

JOURNAL

de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Luis DIEULEFAIT et Xavier TAIXÉS I VENTOSA

Congruences between modular forms and lowering the level mod ℓ^n

Tome 21, n° 1 (2009), p. 109-118.

<http://jtnb.cedram.org/item?id=JTNB_2009__21_1_109_0>

© Université Bordeaux 1, 2009, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (<http://jtnb.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://jtnb.cedram.org/legal/>). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>

Congruences between modular forms and lowering the level mod ℓ^n

par LUIS DIEULEFAIT et XAVIER TAIXÉS I VENTOSA

RÉSUMÉ. Dans cet article, nous étudions le comportement des groupes d'inertie pour des représentations galoisiennes modulaires mod ℓ^n et dans quelques cas on démontre une généralisation du résultat de descente de niveau de Ribet (cf. [9]).

ABSTRACT. In this article we study the behavior of inertia groups for modular Galois mod ℓ^n representations and in some cases we give a generalization of Ribet's lowering the level result (cf. [9]).

1. Introduction

Let $f = q + \sum_2^\infty a_i q^i$ and $g = q + \sum_2^\infty b_i q^i$ be two newforms of weight 2, trivial Nebentypus character and level N_f and N_g respectively. Let K_f and K_g be the fields generated by the coefficients of f and g , and let K be their composite field. We denote by \mathcal{O}_f , \mathcal{O}_g and \mathcal{O} their rings of integers. Let $\ell > 2$ be a prime and let ρ_f (resp. ρ_g) be the 2-dimensional ℓ -adic representation associated to f (resp. g), with values in $\mathcal{O}_{f,\ell} := \mathcal{O}_f \otimes \mathbb{Z}_\ell$ (resp. $\mathcal{O}_{g,\ell}$).

Recall that the representation ρ_f ramifies exactly at the primes in the level of N_f and at ℓ . For any unramified prime t , the image of the arithmetic Frobenius $\text{Frob } t$ has $\text{trace}(\rho_f(\text{Frob } t)) = a_t$, the Fourier coefficient and t -th Hecke eigenvalue of f . Also, the determinant of ρ_f is the ℓ -adic cyclotomic character χ .

For a given integer n , we use the projection

$$\mathcal{O}_{f,\ell} \rightarrow \mathcal{O}_{f,\ell}/\ell^n \mathcal{O}_{f,\ell}$$

and we semi-simplify to obtain the mod ℓ^n representation

$$\bar{\rho}_{f,\ell^n} : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{O}_{f,\ell}/\ell^n \mathcal{O}_{f,\ell}).$$

Using the decomposition of ℓ in K_f , $\ell = \lambda_1^{e_1} \cdots \lambda_k^{e_k}$ and the projection

$$\prod \mathcal{O}_{f,\lambda_i}/\lambda_i^{e_i n} \mathcal{O}_{f,\lambda_i} \rightarrow \mathcal{O}_{f,\lambda_i}/\lambda_i^n \mathcal{O}_{f,\lambda_i}$$

we obtain the mod λ^n representation attached f for a fixed place $\lambda \mid \ell$ in K_f

$$\bar{\rho}_{f,\lambda^n} : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{O}_{f,\lambda}/\lambda^n \mathcal{O}_{f,\lambda}).$$

Let us fix a place $\lambda \mid \ell$ in K and let us denote also by λ its restrictions to K_f and to K_g .

From now on let us assume that the mod λ representation $\bar{\rho}_{f,\lambda}$ is irreducible (then $\bar{\rho}_{f,\lambda}$ is odd and absolutely irreducible), that $N_g \mid N_f$ and that $\ell \nmid N_f$.

If we take the ideal $\lambda^n \subset \mathcal{O}$ and the projection

$$\pi : \mathcal{O} \rightarrow \mathcal{O}/\lambda^n,$$

then we say that two numbers $\alpha \in \mathcal{O}_f$ and $\beta \in \mathcal{O}_g$ are congruent modulo λ^n if $\pi(\alpha) = \pi(\beta)$.

Definition 1. *f and g are **congruent modulo λ^n** if $a_p \equiv b_p \pmod{\lambda^n}$ for almost every prime p .*

In fact, this is equivalent to say that their associated mod λ^n Galois representations are isomorphic.

