

Explicit small image theorems for residual modular representations

Baptiste Peaucelle

*Université Clermont Auvergne, CNRS, LMBP
F-63000 Clermont-Ferrand, France
baptiste.peaucelle@uca.fr*

Received 10 November 2020

Revised 19 August 2021

Accepted 23 August 2021

Published 24 November 2021

Let $\bar{\rho}_{f,\lambda}$ be the residual Galois representation attached to a newform f and a prime ideal λ in the integer ring of its coefficient field. In this paper, we prove explicit bounds for the residue characteristic of the prime ideals λ such that $\bar{\rho}_{f,\lambda}$ is exceptional, that is reducible, of projective dihedral image, or of projective image isomorphic to \mathfrak{A}_4 , \mathfrak{S}_4 or \mathfrak{A}_5 . We also develop explicit criteria to check the reducibility of $\bar{\rho}_{f,\lambda}$, leading to an algorithm that computes the exact set of such λ 's. We have implemented this algorithm in PARI/GP. Along the way, we construct lifts of Katz' θ operator in characteristic zero, and we prove a new Sturm bound theorem.

Keywords: Congruences for modular forms; Galois representations; Sturm bounds.

Mathematics Subject Classification 2020: 11F33, 11F80

0. Introduction

0.1. The setup

Let f be a newform of weight $k \geq 2$, level $N \geq 1$, and character $\varepsilon : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C}^\times$. We denote by K_f the number field generated by the Fourier coefficients of f , and by \mathcal{O}_f its ring of integers. Given a prime number ℓ , let us write $\rho_{f,\ell}$ for the ℓ -adic representation attached to f by Deligne

$$\rho_{f,\ell} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(K_f \otimes \mathbb{Q}_{\ell}),$$

where $G_{\mathbb{Q}}$ denotes the Galois group of an algebraic closure $\bar{\mathbb{Q}}$ of \mathbb{Q} . Choosing a stable lattice for $\rho_{f,\ell}$, we can assume it takes values in $\mathrm{GL}_2(\mathcal{O}_f \otimes \mathbb{Z}_{\ell})$. For a prime ideal λ of \mathcal{O}_f , let us denote by $\mathcal{O}_{f,\lambda}$ the completion of \mathcal{O}_f at λ . The decomposition $\mathcal{O}_f \otimes \mathbb{Z}_{\ell} = \prod_{\lambda|\ell} \mathcal{O}_{f,\lambda}$, where the product runs over all the prime ideals in \mathcal{O}_f above ℓ , gives rise to a Galois representation $\rho_{f,\lambda}$ with values in $\mathrm{GL}_2(\mathcal{O}_{f,\lambda})$. Reducing $\rho_{f,\lambda}$ modulo the maximal ideal of $\mathcal{O}_{f,\lambda}$ and taking the

semi-simplification, we finally get a residual representation $\bar{\rho}_{f,\lambda} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{F}_{\lambda})$ where \mathbb{F}_{λ} denotes the residue field of $\mathcal{O}_{f,\lambda}$. Notice that $\bar{\rho}_{f,\lambda}$ does not depend on the choice of the stable lattice. In this paper, we will be interested in the following result which has been proved by Ribet in 1985 [29]:

Theorem 0.1 ([29]). *For all but finitely many λ the representation $\bar{\rho}_{f,\lambda}$ is irreducible. Furthermore, if f is not a form with complex multiplication (see Definition 5.2), then for all but finitely many λ , the order of the image of $\bar{\rho}_{f,\lambda}$ is divisible by the residue characteristic of λ .*

For simplicity, we shall say that λ is exceptional if one of the conclusions of Ribet's theorem does not hold. Let us denote by $\mathbb{P}\bar{\rho}_{f,\lambda}$ the projectivization of $\bar{\rho}_{f,\lambda}$, that is the composition of $\bar{\rho}_{f,\lambda}$ with the canonical projection map from $\mathrm{GL}_2(\mathbb{F}_{\lambda})$ to $\mathrm{PGL}_2(\mathbb{F}_{\lambda})$. According to the classification of the subgroups of $\mathrm{PGL}_2(\mathbb{F}_{\lambda})$ and $\mathrm{PSL}_2(\mathbb{F}_{\lambda})$ [14, II.8.27], if λ is exceptional, then one of the following is true:

- (1) the representation $\bar{\rho}_{f,\lambda}$ is reducible;
- (2) the image of $\mathbb{P}\bar{\rho}_{f,\lambda}$ is a dihedral group D_{2n} with $\ell \nmid n$;
- (3) the image of $\mathbb{P}\bar{\rho}_{f,\lambda}$ is isomorphic to \mathfrak{A}_4 , \mathfrak{S}_4 or \mathfrak{A}_5 .

Therefore, Ribet's theorem is equivalent to show that the above three cases occur finitely many times (under the assumption that f is non-CM in the second case).

The theorem generalized results of Ribet from 1975 for $N = 1$ [27], which already extended those of Serre and Swinnerton-Dyer from 1973 for $N = 1$ and $K_f = \mathbb{Q}$ [32, 35]. Although the first result of Ribet from 1975 gave an explicit description of the prime ideals for which the associated representation is reducible, it was no more the case in 1985. The second part of the theorem was already ineffective in 1975. The first step in making Ribet's result effective has been accomplished by Billerey and Dieulefait in 2014 [3]. Assuming the character of f is trivial, they gave explicit criteria for the residue characteristics ℓ of λ in terms of k and N , for $\bar{\rho}_{f,\lambda}$ to be reducible. In the two other cases, they gave explicit bounds for ℓ , in terms of k and N .

0.2. Statement of results

In this paper, we extend the results of [3] to all newforms of arbitrary weight, level and character. The argument used to deal with the third case given in [3] can be applied without modifications to a form with non-trivial character. We recall their result for the sake of completeness.

Theorem 0.2. *If the image of $\mathbb{P}\bar{\rho}_{f,\lambda}$ is isomorphic to \mathfrak{A}_4 , \mathfrak{S}_4 or \mathfrak{A}_5 , then either $\ell \mid N$ or $\ell \leq 4k - 3$.*

We now focus on the reducible and dihedral cases. The main idea to deal with these cases is to translate them into congruences between modular forms. In the dihedral case, we get a congruence between twists of f , while in the reducible case

we deal with congruences involving Eisenstein series. To deduce a bound from a congruence between two modular forms, the so-called Sturm bounds are usually used. We generalize them to deal with modular forms of arbitrary weight, level and character (see Proposition 3.17). In the dihedral projective image case, the bound we get for the residue characteristic is the following.

Theorem 0.3 (Theorem 5.10). *Assume $\overline{\rho}_{f,\lambda}$ has dihedral projective image. If $N = 1$ then we have $\ell \leq k$ or $\ell \in \{2k - 1, 2k - 3\}$. Else, if $N \geq 2$ and f does not have complex multiplication, then we have*

$$\ell \leq (2N^{\frac{k-1}{2}})^{[K_f:\mathbb{Q}]} \times \max \left(\left(\frac{k}{3} (2 \log \log(N) + 2.4) \right)^{\frac{k-1}{2}}, \left(\frac{5}{2} N^{\frac{k-1}{2}} \right) \right)^{[K_f:\mathbb{Q}]}.$$

This result gives us indeed an upper bound for ℓ in terms of N and k because $[K_f : \mathbb{Q}]$ can be bounded by the dimension of the \mathbb{C} -vector space generated by the newforms of weight k , level N and character ε (see for example [22]).

The most challenging case is when $\overline{\rho}_{f,\lambda}$ is reducible. In this situation, we generalize the results of [3, Sec. 2] to newforms of arbitrary character. The restriction on the character in [3] was mainly due to a partial knowledge of the constant term of Eisenstein series at arbitrary cusps. This computation has been done in full generality in [4], allowing us to generalize their result. The following theorem then follows from combining this technical result with a detailed study of modular reducible representations, hence extending the strategy used for the proof of [3, Theorem 2.7].

Theorem 0.4 (Theorem 4.22). *Assume $\overline{\rho}_{f,\lambda}$ to be reducible. Then one of following holds:*

- (1) $\ell \leq k + 1$;
- (2) $\ell \mid N\varphi(N)$;
- (3) *there exists a prime-to- ℓ primitive Dirichlet character η of conductor $\mathfrak{c}_0 \mid N$ and such that $\eta(-1) = (-1)^k$ and ℓ divides the algebraic norm of one of the nonzero following quantities:*
 - (a) $p^k - \eta(p)$ for a prime number $p \mid N$;
 - (b) the k th Bernoulli number $B_{k,\eta}$ attached to η (see Definition 2.1).

The precise study of reducible modular representations used in the proof of the previous theorem is the main novelty of the present paper. The basic question we consider is as follows: How to characterize the reducibility of $\overline{\rho}_{f,\lambda}$ by a finite number of explicit congruences? We give two answers to this question. A general one that applies without any restriction on ℓ or f , and, under some assumptions on ℓ , a second one for which the number of congruences to check is independent from ℓ . A weaker form of our first main result in this direction is the following.

Theorem 0.5 (Theorem 4.15). *The following are equivalent:*

- (1) $\overline{\rho}_{f,\lambda}$ is reducible;

- (2) Let \mathfrak{L} be a place of $\overline{\mathbb{Q}}$ above λ . There exist two primitive Dirichlet characters $\varepsilon_1, \varepsilon_2$ of conductor $\mathfrak{c}_1, \mathfrak{c}_2$, respectively, such that $\mathfrak{c}_1 \mathfrak{c}_2 \mid N$, and two integers m_1, m_2 such that $0 \leq m_1 \leq m_2 \leq \ell - 2$ and $\overline{\chi}_\ell^{m_1+m_2} \varepsilon_1 \varepsilon_2 \equiv \overline{\chi}_\ell^{k-1} \varepsilon \pmod{\mathfrak{L}}$. Define

$$\tilde{k} = \begin{cases} 3 + \max(k, m_2 + 2m_1 + 1) & \text{if } \ell \mid N, \\ \ell + 5 + \max(k, m_2 + \ell m_1 + 1) & \text{if } \ell \nmid N. \end{cases}$$

For every prime number $p \leq \frac{N\tilde{k}}{3} \prod_{q \mid 2N} \text{prime}(1 + \frac{1}{q})$ and not dividing 2ℓ , we have

- $p \nmid N$ and $a_p(f) \equiv p^{m_1} \varepsilon_1(p) + p^{m_2} \varepsilon_2(p) \pmod{\mathfrak{L}}$;
- or, $p \mid N$ and $a_p(f) \equiv p^{m_1} b_p \pmod{\mathfrak{L}}$ for some b_p in the set $\{0, \varepsilon_1(p), p^{m_2-m_1} \varepsilon_2(p)\}$.

When this holds, we moreover have $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1} \overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{m_2} \overline{\varepsilon}_2$.

Notice that this result applies with no assumption on f and ℓ . In particular, it can be used to check the reducibility of $\overline{\rho}_{f,\lambda}$ for any given λ , including the ones which residue characteristic is small compared to the weight, or divides the level. Such restrictions appear for instance in the work of Anni [1, Algorithm 7.2.4], where the author develops a different, bottom-up approach, toward these questions in the context of modular forms à la Katz.

In the previous statement, the number of congruences to be satisfied in order to prove the reducibility of $\overline{\rho}_{f,\lambda}$ depends not only on N, k and ε , but also on ℓ . Under some assumptions on ℓ , we have been able to remove this dependency in the bound. A weaker form of our second main result can be stated as follows.

Theorem 0.6 (Theorem 4.20). Assume $\ell > k + 1$ and $\ell \nmid N\varphi(N)$, where φ denotes the Euler totient function. The following are equivalent:

- (1) $\overline{\rho}_{f,\lambda}$ is reducible.
- (2) Let \mathfrak{L} be a place of $\overline{\mathbb{Q}}$ above λ . There exist two primitive Dirichlet characters $\varepsilon_1, \varepsilon_2$ of conductor $\mathfrak{c}_1, \mathfrak{c}_2$ respectively, such that $\mathfrak{c}_1 \mathfrak{c}_2 \mid N$, and $\varepsilon_1 \varepsilon_2 = \varepsilon$. For all odd primes $p \leq \frac{Nk}{3} \prod_{q \mid 2N} \text{prime}(1 + \frac{1}{q})$, we have
 - $p \nmid N$ and $a_p(f) \equiv \varepsilon_1(p) + p^{k-1} \varepsilon_2(p) \pmod{\mathfrak{L}}$;
 - $p \mid N$ and $a_p(f) \equiv b_p \pmod{\mathfrak{L}}$ for some $b_p \in \{0, \varepsilon_1(p), p^{k-1} \varepsilon_2(p)\}$.

When this holds, we moreover have $\overline{\rho}_{f,\lambda} \cong \overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{k-1} \overline{\varepsilon}_2$.

We stress the fact that according to these latter two results, proving the reducibility of $\overline{\rho}_{f,\lambda}$ requires checking almost $Nk^2 \log \log(N)$ congruences (and even $Nk \log \log(N)$ for the primes ℓ satisfying the assumptions $\ell > k + 1$ and $\ell \nmid N\varphi(N)$). Notice that the $\log \log(N)$ part comes from the upper bound we prove in Lemma 3.22.

To achieve such bound, we extensively use the local description of $\overline{\rho}_{f,\lambda}$ at the bad prime numbers (i.e. the prime numbers dividing N), together with generalized Sturm bounds theorems and an appropriate use of degeneracy maps between modular forms spaces of various levels. Having a sharp bound is especially important from a computational point of view. Indeed, those results also provide us with an algorithm that explicitly computes the exact set of λ such that $\overline{\rho}_{f,\lambda}$ is reducible. We have implemented such an algorithm in PARI/GP [36].

0.3. Organization of the paper

In Sec. 1, we collect various results on the local description of residual modular representations. Section 2 is devoted to recall basic facts about Dirichlet characters and Eisenstein series. In Sec. 3, we develop various tools that will play a central role in the proof of the main results. In Sec. 3.1, we construct the so-called theta operators in characteristic zero, that we then use to generalize Sturm bounds results in Sec. 3.2. In Sec. 3.3, we introduce various other operators acting on modular forms spaces that allow us to modify some Fourier coefficients of a given form. The next two sections are devoted to prove the results involving reducible residual modular representations and dihedral representations, respectively. Finally, we explain in the last section how to translate our theoretic results on reducibility into an algorithm that takes a modular form as input, and outputs the exact list of prime ideals λ such that $\overline{\rho}_{f,\lambda}$ is reducible. We then illustrate this algorithm on numerical examples.

0.4. General notations

In the whole paper, for two positive integers k and N , and a Dirichlet character ε modulo N , the notations $M_k(N, \varepsilon)$, $S_k(N, \varepsilon)$ and $S_k^{\text{new}}(N, \varepsilon)$ stand for the complex vector spaces of modular forms, cuspidal modular forms, and new modular forms of weight k , level N , and character ε , respectively. We also denote by $M(N)$ the graded algebra of modular forms of level N . For any modular form g in $M(N)$, we always write $\sum_{n=0}^{\infty} a_n(g)q^n$ for its q -expansion at infinity, with $q = e^{2i\pi z}$ and z in the complex upper-half plane.

1. Background on Newforms and Residual Modular Galois Representations

We fix for this section a newform f of weight $k \geq 2$, level $N \geq 1$, and character ε . Let ℓ be a prime number and let λ be a prime ideal of \mathcal{O}_f above ℓ . We first recall a result on the expression of the p th coefficient of f for a prime p dividing N that we will be using intensively.

Proposition 1.1 ([24, Theorem 4.6.17]). *Let p be a prime dividing N . Write \mathfrak{c} for the conductor of ε .*

(1) *If $v_p(N) = v_p(\mathfrak{c})$, then $|a_p(f)|^2 = p^{k-1}$.*

- (2) If $v_p(N) = 1$ and $v_p(\mathfrak{c}) = 0$, then $a_p(f)^2 = \varepsilon'_p(p)p^{k-2}$, where ε'_p is the prime-to- p component of ε (in particular $\varepsilon'_p(p) \neq 0$).
- (3) If $v_p(N) \geq 2$ and $v_p(N) > v_p(\mathfrak{c})$, then $a_p(f) = 0$.

