# LEVEL-LOWERING FOR HIGHER CONGRUENCES OF MODULAR FORMS

NEIL DUMMIGAN

Abstract. We prove a level-lowering result for modular forms mod $\lambda^n$, and use it to calculate some Tamagawa factors.

## 1. Introduction

Let $f$ be a new Hecke eigenform of weight $k \geq 2$ for the congruence subgroup $\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : N \mid c \right\}$ (level $N$ and trivial character). So $f$ is a holomorphic function on the completed upper half plane, vanishing at the cusps, and satisfying $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$. It is an eigenfunction for all the Hecke operators $T_m$ for $m \geq 1$, and does not arise from a congruence subgroup of level strictly dividing $N$. Write $f = \sum_{m=1}^{\infty} a_m q^m$ for the Fourier expansion of $f$, where $q = e^{2\pi i z}$. We suppose that $f$ is normalised, i.e. $a_1 = 1$, in which case $a_m$ is the eigenvalue of $T_m$ for all $m \geq 1$. These eigenvalues generate a totally real field $E$ of finite degree over $\mathbb{Q}$; in fact they lie in the ring of integers $O_E$.

It follows from a theorem of Deligne [De] that to $f$ may be associated continuous representations

$$\rho_\lambda : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, E_\lambda)$$

for each prime ideal $\lambda$ of $O_E$, where $E_\lambda$ is the completion. Let $l$ be the rational prime that $\lambda$ divides. These representations satisfy the following properties:

(1) For all primes $p \nmid Nl$, $\rho_\lambda$ is unramified at $p$, i.e. the image of an inertia subgroup $I_p$ is trivial.
(2) For any prime $p \nmid Nl$, if $\mathrm{Frob}_p$ is a Frobenius element at $p$, i.e. an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that reduces "mod $p$" to the generating $p^{\mathrm{th}}$-power automorphism of $\overline{\mathbb{F}}_p$, then the characteristic polynomial of $\rho_\lambda(\mathrm{Frob}_p^{-1})$ is $x^2 - a_p x + p^{k-1}$.

By a theorem of Deligne-Langlands [La] and Carayol [Ca1], the prime-to-$l$ parts of $N$ and the conductor of $\rho_\lambda$ agree, and if $p \mid N$ then $\rho_\lambda$ is ramified at $p$. Let $O_\lambda$ be the ring of integers in $E_\lambda$ and choose a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant $O_\lambda$-lattice in the space of $\rho_\lambda$. Then we get a representation to $\mathrm{GL}(2, O_\lambda)$. Now for any $n \geq 1$ we may compose with the reduction map from $O_\lambda$ to $O/\lambda^n$ to get a representation

$$\rho_{\lambda,n} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, O/\lambda^n).$$

Certainly for any $n$ this representation is unramified at $p \nmid Nl$. But now the possibility arises that it is also unramified at some $p \mid N$.

*Date*: October 14th, 2015.
1991 *Mathematics Subject Classification.* 11F33.

Consider the case $n = 1$. We have

$$\rho_{\lambda,1} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, O/\lambda)$$

arising by reduction $\pmod{\lambda}$ from a $\lambda$-adic representation attached to $f$. We shall suppose now that $l$ is odd and that $\rho_{\lambda,1}$ is irreducible. By a well-known argument involving eigenspaces for a complex conjugation, it follows that $\rho_{\lambda,1}$ is in fact absolutely irreducible. (Now the ambiguity about the choice of a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant $O_\lambda$-lattice disappears, in fact each $\rho_{\lambda,n}$ is uniquely determined up to isomorphism by its character, by Théorème 1 of [Ca2].) Suppose that $\rho_{\lambda,1}$ is unramified at some $p \mid N$. Conjectures of Serre [Se] suggested that there should exist another newform $g$, of weight $k$ and level dividing $N/p$, such that a representation from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{GL}(2, \overline{\mathbb{F}}_l)$, attached to $g$ in a similar manner, is isomorphic to $\rho_{\lambda,1}$, thus accounting for the lack of ramification at $p$. This has now been completely proved. For $l$ odd, this was noted in Theorem 1.1 of [Di2], see also [Ri1], [Ri2], and for $l = 2$ it was completed by [KW1, Theorem 1.2(2)]. Moreover, the "strong", or "qualitative" form of Serre's conjecture (i.e. the modularity of certain types of representations from $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ to $\mathrm{GL}(2, \overline{\mathbb{F}}_l)$) has now been proved by Khare and Wintenberger [KW1],[KW2].

The first result on level-lowering was proved by Mazur (Theorem 6.1 of [Ri1]), in the case where $l$ is odd, $k = 2, p \mid\mid N$, $p \not\equiv 1 \bmod l$ and $\rho_{\lambda,1}$ is irreducible. (When $p = l$, the condition that $\rho_{\lambda,1}$ is unramified at $p$ is replaced by a condition that it is "finite at $p$".) The condition $p \not\equiv 1 \bmod l$ was removed by Ribet in [Ri1] (when $k = 2$ and $l^2 \nmid N$). The restriction $k = 2$ was removed by Rajaei [Raj]. The goal of the present paper is to prove an analogue of Mazur's principle for $n > 1$. Since an earlier version of this paper appeared as a preprint in 2005, Tsaknias has attempted to generalise Ribet's work to $n > 1$, hence to remove the condition $p \not\equiv 1 \bmod l$ [T, Theorem 5.1], but currently there is an unresolved problem with the proof.

Let $\mathbb{T}(N)$ be the $\mathbb{Z}$-algebra generated by the Hecke operators $T_q$, for primes $q \nmid N$, acting on the complex vector space $S_k(\Gamma_0(N))$ of cusp forms of weight $k$ for $\Gamma_0(N)$. For a prime $p \mid\mid N$, let $\mathbb{T}'(N/p)$ be the quotient of $\mathbb{T}(N)$ obtained by restricting to the subspace of $p$-old forms (i.e. the span of the images of $S_k(\Gamma_0(N/p))$ under the maps $f(z) \mapsto f(z)$ and $f(z) \mapsto f(pz)$). This is naturally isomorphic to the $\mathbb{Z}$-algebra generated by the Hecke operators $T_q$, for primes $q \nmid N$, acting on $S_k(\Gamma_0(N/p))$. Associated to the normalised newform $f$ for $\Gamma_0(N)$ is a homomorphism $\theta_f : \mathbb{T}(N) \to O_E$ such that $\theta_f(T_q) = a_q$ for each prime $q \nmid N$, and by reduction $\pmod{\lambda^n}$, a homomorphism $\theta_{f,n} : \mathbb{T}(N) \to O/\lambda^n$ for each $n \geq 1$.

**Theorem 1.1.** *Suppose that $k \geq 2$, $p \mid\mid N$, $l \nmid N$, $l > k - 2$ and $p \not\equiv 1 \bmod l$. Suppose also that $\rho_{\lambda,1}$ is irreducible. Suppose that, for some $n \geq 1$, $\rho_{\lambda,n}$ is unramified at $p$. Then $\theta_{f,n} : \mathbb{T}(N) \to O/\lambda^n$ factors through the $p$-old quotient $\mathbb{T}'(N/p)$.*

The proof is largely modelled on Mazur's original argument, and occupies §§2–5. The strategy of reducing to weight two, described in [Ri2], seems to be unavailable here, so instead we work directly with weight $k$, as in [Ja] and [JL]. A proof of the case $n = 1$ is outlined briefly in [JL].

§6 contains several illustrative examples where $k = 2$ and $f$ is associated with an elliptic curve $E/\mathbb{Q}$. Here, by examining the minimal discriminant of $E$, it is possible to verify directly when $\rho_{l,n}$ is unramified at $p$, at least if $p \neq l$ is a prime of multiplicative reduction. When $k > 2$ we cannot do this, but the theorem has an application to calculating the $\lambda$-part of the Tamagawa factor at $p$ appearing in the Bloch-Kato conjecture, in the special case of the $L$-function attached to the newform $f$. In fact, this was our motivation for proving Theorem 1.1. The case $n = 1$ was applied to Tamagawa factors in §4 of [DSW].

§8 contains an extension of the main theorem to the case that $l = p \neq 2$ and $f$ is of weight 2 with rational coefficients, i.e. $l = p \neq 2$ and $f$ is the modular form attached to an elliptic curve over $\mathbb{Q}$.

In §9 we remark on some strengthenings of the main theorem which facilitate some applications.

To find the examples of §§6 and 8 I used J. Cremona's elliptic curve data (http://homepages.warwick.ac.uk/staff/J.E.Cremona/ftp/data/INDEX.html) and W. Stein's modular forms database, which is no longer available in the same form. I also made much use of the computer package Pari-GP. I thank Cremona for explaining how to feed his data into Pari. I thank also K. Buzzard, B. Edixhoven, F. Jarvis, J. Manoharmayum, A. Pacetti, P. Tsaknias and an anonymous referee for very helpful comments and observations, and G. Wiese for prompting me to revive this old paper.

## 2. Auxiliary primes and Hecke rings

When $k > 2$ we need to use an auxiliary prime $r$. When $k = 2$ this is unnecessary, since the sheaves below are constant, and we do not need a universal elliptic curve. For the remainder of this section we suppose that $k > 2$. The arguments in §§3–5 which prove Proposition 2.2 for $k > 2$ and $\Gamma_1(r, N)$ work just the same to prove Theorem 1.1 for $k = 2$ and $\Gamma_0(N)$.

For $M \geq 1$ let

$$\Gamma_1(M) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) : c \equiv 0, a \equiv d \equiv 1 \pmod{M} \right\},$$

and, for $M$ and $N$ coprime, let $\Gamma_1(M, N) := \Gamma_1(M) \cap \Gamma_0(N)$. The following lemma is a direct consequence of Lemma 11 of [DT], and the discussion which follows it.

