ACADEMIC PRESS
Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Number Theory 98 (2003) 329–347
JOURNAL OF Number Theory
http://www.elsevier.com/locate/jnt

Mod pq Galois representations and Serre's conjecture

Chandrashekhar Khare[a,1] and Ian Kiming[b,*]

[a] School of Mathematics, TIFR, Homi Bhabha Road, Mumbai 400 005, India
[b] Department of Mathematics, University of Copenhagen, Universitetsparken 5, DK-2100 Copenhagen Ø, Denmark

Received 6 November 2001; revised 10 May 2002

Abstract

We consider linear representations of the Galois groups of number fields in two different characteristics and examine conditions under which they arise simultaneously from a motive.

1. Introduction

Motives and automorphic forms of arithmetic type give rise to Galois representations that occur in *compatible families*. These compatible families are of p-adic representations (see [8]) with p varying. By reducing such a family mod p one obtains compatible families of mod p representations (see [4]). While the representations that occur in such a p-adic or mod p family are strongly correlated, in a sense each member of the family reveals a new face of the motive. In recent celebrated work of Wiles playing off a pair of Galois representations in different characteristics has been crucial.

In this paper we investigate when a pair of mod p and mod q representations of the absolute Galois group of a number field K simultaneously arises from an *automorphic motive*: we do this in the 1-dimensional (Section 2) and 2-dimensional (Section 3: this time assuming $K = \mathbb{Q}$) cases. In Section 3 we formulate a mod pq

*Corresponding author.
E-mail addresses: shekhar@math.utah.edu (C. Khare), kiming@math.ku.dk (I. Kiming).
[1] Present address: Department of Mathematics, University of Utah, 155 S 1400 E, Salt Lake City, UT 84112-0090, USA

0022-314X/02/$ - see front matter
PII: S0022-314X(02)00043-4

version of Serre's conjecture refining in part the question of Barry Mazur and Ken Ribet in [11] and some of the considerations in [3].

1.1. Notation

Throughout the paper, p and q denote 2 distinct, fixed prime numbers.
We fix the following notation:

K	a finite extension of $\mathbb{Q}$
E	group of global units in K
G_K	the absolute Galois group of K
C_K	the idele class group of K
Σ	the set of embeddings $K \hookrightarrow \bar{\mathbb{Q}}$

By 'Hecke character' of K we shall mean a grossencharacter of type A_0 on C_K.
We fix embeddings $\iota_\infty : \bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$, and for every prime ℓ an embedding $\iota_\ell : \bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_\ell$, and denote by v_ℓ the extension of the ℓ-adic valuation on $\mathbb{Q}_\ell$ to $\bar{\mathbb{Q}}_\ell$. We also fix an isomorphism of the residue field of $\bar{\mathbb{Q}}_\ell$ with $\bar{\mathbb{F}}_\ell$.
Thus, an element $\sigma \in \Sigma$ gives rise to an embedding $K \hookrightarrow \bar{\mathbb{Q}}_\ell$ via composition with ι_ℓ. Abusing notation, with denote again this embedding by σ.
If λ is a finite prime of K of residue characteristic ℓ we denote by

$\mathfrak{p}_\lambda$	maximal ideal of ring of integers in K_λ
k_λ	residue field of λ
U_λ	corresponding unit group

and introduce the subset $\Sigma(\lambda) \subseteq \Sigma$:

$$\Sigma(\lambda) := \{\sigma \in \Sigma \mid v_\ell \circ \sigma \cong \lambda\}.$$

Thus, if $\sigma \in \Sigma(\lambda)$ we have a canonical extension to an embedding $\sigma_\lambda : K_\lambda \hookrightarrow \bar{\mathbb{Q}}_\ell$ inducing an embedding:

$$\bar{\sigma}_\lambda : k_\lambda \hookrightarrow \bar{\mathbb{F}}_\ell.$$

Notice that the sets $\Sigma(\lambda)$ form a partition of Σ when λ runs over the prime divisors of ℓ.

Since we have fixed a prime of $\bar{\mathbb{Q}}$ above λ, we can speak of the inertia group $I_\lambda \leqslant G_K$ at λ. We denote by

$$\theta_\lambda : I_\lambda \to k_\lambda^\times$$

the character (factoring through tame inertia) that gives the action of the Galois group $\mathrm{Gal}(\bar{K}_\lambda/K_\lambda)$ on a $(\#k_\lambda - 1)$st root of a uniformizer of K_λ. Thus, if $\#k_\lambda = \ell^n$

the fundamental characters of level n over K_λ are the n characters:

$$\theta_\lambda^{\ell^i} \quad \text{for } i = 0, \ldots, n-1.$$

We denote by $\tilde{\theta}_\lambda$ the Teichmüller lift of θ_λ, and—as we have fixed an embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{K}_\lambda$—can regard it as taking values in either $\bar{\mathbb{Q}}^\times$, or in $\bar{K}_\lambda^\times$.

In order to reduce the amount of notation, we allow ourselves to use class field theory implicitly. Thus, if $\chi : G_K \to \bar{\mathbb{F}}_\ell^\times$ is a homomorphism we may find occasion to view χ as a homomorphism on C_K.

Generally, if χ is a Hecke character of K and if ℓ is a prime number, there is attached to the pair (χ, ℓ) an ℓ-adic galois representation $\chi_\ell : G_K \to \bar{\mathbb{Q}}_\ell^\times$ satisfying appropriate reciprocity laws (cf. for instance [8,9], or the original construction [14]). The character χ_ℓ lands in the group of units. Reducing 'mod ℓ' we obtain a representation $\bar{\chi}_\ell$:

$$\bar{\chi}_\ell : G_K \to \bar{\mathbb{F}}_\ell^\times.$$

In particular, we use these notations ε_ℓ and $\bar{\varepsilon}_\ell$ if ε is just a finite-order complex character of C_K.

Finally, if x is a complex number, we denote by x^c the complex conjugate of x.

2. One-dimensional mod pq representations

Throughout this section we fix representations $\rho : G_K \to \bar{\mathbb{F}}_p^\times$ and $\rho' : G_K \to \bar{\mathbb{F}}_q^\times$, and we would like to determine when ρ and ρ' arise from one Hecke character simultaneously with respect to the embeddings fixed above. We know of no reasonable notion of finitely many mod p representations with p varying, such as ρ and ρ', being compatible (see [4]) but their arising from a Hecke character (see Section 4 of [4]) is a special circumstance which we will explore below.

2.1. Hecke characters and Galois representations

In this subsection we wish to recall some properties of Hecke characters, in particular properties of their attached mod ℓ Galois representations. We shall follow mainly the exposition of [9, Section 3.4].

2.1.1. Hecke characters

A Hecke character of K is a continuous homomorphism $\chi : C_K \to \mathbb{C}^\times$ whose restriction to the connected component of 1 at infinity has form:

$$x \mapsto \prod_{\sigma \text{ real}} x_\sigma^{n_\sigma} \cdot \prod_{\sigma \text{ complex}} x_\sigma^{n_\sigma} (x_\sigma^c)^{n_{\sigma c}}$$

with integers n_σ, $\sigma \in \Sigma$. We have used σ^c to denote the element of Σ given by $\sigma^c(x) = \sigma(x)^c$.

We can consider the restriction of χ to $U_\lambda \hookrightarrow C_K$ for finite primes λ. As χ is a continuous homomorphism, almost all of these restrictions $\chi \mid_{U_\lambda}$ are trivial and in any case have finite orders and hence conductors. One defines the conductor $\mathfrak{m}$ of χ to be the product of these local conductors.