We now recall some results about the shape of $\bar{\rho}_{f,\lambda}$ restricted to a decomposition subgroup. In the following, given a prime number p we denote by G_p a decomposition subgroup of $G_{\mathbb{Q}}$ at p , and by I_p its inertia subgroup. For some λ -integer x , $\mu_p(x)$ stands for the unique unramified character of G_p sending a Frobenius element at p to the reduction of x modulo λ . We will simply write $\mu(x)$ when no confusion on p can arise. We finally write $\bar{\chi}_{\ell}$ for the cyclotomic character modulo ℓ .

We begin by the local description of $\bar{\rho}_{f,\lambda}$ at ℓ that has been established by Deligne and Fontaine. Their result is the following.

Proposition 1.2 (Deligne–Fontaine, [13, Theorems 2.5 and 2.6]). Assume $2 \leq k \leq \ell + 1$ and $\ell \nmid N$.

- If f is ordinary at λ (that is if $a_{\ell}(f) \not\equiv 0 \pmod{\lambda}$), then $\bar{\rho}_{f,\lambda|G_{\ell}}$ is reducible, and we have

$$\bar{\rho}_{f,\lambda|G_{\ell}} \cong \begin{pmatrix} \bar{\chi}_{\ell}^{k-1} \mu\left(\frac{\varepsilon(\ell)}{a_{\ell}(f)}\right) & \star \\ 0 & \mu(a_{\ell}(f)) \end{pmatrix}.$$

- If not, then $\bar{\rho}_{f,\lambda|G_{\ell}}$ is irreducible, and we have

$$\bar{\rho}_{f,\lambda|I_{\ell}} \cong \begin{pmatrix} \psi^{k-1} & 0 \\ 0 & \psi'^{k-1} \end{pmatrix}.$$

Here $\{\psi, \psi'\} = \{\psi, \psi^{\ell}\}$ stands for the set of fundamental characters of level 2 (see [13, 2.4]).

For the primes p different from ℓ and dividing N , the shape of $\bar{\rho}_{f,\lambda|G_p}$ has been computed by Langlands and compiled in [20, Proposition 2.8].

Proposition 1.3. Let $p \neq \ell$ be a prime dividing N and let \mathfrak{c} be the conductor of ε . We denote by v_p the p -adic valuation.

- If $v_p(N) = 1$ and $v_p(\mathfrak{c}) = 0$, then we have

$$\bar{\rho}_{f,\lambda|G_p} \cong \begin{pmatrix} \mu(a_p(f))\bar{\chi}_{\ell} & \star \\ 0 & \mu(a_p(f)) \end{pmatrix}.$$

- If $v_p(N) = v_p(\mathfrak{c})$, then $a_p(f)$ is a unit in $\mathcal{O}_{f,\lambda}$ and we have

$$\bar{\rho}_{f,\lambda|G_p} \cong \mu(a_p(f)) \oplus \mu(a_p(f)^{-1})\bar{\chi}_{\ell}^{k-1}\overline{\varepsilon|_{G_p}},$$

where $\overline{\varepsilon|_{G_p}}$ stands for the reduction modulo λ of the restriction of ε to G_p .

Proof. From the first case of Proposition 1.1, we have $|a_p(f)|^2 = p^{k-1}$ in the second case. Therefore, $a_p(f)$ is indeed invertible in $\mathcal{O}_{f,\lambda}$ because $p \neq \ell$.

The only thing to prove is that the hypothesis of [20, Proposition 2.8] holds in our cases, namely that f is p -primitive in the terminology of [20, Definition 2.7]. To do so, we use [21, Theorem]. We recall a direct consequence of this result: Define $u = \min(\lfloor \frac{v_p(N)}{2} \rfloor, v_p(N) - v_p(\mathfrak{c}))$. If $u = 0$, then f is p -primitive. We easily check that in our two cases we have $u = 0$. \square

Since the work of Carayol [5, Théorème (A)], it is well known that the value of the prime-to- ℓ part of the Artin conductor of $\rho_{f,\lambda}$ is equal to the prime-to- ℓ part of N . The study of the behavior of the Artin conductor after reduction (i.e. the one of $\overline{\rho}_{f,\lambda}$) has then been established independently by Carayol [6] and Livné [19]. Here is their result.

Proposition 1.4 (Carayol–Livné). *Let $N(\overline{\rho}_{f,\lambda})$ be the prime-to- ℓ part of the Artin conductor of $\overline{\rho}_{f,\lambda}$. We then have*

$$N(\overline{\rho}_{f,\lambda}) \mid N.$$

Moreover, write $e_p := v_p(N) - v_p(N(\overline{\rho}_{f,\lambda}))$ for a prime $p \neq \ell$. If $e_p > 0$, then we have $v_p(N) - v_p(N(\overline{\rho}_{f,\lambda})) \in \{1, 2\}$.

2. Background on Dirichlet Characters and Eisenstein Series

2.1. Generalized Bernoulli numbers and Gauß sums

Let ε be a primitive Dirichlet character of conductor \mathfrak{c} . We recall the definition and properties of the Gauß sums and generalized Bernoulli numbers attached to ε .

Definition 2.1. The Bernoulli numbers $(B_{m,\varepsilon})_{m \geq 0}$ attached to ε are defined by the following generating series:

$$\sum_{n=1}^{\mathfrak{c}} \varepsilon(n) \frac{te^{nt}}{e^{ct} - 1} = \sum_{m=0}^{\infty} B_{m,\varepsilon} \frac{t^m}{m!}.$$

In particular, when ε is odd, we have $B_{1,\varepsilon} = \frac{1}{\mathfrak{c}} \sum_{n=1}^{\mathfrak{c}-1} n\varepsilon(n)$, and when ε is both even and non-trivial, we have $B_{2,\varepsilon} = \frac{1}{\mathfrak{c}} \sum_{n=1}^{\mathfrak{c}-1} n^2\varepsilon(n)$.

Remark 2.2. If $\varepsilon = 1$ is the trivial character modulo 1, we get the classical Bernoulli numbers except when $m = 1$, in which case we have $B_{1,1} = \frac{1}{2} = -B_1$.

We state below the main properties of the Bernoulli numbers. First, we exactly know when the Bernoulli numbers vanish (see [24, Theorem 3.3.4] for a proof).

Proposition 2.3. *We have $B_{m,\varepsilon} = 0$ if and only if $\varepsilon(-1) \neq (-1)^m$.*

Second, the behavior of the Bernoulli numbers after reduction modulo a prime ideal has been studied by Van-Staudt [33] in the case $\varepsilon = 1$, and by Carlitz [7, Theorem 1] in the case $\varepsilon \neq 1$. We summarize their results in the following proposition.

Proposition 2.4. *Let m be a positive integer.*

- (1) *Let ℓ be a prime number. If $\ell - 1$ divides m , then we have the congruence $\ell B_{m,1} \equiv -1 \pmod{\ell}$. Otherwise, $\frac{B_{m,1}}{m}$ is ℓ -integral and its reduction modulo ℓ only depends on m modulo $\ell - 1$. In particular, the denominator of $B_{m,1}$ is equal to $\prod_{\substack{\ell-1|m \\ \ell \text{ prime}}} \ell$.*
- (2) *For $\varepsilon \neq 1$, write $\frac{B_{m,\varepsilon}}{m} = \mathfrak{N}\mathfrak{D}^{-1}$, with \mathfrak{N} and \mathfrak{D} two coprime ideals of $\mathbb{Z}[\varepsilon]$, the ring spanned by the image of ε . If the conductor of ε admits at least two distinct prime factors, then $\mathfrak{D} = 1$. Otherwise, if the conductor of ε is a power of a prime number ℓ , then \mathfrak{D} contains only prime ideals above ℓ .*

Another classical quantity attached to Dirichlet characters is the Gauß sum. We recall its definition and properties below.

Definition 2.5. The Gauß sum attached to ε is

$$W(\varepsilon) = \sum_{n=1}^c \varepsilon(n) e^{\frac{2i\pi n}{c}}.$$

One can find the following result in [3, Lemma 2.1].

Proposition 2.6. *The prime divisors of the algebraic norm of $W(\varepsilon)$ are those of c .*

2.2. Teichmüller lifts

We present here the behavior of roots of unity after reduction modulo \mathfrak{L} .

Lemma 2.7. *Let n be a positive integer and let ζ be a primitive n th root of unity in $\overline{\mathbb{Q}}$. Let ℓ be a prime number and let \mathfrak{L} be a place of $\overline{\mathbb{Q}}$ above ℓ . We have $\zeta \equiv 1 \pmod{\mathfrak{L}}$ if and only if n is a power of ℓ . In particular, a Dirichlet character is trivial modulo \mathfrak{L} if and only if it has order a power of ℓ .*

Proof. According to [9, Proposition 3.5.4], the algebraic norm of $1 - \zeta$ over $\mathbb{Q}(\zeta)$ is equal to

$$\begin{cases} 0 & \text{if } n = 1; \\ q & \text{if } n = q^r \text{ with } q \text{ prime and } r \geq 1; \\ 1 & \text{otherwise.} \end{cases}$$

Thus, if n is not an ℓ -power, then ℓ does not divide the norm of $\zeta - 1$ and we have $\zeta \not\equiv 1 \pmod{\mathfrak{L}}$. Assume $n = \ell^r$, $r \geq 1$. We then have

$$\ell \mathbb{Z}[\zeta] = (1 - \zeta)^{\ell^r - 1} \mathbb{Z}[\zeta].$$

Thus, the only prime ideal above ℓ in $\mathbb{Z}[\zeta]$ is $(1 - \zeta)\mathbb{Z}[\zeta]$, and we therefore have $\zeta \equiv 1 \pmod{\mathfrak{L}}$.

For the second part of the lemma, let ε be a Dirichlet character modulo N . From above, ε is trivial modulo \mathfrak{L} if and only if $\varepsilon(x)$ is a root of unity of order a power of ℓ for every $x \in (\mathbb{Z}/N\mathbb{Z})^\times$. This can happen if and only if ε has order a power of ℓ . \square

Lemma 2.7 implies that the kernel of the reduction modulo \mathfrak{L} from the group of all roots of unity to $\overline{\mathbb{F}}_\ell^\times$, is the subgroup of primitive roots of unity of order a power of ℓ . In particular, the restriction of this map to the subgroup of roots of unity of order prime to ℓ is injective. Moreover, because the subgroup of roots of unity of order $\ell^n - 1$ maps to $\mathbb{F}_{\ell^n}^\times$, it is onto and therefore an isomorphism. The inverse map

$$T_{\mathfrak{L}} : \overline{\mathbb{F}}_\ell^\times \rightarrow \{\zeta \in \mathbb{C}^\times, \gcd(\ell, \text{ord}(\zeta)) = 1\},$$

is the so-called Teichmüller lift with respect to the place \mathfrak{L} . It will allow us to lift multiplicatively characters modulo \mathfrak{L} to Dirichlet characters of prime-to- ℓ order. Moreover, the Dirichlet characters that arise this way are exactly the ones that have the same conductor as a Dirichlet character and as a character modulo \mathfrak{L} .

2.3. Eisenstein series

Let k be a positive integer and let $\varepsilon_1, \varepsilon_2$ be two Dirichlet characters modulo \mathfrak{c}_1 and \mathfrak{c}_2 , respectively, such that $\varepsilon_1 \varepsilon_2(-1) = (-1)^k$. Moreover, if $k = 2$ and $\varepsilon_1, \varepsilon_2$ are both trivial, then assume $\mathfrak{c}_1 = 1$ and \mathfrak{c}_2 is a prime number, otherwise, assume ε_1 and ε_2 are primitive. For a complex number z in the complex upper-half plane \mathcal{H} , consider the following q -expansion:

$$E_k^{\varepsilon_1, \varepsilon_2}(z) := C + \sum_{n=1}^{\infty} \sigma_{k-1}^{\varepsilon_1, \varepsilon_2}(n) q^n, \quad (2.1)$$

with $\sigma_r^{\varepsilon_1, \varepsilon_2}(n) = \sum_{0 < d|n} d^r \varepsilon_1(\frac{n}{d}) \varepsilon_2(d)$ for any $r \geq 0$ and

$$C = \begin{cases} 0 & \left| \begin{array}{l} \text{if } k \geq 2 \text{ and } \varepsilon_1 \neq 1, \\ \text{or if } k = 1 \text{ and } \varepsilon_1, \varepsilon_2 \text{ are both non-trivial;} \end{array} \right. \\ \frac{1}{24}(\mathfrak{c}_2 - 1) & \text{if } k = 2 \text{ and } \varepsilon_1, \varepsilon_2 \text{ both trivial;} \\ -\frac{B_{k, \varepsilon_1 \varepsilon_2}}{2k} & \text{otherwise.} \end{cases}$$

The following result is proved in [24, Theorem 4.7.1] and [24, (4.7.16)].

Proposition 2.8. *The q -series $E_k^{\varepsilon_1, \varepsilon_2}$ defines a modular form of weight k , level $\mathfrak{c}_1 \mathfrak{c}_2$ and character $\varepsilon_1 \varepsilon_2$. It is a normalized eigenform for all the Hecke operators at level $\mathfrak{c}_1 \mathfrak{c}_2$.*

For $\varepsilon_1 = \varepsilon_2 = 1$, the definition of the series $E_k^{1,1}$ agrees with the definition of the classical Eisenstein series of weight k . We simply write it E_k in this case.

For $k = 2$, we denote by E_2 the q -series

$$E_2(z) = -\frac{1}{24} + \sum_{n=1}^{\infty} \left(\sum_{0 < d|n} d \right) q^n.$$

Note that this formula defines a holomorphic function on \mathcal{H} , but E_2 is not modular.

In the case $k \geq 2$ and $\varepsilon_1, \varepsilon_2$ primitive, the behavior of the constant coefficient of $E_k^{\varepsilon_1, \varepsilon_2}$ at a cusp of $\Gamma_1(N)$ has been computed in [4, Proposition 4]. It states the following:

Proposition 2.9. *Assume $k \geq 2$ and $\varepsilon_1, \varepsilon_2$ are primitive. Let M be a positive integer and let $\gamma = \begin{pmatrix} u & \beta \\ v & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Put $\widetilde{v} := \frac{v}{\gcd(v, M)}$ and $\widetilde{M} := \frac{M}{\gcd(v, M)}$. We define*

$$\Upsilon_k^{\varepsilon_1, \varepsilon_2}(\gamma, M) := \lim_{\mathrm{Im}(z) \rightarrow +\infty} (E_k^{\varepsilon_1, \varepsilon_2}(M \cdot) |_k \gamma)(z),$$

where we denote by $|_k$ the classical slash action of weight k .

If $\mathfrak{c}_2 \nmid \widetilde{v}$ then $\Upsilon_k^{\varepsilon_1, \varepsilon_2}(\gamma, M) = 0$. Otherwise, if $\mathfrak{c}_2 \mid \widetilde{v}$ then $\Upsilon_k^{\varepsilon_1, \varepsilon_2}(\gamma, M) \neq 0 \Leftrightarrow \gcd(\mathfrak{c}_1, \frac{\widetilde{v}}{\mathfrak{c}_2}) = 1$. In this case, we moreover have

$$\begin{aligned} \Upsilon_k^{\varepsilon_1, \varepsilon_2}(\gamma, M) &= -\varepsilon_2^{-1}(\widetilde{M}u)_{\varepsilon_1} \left(-\frac{\widetilde{v}}{\mathfrak{c}_2} \right) \frac{W((\varepsilon_1 \varepsilon_2^{-1})_0)}{W(\varepsilon_2^{-1})} \\ &\quad \times \frac{B_{k, (\varepsilon_1^{-1} \varepsilon_2)_0}}{2k} \left(\frac{\mathfrak{c}_2}{\widetilde{M} \mathfrak{c}_0} \right)^k \prod_{p \mid \mathfrak{c}_1 \mathfrak{c}_2} \left(1 - \frac{(\varepsilon_1 \varepsilon_2^{-1})_0(p)}{p^k} \right), \end{aligned}$$

where χ_0 denotes the primitive character associated to a Dirichlet character χ , and \mathfrak{c}_0 the conductor of $\varepsilon_1^{-1} \varepsilon_2$.