**Lemma 2.1.** *Suppose that $k > 2$ and $l > 3$. Let $f$ be a normalised Hecke cusp form for $\Gamma_0(N)$, with an associated $\rho_{f,\lambda,1} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \overline{\mathbb{F}}_l)$ which is irreducible. There exist infinitely many primes $r \nmid lN, r \not\equiv 1 \pmod{l}$ such that if $g$ is a cusp form for $\Gamma_1(r, N)$, a new Hecke eigenform at some level dividing $rN$, with $\rho_{g,\lambda',1}$ equivalent to $\rho_{f,\lambda,1}$, then the level of $g$ divides $N$.*

*Proof.* By [DT, Lemma 11] (which applies for $l > 3$), the irreducibility implies that there exist infinitely many primes $r \nmid lN, r \not\equiv 1 \pmod{l}$ such that $a_r(f)^2 \not\equiv (1+r)^2 \pmod{\lambda}$. This directly excludes one of the possibilities on the Carayol-Livné list [Ca3, Li] of $r$ that can disappear from the conductor on reduction mod $\lambda$ (Case 1 in the introduction to [DT]). In Case 2 ($r \equiv -1 \pmod{l}$), $a_r(f)$ would be $0 \pmod{\lambda}$, which it is not, since $1 + r \equiv 0 \pmod{l}$, while the remaining Case 3 is $r \equiv 1 \pmod{l}$, which we have excluded. □

Let $\mathbb{T}(r, N)$ be the $\mathbb{Z}$-algebra generated by the Hecke operators $T_q$, for primes $q \nmid rN$, and also the diamond operators $\langle a \rangle$, for $a \in (\mathbb{Z}/r\mathbb{Z})^*$, acting on the complex vector space $S_k(\Gamma_1(r, N))$ of cusp forms of weight $k$ for $\Gamma_1(r, N)$. For a prime $p \mid\mid N$, let $\mathbb{T}'(r, N/p)$ be the quotient of $\mathbb{T}(r, N)$ obtained by restricting to the subspace of $p$-old forms. This is naturally isomorphic to the $\mathbb{Z}$-algebra generated by the Hecke operators $T_q$, for primes $q \nmid rN$, and the diamond operators $\langle a \rangle$, for $a \in (\mathbb{Z}/r\mathbb{Z})^*$, acting on $S_k(\Gamma_1(r, N/p))$. For homomorphisms of these Hecke rings attached to $f$ we re-use the earlier notation. In later sections we shall prove the following.

**Proposition 2.2.** *Suppose that $k > 2$, $p \,||\, N$, $l \nmid N$, $l > k-2$ and $p \not\equiv 1 \bmod l$. Suppose also that $\rho_{\lambda,1}$ is irreducible. Let $f$ and $r$ be as in Lemma 2.1, with $r \geq 5$. Suppose that, for some $n \geq 1$, $\rho_{\lambda,n}$ is unramified at $p$. Then $\theta_{f,n} : \mathbb{T}(r, N) \to O/\lambda^n$ factors through the $p$-old quotient $\mathbb{T}'(r, N/p)$.*

**Lemma 2.3.** *Proposition 2.2 implies the case $k > 2$ of Theorem 1.1.*

*Proof.* Let $\mathfrak{m}$ be the maximal ideal that is the kernel of $\theta_{f,1} : \mathbb{T}(r, N) \to O/\lambda$. Let $\mathfrak{m}'$ be its image in $\mathbb{T}'(r, N/p)$. Assume the result of Proposition 2.2. In particular, $\mathfrak{m}'$ is a proper maximal ideal. Let $\mathbb{T}(r, N)_{\mathfrak{m}}$ and $\mathbb{T}'(r, N/p)_{\mathfrak{m}'}$ be completions. These are direct summands of $\mathbb{T}(r, N) \otimes \mathbb{Z}_l$ and $\mathbb{T}'(r, N/p) \otimes \mathbb{Z}_l$ respectively. The extension to $\mathbb{T}(r, N) \otimes \mathbb{Z}_l$ of $\theta_{f,n}$ factors through the summand $\mathbb{T}(r, N)_{\mathfrak{m}}$ thence, by the proposition, through $\mathbb{T}'(r, N/p)_{\mathfrak{m}'}$. Let $\mathbb{T}''(N/p)$ be the $\mathbb{Z}$-algebra generated by the Hecke operators $T_q$, for primes $q \nmid rN$, acting on $S_k(\Gamma_0(N/p))$. It is naturally a quotient of $\mathbb{T}'(r, N/p)$, obtained by restriction to $r$-old forms. Let $\mathfrak{m}''$ be the image of $\mathfrak{m}'$ in $\mathbb{T}''(N/p)$.

I claim that $\mathfrak{m}''$ is a proper maximal ideal, and that the natural restriction map induces an isomorphism $\mathbb{T}'(r, N/p)_{\mathfrak{m}'} \simeq \mathbb{T}''(N/p)_{\mathfrak{m}''}$. This results from the description of $\mathbb{T}'(r, N/p)_{\mathfrak{m}'}$ as the image under $\oplus\, \theta_g$ of $\mathbb{T}'(r, N/p) \otimes \mathbb{Z}_l$ in $\oplus_{[g]} O_g$, where $g$ runs over a set of representatives of $\mathrm{Gal}(\overline{\mathbb{Q}}_l/\mathbb{Q}_l)$-conjugacy classes of normalised newforms of weight $k$ and level dividing $\Gamma_1(r, N/p))$, such that $\ker(\theta_{g,1}) = \mathfrak{m}'$, and $O_g$ is the ring of integers in the extension of $\mathbb{Q}_l$ generated by the eigenvalues of $g$. The condition $\ker(\theta_{g,1}) = \mathfrak{m}'$ is equivalent to $\rho_{g,\lambda',1} \sim \rho_{f,\lambda,1}$, so by choice of $r$ (and Lemma 2.1) these $g$ are all forms for $\Gamma_0(N/p)$. Consequently, $\mathfrak{m}''$ is a proper maximal ideal, and the above description of $\mathbb{T}'(r, N/p)_{\mathfrak{m}'}$ coincides with the analogous description of $\mathbb{T}''(N/p)_{\mathfrak{m}''}$.

Now $\mathbb{T}''(N/p)_{\mathfrak{m}''}$ is the subring of $\mathbb{T}(N/p)_{\mathfrak{n}}$ obtained by dropping $T_r$ and $T_p$, where $\mathfrak{n}$ is the maximal ideal of $\mathbb{T}(N/p)$ associated to $f$ by the usual $n = 1$ level-lowering. As in the proof of Théorème 3 of [Ca2], there is a continuous representation

$$\rho_{\mathfrak{n}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{T}(N/p)_{\mathfrak{n}}),$$

unramified at primes $q \nmid lN/p$, with $\mathrm{tr}(\rho_{\mathfrak{n}}(\mathrm{Frob}_q^{-1})) = T_q$ for such primes. By Chebotarev's Theorem, $T_r$ and $T_p$ belong to the complete subring $\mathbb{T}''(N/p)_{\mathfrak{m}''}$ of $\mathbb{T}(N/p)_{\mathfrak{n}}$. Therefore the subring is the whole ring, and $\theta_{f,n}$ does factor through $\mathbb{T}(N/p)$, hence certainly through $\mathbb{T}'(N/p)$. □

## 3. Galois representations in cohomology

Let $E$, $\lambda$ and $l$ be as in §1. Choose $r$ as in Proposition 2.2. Let $Y_1(r, N)/\mathbb{Z}$ be the scheme representing the functor which, to a scheme $S$, associates the set of isomorphism classes of elliptic curves $E/S$ with Drinfeld $\Gamma_1(r, N)$-structures (see 3.2 and 3.4 of [KM]). This scheme exists by 2.7.4, 4.7.0 and 5.1.1 of [KM], using the fact that $r \geq 4$. Let $f : \mathcal{E} \to Y_1(r, N)$ be the universal elliptic curve. Let $X_1(r, N)/\mathbb{Z}$ be the standard compactification of $Y_1(r, N)$ (see 8.6 of [KM]), and $i : Y_1(r, N) \to X_1(r, N)$ the inclusion. Suppose that $k > 2$, $l > k-2$ and $l \nmid N$. For any $n \geq 1$ let $\mathcal{F}_n$ be the étale sheaf $\mathrm{Sym}^{k-2} R^1 f_*(O/\lambda^n)$ on $Y_1(r, N)/\mathbb{Z}[1/l]$. This sheaf is locally constant, by [Ch I,8.13]FK, since $f$ is proper and smooth and $l$ is invertible on $\mathrm{Spec}(\mathbb{Z}[1/l])$. Denote also by $\mathcal{F}_n$ any base-change of this sheaf. The cohomology with compact supports is defined by

$$H^1_c(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F}_n) := H^1(X_1(r,N)\otimes\overline{\mathbb{Q}}, i_!\mathcal{F}_n)$$

and its image in $H^1(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F}_n)$ by the natural map is, by definition, the parabolic cohomology $H^1_p(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F}_n)$. We may now define $H^1(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F})$, $H^1_c(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F})$ and $H^1_p(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F})$ as inverse limits, with respect to $n$, of the above, and let

$$H^1(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F}(E_\lambda)) = H^1(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F})\otimes_{O_\lambda} E_\lambda, \text{ etc.}$$

It follows from the exactness of inverse limits for systems of finite groups that $H^1_p(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F})$ is the image of $H^1_c(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F})$ in $H^1(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F})$.

By a well-known construction we now get a 2-dimensional $E_\lambda$-subspace $V$ of $H^1_p(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F}(E_\lambda))$ on which $\mathbb{T}(r,N)$ acts via $\theta_f$ (not the full subspace on which $\mathbb{T}(r,N)$ acts via $\theta_f$, but its intersection with invariants of $\mathrm{GL}_2(\mathbb{Z}/r\mathbb{Z})$), stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and realising the representation $\rho_\lambda$. The action of the Hecke operators on the cohomology groups is defined as in [De, (4.5)].

