Journal de Théorie des Nombres
de Bordeaux **16** (2004), 179–185

Modularity of p-adic Galois representations via p-adic approximations

Dedicated to the memory of my mother Nalini B. Khare
30th August 1936–12th March 2002

par CHANDRASHEKHAR KHARE

RÉSUMÉ. Dans cette courte note, nous donnons une nouvelle approche pour prouver la modularité des représentations galoisiennes p-adiques en utilisant une méthode d'approximations p-adiques. Cela englobe quelques uns des résultats bien connus de Wiles et Taylor dans de nombreux cas mais pas tous. Une caractéristique de cette nouvelle approche est qu'elle travaille directement avec la représentation galoisienne p-adique dont on cherche à établir la modularité. Les trois ingrédients essentiels sont une technique de cohomologie galoisienne de Ramakrishna, un résultat de montée de niveau de Ribet, Diamond, Taylor et une version mod p^n du principe de descente de niveau de Mazur.

ABSTRACT. In this short note we give a new approach to proving modularity of p-adic Galois representations using a method of p-adic approximations. This recovers some of the well-known results of Wiles and Taylor in many, but not all, cases. A feature of the new approach is that it works directly with the p-adic Galois representation whose modularity is sought to be established. The three main ingredients are a Galois cohomology technique of Ramakrishna, a level raising result due to Ribet, Diamond, Taylor, and a mod p^n version of Mazur's principle for level lowering.

Modularity lifting theorem

In the work of Wiles in [W], as completed by Taylor and Wiles in [TW], the modularity of many 2-dimensional p-adic representations of the absolute Galois group $G_{\mathbf{Q}}$ of $\mathbf{Q}$ was proven assuming that the mod p reduction of the representation was irreducible and modular. The proof was via proving the isomorphism of certain deformation and Hecke rings. A more naive approach to proving the modularity of a p-adic representation, say

$$\rho : G_{\mathbf{Q}} \to GL_2(\mathbf{Z}_p),$$

Manuscrit reçu le 10 janvier 2003.

assuming that its reduction $\overline{\rho}$ is modular, that works directly with ρ instead of fitting it into a family (i.e., interpreting it as a point in the spectrum of a deformation ring), and then proving modularity for the family as is done in [W] and [TW], would be as follows: Starting from the assumption that $\overline{\rho}$ is modular prove successively that the mod p^n reductions ρ_n of ρ occur in the p-power torsion of the abelian variety $J_1(N)$ for a fixed N. In this note we give a proof of modularity lifting results in this more direct style. Here like in [K] we merely want to present a new method for proving known results, and will illustrate the method by rederiving the following special case of the results proven in [W] and [TW]. This is not the optimal result that can be obtained by this method: see the end of the note for the statement of some refinements.

Theorem 1. *(A. Wiles, R. Taylor) Let $\rho : G_{\mathbf{Q}} \to GL_2(W(k))$ be a continous representation, with $W(k)$ the Witt vectors of a finite field k of residue characteristic $p > 5$.*

Assume that the mod p reduction $\overline{\rho}$ of ρ has the following properties:

- *$\mathrm{Ad}^0(\overline{\rho})$ is absolutely irreducible,*
- *$\overline{\rho}$ is modular.*

Further assume that:

- *ρ is semistable at all primes,*
- *ρ is of weight 2 at p and Barsotti-Tate at p if $\overline{\rho}$ is finite, flat at p,*
- *and that the primes ramified in ρ are finitely many and not ± 1 mod p.*

Then ρ arises from $S_2(\Gamma_0(N))$ for some integer N.

Remarks:

1. The idea of such a proof was proposed in [K1], but at that time we could not put it into practise. In [K1] we had observed that for many ρ's (for examples the ones in the theorem), assuming $\overline{\rho}$ is modular one can show that ρ_n arises from $J_1(N(n))$ for a positive integer $N(n)$ that depends on n. The new observation of the present note is that in many circumstances using this we can deduce (see Proposition 1) that ρ_n arises from $J_1(N)$ for a *fixed* N.