The proof of [4] is only given in the cases $k \geq 3$, and $k = 2$ and $\varepsilon_1, \varepsilon_2$ non-trivial. We give a proof of the result in the case $k = 2$, $\varepsilon_1 = \varepsilon_2 = \mathbb{1}$, based on the techniques used in [4].

Proof. As in [4, §1.3], we write for $\mathrm{Re}(\varepsilon) > 0$ and $z \in \mathcal{H}$,

$$G_{2, \varepsilon}(z) := \sum_{(m, n) \in \mathbb{Z}^2 \setminus \{(0, 0)\}} \frac{1}{(mz + n)^2 |mz + n|^{2\varepsilon}}.$$

By [24, Corollary 7.2.10 and Theorem 7.2.12], the function $\varepsilon \mapsto G_{2, \varepsilon}(z)$ is holomorphically continued to $\mathrm{Re}(\varepsilon) > -\frac{1}{2}$ and we have

$$\lim_{\varepsilon \rightarrow 0} G_{2, \varepsilon}(z) = -8\pi^2 E_2(z) - \frac{\pi}{\mathrm{Im}(z)}.$$

Now, because $\text{Im}(M \frac{uz+\beta}{vz+\delta}) = \frac{M\text{Im}(z)}{|vz+\delta|^2}$, we get that

$$\begin{aligned} \Upsilon_2^{1,1}(\gamma, M) &= \lim_{\text{Im}(z) \rightarrow +\infty} \lim_{\varepsilon \rightarrow 0} \left(-\frac{1}{8\pi^2} G_{2,\varepsilon}(M \cdot) |_2 \gamma(z) + \frac{1}{(vz+\delta)^2} \frac{1}{8\pi \text{Im}\left(M \frac{uz+\beta}{vz+\delta}\right)} \right) \\ &= -\frac{1}{8\pi^2} \lim_{\text{Im}(z) \rightarrow +\infty} \lim_{\varepsilon \rightarrow 0} G_{2,\varepsilon}(M \cdot) |_2 \gamma(z) + \lim_{\text{Im}(z) \rightarrow +\infty} \frac{|vz+\delta|^2}{8\pi M(vz+\delta)^2 \text{Im}(z)} \\ &= -\frac{1}{8\pi^2} \lim_{\text{Im}(z) \rightarrow +\infty} \lim_{\varepsilon \rightarrow 0} G_{2,\varepsilon}(M \cdot) |_2 \gamma(z). \end{aligned}$$

From this identity the proof of [4] still applies. Let us write $z^{2,\varepsilon} := z^2 |z|^{2\varepsilon}$. The function $G_{2,\varepsilon}(M \cdot) |_2 \gamma(z)$ writes as $T_\varepsilon(z) + R_\varepsilon(z)$, with

$$\begin{aligned} T_\varepsilon(z) &= \sum_{\substack{mMu+nv=0 \\ (m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}}} \frac{1}{(mM\beta + n\delta)^{2,\varepsilon}} \quad \text{and} \\ R_\varepsilon(z) &= \sum_{\substack{mMu+nv \neq 0 \\ (m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}}} \frac{1}{((mMu + nv)z + (mM\beta + n\delta))^{2,\varepsilon}}. \end{aligned}$$

The function T_ε is independent of z and the series obtained by setting ε to 0 is absolutely convergent. Therefore, we have

$$\lim_{\text{Im}(z) \rightarrow +\infty} \lim_{\varepsilon \rightarrow 0} T_\varepsilon(z) = \sum_{\substack{mMu+nv=0 \\ (m,n) \in \mathbb{Z}^2 \setminus \{(0,0)\}}} \frac{1}{(mM\beta + n\delta)^2}.$$

Finally, writing n in $R_\varepsilon(z)$ as $Mn' + \rho$, with ρ between 0 and $M-1$, we have

$$\begin{aligned} R_\varepsilon(z) &= \sum_{(m,n') \in \mathbb{Z}^2} \sum_{\substack{M(mu+n'v)+v\rho \neq 0 \\ 0 \leq \rho \leq M-1}} \frac{1}{(z(M(mu+n'v) + v\rho) + M(m\beta + n'\delta) + \rho\delta)^{2,\varepsilon}} \\ &= \sum_{\rho=0}^{M-1} \sum_{\substack{Mp+v\rho \neq 0 \\ (p,q) \in \mathbb{Z}^2}} \frac{1}{(z(Mp + v\rho) + Mq + \delta\rho)^{2,\varepsilon}}. \end{aligned}$$

The last equation is justified by the fact that $(mu + n'v, m\beta + n'\delta) = (m, n')\gamma$. Applying [4, Lemma 9] with $a_1 = v\rho$, $a_2 = \delta\rho$ and $D = M$, we get

$$\lim_{\text{Im}(z) \rightarrow +\infty} \lim_{\varepsilon \rightarrow 0} R_\varepsilon(z) = 0.$$

Lemma 6 of [4] therefore still applies in the case $(k, \varepsilon_1, \varepsilon_2) = (2, 1, 1)$ and one easily checks that the proof of Lemma 7 and Proposition 4 of [4] only uses the fact that ε_1 and ε_2 are Dirichlet characters satisfying $\varepsilon_1 \varepsilon_2(-1) = (-1)^k$. \square

3. Preliminary Results on Modular Forms

3.1. Theta operators

We fix for this paragraph a place \mathfrak{L} of $\overline{\mathbb{Q}}$. Consider the operator θ acting on the space of holomorphic functions on \mathcal{H} by $\frac{1}{2i\pi} \frac{d}{dz} = q \frac{d}{dq}$. On q -expansions, this operator maps $\sum_{n \geq 0} a_n q^n$ to $\sum_{n \geq 0} n a_n q^n$. It is well known that if g is a modular form, then θg is no longer modular (see for example [37, Chap. 5]). However, Swinnerton–Dyer and Serre [35, §3] have proved that for $\ell \geq 5$ and a level 1 modular form g with \mathfrak{L} -integral Fourier coefficients, one can construct a level 1 form with \mathfrak{L} -integral Fourier coefficients and which Fourier coefficients are congruent modulo \mathfrak{L} to the one of θg . More generally, Katz [16] has proved using his geometric theory of modular forms that there is an operator on the space of modular forms with coefficients in an algebraic closure of \mathbb{F}_ℓ , which action on the q -expansions is the same as the one of θ . For our purposes, the main drawbacks of this latter approach is that Katz' modular forms modulo \mathfrak{L} do not always lift in characteristic 0, and have by essence a prime-to- ℓ level. To remedy this, we will construct for any given level $N \geq 1$ and place \mathfrak{L} , an operator $\tilde{\theta}$ acting on $M(N)$, stabilizing the subspace of modular forms with \mathfrak{L} -integral Fourier coefficients, and such that for every modular form g with \mathfrak{L} -integral coefficients we have

$$\tilde{\theta}g \equiv \theta g \pmod{\mathfrak{L}},$$

meaning that $a_n(\tilde{\theta}g)$ and $na_n(g)$ are congruent modulo \mathfrak{L} for all n .

The main tool we will use in the construction of $\tilde{\theta}$ is the Rankin–Cohen bracket, introduced by Cohen in [8, Corollary 7.2]. We recall its definition and properties in what follows.

Proposition 3.1 (Rankin–Cohen bracket). *Let g and h be two modular forms of weight k_g and k_h , level N_g and N_h , and character ε_g and ε_h , respectively. The Rankin–Cohen bracket of g and h is*

$$[g, h] := k_g g \theta h - k_h h \theta g.$$

It is a modular form of weight $k_g + k_h + 2$, level $\text{lcm}(N_g, N_h)$ and character $\varepsilon_g \varepsilon_h$. Moreover, if both g and h have their Fourier coefficients in a ring R , then so has $[g, h]$.

Let N be a positive integer. For a prime number p , we denote by T_p^N the p th Hecke operator acting on $M(N)$. Recall that a modular form $g \in M_k(N, \varepsilon)$ is an eigenform for T_p^N modulo \mathfrak{L} with eigenvalue $a_p \in \overline{\mathbb{F}_\ell}$ in the sense of [11, §6(b)] if g has \mathfrak{L} -integral Fourier coefficients, and if $T_p^N g$ is congruent to $a_p g$ modulo \mathfrak{L} . If g is moreover normalized modulo \mathfrak{L} , that is if $a_1(g) \equiv 1 \pmod{\mathfrak{L}}$, then g is an eigenform for T_p^N modulo \mathfrak{L} if and only if for all integer $n \geq 0$ prime to p , and all $\alpha \geq 1$, we have

$$\begin{cases} a_{np^\alpha}(g) \equiv a_n(g) a_{p^\alpha}(g) \pmod{\mathfrak{L}}; \\ a_{p^{\alpha+1}}(g) \equiv a_p(g) a_{p^\alpha}(g) - p^{k-1} \varepsilon(p) a_{p^{\alpha-1}}(g) \pmod{\mathfrak{L}}. \end{cases}$$

The eigenvalue is then moreover the reduction of $a_p(g)$ modulo \mathfrak{L} . The following lemma is the central result that shows how to construct an operator $\tilde{\theta}$ satisfying the properties described above, using Rankin–Cohen brackets.

Lemma 3.2. *Let k_A be a positive integer, and let χ_A be a Dirichlet character modulo N . Let $A \in M_{k_A}(N, \chi_A)$ be such that A and $\frac{1}{k_A}\theta A$ have \mathfrak{L} -integral Fourier coefficients and satisfy*

$$A \equiv 1 \pmod{\mathfrak{L}}, \quad \frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}, \quad \text{and} \quad \chi_A \equiv \overline{\chi_\ell}^{-k_A} \pmod{\mathfrak{L}}.$$

Then, we have a well-defined operator $\tilde{\theta}_A$ on $M(N)$ given by $\tilde{\theta}_A g = -\frac{1}{k_A}[g, A]$. For every $g \in M_k(N, \varepsilon)$ with \mathfrak{L} -integral Fourier coefficients, this operator satisfies the following properties:

- $\tilde{\theta}_A g \in M_{k+k_A+2}(N, \varepsilon\chi_A)$ and has \mathfrak{L} -integral Fourier coefficients;
- $\tilde{\theta}_A g \equiv \theta g \pmod{\mathfrak{L}}$;
- Moreover, if for some prime number p , g is a normalized eigenform for T_p^N modulo \mathfrak{L} then $\tilde{\theta}_A g$ is also a normalized eigenform for T_p^N modulo \mathfrak{L} , with eigenvalue $pa_p(g)$.

In the following, when there will be no confusion on the form A , we shall write $\tilde{\theta}$ for the operator $\tilde{\theta}_A$.

Proof. According to Proposition 3.1 above, this is clear that $\tilde{\theta}_A$ is a well-defined operator and that $\tilde{\theta}_A g$ has the announced weight, level, and character. Furthermore, we have $\tilde{\theta}_A g = -\frac{k}{k_A}g\theta A + A\theta g$. Therefore, from the assumption, if g has \mathfrak{L} -integral Fourier coefficients, then so does $\tilde{\theta}_A g$ and we have

$$\tilde{\theta}_A g = A\theta g - \frac{k}{k_A}g\theta A \equiv \theta g \pmod{\mathfrak{L}}.$$

Assume g is a normalized eigenform for T_p^N modulo \mathfrak{L} . Then, $\tilde{\theta}_A g$ is also normalized modulo \mathfrak{L} because we have $a_1(\tilde{\theta}_A g) \equiv 1 \times a_1(g) \equiv 1 \pmod{\mathfrak{L}}$. Let $n \geq 0$ be prime to p , and $\alpha \geq 1$. We have

$$\begin{aligned} a_{np^\alpha}(\tilde{\theta}_A g) &\equiv np^\alpha a_{np^\alpha}(g) \pmod{\mathfrak{L}} \\ &\equiv (na_n(g))(p^\alpha a_{p^\alpha}(g)) \pmod{\mathfrak{L}} \\ &\equiv a_n(\tilde{\theta}_A g)a_{p^\alpha}(\tilde{\theta}_A g) \pmod{\mathfrak{L}} \end{aligned}$$

and

$$\begin{aligned} a_{p^{\alpha+1}}(\tilde{\theta}_A g) &\equiv p^{\alpha+1}a_{p^{\alpha+1}}(g) \pmod{\mathfrak{L}} \\ &\equiv p^{\alpha+1}(a_p(g)a_{p^\alpha}(g) - p^{k-1}\varepsilon(p)a_{p^{\alpha-1}}(g)) \pmod{\mathfrak{L}} \\ &\equiv a_p(\tilde{\theta}_A g)a_{p^\alpha}(\tilde{\theta}_A g) - p^{k+1}\varepsilon(p)a_{p^{\alpha-1}}(\tilde{\theta}_A g) \pmod{\mathfrak{L}}. \end{aligned}$$

If $p \mid N\ell$, we have $p^{k+1}\varepsilon(p) \equiv 0 \equiv p^{(k+k_A+2)-1}\varepsilon\chi_A(p) \pmod{\mathfrak{L}}$. Otherwise, we have $p^{k_A}\chi_A(p) \equiv 1 \pmod{\mathfrak{L}}$ by assumption, and we again have $p^{k+1}\varepsilon(p) \equiv p^{(k+k_A+2)-1}\varepsilon\chi_A(p) \pmod{\mathfrak{L}}$. As desired, we get

$$a_{p^{\alpha+1}}(\tilde{\theta}_{Ag}) \equiv a_p(\tilde{\theta}_{Ag})a_{p^\alpha}(\tilde{\theta}_{Ag}) - p^{(k+k_A+2)-1}\varepsilon\chi_A(p)a_{p^{\alpha-1}}(\tilde{\theta}_{Ag}) \pmod{\mathfrak{L}},$$

and the form $\tilde{\theta}_{Ag}$ is thus a normalized eigenform modulo \mathfrak{L} . \square

Remark 3.3. When ℓ does not divide N , the reduction of A modulo \mathfrak{L} is the so-called Katz' Hasse invariant.

The rest of this paragraph is devoted to construct, for each level N and place \mathfrak{L} , a form A that satisfies the hypotheses of Lemma 3.2 that we will constantly use. Among all possible forms, the ones presented in Table 1 are those we found with the smallest weight. Notice that if we have a form A of level M satisfying the hypotheses of Lemma 3.2 for a given place \mathfrak{L} , this form also satisfies the hypotheses of Lemma 3.2 at the multiple-of- M levels. We will use this fact to consider the smallest set of level possible.

3.1.1. Theta operators in characteristic greater than 3

The following proposition was already known to Swinnerton-Dyer in [35, Theorem 2].

Proposition 3.4. *Assume $\ell \geq 5$. The form $A := -2\ell E_{\ell-1} \in M_{\ell-1}(1, 1)$ satisfies the hypotheses of Lemma 3.2 for any level N .*

Proof. Since $\ell \geq 5$, A is well defined and the constant coefficient of A is equal to $\frac{\ell B_{\ell-1,1}}{\ell-1}$. From Proposition 2.4, it is \mathfrak{L} -integral and congruent to 1 modulo \mathfrak{L} . Moreover, because $E_{\ell-1}$ has integral coefficients, away from the constant one, it follows that A and $-\frac{1}{k_A}\theta A$ have \mathfrak{L} -integral Fourier coefficients and that $A \equiv 1 \pmod{\mathfrak{L}}$ and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. Finally, we have $\overline{\chi}_\ell^{-k_A} = \overline{\chi}_\ell^{1-\ell} \equiv 1 \pmod{\mathfrak{L}}$. \square

If the level N is divisible by ℓ , the situation is in fact much more pleasant for us, in the sense that we can find a form with $k_A = 1$. We find a record of the following fact in [30, (2.1) Theorem].