Since $l\nmid rN$ and $l>k$, $H^0(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F}_1)\simeq \mathrm{Sym}^{k-2}((O/\lambda)^2)^{\Gamma(r,N)}$ is trivial, and so $H^1(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F})$ is torsion-free. Hence $H^1_p(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F})$ is torsion-free, so may be thought of as a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant lattice in $H^1_p(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F}(E_\lambda))$. Intersecting $V$ with $H^1_p(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F})$ and projecting to $H^1_p(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F}_n)$ gives us a rank-2 $(O/\lambda^n)$-module $M_n$ (for this we need the irreducibility of $\rho_{\lambda,1}$) realising the representation $\rho_{\lambda,n}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

**Lemma 3.1.** *$M_n$ may be lifted to a Hecke and $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-invariant, rank-2 $(O/\lambda^n)$-submodule of $H^1_c(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F}_n)$, also realising the representation $\rho_{\lambda,n}$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.*

*Proof.* Let $\phi_n : H^1_c(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F}_n)\to H^1_p(Y_1(r,N)\otimes\overline{\mathbb{Q}},\mathcal{F}_n)$ be the natural map. All these cohomology groups can be constructed using local systems on analytic spaces over $\mathbb{C}$. The étale cohomology construction is only needed to get a Galois action. The kernel of $\phi_n$ may be identified with the image in $H^1_c(Y_1(r,N)(\mathbb{C}),\mathcal{F}_n)$ of $\bigoplus_x H^0(\Delta^*_x,\mathcal{F}_n)$, where $x$ runs over cusps (i.e. $X_1(r,N)(\mathbb{C})\backslash Y_1(r,N)(\mathbb{C})$), and $\Delta^*_x$ is a sufficiently small punctured disc centred on $x$. This in turn is identified with $\bigoplus_x H^0(\Gamma_1(r,N)_x,\mathrm{Sym}^{k-2}((O/\lambda^n)^2))$, where $\Gamma_1(r,N)_x$ is the stabiliser of some representative in $\mathfrak{H}^*$ of $x$. This stabiliser is conjugate in $\mathrm{SL}(2,\mathbb{Z})$ to $\langle\begin{pmatrix}1 & h\\ 0 & 1\end{pmatrix}\rangle$, for some divisor $h$ of $rN$. Since $l\nmid rN$ and $l>k-2$, the submodule of invariants of $\Gamma_1(r,N)_x$ in $\mathrm{Sym}^{k-2}((O/\lambda^n)^2)$ has rank one over $O/\lambda^n$, generated by $e_1^{k-2}$, where $\{e_1,e_2\}$ is the appropriate ordered basis of $(O/\lambda^n)^2$.

An explicit calculation now shows that on the part of $\ker\phi_n$ where all the $\langle a\rangle$ (for $a\in(\mathbb{Z}/r\mathbb{Z})^*$) act trivially, the Hecke operator $T_q$ (for prime $q\nmid rN$) acts as multiplication by $1+q^{k-1}$. Since $\rho_\lambda$ is irreducible, it is not the case that $a_q\equiv 1+q^{k-1} \pmod{\lambda}$ for all primes $q\nmid rN$. Choosing a $q$ for which the congruence fails, and taking the intersection of $\phi_n^{-1}M_n$ with $\ker(T_q-a_q)$ produces the desired submodule, which we shall just call $M_n$ from now on. □

## 4. Some exact sequences

As before, $k > 2$, $l \nmid N$, $l > k-2$ and $p \,||\, N$. Choosing an embedding of $\overline{\mathbb{Q}}$ in $\overline{\mathbb{Q}}_p$, there is a natural identification between $H^1_c(Y_1(r,N) \otimes \overline{\mathbb{Q}}, \mathcal{F}_n) \simeq H^1(X_1(r,N) \otimes \overline{\mathbb{Q}}, i_!\mathcal{F}_n)$ and $H^1(X_1(r,N) \otimes \overline{\mathbb{Q}}_p, i_!\mathcal{F}_n)$, compatible with the actions of the subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

The special fibre $X_1(r,N) \otimes \overline{\mathbb{F}}_p$ is composed of two copies of $X_1(r,N/p) \otimes \overline{\mathbb{F}}_p$, which cross at supersingular points (see the proof of Proposition 5.2 below for more detail). Let $\Sigma$ be the set of these supersingular points, viewed as double points on $X_1(r,N) \otimes \overline{\mathbb{F}}_p$.

Let $x$ and $y$ be the inclusions of, respectively, $X_1(r,N) \otimes \overline{\mathbb{F}}_p$ and $X_1(r,N) \otimes \overline{\mathbb{Q}}_p$ in $X_1(r,N) \otimes \mathbb{Z}_p^{\mathrm{un}}$, where $\mathbb{Z}_p^{\mathrm{un}}$ is the ring of integers in the maximal unramified extension of $\mathbb{Q}_p$. (Recall that we have defined $\mathcal{F}_n$ on $Y_1(r,N) \otimes \mathbb{Z}[1/l]$.) By [SGA7, XIII, 2.4.6.6] there is an exact sequence (A)

$$0 \longrightarrow H^1(X_1(r,N) \otimes \overline{\mathbb{F}}_p, i_!\mathcal{F}_n) \longrightarrow H^1(X_1(r,N) \otimes \overline{\mathbb{Q}}_p, i_!\mathcal{F}_n) \longrightarrow X$$

where $X = \bigoplus_{x \in \Sigma} (R^1\Phi_{\overline{\eta}}(\mathcal{F}_n))_x$, in the notation of [SGA7, XIII]. This is compatible with actions of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and Hecke operators $T_q$ for primes $(q, rN) = 1$. The definition of the Hecke operators on $H^1(X_1(r,N) \otimes \overline{\mathbb{F}}_p, i_!\mathcal{F}_n)$ via the same formula as in [De, (4.5)] works because the degeneracy maps $q_1', q_2' : Y_1(r,Nq) \to Y_1(r,N)$ (in Deligne's notation) are étale and finite over the base $\mathbb{Z}[1/q]$, $q_1'$ by [KM, Theorem 3.7.1] (with $\mathcal{E}/(Y_1(r,N) \otimes \mathbb{Z}[1/q])$ for $E/S$), then also $q_2'$, since $q_2' = q_1' \cdot W_q$, with the automorphism $W_q$ as in §5 below.

There is a natural map $q$ from the normalisation $Z := (X_1(r,N/p) \otimes \overline{\mathbb{F}}_p) \amalg (X_1(r,N/p) \otimes \overline{\mathbb{F}}_p)$ to $X_1(r,N) \otimes \overline{\mathbb{F}}_p$. There is an exact sequence

$$0 \longrightarrow i_!\mathcal{F}_n \longrightarrow q_*q^*i_!\mathcal{F}_n \longrightarrow E_n \longrightarrow 0$$

of sheaves on $X_1(r,N) \otimes \overline{\mathbb{F}}_p$ defining a sheaf $E_n$ supported on $\Sigma$. There is an isomorphism between $H^1(X_1(r,N) \otimes \overline{\mathbb{F}}_p, q_*q^*i_!\mathcal{F}_n)$ and $H^1(Z, q^*i_!\mathcal{F}_n)$, which in turn is isomorphic to $(H^1(X_1(r,N/p) \otimes \overline{\mathbb{F}}_p, i_!\mathcal{F}_n))^2 \simeq (H^1(X_1(r,N/p) \otimes \overline{\mathbb{Q}}_p, i_!\mathcal{F}_n))^2$. See Lemma 16.1 of [Ja]. We get then an exact sequence (B)

$$\begin{aligned} H^0(X_1(r,N) \otimes \overline{\mathbb{F}}_p, E_n) &\longrightarrow H^1(X_1(r,N) \otimes \overline{\mathbb{F}}_p, i_!\mathcal{F}_n) \longrightarrow \\ (H^1(X_1(r,N/p) \otimes \overline{\mathbb{F}}_p, i_!\mathcal{F}_n))^2 &\longrightarrow \quad 0. \end{aligned}$$

This is compatible with actions of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ and Hecke operators $T_q$ for primes $(q, rN) = 1$.

In fact, the left-most map in Exact Sequence (B) is an injection, since the kernel is the image of $H^0(X_1(r,N) \otimes \overline{\mathbb{F}}_p, q_*q^*i_!\mathcal{F}_n) \simeq (H^0(X_1(r,N/p) \otimes \overline{\mathbb{F}}_p, i_!\mathcal{F}_n))^2$, which is trivial. [Note that when $k = 2$ and $i_!\mathcal{F}_n$ is replaced by a constant sheaf, this map is not an injection. Its kernel is the set of constant functions on $\Sigma$. But a non-zero such function cannot be in $M_n$ without contradicting the irreducibility of $\rho_{\lambda,1}$, since $T_q$ acts on it as $q+1$ (for $q \nmid rN$).]

**Proposition 4.1.** *Suppose that the action of* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ *on* $M_n$ *(as in Lemma 3.1) is unramified at* $p$*. Then* $M_n$*, thought of as a submodule of* $H^1(X_1(r,N) \otimes \overline{\mathbb{Q}}_p, i_!\mathcal{F}_n)$*, lies within (the image of)* $H^1(X_1(r,N) \otimes \overline{\mathbb{F}}_p, i_!\mathcal{F}_n)$*.*

*Proof.* Given $\sigma \in I_p$, the action of $\sigma - 1$ on $H^1(X_1(r,N) \otimes \overline{\mathbb{Q}}_p, i_!\mathcal{F}_n)$ is given, according to [SGA7, XIII,2.4.6.5], by first projecting to $X$ (as in Exact Sequence

(A)), then applying a map $\mathrm{Var}(\sigma)$ to $Y := \bigoplus_{x\in\Sigma} \mathbb{H}^1_{\{x\}}(X_1(r,N)\otimes\overline{\mathbb{F}}_p, R\Psi_{\overline{\eta}}(\mathcal{F}_n))$ (notation as in [SGA7, XIII]), then mapping $Y$ back into $H^1(X_1(r,N)\otimes\overline{\mathbb{Q}}_p, i_!\mathcal{F}_n)$ via a certain map.