Theorem 1. $f \equiv g \pmod{\lambda^n} \iff \bar{\rho}_{f,\lambda^n} \sim \bar{\rho}_{g,\lambda^n}$.

This is just an automatic consequence of Chebotarev's density theorem since we are assuming that the traces of the images of almost all Frobenius elements are congruent to each other. The Brauer-Nesbitt theorem guarantees that these elements determine the representation for $\ell > 2$ and $n = 1$, and for $n > 1$ Mazur ([7], p.253) gives an analogous result. Observe that we do not have to consider the semi-simplifications of the mod λ^n representations since we are assuming that they are absolutely irreducible.

Given a representation ρ , let $n_{\rho,p}$ (resp. $n_{\bar{\rho},p}$) be the conductor of ρ (resp. $\bar{\rho}$) in the prime p . In [1], Carayol studies for a given mod ℓ representation, how much the conductor of a deformation can increase. He proves the following result.

Proposition 1. *Let $N = p_1^{n_{p_1}} \dots p_k^{n_{p_k}}$ and $\bar{N} = p_1^{\bar{n}_{p_1}} \dots p_k^{\bar{n}_{p_k}}$ be the conductors of a λ -adic representation ρ and the corresponding mod λ representation $\bar{\rho}_\lambda$, respectively. Let p be a prime dividing N , $p \neq \ell$, and suppose ρ is such that $n_p > \bar{n}_p$. Then locally at p ρ is of one of the following types*

- (1) $\rho_p = \mu \oplus v$, with $n_{\mu,p} = 1$ and $n_{\bar{\mu},p} = 0$, and then $n_p = n_{v,p} + 1$
- (2) $\rho_p = \mu \otimes sp(2)$, with $n_{\mu,p} = 0$, and then $n_p = 1$.
- (3) $\rho_p = \mu \otimes sp(2)$, with $n_{\mu,p} = 1$ and $n_{\bar{\mu},p} = 0$, and then $n_p = 2$.
- (4) *The irreducible case in which $n_p = 2$.*

In our case, since we are working without nebentypus, the first case reduces to $\rho_p = \mu \oplus \mu^{-1}$ and then $n_p = n_{v,p} + 1 = n_{\mu,p} + 1 = 2$. Since in all the cases $n_p \leq 2$ we get the following Corollary.

Corollary 1. *If f and g are congruent mod λ with $N_g \mid N_f$, then for any prime p dividing N_f but not dividing ℓN_g , $p^3 \nmid N_f$.*

More specifically, if we fix a mod λ representation $\bar{\rho}$ of conductor \bar{N} , the level of all the modular deformations of $\bar{\rho}$ with trivial character, unramified outside $p\bar{N}$ for a prime $p \nmid \ell\bar{N}$ and minimal at \bar{N} , divides $N = p^2\bar{N}$.

In the following section we state the main results of this article. They describe, under certain conditions, how the inertia group of the Galois representations discussed above behave. In the next section we introduce Taylor-Wiles' Theorem as we need it for our proof, which will be given in §4. Finally we discuss possible developments of this work.

Acknowledgments: the second named author wants to thank G. Böckle for interesting conversations and also Prof. G. Frey and G. Wiese for their several helpful corrections and remarks.

2. Main results

When we have two newforms f and g as in the previous section, such that they are congruent mod λ , $N_g \mid N_f$, and g is minimal in the sense that the conductor \bar{N} of the residual representations $\bar{\rho}_{f,\lambda} \sim \bar{\rho}_{g,\lambda}$ equals N_g , we ask ourselves the following two related questions: Which is the biggest n such that f and g are congruent modulo λ^n ? Once this value of n is known, is there a reason that explains why f and g are not congruent anymore mod λ^{n+1} ?

In [11] we give an algorithm that answers the first question for every possible λ . Theorem 2 below is a result that answers the second question in some cases.

Definition 2. Let $L = \mathbb{Q}(\sqrt{(-1)^{(\ell-1)/2}\ell})$. Then $\bar{\rho}_{g,\lambda}$ is strongly irreducible if $\bar{\rho}_{g,\lambda}|_{G_L}$ is irreducible.

Proposition 2. Let $\ell > 3$. Then $\bar{\rho}_{g,\lambda}$ is strongly irreducible.