Proposition 3.5. *Assume $\ell \geq 5$ and $\ell \mid N$. Let $\chi_\mathfrak{L}$ be the Teichmüller lift of $\overline{\chi}_\ell$ with respect to the place \mathfrak{L} , viewed as a primitive character Dirichlet modulo ℓ . The form $A := 2\ell E_1^{\mathbf{1}, \chi_\mathfrak{L}^{-1}} \in M_1(\ell, \chi_\mathfrak{L}^{-1})$ satisfies the hypotheses of Lemma 3.2.*

Proof. The form A is well defined because $\chi_\mathfrak{L}^{-1}$ is an odd character. Indeed, we have $\chi_\mathfrak{L}^{-1}(-1) \equiv \overline{\chi}_\ell^{-1}(-1) \equiv -1 \pmod{\mathfrak{L}}$, and because ℓ is odd, this lifts to $\chi_\mathfrak{L}^{-1}(-1) = -1$. The constant term of A is equal to $-\ell B_{1, \chi_\mathfrak{L}^{-1}} = -\sum_{i=1}^{\ell-1} i \chi_\mathfrak{L}^{-1}(i)$ which is \mathfrak{L} -integral. Therefore, because $\chi_\mathfrak{L}$ induces the identity modulo \mathfrak{L} , this

coefficient is congruent to 1 modulo \mathfrak{L} , and because $E_1^{\mathbb{1}, \chi_{\mathfrak{L}}^{-1}}$ has integral coefficients away from the constant one, A and $\frac{1}{k_A}\theta A$ have \mathfrak{L} -integral Fourier coefficients. Moreover, we also get $A \equiv 1 \pmod{\mathfrak{L}}$ and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. Finally, by definition we have $\overline{\chi_{\ell}}^{-k_A} = \overline{\chi_{\ell}}^{-1} \equiv \chi_A \pmod{\mathfrak{L}}$. Thus, A satisfies the hypotheses of Lemma 3.2. \square

This finishes the case $\ell \geq 5$. For $\ell \leq 3$, the two previous constructions do not always give well-defined modular forms. We present in the next two paragraphs specific constructions in the cases $\ell = 2$ and $\ell = 3$.

3.1.2. Theta operators in characteristic 2

For $\ell = 2$, the most favorable case is when $4 \mid N$. The following construction is very analogous to the one of Proposition 3.5.

Proposition 3.6. *Assume $\ell = 2$ and N is divisible by 4. Let χ_4 be the only non-trivial Dirichlet character modulo 4. The form $A := 4E_1^{\mathbb{1}, \chi_4} \in M_1(4, \chi_4)$ satisfies the hypotheses of Lemma 3.2.*

Proof. The form A is well defined because χ_4 is odd. Moreover, the constant coefficient of A is equal to $-2B_{1, \chi_4} = -\frac{1}{2}(1\chi_4(1) + 3\chi_4(3)) = 1$. Therefore, the constant coefficient of A is equal to 1 and because $E_1^{\mathbb{1}, \chi_4}$ has integral coefficients away from the constant one, A and $\frac{1}{k_A}\theta A$ have \mathfrak{L} -integral coefficients. Moreover, we also get $A \equiv 1 \pmod{\mathfrak{L}}$ and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. Finally, it is straightforward that χ_4 is trivial modulo \mathfrak{L} , as is the cyclotomic character modulo 2. \square

The next favorable case is when N admits at least one odd prime divisor. The following result was inspired by [23, Appendix A]. As it has never been published, we prove it for the sake of completeness.

Proposition 3.7. *Assume $\ell = 2$ and N has an odd prime divisor. Let p be the least odd prime divisor of N , and let χ_N be a Dirichlet character modulo p of order 2^m , the greatest power of 2 dividing $p-1$. Let ζ be any 2^m th root of unity. The form $A := (\zeta - 1)E_1^{\mathbb{1}, \chi_N} \in M_1(p, \chi_N)$ satisfies the hypotheses of Lemma 3.2.*

Proof. Let g be an integer generating $(\mathbb{Z}/p\mathbb{Z})^\times$ and such that $\chi_N(g) = \zeta$. Because ζ is a root of unity of order 2^m , we have $\chi_N(-1) = \chi_N(g)^{\frac{p-1}{2}} = -1$. Therefore, χ_N is odd and A is well defined and its constant coefficient is equal to

$$\frac{1-\zeta}{2}B_{1, \chi_N} = \frac{1-\zeta}{2p} \sum_{a=1}^{p-1} a\chi_N(a).$$

For i between 0 and $2^{m-1} - 1$, we have $\chi_N(g^i) = \zeta^i$, and

$$\chi_N(-g^i) = -\zeta^i = \zeta^{i+2^{m-1}} = \chi_N(g^{i+2^{m-1}}).$$

Therefore, the set $\{\pm g^i, 0 \leq i \leq 2^{m-1} - 1\}$ is a set of representatives of $(\mathbb{Z}/p\mathbb{Z})^\times / \text{Ker}(\chi_N)$. For an integer x , we write $[x]$ for the only integer between 0 and $p-1$ that is congruent to x modulo p . We then have

$$\begin{aligned} \frac{1-\zeta}{2} B_{1,\chi_N} &= \frac{1-\zeta}{2p} \sum_{e \in \text{Ker}(\chi_N)} \sum_{i=0}^{2^{m-1}-1} ([eg^i]\chi_N(g^i) + [-eg^i]\chi_N(-g^i)) \\ &= \frac{1-\zeta}{2p} \sum_{i=0}^{2^{m-1}-1} \sum_{e \in \text{Ker}(\chi_N)} ([eg^i]\zeta^i - (p - [eg^i])\zeta^i) \\ &= \frac{1-\zeta}{2p} \sum_{i=0}^{2^{m-1}-1} \zeta^i \left(-p \cdot \#\text{Ker}(\chi_N) + 2 \sum_{e \in \text{Ker}(\chi_N)} [eg^i] \right) \\ &= -\frac{p-1}{2^m} + (1-\zeta) \left(\frac{1}{p} \sum_{i=0}^{2^{m-1}-1} \zeta^i \sum_{e \in \text{Ker}(\chi_N)} [eg^i] \right). \end{aligned}$$

The term inside the parentheses is \mathfrak{L} -integral and $\frac{p-1}{2^m}$ is odd. Moreover, the only prime ideal above 2 in the ring $\mathcal{O}_{\mathbb{Q}(\zeta)} = \mathbb{Z}[\zeta]$ is $(1-\zeta)\mathbb{Z}[\zeta]$. Therefore, we have $\frac{1-\zeta}{2} B_{1,\chi_N} \equiv 1 \pmod{\mathfrak{L}}$. Because the non-constant Fourier coefficients of E_1^{1,χ_N} are integral, A and $\frac{1}{k_A}\theta A$ have \mathfrak{L} -integral coefficients, and we get $A \equiv 1 \pmod{\mathfrak{L}}$ and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. Finally, from Lemma 2.7, because χ_N has order a power of 2, it is trivial modulo \mathfrak{L} as well as the cyclotomic character modulo 2. This finishes the proof. \square

We are left with the cases $N = 1$ and $N = 2$. There is no modular form of weight 1 of these levels, so we have to look at bigger weights in order to construct the form A . For level 2, we show that weight 2 suffices.

Proposition 3.8. *Assume that $\ell = 2$ and $N = 2$. Let $\mathbb{1}_{(2)}$ be the trivial character modulo 2. The modular form $A := 24E_2^{\mathbb{1},\mathbb{1}_{(2)}} \in M_2(2, \mathbb{1}_{(2)})$ satisfies the hypotheses of Lemma 3.2.*

Proof. The constant coefficient of A is equal to 1 and $E_2^{\mathbb{1},\mathbb{1}_{(2)}}$ has integral coefficients away from the constant one. Therefore, the forms A and $\frac{1}{k_A}\theta A$ have both \mathfrak{L} -integral Fourier coefficients, and we have $A \equiv 1 \pmod{\mathfrak{L}}$ and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. Finally, the character of A is trivial modulo \mathfrak{L} as well as the cyclotomic character modulo 2. \square

For $N = 1$, the weight needs to be at least 4, and we have the following result.

Proposition 3.9. *Assume $\ell = 2$ and $N = 1$. The form $A := 240E_4 \in M_4(1, \mathbb{1})$ satisfies the hypotheses of Lemma 3.2.*

Proof. The constant coefficient of A is equal to 1 and the non-constant Fourier coefficients of E_4 are integers. Therefore, A and $\frac{1}{k_A}\theta A$ have integer coefficients, and we have $A \equiv 1 \pmod{\mathfrak{L}}$, and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. The character of A is again trivial, as well as the cyclotomic character modulo 2. \square

3.1.3. Theta operators in characteristic 3

For N divisible by 3, the form of Proposition 3.5 is still appropriate.

Proposition 3.10. *Assume $\ell = 3$ and N is divisible by 3. Let χ_3 be the unique non-trivial Dirichlet character modulo 3. The form $A := 6E_1^{\mathbb{1}, \chi_3} \in M_1(3, \chi_3)$ satisfies the hypotheses of Lemma 3.2.*

Proof. We have $\chi_3 \equiv \overline{\chi}_\ell^{-1} \pmod{\mathfrak{L}}$ and the proof is exactly the same as the one of Proposition 3.5. \square

For the levels containing a prime divisor congruent to 2 modulo 3, we can still consider an Eisenstein series for the form A .

Proposition 3.11. *Assume $\ell = 3$ and N has a prime divisor congruent to 2 modulo 3. Let p be the least such prime divisor, and let $\mathbb{1}_{(p)}$ be the trivial Dirichlet character modulo p . The form $A := \frac{24}{p-1}E_2^{\mathbb{1}, \mathbb{1}_{(p)}} \in M_2(p, \mathbb{1}_{(p)})$ satisfies the hypotheses of Lemma 3.2.*

Proof. The constant coefficient of A is equal to 1. Moreover, $E_2^{\mathbb{1}, \mathbb{1}_{(p)}}$ has integral Fourier coefficients away from the constant one. Because, p is congruent to 2 modulo 3, $\frac{24}{p-1}$ is 0 modulo \mathfrak{L} . Therefore, A and $\frac{1}{k_A}\theta A$ have \mathfrak{L} -integral Fourier coefficients, and we have $A \equiv 1 \pmod{\mathfrak{L}}$ and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. Finally, the character of A is trivial, and we have $\overline{\chi}_3^{-2} = \mathbb{1}$. \square

The remaining cases are the levels containing only prime factors that are congruent to 1 modulo 3. For the levels divisible by a prime p congruent to 4 modulo 9 (that is if 3 divides $p-1$ only once), we found the following construction.

Proposition 3.12. *Assume $\ell = 3$ and N has a prime divisor congruent to 4 modulo 9. Let p be the least such prime divisor of N , and let χ^N be a Dirichlet character modulo p of order 3. The modular form $A := \frac{3}{p-1}(E_2^{\mathbb{1}, \chi^N} - E_2^{\chi^N, \mathbb{1}}) \in M_2(p, \chi^N)$ satisfies the hypotheses of Lemma 3.2.*

Proof. First notice that χ^N indeed exists as $(\mathbb{Z}/p\mathbb{Z})^\times$ is a cyclic group of order $p-1$ that is divisible by 3. Moreover, χ^N has order 3. Therefore, it is trivial modulo \mathfrak{L} and even, and the two Eisenstein series $E_2^{\mathbb{1}, \chi^N}$ and $E_2^{\chi^N, \mathbb{1}}$ exist.

The constant coefficient of A is equal to $\frac{3}{4(1-p)}B_{2,\chi^N}$ which is \mathfrak{L} -integral by Proposition 2.4. We have

$$\begin{aligned}\frac{3}{4(1-p)}B_{2,\chi^N} &= \frac{3}{4p(1-p)}\sum_{a=1}^{p-1}a^2\chi^N(a) \\ &\equiv \frac{3}{1-p}\sum_{a=1}^{p-1}a^2 \pmod{\mathfrak{L}} \\ &\equiv \frac{3}{1-p}\frac{p(p-1)(2p-1)}{6} \pmod{\mathfrak{L}} \\ &\equiv 1 \pmod{\mathfrak{L}}.\end{aligned}$$

Therefore, the constant coefficient of A is 1 modulo \mathfrak{L} , and because the non-constant Fourier coefficients of $E_2^{\mathbb{1},\chi^N}$ and $E_2^{\chi^N,\mathbb{1}}$ are integral, A and $\frac{1}{k_A}\theta A$ have \mathfrak{L} -integral coefficients. The weight k_A is invertible modulo 3, it consequently suffices to prove that $A \equiv 1 \pmod{\mathfrak{L}}$ to conclude.

The forms $E_2^{\mathbb{1},\chi^N}$ and $E_2^{\chi^N,\mathbb{1}}$ are both normalized eigenforms for all the Hecke operators at level p , and have the same weight and character. Thus, it is enough to prove that $a_r(E_2^{\mathbb{1},\chi^N}) \equiv a_r(E_2^{\chi^N,\mathbb{1}}) \pmod{\mathfrak{L}}$ for all prime numbers r . This last congruence is straightforward, because we have

$$a_r(E_2^{\mathbb{1},\chi^N}) = 1 + r\chi^N(r) \equiv \chi^N(r) + r = a_r(E_2^{\chi^N,\mathbb{1}}) \pmod{\mathfrak{L}}. \quad \square$$

It only remains the levels containing only primes congruent to 1 modulo 9. We found no general way to express the modular form A as form of weight 2. Using computations in PARI/GP, we look for a modular form of level $p \equiv 1 \pmod{9}$ satisfying the hypotheses of Lemma 3.2 for p up to 1000. We always find a form except for $p \in \{307, 379, 433, 487, 523, 613, 631, 757, 811, 829, 991\}$, i.e. we found 16 forms out of the 27 we were looking for. It can be proved that such a modular form cannot be expressed as a linear combination of forms in the Eisenstein space, meaning that one has necessarily to consider cusp forms to construct A . To fill this gap anyway, we can still consider the modular form $A := 240E_4$ as in the case of Proposition 3.9.

Proposition 3.13. *Assume $\ell = 3$, and N contains only prime factors congruent to 1 modulo 9. The modular form $A := 240E_4$ satisfies the hypotheses of Lemma 3.2.*

Proof. The constant coefficient of A is equal to 1 and the non-constant Fourier coefficients of E_4 are integral. Therefore, the forms A and $\frac{1}{k_A}\theta A$ have both \mathfrak{L} -integral Fourier coefficients, and we have $A \equiv 1 \pmod{\mathfrak{L}}$ and $\frac{1}{k_A}\theta A \equiv 0 \pmod{\mathfrak{L}}$. Finally, the character of A is trivial, and we have $\overline{\chi}_\ell^{k_A} = \overline{\chi}_\ell^{-4} \equiv \mathbb{1} \pmod{\mathfrak{L}}$. \square

We have compiled in Table 1 the definition of A depending on ℓ and N . When multiple definitions were possible, we have taken the one with the least weight

Table 1. Various modular forms A used to construct the operator $\tilde{\theta}$

$\ell \geq 5$	Form A	Proposition
$\ell \nmid N$	$-2\ell E_{\ell-1}$	3.4
$\ell \mid N$	$2\ell E_1^{\mathbb{1}, \chi_{\mathfrak{L}}^{-1}}$	3.5

$\ell = 2$	Form A	Proposition
$4 \mid N$	$4E_1^{\mathbb{1}, \chi_4}$	3.6
$N \geq 3$ and $4 \nmid N$	$(\zeta - 1)E_1^{\mathbb{1}, \chi_N}$	3.7
$N = 2$	$24E_2^{\mathbb{1}, \mathbb{1}^{(2)}}$	3.8
$N = 1$	$240E_4$	3.9

$\ell = 3$	Form A	Proposition
$\ell \mid N$	$6E_1^{\mathbb{1}, \chi_3}$	3.10
$\ell \nmid N$ and N has a prime factor $q \equiv 2 \pmod{3}$	$\frac{24}{p-1} E_2^{\mathbb{1}, \mathbb{1}_{(p)}}$	3.11
$\forall d \mid N, d \equiv 1 \pmod{3}$ and N has a prime factor $p \equiv 4 \pmod{9}$	$\frac{3}{p-1} (E_2^{\mathbb{1}, \chi^N} - E_2^{\chi^N, \mathbb{1}})$	3.12
$\forall p \mid N, p \equiv 1 \pmod{9}$	$240E_4$	3.13

among all the possible forms. The third column corresponds to the proposition where the properties of the form have been proved.