One may show as in [Ja, Lemmas 17.1, 17.3,Proposition 17.4] that $Y$, with its map to $H^1(X_1(r,N)\otimes\overline{\mathbb{Q}}_p, i_!\mathcal{F}_n)$, may be identified with $H^0(X_1(r,N)\otimes\overline{\mathbb{F}}_p, E_n)$ and its map to $H^1(X_1(r,N)\otimes\overline{\mathbb{Q}}_p, i_!\mathcal{F}_n)$ via exact sequences (B) and (A). We have seen that this map is an inclusion. Furthermore, for $\sigma$ whose image in the tame quotient is not an $l^{th}$ power, the map $\mathrm{Var}(\sigma)$ is an isomorphism. This follows from the description of $\mathrm{Var}(\sigma)$ in [SGA7, XV,3.3.5]. Anything in $H^1(X_1(r,N)\otimes\overline{\mathbb{Q}}_p, i_!\mathcal{F}_n)$ killed by $\sigma-1$, for such a $\sigma$, must project to zero in $X$, hence comes from $H^1(X_1(r,N)\otimes\overline{\mathbb{F}}_p, i_!\mathcal{F}_n)$. □

## 5. Lowering the level

The modular curve $Y_1(r,N)$ can be thought of as parametrising quadruples $(E,P,Q,C)$, where $E$ is an elliptic curve over a $\mathbb{Z}[1/r]$-scheme, with a $\Gamma_1(r)$-structure $P$, a $\Gamma_0(N/p)$-structure $Q$ and $C$ a sub-group scheme of order $p$. There is an automorphism $W_p$ taking $(E,P,Q,C)$ to $(E/C, P \pmod C, Q \pmod C, E[p]/C)$. It satisfies $W_p^2 = I_p$, where $I_p(E,P,Q,C) = (E,pP,Q,C)$. (Note that $I_p$ induces the diamond operator $\langle p\rangle$ on $S_k(\Gamma_1(r,N))$.)

**Lemma 5.1.** *$W_p$ acts naturally on $M_n$ as multiplication by $\pm p^{(k/2)-1}$.*

*Proof.* The isogeny of $\mathcal{E}$ associated to $W_p$ gives rise to a morphism from $W_p^*\mathcal{F}_n$ to $\mathcal{F}_n$, hence from $H^1(X_1(r,N)\otimes\overline{\mathbb{F}}_p, i_!W_p^*\mathcal{F}_n)$ to $H^1(X_1(r,N)\otimes\overline{\mathbb{F}}_p, i_!\mathcal{F}_n)$. Composing this with pull-back gives a map "$W_p$" from $H^1(X_1(r,N)\otimes\overline{\mathbb{F}}_p, i_!\mathcal{F}_n)$ to itself. The square of the isogeny of $\mathcal{E}$ associated to $W_p$ maps any fibre $E$ to an isomorphic fibre $E$ (with different level structure), and induces the multiplication-by-$p$ map on $E$. It follows that $W_p^2$ acts as $p^{k-2}$ on the part of $H^1_c(Y_1(r,N)\otimes\overline{\mathbb{F}}_p, \mathcal{F}_n)$ on which the action of $(\mathbb{Z}/r\mathbb{Z})^*$ by diamond operators is trivial, in particular on $M_n$. (Note that since $l \nmid r-1$, this part is obtained by applying a suitable projection operator.) Following through the construction of $M_n$, it is easy to see that it is preserved by $W_p$. Since $p \neq l$ and $l$ is odd, $M_n$ is a direct sum of eigenspaces where $W_p$ acts by $\pm p^{(k/2)-1}$. Moreover, the action of $W_p$ on $M_1$ commutes with the irreducible action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, so one of the eigenspaces must be the whole of $M_n$. □

**Proposition 5.2.** *Suppose that $p \not\equiv 1 \bmod l$. Then $M_n \subset H^1(X_1(r,N)\otimes\overline{\mathbb{F}}_p, i_!\mathcal{F}_n)$ contains at least a rank-1 $O/\lambda^n$-submodule that maps injectively to $(H^1(X_1(r,N/p)\otimes\overline{\mathbb{F}}_p, i_!\mathcal{F}_n))^2$ via Exact Sequence (B).*

*Proof.* If the proposition is false then all the $\lambda$-torsion $M_n[\lambda]$ of $M_n$ comes from $Y$, so we think of $M_n[\lambda]$ as a submodule of $Y$, seeking a contradiction. Recall that $Y = H^0(X_1(r,N)\otimes\overline{\mathbb{F}}_p, E_n)$, with $E_n$ a certain sheaf supported on $\Sigma$. Then $Y$ can be identified with $\bigoplus_{z\in\Sigma} E_{n,z} \simeq \bigoplus_{z\in\Sigma} \mathcal{F}_{n,z_1}$. Here $z_1$ and $z_2$ are the points of $Y_1(r,N/p)\otimes\overline{\mathbb{F}}_p$ mapping to $z\in\Sigma$ under the two maps $\Phi_1$ and $\Phi_2 = W_p\cdot\Phi_1$, respectively, from $Y_1(r,N/p)\otimes\overline{\mathbb{F}}_p$ to $Y_1(r,N)\otimes\overline{\mathbb{F}}_p$.

Changing the use of notation slightly, let $Z = Z_1 \amalg Z_2$ be the normalisation of $Y_1(r,N)\otimes\overline{\mathbb{F}}_p$, where each $Z_i$ is a copy of $Y_1(r,N/p)\otimes\overline{\mathbb{F}}_p$ and $\Phi_i : Z_i \to Y_1(r,N)\otimes\overline{\mathbb{F}}_p$. Let $q = \Phi_1 \amalg \Phi_2 : Z \to Y_1(r,N)\otimes\overline{\mathbb{F}}_p$. Let $\pi_1,\pi_2 : Y_1(r,N)\otimes\overline{\mathbb{F}}_p \to Y_1(r,N/p)\otimes\overline{\mathbb{F}}_p$

be the two degeneracy maps. Then

$$W_p\Phi_1 = \Phi_2,\ \pi_2 = \pi_1 W_p,\ \pi_1\Phi_1 = \mathrm{id},\ \pi_2\Phi_2 = I_p,$$

and $\pi_1\Phi_2 = \pi_2\Phi_1 = F$, where $F$ is the geometric Frobenius morphism. Note that

$$F(z_2) = \pi_1\Phi_2(z_2) = \pi_1(z) = \pi_1\Phi_1(z_1) = z_1 \text{ and}$$

$$F(z_1) = \pi_2\Phi_1(z_1) = \pi_2(z) = \pi_2\Phi_2(z_2) = I_p(z_2).$$

$$q^*\mathcal{F}_n = q^*\pi_1^*\mathcal{F}_n = \Phi_1^*\pi_1^*\mathcal{F}_n \amalg \Phi_2^*\pi_1^*\mathcal{F}_n = \mathcal{F}_n \amalg F^*\mathcal{F}_n.$$

For $z \in \Sigma$ with $\Phi_1(z_1) = \Phi_2(z_2) = z$, we have

$$(q_*q^*\mathcal{F}_n)_z = (q_*(\mathcal{F}_n \amalg F^*\mathcal{F}_n))_z = \mathcal{F}_{n,z_1} \oplus \mathcal{F}_{n,F(z_2)} = \mathcal{F}_{n,z_1} \oplus \mathcal{F}_{n,z_1}.$$

The stalk $\mathcal{F}_{n,z_1}$ is $(\mathrm{Sym}^{k-2}H^1(\mathcal{E}_{z_1}, O_\lambda))/\lambda^n$.

There is an exact sequence

$$0 \longrightarrow \mathcal{F}_{n,z} \longrightarrow \mathcal{F}_{n,z_1} \oplus \mathcal{F}_{n,z_1} \xrightarrow{\alpha} E_{n,z} \longrightarrow 0,$$

where $\alpha(s_1, s_2) = s_1 - s_2$. We wish to investigate the effect of $W_p$ on the subgroup $H^0(Y_1(r,N) \otimes \overline{\mathbb{F}}_p, E_n) = \bigoplus_{z\in\Sigma} E_{n,z}$ of $H^1_c(Y_1(r,N) \otimes \overline{\mathbb{F}}_p, \mathcal{F}_n)$. For this we use a map $\omega_p : Z \to Z$ such that $W_p q = q\omega_p$, and a map from $\omega_p^*(q^*\mathcal{F}_n)$ to $q^*\mathcal{F}_n$ compatible with the map $\phi_{W_p}$ from $W_p^*\mathcal{F}_n$ to $\mathcal{F}_n$ used to get the action of $W_p$ on $H^1_c(Y_1(r,N) \otimes \overline{\mathbb{F}}_p, \mathcal{F}_n)$. The map $\omega_p : Z \to Z$ is defined by $\omega_p(z \in Z_1) = z \in Z_2$ and $\omega_p(z \in Z_2) = I_p(z) \in Z_2$. This satisfies $W_p q = q\omega_p$ because $W_p\Phi_1(z) = \Phi_2(z)$ and if $W_p\Phi_2(z) = \Phi_1(x)$ then $x = \pi_1\Phi_1(x) = \pi_1 W_p\Phi_2(z) = \pi_2\Phi_2(z) = I_p(z)$. It follows that

$$\omega_p^* q^*\mathcal{F}_n = \omega_p^*(\mathcal{F}_n \amalg F^*\mathcal{F}_n) = F^*\mathcal{F}_n \amalg I_p^*\mathcal{F}_n.$$

The natural map $\phi : \omega_p^* q^*\mathcal{F}_n \to q^*\mathcal{F}_n$ is given by $\phi_F : F^*\mathcal{F}_n \to \mathcal{F}_n$ and $\phi_V : I_p^*\mathcal{F}_n \to F^*\mathcal{F}_n$ associated to universal isogenies $F$ over $Z_1$ and $V$ over $Z_2$. Note that for $(E,P,Q,C) \in \Phi_1(Z_1)$, $C = \ker(F : E \to E^{(p)})$, and for $(E,P,Q,C) \in \Phi_2(Z_2)$, $C = \ker(V : E \to E^{(p^{-1})})$. The operator $W_p$ takes $(E,P,Q,\ker F)$ on $\Phi_1(Z_1)$ to $(E^{(p)}, F(P), F(Q), \ker V)$ on $\Phi_2(Z_2)$, and takes $(E,P,Q,\ker V)$ on $\Phi_2(Z_2)$ to $(E^{(p^{-1})}, V(P), V(Q), \ker F)$ on $\Phi_1(Z_1)$.