Proof. Assuming that $\bar{\rho}_{g,\lambda}$ is irreducible as in our case, if g is a newform of weight 2 and ℓ does not divide its level, clearly the residual representation $\bar{\rho}_{g,\lambda}$ has Serre's weight 2. Thus, this gives a precise information of the action of inertia at ℓ , and this is enough to show that $\bar{\rho}_{g,\lambda}|_{G_L}$ is irreducible if $\ell > 3$. This is proved in [10] as part of the proof that the dihedral case can not occur for semistable weight 2 representations. □

Let us remark that the condition of $\bar{\rho}|_{G_L}$ being irreducible for $\ell = 3$ is easily checked just by finding a prime $p \equiv 2 \pmod{3}$ such that $b_p \not\equiv 0 \pmod{\lambda}$, $\lambda \mid 3$, or equivalently, such that $\text{Norm}(b_p) \not\equiv 0 \pmod{3}$ (where b_p is the p -coefficient of g).

Theorem 2. Let $\ell, p \nmid N_g$, $\ell > 2$ be two different prime numbers. Let f be in $S_2(p^k N_g)$, $k \geq 1$, and let $g \in S_2(N_g)$ be minimal with respect to λ in the sense defined above. Both cusp forms are assumed to have trivial

nebentypus. Suppose that $\bar{\rho}_{f,\lambda} \sim \bar{\rho}_{g,\lambda}$ and they are irreducible, and assume that for any other $h \in S_2(N_g)$, $\bar{\rho}_{g,\lambda} \not\sim \bar{\rho}_{h,\lambda}$. If $\ell = 3$, let $L = \mathbb{Q}(\sqrt{-3})$ and suppose that $\bar{\rho}_{g,\lambda}|_{G_L}$ is irreducible. Then,

$$m := \min\{n \in \mathbb{N} : \bar{\rho}_{f,\lambda^n} \not\sim \bar{\rho}_{g,\lambda^n}\} = \min\{n \in \mathbb{N} : \bar{\rho}_{f,\lambda^n}|_{I_p} \not\sim \bar{\rho}_{g,\lambda^n}|_{I_p}\}.$$

Hence, what we show is that in many cases the cause of the break of the congruence when increasing the power of λ is due precisely to the non-triviality of the action of the inertia group at a prime in N_f/N_g . Let us remark that this is specific to the situation we are in, namely when N_g is a proper divisor of N_f . If this were not the case and $N_f = N_g$ were congruent modulo some λ^n (in [11] we compute dozens of examples), it is clear that the reason of not being congruent anymore modulo λ^{n+1} can not be related to ramification at any place.

Theorem 2 can be reinterpreted as a generalization to higher exponents of Ribet's Lowering the Level result [9].

Corollary 2 (Lowering the level modulo λ^n). *Let f be a newform of weight 2, trivial character and level $p^k N$ ($p \nmid N$) such that for a given $\lambda \nmid 2pN$ and an integer n , $\bar{\rho}_{f,\lambda^n}$ does not ramify at p . Let us suppose that there exists exactly one modular form g of weight 2 and level N congruent to f modulo λ (Ribet's lowering the level provides **at least one**) satisfying the strong irreducibility condition. Then, lowering the level can be generalized modulo λ^n , i.e., f and g are congruent also modulo λ^n .*

In the previous section we saw that there is no congruence between two newforms of level N and $p^k N$ if $k > 2$. In the case $k = 1$, we can rewrite the Theorem as follows.

Corollary 3. *With the same conditions as in Theorem 2, let $k = 1$. Then*

$$\rho_f|_{I_p} = \left\langle \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \right\rangle$$

where $v_\ell(a) = m - 1$. So, the image of the mod λ^m representation of f contains an ℓ -group.

Proof. It is well known that if a representation is semi-stable at p , the restriction of ρ on the inertia at p is

$$\left(\begin{array}{cc} 1 & * \\ 0 & 1 \end{array} \right)$$

for some $* \neq 0$. Since we know that the inertia at p vanishes modulo λ^n exactly when $n < m$, then we know that $* \equiv 0 \pmod{\lambda^n}$ if and only if $n < m$. Then $v_\ell(*) = m - 1$. \square

In [11] we computed several examples where we can apply Theorem 2. It is easy to check that most of them satisfy also the hypothesis of Corollary 3.

In Table 1 we show some of these examples. In particular, we can see that all but one of them (the one with $p = 13^2$) satisfy also the conditions from Corollary 3.