As in [9], we define for an arbitrary prime λ of K the group $U_{\lambda,\mathfrak{m}}$: If $\mathfrak{m} = \prod_{v \in S} \mathfrak{p}_v^{m_v}$ with S a finite set of finite primes of K, the group $U_{\lambda,\mathfrak{m}}$ is defined to be the connected component of $1 \in K_\lambda^\times$ if λ is infinite, the whole of U_λ if $\lambda \notin S$, and finally the group of units in U_λ of level $\geqslant m_\lambda$ if $\lambda \in S$. We may also define $U_\mathfrak{m}$ as the product of all $U_{\lambda,\mathfrak{m}}$.

The integers n_σ, $\sigma \in \Sigma$, are uniquely determined by χ. We can thus refer to the formal expression $\sum_{\sigma \in \Sigma} n_\sigma \cdot \sigma \in \mathbb{Z}[\Sigma]$ as the ∞-type of χ.

The classification of those elements in $\mathbb{Z}[\Sigma]$ that occur as the ∞-type of *some* Hecke character is known, cf. [8,14], but we shall not need to go into this.

2.1.2. Galois representations attached to Hecke characters

Suppose that χ is a Hecke character of ∞-type $\sum_{\sigma \in \Sigma} n_\sigma \cdot \sigma$ and conductor $\mathfrak{m}$. Let ℓ be a prime number. To χ is attached an ℓ-adic representation χ_ℓ of G_K. The character χ_ℓ takes its values in the group of units of $\bar{\mathbb{Q}}_\ell$, and as we have fixed an isomorphism of the residue field of $\bar{\mathbb{Q}}_\ell$ with $\bar{\mathbb{F}}_\ell$, we can speak of the mod ℓ reduction $\bar{\chi}_\ell$ of χ_ℓ. We shall recall, cf. [9, Section 3.4], the description of χ_ℓ and $\bar{\chi}_\ell$ on inertia groups, i.e. on local units groups if we view these characters as characters on C_K.

Let λ be a finite prime. Define the character ε_λ of U_λ as the restriction $\chi \mid_{U_\lambda}$. Then by construction of χ_ℓ, cf. [9, Section 3,4], we have on U_λ:

$$\chi_\ell(x) := \begin{cases} \varepsilon_\lambda(x) & \text{for } x \in U_\lambda,\ \lambda \nmid \ell, \\ \varepsilon_\lambda(x) \cdot \prod_{\sigma \in \Sigma(\lambda)} \sigma_\lambda(x^{-1})^{-n_\sigma} & \text{for } x \in U_\lambda,\ \lambda \mid \ell. \end{cases}$$

(Notice that there are two different ways of establishing a correspondence between the point of view of [9] and our view of a Hecke character as a character of C_K. We could have changed signs on the n_σ's but would then have to define ε_λ as the *inverse* of the restriction of χ to U_λ.)

Notice, that as a consequence of definitions we have for a totally positive global unit u that

$$\prod_{\lambda \text{ finite}} \varepsilon_\lambda(u) = \prod_{\sigma \in \Sigma} \sigma(u)^{-n_\sigma}.$$

The following lemma reverses this line of reasoning.

Lemma 1. *Suppose that for each finite prime λ of K a continuous character*

$$\varepsilon_\lambda : U_\lambda \to \mathbb{C}^\times$$

is given such that only finitely many ε_λ are non-trivial. Suppose also that integers n_σ, $\sigma \in \Sigma$, are given.

Then there exists a Hecke character χ on C_K of ∞-type $\sum_{\sigma\in\Sigma} n_\sigma \cdot \sigma$ whose restriction to U_λ is ε_λ for all λ if and only if

$$\prod_{\lambda \text{ finite}} \varepsilon_\lambda(u) = \prod_{\sigma\in\Sigma} \sigma(u)^{-n_\sigma}$$

for every totally positive global unit u.

Proof. As we saw above, the condition is necessary.

To prove sufficiency, consider the group

$$U := \prod_{\lambda \text{ finite}} U_\lambda$$

as a compact subgroup of C_K. The ε_λ define a continuous character

$$\varepsilon := \prod_{\lambda \text{ finite}} \varepsilon_\lambda$$

on U. There is an extension χ of ε to a continuous character of C_K. The question is whether there is an extension which has the desired shape on the connected component D_K of 1 in C_K.

Consider first the case where all $n_\sigma = 0$. The question is then whether ε extends to a continuous character of C_K vanishing on the closed subgroup D_K. This will be the case if and only if ε vanishes on the intersection $U \cap D_K$. As this intersection consists precisely of the embeddings into U of totally positive global units, the desired vanishing is implied by the condition we have imposed.

In the general case let $\mathfrak{m}$ be the conductor of ε. A consequence of our hypothesis is then that

$$\prod_{\sigma\in\Sigma} \sigma(u)^{n_\sigma} = 1$$

for every $u \in E_{\mathfrak{m}} := E \cap U_{\mathfrak{m}}$. This is sufficient to ensure the existence of *some* Hecke character χ on C_K with ∞-type $\sum_{\sigma\in\Sigma} n_\sigma \cdot \sigma$. The question is then whether the character $\varepsilon \cdot (\chi \mid_U)^{-1}$ extends to a character of finite order on C_K, and we are reduced to the previous case. $\square$

Returning now to the discussion before the lemma, we find for the mod ℓ reduction $\bar{\chi}_\ell$ of the Galois representation χ_ℓ that

$$\bar{\chi}_\ell(x) = (\varepsilon_\lambda \bmod \ell)(x) \cdot \begin{cases} 1 & \text{for } x \in U_\lambda,\ \lambda \nmid \ell, \\ \prod_{\sigma\in\Sigma(\lambda)} \bar{\sigma}_\lambda((x \bmod \lambda)^{-1})^{-n_\sigma} & \text{for } x \in U_\lambda,\ \lambda \mid \ell. \end{cases}$$

So, we may view this as describing the Galois representation $\bar{\chi}_\ell$ on inertia. Viewing the homomorphisms

$$(x \bmod \lambda) \mapsto \bar{\sigma}_\lambda((x \bmod \lambda)^{-1})$$

as characters on tame inertia above λ, these characters are *fundamental characters* of level n if $\# k_\lambda = \ell^n$, with ℓ the residue characteristic of λ, cf. again [9]. So, for each $\sigma \in \Sigma(\lambda)$ we have a well-defined number $\kappa(\lambda, \sigma) \in \{0, \dots, n-1\}$ such that:

$$\bar{\sigma}_\lambda = \theta_\lambda^{\ell^{\kappa(\lambda,\sigma)}}.$$

Summing up, and viewing $\bar{\chi}_\ell$ as a character on G_K, we have a description of $\bar{\chi}_\ell$ on inertia groups:

$$\bar{\chi}_\ell|_{I_\lambda} = \begin{cases} (\varepsilon_\lambda \bmod \ell) & \text{for } \lambda \nmid \ell \\ (\varepsilon_\lambda \bmod \ell) \cdot \theta_\lambda^{-\sum_{\sigma \in \Sigma(\lambda)} n_\sigma \cdot \ell^{\kappa(\lambda,\sigma)}} & \text{for } \lambda \mid \ell \end{cases}$$

with ε_λ the complex character obtained by restricting χ to U_λ, viewed as a character on I_λ.

2.2. Preliminary lemmas

We begin by disposing off the easy case of *Artin lifts*.

