On ordinary forms & ordinary Galois representations

Kirti Joshi & Chandrashekhar Khare

1 Introduction

Let $p \geq 5$ be a prime. A well-known conjecture of Serre (see [20]) asserts that any two dimensional irreducible representation

$$\rho : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\bar{\mathbf{F}}_p),$$

which is odd (in the sense that $\det(c) = -1$, where c is complex conjugation), arises from reduction modulo p of the p-adic representation attached to a newform by Deligne (see [3]). In such a situation, we say that ρ is a *modular mod p Galois representation.*

To make this more precise, let us fix once for all an embedding $\iota_p : \bar{\mathbf{Q}} \hookrightarrow \bar{\mathbf{Q}}_p$. This at once provides us with a place of $\bar{\mathbf{Q}}$ lying over p; we will denote this place by $\mathfrak{p}$. The qualitative form of Serre's conjecture predicts that there is a newform f in the space $S_k(\Gamma_0(N), \chi)$ of newforms of weight k (throughout this note we assume that $k \geq 2$), level N and Nebentype χ, such that for any prime ℓ not dividing pN, we have

$$\mathrm{Tr}(\rho(\mathrm{Frob}_\ell)) = a_\ell \bmod \mathfrak{p}$$

and $\det(\rho(\mathrm{Frob}_\ell)) = \chi(\ell)\ell^{k-1} \bmod \mathfrak{p}$, where a_ℓ is the eigenvalue of the Hecke operator T_ℓ, for $\ell \neq p$. In fact, Serre made precise certain minimal invariants $N(\rho), k(\rho), \varepsilon(\rho)$, where $\varepsilon(\rho)$ is a primitive character of conductor dividing $N(\rho)$, such that there is a newform f of weight $k(\rho)$, level $N(\rho)$ and nebentype $\varepsilon(\rho)$, which gives rise to the representation ρ. We will call these the *Serre invariants* of ρ. We note that $N(\rho)$ is prime to p, $2 \leq k(\rho) \leq p^2 - 1$ and $\varepsilon(\rho)$ is a character of conductor dividing $N(\rho)$ and order prime to p; we refer the reader to [20] for the precise definitions of these invariants. As a consequence of the work of Mazur, Ribet, Carayol, Gross, Edixhoven and Diamond (see [5]) one now knows that if ρ is modular, then it does indeed arise from a newform with the corresponding *Serre invariants*.

But there are infinitely many distinct newforms that give rise to the same modular mod p Galois representation. We say that such forms are *congruent*. We emphasise that a congruence in our sense means that the Fourier coefficients of congruent newforms at almost all primes are congruent mod $\mathfrak{p}$.

In this note we prove results linking the behaviour of congruent newforms. In Section 2 we relate the mod p ordinarity of a modular mod p Galois representation as above to the ordinarity (or the lack of it) of the forms which gives rise to it (see Theorems 2.2, 2.5, 2.6). In section 3 we state results about the local component at p of an automorphic representation and the local representation at p of the p-adic representation associated to the form. These results answer what were posed as questions in earlier versions of this article: the answers are available thanks to [18].

This note was written in 1995. In spite of it not having been published till now, as it still gets occasionally referred to as a preprint ([9] for a recent instance), we felt encouraged to rescue it from the limbo.

We thank H. Hida, Dipendra Prasad and J. Tilouine for conversations.

2 Mod p representations

Recall that we have fixed an embedding $\iota_p : \bar{\mathbf{Q}} \hookrightarrow \bar{\mathbf{Q}}_p$. This provides us with a place $\mathfrak{p}$ lying over p in $\bar{\mathbf{Q}}$. Let D_p be the decomposition group of p, with respect to the place $\mathfrak{p}$, in $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$; let I_p be the inertia subgroup of D_p. If f is a newform, we will frequently use the symbol $\pi(f)$ to denote the corresponding automorphic representation and $\pi_p(f)$ for its p-component.

We begin by recalling:

Definition: Let $\rho : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\bar{\mathbf{F}}_p)$ be an irreducible Galois representation. We say that ρ is ordinary at p if $\rho|_{D_p}$ is reducible and has an unramified one-dimensional quotient.