2. By semistable at primes $q \neq p$ we simply mean that the restriction to the inertia at q should be unipotent, and at p semistable of weight 2 we mean that ρ at p should either be *Barsotti-Tate*, i.e., arise from a p-divisible group, or be ordinary and the restriction to the inertia at p should be of the form $\begin{pmatrix} \varepsilon & * \\ 0 & 1 \end{pmatrix}$ with ε the p-adic cyclotomic character. Note that the determinant of such a ρ is ε.

3. $\mathrm{Ad}^0(\overline{\rho})$ is absolutely irreducible in fact follows from the other assumptions of the theorem and the weaker hypothesis that $\overline{\rho}$ is irreducible.

Proof

The rest of the paper will be occupied with the proof of this theorem. The proof will have 2 steps: We first prove that the reduction mod p^n of ρ, $\rho_n : G_{\mathbf{Q}} \to GL_2(W_n(k))$ with $W_n(k)$ the Witt vectors of length n of k, arises in the p-power torsion of $J_0(Q_n)$ where Q_n is the (square-free) product of a finite set of primes that depends on n. For this we use the Ramakrishna-lifts or R-lifts of [R] and the determination of their limit points in Theorem 1 of [K1]. In the second step, we deduce from the first step that ρ_n arises from $J_0(N)$ for a positive integer N independent of n (see Proposition 1 below). From this we will deduce the theorem easily.

Step 1. Let S be the set of ramification of $\overline{\rho}$. We repeat the following lemma from [K1] and its proof for convenience. To explain the notation used, by *R-primes* we mean primes q that are not ± 1 mod p, unramified for the residual representation $\overline{\rho}$ and for which $\overline{\rho}(\mathrm{Frob}_q)$ has eigenvalues with ratio $q^{\pm 1}$ with Frob_q an arithmetic Frobenius element at q. We say that a finite set of *R-primes* Q is *auxiliary* if certain maps on H^1 and H^2, namely $H^1(G_{S\cup Q}, \mathrm{Ad}^0(\overline{\rho})) \to \oplus_{v\in S\cup Q} H^1(G_v, \mathrm{Ad}^0(\overline{\rho}))/\mathcal{N}_v$ and $H^2(G_{S\cup Q}, \mathrm{Ad}^0(\overline{\rho})) \to \oplus_{v\in S\cup Q} H^2(G_v, \mathrm{Ad}^0(\overline{\rho}))$ considered in [R] are isomorphisms. We refer to [R] for the notation used: recall that $\mathcal{N}_v$ for $v \in Q$ is the mod p cotangent space of a smooth quotient of the local deformation ring at v which parametrises *special* lifts. These isomorphisms result in the fact that there is a lift $\rho_{S\cup Q}^{Q-new} : G_{\mathbf{Q}} \to GL_2(W(k))$ of $\overline{\rho}$ which is furthermore the unique lift of $\overline{\rho}$ to a representation to $GL_2(\mathcal{O})$ (with $\mathcal{O}$ ring of integers of any finite extension of $\mathbf{Q}_p$) that has the properties of being semistable of weight 2, unramified outside $S \cup Q$, minimally ramified at primes in S, with determinant ε, and *special* at primes in Q. Here by *special* at q we mean that the restriction of the representation to a decomposition group D_q at q should up to twist be of the form $\begin{pmatrix} \varepsilon & * \\ 0 & 1 \end{pmatrix}$: we use this definition even for representations into $GL_2(R)$ with R a $W(k)$-algebra.

Lemma 1. *Let Q'_n be any finite set primes that includes the primes of ramification of ρ_n, such that $Q'_n \backslash S$ contains only R-primes and such that $\rho_n|_{D_q}$ is special for $q \in Q'_n \backslash S$. Then there exists a finite set of primes Q_n that contains Q'_n, such that $\rho_n|_{D_q}$ is special for $q \in Q_n \backslash S$, $Q_n \backslash S$ contains only R-primes and $Q_n \backslash S$ is auxiliary.*

