \{V_{0,b}, V_{b-1, \ell+1-b}\}$. In the second case, we have the following possibilities:

$$W'(\chi_1, \chi_2) = \begin{cases} \{(V_{0,b}, S), (V_{b, \ell-1-b}, \emptyset)\}, & \text{if } 1 < b < \ell - 2, \\ \{(V_{0, \ell-1}, S), (V_{0, \ell-1}, \emptyset)\}, & \text{if } b = \ell - 1 \text{ and } \ell > 2, \\ \{(V_{0, \ell}, S), (V_{0,1}, S), (V_{1, \ell-2}, \emptyset)\}, & \text{if } b = 1 \text{ and } \ell > 3, \\ \{(V_{0, \ell-2}, S), (V_{\ell-2, \ell}, \emptyset), (V_{\ell-2, 1}, \emptyset)\}, & \text{if } b = \ell - 2 \text{ and } \ell > 3, \\ \{(V_{0, \ell}, S), (V_{0,1}, S), (V_{1, \ell}, \emptyset), (V_{1,1}, \emptyset)\}, & \text{if } b = 1 \text{ and } \ell \leq 3. \end{cases}$$

Moreover, dimension considerations show that $L_{(V,J)} = H^1(G_{\mathbf{Q}_\ell}, \overline{\mathbf{F}}(\chi_1 \chi_2^{-1}))$ whenever $J = S$, unless $\chi_1 \chi_2^{-1} = \omega$ and $V = V_{(0,1)}$, in which case the construction of $L_{(V,J)}$ shows that the corresponding extensions arise from finite flat group schemes over \mathbf{Z}_ℓ , hence are peu ramifiées in the sense of Serre [23]. Considering dimensions in this case then gives that $L_{(V,J)}$ consists precisely of the classes which are peu ramifiées. Note also that $L_{(V,J)} = 0$ whenever $J = \emptyset$ unless $\chi_1 \chi_2^{-1}$ is trivial, in which case we do not need an explicit description of $L_{(V,J)}$. This gives

$$W(\rho) = \begin{cases} \{V_{0,b}\}, & \text{if } 1 < b < \ell - 1 \text{ and } \rho|_{G_{\mathbf{Q}_\ell}} \text{ is non-split,} \\ \{V_{0,b}, V_{b, \ell-1-b}\}, & \text{if } 1 < b < \ell - 2 \text{ and } \rho|_{G_{\mathbf{Q}_\ell}} \text{ is split,} \\ \{V_{0, \ell-2}, V_{\ell-2, \ell}, V_{\ell-2, 1}\}, & \text{if } b = \ell - 2, \ell > 3 \text{ and } \rho|_{G_{\mathbf{Q}_\ell}} \text{ is split,} \\ \{V_{0, \ell-1}\}, & \text{if } b = \ell - 1 \text{ and } \ell > 2, \\ \{V_{0, \ell}\}, & \text{if } b = 1, \chi_1 \chi_2^{-1} = \omega \text{ and } \rho|_{G_{\mathbf{Q}_\ell}} \text{ is très ramifiée,} \\ \{V_{0, \ell}, V_{0,1}, V_{1, \ell-2}\}, & \text{if } b = 1, \ell > 3 \text{ and } \rho|_{G_{\mathbf{Q}_\ell}} \text{ is split,} \\ \{V_{0,3}, V_{0,1}, V_{1,3}, V_{1,1}\}, & \text{if } b = 1, \ell = 3 \text{ and } \rho|_{G_{\mathbf{Q}_\ell}} \text{ is split,} \\ \{V_{0, \ell}, V_{0,1}\}, & \text{otherwise.} \end{cases}$$

Propositions 2.2 and 3.13 show that ρ is modular of weight¹ $b + 1$ and level prime to ℓ if and only if $\omega^{a+b}\rho$ is modular of weight $V_{a,b}$. If ρ is modular of weight 2 and level prime to ℓ , then $\omega\rho|_{G_{\mathbf{Q}_\ell}}$ arises from a finite flat group scheme over \mathbf{Z}_ℓ , so it follows from results of Deligne and Fontaine ([13, 2.5,2.6]) and the explicit description of $W(\rho)$ above that if ρ is modular of weight V , then $V \in W(\rho)$.

To show that if $V \in W(\rho)$, then ρ is modular of weight V , we combine the following four results. The first of these is a standard consequence of multiplication by the Hasse invariant (or Eisenstein series) of weight $\ell - 1$.

Lemma 3.16. *If ρ is modular of weight 2 and level prime to ℓ , then ρ is modular of weight $\ell + 1$ and level prime to ℓ .*

The theorem in the irreducible case is then a consequence of the following result of Edixhoven; see the second paragraph of [13, 4.5].

¹Recall that our notion of *modular of weight k* uses the geometric conventions of [6]. Translating from the arithmetic conventions of other authors introduces the twist by ω^{k-1} when citing their results.