Lemma 2. *Let G be a profinite group and let $\tau : G \to \bar{\mathbb{F}}_p^\times$ and $\tau' : G \to \bar{\mathbb{F}}_q^\times$ be two continuous (the target is given the discrete topology), 1-dimensional characters of G. Then there is a complex character $\varepsilon : G \to \mathbb{C}^\times$ which lifts τ and τ' (w.r.t. the embeddings ι_p and ι_q fixed earlier) if and only if for any two Artin lifts $\tilde{\tau}$ and $\tilde{\tau}'$ of τ and τ' the order of the character $\tilde{\tau}\tilde{\tau}'^{-1}$ divides a power of pq.*

If a lift ε exists it is unique and in fact $\varepsilon = \tilde{\tau}\psi' = \tilde{\tau}'\psi$ if $\tilde{\tau}$ and $\tilde{\tau}'$ are Artin lifts and $\tilde{\tau}\tilde{\tau}'^{-1} = \psi\psi'^{-1}$ with ψ and ψ' characters of p- and q-power order, respectively.

Proof. This follows from the fact that the only roots of unity that have trivial reduction $\bmod\, p$ are those that have order a power of p. □

Lemma 3. *Let G be a profinite group and G' a closed subgroup of finite index. Then for a (finite order, continuous) $\varepsilon' : G' \to \mathbb{C}^\times$ to be the restriction of a (finite order, continuous) character $\varepsilon : G \to \mathbb{C}^\times$ it is necessary and sufficient that $\bar{\varepsilon}'_p$ and $\bar{\varepsilon}'_q$, the reductions of ε' $\bmod\, p$ and $\bmod\, q$, arise by restriction from characters of G.*

Proof. As $\bar{\varepsilon}'_p$ arises by restriction of a $\bmod\, p$ character $\bar{\varepsilon}_p$ of G it follows by choosing any lift of $\bar{\varepsilon}_p$ to a complex character that ε'^{p^α} arises by restriction from G for some non-negative integer α. Similarly ε'^{q^β} arises by restriction from G. Choosing integers a and b such that $ap^\alpha + bq^\beta = 1$ we are done. □

Remark 1. It will be interesting to resolve the following question. Let $\rho : G_K \to \bar{\mathbb{F}}_p^\times$ and $\rho' : G_K \to \bar{\mathbb{F}}_q^\times$ be two continuous 1-dimensional characters of G_K. Let L/K be a finite Galois extension of K such that the restrictions $\rho|_{G_L}$ and $\rho'|_{G_L}$ arise from a Hecke character χ' of L. Then do these restrictions also arise from $\chi \circ \mathrm{Nm}_{L/K}$ for some Hecke character χ of K? The case when χ' is of finite order is dealt with by Lemma 3, and then χ' itself arises by base change from K which certainly will not be true in general.

Lemma 4. *A necessary condition for ρ and ρ' to arise from a Hecke character is that for all primes λ of K not above p and q, and any two Artin lifts $\tilde{\rho}|_{I_\lambda}$ and $\tilde{\rho}'|_{I_\lambda}$ of $\rho|_{I_\lambda}$ and $\rho'|_{I_\lambda}$ the order of the character $\tilde{\rho}|_{I_\lambda}\tilde{\rho}'|_{I_\lambda}^{-1}$ divides a power of pq.*

Proof. This is clear from the construction of p-adic representations from Hecke characters (see [8]) and Lemma 2 (see Section 4 of [4]). The point here is that if χ is a Hecke character and if χ_p is the 1-dimensional p-adic representation of G_K associated to it, then the image of a inertia group at any prime λ not above p is finite and does not depend on the p of the compatible system of p-adic representations that χ gives rise to as long as the residue characteristics of p and ℓ are coprime. $\square$

Lemma 5. *Assume the necessary conditions above. Then there is an Artin character $\varepsilon : G_K \to \mathbb{C}^\times$ such that $\bar{\varepsilon}_p^{-1}\rho$ and $\bar{\varepsilon}_q^{-1}\rho'$ are unramified outside primes above p and q and the infinite places.*

Proof. Let L be the finite abelian extension of K that is the compositum of the fixed fields of the kernels of ρ and ρ'. Let K' be the fixed field of L under the action of all the inertia groups I_v for v a finite place of K not above p or q. As we are assuming the necessary conditions of Lemma 4, we deduce that there are lifts $\tilde{\rho}$ and $\tilde{\rho}'$ of $\rho|_{G_{K'}}$ and $\rho'|_{G_{K'}}$, respectively, such that the order of $\tilde{\rho}\tilde{\rho}'^{-1}$ is of the form $p^\alpha q^\beta$. Then by Lemma 2, there is an Artin character ε' of $G_{K'}$ such that $\bar{\varepsilon}'_p = \rho|_{G_{K'}}$ and $\bar{\varepsilon}'_q = \rho|_{G_{K'}}$. Using Lemma 3, we get an Artin character ε of G_K such that $\bar{\varepsilon}_p = \rho|_{G_{K'}}$ and $\bar{\varepsilon}_q = \rho|_{G_{K'}}$. Now as $\bar{\varepsilon}_p^{-1}\rho|_{G_{K'}}$ and $\bar{\varepsilon}_q^{-1}\rho'|_{G_{K'}}$ are trivial and K'/K is unramified outside primes dividing pq and the infinite places we are done. $\square$

Lemma 6. *If ρ, ρ' as above are unramified outside primes above p and q and the infinite places, then any Hecke character χ that gives rise to both ρ and ρ' is of conductor that divides $p^\alpha q^\beta$ for some non-negative integers α, β. More precisely, the conductor of any Hecke character that gives rise to ρ and ρ' divides $\mathfrak{m} = \prod_{v_i}$ l.c.m. $\{\mathfrak{p}_{v_i}, \mathrm{cond}(\rho'|_{I_{v_i}})\} \prod_{v'_j}$ l.c.m. $\{\mathfrak{p}_{v'_j}, \mathrm{cond}(\rho|_{I_{v'_j}})\}$. Here, the v_i and the v'_j are the places of K above p and q, respectively.*

Proof. This is again clear from the construction of λ-adic representations from Hecke characters (see [8] or the above review in Section 2.1.2) and Lemma 2, by considering the restrictions $\rho|_{I_{v'_j}}$ and $\rho'|_{I_{v_i}}$. $\square$

Lemmas 5 and 6 reduce us to examining ρ, ρ' that are unramified outside primes above p and q and the infinite places, and looking for lifts by Hecke characters that are of conductor divisible only by primes above p and q.

2.3. The case $K = \mathbb{Q}$

Before studying the general case we first study the case $K = \mathbb{Q}$ that will highlight the essential features. Assume that p, q are odd primes. As notation, for any prime p we denote by $\theta_p := \theta_{\mathbb{F}_p}$ the mod p cyclotomic character and by $\tilde{\theta}_p$ its Teichmüller lift (we will regard the latter as a character taking values either in $\bar{\mathbb{Q}}^\times$ or in $\bar{\mathbb{Q}}_p^\times$).

Proposition 1. *Assume $K = \mathbb{Q}$, and assume the conditions of the Lemma 4 above. Let k_p be an integer defined $\bmod\, p-1$ such that $\rho|I_p = \theta_p^{k_p}$ and let a_p be an integer well-defined $\bmod\, A_p :=$ (the prime to q part of $p-1$) such that $\rho'|_{I_p}$ is the reduction $\bmod\, q$ of $\tilde{\theta}_p^{a_p} \cdot \psi_p$ where ψ_p is a character of conductor and order a power of p. Define k_q, a_p, B_q similarly (where this time for instance B_q is the prime to p part of $q-1$). The representations ρ and ρ' arise simultaneously from a Hecke character if and only if there is an integer k that is simultaneously congruent to $k_p - a_p \bmod A_p$ and $k_q - a_p \bmod B_q$. Note that the above conditions depends only on $\rho|_{I_p}, \rho|_{I_q}, \rho'|_{I_q}, \rho'|_{I_p}$.*

Proof. We will assume (w.l.o.g. because Lemma 5 ensures this situation after twisting by an Artin character) above that ρ and ρ' are unramified outside p, q and the infinite place.