Proof: We use [R] and Lemma 8 of [KR] (that latter being a certain mutual disjointness result for field extensions cut out by ρ_n and extensions cut out by elements of $H^1(G_{\mathbf{Q}}, \mathrm{Ad}^0(\overline{\rho}))$ and $H^1(G_{\mathbf{Q}}, \mathrm{Ad}^0(\overline{\rho})^*)$ with $\mathrm{Ad}^0(\overline{\rho})^*$ the dual of $\mathrm{Ad}^0(\overline{\rho})$) to construct an auxiliary set of primes V_n such that $\rho_n|_{D_q}$ is special for $q \in V_n$. Then as $Q'_n \backslash S$ contains only R-primes, it follows from

Proposition 1.6 of [W] that the kernel and cokernel of the map

$$H^1(G_{S\cup V_n\cup Q'_n}, \mathrm{Ad}^0(\overline{\rho})) \to \oplus_{v\in S\cup V_n\cup Q'_n} H^1(G_v, \mathrm{Ad}^0(\overline{\rho}))/\mathcal{N}_v$$

have the same cardinality, as the domain and range have the same cardinality. Then using Proposition 10 of [R], or Lemma 1.2 of [T], and Lemma 8 of [KR], we can augment the set $S \cup V_n \cup Q'_n$ to get a set Q_n as in the statement of the lemma.

Remark: We can choose Q'_n as in the lemma such that Q'_n is independent of n (as ρ is ramified at only finitely many primes). But the set Q_n that the lemma produces depends much on n, and can be chosen to be independent of n only if ρ is itself a R-lift. Further note that just like the auxiliary primes in [TW], the sets Q_n have no coherence property in general.

We choose a finite set of primes Q'_n as in Lemma 1 and use the lemma to complete Q'_n to a set Q_n such that $Q_n\backslash S$ is auxiliary and $\rho_n|_{D_q}$ is special for $q \in Q_n\backslash S$. Then we claim $\rho_{Q_n}^{Q_n\backslash S-new} \equiv \rho \bmod p^n$. The claim is true, as the set $Q_n\backslash S$ being auxiliary, there is a *unique* representation $G_{\mathbf{Q}} \to GL_2(W(k)/(p^n))$ (with determinant ε) that reduces to $\overline{\rho}$ mod p and is unramified outside Q_n, minimal at S and special at primes of $Q_n\backslash S$. It is of vital importance that ρ is $GL_2(W(k))$-valued as otherwise we would not be able to invoke the disjointness results that are used in the proof of Lemma 1 (Lemma 8 of [KR]).

Because of the uniqueness alluded to above, it follows from the level-raising results of [DT] (see Theorem 1 of [K]) that $\rho_{Q_n}^{Q_n\backslash S-new}$ arises from $J_0(Q_n)$ (where abusively we denote by Q_n the product of primes in Q_n), and hence because of the congruence $\rho_{Q_n}^{Q_n\backslash S-new} \equiv \rho \bmod p^n$, we deduce that ρ_n arises from (i.e., is isomorphic as a $G_{\mathbf{Q}}$-module to a submodule of) the p-power torsion of $J_0(Q_n)$ and for primes r prime to Q_n, T_r acts on ρ_n via $\mathrm{tr}(\rho(\mathrm{Frob}_r))$.

Step 2. Let W_n be the subset of Q_n at which ρ_n is unramified (note that the set $Q_n\backslash W_n$ is independent of n for $n >> 0$ as ρ is *finitely* ramified). Then we have the proposition:

Proposition 1. *The representation ρ_n arises from the W_n-old subvariety of $J_0(Q_n)$, and furthermore all the Hecke operators T_r, for r a prime not dividing Q_n, act on ρ_n by* $\mathrm{tr}(\rho_n(\mathrm{Frob}_r))$.

Proof: This is a simple application of Mazur's principle (see Section 8 of [Ri]). The principle relies on the fact that on torsion points of Jacobians of modular curves with semistable reduction at a prime q, which are unramified at q and which reduce to lie in the "toric part" of the reduction mod q of these Jacobians, the Frobenius action is constrained. Namely,

on the "toric part" the Frobenius Frob_q acts by $-w_q q$ where w_q is the Atkin-Lehner involution. We flesh this out this below.

