Two-dimensional representations in the arithmetic of modular curves

B. Mazur K. A. Ribet

In the theory of automorphic representations of a reductive algebraic group G over a number field K, it is broadly — but not always — true that irreducible representations occurring in $L^2(G_{\mathbf{A}}/G_K)$ occur with multiplicity one. In a *classical special case* ($G = \mathbf{GL}(2)$, $K = \mathbf{Q}$, and where we restrict attention to automorphic representations which are holomorphic, cuspidal, and of weight 2), the Galois-theoretic counterpart of the above "multiplicity one phenomenon" is the assertion that given a newform of the above type, of level N, the (two-dimensional p-adic) $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$-representation associated to it occurs *with multiplicity one* in the p-adic Tate module of $J_1(N)$.

For some important arithmetic applications, however, one is led to search for criteria guaranteeing certain analogues of the above "multiplicity one phenomenon" valid for the mod p Galois representations associated to newforms. The "mod p multiplicity" questions are somewhat more delicate than their p-adic counterparts. Indeed, to our knowledge, the main cases where the mod p Galois representation questions have been treated seriously so far are for cuspidal newforms of weight two which are either unramified at p [20, 30] or ordinary and nonspecial at p [25, 43].

The present article concerns itself with a "missing p-ordinary case," one for which the newform is "special" at p.[1] We assume, more precisely, that the level of the newform is divisible by p but not by p^2, and also that the Nebentypus character of the form is trivial. (Our method might also treat the more general case in which the character is unramified at p, but possibly non-trivial.) For the case where the character is ramified at p, see [12].

[1] We also require that the associated mod p Galois representation be absolutely irreducible, avoiding the important, but much more difficult, case of *Eisenstein primes* [20, 24].

This case arises in the second author's article [30] on Serre's conjectures. Assume that p is an odd prime, and suppose that ρ is an irreducible mod p representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ which arises from the space of weight-2 modular forms on $\Gamma_o(M)$. (We then say that ρ is *modular of level* M.) Assume that $\ell \neq p$ is a prime factor of M for which ρ is unramified at ℓ. Then Serre's conjectures [37] predict that ρ is modular of level M_o, where M_o is the prime-to-ℓ part of M. This statement was proved by the first author [22] in case ℓ "exactly divides M" (i.e., $M_o = M/\ell$) and the congruence $\ell \equiv 1 \bmod p$ is *not* satisfied. (See [30], Theorem 6.1.) It was proved by the second author if ℓ exactly divides M and the newform giving ρ is unramified at p, i.e., p is prime to M ([30], Theorem 8.2). The methods of [30] show, more generally, that ρ is modular of level M_o whenever ℓ exactly divides M and ρ occurs with multiplicity one in the Jacobian $J_o(M)$. This motivated our interest in the mod p multiplicity one question for Galois representations.

The mod p multiplicity-one question for Galois representations has an intriguing, and relatively complicated, answer for twisted forms of $\mathbf{GL}(2)$ [32]. It would be quite interesting to have even a conjectural picture telling us what to expect for multiplicities of mod p Galois representations in a more general context.

We would like to thank Bas Edixhoven for enlightening conversations on subjects related to this article and for detailed comments on our preliminary versions. We also thank the IHES for providing the congenial setting in which much of this work was done.

Contents

1 Introduction and statement of the main theorem 217
1.1 The representations V_φ 217
1.2 Questions of multiplicity 219
1.3 mod p Galois representations ρ and homomorphisms φ . . . 220
2 Admissible models and admissible morphisms 224
3 The graph S 228
4 $\mathrm{Pic}^o(X_{/\mathcal{O}})$ 230
5 Semi-stable filtrations 231
6 Rosenlicht differentials 234
7 Regular differentials on $X_{/\mathcal{O}}$ 237
8 Admissible correspondences 238
9 Local admissible data 239
10 Global admissible data 241
11 Modular curves and Hecke operators 243
12 Admissible data coming from modular curves 246
13 Higher multiplicities 249

1 Introduction and statement of the main theorem

1.1 The representations V_φ

Let M be a positive integer. Let $\Gamma_o(M)$ be (as usual) the subgroup of $\mathbf{SL}(2,\mathbf{Z})$ which consists of matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}(2,\mathbf{Z})$ with $c \equiv 0 \pmod{M}$. Let $X_o(M)$ be the associated modular curve over $\mathbf{Q}$. Finally, let T_n for $n \geq 1$ denote the standard Hecke correspondences on $X_o(M)$. (See, for example, [24], Chapter 2, §5 for a description of the Hecke operators T_q for q prime. When q divides M, our operator T_q is the "Atkin operator" denoted U_q in [24].)