Definition: A newform of level N, p not dividing N (resp. p dividing N) on $\Gamma_1(N)$ is said to be ordinary at p if the eigenvalue of T_p is a $\mathfrak{p}$-adic unit (resp. the eigen value of U_p on f is a $\mathfrak{p}$-adic unit).

Remark: If a newform $f \in S_k(\Gamma_1(N))$, with N prime to p, is ordinary at p, then from f we can create in the usual way 2 ordinary p-old forms $f', f'' \in S_k(\Gamma_1(Np))$ which have the same eigenvalues as f outside p by the usual recipe. We recall the recipe. If α, β are the roots of the Euler factor at p of $L(f, s)$, then we may assume, without loss of generality, that α is a $\mathfrak{p}$-unit. Then $f'(z) = f(z) - \beta f(pz)$, $f''(z) = f(z) - \alpha f(pz)$ are the required forms whose eigenvalues under U_p are α and β respectively.

The following result of Deligne, Hida, Mazur-Wiles and Wiles (see Section 12 of [8] for instance), which is well-known, is the starting point for our note.

Theorem 2.1 *Let $f \in S_k(\Gamma_1(N))$ be an Hecke eigen form which is a new form. Assume that the eigen value of T_p (or U_p) is a p-adic unit. Also assume that the mod p representation $\rho_{f,p}$ is irreducible. Then $\rho_{f,p}|_{D_p}$ is ordinary at p.*

This motivates the following question.

Question 1 *Suppose ρ is an irreducible representation. Assume that ρ is ordinary and is modular. Then is there at least one ordinary modular form which gives rise to ρ?*

The following theorem provides a reasonable answer to this question (part 1 of the following theorem can also be found in Theorem 6.4 of [5]).

Theorem 2.2 *Assume that we are given a modular mod p Galois representation ρ as above.*

1. *If ρ is ordinary at p then there is one (and hence infinitely many) ordinary newform(s) which give rise to ρ.*

2. *If ρ is not ordinary, then no ordinary form can give rise to it.*

3. *Given a ρ as above, there are infinitely many distinct newforms which are non-ordinary at p which give rise to ρ. Moreover these may be chosen to be either principal series or supercuspidal at p.*

Remark: If f gives rise to ρ then one can twist f by a character of p-power conductor and p-power order to get non-ordinary forms which give rise to ρ. But using the theorem stated in the introduction of [13], we can get non-ordinary forms which give rise to ρ in other less obvious ways.

Proof: We assume that ρ is modular and ordinary at p, i.e

$$\rho|_{I_p} \sim \begin{pmatrix} \chi & * \\ 0 & 1 \end{pmatrix},$$

where χ is a power of the mod p cyclotomic character ω (recall that $\omega : \mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p) \to \mathbf{F}_p^*$ is defined by $\sigma(\zeta_p) = \zeta_p^{\omega(\sigma)}$, where ζ_p is a primitive pth root of unity). Thus $\chi = \omega^a$ for some integer a. We normalise a to be between 1 and $p-1$. Then Serre defines:

$$k(\rho) = \begin{cases} 1+a & \text{if } a \neq 1 \\ 2 & \text{if } a = 1 \text{ and } \rho \text{ is peu ramifiée at } p \\ p+1 & \text{if } a = 1 \text{ and } \rho \text{ is très ramifiée at } p \end{cases}$$

As a consequence of Edixhoven's work (see [6]), it is known that ρ arises from a form of weight $k(\rho)$ on $\Gamma_1(N)$ for some N such that $(N,p)=1$. From the above we see that $2 \leq k(\rho) \leq p+1$. We now need to recall theorems of Deligne and Fontaine (see Theorem 2.5 and 2.6 of [6] respectively).

Theorem 2.3 (Deligne) *Let f be a newform of level N prime to p and weight k, with $2 \leq k \leq p+1$. If $a_p \not\equiv 0 \bmod \mathfrak{p}$ then $\rho|_{D_p}$ is reducible and has an unramified quotient of dimension one on which the Frobenius at p, Frob_p, acts by multiplication by the unique root of $x^2 - a_p(f)x + p$ that is a $\mathfrak{p}$-unit and where $a_p(f)$ is the pth Fourier coefficient of f.*

Theorem 2.4 (Fontaine) *With the same hypothesis as the above theorem, if $a_p \equiv 0 \bmod \mathfrak{p}$, then $\rho|_{D_p}$ is irreducible.*

Thus it follows from these two theorems that any form $f \in S_{k(\rho)}(\Gamma_1(N))$ which gives rise to ρ is ordinary. After this the existence of infinitely many ordinary newforms which give rise to ρ follows from the work of Hida (see [12]).