The Hecke characters for $\mathbb{Q}$ have a particularly simple description: they are of the form $\varepsilon \cdot \mathrm{Nm}^k$ where ε is an Artin character, Nm is the norm character, and k is an integer. The proof will be accomplished by analyzing $\bmod\, p$ and $\bmod\, q$ representations which arise from a character $\chi := \varepsilon\varepsilon'\mathrm{Nm}^k$ where ε is primitive of conductor a power of p, and ε' is primitive of conductor a power of q (we need only study such characters because of Lemma 6). The $\bmod\, p$ and $\bmod\, q$ (i.e., more precisely w.r.t. embeddings ι_p, ι_q fixed above) characters of G_K that arise from χ are $\bar{\chi}_p := \bar{\varepsilon}_p\bar{\varepsilon}'_p\theta_p^k$ and $\bar{\chi}_q := \bar{\varepsilon}_q\bar{\varepsilon}'_q\theta_q^k$.

We want to determine conditions on ρ and ρ' such that there is a triple $(\varepsilon, \varepsilon', k)$ and the corresponding Hecke character $\chi = \varepsilon\varepsilon'\mathrm{Nm}^k$ has the property $\bar{\chi}_p = \rho$ and $\bar{\chi}_q = \rho'$, i.e., gives rise to ρ and ρ'. It will be useful first to determine to what extent $\bar{\chi}_p$ and $\bar{\chi}_q$ determines the triple $(\varepsilon, \varepsilon', k)$. For this note that $\bar{\chi}_q|_{I_p} = \bar{\varepsilon}_q|_{I_p}$, and thus the Artin character ε which is of conductor a power of p is determined up to characters (of conductor a power of p) that have order a power of q. This determines the wild part of ε, and determines the tame part up to characters of order a power of q.

By considering $\rho'|_{I_p}$ we get an integer a_p that is well-defined mod A_p (the prime to q part of $p-1$) such that $\bar{\chi}_q|_{I_p}$ is the reduction mod the place above q (fixed by ι_q) of $\tilde{\theta}_p^{a_p}$ where now a_p can vary mod A_p (the reduction of a power of $\tilde{\theta}_p$ mod q is constant when the power varies in a congruence class mod A_p). A similar analysis applies to ε' and gives an integer b_q that is well defined mod B_q (the prime to p part of $q-1$) and such that $\bar{\chi}_p|_{I_q}$ is the reduction mod the place above p (fixed by ι_p) of $\tilde{\theta}_p^{b_q}$ where now b_q can vary mod B_q. Consider $\bar{\chi}_p|_{I_p} = \theta_p^{k_p}$ and $\bar{\chi}_q|_{I_q} = \theta_q^{k_q}$ where k_p and k_q are integers that are well-defined modulo $p-1$ and $q-1$, respectively, by these equations.

We deduce from the above analysis, using further the fact that the abelian extension L of $\mathbb{Q}$ which is the compositum of the fixed fields of the kernels of ρ and ρ' is generated by the inertia groups above p and q in $\mathrm{Gal}(L/\mathbb{Q})$ ($\mathbb{Q}$ has no non-trivial unramified extensions), that there is a Hecke character χ with $\bar{\chi}_p = \rho$ and $\bar{\chi}_q = \rho'$, if and only if there exists an integer k that is congruent to $k_p - a_p$ mod A_p and $k_q - b_q$ mod B_q. Thus, we have completely explicit necessary and sufficient conditions for the existence of a χ such that $\chi_p = \rho$ and $\chi_q = \rho'$ and these conditions depend only on $\rho|_{I_p}, \rho|_{I_q}, \rho'|_{I_q}, \rho'|_{I_p}$. $\square$

Remark 2. *By examining the proof we see that we have a classification of the lifts of* ρ *and* ρ' *by Hecke characters.*

2.4. The case of general K

We retain of course the notation of 1.1, but also of Section 2.1.2 above.

The following theorem will give a general criterion for the existence of a Hecke character χ of K, such that

$$\bar{\chi}_p \cong \rho \otimes \phi \quad \text{and} \quad \bar{\chi}_q \cong \rho' \otimes \phi'$$

for some *unramified* characters ϕ, ϕ' on G_K.

Because of Lemma 5 we may, and will, restrict ourselves to the case where ρ and ρ' are both unramified outside p and q.

Before stating the theorem we introduce some data attached to the given representations ρ and ρ':

Let $v_1, \dots, v_s$ and $v'_1, \dots, v'_t$ be the primes of K above p and q, respectively. Define the natural numbers A_i, B_j by the requirements:

$$\#k_{v_i} - 1 = A_i \cdot (\text{power of} q), \quad q \nmid A_i,$$

and similarly

$$\#k_{v'_j} - 1 = B_j \cdot (\text{power of } p), \quad p \nmid B_j.$$

Let k_i and k'_j be integers such that:

$$\rho|_{I_{v_i}} = \theta_{v_i}^{k_i}, \quad i = 1, \dots, s,$$

$$\rho'|_{I_{v'_j}} = \theta_{v'_j}^{k'_j}, \quad j = 1, \dots, t.$$

Also, there are integers b_j, well-defined modulo B_j, and a complex character $\psi_j : I_{v'_j} \to \mathbb{C}^\times$ of q-power order such that:

$$(\rho|_{I_{v'_j}}) = (\tilde{\theta}_{v'_j}^{b_j} \bmod p) \cdot (\psi_j \bmod p),$$

and similarly we have integers a_i, well-defined modulo A_i, such that:

$$(\rho'|_{I_{v_i}}) = (\tilde{\theta}_{v_i}^{a_i} \bmod q) \cdot (\psi'_i \bmod q),$$

with a complex character $\psi'_i : I_{v_i} \to \mathbb{C}^\times$ of p-power order.

Finally, we shall denote by rec_λ the reciprocity map $K_\lambda^\times \to \mathrm{Gal}(K_\lambda^{ab}/K_\lambda)$.

Theorem 1. *Consider the above situation and suppose that integers n_σ, $\sigma \in \Sigma$, are given. Then there exists a Hecke character χ of ∞-type $\sum_{\sigma\in\Sigma} n_\sigma \cdot \sigma$, and unramified characters*

$$\phi : G_K \to \bar{\mathbb{F}}_p^\times, \quad \phi' : G_K \to \bar{\mathbb{F}}_q^\times,$$

such that

$$\bar{\chi}_p \cong \rho \otimes \phi \quad \textit{and} \quad \bar{\chi}_q \cong \rho' \otimes \phi', \tag{$*$}$$

if and only if the following conditions (1), (1′), *and* (2) *hold*:

$$k_i - a_i \equiv -\sum_{\sigma\in\Sigma(v_i)} n_\sigma \cdot p^{\kappa(v_i,\sigma)} =: \xi_i \quad \bmod A_i \quad \textit{for } i = 1, \ldots, s, \tag{1}$$

and

$$k'_j - b_j \equiv -\sum_{\sigma\in\Sigma(v_j)} n_\sigma \cdot q^{\kappa(v_j,\sigma)} =: \xi'_j \quad \bmod B_j, \quad \textit{for } j = 1, \ldots, t, \tag{1′}$$

and furthermore,

$$\prod_i (\tilde{\theta}_{v_i}^{k_i-\xi_i} \cdot \psi'_i) \circ \mathrm{rec}_{v_i}(u) \cdot \prod_j (\tilde{\theta}_{v'_j}^{k'_j-\xi'_j} \cdot \psi_j) \circ \mathrm{rec}_{v'_j}(u) = \prod_{\sigma\in\Sigma} \sigma(u)^{-n_\sigma} \tag{2}$$

for every totally positive global unit u.