Lemma 3.17. *Suppose that ρ is modular of weight $b + 1$ and level prime to ℓ with $2 \leq b \leq \ell$. If $\rho|_{G_{\mathbf{Q}_\ell}}$ is irreducible, then $\omega^{b-1}\rho$ is modular of weight $\ell + 2 - b$ and level prime to ℓ .*

To treat the reducible case, we first apply Mazur's Principle [13, 2.8].

Theorem 3.18. *Suppose that ρ is modular of weight $\ell + 1$ and level prime to ℓ . If ρ is not modular of weight 2 and level prime to ℓ , then $\omega\rho|_{G_{\mathbf{Q}_\ell}}$ is a très ramifiée representation of the form $\begin{pmatrix} \omega\chi_2 & * \\ 0 & \chi_2 \end{pmatrix}$ for some unramified character χ_2 .*

The theorem is then a consequence of the companion forms theorem, proved by Gross [17], subject to unchecked compatibilities, then by Coleman and Voloch [7], but under slightly different hypotheses than we need. Yet another proof was given by Faltings and Jordan [14], whose version we cite:

Theorem 3.19. *Suppose that ρ is modular of weight $b + 1$ and level prime to ℓ with $1 \leq b \leq \ell - 2$. If $\rho|_{G_{\mathbf{Q}_\ell}}$ is reducible and split, then $\omega^b\rho$ is modular of weight $\ell - b$ and level prime to ℓ .*

□

4. THE STRONG WEIGHT $(2, \dots, 2)$ CONJECTURE

Define $\tau_{\mathfrak{p}}(\pi)$ to be the inertia type of $\pi_{\mathfrak{p}}$. (This is the same as a type unless $\tau_{\mathfrak{p}}(\pi)$ is a twist of semistable, in which case the inertia type says whether the twist is unramified or special.)

Define what it means for $\rho_{\mathfrak{p}} = \rho|_{G_{\mathfrak{p}}}$ to be compatible with an inertia type $\tau_{\mathfrak{p}}$. For $\mathfrak{p} \nmid \ell$, this means $\rho_{\mathfrak{p}}$ has a lift whose restriction to $I_{\mathfrak{p}}$ corresponds to $\tau_{\mathfrak{p}}$. For $\mathfrak{p} \mid \ell$ and $\tau_{\mathfrak{p}}$ not twist of semistable, this means $\overline{T}_{\mathfrak{p}}$ has a Jordan-Hölder constituent in $W_{\mathfrak{p}}(\rho)$. If $\tau_{\mathfrak{p}}$ is twist of semistable, then $\overline{T}_{\mathfrak{p}} = V_{\vec{a}, \vec{1}} \oplus V_{\vec{a}, \vec{\ell}}$ for some \vec{a} . If $\tau_{\mathfrak{p}}$ is twist of unramified, then $\rho_{\mathfrak{p}}$ is compatible with it if and only if $V_{\vec{a}, \vec{1}} \in W_{\mathfrak{p}}(\rho)$. If $\tau_{\mathfrak{p}}$ is a twist of special, then $\rho_{\mathfrak{p}}$ is compatible with it if and only if

$$\rho_{\mathfrak{p}} \sim \chi \otimes \begin{pmatrix} \omega & * \\ 0 & 1 \end{pmatrix}$$

for some χ such that $\chi|_{I_{\mathfrak{p}}} = \prod_{\tau \in S} \omega_{\tau}^{a_{\tau}}$, where ω is the mod ℓ cyclotomic character of $G_{\mathfrak{p}}$. (Note that this is specifically geared to weight $(2, \dots, 2)$.)

Conjecture 4.1. *Suppose that $\rho : G_K \rightarrow \mathrm{GL}_2(\overline{F}_{\ell})$ is continuous, irreducible and totally odd. Suppose also that the restriction of ρ to $G_{K(\mu_4)}$ (resp. $G_{K(\mu_3)}$) is irreducible if $\ell = 2$ (resp. $\ell = 3$). For each prime \mathfrak{p} of K , let $\tau_{\mathfrak{p}}$ be an inertia type. Suppose further that $\tau_{\mathfrak{p}}$ unramified for all but finitely many primes \mathfrak{p} . Then there exists a cuspidal automorphic representation π of of weight $(2, \dots, 2)$ such that $\rho \sim \bar{\rho}_{\pi}$ and $\tau_{\mathfrak{p}} = \tau_{\mathfrak{p}}(\pi)$ for all \mathfrak{p} if and only if $\tau_{\mathfrak{p}}$ is compatible with $\tau_{\mathfrak{p}}(\rho)$ for all \mathfrak{p} .*

Note that we're assuming ℓ is unramified in K , otherwise we haven't defined compatibility for $\mathfrak{p} \mid \ell$ since we haven't defined $W_{\mathfrak{p}}(\rho)$. Also one would expect the technical hypothesis to arise for ℓ such that $K(\mu_{\ell})^+ \subset K$.