Now take $s \in \bigoplus_{z\in\Sigma} E_{n,z}$, so $s(z) = s_1(z_1) - s_2(z_2) = (s_1 \amalg s_2)(z_1 \in Z_1) - (s_1 \amalg s_2)(z_2 \in Z_2)$ with $s_1(z_1) \in \mathcal{F}_{n,z_1}$ and $s_2(z_2) \in \mathcal{F}_{n,F(z_2)} = \mathcal{F}_{n,z_1}$. Then $\omega_p^*((s_1 \amalg s_2))(z_1 \in Z_1) = s_2(z_1 \in Z_2)$ and $\omega_p^*((s_1 \amalg s_2))(z_2 \in Z_2) = s_1(I_p(z_2) \in Z_1)$. Hence

$$W_p^* s(z) = \omega_p^*((s_1 \amalg s_2))(z_1 \in Z_1) - \omega_p^*((s_1 \amalg s_2))(z_2 \in Z_2)$$

$$= s_2(z_1 \in Z_2) - s_1(I_p(z_2) \in Z_1) = s_2(F(z_2) \in Z_2) - s_1(F(z_1) \in Z_1) = -s(F(z))$$

and

$$\phi_{W_p} W_p^* s(z) = \phi_V(s_2(F(z_2) \in Z_2) - \phi_F(s_1(F(z_1) \in Z_1)) = -\phi_F(s(F(z)))$$

since $\phi_F = \phi_V$ on the stalk at a supersingular point. Hence the natural actions of $W_p$ and $-F$ on $Y$ are the same.

Since $F$ and $\mathrm{Frob}_p^{-1}$ act on $Y$ in the same way, we find that $\mathrm{Frob}_p^{-1}$ acts on $M_n[\lambda]$ as multiplication by $\pm p^{(k/2)-1}$. But the determinant of $\rho_\lambda$ is the $(k-1)$-power of the inverse of the cyclotomic character, so $p^{k-2}$ and $p^{k-1}$ must be the same in $O/\lambda$, so $p \equiv 1 \bmod l$. This is the contradiction which Mazur produced in his original argument, and it shows that the proposition is true. □

*Proof of Theorem 1.1.* Proposition 5.2 implies the existence of at least a rank-one $O/\lambda^n$-submodule $W$ of $H^1(X_1(r,N/p)\otimes\overline{\mathbb{F}}_p, i_!\mathcal{F}_n)^2$ (and therefore, by projection, of one factor or the other) coming from $M_n$. We claim that the natural injection from $(H^1_c(Y_1(r,N/p)\otimes\overline{\mathbb{F}}_p,\mathcal{F}))/\lambda^n$ to $H^1_c(Y_1(r,N/p)\otimes\overline{\mathbb{F}}_p,\mathcal{F}_n)$ is an isomorphism. By Lemma 1.11 in Chapter 5 of [Mi], the cokernel is the $\lambda^n$-torsion in $H^2_c(Y_1(r,N/p)\otimes\overline{\mathbb{F}}_p,\mathcal{F})$. The triviality of this follows, by Poincaré duality (see Proposition 2.2(b) in Chapter 5 of [Mi]), from the triviality of $H^0(Y_1(r,N/p)\otimes\overline{\mathbb{F}}_p,\mathcal{F}_1)$, when $k>2$ (and $l\nmid N$, $l>k-2$). (When $k=2$ we use instead the fact that the map from $H^1(X_0(N/p)\otimes\overline{\mathbb{F}}_p,O_\lambda)$ to $H^1(X_0(N/p)\otimes\overline{\mathbb{F}}_p,O/\lambda^n)$ is surjective, both having rank equal to twice the genus.)

Having projected $W$ to the appropriate factor of $H^1(X_1(r,N/p)\otimes\overline{\mathbb{F}}_p,i_!\mathcal{F}_n)^2$ we may then view it as being inside $(H^1(X_1(r,N/p)\otimes\overline{\mathbb{F}}_p,i_!\mathcal{F}))/\lambda^n\simeq(H^1(X_1(r,N/p)\otimes\overline{\mathbb{Q}},i_!\mathcal{F}))/\lambda^n$. Arguing as in the proof of Lemma 3.1, we see that $W$ is then mapped injectively to $(H^1_p(Y_1(r,N/p)\otimes\overline{\mathbb{Q}},\mathcal{F}))/\lambda^n$. (Note that the cokernel of $\phi_n: H^1_c(Y_1(r,N/p)\otimes\overline{\mathbb{Q}},\mathcal{F}_n)\to H^1_p(Y_1(r,N/p)\otimes\overline{\mathbb{Q}},\mathcal{F}_n)$ is contained in the sum over cusps $\bigoplus_x H^1(\Gamma_1(r,N)_x,\mathrm{Sym}^{k-2}((O/\lambda)^2))$, which is torsion-free, using $l\nmid N$ and $l>k-2$.)

The action of $\mathbb{T}'(r,N/p)$ on $(H^1(Y_1(r,N/p)\otimes\overline{\mathbb{F}}_p,\mathcal{F}))\simeq(H^1(Y_1(r,N/p)\otimes\overline{\mathbb{Q}},\mathcal{F}))$ arising from the inclusion $\Phi_1$ or $\Phi_2$ of $Y_1(r,N/p)\otimes\overline{\mathbb{F}}_p$ in $Y_1(r,N)\otimes\overline{\mathbb{F}}_p$ is compatible with the usual action, since $\pi_1\Phi_1=\mathrm{id}$ and $\pi_2\Phi_2=I_p$. The homomorphism from $\mathbb{T}'(r,N/p)$ to $O/\lambda^n$ arising from its action on $W$ inside $(H^1_p(Y_1(r,N/p)\otimes\overline{\mathbb{Q}},\mathcal{F}))/\lambda^n$ factors $\theta_{f,n}:\mathbb{T}(r,N)\to O/\lambda^n$.
□

## 6. Examples in weight two

Let $f$ be as in §1, with $k=2$. If $f$ has rational Fourier coefficients then it is associated with an elliptic curve $E/\mathbb{Q}$, of conductor $N$. If $p\,||\,N$ then $E$ has multiplicative reduction at $p$, and has a Tate model over $\mathbb{Q}_p$ or an unramified quadratic extension of $\mathbb{Q}_p$, according as the reduction is split or non-split, respectively. If $\Delta$ is the minimal discriminant and $q$ is the Tate parameter then $\mathrm{ord}_p(\Delta)=\mathrm{ord}_p(q)$ and $E[l^n]\simeq\mu_{l^n}\times\langle q^{1/l^n}\rangle/q^{\mathbb{Z}}$. If $l\neq p$ is a prime and $l^n\mid\mathrm{ord}_p(\Delta)$, it follows that $\rho_{l,n}$ is unramified at $p$. It is not difficult to find examples with $n>1$ for small $l$, especially $l=3$. We list some below to illustrate Theorem 1.1. In all these examples, $\rho_{l,1}$ is irreducible. For elliptic curves we use the same notation as Cremona. For modular forms of weight two with non-rational coefficients we use the same notation as Stein, since it is convenient to call them something, though his tables have now disappeared. The reader who asks the computer package Magma for newforms of weight 2 and the given level will recognise in the output the forms in question, from their stated properties.

(1) The elliptic curve **298A1** has $\Delta=-2^9 149$, so $\rho_{3,2}$ is unramified at $p=2$. The form **149B1** has Fourier coefficients in a field of degree 9, in which $l=3$ has an unramified prime divisor $\lambda$ of degree 1. The forms $f:=$**298A1** and $g:=$**149B1** appear to be congruent modulo $\lambda^2$, by which I mean that the Fourier coefficients of index coprime to $N$ appear to be congruent modulo $\lambda^2$, based on examination of the first few Hecke eigenvalues. (We think of an elliptic curve and its associated modular form interchangeably.) Apparently then $\theta_{f,2}$ factors through $\theta_{g,2}$.

(2) The elliptic curve **326A1** has $\Delta = 2^9 163$, so $\rho_{3,2}$ is unramified at $p = 2$. There is an elliptic curve **163A1** that appears to be congruent to **326A1** modulo 3 but not modulo $3^2$. By Theorem 1.1 we know that **163A1** cannot be unique. Indeed there is a form **163B1** with Fourier coefficients in a field of degree 5, in which $l = 3$ has an unramified prime divisor $\lambda$ of degree 1, such that **163B1** appears to be congruent to **163A1** $\pmod{\lambda}$ (but not $\pmod{\lambda^2}$). Theorem 1.1 forces these apparent congruences to actually hold, but they could also be checked using Sturm's theorem [St].

Further insight may be gained by closer scrutiny of examples such as this where "$g$" is not unique, as was pointed out to me by K. Buzzard. Let **326A1** $= f = \sum a_n q^n$, **163A1** $= g = \sum b_n q^n$ and **163B1** $= h = \sum c_n q^n$. For primes $q$ coprime to 326, the coefficients $b_q$ and $c_q$ in $\mathbb{Z}_3$ are certainly not congruent modulo anything greater than 3. Since the congruence modulo 3 does hold, $\mathbb{T}'(163)_{\mathfrak{m}} \simeq \{(b, c) \in \mathbb{Z}_3 \oplus \mathbb{Z}_3 | b \equiv c \pmod{3}\}$ via $T_q \mapsto (b_q, c_q)$. This in turn is isomorphic to $\mathbb{Z}_3[X]/(X^2 - 3X)$ via $\alpha \mapsto (\alpha, \alpha)$ for all $\alpha \in \mathbb{Z}_3$ and $X \mapsto (0, 3)$. We have $T_q \mapsto b_q + \frac{c_q - b_q}{3} X$. The *three* homomorphisms from $\mathbb{T}'(163)_{\mathfrak{m}}$ to $\mathbb{Z}/9\mathbb{Z}$ are then given by $X \mapsto 0$, $X \mapsto 3$ and $X \mapsto 6$. These are, respectively, $T_q \mapsto b_q$, $T_q \mapsto c_q$ and $T_q \mapsto 2c_q - b_q$. The first two correspond to $g$ and $h$ but it is the third one which induces $\theta_{f,2}$ : $\mathbb{T}(326) \to \mathbb{Z}/9\mathbb{Z}$. The numerical data does indeed support the conclusion that $a_n = 2c_n - b_n$ in $\mathbb{Z}/9\mathbb{Z}$, for all $n$ coprime to 326, and Buzzard has checked this for $2 < n < 50$.