Proof. The structure of the proof is as follows. We first seek to determine the restriction of χ to local unit groups U_λ for primes λ lying above p or q. This is done via matching the description we have from Section 2.1.2 with the information coming from the behaviour of ρ and ρ' at local inertia groups. Then Lemma 2 is invoked to give local conditions which will turn out as conditions (1) and (1′). Once these restrictions of χ have been determined, the existence of χ amounts to the global condition of Lemma 1 which will turn into condition (2).

Proof of necessity. Assume that χ exists with the stated properties. According to Lemma 6, χ is unramified outside the primes dividing p or q, and the infinite primes. If ℓ is a prime number and λ a finite prime of K, we have—retaining the notation of Section 2.1.2—that

$$\bar{\chi}_\ell|_{I_\lambda} = \begin{cases} (\varepsilon_\lambda \bmod \ell) & \text{for } \lambda \nmid \ell, \\ (\varepsilon_\lambda \bmod \ell) \cdot \theta_\lambda^{-\sum_{\sigma \in \Sigma(\lambda)} n_\sigma \cdot \ell^{\kappa(\lambda,\sigma)}} & \text{for } \lambda \mid \ell. \end{cases}$$

In particular, we have for $i = 1, \ldots, s$:

$$\bar{\chi}_q|_{I_{v_i}} = (\varepsilon_{v_i} \bmod q) = \rho'|_{I_{v_i}} = (\tilde{\theta}_{v_i}^{a_i} \bmod q) \cdot (\psi_i' \bmod q)$$

and

$$\bar{\chi}_p|_{I_{v_i}} = (\varepsilon_{v_i} \bmod p) \cdot \theta_{v_i}^{\xi_i} = \rho|_{I_{v_i}} = \theta_{v_i}^{k_i}.$$

We conclude that the $\bmod\, p$ and $\bmod\, q$ characters

$$\theta_{v_i}^{k_i - \xi_i} \quad \text{and} \quad (\tilde{\theta}_{v_i}^{a_i} \bmod q) \cdot (\psi_i' \bmod q)$$

of I_{v_i} simultaneously lift to a (uniquely determined) complex character of I_{v_i}, namely ε_{v_i}. On the other hand, as individual lifts of these characters are

$$\tilde{\theta}_{v_i}^{k_i - \xi_i} \quad \text{and} \quad \tilde{\theta}_{v_i}^{a_i} \cdot \psi_i',$$

where ψ_i' has p-power order, and as $\tilde{\theta}_{v_i}$ has order prime to p, we deduce from Lemma 2 that the character

$$\tilde{\theta}_{v_i}^{a_i - k_i + \xi_i}$$

has q-power order. This implies (1) by the definition of A_i. Lemma 2 also gives

$$\varepsilon_{v_i} = \tilde{\theta}_{v_i}^{k_i - \xi_i} \cdot \psi_i'. \qquad (**)$$

Similarly, ($1'$) follows from the fact χ gives a simultaneous lift of the representations ρ and ρ' restricted to $I_{v_j'}$, and we see that in fact

$$\varepsilon_{v_j'} = \tilde{\theta}_{v_j'}^{k_j' - \xi_j'} \cdot \psi_j. \qquad (***)$$

Now, as χ is unramified outside pq and the infinite primes, condition (2) follows from Lemma 1, $(**)$ and $(***)$.

Proof of sufficiency. Define complex characters on inertia at the primes v_i, $i = 1, \ldots, s$, and v_j', $j = 1, \ldots, t$, according to $(**)$ and $(***)$ above. Define also ε_λ to be the trivial character on I_λ if λ is a finite prime not above p or q.

If these characters are viewed as characters on local unit groups U_λ, then (2) combined with Lemma 1 imply that these local characters are in fact restrictions to the U_λ of a Hecke character χ with ∞-type $\sum_{\sigma\in\Sigma} n_\sigma \cdot \sigma$.

For such a χ we deduce, utilizing (1) and (1′), and reversing the pertinent reasoning in the proof of necessity above, that the characters $\bar{\chi}_p^{-1} \cdot \rho$ and $\bar{\chi}_q^{-1} \cdot \rho'$ vanish on every inertia group, and hence are both globally unramified. □

Remark 3. As will be seen from the proof of the theorem, the contribution at the place v_i to the conductor of a lift χ is 'essentially'

$$\text{l.c.m.}\{\mathfrak{p}_{v_i}, \operatorname{cond}(\psi'_i)\} = \text{l.c.m.}\{\mathfrak{p}_{v_i}, \operatorname{cond}(\rho'|_{I_{v_i}})\}.$$

We say 'essentially' because this is definitely true if ψ'_i is nontrivial. If, however, ψ'_i is trivial the conductor is 1 or $\mathfrak{p}_{v_i}$ depending on whether $k_i - \xi_i$ is divisible by $\# k_{v_i} - 1$ or not; however, this condition depends on the n_σ's. Similar remarks apply to the places dividing q of course.

Remark 4. We chose to formulate a theorem considering only representations unramified outside pq and the infinite primes. The reason is first of all that this is the crucial case, and secondly that we wanted to avoid an unnecessarily complicated statement. However, the observant reader will notice that our reduction to the above case via Lemma 5 is not completely explicit: The behavior of an ε from Lemma 5 at primes above p or q is not given explicitly.

However, this situation can easily be rectified, and we shall limit ourselves to some indications: If one wants to prove a statement as in Theorem 1 for arbitrarily ramified representations, there are two possible, essentially equivalent, ways of accomplishing this. First, an inspection of the proof of Theorem 1 reveals immediately that the method extends without any difficulty to the general case of arbitrary ramification: First, one would have conditions like (1), (1′) for each ramification point w not dividing $pq \cdot \infty$; these are purely local conditions coming directly from Lemma 2. Secondly, condition (2) would change by incorporating certain factors on the left-hand side; these factors would depend on the restrictions $\rho|_{I_w}$ and $\rho'|_{I_w}$ for each w as above. We shall leave it to the reader to work out the exact form of these factors.

The second way to extend Theorem 1 to the case of arbitrary ramification is to be more precise about the behavior of an ε as in Lemma 5 at the primes dividing pq. A possible way to do this would be to use Lemma 1 for the case $n_\sigma = 0$—under the assumptions of Lemma 5—to 'shift' (via twisting) any ramification outside $pq \cdot \infty$ to a prime above p (say). After this, one could plug the data into Theorem 1 and get explicit conditions. As the reader will however quickly ascertain, this method would result in exactly the same modified conditions (1), (1′) and (2) that result from the first method.

Remark 5. Notice that if χ_1 and χ_2 are two Hecke characters with the same ∞-type which are both 'solutions' to $(*)$, i.e. have their $\bmod p$ and $\bmod q$ representations isomorphic up to twist by unramified to ρ and ρ', respectively, then χ_1 and χ_2 differ by a globally unramified Artin character. For the Hecke character $\varepsilon := \chi_1\chi_2^{-1}$ has trivial ∞-type, i.e. is an Artin character, and its $\bmod p$ and $\bmod q$ reductions are by hypothesis both unramified whence the claim by Lemma 2.

Remark 6. The reason why we consider only 'lifting up to unramified' as in the theorem above is to be found in the nature of the conditions we impose: As an analysis of the argument quickly reveals, in order to discuss *exact* lifting, and not just 'up to unramified', we would have to consider some sort of analogue to Lemma 1 but with given restrictions to decomposition groups instead of inertia groups. This ties up with the Grunwald–Wang theorem where of course the problem is that one cannot in general lift without introducing additional ramification. We have not been able to find a reasonable characterization of pairs (ρ, ρ') with 'exact' lifts and doubt whether there is one. The following example—a simple counting argument—shows that in general one cannot lift an arbitrary pair of unramified characters.