For the second assertion, we just need remark that this is a result of Deligne, Hida and Mazur-Wiles quoted above.

For the third assertion, we just note that ρ arises from a newform in $S_{k(\rho)}(\Gamma_1(N(\rho))$. Then by the main theorem of [13] (there is a restriction on the determinant of ρ in that paper which is easily seen to be superfluous in the present application of the main theorem of that paper: [15] is a more recent reference), we see that ρ arises from a newform in $S_2(N(\rho)p^r, \varepsilon(\rho))^{p-new}$ for all $r \geq 3$. Any such form is supercuspidal at p if r is odd (see Remark 4.25 of [10]). If r is even then the form in the p-new part of $S_2(N(\rho)p^r, \varepsilon(\rho))$ which gives rise to ρ can be chosen to be principal series at p. This is an application of Carayol's lemma (see [13], Remarks 11.2 and 11.3). From this the third assertion of the theorem follows from the result that a form in the p-new part of $S_2(\Gamma_0(N(\rho)p^r), \chi)$ with $\mathrm{cond}(\chi) = p^s$ and $s < r$ ($r > 1$) has p-eigenvalue zero (see [16]). $\square$

We now take up another aspect of Question 1. We have seen in the above theorem that if we start with a mod p modular representation ρ which is ordinary, then any form of minimal weight and level prime to p which gives rise to ρ is ordinary. In the theorem which follows we prove a similar result about the forms of weight two and minimal p-power level which give rise to ρ.

Theorem 2.5 *Let ρ be an irreducible modular mod p representation which is ordinary at p. Then ρ arises from a form $f \in S_2(\Gamma_1(N(\rho)p))$ with $N(\rho)$ prime to p. Further any form in $S_2(\Gamma_1(Np))$ (for any N which satisfies $(N,p) = 1$) which gives rise to ρ is ordinary at p if $k(\rho) \neq 2$; otherwise the form in $S_2(\Gamma_1(N))$ is ordinary while there exists a p-old form in $S_2(\Gamma_1(Np))$ which is not ordinary and which gives rise to ρ.*

Proof: That ρ arises from $S_2(\Gamma_1(N(\rho)p))$ follows from the level lowering results of Mazur, Ribet, Diamond and Carayol and Edixhoven's proof of the weight part of Serre's conjecture upon using the result (see [1]) that a representation ρ which arises from $S_k(\Gamma_1(N(\rho)))$ ($2 \leq k \leq p+1$) also arises from $S_2(\Gamma_1(N(\rho)p))$.

Suppose first that $\rho|_{I_p} \sim \begin{pmatrix} \omega & * \\ 0 & 1 \end{pmatrix}$, where ω is the mod p cyclotomic character. If ρ is finite at p then we know that ρ arises from a form f in $S_2(\Gamma_1(N))$ (for some N prime to p, this is a consequence of Mazur's principle cf. [19]) else ρ arises from a form in $S_2(\Gamma_1(N) \cap \Gamma_0(p))^{p-new}$. We see easily from Theorem 2.5 and Theorem 2.6 of [6], that a newform f in $S_2(\Gamma_1(N))$ which gives to ρ is ordinary at p; while it is easily seen that from such an f we can create a non-ordinary p-old form in $S_2(\Gamma_1(Np))$ which gives rise to ρ. If ρ arises from $S_2(\Gamma_1(N) \cap \Gamma_0(p))^{p-new}$ (with $(N,p)=1$) then we use the well-known result that a form in this space has p-th eigen value such that its square is $\varepsilon(p)$, where ε is the nebentype and is consequently ordinary at p.