(3) The elliptic curve **730D1** has $\Delta = 2^{27} 5 \cdot 73$, so $\rho_{3,3}$ is unramified at $p = 2$. The form **365D1** has Fourier coefficients in a field of degree 7, in which $l = 3$ has an unramified prime divisor $\lambda$ of degree 1. **730D1** and **365D1** appear to be congruent modulo $\lambda^3$.

(4) The elliptic curve **606E1** has $\Delta = -2^9 3^6 101$, so $\rho_{3,2}$ is unramified at $p = 2$. The form **303D1** has Fourier coefficients in a field of degree 6, in which $l = 3$ has an unramified prime divisor $\lambda$ of degree 1. In this example $l \mid N$ so Theorem 1.1 does not apply, but **606E1** and **303D1** do appear to be congruent modulo $\lambda^2$, suggesting that, at least for $k = 2$, the condition $l \nmid N$ may not be necessary.

(5) The elliptic curve **329A1** has $\Delta = -7^9 47$, so $\rho_{3,2}$ is unramified at $p = 7$. The form **47A1** has Fourier coefficients in a field of degree 4, in which $l = 3$ has an unramified prime divisor $\lambda$ of degree 1. Now $7 \equiv 1 \pmod{3}$ so Theorem 1.1 does not apply. However, **329A1** and **47A1** do appear to be congruent modulo $\lambda^2$. This example suggests that perhaps the condition $p \equiv 1 \pmod{l}$ is not really necessary. Of course, in the case $n = 1$ it was removed by Ribet [Ri1], for $k = 2$, and by Rajaei [Raj] for $k > 2$.

(6) Just to check $l = 2$ really works. The elliptic curve **415A1** has $\Delta = -5^4 83$, so $\rho_{2,2}$ is unramified at $p = 5$. The forms **415A1** and **83A1** appear to be congruent modulo $2^2$ (for $(m, 2N) = 1$, but $a_2 = 1$ and $b_2 = -1$).

## 7. Application to Tamagawa factors

Let $f$ be as in §1 and let $L_f(s)$ be the $L$-function attached to $f$, the analytic continuation of the Dirichlet series $\sum_{m=1}^{\infty} a_m m^{-s}$. When testing the Bloch-Kato conjecture [BK], applied to the values of $L_f(s)$ at integer points $s = j$ (especially critical points $1 \leq j \leq k - 1$, such as the central point $j = k/2$ [Du],[DSW]), one needs to know about certain "Tamagawa factors" $c_p(j)$. If we wish to test the $\lambda$-part of the Bloch-Kato conjecture at $s = j$ then we need to know the $\lambda$-part of $c_p(j)$, for all primes $p$.

For $l \neq p$,

$$\mathrm{ord}_\lambda(c_p(j)) := \text{length}\,\left(H^0(\mathbb{Q}_p, A_\lambda(j))/H^0\left(\mathbb{Q}_p, V_\lambda(j)^{I_p}/T_\lambda(j)^{I_p}\right)\right),$$

where $T_\lambda := M$, the space of $\rho_\lambda$, $V_\lambda := M \otimes_{O_\lambda} E_\lambda$ and $A_\lambda := V_\lambda/T_\lambda$. Note that $H^0(\mathbb{Q}_p, A_\lambda(j))$ is the part of $A_\lambda(j)^{I_p}$ on which $\mathrm{Frob}_p$ acts trivially. Note also that $M_n$ is isomorphic to the $\lambda^n$-torsion in $A_\lambda$, which we also denote $A[\lambda^n]$.

Assuming that $l > k$ and $l \nmid N$, Lemmas 4.3 and 4.6 of [DSW] tell us that the $\lambda$-part of $c_p(j)$ is trivial if $p \nmid N$, so we only need to worry about the case $p \mid N$. (Note that in Lemma 4.6 of [DSW] we really need $-(l-k) < j < l-1$, so that the condition (*) in Theorem 4.1(iii) of [BK] holds. There is certainly no problem if $l > k$ and $1 \leq j \leq k-1$.) Let $w_p = \pm 1$ be the scalar by which the Atkin-Lehner involution $W_p$ acts on $f$.

**Proposition 7.1.** *Suppose that $l > k$, $l \nmid N$, $p \not\equiv 1 \bmod l$, $p \mid\mid N$ and $\rho_{\lambda,1}$ is irreducible. Let $n \geq 1$ be the largest integer such that the homomorphism $\theta_{f,n} : \mathbb{T}(N) \to O/\lambda^n$ factors through the $p$-old quotient $\mathbb{T}'(N/p)$. If $w_p = -1$ then $\mathrm{ord}_\lambda(c_p(k/2)) = n$, otherwise $\mathrm{ord}_\lambda(c_p(k/2)) = 0$.*

*Proof.* First we show that $A[\lambda^n]$ is unramified at $p$. As in the proof of Lemma 2.3 $\theta_{f,n}$ factors through some $h : \mathbb{T}(N/p)_{\mathfrak{n}} \to O/\lambda^n$, where $\mathfrak{n}$ is the maximal ideal of $\mathbb{T}(N/p)$ associated to $f$ by the usual $n = 1$ level-lowering. Again as in the proof of Théorème 3 of [Ca2], there is a continuous representation

$$\rho_{\mathfrak{n}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(2, \mathbb{T}(N/p)_{\mathfrak{n}}),$$

unramified at primes $q \nmid lN/p$, with $\mathrm{tr}(\rho_{\mathfrak{n}}(\mathrm{Frob}_q^{-1})) = T_q$ for such primes. By Théorème 1 of [Ca2], the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $A[\lambda^n]$ is equivalent to the representation obtained from $\rho_{\mathfrak{n}}$ by "composing with $h$", since these two representations have the same trace. Since $\rho_{\mathfrak{n}}$ is unramified at $p$, so is $A[\lambda^n]$.

By Theorems 3(ii) and 5 of [AL], the Euler factor at $p$ of $L_f(s)$ is $(1+w_p p^{(k/2)-1}p^{-s})^{-1}$. It follows from Théorème A of [Ca1] that this is the same as the Euler factor obtained as $\det(1 - \mathrm{Frob}_p^{-1}p^{-s}|V_\lambda^{I_p})$. Hence $V_\lambda^{I_p}$ is one-dimensional, and $\mathrm{Frob}_p^{-1}$ acts on it as multiplication by $-w_p p^{(k/2)-1}$. The rank-one $O/\lambda^n$-submodule of $A[\lambda^n](j)$ making up the image of $V_\lambda^{I_p}(j)$ contributes nothing to $\mathrm{ord}_\lambda(c_p(j))$, for any integer $j$. The element $\mathrm{Frob}_p^{-1}$ acts on the exterior square of $V_\lambda$ as $p^{k-1}$. Therefore it must act as $-w_p p^{k/2}$ on the quotient of $A[\lambda^n]$ by the image of $V_\lambda^{I_p}$. Since $p \neq l$ and $p \not\equiv 1 \pmod{l}$, the difference between $-w_p p^{(k/2)-1}$ and $-w_p p^{k/2}$ is invertible in $O/\lambda^n$. It follows easily that there is a rank-one $O/\lambda^n$-submodule of $A[\lambda^n]$ on which $\mathrm{Frob}_p^{-1}$ acts as $-w_p p^{k/2}$. This gives a rank-one $O/\lambda^n$-submodule of $A[\lambda^n](k/2)$ on which $\mathrm{Frob}_p^{-1}$ acts as $-w_p$, thus contributing $n$ to $\mathrm{ord}_\lambda(c_p(k/2))$ when $w_p = -1$, nothing when $w_p = 1$.

In the case $w_p = -1$ we have just seen that $\mathrm{ord}_\lambda(c_p(k/2)) \geq n$. To show that this inequality is in fact an equality, we merely observe that by Theorem 1.1 and the maximality of $n$, $A[\lambda^{n+1}]$ is ramified at $p$. □

We have concentrated here on the case $j = k/2$, but clearly $k/2$ may be replaced (in the statement of the proposition) by any integer $j$ such that $p^{j-(k/2)} \equiv -w_p$

(mod $l$). For other values of $j$ (retaining the other conditions of the proposition), $\mathrm{ord}_\lambda(c_p(j))$ is trivial.

In §7.4 of [DSW] we gave an example where $\mathrm{ord}_\lambda(c_p(j)) > 0$. Now we may use Proposition 7.1 to determine $\mathrm{ord}_\lambda(c_p(j))$ precisely. The example is $f = \sum a_m q^m$ of weight 4 and level 39, $l = 19, p = 3$ and $j = k/2 = 2$. This was **39k4C** in Stein's Modular Forms Explorer. It has coefficients in a field of degree 3 over $\mathbb{Q}$, and $w_3 = -1$. There is a prime ideal $\lambda \mid 19$ of degree one, such that $a_m \equiv b_m \pmod{\lambda}$ for all $m$ coprime to $39 \cdot 19$, where $g = \sum b_m q^m$ is a normalised newform (**13k4A** in Stein's tables) of weight 4 for $\Gamma_0(13)$. The form $g$ has rational Fourier coefficients. It is the unique form of level 13 congruent to $f$ (for $m$ coprime to $39 \cdot 19$) modulo a divisor of 19. Hence any homomorphism from $\mathbb{T}'(13)$ to $O/\lambda^n$, inducing $\theta_{f,n} : \mathbb{T}(39) \to O/\lambda^n$, factors through $\theta_g$. Since the congruence between $f$ and $g$ does not hold $\pmod{\lambda^2}$, Proposition 7.1 shows that $\mathrm{ord}_\lambda(c_3(2)) = 1$.

The examples of §6, and §8 below, are consistent with the possibility that the conditions $p \not\equiv 1 \pmod{l}$, $l \neq p$, $l \nmid N$ may not be necessary. Note, however, that in the application to Tamagawa factors we have used all these conditions anyway.

## 8. The case $l = p$ for elliptic curves

**Proposition 8.1.** *Suppose that $E/\mathbb{Q}$ is an elliptic curve of conductor $N$ with $p \,||\, N$ ($p \neq 2$ a prime). Letting $\Delta$ be the minimal discriminant of $E$, suppose that $p^n \mid \mathrm{ord}_p(\Delta)$. Then there exists a finite flat group-scheme $\mathcal{G}_n/\mathbb{Z}_p$ whose generic fibre $G_n/\mathbb{Q}_p$ gives rise to a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-representation isomorphic to $E[p^n]$.*

*Proof.* A proof of the case $n = 1$ is sketched at the end of 2.8 of [Se], with full details in the proof of Proposition 8.2 of [E]. That proof appears to generalise to the case $n > 1$, but here is an alternative.