Example. Suppose that K is an imaginary quadratic field containing no other roots of unity that ± 1. Let p and q be odd primes that split in K. Fix an embedding $\sigma : K \hookrightarrow \mathbb{C}$ and consider an ∞-type $m \cdot \sigma + n \cdot \sigma^c$, with integers m and n. We apply Theorem 1 to find the conditions on m and n necessary and sufficient for the existence of a Hecke character χ with ∞-type $m \cdot \sigma + n \cdot \sigma^c$ and both $\bar{\chi}_p$ and $\bar{\chi}_q$ globally unramified. So, we apply Theorem 1 for the case $\rho = \rho' = 1$ and hence $k_i = k'_j = a_i = b_j = 0$, and $\psi_i = \psi'_j = 1$ for all i, j.

Conditions (1) and (1′) of the theorem amount then to four congruence conditions on n and m which are seen to boil down to

$$n, m \equiv 0 \bmod C,$$

where $C := \text{l.c.m.}\{A, B\}$ with $A := A_1 = A_2$ and $B := B_1 = B_2$ as in the definitions preceding the theorem. Now, C is an even number so if n and m are both divisible by C, then condition (2) of the theorem is automatically satisfied as ± 1 are the only units in K.

So there exist Hecke characters χ_1 and χ_2 with ∞-types $C \cdot \sigma$ and $C \cdot \sigma^c$, respectively, such that

$$((\overline{\chi_i})_p, (\overline{\chi_i})_q) = (\phi_i, \phi'_i), \quad i = 1, 2,$$

where ϕ_i, ϕ'_i, $i = 1, 2$, are unramified characters. Now, if χ is any Hecke character such that $\bar{\chi}_p$ and $\bar{\chi}_q$ are both unramified, its ∞-type has shape $\mu C \cdot \sigma + \nu C \cdot \sigma^c$ with integers μ and ν. Consequently, $\chi = \varepsilon \chi_1^{\mu} \chi_2^{\nu}$ with ε an Artin character which must be globally unramified (cf. Remark 5 above).

So any pair (ρ, ρ') of unramified $\bmod p$ and $\bmod q$ characters that lifts *exactly* to a Hecke character necessarily has form:

$$(\rho, \rho') = (\bar{\varepsilon}_p \phi_1^{\mu} \phi_2^{\nu}, \bar{\varepsilon}_q (\phi'_1)^{\mu} (\phi'_2)^{\nu})$$

with an unramified Artin character ε. If the class group of K has exponent α and order h, it follows that the number of such pairs (ρ, ρ') is bounded by $\alpha^2 \cdot h$. On the other hand, if h is not divisible by p or q, then the total number of pairs of unramified $\bmod p$ and $\bmod q$ characters is at least h^2. Hence, if further $h > \alpha^2$ there necessarily exist at least 1 such pair that does not lift 'exactly' to a Hecke character. As a concrete example, one can take $K = \mathbb{Q}(\sqrt{-3 \cdot 5 \cdot 7 \cdot 11})$, which has class group isomorphic to $(\mathbb{Z}/2\mathbb{Z})^3$, and for p and q any two distinct odd primes that split in K.

3. Serre's conjecture mod pq

This will be a speculative section on issues surrounding $\bmod pq$ versions of Serre's conjectures in [10]. Let p and q be odd primes and fix as above embeddings ι_p and ι_q of $\bar{\mathbb{Q}}$ in $\bar{\mathbb{Q}}_p$ and $\bar{\mathbb{Q}}_q$ as before. Barry Mazur and Ken Ribet had investigated the question of when a pair of odd continuous irreducible $\bmod p$ and $\bmod q$ Galois representations

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$$

and

$$\rho' : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_q)$$

arise from a newform $f \in S_2(\Gamma_1(N))$ for some level N and with respect to the embeddings ι_p and ι_q that have been fixed. William Stein made some computations [11] towards this question in which the level N was varied in order to discover a newform $f \in S_2(\Gamma_0(N))$ of the desired sort.

There are certain local constraints that one must impose, and which we will come to later (see Conjecture 1 below), to expect to have an affirmative answer. It must be pointed out here that even assuming Serre's original conjecture [10], i.e., assuming that ρ and ρ' are individually modular, proving that they are *simultaneously* modular is a different ball game. Even after having imposed these necessary local constraints what makes this question difficult to address even computationally is that there seems no a priori way of guessing what levels N one should be looking at (though one does know by the analysis in [2] what levels one should not be looking at as local constraints preclude some primes dividing the levels of newforms which give rise to either of the ρ or ρ'!). Unlike the situation in Serre's conjecture where he did specify a minimal level at which a representation like ρ should be found (before Ribet et al. cf. [7], proved this ε-conjecture one did not even know whether there existed a minimal level even without caring about what it exactly was), there does not seem to be a "minimal level" $N_{\rho,\rho'}$ at which ρ and ρ' should arise from a newform $f \in S_2(\Gamma_1(N_{\rho,\rho'}))$, i.e., all other levels M at which ρ and ρ' arise from a newform in $S_2(\Gamma_1(M))$ should be divisible by $N_{\rho,\rho'}$.

There is one natural guess for which levels N one can look at which unfortunately is very unlikely to be correct. Let $N(\rho)$, resp., $N(\rho')$, be the prime to p, resp., prime to q, part of the Artin conductor of ρ, resp. ρ'. Then we can try to look for the desired newform from which ρ, ρ' arise simultaneously in $S_2(\Gamma_1(N(\rho)N(\rho')p^\alpha q^\beta))$ where α, β vary. The reason why this is unlikely to work is that there are only *finitely many* α, β such that there will exist a newform $f \in S_2(\Gamma_1(N(\rho)N(\rho')p^\alpha q^\beta))^{\mathrm{new}}$ that can give rise both ρ and ρ'. This follows from the analysis in [2] which gives that if ρ (resp., ρ') arises from $S_2(\Gamma_1(N(\rho)N(\rho')p^\alpha q^\beta))^{\mathrm{new}}$ then β (resp., α) is bounded. (Note that on the contrary by Lemma 1 of [2] ρ, resp. ρ', does arise from $S_2(\Gamma_1(N(\rho)p^\alpha))^{\mathrm{new}}$, resp., $S_2(\Gamma_1(N(\rho')q^\beta))^{\mathrm{new}}$ for all $\alpha \geqslant 2$, resp., $\beta \geqslant 2$.) Further again unlike the situation for a single representation ρ, if there does exist a newform f which gives rise to ρ and ρ', it is not clear that there are infinitely many, i.e., there is no known way that one can systematically raise levels mod pq unlike in the case of mod p representations where a complete study is available because of the work of Ribet (cf. [6]) and others.

In the questions raised by Mazur and Ribet and the subsequent computations of William Stein only the level aspect of this question was considered. In the following paragraphs we discuss the "weight aspect".