We divided the table in 3 different parts: the first one has some of the elements with the biggest ℓ 's that we found. The greatest one is as big as $1.75 \cdot 10^{18}$. The next part includes the elements with a big p . Since we worked with elements with $N \leq 2000$ and the smallest level appearing is $N = 11$, we know that p can not be bigger than 181. We have actually precisely one example with this p . Finally, in the last section we have the couples with the biggest m 's. It is remarkable to see that there is one element where m is bounded between $m \geq 10$ and $m \leq 11$.

Every pair (N, i) in Table 1 corresponds to the i -th element of the basis of S_2^{new} sorted with the `SortDecomposition` function of Magma [6].

For any two-dimensional Galois representation ρ , let us denote by ρ' its projectivization. Then we have the following:

Corollary 4. *With the same conditions as in Theorem 2, let $k = 1$. Let us suppose also that g has Complex Multiplication (in this case, $\text{Im}(\rho'_{g,\lambda})$ is a dihedral group). Then the image of $\rho'_{f,\lambda}$ is not dihedral and the number m of the Theorem is the smallest one such that the first of the following inclusions is not an equality:*

$$\text{Dihedral group} \subsetneq \bar{\rho}'_{f,\lambda^m} \subsetneq PGL_2(\mathcal{O}_{f,\lambda}/\lambda^m \mathcal{O}_{f,\lambda}).$$

Proof. It is clear that for $m - 1$, $\bar{\rho}'_{g,\lambda^{m-1}} \sim \bar{\rho}'_{f,\lambda^{m-1}}$, and since g has CM, $\bar{\rho}'_{f,\lambda^{m-1}}$ must be a dihedral group. However, for m , since $\bar{\rho}'_{f,\lambda^m}$ contains an element provided by Theorem 2 which can not be contained in a dihedral group, it is clear that $\bar{\rho}'_{f,\lambda^m}$ is not a dihedral group anymore.

For the other inequality it is clear that it is never an equality, because if it were, $\bar{\rho}'_{f,\lambda^n}$ would always equal $PGL_2(\mathcal{O}_{f,\lambda}/\lambda^n \mathcal{O}_{f,\lambda})$, for every n . And this is impossible, since we know that for $n < m$, $\bar{\rho}'_{f,\lambda^n}$ is a dihedral group. \square

Let us remark that the conditions in the Theorem are not too restrictive. For example, just by taking one newform g of level N with residual mod λ representation satisfying the strong irreducibility condition, minimal with respect to λ and not congruent to any other newform of the same level, using Ribet's Raising the Level we can find infinitely many examples in which we can apply our results.

The conditions we are imposing on the pair (g, ℓ) are generic in the following sense: given g they are satisfied for almost every prime ℓ . In fact, given g it is well-known that for almost every prime ℓ the representation

TABLE 1. Examples satisfying Theorem 2

N_f	i	N_g	j	ℓ^{m-1}	p^k	m
$1678 = 2 \cdot 839$	8	839	2	1750283935190857471	2	2
$1707 = 3 \cdot 569$	4	569	2	122272440801294601	3	2
$1941 = 3 \cdot 647$	4	647	3	5539230441648341	3	2
$1839 = 3 \cdot 613$	4	613	3	3726338419619653	3	2
$1757 = 7 \cdot 251$	5	251	2	902088490528867	7	2
$1797 = 3 \cdot 599$	6	599	3	779881437372101	3	2
$1941 = 3 \cdot 647$	3	647	3	665741756680589	3	2
$1945 = 5 \cdot 389$	5	389	5	571255479184807	5	2
$1754 = 2 \cdot 877$	4	877	3	551522526259063	2	2
$1706 = 2 \cdot 853$	5	853	2	372293980443053	2	2
$1906 = 2 \cdot 953$	6	953	2	303408887531093	2	2
$1851 = 3 \cdot 617$	7	617	2	286866593268389	3	2
$1991 = 11 \cdot 181$	4	11	1	$3^2 \leq \ell^{m-1} \leq 3^3$	181	$3 \leq m \leq 4$
$1969 = 11 \cdot 179$	4	11	1	3	179	2
$1903 = 11 \cdot 173$	4	11	1	7	173	2
$1859 = 11 \cdot 13^2$	8	11	1	3	13^2	2
$1837 = 11 \cdot 167$	5	11	1	13	167	2
$1937 = 13 \cdot 149$	4	149	2	$3^9 \leq \ell^{m-1} \leq 3^{10}$	13	$10 \leq m \leq 11$
$1934 = 2 \cdot 967$	2	967	1	$625 = 5^4$	2	5
$1708 = 2^2 \cdot 7 \cdot 61$	6	$2^2 \cdot 61$	2	$3^3 \leq \ell^{m-1} \leq 3^4$	7	$4 \leq m \leq 5$
$1643 = 31 \cdot 53$	3	53	2	$5^3 \leq \ell^{m-1} \leq 5^4$	31	$4 \leq m \leq 5$
$1426 = 2 \cdot 23 \cdot 31$	13	$23 \cdot 31$	5	$81 = 3^4$	2	5
$1401 = 3 \cdot 467$	1	467	2	$625 = 5^4$	3	5
$1298 = 2 \cdot 11 \cdot 59$	11	$11 \cdot 59$	4	$81 = 3^4$	2	5
$1158 = 2 \cdot 3 \cdot 193$	13	$2 \cdot 193$	4	$625 = 5^4$	3	5
$1115 = 5 \cdot 223$	8	223	2	$81 = 3^4$	5	5