Let $T_p(E) = \varprojlim E[p^n]$ be the $p$-adic Tate module of $E$ and $V_p(E) = T_p(E) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$. Then $T_p(E)$ is a $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$-stable $\mathbb{Z}_p$-lattice in the semistable (see [Br]) representation $V_p(E)$ of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$. We may write down a "strongly divisible" $S$-module $\mathcal{M}$ that maps to $T_p(E)$ by Breuil's functor $V_{\mathrm{st}}$ (see 3.1.3 and 4.1.1 of [Br]). Here $S$ is the $p$-adic completion of the divided power algebra $\mathbb{Z}_p\langle u\rangle$, as in 2.1.1 of [Br]. It is naturally filtered by $\{S \cap (u-p)^i S[1/p]\}$.

First we define a filtered $\mathbb{Z}_p$-module $M$ with frobenius and monodromy operators $\phi$ and $N$. Let $\alpha := \mathrm{ord}_p(q)$ and $\lambda := \log_p(q)$, where $q$ is the Tate parameter of $E/\mathbb{Q}_p$. $M$ is defined to be the $\mathbb{Z}_p$-span of basis elements $e_0$ and $e_1$, with

$$\phi e_1 = \pm p e_1,\ \phi e_0 = \pm e_0,$$

$$N e_1 = \alpha e_0,\ N e_0 = 0,$$

$$M^0 = M,\ M^1 = \langle e_1 - \lambda e_0\rangle,\ M^2 = \{0\}.$$

Take the upper or lower sign according as the multiplicative reduction of $E$ at $p$ is split or non-split, respectively. Then let $\mathcal{M} := M \otimes_{\mathbb{Z}_p} S$ with the tensor product filtration. That $V_{\mathrm{st}}(\mathcal{M})$ is isomorphic to $T_p(E)$ may be proved as in 3.4 and 3.5 of [P].

For $r \geq 1$ let $M_r := M/p^r M$ and $\mathcal{M}_r := M_r \otimes_{\mathbb{Z}_p} S$. Then $V_{\mathrm{st}}(\mathcal{M}_r)$ is isomorphic to the finite $\mathbb{Z}_p[\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)]$-module $E[p^r]$. Now, since $p^n \mid \alpha$ (because $p^n \mid \mathrm{ord}_p(\Delta)$), $N = 0$ on $M_r$ for $r \leq n$. In particular $M_n$ may be regarded as an object of the category $\underline{MF}^{f,2}_{\mathrm{tor}}$ of [FL], and $V_{\mathrm{cris}}(M_n)$ is isomorphic to $V_{\mathrm{st}}(\mathcal{M}_n) \simeq E[p^n]$, by Proposition 3.2.1.1 of [Br]. (Note that the map $\phi_1 : M_n^1 \to M_n$ is the restriction of $\phi$, divided by $p$.)

By 9.11 of [FL], $\underline{MF}_{\mathrm{tor}}^{f,2}$ is anti-equivalent to the category of commutative, finite, flat group-schemes over $\mathbb{Z}_p$ of $p$-power order. Let $\mathcal{G}_n$ be the group-scheme corresponding to $M_n$. Then by Proposition 9.12 of [FL], the representation $\mathcal{G}_n(\overline{\mathbb{Q}}_p)$ of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is isomorphic to $V_{\mathrm{cris}}(M_n) \simeq E[p^n]$. □

**Lemma 8.2.** *Let $E$ and $\mathcal{G}_n$ be as in Proposition 8.1. Suppose that $E[p]$ is an irreducible $\mathbb{F}_p[\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module. $\mathcal{G}_n$ is isomorphic to a sub-group-scheme of $\mathcal{J}_0(N)$, the Néron model of $J_0(N)/\mathbb{Q}_p$.*

*Proof.* Let $E'/\mathbb{Q}$ be the optimal (i.e. strong Weil) curve in the isogeny class of $E$. Since $E[p]$ is absolutely irreducible, $E'[p^n]$ and $E[p^n]$ (having the same character) must be isomorphic as representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ with coefficients in $\mathbb{Z}/p^n$, by Théorème 1 of [Ca2]. Hence they are isomorphic as representations of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ with coefficients in $\mathbb{Z}/p^n$, and therefore as group-schemes over $\mathbb{Q}_p$. Since $E'/\mathbb{Q}$ injects into $J_0(N)/\mathbb{Q}$ (by optimality), $G_n$ is isomorphic to a sub-group-scheme of $J_0(N)/\mathbb{Q}_p$.

To show that the embedding of $G_n$ into $J_0(N)/\mathbb{Q}_p$ prolongs to an embedding of $\mathcal{G}_n$ into $\mathcal{J}_0(N)$ one simply copies the proof of Lemma 6.2 of [Ri1], noting that all the references to [Gr] and [Ray] apply just as well to $p^n$-torsion group-schemes as to $p$-torsion group-schemes. □

**Lemma 8.3.** *The special fibre $\mathcal{G}_{n,s}$ is contained in $J^0$, the connected component of the identity in the special fibre $\mathcal{J}_0(N)_s$ of $\mathcal{J}_0(N)$.*

This can be proved exactly as in the first line of the proof of Lemma 6.3 of [Ri1], using the irreducibility of the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module $E[p]$ and the fact that the action of $\mathbb{T}$ on the group of components of $\mathcal{J}_0(N)_s$ is Eisenstein.

If, as above, $J^0$ is the connected component of the identity in the special fibre $\mathcal{J}_0(N)_s$ of $\mathcal{J}_0(N)$, then, by [MR], there is an exact sequence

$$0 \to T \to J^0 \to \mathcal{J}_0(N/p)_s \times \mathcal{J}_0(N/p)_s \to 0,$$

where $T/\mathbb{F}_p$ is a torus.

**Lemma 8.4.** *$\mathcal{G}_{n,s}$ has a sub-group-scheme $\mathbb{V}$ of rank at least $p^n$, not annihilated by $p^{n-1}$, such that $\mathbb{V}$ embeds in $\mathcal{J}_0(N/p)_s \times \mathcal{J}_0(N/p)_s$ via the exact sequence above.*

*Proof.* By Lemma 8.3, $\mathcal{G}_{n,s}$ embeds in $J^0$. Seeking a contradiction, we suppose that the image of $\mathcal{G}_{n,s}$ in $\mathcal{J}_0(N/p)_s \times \mathcal{J}_0(N/p)_s$ is killed by $p^{n-1}$. Then $p^{n-1}\mathcal{G}_{n,s} \simeq \mathcal{G}_{1,s}$ is contained in $T$. Now copying [Ri1], from the second paragraph of the proof of Lemma 6.3 to the end of the proof of Theorem 6.1, produces a contradiction. □

One easily deduces the following.

**Theorem 8.5.** *Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N$, $p \neq 2$ a prime such that $p \mid\mid N$. Let $f = \sum_{m=1}^{\infty} a_m q^m$ be the newform of level $N$ associated with $E$. Suppose that $p^n \mid \mathrm{ord}_p(\Delta)$, where $\Delta$ is the minimal discriminant of $E$. Suppose also that $\rho_{p,1}$, the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on $E[p]$, is irreducible. The homomorphism $\theta_{f,n} : \mathbb{T}(N) \to \mathbb{Z}/p^n$ factors through the $p$-old quotient $\mathbb{T}'(N/p)$.*

The proof works just as well if $f$ is any newform of weight 2 for $\Gamma_1(N/p)\cap\Gamma_0(p)$, not necessarily with rational coefficients. The condition $p^n \mid \mathrm{ord}_p(\Delta)$ would be replaced by a condition that $\rho_{\lambda,n}$ is finite flat at $p$.

*Example.* The elliptic curve **339A1** has $\Delta = -3^9 113$. We find a form **113D1** with Fourier coefficients in a field of degree 3, in which $l = 3$ has an unramified prime divisor $\lambda$ of degree 1. **339A1** and **113D1** appear to be congruent modulo $\lambda$, and **113D1** is unique with this property. In line with the theorem, **339A1** and **113D1** appear to be congruent modulo $\lambda^2$.

Theorem 3.14 of [CE] extends the above to the case $l = 2$. They work with any Artinian ring with finite residue field of characteristic 2, and have to prove a multiplicity-one result.

## 9. Further remarks

In Theorem 1.1, the input is a Galois representation $\rho_{\lambda,n}$, *from which* one gets a Hecke map $\theta_{f,n} : \mathbb{T}(N) \to O/\lambda^n$, and the output is the factor (with the same name) $\theta_{f,n} : \mathbb{T}'(N/p) \to O/\lambda^n$. This difference in the forms of the input and the output does not lend itself to repeated application of the theorem to remove several primes from the level, as in work of Camporino and Pacetti [CP, Corollary 1.1]. It was observed by Tsaknias that one can modify the theorem to input directly a Hecke map (not necessarily coming from a single modular form), then to get *from this* a Galois representation, by composing Carayol's universal Galois representation [Ca2] with (roughly speaking) the Hecke map. In his terminology, one starts with a "weakly modular" mod $\lambda^n$ Galois representation. See [T, Theorem 5.1], and note that $l \neq 2$ there. To adapt the proof, one needs to know that the Galois representation occurs in cohomology. This is dealt with by [T, Proposition 5.4], using [Ca2, 3.3.2] and [Ri1, Theorem 5.2(b)].

As pointed out to me by Pacetti, for the application in [CP, Corollary 1.1], one also needs to extend the output map $\theta_{f,n} : \mathbb{T}'(N/p) \to O/\lambda^n$ to $\mathbb{T}(N/p)$, i.e. to include $T_p$, and one can do this as in the last paragraph of the proof of Lemma 2.3 above.