Suppose for simplicity for this paragraph that ρ and ρ' arise individually (with respect to the embeddings ι_p, ι_q) from newforms of level N in $S_k(\Gamma_0(N))$ with N squarefree and $(N, pq) = 1$. (This ensures that the necessary local conditions of Conjecture 1 below are satisfied.) Then we can ask if they arise *simultaneously* from a newform $f \in S_{k'}(\Gamma_0(N))$ for some $k' \geqslant 0$. Unlike the previous paragraph this is more difficult to rule out as for all k' congruent to $k \bmod \mathrm{l.c.m.}(p-1, q-1)$ the ρ and ρ' *individually* do arise from $S_{k'}(\Gamma_0(N))$. This of course can be seen by multiplication by powers of the normalized Eisenstein series E_{p-1} and E_{q-1} (Hasse invariants mod p and mod q) that are congruent to 1 mod p and 1 mod q, respectively, and then applying the mod p or mod q Deligne–Serre lifting lemma, or better still in the present context by multiplication by a suitable power of the souped up "mod pq Hasse invariant"

$$E_{\mathrm{l.c.m.}(p-1,q-1)} = 1 - \frac{2(\mathrm{l.c.m.}(p-1, q-1))}{B_{\mathrm{l.c.m.}(p-1,q-1)}} . \sum_{n \geqslant 1} \sigma_{\mathrm{l.c.m.}(p-1,q-1)-1}(n) q^n$$

(where by B_k we mean the kth Bernoulli number and $\sigma_k(n) = \sum_{d|n} d^k$) which by the von-Staudt–Clausen theorem is congruent to $1 \bmod pq$. Unfortunately, there is no mod pq Deligne–Serre lifting lemma, and so we do not know and perhaps do not even expect that there is any periodicity with respect to weight of newforms in $S_k(\Gamma_0(N))$ which give rise to ρ and ρ' simultaneously.

It will be interesting to investigate the issues raised in the paragraph computationally. What makes the possibility of ρ and ρ' arising simultaneously from $S_{k'}(\Gamma_0(N))$ attractive is that arithmetically the weight is just one parameter (or automorphically, the component at the archimedean place) while if we were to look at $S_k(\Gamma_0(N))$ for fixed k and varying N we would *have* to allow N to be divisible by varying primes (as follows from the analysis in [2]), so arithmetically vary infinitely many independent parameters (or automorphically, vary infinitely many non-archimedean local components).

In [3] one set of local constraints for ρ and ρ' to arise simultaneously from a newform were highlighted: this may be called the *semistable case*. We will formulate here a finer mod pq Serre conjecture.

Given a (algebraic) Weil–Deligne parameter (τ_ℓ, N_ℓ) (for this see [12]) with $\tau_\ell : W_{\mathbb{Q}_\ell} \to \mathrm{GL}_2(\bar{\mathbb{Q}})$ a continuous representation of $W_{\mathbb{Q}_\ell}$, the Weil group of $\mathbb{Q}_\ell$, with the target given the discrete topology, and N_ℓ a nilpotent matrix in $M_2(\bar{\mathbb{Q}})$, and $p \neq \ell$ is a prime then the corresponding 2-dimensional p-adic representation $(\tau_\ell, N_\ell)_p :\ \mathrm{Gal}(\bar{\mathbb{Q}}_\ell/\mathbb{Q}_\ell) \to \mathrm{GL}_2(\bar{\mathbb{Q}}_p)$ is:

- $N_\ell = 0$, τ_ℓ reducible: $\tau_\ell = \varepsilon_1 \oplus \varepsilon_2$, the sum of a pair of quasicharacters of the Weil group $W_{\mathbb{Q}_\ell}$ taking values in $\bar{\mathbb{Q}}^\times$, then $(\tau_\ell, N_\ell)_p := \varepsilon_{1,p} \oplus \varepsilon_{2,p}$, and $\varepsilon_{1,p}, \varepsilon_{2,p}$ the corresponding p-adic characters arising via the fixed embedding $\iota_p : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$.
- $N_\ell = 0$, τ_ℓ irreducible: then up to twisting by a character $\varepsilon : W_{\mathbb{Q}_\ell} \to \bar{\mathbb{Q}}^\times$, τ_ℓ has finite image. Then $(\tau_\ell, N_\ell)_p := (\tau_\ell \otimes \varepsilon)_p \otimes \varepsilon_p^{-1}$ with $(\tau_\ell \otimes \varepsilon)_p$ the embedding of the finite image of $\tau_\ell \otimes \varepsilon$ in $\mathrm{GL}_2(\bar{\mathbb{Q}})$ into $\mathrm{GL}_2(\overline{\mathbb{Q}_p})$ and ε_p the p-adic character corresponding to ε arising via the fixed embedding $\iota_p : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$.
- $N_\ell \neq 0$: then τ_ℓ is forced to be of the form $\varepsilon \oplus \varepsilon \| \ \|$ with ε a quasicharacter of the Weil group $W_{\mathbb{Q}_\ell}$ taking values in $\bar{\mathbb{Q}}^\times$ and $\| \ \|$ the "norm character" (i.e., unramified character with $\|\mathrm{Frob}_\ell\| = \ell$) then $(\tau_\ell, N_\ell)_p$ is $\begin{pmatrix} \varepsilon_p \| \ \|_p & 0 \\ 0 & \varepsilon_p \end{pmatrix} \exp(N_\ell t_p)$: here ε_p is the p-adic character corresponding to ε w.r.t. the embedding $\iota_p : \bar{\mathbb{Q}} \to \bar{\mathbb{Q}}_p$ as before, t_p is the homomorphism of the Galois group of the maximal tamely ramified extension of $\mathbf{Q}_\ell$ which arises by projecting first to I_ℓ^t, the tame inertia at ℓ (i.e., after choosing a Frobenius σ, $\sigma^n \tau \to \tau$ where $\tau \in I_\ell^t$), followed by a $\mathbb{Z}_p$-valued homomorphism of I_ℓ^t which is the projection to the unique $\mathbb{Z}_p$ quotient of I_ℓ^t and $\| \ \|_p$ is the p-adic cyclotomic character (the isomorphism class of $(\tau_\ell, N_\ell)_p$ is independent of the choices made).

Conjecture 1. *Let* $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$ *and* $\rho' : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_q)$ *be continuous, odd, absolutely irreducible representations and assume that* ρ *is unramified at* q *and* ρ' *is unramified at* p. *Let* $k(\rho)$ *and* $k(\rho')$ *be the Serre invariants of* ρ, ρ' *as in* [10]. *Then* ρ *and* ρ' *are the reductions mod* p *and* mod q *of the* p*-adic and* q*-adic representations* (*w.r.t.* ι_p, ι_q) *attached to a newform in* $S_k(\Gamma_1(N))$ *for some integer* $k \geqslant 2$ *and some positive integer* N *with* $(N, pq) = 1$ *if and only if*

- *there is an integer congruent to* $k(\rho) \bmod p - 1$ *and* $k(\rho') \bmod q - 1$,
- *and further for every prime* $\ell \neq p, q$, *there is a* (*algebraic*) *Weil–Deligne parameter* (τ_ℓ, N_ℓ) *and a choice of integral models for* $(\tau_\ell, N_\ell)_p$ *and* $(\tau_\ell, N_\ell)_q$ *such that their* mod p *and* mod q *reductions are isomorphic to* $\rho|_{D_\ell}$ *and* $\rho'|_{D_\ell}$ *respectively.*

Discussion of the conjecture. The main feature of the conjecture is that the conditions are local (recall that in [10] the definition of $k(\rho), k(\rho')$ is purely in terms of $\rho|_{I_p}, \rho'|_{I_q}$). The condition in the conjecture at primes ℓ is empty for ℓ that are $\neq p, q$ and unramified in both ρ and ρ', and thus there are only finitely many conditions that need to be checked as per the conjecture. The restriction that ρ is unramified at q and ρ' is unramified at p is a technical restriction which arises from the difficulties of studying mod p representation restricted to D_p arising from newforms with levels divisible by powers of p (there are some results towards this in [1,13]): it will be nice to remove this technical restriction and refine the above conjecture to allow ρ and ρ' to be ramified at q and p, respectively.