$\rho_{g,\lambda}$ is irreducible, as proved by Ribet in [8] (see also [5] for an explicit determination of the finite set of reducible primes), and as we have already explained the strong irreducibility condition is automatic if $\ell > 3$. It is also well-known that the number of primes giving congruences between modular forms of fixed (or bounded) level, called “congruence primes”, is finite: this can easily be proved by applying Dirichlet’s principle (there are only finitely many cusp forms of bounded level) and the fact that two newforms that are congruent modulo infinitely many primes must be equal. Also, the condition of being minimal with respect to λ is equivalent, by Ribet’s lowering the level, to the fact that g is not congruent to some modular form g' of level equal to a proper divisor of N , and so if this condition is not satisfied ℓ has to be a congruence prime and we know that there are only finitely many of them because the levels of g and g' are both bounded by N . We conclude that for any level N there is constant C such that for any weight

2 modular form g of level N and any prime $\ell > C$ the pair (g, λ) satisfies the conditions of the Theorem.

3. Taylor-Wiles

To prove Theorem 2, the main result we need is an extended version of the Taylor-Wiles Theorem. In order to state it, we have to introduce some notation.

Let $\bar{\rho} := \bar{\rho}_{g,\lambda}$, which we assume to be strongly irreducible. Let Σ be a finite set of prime numbers. We say that a representation ρ deforming $\bar{\rho}$ is of type Σ if

- (1) $\chi_\ell^{-1} \det \rho$ has finite order not divisible by ℓ .
- (2) ρ is minimally ramified outside Σ .
- (3) ρ is flat at ℓ in the sense of [3] (see also [2]).

Let R_Σ be the $\mathcal{O}_{g,\lambda}$ -algebra corresponding to the universal deformation of type Σ . Let Φ_Σ be the set of newforms f such that $\rho_{f,\lambda}$ is a deformation of $\bar{\rho}$ of type Σ .

For every f in Φ_Σ , consider the map $R_\Sigma \rightarrow \mathcal{O}_{f,\lambda}$ corresponding to $\rho_{f,\lambda}$. We define $\mathbb{T}_\Sigma \subset \prod_{f \in \Phi_\Sigma} \mathcal{O}_{f,\lambda}$ as the image of R_Σ .

Let ϕ_Σ be the surjective map

$$\phi_\Sigma : R_\Sigma \rightarrow \mathbb{T}_\Sigma.$$

Theorem 3 (Taylor-Wiles). *Let ℓ be an odd prime. If $\ell = 3$, let $L = \mathbb{Q}(\sqrt{-3})$ and suppose $\bar{\rho}|_{G_L}$ is irreducible. Then ϕ_Σ is an isomorphism and R_Σ is a complete intersection.*

Proof. In [3] and [4] this is proved with the condition $\bar{\rho}|_{G_L}$ irreducible with $L = \mathbb{Q}(\sqrt{(-1)^{(\ell-1)/2}\ell})$ and in Proposition 2 we already saw that for $\ell > 3$ this condition is always satisfied. □

4. Proof of the Theorem

We will need first to introduce three auxiliary results.