Looking at the various results above, we state the following definition that will be useful in the proofs of the next paragraph.

Definition 3.14. We say a pair (ℓ, N) is bad, if we have one of the following.

- $\ell = 2$ and $N = 1$;
- $\ell = 3$ and all the prime factors of N are congruent to 1 modulo 9.

Remark 3.15. When (ℓ, N) is bad, the modular form $-504E_6$ is also congruent to 1 modulo \mathfrak{L} . Its weight is greater than the one of Table 1, but we will have to use it in the proof of Proposition 3.17 in the next section.

3.2. Sturm bounds

A Sturm bound for a space of modular forms is an upper bound on the number of leading coefficients that characterize a form of this space. Equivalently, it is the maximal number of zero leading coefficients that a nonzero form of this space can have. The study of such bounds has first been made by Sturm [34] and was later

generalized among others by Murty [25]. The same kind of bounds exists if we look at modular forms modulo a prime ideal — and are in fact the same as the first one. In the next lemma, we give a slight improvement of Murty's result for modular forms of same weight. We then state a more general result for modular forms of any weight and level.

For all the subsection, we fix a prime number ℓ and a place \mathfrak{L} of $\overline{\mathbb{Q}}$ above ℓ .

Lemma 3.16. *Let f, g be two modular forms of same weight $k \geq 0$, level N_f, N_g and character $\varepsilon_f, \varepsilon_g$, respectively. Let N be the lcm of N_f and N_g . Assume that f and g have both \mathfrak{L} -integral Fourier coefficients and that $\varepsilon_f \equiv \varepsilon_g \pmod{\mathfrak{L}}$.*

If

$$a_n(f) \equiv a_n(g) \pmod{\mathfrak{L}}, \text{ for every integer } n \leq \frac{kN}{12} \prod_{\substack{p \text{ prime} \\ p|N}} \left(1 + \frac{1}{p}\right),$$

then $f \equiv g \pmod{\mathfrak{L}}$.

Proof. Let us write $B := \frac{kN}{12} \prod_{p|N} (1 + \frac{1}{p})$. We follow substantially the proof of Murty of [25, §4]. Consider $\phi = f - g$ and suppose that the vanishing order modulo \mathfrak{L} at infinity of ϕ is at least equal to B , that is $a_n(\phi) \equiv 0 \pmod{\mathfrak{L}}$ for all $n \leq B$. If $\phi = 0$, there is nothing to prove. Otherwise, as explained in [25, §4], for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ there is an element $A_\gamma \in \overline{\mathbb{Q}}^\times$ such that the modular form $A_\gamma \phi|_k \gamma$ has \mathfrak{L} -integral coefficients and is not congruent to 0 modulo \mathfrak{L} .

We write $m := [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} (1 + \frac{1}{p})$ and consider a system of representatives $(\gamma_i)_{1 \leq i \leq m}$ of right cosets of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. We can further assume $\gamma_1 = I_2$, the identity matrix. Also choose a set $(\tau_j)_{1 \leq j \leq \varphi(N)}$ of representatives of $\Gamma_1(N)$ in $\Gamma_0(N)$ with $\tau_1 = I_2$. We then have

$$\mathrm{SL}_2(\mathbb{Z}) = \bigcup_{i=1}^m \Gamma_0(N) \gamma_i = \bigcup_{i=1}^m \bigcup_{j=1}^{\varphi(N)} \Gamma_1(N) \tau_j \gamma_i.$$

Taking the norm function of ϕ according to this system of representatives, we define

$$F := \left(\prod_{j=1}^{\varphi(N)} \phi|_k \tau_j \right) \prod_{i=2}^m \prod_{j=1}^{\varphi(N)} A_{\tau_j \gamma_i} \phi|_k \tau_j \gamma_i \in M_{km\varphi(N)}(\mathrm{SL}_2(\mathbb{Z})).$$

For $i = 1$ and j between 1 and $\varphi(N)$, we have

$$\phi|_k \tau_j \gamma_1 = \phi|_k \tau_j = (\varepsilon_f(\tau_j)f - \varepsilon_g(\tau_j)g) \equiv \varepsilon_f(\tau_j)\phi \pmod{\mathfrak{L}}.$$

Therefore, the forms $\phi|_k \tau_j$ have \mathfrak{L} -integral Fourier coefficients, and thereby the form F too by the construction of the coefficients $A_{\tau_j \gamma_i}$. Moreover, by assumption the vanishing order at infinity of ϕ modulo \mathfrak{L} is at least equal to $\frac{km}{12}$. Therefore, the one of the modular form $\Phi := \prod_{j=1}^{\varphi(N)} \phi|_k \tau_j$ is at least equal to $\frac{km\varphi(N)}{12}$, and the same is true for F . Applying Sturm's theorem for level 1 modular forms [25, Theorem 5],

F must vanish modulo \mathfrak{L} and by construction of the coefficients $A_{\tau_j \gamma_i}$, the modular forms $A_{\tau_j \gamma_i} \phi|_k \tau_j \gamma_i$ are not trivial modulo \mathfrak{L} . Thus Φ and hence ϕ must be trivial modulo \mathfrak{L} . \square

The following proposition generalizes the previous lemma to modular forms of arbitrary weights and levels. The proof uses extensively the construction of theta operators given in Sec. 3.1. We warn the reader that we will write $0^0 = 1$.

Proposition 3.17. *Let f, g be two modular forms of weight $k_f, k_g \geq 0$, level $N_f, N_g \geq 1$ and character $\varepsilon_f, \varepsilon_g$, respectively. Let m_f, m_g be two non-negative integers. Assume that f and g have both \mathfrak{L} -integral Fourier coefficients and that $\overline{\chi}_\ell^{k_f+2m_f} \varepsilon_f \equiv \overline{\chi}_\ell^{k_g+2m_g} \varepsilon_g \pmod{\mathfrak{L}}$. Let N be the lcm of N_f and N_g , and define*

$$a = \begin{cases} 4 & \text{if } \begin{cases} k_f + 2m_f \equiv k_g + 2m_g + 2 \pmod{4} \\ \text{and } (\ell, N) \text{ is bad} \end{cases} \\ 0 & \text{otherwise} \end{cases}$$

$$b = \begin{cases} 4 & \text{if } \ell = 2 \text{ and } N = 2 \\ 3 & \text{if } \ell \mid N \text{ and } (\ell, N) \neq (2, 2) \\ 6 & \text{if } (\ell, N) \text{ is bad} \\ \ell + 1 & \text{otherwise} \end{cases} \quad \text{and} \quad k = a + \max(k_f + bm_f, k_g + bm_g),$$

where “bad” refers to Definition 3.14.

If

$$n^{m_f} a_n(f) \equiv n^{m_g} a_n(g) \pmod{\mathfrak{L}}, \text{ for every integer } n \leq \frac{Nk}{12} \prod_{\substack{p \text{ prime} \\ p \mid N}} \left(1 + \frac{1}{p}\right),$$

then this holds for all integers $n \geq 0$.

Proof. For the whole proof, we write A for the modular form associated with \mathfrak{L} and N constructed in Sec. 3.1. According to Table 1, it has weight $b - 2$ and level N . We write χ_A for the character of A and $B(N, k) := \frac{Nk}{12} \prod_{\substack{p \text{ prime} \\ p \mid N}} (1 + \frac{1}{p})$.

Assume without loss of generality that $k_f + bm_f \leq k_g + bm_g$. We first prove that, assuming $b - 2$ divides $k_g - k_f + b(m_g - m_f)$, we have $n^{m_f} a_n(f) \equiv n^{m_g} a_n(g) \pmod{\mathfrak{L}}$ for all non-negative integers n if these congruences hold for $n \leq B(N, k_g + bm_g)$. Applying Lemma 3.2 recursively, we have

$$\tilde{\theta}^{m_f} f \in M_{k_f + bm_f}(N, \varepsilon_f \chi_A^{m_f}) \quad \text{and} \quad \tilde{\theta}^{m_g} g \in M_{k_g + bm_g}(N, \varepsilon_g \chi_A^{m_g}).$$

We cannot apply Lemma 3.16 to $\tilde{\theta}^{m_f} f$ and $\tilde{\theta}^{m_g} g$ directly since they do not have the same weight. However, the functions $A^{\frac{k_g - k_f + b(m_g - m_f)}{b-2}} \tilde{\theta}^{m_f} f$ and $\tilde{\theta}^{m_g} g$ are well-defined modular forms by assumption. They have the same weight $k_g + bm_g$, the same level N and characters $\varepsilon_f \chi_A^{m_f + \frac{k_g - k_f + b(m_g - m_f)}{b-2}}$ and $\varepsilon_g \chi_A^{m_g}$, respectively.

Moreover, by Lemma 3.2 again, we have $\chi_A \equiv \overline{\chi}_\ell^{2-b} \pmod{\mathfrak{L}}$. By the assumption on the characters we get

$$\begin{aligned} \varepsilon_f \chi_A^{m_f + \frac{k_g - k_f + b(m_g - m_f)}{b-2}} &\equiv \varepsilon_f \overline{\chi}_\ell^{-(b-2)\left(m_f + \frac{k_g - k_f + b(m_g - m_f)}{b-2}\right)} \pmod{\mathfrak{L}} \\ &\equiv \overline{\chi}_\ell^{k_f + 2m_f} \varepsilon_f \cdot \overline{\chi}_\ell^{-(k_g + bm_g)} \pmod{\mathfrak{L}} \\ &\equiv \overline{\chi}_\ell^{k_g + 2m_g} \varepsilon_g \cdot \overline{\chi}_\ell^{-(k_g + bm_g)} \equiv \varepsilon_g \chi_A^{m_g} \pmod{\mathfrak{L}}. \end{aligned}$$

Therefore, the assumptions of Lemma 3.16 are satisfied for these two modular forms. Since A reduces to 1 modulo \mathfrak{L} , we get that if the coefficients of $\tilde{\theta}^{m_f} f$ and $\tilde{\theta}^{m_g} g$ are congruent up to the $B(N, k_g + bm_g)$ th one, then $\tilde{\theta}^{m_f} f$ and $\tilde{\theta}^{m_g} g$ are congruent modulo \mathfrak{L} by Lemma 3.16.

We now look at the hypothesis $b - 2 \mid k_g - k_f + b(m_g - m_f)$. We claim that if (ℓ, N) is not bad, then it is always satisfied. We have three cases: (i) $\ell = N = 2$, (ii) $\ell \mid N$ and $(\ell, N) \neq (2, 2)$, (iii) $\ell \nmid N$ and (ℓ, N) is not bad.

- (i) If $\ell = N = 2$, then $b - 2 = 2$, and $k_f \equiv k_g \equiv 0 \pmod{2}$, because the weight of a modular form of level 2 is necessarily even. Thus, $k_g - k_f + 4(m_g - m_f)$ is divisible by $b - 2$.
- (ii) If $\ell \mid N$, then $b - 2 = 1$ and there is nothing to prove.
- (iii) If $\ell \nmid N$ and (ℓ, N) is not bad, we have $b - 2 = \ell - 1$. Because $\ell \nmid N$, ε_f and ε_g are unramified at ℓ . From the assumption $\overline{\chi}_\ell^{k_f + 2m_f} \varepsilon_f \equiv \overline{\chi}_\ell^{k_g + 2m_g} \varepsilon_g \pmod{\mathfrak{L}}$, we get that $k_g - k_f + 2(m_g - m_f) \equiv 0 \pmod{\ell - 1}$, hence $b - 2 \mid k_g - k_f + b(m_g - m_f)$.

Therefore, when (ℓ, N) is not bad, the proposition is proved because we have $a = 0$ and $k = k_g + bm_g$.

From now on, assume that (ℓ, N) is bad. By definition, we have $b = 6$, and either $(\ell, N) = (2, 1)$, or $\ell = 3$ and $\ell \nmid N$. Let us first prove that we have $k_g - k_f + 6(m_g - m_f) \equiv 0 \pmod{2}$ (i.e. $k_g \equiv k_f \pmod{2}$). When $(\ell, N) = (2, 1)$, it is true because the weights k_f and k_g are both even. When $\ell = 3$ and $\ell \nmid N$, the hypothesis on the characters again implies that $k_f + 2m_f \equiv k_g + 2m_g \pmod{2}$ and the conclusion follows.

If the even number $k_g - k_f + 6(m_g - m_f)$ is divisible by $4 = b - 2$, then by definition we have $a = 0$ and $k = k_g + bm_g$. The result follows as before in this case. Otherwise, we have $4 \mid k_g - k_f + 6(m_g - m_f) - 2$ and $a = 4$. Write $A_4 := 240E_4$ and $A_6 := -504E_6$. We have seen in Proposition 3.13 and Remark 3.15, that both A_4 and A_6 are congruent to 1 modulo \mathfrak{L} . We set

$$f' := A_6 f \quad \text{and} \quad g' = A_4 g.$$

Then f' and g' are modular forms with \mathfrak{L} -integral Fourier coefficients of weight $k_{f'} = k_f + 6$, $k_{g'} = k_g + 4$, level N and character $\varepsilon_f, \varepsilon_g$, respectively. Since $\overline{\chi}_\ell^2$ is trivial for $\ell = 2, 3$, the congruence

$$\overline{\chi}_\ell^{k_{f'} + bm_{f'}} \varepsilon_f \equiv \overline{\chi}_\ell^{k_{g'} + bm_{g'}} \varepsilon_g \pmod{\mathfrak{L}}$$

is satisfied. Moreover, we have $k_{f'} + bm_f \leq k_{g'} + bm_g$, and $b - 2 = 4$ divides $k_{g'} - k_{f'} + b(m_g - m_f)$. According to the discussion at the beginning of the proof, we therefore get the desired result since f', g' reduce to f, g , respectively and $k_{g'} + bm_g = a + k_g + bm_g = k$. \square

Remark 3.18. Notice that Lemma 3.16 corresponds to the special case $m_f = m_g = 0$ and $k_f = k_g = k$. Moreover, in practice we can always take $m_f \in \{0, 1\}$ and $0 \leq m_g \leq \ell - 1$.

In Sec. 4, we will mainly deal with eigenforms. It is well known that the knowledge of the Fourier coefficients of prime index and of the constant coefficient characterizes such forms. We can therefore simplify Proposition 3.17 and get the following corollary.

Corollary 3.19. *Let f, g be as in Proposition 3.17 and define also N and k similarly. Assume further that f and g are normalized eigenforms for the Hecke operators at level N modulo \mathfrak{L} of prime index less than $\frac{Nk}{12} \prod_{p|N} \text{prime}(1 + \frac{1}{p})$ (and different from ℓ if $m_f, m_g \geq 1$).*

If $0^{m_f} a_0(f) \equiv 0^{m_g} a_0(g) \pmod{\mathfrak{L}}$ (with $0^0 = 1$) and if for every prime number $p \leq \frac{Nk}{12} \prod_{p|N} \text{prime}(1 + \frac{1}{p})$ we have $p^{m_f} a_p(f) \equiv p^{m_g} a_p(g) \pmod{\mathfrak{L}}$, then we have $n^{m_f} a_n(f) \equiv n^{m_g} a_n(g) \pmod{\mathfrak{L}}$ for every non-negative integer n .