These operators induce endomorphisms on the space $S_2(\Gamma_o(M))$ of weight-2 cusp forms on the group $\Gamma_o(M)$ and on the Jacobian

$$J = J_o(M) = \mathrm{Pic}^o(X_o(M))$$

of $X_o(M)$. We write simply T_n for each of these endomorphisms. (The endomorphism T_n of $J_o(M)$ is denoted T_n^* in [18].) The subrings of $\mathrm{End}(J_o(M))$ and of $\mathrm{End}(S_2(\Gamma_o(M)))$ which these operators generate are the "same." More precisely, the faithful operation of $\mathrm{End}(J_o(M))$ on $S_2(\Gamma_o(M))$ (coming from the fact that this latter space is the cotangent space of the abelian variety dual to $J_o(M)$) maps the endomorphism labeled T_n of $J_o(M)$ to the endomorphism of $S_2(\Gamma_o(M))$ labeled T_n. We let $\mathbf{T}_M$ be the subring of $\mathrm{End}(J_o(M))$

generated by the T_n, viewing this ring, when convenient, as operating on $S_2(\Gamma_o(M))$.

Let $\varphi : \mathbf{T}_M \to \overline{\mathbf{F}}_p$ be a ring homomorphism. The kernel of φ is a maximal ideal $\mathfrak{m} = \mathfrak{m}_\varphi$ of $\mathbf{T}_M$. As usual, we denote by $J[\mathfrak{m}]$ the "kernel of $\mathfrak{m}$ on J," i.e., the intersection of the kernels of all elements of $\mathfrak{m}$ acting on $J(\overline{\mathbf{Q}})$. This subgroup of the finite group $J[p]$ has natural commuting actions of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ and of the residue field $k_\mathfrak{m} = T_M/\mathfrak{m}$. Further, the field $k_\mathfrak{m}$ is embedded in $\overline{\mathbf{F}}_p$ by φ. Let

$$V_\varphi := J[\mathfrak{m}] \otimes_{k_\mathfrak{m}} \overline{\mathbf{F}}_p.$$

Then V_φ is a finite-dimensional (continuous) representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $\overline{\mathbf{F}}_p$. The vector space V_φ is easily seen to be non-zero.

The representations $J[\mathfrak{m}]$ and V_φ may be compared with the canonical two-dimensional representation $\rho_\mathfrak{m}$ of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ which is associated to $\mathfrak{m}$ ([11], Th. 6.7 or [30], Prop. 5.1). Recall that this is the semisimple representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $k_\mathfrak{m}$, unique up to isomorphism, which is unramified outside the set of primes dividing pM and which satisfies

$$\mathrm{trace}(\rho_m(\sigma_r)) \equiv T_r \bmod \mathfrak{m}, \qquad \det(\rho_\mathfrak{m}(\sigma_r)) \equiv r \bmod \mathfrak{m}$$

for all primes r not dividing pM. (Here σ_r is a Frobenius element for r in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$.) We define ρ_φ to be the representation $\rho_\mathfrak{m} \otimes_{k_\mathfrak{m}} \overline{\mathbf{F}}_p$, i.e., the representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ deduced from $\rho_\mathfrak{m}$ by the base change $k_\mathfrak{m} \to \overline{\mathbf{F}}_p$ induced by φ.

These two-dimensional representations are said to be *modular of level M*. More generally, suppose that $\mathbf{F}$ is an algebraic extension of $\mathbf{F}_p$. We say that a semisimple representation $\rho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \mathbf{GL}(2, \mathbf{F})$ is modular of level M if there is an embedding $\iota : \mathbf{F} \hookrightarrow \overline{\mathbf{F}}_p$ so that ρ, when viewed over $\overline{\mathbf{F}}_p$ via ι, is isomorphic to some ρ_φ. It is equivalent to ask that the representation $\rho \otimes_\mathbf{F} \overline{\mathbf{F}}_p$ be of the form ρ_φ for *each* embedding $\iota : \mathbf{F} \hookrightarrow \overline{\mathbf{F}}_p$.