Proposition 3. *Let f be a modular form in $S_2(N)$, and suppose that there exists no other modular form g of level N congruent to f modulo λ . Then K_f is unramified at λ .*

Proof. If K_f ramifies at λ , there exists a non trivial Galois conjugation σ such that $\alpha \equiv \sigma(\alpha) \pmod{\lambda}$ for every algebraic integer α in K_f . In this case, $\sigma(f)$ is congruent with f modulo λ , which is not possible by hypothesis. □

Proposition 4. *Let $\bar{\rho}$ be a mod λ irreducible representation of conductor N , with $\ell > 2$. If $\ell = 3$, suppose that $\bar{\rho}|_{G_L}$ is irreducible. Let us suppose that*

there exists only one newform g of weight 2, trivial character, and level N such that $\bar{\rho} = \bar{\rho}_{g,\lambda}$. Let \mathcal{Q} be the following set of deformation conditions:

- The deformations are unramified outside ℓN .
- The deformations are minimally ramified everywhere.
- The determinant of the deformations is the cyclotomic character.
- The deformations are flat (locally at ℓ).

Then, the deformation ring $\mathcal{R}_{\mathcal{Q}}$ is the ring of integers $\mathcal{O}_{g,\lambda}$.

Proof. What we are considering is the problem of deformations of type $\Sigma = \emptyset$. By the Theorem of Taylor-Wiles, we know that the universal deformation ring R_{Σ} must be isomorphic to \mathbb{T}_{Σ} . By hypothesis, there is only one $\overline{\mathbb{Q}}_{\ell}$ -point in \mathbb{T}_{Σ} . Then \mathcal{R}_{Σ} must be $\mathcal{O}_{g,\lambda}$ itself. \square

Lemma 1. *Let \mathcal{O}_{λ} be the ring of integers of a finite unramified extension of \mathbb{Q}_{ℓ} . Let ρ_1 and ρ_2 be two representations, both deforming $\bar{\rho}$*

$$\rho_1, \rho_2 : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{O}_{\lambda}/\lambda^n \mathcal{O}_{\lambda})$$

satisfying the same deformation conditions \mathcal{Q} , such that for these conditions the universal deformation ring is \mathcal{O}_{λ} . Then, ρ_1 is equivalent to ρ_2 .

Proof. We suppose they are different. The universal deformation (under conditions \mathcal{Q}) is

$$\rho^{univ} : G_{\mathbb{Q}} \rightarrow GL_2(\mathcal{O}_{\lambda}).$$

Then, we have that there exist two homomorphisms h_1 and h_2

$$h_1, h_2 : \mathcal{O}_{\lambda} \rightarrow \mathcal{O}_{\lambda}/\lambda^n \mathcal{O}_{\lambda}$$

such that they induce the identity in the residue fields and also $h_i \circ \rho^{univ} = \rho_i$. Then h_1 and h_2 must be different homomorphisms, but since there exists only one natural projection from \mathcal{O}_{λ} to $\mathcal{O}_{\lambda}/\lambda^n \mathcal{O}_{\lambda}$ fixing the residue fields, we arrive at a contradiction. \square

Proof of Theorem 2. We consider the same set of deformation conditions \mathcal{Q} as in Proposition 4, with $N = N_g$. We consider also the set of conditions \mathcal{Q}' as follows:

- The deformations are unramified outside $\ell p N_g$.
- The deformations are minimally ramified locally at every place $q \neq p$.
- The determinant of the deformations is the cyclotomic character.
- The deformations are flat locally at ℓ .

So, the set of conditions \mathcal{Q}' is different from the set of conditions \mathcal{Q} only because now we allow ramification at p .

By Carayol's result, we know that all such deformations must be in level $p^k N_g$ with $k \leq 2$. Then, by Taylor-Wiles $\mathcal{R}_{\mathcal{Q}'}$ is isomorphic to a Hecke algebra $\mathbb{T}_{\mathcal{Q}'}$ of level $p^2 N_g$.

Obviously $\bar{\rho}_{g,\lambda^{m-1}}$ and $\bar{\rho}_{g,\lambda^m}$ satisfy conditions \mathcal{Q} and \mathcal{Q}' . Since $\bar{\rho}_{f,\lambda^{m-1}} \sim \bar{\rho}_{g,\lambda^{m-1}}$, $\bar{\rho}_{f,\lambda^{m-1}}$ satisfies also \mathcal{Q} and \mathcal{Q}' .