We finally state a Sturm bound result in characteristic zero that we will be used in the proof of Theorem 5.10. It is a well-known result, but we do not find a suitable reference for it. For the sake of completeness, we give a proof of it essentially due to Buzzard.

Proposition 3.20. *Let f, g be two modular forms of same weight $k \geq 0$, level N and character ε . If $a_n(f) = a_n(g)$ for every integer $n \leq \frac{kN}{12} \prod_{p|N} \text{prime}(1 + \frac{1}{p})$, then $f = g$.*

Proof. We reduce to the case of trivial character. Let s be the order of the character ε , and define

$$\phi := (f - g)^s \in M_{ks}(N, \mathbb{1}).$$

By assumption, the first $s \cdot \frac{kN}{12} \prod_{p|N} \text{prime}(1 + \frac{1}{p})$ Fourier coefficients of ϕ vanish. Applying [25, Theorem 1], we get $\phi = 0$ and therefore $f = g$. \square

Remark 3.21. We can in fact deduce Proposition 3.20 from Lemma 3.16. Indeed, it is well known that the denominators of the Fourier coefficients of a modular form are bounded. Therefore, we can reduce f and g modulo infinitely many places \mathfrak{L} . Applying Lemma 3.16, f and g are congruent modulo infinitely many places \mathfrak{L} and are thus equal.

We now give an upper-bound for the product appearing in the Sturm bound. We use a technique of Kraus [17] to get a slightly better bound than the one suggested by Serre in Kraus' paper.

Lemma 3.22. *Let n be an integer greater than or equal to 2, we have*

$$\prod_{\substack{p \text{ prime} \\ p|n}} \left(1 + \frac{1}{p}\right) \leq 2 \log \log(n) + 2.4.$$

Proof. We first split the product in two parts: $\prod_{\substack{p \text{ prime} \\ p|n}} (1 + \frac{1}{p}) = P(n)Q(n)$ with

$$P(n) = \prod_{\substack{p > \log n \\ p|n}} \left(1 + \frac{1}{p}\right) \quad \text{and} \quad Q(n) = \prod_{\substack{p \leq \log n \\ p|n}} \left(1 + \frac{1}{p}\right).$$

Let m be the number of primes p dividing n and being greater than $\log n$. As $n \geq \log(n)^m$, we get $m \leq \frac{\log n}{\log \log n}$. Thus,

$$P(n) \leq \exp\left(\frac{\log n}{\log \log n} \log\left(1 + \frac{1}{\log n}\right)\right) \leq \exp\left(\frac{1}{\log \log n}\right). \quad (3.1)$$

Applying [31, (3.27)], we get an upper bound for Q :

$$Q(n) \leq \prod_{p \leq \log n} \left(1 - \frac{1}{p}\right)^{-1} < e^\gamma \log \log(n) \left(1 - \frac{1}{(\log \log n)^2}\right)^{-1}, \quad (3.2)$$

where γ is the Euler–Mascheroni constant.

Putting (3.1) and (3.2) together, we have

$$\prod_{\substack{p \text{ prime} \\ p|n}} \left(1 + \frac{1}{p}\right) \leq e^\gamma \log \log(n) \exp\left(\frac{1}{\log \log n}\right) \left(1 - \frac{1}{(\log \log n)^2}\right)^{-1}.$$

The function $x \mapsto e^{\gamma+x}(1-x^2)^{-1}$ is bounded by 2 for $x \in [0, 0.1]$. Therefore, the lemma holds for all integers $n \geq \exp(\exp(10))$. For n between 2 and $\exp \exp(10)$, we first notice that we only have to deal with square-free integers. Then, among the square-free integers having k prime factors, it suffices to only check the lemma for $n_k = \prod_{i=1}^k p_i$, p_i being the i th prime number. The greatest k such that $n_k \leq \exp \exp(10)$ is 2486, and we have checked the lemma with a computer for all those n_k . \square

3.3. Modifying modular forms

In this section, we discuss a way to construct from a given eigenform, another eigenform with slightly different Fourier coefficients but with a bigger level. It will be crucial in Sec. 4.

Let $\mathcal{O}(\mathcal{H})$ be the space of holomorphic functions on the complex upper-half plane. For an integer $n \geq 1$ and a complex number b , we define two operators V_n and $S_n(b)$ on $\mathcal{O}(\mathcal{H})$ by

$$V_n : \begin{cases} \mathcal{O}(\mathcal{H}) \rightarrow \mathcal{O}(\mathcal{H}) \\ h \mapsto (z \mapsto h(nz)) \end{cases} \quad \text{and} \quad S_n(b) : \begin{cases} \mathcal{O}(\mathcal{H}) \rightarrow \mathcal{O}(\mathcal{H}) \\ h \mapsto h - bV_nh. \end{cases}$$

For a prime number p , we denote by U_p the operator which action on Fourier expansions is given by

$$U_p \left(\sum_{n=0}^{\infty} a_n q^n \right) := \sum_{n=0}^{\infty} a_{np} q^n.$$

We recall the following facts about the operators U_p and V_p : for any primes p and r , the operators V_p and V_r commute and the image of $M_k(M, \varepsilon)$ by V_p is $M_k(Mp, \varepsilon)$. Letting V_p act on q -expansions, it commutes with U_r for $r \neq p$ and satisfies $U_p V_p = \text{Id}$. Moreover, T_p^M decomposes on the space $M_k(M, \varepsilon)$ as

$$T_p^M = U_p + p^{k-1} \varepsilon(p) V_p.$$

From now on, consider a modular form g of weight $k \geq 1$, level $M \geq 1$ and character ε that is a normalized eigenform for all the Hecke operators at level M . For any prime number p , we denote by α_p, β_p the roots of the Hecke polynomial $X^2 - a_p(g)X + p^{k-1} \varepsilon(p)$.

Lemma 3.23. *Let p be a prime number and let $b \in \{\alpha_p, \beta_p\}$. The function $S_p(b)g$ is a modular form of same weight and character as g and of level Mp^{n_p} with*

$$n_p = \begin{cases} 1 & \text{if } b \neq 0, \\ 0 & \text{if } b = 0. \end{cases}$$

It is a normalized eigenform for all the Hecke operators at level Mp^{n_p} , and for any prime r , we have

$$a_r(S_p(b)g) = \begin{cases} a_r(g) & \text{if } r \neq p, \\ a_p(g) - b & \text{if } r = p. \end{cases}$$

Moreover, if g has Fourier coefficients in a ring R , then those of $S_p(b)g$ lie in the ring $R(b)$.

Proof. If $b = 0$, then there is nothing to prove as $S_p(0)g = g$. Assume $b \neq 0$. Because both g and $V_p g$ are modular forms of weight k , level Mp and character ε , it is also the case for $S_p(b)g$. Let us compute the action of the Hecke operators at level Mp on $S_p(b)g$.

Let r be a prime number different from p . The operator T_r^{Mp} has the same action as T_r^M . Thus, because the operators V_p and T_r^M commute, we have

$$T_r^{Mp} S_p(b)g = T_r^M g - bV_p T_r^M g = a_r(g)g - ba_r(g)V_p g = a_r(g)S_p(b)g.$$

For $r = p$, we have $T_p^{Mp}g = U_pg = T_p^Mg - p^{k-1}\varepsilon(p)V_pg = a_p(g)g - p^{k-1}\varepsilon(p)V_pg$. It gives

$$T_p^{Mp}S_p(b)g = (a_p(g)g - p^{k-1}\varepsilon(p)V_pg) - bU_pV_pg = (a_p(g) - b)g - p^{k-1}\varepsilon(p)V_pg.$$

As b is a root of $X^2 - a_p(g)X + p^{k-1}\varepsilon(p)$, it satisfies $b(a_p(g) - b) = p^{k-1}\varepsilon(p)$. We finally get

$$T_p^{Mp}S_p(b)g = (a_p(g) - b)g - (a_p(g) - b)bV_pg = (a_p(g) - b)S_p(b)g.$$

The form $S_p(b)g$ is thus a normalized eigenform for the all Hecke operators at level Mp . The fact about the ring of Fourier coefficients of $S_p(b)g$ is straightforward. \square

We now apply this result to construct from the eigenform g , an eigenform which p th Fourier coefficient is a chosen number b in $\{\alpha_p, \beta_p, 0\}$.

Proposition 3.24. *Let p be a prime number and let $b \in \{\alpha_p, \beta_p, 0\}$. Define*

$$\begin{cases} g_p^b = g \text{ and } n_p = 0, & \text{if } b = a_p(g), \\ g_p^b = S_p(a_p(g) - b)g \text{ and } n_p = 1, & \text{if } b \neq a_p(g) \text{ and } b \in \{\alpha_p, \beta_p\}, \\ g_p^b = S_p(\alpha_p) \circ S_p(\beta_p)g \text{ and } n_p = 2, & \text{if } b \neq a_p(g) \text{ and } b \notin \{\alpha_p, \beta_p\}. \end{cases}$$

Then, g_p^b is a modular form of same weight and character as g and of level Mp^{n_p} . It is a normalized eigenform for all the Hecke operators at level Mp^{n_p} , and for any prime r we have

$$a_r(g_p^b) = \begin{cases} a_r(g) & \text{if } r \neq p, \\ b & \text{if } r = p. \end{cases}$$

Moreover, if g has Fourier coefficients in a ring R , then those of g_p^b lie in the ring $R(b)$.

Proof. In the first two cases, we have $g_p^b = S_p(a_p(g) - b)g$. Lemma 3.23 gives directly the result. In the third case, we necessarily have $b = 0$ and α_p, β_p non-zero. From Lemma 3.23 apply to g and β_p , the p th Hecke polynomial of $S_p(\beta_p)g$ is $X^2 - \alpha_p X$, which α_p is a root. We can then apply Lemma 3.23 to $S_p(\beta_p)g$ and α_p to conclude. Finally, the calculation

$$\begin{aligned} S_p(\alpha_p) \circ S_p(\beta_p)g &= (g - \beta_p V_pg) - \alpha_p V_p(g - \beta_p V_pg) \\ &= g - (\alpha_p + \beta_p)V_pg + \alpha_p \beta_p V_p^2 g \\ &= g - a_p(g)V_pg + p^{k-1}\varepsilon(p)V_p^2 g, \end{aligned}$$

proves that the Fourier coefficients of g_p^b lie in the same ring as g , because the values of the character of an eigenform always lie in the ring of coefficients of it (see [28, Corollary (3.1)]). \square

Remark 3.25. Notice that the modular form g_p^b is always of the shape $P(V_p)g$ with $P = 1 - \varepsilon_p X + \delta_p X^2$ and $(\varepsilon_p, \delta_p) \in \{(\alpha_p, 0), (\beta_p, 0), (a_p(g), p^{k-1}\varepsilon(p))\}$.

For any prime number p and $b_p \in \{0, \alpha_p, \beta_p\}$, define

$$S_p^{b_p} = \begin{cases} \text{Id} & \text{if } b_p = a_p(g), \\ \text{Id} - (a_p(g) - b_p)V_p & \text{if } b_p \neq a_p(g) \text{ and } b_p \in \{\alpha_p, \beta_p\}, \\ \text{Id} - a_p(g)V_p + p^{k-1}\varepsilon(p)V_p^2 & \text{if } b_p \neq a_p(g) \text{ and } b_p \notin \{\alpha_p, \beta_p\}, \end{cases}$$

so that we have $g_p^{b_p} = S_p^{b_p}g$. By Proposition 3.24, applying $S_p^{b_p}$ to g only modifies the Fourier coefficients of index divisible by p . Moreover, it gives us a modular form that is still a normalized eigenform for the whole Hecke algebra at its level. It means that for another prime r and $b_r \in \{0, \alpha_r, \beta_r\}$, the modular forms $(g_p^{b_p})_r^{b_r}$ and $(g_r^{b_r})_p^{b_p}$ are well defined and equal to $S_p^{b_p}S_r^{b_r}g = S_r^{b_r}S_p^{b_p}g$.

For any finite set of primes \mathbf{P} and any $\mathbf{b} \in \prod_{p \in \mathbf{P}} \{0, \alpha_p, \beta_p\}$, we define

$$g_{\mathbf{P}}^{\mathbf{b}} := \prod_{p \in \mathbf{P}} S_p^{b_p}g.$$

With the notations of Proposition 3.24, we deduce the following result.

Corollary 3.26. *The function $g_{\mathbf{P}}^{\mathbf{b}}$ is a modular form of same weight and character as g and of level $M \prod_{p \in \mathbf{P}} p^{n_p}$. It is a normalized eigenform for all the Hecke operators at level $M \prod_{p \in \mathbf{P}} p^{n_p}$, and for any prime r we have*

$$a_r(g_{\mathbf{P}}^{\mathbf{b}}) = \begin{cases} a_r(g) & \text{if } r \notin \mathbf{P}, \\ b_r & \text{if } r \in \mathbf{P}. \end{cases}$$

Moreover, if g has Fourier coefficients in a ring R , then those of $g_{\mathbf{P}}^{\mathbf{b}}$ lie in the ring $R(\mathbf{b})$.

Since the beginning of this section, our results were about “true” modular forms. There is another function that we can modify with the operator $S_p(b)$ and get a modular form: the Eisenstein series E_2 .

Proposition 3.27. *Let p be any prime number and $b \in \{1, 0\}$. Define*

$$\begin{cases} (E_2)_p^b = S_p(p)E_2 \text{ and } n_p = 1 & \text{if } b = 1, \\ (E_2)_p^b = S_p(1) \circ S_p(p)E_2 \text{ and } n_p = 2 & \text{if } b = 0. \end{cases}$$

The function $(E_2)_p^b$ is a modular form of weight 2, level p^{n_p} , and trivial character. It is a normalized eigenform for all the Hecke operators at level p^{n_p} , and for any prime r we have

$$a_r((E_2)_p^b) = \begin{cases} r + 1 & \text{if } r \neq p, \\ b & \text{if } r = p. \end{cases}$$

Moreover, all the Fourier coefficients of $(E_2)_p^b$ are integers, except maybe the constant one that is rational.

Proof. An easy computation shows that for any prime p , we have $S_p(p)E_2 = E_2^{\mathbf{1}, \mathbf{1}_{(p)}}$. In particular, the form $S_p(p)E_2 = S_p(a_p(E_2) - 1)E_2$ is a normalized eigenform of weight 2, level p , trivial character, and for any prime r , its r th Fourier coefficient is equal to $r + 1 = a_r(E_2)$ if $r \neq p$, and 1 if $r = p$. Moreover, the Hecke polynomial at p of $E_2^{\mathbf{1}, \mathbf{1}_{(p)}}$ is $X(X - 1)$. Thus, $S_p(1)E_2^{\mathbf{1}, \mathbf{1}_{(p)}} = S_p(1) \circ S_p(p)E_2$ is a normalized eigenform of weight 2, trivial character and level p^2 and we have $a_p(S_p(1) \circ S_p(p)E_2) = 0$. \square

We can then state a result of the shape of Corollary 3.26 for E_2 .

Corollary 3.28. *Let \mathbf{P} be a finite set of primes and let $\mathbf{b} \in \prod_{p \in \mathbf{P}} \{0, 1, p\} \setminus \{(p)_{p \in \mathbf{P}}\}$. There is a modular form $(E_2)_{\mathbf{P}}^{\mathbf{b}}$ of weight 2, level $\prod_{p \in \mathbf{P}} p^{n_p}$, and trivial character. It is a normalized eigenform for all the Hecke operators at its level, and for any prime number r we have*

$$a_r((E_2)_{\mathbf{P}}^{\mathbf{b}}) = \begin{cases} r + 1 & \text{if } r \notin \mathbf{P}, \\ b_r & \text{if } r \in \mathbf{P}. \end{cases}$$

Moreover, all the Fourier coefficients of $(E_2)_{\mathbf{P}}^{\mathbf{b}}$ are integers, except maybe the constant one that is rational.