Now suppose that $\rho|_{I_p} \sim \begin{pmatrix} \omega^a & * \\ 0 & 1 \end{pmatrix}$ with $a \not\equiv 1 \bmod p-1$. Then Proposition 8.13 of [8] says that we have a Hecke equivariant isomorphism

$$\overline{L}(k-2) \simeq M_k^0 \oplus M_{p+3-k}^0[k-2]$$

for $3 \leq k \leq p$, where we use the notation of *loc. cit.* Namely, $\overline{L}(k-2)$ is the space of mod p cusp forms on $\Gamma_1(Np)$ on which $a \in (\mathbf{Z}/p\mathbf{Z})^*$ acts by a^{k-2}, i.e., the $k-2$nd power of the identity character, and M_k^0 (resp., $M_{p+3-k}^0[k-2]$) is the space of mod p cusp forms on $\Gamma_1(N)$ of weight k (resp., the mod p space of cusp forms on $\Gamma_1(N)$ and weight $p+3-k$ with the Hecke action twisted by the $k-2$nd power of the identity character as in the discussion before *loc. cit.*). Now on the one hand irreducible mod p representations which arise from $M_{p+3-k}^0[k-2]$ are never ordinary, as such representations which are reducible on restriction to D_p are of the form

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

On the other hand as we have seen in the proof of Theorem 2.2, it follows from Theorems 2.3 and 2.4, that a newform in $f \in S_k(\Gamma_1(N))$ ($(N,p)=1, 2 \leq k \leq p+1$) gives rise to an irreducible mod p representation that is ordinary at p if and only if f is ordinary.

□

Remark: This result is essentially best possible as there are forms in $S_2(\Gamma_0(Np^2))^{p-new}$ (which can be even supercuspidal at p: see Remark 11.1 of [13]) which give rise to ordinary mod p representations though any form in this space has p^{th} eigenvalue zero. This may be seen from Theorem 3 of [13], where it is shown that if a mod p representation arises from $S_2(\Gamma_0(N))$, then it also arises from the p-new part of $S_2(\Gamma_0(Np^2))$: see also [15].

We prove a result using the methods here that responds to a question that was posed to one of us by Dipendra Prasad

Theorem 2.6 *If two newforms f, f' in $S_k(\Gamma_0(N))$ with N prime to p and $1 \leq k \leq p+1$ give rise to the same irreducible mod $\mathfrak{p}$ representation, then their pth Fourier coefficients are also congruent.*

Proof: The weight 1 case is easy as then the mod $\mathfrak{p}$ representations corresponding to f, f' are unramified at p and the pth Fourier coefficients are recovered as the traces of Frob_p. So we assume that $2 \leq k \leq p+1$. We claim that the pth Fourier coefficients $a_p(f)$ and $a_p(f')$ of f and f' are either both divisible by $\mathfrak{p}$ or they are both units at $\mathfrak{p}$. This claim follows from Theorems 2.3 and 2.4. Then as $k \geq 2$ at most one of the roots of $x^2 - a_p(f)x + p^{k-1}$ (resp., $x^2 - a_p(f')x + p^{k-1}$) is a unit at $\mathfrak{p}$ and if one of them is a unit it arises as the eigenvalue of Frob_p acting on the unique unramified quotient of the mod $\mathfrak{p}$ representation associated to f (resp, f'). As we are assuming that the mod $\mathfrak{p}$ representations associated to f, f' are isomorphic, and hence in particular their restrictions to D_p are isomorphic, we have completed the proof. $\square$

Remark: The above theorem is false when we do not have hypotheses on levels as follows from the first remark of this section. This issue is related to the results of [8] about *companion forms*, and it is also this failure that results in the *twin form* phenomena of [11]. We do not know what happens for weights $> p+1$ and levels prime to p.

3 p-adic representations

3.1 p-adic ordinarity

Now we turn to the p-adic analogue of the above question. At the time we wrote this note in 1995 we could answer these p-adic analogues in some cases using the results of Wiles. But now it is indeed possible to give clean answers as a consequence of the work of [18] (see also [17]).

To fix notations, we work with a ring $\mathcal{O}_p$ that is the ring of integers of a finite extension of $\mathbf{Q}_p$, which we will assume to be large enough so that the eigen values of Hecke operators of the form in question lie in it. Typically, we can take this to be the ring of integers in the completion of the coefficient field E_f of f along the valuation given by $\mathfrak{p}$. We now recall the definition of ordinarity.

Definition: Let $\sigma : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathcal{O}_p)$ be an absolutely irreducible Galois representation. We say that it is ordinary at p if $\sigma|_{D_p}$ is reducible and has an unramified one-dimensional quotient.