Consider a prime $q \in W_n$. Then decompose $\rho_n|_{D_q}$ (which is unramified by hypothesis) into $W(k)/p^n \oplus W(k)/p^n$ where on the first copy Frob_q acts by a scalar that is not $\pm q$: this is possible as q^2 is not 1 mod p and ρ_n is special at q. Let e_n be a generator for the first summand. We would like to prove that ρ_n occurs in the q-old subvariety of $J_0(Q_n)$. Note that using irreducibility of $\overline{\rho}$, Burnside's lemma gives that $\overline{\rho}(k[G_{\mathbf{Q}}]) = M_2(k)$ and hence by Nakayama's lemma $\rho_n(W_n(k)[G_{\mathbf{Q}}]) = M_2(W_n(k))$. Thus using the fact that the q-old subvariety is stable under the Galois and Hecke action, the fact that ρ_n occurs in the q-old subvariety of $J_0(Q_n)$ is implied by the claim that e_n is contained in the q-old subvariety of $J_0(Q_n)$. Let $\mathcal{J}$ be the Néron model at q of $J_0(Q_n)$. Note that as ρ_n is unramified at q it maps injectively to $\mathcal{J}_{/\mathbf{F}_q}(\overline{\mathbf{F}_q})$ under the reduction map. Now if the claim were false, as the group of connected components $\mathcal{J}$ is Eisenstein (see loc. cit.), we would deduce that the reduction of e_n in $\mathcal{J}^0_{/\mathbf{F}_q}(\overline{\mathbf{F}}_q)$ maps non-trivially (and hence its image has order divisible by p) to the $\overline{\mathbf{F}}_q$-points of the torus which is the quotient of $\mathcal{J}^0_{/\mathbf{F}_q}$ by the image of the q-old subvariety (in characteristic q). But as we recalled above, it is well known (see loc. cit.) that Frob_q acts on the $\overline{\mathbf{F}}_q$-valued points of this toric quotient (isogenous to the torus T of $\mathcal{J}^0_{\mathbf{F}_q}$, the latter being a semiabelian variety that is an extension of $J_0(\frac{Q_n}{q})^2_{/\mathbf{F}_q}$ by T) by $-w_q q$ which gives the contradiction that q^2 is 1 mod p. This contradiction proves the claim. Now taking another prime $q' \in W_n$ and working within the q-old subvariety of $J_0(Q_n)$, by the same argument we see that ρ_n occurs in the $\{q, q'\}$-old subvariety of $J_0(Q_n)$, and eventually that ρ_n occurs in the W_n-old subvariety of $J_0(Q_n)$. Furthermore by inspection the last part of the proposition is also clear.

ρ is modular. From the above proposition it is easy to deduce that ρ_n arises from $J_0(N)$ for some fixed integer N that is independent of n. Let $\mathbf{T}$ be the Hecke algebra for $J_0(N)$, generated by the Hecke operators T_r with r prime and prime to N. We claim that the ρ_n give compatible morphisms from $\mathbf{T}$ to the $W(k)/p^n W(k)$. To get these morphisms, let V_n denote a realization of the representation ρ_n in $J_0(N)$ which exists by the above proposition. Then V_n is $G_{\mathbf{Q}}$-stable, and hence $\mathbf{T}$-stable (because of the Eichler-Shimura congruence relation mod r, that gives an equality of correspondences $T_r = \mathrm{Frob}_r + r.\mathrm{Frob}_r{}^{-1}$ where Frob_r is the Frobenius morphism at r). So V_n is a $\mathbf{T}$-module, and because of the aboslute irreducibility (only the scalars commute with the $G_{\mathbf{Q}}$-action) $\mathbf{T}$ acts via a morphism $\pi_n : \mathbf{T} \to W(k)/p^n W(k)$ as desired, and the π_n's are compatible again because of the congruence relation. This gives a morphism $\pi : \mathbf{T} \to W(k)$ such that the Eichler-Shimura representation associated to π is isomorphic

to ρ which finishes proof of Theorem 1. We owe this efficient argument to Bas Edixhoven: in an earlier version we had given a clumsier argument.