We finally give a result on the constant coefficient of an Eisenstein series that has been modified with Corollary 3.26.

Proposition 3.29. *Let $k \geq 2$, let $\varepsilon_1, \varepsilon_2$ be two primitive Dirichlet characters. Let \mathbf{P} be a finite set of prime numbers and let $\mathbf{b} := (b_p) \in \prod_{p \in \mathbf{P}} \{0, \varepsilon_1(p), p^{k-1}\varepsilon_2(p)\}$, different from $(p)_{p \in \mathbf{P}}$ if $(k, \varepsilon_1, \varepsilon_2) = (2, \mathbf{1}, \mathbf{1})$. Then the constant coefficient of $(E_k^{\varepsilon_1, \varepsilon_2})_{\mathbf{P}}^{\mathbf{b}}$ is equal to*

$$\begin{cases} 0 & \text{if } \varepsilon_1 \neq \mathbf{1}, \\ -\frac{B_{k, \varepsilon_2}}{2k} \prod_{p \in \mathbf{P}} b_p (b_p - p^{k-1}\varepsilon_2(p)) & \text{if } \varepsilon_1 = \mathbf{1}. \end{cases}$$

Proof. First, if $\varepsilon_1 \neq \mathbf{1}$, then the constant coefficient of $E_k^{\varepsilon_1, \varepsilon_2}$ is trivial by (2.1). Assume $\varepsilon_1 = \mathbf{1}$. Then the modular form $(E_k^{\varepsilon_1, \varepsilon_2})_{\mathbf{P}}^{\mathbf{b}}$ is equal to

$$\prod_{p \in \mathbf{P}} (\text{Id} - \varepsilon_p V_p + \delta_p V_p^2) E_k^{\varepsilon_1, \varepsilon_2},$$

where

$$(\varepsilon_p, \delta_p) = \begin{cases} (1 + p^{k-1}\varepsilon_2(p), p^{k-1}\varepsilon_2(p)) & \text{if } b_p = 0, \\ (1, 0) & \text{if } b_p = p^{k-1}\varepsilon_2(p), \\ (p^{k-1}\varepsilon_2(p), 0) & \text{if } b_p = 1. \end{cases} \quad (3.3)$$

Therefore, the constant coefficient is equal to $-\frac{B_{k, \varepsilon_2}}{2k} \prod_{p \in \mathbf{P}} (1 - \varepsilon_p + \delta_p)$. A straightforward computation gives that $1 - \varepsilon_p + \delta_p$ is equal to 0 if $b_p \in \{0, p^{k-1}\varepsilon_2(p)\}$, and

to $1 - p^{k-1}\varepsilon_2(p)$ if $b_p = 1$. Therefore, if one of the b_p 's is equal to 0 or $p^{k-1}\varepsilon_2(p)$, then the constant coefficient is equal to

$$0 = -\frac{B_{k,\varepsilon_2}}{2k} \prod_{p \in \mathbf{P}} b_p(b_p - p^{k-1}\varepsilon_2(p)).$$

Else, if all the b_p 's are equal to 1, then the constant coefficient is equal to

$$-\frac{B_{k,\varepsilon_2}}{2k} \prod_{p \in \mathbf{P}} (1 - p^{k-1}\varepsilon_2(p)) = -\frac{B_{k,\varepsilon_2}}{2k} \prod_{p \in \mathbf{P}} b_p(b_p - p^{k-1}\varepsilon_2(p)). \quad \square$$

Proposition 3.30. *Let $k, \varepsilon_1, \varepsilon_2, \mathbf{P}$ and \mathbf{b} be as in Proposition 3.29. Let $\mathbf{c}_1, \mathbf{c}_2$ be the conductors of ε_1 and ε_2 , respectively. Then the constant coefficient of $(E_k^{\varepsilon_1, \varepsilon_2})_{\mathbf{P}}^{\mathbf{b}}$ at the cusp $\frac{1}{\mathbf{c}_2}$ is equal to*

$$\begin{aligned} & -\varepsilon_1(-1) \frac{W((\varepsilon_1 \varepsilon_2^{-1})_0)}{W(\varepsilon_2^{-1})} \frac{B_{k, (\varepsilon_1^{-1} \varepsilon_2)_0}}{2k} \left(\frac{\mathbf{c}_2}{\mathbf{c}_0} \right)^k \prod_{p | \mathbf{c}_1 \mathbf{c}_2} \left(1 - \frac{(\varepsilon_1 \varepsilon_2^{-1})_0(p)}{p^k} \right) \\ & \times \prod_{b_p \neq \varepsilon_1(p)} \left(1 - \frac{\varepsilon_1 \varepsilon_2^{-1}(p)}{p^k} \right) \prod_{b_p \neq p^{k-1} \varepsilon_2(p)} \left(1 - \frac{1}{p} \right). \end{aligned}$$

Proof. Let $\gamma := \begin{pmatrix} 1 & 0 \\ \mathbf{c}_2 & 1 \end{pmatrix}$ be an element of $\mathrm{SL}_2(\mathbb{Z})$ such that $\gamma\infty = \frac{1}{\mathbf{c}_2}$. Write the modular form $(E_k^{\varepsilon_1, \varepsilon_2})_{\mathbf{P}}^{\mathbf{b}}$ as

$$\prod_{p \in \mathbf{P}} (\mathrm{Id} - \varepsilon_p V_p + \delta_p V_p^2) E_k^{\varepsilon_1, \varepsilon_2},$$

with ε_p and δ_p defined by (3.3). By Proposition 2.9, for an integer M , the constant coefficient of $(V_M E_k^{\varepsilon_1, \varepsilon_2})|_k \gamma$ is nonzero if and only if M and \mathbf{c}_2 are coprime. Under this assumption, we have, with the notations of Proposition 2.9,

$$\begin{aligned} \Upsilon_k^{\varepsilon_1, \varepsilon_2}(\gamma, M) &= \frac{\varepsilon_2^{-1}(M)}{M^k} \left[-\varepsilon_1(-1) \frac{W((\varepsilon_1 \varepsilon_2^{-1})_0)}{W(\varepsilon_2^{-1})} \frac{B_{k, (\varepsilon_1^{-1} \varepsilon_2)_0}}{2k} \right. \\ & \quad \left. \times \left(\frac{\mathbf{c}_2}{\mathbf{c}_0} \right)^k \prod_{p | \mathbf{c}_1 \mathbf{c}_2} \left(1 - \frac{(\varepsilon_1 \varepsilon_2^{-1})_0(p)}{p^k} \right) \right]. \end{aligned} \quad (3.4)$$

The expression in brackets is independent of M , let write it \mathbf{D} . Notice that if M is not coprime to \mathbf{c}_2 , the formula still holds, as $\varepsilon_2(M) = 0$. Define

$$P := \prod_{p \in \mathbf{P}} (1 - \varepsilon_p X_p + \delta_p X_p^2) \in \mathbb{C}[(X_p)_{p \in \mathbf{P}}].$$

As (3.4) is fully multiplicative in M , the constant coefficient of $(E_k^{\varepsilon_1, \varepsilon_2})_{\mathbf{P}}^{\mathbf{b}}$ is then equal to

$$\lim_{\mathrm{Im}(z) \rightarrow +\infty} P((V_p)_{p \in \mathbf{P}}) E_k^{\varepsilon_1, \varepsilon_2}|_k \gamma(z) = \mathbf{D} \cdot P \left(\left(\frac{\varepsilon_2^{-1}(p)}{p^k} \right)_{p \in \mathbf{P}} \right).$$

We just have to compute the value of $P((\frac{\varepsilon_2^{-1}(p)}{p^k})_{p \in \mathbf{P}})$ to conclude. Let $P_p(X_p) = 1 - \varepsilon_p X_p + \delta_p X_p^2$, so that we have $P = \prod_{p \in \mathbf{P}} P_p(X_p)$. A straightforward calculation shows that the value of $P_p(\frac{\varepsilon_2^{-1}(p)}{p^k})$ is

$$\begin{cases} \left(1 - \frac{\varepsilon_1 \varepsilon_2^{-1}(p)}{p^k}\right) \left(1 - \frac{1}{p}\right) & \text{if } (\varepsilon_p, \delta_p) = (\varepsilon_1(p) + p^{k-1} \varepsilon_2(p), p^{k-1} \varepsilon_1 \varepsilon_2(p)); \\ 1 - \frac{\varepsilon_1 \varepsilon_2^{-1}(p)}{p^k} & \text{if } (\varepsilon_p, \delta_p) = (\varepsilon_1(p), 0); \\ 1 - \frac{1}{p} & \text{if } (\varepsilon_p, \delta_p) = (p^{k-1} \varepsilon_2(p), 0). \end{cases} \quad \square$$

4. Reducible Galois Representations

4.1. Reducible Galois representations and Eisenstein series

Before dealing with the reducibility of a residual representation attached to a newform, we examine the general case of a reducible, residual, semi-simple, odd Galois representation. We begin by a definition that will be enlightened in the following proposition. Throughout this section, we fix a prime number ℓ and a place \mathfrak{L} of $\overline{\mathbb{Q}}$ above ℓ .

Definition 4.1. Define $R(\ell)$ as the set of quadruplets $(\varepsilon_1, \varepsilon_2, m_1, m_2)$ consisting of two primitive Dirichlet characters ε_1 and ε_2 that are of prime-to- ℓ order and unramified at ℓ , and of two integers m_1, m_2 such that $0 \leq m_1 \leq m_2 < \ell - 1$, and $\varepsilon_1 \varepsilon_2(-1) \equiv (-1)^{m_1+m_2+1} \pmod{\ell}$.

Proposition 4.2. Let $\bar{\rho} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_{\ell})$ be a semi-simple, odd representation. Then, $\bar{\rho}$ is reducible if and only if there exists $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R(\ell)$ such that $\bar{\rho} \cong \overline{\chi}_{\ell}^{m_1} \overline{\varepsilon}_1 \oplus \overline{\chi}_{\ell}^{m_2} \overline{\varepsilon}_2$, where $\overline{\varepsilon}_1$ and $\overline{\varepsilon}_2$ correspond to the reduction modulo \mathfrak{L} of ε_1 and ε_2 , respectively.

Proof. If $\bar{\rho}$ is reducible, then we can decompose it as $\varphi_1 \overline{\chi}_{\ell}^{m_1} \oplus \varphi_2 \overline{\chi}_{\ell}^{m_2}$, with φ_1, φ_2 two characters modulo \mathfrak{L} unramified at ℓ , and $0 \leq m_1 \leq m_2 < \ell - 1$. Let ε_i be the Teichmüller lift of φ_i with respect to \mathfrak{L} (see Sec. 2.2). By construction, the characters $\varepsilon_1, \varepsilon_2$ are primitive and have prime-to- ℓ order. Finally, if c is a complex conjugation, then we have

$$-1 = \det(\bar{\rho}(c)) = \overline{\varepsilon}_1 \overline{\varepsilon}_2(-1) \overline{\chi}_{\ell}(c)^{m_1+m_2} = (-1)^{m_1+m_2} \overline{\varepsilon}_1 \overline{\varepsilon}_2(-1).$$

Therefore, we have $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R(\ell)$. □

Our goal is now to construct from an element $(\varepsilon_1, \varepsilon_2, m_1, m_2)$ of $R(\ell)$, various modular forms that correspond to the representation $\overline{\chi}_{\ell}^{m_1} \overline{\varepsilon}_1 \oplus \overline{\chi}_{\ell}^{m_2} \overline{\varepsilon}_2$. By this we

mean, in the spirit of [11, Théorème 6.7], modular forms $g \in M_{k_g}(N_g, \varepsilon_g)$ such that

- g has \mathfrak{L} -integral Fourier coefficients;
- g is a normalized eigenform for the Hecke operators $T_p^{N_g}$ modulo \mathfrak{L} of prime index p not dividing ℓN_g ;
- $\det(\overline{\chi_\ell^{m_1} \varepsilon_1} \oplus \overline{\chi_\ell^{m_2} \varepsilon_2}) = \overline{\chi_\ell^{m_1+m_2} \varepsilon_1 \varepsilon_2} = \overline{\chi_\ell^{k_g-1} \varepsilon_g}$;
- $\mathrm{Tr}((\overline{\chi_\ell^{m_1} \varepsilon_1} \oplus \overline{\chi_\ell^{m_2} \varepsilon_2})(\mathrm{Frob}_p)) = p^{m_1} \overline{\varepsilon_1}(p) + p^{m_2} \overline{\varepsilon_2}(p) = \overline{a_p(g)}$, for all primes p not dividing ℓN_g .

The motivation to seek such forms comes from the fact that if $f \in S_k^{\mathrm{new}}(N, \varepsilon)$ is a newform such that $\overline{\rho}_{f, \mathfrak{L}} \cong \overline{\chi_\ell^{m_1} \varepsilon_1} \oplus \overline{\chi_\ell^{m_2} \varepsilon_2}$, then for any g as above, we will have

$$\overline{\chi_\ell^{k-1} \varepsilon} = \overline{\chi_\ell^{k_g-1} \varepsilon_g} \quad \text{and} \quad a_p(f) \equiv a_p(g) \pmod{\mathfrak{L}}, \quad \text{for all primes } p \nmid \ell N N_g.$$

For $(\varepsilon_1, \varepsilon_2, m_1, m_2)$ in $R(\ell)$, define

$$k' := \begin{cases} m_2 - m_1 + 1 & \text{if } \ell > 2; \\ 2 & \text{if } \ell = 2, \end{cases} \quad \text{and} \quad E_0 := E_{k'}^{\varepsilon_1, \varepsilon_2}. \quad (4.1)$$

Proposition 4.3. *We have $\varepsilon_1 \varepsilon_2(-1) = (-1)^{k'}$. In particular, E_0 is well defined and modular if and only if $(k', \varepsilon_1, \varepsilon_2) \neq (2, \mathbb{1}, \mathbb{1})$, in which case E_0 is a normalized eigenform of weight k' , level $\mathfrak{c}_1 \mathfrak{c}_2$, and character $\varepsilon_1 \varepsilon_2$. Moreover, for any prime number p we have $a_p(E_0) = \varepsilon_1(p) + p^{k'-1} \varepsilon_2(p)$ in any case.*

Proof. If $\ell = 2$, then ε_1 and ε_2 are even, and we have $\varepsilon_1 \varepsilon_2(-1) = 1 = (-1)^{k'}$. Otherwise, we have

$$\varepsilon_1 \varepsilon_2(-1) = (-1)^{m_2+m_1+1} = (-1)^{m_2-m_1+1} = (-1)^{k'}.$$

The rest of the proposition follows from Proposition 2.8 and (2.1). \square

To be sure that we can associate a Galois representation modulo \mathfrak{L} to E_0 , we study the integrality of its Fourier coefficients. The following lemma states when the coefficients of E_0 may not be \mathfrak{L} -integral.

Lemma 4.4. *Assume $(k', \varepsilon_1, \varepsilon_2) \neq (2, \mathbb{1}, \mathbb{1})$. The Fourier coefficients of E_0 are \mathfrak{L} -integral unless perhaps in the following cases:*

- $\ell = 2$, $\varepsilon_1 = \mathbb{1}$ and $\varepsilon_2 \neq \mathbb{1}$;
- $\ell \geq 5$, $\varepsilon_1 = \varepsilon_2 = \mathbb{1}$, and $(m_1, m_2) = (0, \ell - 2)$.

Proof. Apart from the constant one, the coefficients of E_0 are all algebraic integers. We therefore only need to focus on the constant Fourier coefficient a_0 of E_0 .

In the case $\ell \neq 2$, if $(\varepsilon_1, \varepsilon_2) \neq (\mathbb{1}, \mathbb{1})$, then a_0 is always \mathfrak{L} -integral by Proposition 2.4, because ε_1 and ε_2 are unramified at ℓ . If $\varepsilon_1 = \varepsilon_2 = \mathbb{1}$, then $a_0 = -\frac{1}{2k'} B_{k'}$.