Theorem 3.1 *Let $\sigma : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \to GL_2(\mathcal{O}_p)$ be the $\mathfrak{p}$-adic representation attached to a newform f such that the residual representation is absolutely irreducible and such that σ is ordinary at p. Then f is ordinary.*

Theorem 3.2 *Let f be a newform such that the corresponding automorphic representation $\pi_p(f)$ is supercuspidal and let σ be the p-adic representation associated to f. Then $\sigma|_{D_p}$ is irreducible.*

Proof: The proofs of both the theorems follow from results in [18]. For Theorem 3.1 see Proposition 3.6 of [17]. Theorem 3.2 follows from the main theorem of [18] and the fact that the restriction of the Weil-Deligne parameter of a supercuspidal representation of $GL_2(\mathbf{Q}_p)$ to the Weil group of $\mathbf{Q}_p$ is irreducible. □

Remark: As noted above it is also possible to give a different proof in many cases using the theorems of the type proven by Wiles (see [23]) identifying ordinary deformation rings and ordinary Hecke rings of fixed tame level, under some technical conditions.

3.2 Images of p-adic representations

One can also ask for more detailed information about the local image at p, $\sigma|_{D_p}$, of the p-adic representation σ associated to a newform f, in terms of $\pi_p(f)$ in general. If f is ordinary, then by Deligne's theorem we have a good answer, though we do not know if this representation can ever be semisimple upon restriction to an open subgroup of the inertia group. We have the following result in the weight 2 case whose argument was pointed out to us by Dipendra Prasad:

Proposition 1 *Let f be a non-CM newform of level prime to p, weight 2, and is ordinary at $\mathfrak{p}$. Then the corresponding $\mathfrak{p}$-adic representation σ associated to f is non-semisimple when restricted to any open subgroup of D_p.*

Proof: This follows from the theory of Serre-Tate liftings. Namely from Theorem 2 of A.2.3 of Chapter IV of [21], assuming the contrary leads to the conclusion that f has CM. □

The following result is a simple consequence of Fontaine's theory (see [7]) but seems worth spelling out as we find the result striking (see [22] for a much more extensive study of p-adic representations that arise from elliptic curves over $\mathbf{Q}_p$).

Theorem 3.3 *If $E_{/\mathbf{Q}_p}$ is an elliptic curve with good supersingular reduction. Let V_p the representation of the Galois group $G = \mathrm{Gal}(\bar{\mathbf{Q}}_p/\mathbf{Q}_p)$ on $V_p = H^1_{et}(E \otimes \bar{\mathbf{Q}}_p, \mathbf{Q}_p)$. The image of G in $GL(V_p)$ is dihedral, i.e., all supersingular elliptic curves over $\mathbf{Q}_p$ have formal CM.*

Proof: Let E be an elliptic curve with good supersingular reduction over $\mathbf{Q}_p$. We choose a model for it over $\mathbf{Z}_p$ will write E_0 for the special fibre of this model. What is being asserted here is essentially independent of the choice of the integral model.

Fontaine's theory provides a complete description of V_p in terms of the crystalline cohomology $H^1_{cris}(E_0/\mathbf{Z}_p)$ of the special fibre E_0 together with a Frobenius map and a Hodge filtration arising from comparison of $H^1_{cris}(E_0/\mathbf{Z}_p)$ and the de Rham cohomology of $E/\mathbf{Q}_p$. Let $V_{dr} = H^1_{dR}(E/\mathbf{Q}_p)$, together with its Hodge filtration $F^1 H^1_{dR}(E/\mathbf{Q}_p) \subset H^1_{dR}(E/\mathbf{Q}_p)$. Let$V_{cris} = H^1_{cris}(E_0/\mathbf{Z}_p) \otimes \mathbf{Q}_p$. This comes equipped with a Frobenius automorphism (this is because we are over $\mathbf{Q}_p$) $\phi : V_{cris} \to V_{cris}$. By a well-known theorem of Berthelot, there is a canonical $V_{dr} \simeq V_{cris}$.

By [7] we know that the G-representation V_p is completely determined by V_{cris}, ϕ and the Hodge filtration, and in particular $\mathrm{End}_G(V_p)$ (as a Galois module) is the same as the endomorphism algebra of the filtered ϕ-module V_{cris}. So we now compute the endomorphisms of the filtered ϕ-module V_{cris}. Because our curve has good supersingular reduction and because we are over $\mathbf{Q}_p$ the characteristic polynomial of ϕ is $X^2 + p$, more over ϕ is semi-simple.