Assume that the two-dimensional representation $\rho_\mathfrak{m}$ is irreducible. Then by the Eichler-Shimura relations, the Cebotarev Density Theorem, and the Brauer-Nesbitt Theorem, one sees that the semisimplification of $J[\mathfrak{m}]$ as a $k_\mathfrak{m}[\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})]$-module is a direct sum of some number of copies of $\rho_\mathfrak{m}$ ([20], Chapter II,§14 or [30], Th. 5.2). Also, the representation ρ_φ is automatically an irreducible representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $\overline{\mathbf{F}}_p$, provided that $p \neq 2$.[2]

[2]According to a recent theorem of Boston, Lenstra and the second author [6], $J[\mathfrak{m}]$ is semisimple whenever ρ_φ is irreducible over $\overline{\mathbf{F}}_p$.

1.2 Questions of multiplicity

Definition 1 The *multiplicity* of $\rho_{\mathfrak{m}}$ in the representation $J[\mathfrak{m}]$ is the multiplicity of $\rho_{\mathfrak{m}}$ in the semisimplification of $J[\mathfrak{m}]$. We denote this integer by $\mu_{\mathfrak{m}}$ or μ_{φ}. We have $\mu_{\varphi} = \dim V_{\varphi}/2$.

The multiplicity $\mu_{\mathfrak{m}}$ is "typically" equal to 1. To cite the simplest possible example, take $M = 11$. Then $J_o(11)$ is an elliptic curve, $\mathbf{T} = \mathbf{Z}$, and the ideals $\mathfrak{m}$ are the prime ideals (p) of $\mathbf{Z}$. The kernel $J_o(11)[p]$ is then an $\mathbf{F}_p$-vector space of dimension two. In [20], the first author showed more generally that $\mu_{\mathfrak{m}} = 1$ when M is a *prime*, except perhaps in a small number of special situations when $p = 2$. (In these special situations, no example has been found where $\mu_{\mathfrak{m}} \neq 1$.) In [30] (Th. 5.2b), the second author employed the techniques of [20] to prove a theorem valid when M is not necessarily prime, but p does not divide $2M$.

MAIN THEOREM *Let $M = pN$, where N is prime to p. Let $\mathfrak{m}$ be a maximal ideal of the Hecke ring $\mathbf{T}_M$ with $\mathbf{T}/\mathfrak{m}$ of characteristic p. Suppose that $\rho_{\mathfrak{m}}$ is an absolutely irreducible representation of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Assume further that $\rho_{\mathfrak{m}}$ is not modular of level N. Then $\mu_{\mathfrak{m}} = 1$.*

The absolute irreducibility of $\rho_{\mathfrak{m}}$, is equivalent to the irreducibility of $\rho_{\mathfrak{m}}$ as a representation of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ over $\mathbf{T}/\mathfrak{m}$ whenever p is odd. This follows from the fact that $\rho_{\mathfrak{m}}(c)$, where c is a complex conjugation in $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, then has the distinct eigenvalues $+1$, -1 in $\mathbf{T}/\mathfrak{m}$.

The condition that $\rho_{\mathfrak{m}}$ is not modular of level N may be examined from varied perspectives. Serre conjectured in 1985 that $\rho_{\mathfrak{m}}$ is *finite* at p ([37], p. 189) if and only if $\rho_{\mathfrak{m}}$ is modular of level N ([36], Conjecture C_2, cf. [37]). This conjecture was proved by the first author soon afterwards: see [22], or [30], Theorem 6.1.

The condition may also be expressed in terms of newforms of weight 2. To say that $\rho_{\mathfrak{m}}$ is modular of level pN means, concretely, that it is a mod p representation attached to a weight-2 newform f, having trivial character, whose level divides pN. To say that it is not modular of level N then means that every f giving rise to $\rho_{\mathfrak{m}}$ has level divisible by p. In the language of representation theory, f is "special" at p in the sense that the component at p of the adelic representation of $\mathbf{GL}(2)$ associated to f is a special representation of $\mathbf{GL}(2, \mathbf{Q}_p)$. (See [25] for results in the case of weight-two p-ordinary modular forms which are not special at p.)

Suppose, more generally, that $\mathfrak{m} \subset \mathbf{T}_M$ is a maximal ideal, and assume that ρ_m is absolutely irreducible. What is the multiplicity of ρ_m in $J_o(M)[\mathfrak{m}]$?