Remarks:

1. In [K], the R-lifts of [R] were used to give new proofs of modularity theorems that did not use TW systems but nevertheless generally relied on the set-up in [W] of comparing deformation and Hecke rings and the numerical criterion for isomorphisms of complete intersections of [W].

2. By cutting the Jacobians we work with into pieces according to the action of the Atkin-Lehner involutions we can make the proof of Proposition 1 work when the prime q is not 1 mod p.

3. It is possible to prove the following more refined theorem using the methods here.

Theorem 2. *Let $\overline{\rho} : G_{\mathbf{Q}} \rightarrow GL_2(k)$ be a continous, odd representation, with k a finite field of characteristic bigger than 3, such that $Ad^0(\overline{\rho})$ is irreducible. Assume that $\overline{\rho}$ is modular, and at p is up to twist neither the trivial representation nor unramified with image of order divisible by p.*

Let $\rho : G_{\mathbf{Q}} \rightarrow GL_2(W(k))$ be a continuous lift of $\overline{\rho}$ that has the following properties:

- *ρ is minimally ramified at the primes of ramification* $\mathrm{Ram}(\overline{\rho})$ *of $\overline{\rho}$,*
- *ρ is of weight 2 at p, and Barsotti-Tate at p if $\overline{\rho}$ is finite, flat at p,*
- *the set of primes* $\mathrm{Ram}(\rho)$ *ramified in ρ is finite,*
- *ρ is semistable at all the primes of* $\mathrm{Ram}(\rho) \backslash \mathrm{Ram}(\overline{\rho})$,
- *for the primes q in* $\mathrm{Ram}(\rho)$ *that are not in* $\mathrm{Ram}(\overline{\rho})$, $\overline{\rho}|_{D_q}$ *is not a scalar.*

Then ρ arises from a newform of weight 2.

It will be of interest to have a less restrictive theorem accessible by the methods of this paper, for instance be able to treat (many) 3-adic representations. Conditions ensuring minimality of ramification of ρ at $\mathrm{Ram}(\overline{\rho}) \cup p$ seem essential.

Acknowledgements: I would like to thank Srinath Baba for a conversation in May, 2002 in Montreal which prompted me to think again of the idea of [K1] after a lapse of 2 years, and Bas Edixhoven for some helpful comments.

References

[DT] F. DIAMOND, R. TAYLOR, *Lifting modular mod l representations.* Duke Math. J. **74** no. **2** (1994), 253–269.

[K] C. KHARE, *On isomorphisms between deformation rings and Hecke rings.* To appear in Inventiones mathematicae, preprint available at `http://www.math.utah.edu/~shekhar/papers.html`

[K1] C. KHARE, *Limits of residually irreducible p-adic Galois representations.* Proc. Amer. Math. Soc. **131** (2003), 1999–2006.

[KR] C. KHARE, R. RAMAKRISHNA, *Finiteness of Selmer groups and deformation rings.* To appear in Inventiones mathematicae, preprint available at `http://www.math.utah.edu/~shekhar/papers.html`

[Ri] K. RIBET, *Report on mod ℓ representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. In Motives, Proc. Sympos. Pure Math. **55**, part **2** (1994), 639–676.

[R] R. RAMAKRISHNA, *Deforming Galois representations and the conjectures of Serre and Fontaine-Mazur.* Annals of Math. **156** (2002), 115–154.

[T] R. TAYLOR, *On icosahedral Artin representations II.* To appear in American J. of Math.

[TW] R. TAYLOR, A. WILES, *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. (2) **141** (1995), 553–572.

[W] A. WILES, *Modular elliptic curves and Fermat's last theorem.* Ann. of Math. **141** (1995), 443–551.

Chandrashekhar KHARE
Department of Mathematics
University of Utah
155 S 1400 E
Salt lake City, UT 84112
E-mail : `shekhar@math.utah.edu`

School of Mathematics
TIFR
Homi Bhabha Road
Mumbai 400 005, INDIA
E-mail : `shekhar@math.tifr.res.in`