As the referee has remarked, in general the local constraints in the conjecture are non-empty: We can find distinct primes ℓ, p and q, and representations $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_p)$, $\rho' : G_{\mathbb{Q}} \to \mathrm{GL}_2(\bar{\mathbb{F}}_q)$ such that ρ has conductor divisible exactly by ℓ^3 whereas ρ' is unramified at ℓ. The results due to Carayol [2] show that the pair (ρ, ρ') definitely cannot arise from a modular form.

We could make a more optimistic conjecture and *fix* a weight $k \geqslant 2$ congruent to $k(\rho) \bmod p-1$ and $k(\rho') \bmod q-1$, and ask that ρ and ρ' arise from $S_k(\Gamma_1(N))$ for some (variable) N prime to pq (as in [11]), or we can *fix* N prime to pq and divisible by $N(\rho)$ and $N(\rho')$, the prime-to-p and prime-to-q parts of the Artin conductors of ρ and ρ' respectively, and ask that ρ and ρ' arise from $S_k(\Gamma_1(N))$ for some (variable) k as in the discussion above. We can also weaken the conjecture and instead of asking that ρ and ρ' arise from a common newform with respect to fixed embeddings ι_p, ι_q, allow these embeddings to vary, or alternatively ask that ρ and ρ' arise simultaneously (w.r.t. the fixed embeddings ι_p and ι_q) from the *Galois orbit* of a newform f.

One can also formulate a conjecture entirely analogous to Conjecture 1 for compatible lifts of ρ and ρ' to p-adic and q-adic representations of $G_{\mathbb{Q}}$, which we leave as an exercise for the interested reader. As was pointed out in [3] such a conjecture has relevance to Serre's *original* conjecture in [10] because of the modularity lifting theorems of Wiles et al.

In connection with Conjecture 1 it is important to notice that the weight k may very well depend on the choice of primes of $\bar{\mathbb{Q}}$ over p and q. The following simple example illustrates this.

Example. Suppose that f and f' are two newforms on $\mathrm{SL}_2(\mathbb{Z})$ of some weight k and let ρ and ρ' be the mod p and mod q representations attached to f and f', respectively. The conditions of Conjecture 1 are then satisfied so that the conjecture would have ρ and ρ' arising from a newform $F \in S_m(\Gamma_1(N))$ for some $m \geqslant 2$ and some N prime to pq.

To illustrate with a simple example that the possible weights m may depend on our choice of primes over p and q, suppose that $p = 5$, $q = 7$, and that f and f' are the 2 newforms of weight 24 and level 1:

$$f = 24\alpha\Delta^2 + Q^3\Delta \quad \text{and } f' = 24\alpha'\Delta^2 + Q^3\Delta$$

with $\{\alpha, \alpha'\} := \{-13/2 \pm \sqrt{144169}/2\}$. The primes 5 and 7 both split in the quadratic field $\mathbb{Q}(\sqrt{144169})$, say $5 = \mathfrak{p}_5 \cdot \mathfrak{p}_5'$ and $7 = \mathfrak{p}_7 \cdot \mathfrak{p}_7'$. Now, Δ is congruent mod $\mathfrak{p}_7$ to either f or f'. Let us assume notation so that $\Delta \equiv f(\mathfrak{p}_7)$. As $Q \equiv 1(5)$ we have then

$$\Delta \equiv f(\mathfrak{p}_5), \quad \Delta \equiv f'(\mathfrak{p}_7').$$

On the other hand, as $\alpha\alpha'$ is divisible by 5 we have

$$f' \equiv f(\mathfrak{p}_5), \quad f' \equiv f'(\mathfrak{p}_7)$$

and f' is the solution to these congruences with smallest possible weight.

Remark 7. Unlike the case of 1-dimensional mod pq representations (see Lemma 6) one would expect that there are modular forms of levels divisible by arbitrarily many primes that give rise to ρ and ρ' if the local conditions are met (this is substantiated by the tables in [11]). Here the point is that one can attempt to raise levels at primes that are "Steinberg" for ρ and ρ' and Steinberg lifts have the property that the image of inertia is unipotent and hence infinite. Thus Lemma 2 on which Lemma 6 relies does not apply.

Remark 8. A mod pq descent result of the type suggested in Remark 1 is not true for 2-dimensional representations even in the simplest case when $K/\mathbb{Q}$ is a quadratic extension. The principle for constructing a counterexample is the following: Consider representations ρ and ρ' as above such that ρ is ramified at a prime $\ell \neq p, q$ and >2, and ℓ is not congruent to ± 1 either mod p or mod q, with the image of inertia $\rho(I_\ell)$ non-trivial and unipotent, ρ' unramified at ℓ and such that $\rho'(\mathrm{Frob}_\ell)$ has eigenvalues with ratio $-\ell$. Let $\rho_\ell := \rho|_{D_\ell}$ and $\rho'_\ell := \rho|_{D_\ell}$. Then it is easy from local computations at ℓ that use structure of tame inertia to see that while ρ_ℓ and ρ'_ℓ cannot arise from a single Weil–Deligne representation (τ, N) as above, the restriction of ρ_ℓ and ρ'_ℓ to the absolute Galois group of the unramified quadratic extension of $\mathbb{Q}_\ell$ can arise in this way. From this it is easy to construct counterexamples remarking that if ρ and ρ' are irreducible on restriction to a quadratic extension K of $\mathbb{Q}$ (with ℓ inert in K), the extensions of $\rho|_{G_K}$ and $\rho'|_{G_K}$ to $G_\mathbb{Q}$ are unique up to twisting by characters, and the condition that $\rho'(\mathrm{Frob}_\ell)$ has eigenvalues with ratio $-\ell$ is invariant under twisting. (The case of solvable mod p automorphic descent for 2-dimensional representations is the main theorem of [3].)

Remark 9. In a recent preprint of Manoharmayum [5], results towards Serre's conjecture mod 6 are proven.

Acknowledgments

The authors thank the referee for a number of remarks that helped improve the presentation.

References

[1] C. Breuil, A. Mezard, Multiplicités modulaires et représentations de $GL_2(\mathbb{Z}_p)$ et de $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ en $\ell = p$, Prépublications de Université de Paris-Sud, 2000-45.

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

[3] C. Khare, Mod p descent for Hilbert modular forms, Math. Res. Lett. 7 (2000) 455–462.

[4] C. Khare, Compatible systems of mod p Galois representations and Hecke characters, Math. Res. Lett., to appear.

[5] J. Manoharmayum, Note on Serre's conjecture modulo 6, Preprint.

[6] K. Ribet, Congruence relations between modular forms, Proceedings of the ICM, Warsaw 1983, pp. 503–514.

[7] K. Ribet, Report on mod ℓ representations of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, in Motives, Proc. Sympos. Pure Math. 55 (Part 2) (1994) 639–676.

[8] J.-P. Serre, Abelian l-adic Representations and Elliptic Curves, Addison–Wesley, Reading, MA, 1989.

[9] J.-P. Serre, Propriétés galoisiennes des points d'ordre finides courbes elliptiques, Invent. Math. 15 (1972) 259–331.

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

[11] W. Stein, Serre's conjecture mod pq? available at http://modular.fas.harvard.edu/Tables/serremodpq/.

[12] J. Tate, Number theoretic background, in: Automorphic forms, representations and L-functions, Proc. Sympos. Pure Math. 33(Part 2) (1979) 3–26.

[13] D. Ulmer, Slopes of modular forms and congruences, Ann. Inst. Fourier 46 (1996) 1–32.

[14] A. Weil, On a certain type of characters of the idèle-class group of an algebraic number-field, in: Proceedings of the International Symposium on Algebraic Number Theory, Tokyo–Nikko, 1955, pp. 1–7.