Further we may assume without loss of generality that ϕ is given by the matrix

$$\phi = \begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix}$$

for some basis e_1, e_2 of V_{cris}. The matrix of ϕ with respect to any other basis e_1', e_2' is then of the form $A\phi A^{-1}$ for a suitable $A \in GL_2(\mathbf{Q}_p)$.

Note that since our curve E_0 is defined over $\mathbf{F}_p$ and is supersingular, not all its endomorphisms are defined over $\mathbf{F}_p$. All the endomorphisms of E_0 become visible over $\mathbf{F}_{p^2}$. The key point is the following elementary fact that the endomorphisms of the pair (V'_{cris}, ϕ') is a quaternion algebra ramified at p, ∞ given explicitly as $\begin{pmatrix} a & b \\ pb^\sigma & a^\sigma \end{pmatrix}$. From this by a simple calculation that we omit it follows that the endomorphisms of the filtered module (V_{cris}, ϕ) which are defined over $\mathbf{Q}_p$ are the scalars (we do a more involved calculation of the same type below).

We pass to $\mathbf{F}_{p^2}$ to do the main calculation of endomorphisms of filtered modules which shows that the endomorphisms of V_p $(\otimes \mathbf{Q}_p)$ considered as a module for the Galois group of $\mathbf{Q}_{p^2}$, the unramified quadratic extension of $\mathbf{Q}_p$, are $\mathbf{Q}_{p^2}$. It is easy to verify (using for instance the proper base change theorem) that the crystalline cohomology of the curve over $\mathbf{F}_{p^2}$ can be obtained from the curve over $\mathbf{F}_p$ as follows: the underlying $\mathbf{Q}_{p^2}$-vector spaces is

$$V'_{cris} = \mathbf{Q}_{p^2} \otimes_{\mathbf{Q}_p} V_{cris},$$

we have to define the Frobenius on V'_{cris}. This is done in the obvious way:

$$\phi' : V'_{cris} \to V'_{cris}$$

is defined by

$$\phi'(x \otimes v) = \sigma(x) \otimes \phi(v),$$

where $\phi : V_{cris} \to V_{cris}$ is the Frobenius on V_{cris} and $\sigma : \mathbf{Q}_{p^2} \to \mathbf{Q}_{p^2}$ is the non-trivial Galois automorphism of $\mathbf{Q}_{p^2}/\mathbf{Q}_p$. In particular: ϕ' is σ-semilinear automorphism (hence it is $\mathbf{Q}_p$-linear). Also note that Fontaine's comparison theorem is compatible with this base change as B_{cris} is a $\mathbf{Q}_p^{nr}$-algebra.

Now one reduces to doing some elementary semilinear algebra. We want to compute the endomorphisms of V'_{cris} as a filtered ϕ'-module. An endomorphism of such data is a linear map of $\mathbf{Q}_{p^2}$-vector spaces, which commutes with the Frobenius ϕ' and preserve the filtration. To compute explicitly it is convenient do our calculations for a particular form of the Frobenius:

$$\phi : V \to V$$

given by the matrix

$$\phi = \begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix}$$

Notice that ϕ' is also given by the matrix above for ϕ (merely extend the basis of V to V'). But now ϕ' is σ-semilinear: so on the coefficients of the basis vectors σ will operate. Let $\tau : V' \to V'$ be any endomorphism of V'. We may assume without loss of generality that τ preserves our basis vector e_1. So it is upper triangular. Thus we can suppose $\tau = \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix}$, with respect to our basis. The condition that $\phi'\tau = \tau\phi'$ means that the matrices corresponding to them σ-commute, in symbols:

$$\begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -p & 0 \end{pmatrix} \begin{pmatrix} \alpha^\sigma & \beta^\sigma \\ 0 & \delta^\sigma \end{pmatrix}.$$

This gives us the relations: $\delta = \alpha^\sigma$ and $\beta = 0$. So any τ which commutes with ϕ' and which preserves the basis e_1, e_2 must be of the form

$$\tau = \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^\sigma \end{pmatrix}$$

for some $\alpha \in \mathbf{Q}_{p^2}$.