Some consequences:

Proposition 4.2. *If the conjecture holds for ρ , then ρ is modular of weight $(2, \dots, 2)$ and level dividing $n\ell^2$.*

Proposition 4.3. *If the conjecture holds for K and ℓ , then there are only finitely many continuous, irreducible, totally odd $\rho : G_K \rightarrow \mathrm{GL}_2(\overline{\mathbf{F}}_\ell)$ of conductor dividing n .*

Proposition 4.4. *If the conjecture holds for K and E is an elliptic curve over K , then E is modular.*

REFERENCES

- [1] A.Ash, D.Doud, D.Pollack, Galois representations with conjectural connections to arithmetic cohomology, *Duke Math. J.* 112 (2002), 521–579.
- [2] A.Ash, W.Sinnott, An analogue of Serre's conjecture for Galois representations and Hecke eigenclasses in the mod p cohomology of $\mathrm{GL}(n, \mathbf{Z})$. *Duke Math. J.* 105 (2000), 1–24.
- [3] S.Bloch, K.Kato, L -functions and Tamagawa numbers of motives, *Grothendieck Festschrift*, Vol.1, 333–400, *Progr. Math.*, 86, Birkhäuser, Boston (1990)
- [4] K. Buzzard, "On level lowering for mod 2 representations", *Mathematical Research Letters* 7, pp95–110 (2000).
- [5] H.Carayol, Sur la mauvaise réduction des courbes de Shimura, *Compositio Math* 59 (1986) 151–230.
- [6] H. Carayol, Sur les représentations l -adiques associées aux formes modulaires de Hilbert, *Ann. Sci. ENS* 19 (1986) 409–468.
- [7] R.Coleman, J.-F.Voloch, Companion forms and Kodaira-Spencer theory, *Invent. Math.* 110 (1992) 263–282
- [8] C, Cornut and V. Vatsal, CM points and quaternion algebras, preprint 2004.
- [9] L.Dembélé, F.Diamond, Roberts, in preparation.
- [10] F.Diamond, The refined conjecture of Serre, in *Elliptic Curves and Fermat's Last Theorem*, J.Coates and S.-T.Yau (eds.), Hong Kong 1993, International Press, 2nd. ed. (1997) 172–186
- [11] F.Diamond, A correspondence between representations of local Galois groups and Lie-type groups, preprint.
- [12] F.Diamond, R.Taylor, Lifting modular mod ℓ representations, *Duke Math. J.* 74 (1994) 253–269.
- [13] B.Edixhoven, The weight in Serre's conjectures on modular forms. *Invent. Math.* 109 (1992), no. 3, 563–594.
- [14] G.Faltings, B. Jordan, Crystalline cohomology and $\mathrm{GL}(2, \mathbf{Q})$. *Israel J. Math.* 90 (1995), 1–66.
- [15] J.-M.Fontaine, G.Laffaille, Construction de représentations p -adiques, *Ann. Sci. Ecole Norm. Sup.* 15 (1982) 547–608
- [16] T.Gee, Companion forms over totally real fields, PhD Thesis, Imperial College London (2004)
- [17] B.Gross, A tameness criterion for Galois representations associated to modular forms (mod p), *Duke Math. J.* 61 (1990) 445–516
- [18] F.Jarvis, Correspondances on Shimura curves and Mazur's Principle at p , *Pacific J. Math.* 213 (2004) 267–280
- [19] C.Khare, A local analysis of congruences in the (p, p) case. II, *Invent. Math.* 143 (2001), 129–155.
- [20] C. Khare, On Serre's modularity conjecture for 2-dimensional mod p representations of the absolute Galois group of the rationals unramified outside p , preprint.
- [21] C. Khare and J.-P. Wintenberger, On Serre's reciprocity conjecture for 2-dimensional mod p representations of the absolute Galois group of the rationals, preprint.
- [22] K.Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms, *Invent. Math.* 100 (1990)
- [23] J.-P.Serre, Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, *Duke Math. J.* 54 (1987) 179–230
- [24] R.Taylor, On Galois representations associated to Hilbert modular forms, *Invent. Math.* 98 (1989) 265–280

DEPARTMENT OF MATHEMATICS, IMPERIAL COLLEGE, 180 QUEEN'S GATE, LONDON SW7 2AZ,
UK

E-mail address: k.buzzard@imperial.ac.uk

DEPARTMENT OF MATHEMATICS, BRANDEIS UNIVERSITY, WALTHAM, MA 02454, USA

E-mail address: fdiamond@math.brandeis.edu

DEPARTMENT OF PURE MATHEMATICS, UNIVERSITY OF SHEFFIELD, SHEFFIELD S3 7RH, UK

E-mail address: A.F.Jarvis@sheffield.ac.uk