Another way in which one may modify Theorem 1.1, again necessary for [CP, Corollary 1.1], is to replace $\Gamma_0(N)$ by $\Gamma_1(N)$. One must add the diamond operators $\langle a\rangle$, for $a \in (\mathbb{Z}/N\mathbb{Z})^\times$, to the Hecke algebra $\mathbb{T}(N)$. If $f$ is a Hecke eigenform with character $\epsilon$, the assumption that $\rho_{\lambda,n}$ is unramified at $p$ forces the $p$-component of $\epsilon$ to be trivial, given that $p \not\equiv 1 \pmod{l}$. So one can use the group $\Gamma_1(N/p)\cap\Gamma_0(p)$, and the proofs work just the same. The introduction of the auxiliary prime $r$ is necessary only if $N/p < 4$.

Dahmen and Yazdani have made an application of mod 9 level-lowering to Diophantine equations [DY]. Their level-lowering theorem, like that of Dieulefait and Taixés i Ventosa [DXT], is proved using deformation rings, for weight 2, and likewise has a further restrictive condition to make the (completed) Hecke ring as simple as possible, but it suffices for their application. One might ask why we cannot prove Theorem 1.1 using some generalisation to weight $k \geq 2$ of Diamond's $R_\Sigma \simeq \mathbb{T}_\Sigma$ results, which apply for $k = 2$ [Di1, Theorem 6.1]. (Further, he does not require $p \not\equiv 1 \bmod l$, though there is an irreducibility condition on the restriction of $\rho_{\lambda,1}$ to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{(-1)^{(l-1)/2}l}))$.) But in fact this would not work even for $k = 2$. In our application, $\Sigma$ would be the finite set of primes at which $\rho_{\lambda,1}$ is unramified but $\rho_{\lambda,n}$ is ramified. The idea is that $\rho_{\lambda,n}$ would factor through $R_\Sigma$. Since $R_\Sigma \simeq \mathbb{T}_\Sigma$

and $p \notin \Sigma$, we might hope that this shows that $\theta_{f,n}$ factors through $\mathbb{T}(N/p)$. The trouble is, there might be a prime $q \in \Sigma$ such that $q \mid\mid N/p$ whereas $q^2$ divides the level of the Hecke algebra whose localisation is $\mathbb{T}_\Sigma$ (cf.[W, (2.24)]). Therefore $\mathbb{T}_\Sigma$ would not be a quotient of $\mathbb{T}(N/p)_\mathfrak{n}$. One might think that we can easily overcome this difficulty and pass to a greatest common divisor of levels, but since we are working with Hecke algebras over $\mathbb{Z}_l$, not $\mathbb{Q}_l$, this is not the case. Note also that, in an $R_\Sigma \simeq \mathbb{T}_\Sigma$ proof, in order for the process of enlarging $\Sigma$ to be one of relaxing conditions, the deformation condition at $q \in \Sigma$ must be no condition; there is no deformation condition corresponding to "$q \nmid N$ or $q \mid\mid N$", since a union of deformation conditions is not a deformation condition. We could possibly get somewhere if we were willing to impose conditions $q \not\equiv -1 \pmod{l}$ for every $q \in \Sigma$, to eliminate Case 3 of [Li, Proposition 2.3].

## References


[AL] A. O. L. Atkin, J. Lehner, Hecke operators on $\Gamma_0(m)$, *Math. Ann.* **185** (1970), 135–160.

[BK] S. Bloch, K. Kato, $L$-functions and Tamagawa numbers of motives, The Grothendieck Festschrift Volume I, 333–400, Progress in Mathematics, 86, Birkhäuser, Boston, 1990.

[Br] C. Breuil, Construction de représentations $p$-adiques semi-stables, *Ann. Sci. École Norm. Sup. (4)* **31** (1998), 281–327.

[Bz] K. Buzzard, On level-lowering for mod 2 representations, *Math. Res. Lett.* **7** (2000), 95–110.

[CE] F. Calegari, M. Emerton, Elliptic curves of odd modular degree, *Israel J. Math.* **169** (2009), 417–444.

[CP] M. Camporino, A. Pacetti, Congruences between modular forms modulo prime powers, preprint. http://mate.dm.uba.ar/ apacetti/

[Ca1] H. Carayol, Sur les représentations $\ell$-adiques associées aux formes modulaires de Hilbert, *Ann. Sci. École Norm. Sup. (4)* **19** (1986), 409–468.

[Ca2] H. Carayol, Formes modulaires et repésentations galoisiennes à valeurs dans un anneau local complet. $p$-adic Monodromy and the Birch and Swinnerton-Dyer Conjecture (Boston, MA, 1991), 213–237, Contemp. Math., **165**, Amer. Math. Soc., Providence, RI, 1994.

[Ca3] H. Carayol, Sur les représentations Galoisiennes modulo $l$ attachées aux formes modulaires, *Duke Math. J.* **59** ,(1989), 785–801.

[DDT] H. Darmon, F. Diamond, R. Taylor, Fermat's Last Theorem. Elliptic Curves, Modular Forms and Fermat's Last Theorem (2nd ed.), 2–140, International Press, Cambridge MA, 1997.

[De] P. Deligne, Formes modulaires et représentations $\ell$-adiques. Sém. Bourbaki, éxp. 355, Lect. Notes Math. **179,** 139–172, Springer-Verlag, 1969.

[DR] P. Deligne, M. Rapoport, Les schémas de modules de courbes elliptiques, in *Modular Functions of One Variable II,* Lect. Notes Math. **349,** 143–316, Springer-Verlag, 1973.

[Di1] F. Diamond, An extension of Wiles' results, *in* Modular Forms and Fermat's Last Theorem, (G. Cornell, J. H. Silverman, G. Stevens, eds.), 475–489, Springer-Verlag, New York, 1997.

[Di2] F. Diamond, The refined conjecture of Serre, *in* Elliptic Curves, Modular Forms and Fermat's Last Theorem, J. Coates, S.T. Yau, eds., 172–186, International Press, Cambridge MA, 1995.

[DT] F. Diamond, R. Taylor, Non-optimal levels of mod $l$ modular representations, *Invent. Math.* **115** (1994), 435–462.

[DXT] L. Dieulefait, X. Taixés i Ventosa, Congruences between modular forms and lowering the level mod $l^n$, *J. Th. Nombres Bordeaux* **21** (2009), 109–118.

[Du] N. Dummigan, Period ratios of modular forms, *Math. Ann.* **318** (2000), 621–636.

[DSW] N. Dummigan, W. Stein, M. Watkins, Constructing elements in Shafarevich-Tate groups of modular motives, in *Number Theory and Algebraic Geometry,* M. Reid, A. Skorobogatov, eds., London Math. Soc. Lecture Note Series 303, 91–118, Cambridge University Press, 2003.

[DY] S. Dahmen, S. Yazdani, Level lowering modulo prime powers and twisted Fermat equations, *Canad. J. Math.* **64** (2012), 282–300.

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

[FL] J.-M. Fontaine, G. Lafaille, Construction de représentations $p$-adiques, *Ann. Sci. École Norm. Sup. (4)* **15** (1982), 547–608.

[FK] E. Freitag, R. Kiehl, *Étale cohomology and the Weil conjecture,* Springer-Verlag, Berlin, 1988.

[Gr] A. Grothendieck, SGA7 I, Exposé IX, Lect. Notes Math. **288**, 313–523, Springer-Verlag, 1972.

[Ja] F. Jarvis, Mazur's principle for totally real fields of odd degree, *Compositio Math.* **116** (1999), 39–79.

[JL] B. W. Jordan, R. Livné, Conjecture "epsilon" for weight $k > 2$, *Bull. Amer. Math. Soc.* **21** (1989), 51–56.

[KM] N. Katz, B. Mazur, *Arithmetic Moduli of Elliptic Curves,* Ann. of Math. Stud. 108, Princeton Univ. Press, 1985.

[KW1] C. Khare, J.-P. Wintenberger, Serre's modularity conjecture (I), *Invent. Math.* **178** (2009), 485–504.

[KW2] C. Khare, J.-P. Wintenberger, Serre's modularity conjecture (II), *Invent. Math.* **178** (2009), 505–586.

[La] R. P. Langlands, Modular forms and $\ell$-adic representations, in *Modular Functioms of One Variable II,* Lect. Notes Math. **349,** 361–500, Springer-Verlag, 1973.

[Li] R. Livné, On the conductors of mod $l$ representations coming from modular forms, *J. Number Theory***31** (1989), 133–141.

[MR] B. Mazur, M. Rapoport, Appendix to B. Mazur, Modular curves and the Eisenstein ideal, *Publ. Math. IHES* **47** (1977), 33–186.

[Mi] J. S. Milne, *Étale Cohomology,* Princeton University Press, 1980.

[P] B. Perrin-Riou, Répresentations $p$-adiques ordinaires, *Astérisque* **223** (1994), 185–207.

[Raj] A. Rajaei, On the levels of mod $l$ Hilbert modular forms, *J. Reine Angew. Math.* **537** (2001), 33–65.

[Ray] M. Raynaud, Schémas en groupes de type $(p, \dots, p)$, *Bull. Soc. Math. France* **102** (1974), 241–280.

[Ri1] K. Ribet, On modular representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, *Invent. Math.* **100** (1990), 431–476.

[Ri2] K. Ribet, Report on $\pmod{l}$ representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, *in* Motives, A.M.S. Proc. Symp. Pure Math. **55**:2 (1994), 639–676.

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

[St] J. Sturm, On the congruence of modular forms, in *Number theory (New York 1984–1985),* 275–280, Lect. Notes Math. **1240,** Springer-Verlag, 1987.

[SGA7] P. Deligne, N. Katz, *Séminaire de Géometrie Algébrique 7, Groupes de Monodromie en Géométrie Algébrique,* Lect. Notes Math. **340,** Springer-Verlag, 1973.

[T] P. Tsaknias, On higher congruences of modular Galois representations, Ph. D. thesis, University of Sheffield, 2009. http://math.uni.lu/ tsaknias/Thesis.pdf

[W] A. Wiles, Modular elliptic curves and Fermat's Last Theorem, *Ann. Math.* **141** (1995), 443–551.



University of Sheffield, Department of Pure Mathematics, Hicks Building, Hounsfield Road, Sheffield, S3 7RH, U.K.

*E-mail address*: `n.p.dummigan@shef.ac.uk`