By Proposition 4, $\mathcal{R}_{\mathcal{Q}} = \mathcal{O}_{g,\lambda}$. Since K_g is unramified by Proposition 3, we can apply Lemma 1 to assert that any two mod λ^n deformations satisfying the deformation conditions \mathcal{Q} must be the same. By hypothesis we know that $\bar{\rho}_{f,\lambda^m} \not\sim \bar{\rho}_{g,\lambda^m}$. This means that $\bar{\rho}_{f,\lambda^m}$ can not satisfy conditions \mathcal{Q} . However, $\bar{\rho}_{f,\lambda^m}$ clearly satisfies conditions \mathcal{Q}' . Since the only difference between both conditions is the ramification at p , the reason for $\bar{\rho}_{f,\lambda^m}$ not to satisfy \mathcal{Q} must be precisely that $\bar{\rho}_{f,\lambda^m}$ ramifies at p , as we wanted to prove. □

5. Further work

It would be interesting to improve the main result by relaxing the assumptions. For example, one should consider in which cases it is possible to eliminate the condition “for any other $h \in S_2(N_g)$, $\bar{\rho}_{g,\lambda} \not\sim \bar{\rho}_{h,\lambda}$ ” in the main theorem. In this more general case, the minimal universal deformation ring will be more complicated, though it is known to be finite flat complete intersections by the result of Taylor-Wiles.

Looking at Table 1 we saw that ℓ and p seem not to be bounded (p is clear). However, we wonder if there is any global bound for m or there are examples with m arbitrarily large.

References

- [1] HENRI CARAYOL, *Sur les Représentations Galoisienne modulo ℓ attachées aux formes modulaires*. Duke mathematical journal **59**, 3 (1989), 785–801.
- [2] HENRI DARMON, FRED DIAMOND AND RICHARD TAYLOR, *Fermat’s Last Theorem*. International Press, 1995.
- [3] EHUD DE SHALIT, *Hecke rings and universal deformation rings*, in *Modular Forms and Fermat’s Last Theorem*. Springer, New York, 1997.
- [4] FRED DIAMOND, *An extension of Wiles’ results*, in *Modular Forms and Fermat’s Last Theorem*. Springer, New York, 1997.
- [5] LUIS DIEULEFAIT AND NURIA VILA, *Projective linear groups as Galois groups over \mathbb{Q} via modular representations*. J. Symbolic Comput. **30** (2000), 799–810.
- [6] WIEB BOSMA, JOHN CANNON AND CATHERINE PLYOUST, *The Magma algebra system I: The user language*. Journal of Symbolic Computation **24**, 3-4 (1997), 235–265.
- [7] BARRY MAZUR, *An introduction to the deformation theory of Galois representations*, in *Modular Forms and Fermat’s Last Theorem*. Tata Institute of Fundamental Research Studies in Mathematics, Springer, New York, 1997, 243–311.
- [8] KENNETH A. RIBET, *On ℓ -adic representations attached to modular forms II*. Glasgow Math. J. **27** (1985), 185–194.
- [9] KENNETH A. RIBET, *On Modular Representations of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms*. Invent. Math. **100** (1990), 431–476.
- [10] KENNETH A. RIBET, *Images of semistable Galois representations*. Olga Taussky-Todd: in memoriam. Pacific J. Math. (1997), Special Issue, 277–297.
- [11] XAVIER TAIXÉS I VENTOSA, *Theoretical and algorithmic aspects of congruences between modular Galois representations*. Ph.D. Thesis, Institut für Experimentelle Mathematik (Universität Duisburg-Essen) (2009).

Luis DIEULEFAIT

Dept. d'Àlgebra i Geometria, Universitat de Barcelona

Gran Via de les Corts Catalanes 585

08007 - Barcelona, Catalonia, Spain

E-mail: ldieulefait@ub.edu

URL: <http://atlas.mat.ub.es/personals/dieulefait>

Xavier TAIXÉS I VENTOSA

Institut für Experimentelle Mathematik, Universität Duisburg-Essen

Ellernstraße 29

45326 Essen, Germany

E-mail: xavier@iem.uni-due.de

URL: <http://www.exp-math.uni-essen.de/~xavier>