Now to recover results for our filtration basis e'_1, e'_2 we note that if $\tau\phi' = \phi'\tau$ for the above basis, we have the identity

$$(A\tau A^{-1})(A\phi' A^{-1}) = (A\phi' A^{-1})(A\tau^\sigma A^{-1}),$$

which says, as $A^\sigma = A$, that $A\tau A^{-1}$ σ-commutes with $A\phi' A^{-1}$ if τ σ-commutes with ϕ' (with respect to the new basis).

So we see that if we restrict our Galois representation to $\mathbf{Q}_{p^2}$, then the algebra of endomorphisms of the Tate module of our curve E is isomorphic to the two dimensional $\mathbf{Q}_p$ vector-space $\mathbf{Q}_{p^2}$. By a standard argument using the double commutant theorem or more directly one deduces that the Lie algebra of the image of G (and more generally of any open subgroup of finite index) is toral. Hence by the irreducibility of the the representation V_p that we saw earlier, we conclude that the image of G is dihedral. □

Remark: A more direct argument using formal groups to prove this result was given by Dipendra Prasad, and is as follows. The formal group of an elliptic curve over $\mathbf{Q}_p$ with good supersingular reduction is a height 2 formal group which is a Lubin-Tate formal group over the quadratic unramified extension of $\mathbf{Q}_p$. Hence from the Lubin-Tate theory, the maximal compact subring of this quadratic unramified extension operates on the formal group, and thus the elliptic curve has formal CM.

References

[1] A. Ash and G. Stevens. Modular forms in characteristic ℓ and special values of their L-functions. *Duke Math. J.*, 53:849–868, 1986.

[2] P. Deligne. Letter from Deligne to Serre, May 28th, 1974. Unpublished.

[3] P. Deligne. Formes modulaires et représentations ℓ-adiques. *Sém. Bourbaki*, 355, 1968/69.

[4] P. Deligne and J.-P. Serre Formes modulaires de poids 1. Ann. Sci. Ec. Norm. Sup,ivi, ser. 7, 1974.

[5] F. Diamond. The refined conjectures of Serre. Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), 22–37.

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

[7] J.-M. Fontaine. Représentations p-adiques semi-stable Astérisque, 223:113-184, 1994.

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

[9] F. Gouvea Deformations of Galois representations. to appear in Park City Mathematics Institute Proceedings, 1999.

[10] S. Gelbart. *Automorphic forms on adele groups.* Number 83 in Annals of Math. Studies. Princeton University, 1975.

[11] F. Gouvêa and B. Mazur. Families of modular eigenforms. *Math. of Comp.*, 58:793-805, 1992.

[12] H. Hida. Galois representations in $GL_2(\mathbf{Z}_p[[X]])$ attached to ordinary cusp forms. *Invent. Math.*, 85:545–613, 1986.

[13] C. Khare. Congruences between cusp forms: the (p, p) case. Duke Math. J. 80 (1995), 31–68.

[14] C. Khare. A local analysis of congruences in the (p, p) case: Part I. Compositio Math. 112 (1998), 363–376.

[15] C. Khare. A local analysis of congruences in the (p, p) case: Part II. *Invent. Math.*, 143 (2001), 129-155

[16] W. Li. New forms and functional equations. *Math. Ann.*, 212:285–315, 1975.

[17] A. Mokrane. Quelques remarques sur l'ordinarité. Journal of Number Theory 73 (1998), 162–181.

[18] T. Saito. Modular forms and p-adic Hodge theory. Invent. Math. 129 (1997), 607–620.

[19] K. Ribet. On modular representations of Gal$(\bar{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. *Invent. Math.*, 100:431–476, 1990.

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

[21] J.-P. Serre. *Abelian ℓ-adic representations and elliptic curves.* Addison-Wesley, 1989.

[22] Maja Volkov. Les représentations ℓ-adiques associeés aux courbes elliptiques sur $\mathbf{Q}_p$. preprint.

[23] A. Wiles. Modular elliptic curves and Fermat's last theorem. Preprint.

Addresses of the authors: School of Mathematics, TIFR, Homi Bhabha Road,
Mumbai 400 005, INDIA. e-mail address: kirti@math.tifr.res.in, shekhar@math.tifr.res.in