By Proposition 2.4 again, if $(m_1, m_2) \neq (0, \ell - 2)$, then a_0 is always \mathfrak{L} -integral. If $(m_1, m_2) = (0, \ell - 2)$, then a_0 is always not \mathfrak{L} -integral. Notice moreover that we must have $\ell \neq 3$, because otherwise $k' = 2$ and $\varepsilon_1 = \varepsilon_2 = 1$, which is excluded.

Assume $\ell = 2$, hence $k' = 2$. If $\varepsilon_1 \neq 1$, then as before we have $a_0 = 0$. Else, if $\varepsilon_1 = 1$, then $a_0 = -\frac{B_{2,\varepsilon_2}}{4}$ which may not be \mathfrak{L} -integral. Moreover, we must have $\varepsilon_2 \neq 1$ because otherwise we would have $(k', \varepsilon_1, \varepsilon_2) = (2, 1, 1)$. \square

We can now construct from $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_\ell$ (and hence k_0 and E_0), a modular form with the properties discussed above. With the notations of Propositions 3.24 and 3.27, we define

$$\left\{ \begin{array}{ll} r := 4 \text{ and } E := (E_0)_2^0 & \text{if } \left| \begin{array}{l} \text{we are in one of the cases listed in Lemma 4.4} \\ \text{or } (k', \varepsilon_1, \varepsilon_2) = (2, 1, 1); \end{array} \right. \\ r := 1 \text{ and } E := E_0 & \text{otherwise.} \end{array} \right. \quad (4.2)$$

The following proposition sums up the properties of E .

Proposition 4.5. *The function E is a modular form of weight k' , level $M := \text{lcm}(\mathfrak{c}_1 \mathfrak{c}_2, r)$, and character $\varepsilon_1 \varepsilon_2$. It is a normalized eigenform for all the Hecke operators at level M , all its Fourier coefficients are \mathfrak{L} -integral, and for any prime $p \nmid r$, we have $a_p(E) = \varepsilon_1(p) + p^{k'-1} \varepsilon_2(p)$.*

Proof. The only thing to prove is that M is indeed the level of E . The rest of the proposition then follows from Propositions 3.24, 3.27, Lemma 4.4 and Proposition 4.3. If $r = 1$, the level of E is equal to $\mathfrak{c}_1 \mathfrak{c}_2 = \text{lcm}(\mathfrak{c}_1 \mathfrak{c}_2, r)$. Assume $r = 4$. We then always have $\mathfrak{c}_1 = 1$ and either $\varepsilon_2 = 1$ or $\ell = 2$. In the first case, $\mathfrak{c}_2 = 1$ and $\varepsilon_2(2) = 1 \neq 0$. In the second case, \mathfrak{c}_2 is odd because prime to ℓ . Thus, we have $\varepsilon_2(2) \neq 0$. In every case, the level of E is equal to $4\mathfrak{c}_1 \mathfrak{c}_2 = \text{lcm}(\mathfrak{c}_1 \mathfrak{c}_2, 4)$. \square

The final step to have a modular form that has a Galois representation modulo \mathfrak{L} that is isomorphic to $\overline{\chi}_\ell^{m_1} \overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{m_2} \overline{\varepsilon}_2$ is to apply the operator $\tilde{\theta}$ that we have constructed in Sec. 3.1.

Proposition 4.6. *Let $\bar{\rho} : G_{\mathbb{Q}} \rightarrow \text{GL}_2(\overline{\mathbb{F}}_\ell)$ be a residual, semi-simple, odd Galois representation. Then $\bar{\rho}$ is reducible if and only if there exist $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R(\ell)$ such that $\bar{\rho} \cong \bar{\rho}_{\tilde{\theta}^{m_1} E, \mathfrak{L}}$, where E is the Eisenstein series associated to $(\varepsilon_1, \varepsilon_2, m_1, m_2)$ in (4.2).*

Moreover, if \mathbf{P} is a finite set of primes, and $\mathbf{b} \in \prod_{p \in \mathbf{P}} \{0, \varepsilon_1(p), p^{k'-1} \varepsilon_2(p)\}$, then we also have $\bar{\rho} \cong \bar{\rho}_{\tilde{\theta}^{m_1} E_{\mathbf{P}}, \mathfrak{L}}$, where $E_{\mathbf{P}}^{\mathbf{b}}$ is defined in Corollary 3.26.

Proof. From Proposition 4.2, we only have to prove that for a quadruplet $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R(\ell)$, we have $\bar{\rho}_{\tilde{\theta}^{m_1} E, \mathfrak{L}} \cong \overline{\chi}_\ell^{m_1} \overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{m_2} \overline{\varepsilon}_2$. It follows from Proposition 4.5 and Lemma 3.2 that the representation $\bar{\rho}_{\tilde{\theta}^{m_1} E, \mathfrak{L}}$ is well defined. Moreover,

from Lemma 3.2 again, the form $\tilde{\theta}_A^{m_1} E$ is of weight $k' + m_1(k_A + 2)$, level M , and character $\varepsilon_1 \varepsilon_2 \chi_A^{m_1}$, the value of k_A and χ_A depending on the level M and the place \mathfrak{L} (see Table 1). Recall that in any case we have $\chi_A \equiv \overline{\chi}_\ell^{k_A} \pmod{\mathfrak{L}}$ and $k' \equiv m_2 - m_1 + 1 \pmod{\ell - 1}$. Therefore, we have

$$\begin{aligned} \overline{\chi}_\ell^{(k' + m_1(k_A + 2)) - 1} \chi_A^{m_1} \varepsilon_1 \varepsilon_2 &\equiv \overline{\chi}_\ell^{m_2 - m_1 + 1 + m_1(k_A + 2) - 1 - m_1 k_A} \varepsilon_1 \varepsilon_2 \pmod{\mathfrak{L}} \\ &\equiv \overline{\chi}_\ell^{m_1 + m_2} \varepsilon_1 \varepsilon_2 \pmod{\mathfrak{L}}. \end{aligned}$$

Finally, from Lemma 3.2, Proposition 4.5, and again the congruence $k' \equiv m_2 - m_1 + 1 \pmod{\ell - 1}$, we have for any prime number $p \nmid r\ell$,

$$\begin{aligned} a_p(\tilde{\theta}^{m_1} E) &\equiv p^{m_1} a_p(E) \pmod{\mathfrak{L}} \\ &\equiv p^{m_1} \varepsilon_1(p) + p^{k' + m_1 - 1} \varepsilon_2(p) \pmod{\mathfrak{L}} \\ &\equiv p^{m_1} \varepsilon_1(p) + p^{m_2} \varepsilon_2(p) \pmod{\mathfrak{L}}. \end{aligned}$$

By the discussion at the beginning of the section, we get

$$\overline{\rho}_{\tilde{\theta}^{m_1} E, \mathfrak{L}} \cong \overline{\chi}_\ell^{m_1} \overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{m_2} \overline{\varepsilon}_2.$$

By Corollary 3.26 and Lemma 3.2, the modular form $\tilde{\theta}^{m_1} E_{\mathbf{P}}^{\mathbf{b}}$ still has \mathfrak{L} -integral Fourier coefficients, and is again an eigenform for all the Hecke operators modulo \mathfrak{L} at its level. Moreover, by the same computations as above, the determinant of $\overline{\rho}_{\tilde{\theta}^{m_1} E_{\mathbf{P}}^{\mathbf{b}}, \mathfrak{L}}$ is still equal to $\overline{\chi}_\ell^{m_1 + m_2} \overline{\varepsilon}_1 \overline{\varepsilon}_2$, and for any prime number $p \nmid r\ell$, $p \notin \mathbf{P}$, we have $a_p(\tilde{\theta}^{m_1} E_{\mathbf{P}}^{\mathbf{b}}) \equiv p^{m_1} a_p(E_{\mathbf{P}}^{\mathbf{b}}) \equiv p^{m_1} \varepsilon_1(p) + p^{m_2} \varepsilon_2(p) \pmod{\mathfrak{L}}$. Therefore, we also have $\overline{\rho} \cong \overline{\rho}_{\tilde{\theta}^{m_1} E_{\mathbf{P}}^{\mathbf{b}}, \mathfrak{L}}$. \square

Remark 4.7. Be careful that the operator $\tilde{\theta}$ we apply to $E_{\mathbf{P}}^{\mathbf{b}}$ is not strictly the same as the one we apply to E , the levels of these two forms not being the same.

4.2. General study of modular reducible representations

Let $f = q + \sum_{n=2}^{\infty} a_n(f) q^n$ be a newform of weight $k \geq 2$, level $N \geq 1$, and character ε of conductor \mathfrak{c} . Let K_f be the number field generated by $(a_n(f))_{n \geq 2}$ and let λ be a prime ideal of the ring of integers of K_f above a prime number ℓ . As in the previous section, we begin with the definition of a set that corresponds to the possible reductions of $\overline{\rho}_{f, \lambda}$.

Definition 4.8. Let \mathfrak{L} be a place of $\overline{\mathbb{Q}}$ above ℓ . Define the set $R_{N, k, \varepsilon}(\mathfrak{L})$ as the subset of $R(\ell)$ (see Definition 4.1) consisting of the quadruples $(\varepsilon_1, \varepsilon_2, m_1, m_2)$ such that $\overline{\chi}_\ell^{m_1 + m_2} \overline{\varepsilon}_1 \overline{\varepsilon}_2 = \overline{\chi}_\ell^{k-1} \overline{\varepsilon}$, and for every prime $p \neq \ell$, we have $v_p(\frac{N}{\mathfrak{c}_1 \mathfrak{c}_2}) \in \{0, 1, 2\}$, where $\overline{}$ denotes the reduction modulo \mathfrak{L} , and \mathfrak{c}_i is the conductor of ε_i .

Notice that in particular if $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N, k, \varepsilon}(\mathfrak{L})$, then $\mathfrak{c}_1 \mathfrak{c}_2 \mid N$. The set $R_{N, k, \varepsilon}(\mathfrak{L})$ is therefore finite.

Remark 4.9. We will see later that the set $R_{N,k,\varepsilon}(\mathfrak{L})$ depends in fact only on $\mathfrak{L} \cap \mathbb{Q}(\varepsilon)$ (and obviously on N , k and ε). For now, this dependency will not matter, and we postpone this proof to Sec. 6.

From now on, assume that \mathfrak{L} is a place of $\overline{\mathbb{Q}}$ extending λ .

Proposition 4.10. *The representation $\overline{\rho}_{f,\lambda}$ is reducible if and only if there exists $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$ such that $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1} \overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{m_2} \overline{\varepsilon}_2$, where $\overline{\varepsilon}_i$ denotes the reduction of ε_i modulo \mathfrak{L} .*

Proof. The representation $\overline{\rho}_{f,\lambda}$ is semi-simple and odd. Therefore, by Proposition 4.2, it is reducible if and only if there exist a place \mathfrak{L} above ℓ and $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R(\ell)$ such that $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1} \overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{m_2} \overline{\varepsilon}_2$. We just have to check that in this case we have $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$. The determinant of $\overline{\rho}_{f,\lambda}$ is $\overline{\chi}_\ell^{k-1} \overline{\varepsilon}$. Therefore, we have $\overline{\chi}_\ell^{m_1+m_2} \overline{\varepsilon}_1 \overline{\varepsilon}_2 = \overline{\chi}_\ell^{k-1} \overline{\varepsilon}$. Moreover, the prime-to- ℓ part of the Artin conductor of $\overline{\chi}_\ell^{m_1} \overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{m_2} \overline{\varepsilon}_2$ is equal to $\mathfrak{c}_1 \mathfrak{c}_2$. By Proposition 1.4, we necessarily have $v_p(\frac{N}{\mathfrak{c}_1 \mathfrak{c}_2}) \in \{0, 1, 2\}$ for all primes $p \nmid N$, $p \neq \ell$. \square

In regard of Proposition 4.6, this result is equivalent to saying that the prime index coefficients of f are all but finitely many congruent modulo \mathfrak{L} to those of any of the forms $\tilde{\theta}^{m_1} E_{\mathbf{P}}^{\mathbf{b}}$ described in Sec. 4.1. We will prove that there exist in fact \mathbf{P} and \mathbf{b} such that f is congruent to $\tilde{\theta}^{m_1} E_{\mathbf{P}}^{\mathbf{b}}$ except maybe at the primes dividing ℓ and r . The following result is the key step in this direction. It uses in a crucial way the local description of $\overline{\rho}_{f,\lambda}$ at the bad prime numbers (see Sec. 1).

Lemma 4.11. *If the representation $\overline{\rho}_{f,\lambda}$ is reducible, then there exists $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$ such that for any prime number $p \neq \ell$, we have*

$$a_p(f) \equiv \begin{cases} p^{m_1} \varepsilon_1(p) + p^{m_2} \varepsilon_2(p) \pmod{\mathfrak{L}} & \text{if } p \nmid N, \\ p^{m_1} b_p \pmod{\mathfrak{L}} & \text{if } p \mid N, \end{cases}$$

for some $b_p \in \{0, \varepsilon_1(p), p^{m_2-m_1} \varepsilon_2(p)\}$.

Conversely, if for some $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$, those congruences hold for every prime p in a set of density 1, then we have $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1} \overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{m_2} \overline{\varepsilon}_2$.

Proof. Let us first prove the second statement. Write $\overline{\rho} := \overline{\chi}_\ell^{m_1} \overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{m_2} \overline{\varepsilon}_2$. By construction, the determinants of $\overline{\rho}_{f,\lambda}$ and $\overline{\rho}$ agree. Moreover, by assumption for any prime number $p \nmid N\ell$ in a set of density 1, we have

$$\text{Tr}(\overline{\rho}_{f,\lambda}(\text{Frob}_p)) \equiv a_p(f) \equiv p^{m_1} \varepsilon_1(p) + p^{m_2} \varepsilon_2(p) \equiv \text{Tr}(\overline{\rho}(\text{Frob}_p)) \pmod{\mathfrak{L}}.$$

By Brauer–Nesbitt theorem [11, Lemma 3.2], $\overline{\rho}_{f,\lambda}$ must be isomorphic to $\overline{\rho}$ and is thus reducible.

We now prove the first statement. Assume $\bar{\rho}_{f,\lambda}$ to be reducible. Proposition 4.10 gives us the existence of $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$, such that $\bar{\rho}_{f,\lambda} \cong \bar{\chi}_\ell^{m_1} \bar{\varepsilon}_1 \oplus \bar{\chi}_\ell^{m_2} \bar{\varepsilon}_2$. For any prime $p \nmid N\ell$, taking the trace at a Frobenius at p gives the congruence $a_p(f) \equiv p^{m_1} \varepsilon_1(p) + p^{m_2} \varepsilon_2(p) \pmod{\mathfrak{L}}$. Let us now consider a prime $p \mid N$ and different from ℓ . We treat three cases separately:

- (i) If $v_p(N) \geq 2$ and $v_p(N) > v_p(\mathfrak{c})$, we know from Proposition 1.1 that $a_p(f) = 0$. Hence, we have $a_p(f) \equiv p^{m_1} b_p \pmod{\mathfrak{L}}$ with $b_p = 0$.
- (ii) If $v_p(N) = 1$ and $v_p(\mathfrak{c}) = 0$, then ε is unramified at p . Moreover, by the congruence $\bar{\chi}_\ell^{k-1} \varepsilon \equiv \bar{\chi}_\ell^{m_1+m_2} \varepsilon_1 \varepsilon_2 \pmod{\mathfrak{L}}$, the character $\varepsilon_1 \varepsilon_2$ is then also unramified at p . Therefore, $p \mid \mathfrak{c}_1$ if and only if $p \mid \mathfrak{c}_2$, and because $v_p(N) = 1$ and $\mathfrak{c}_1 \mathfrak{c}_2 \mid N$, we deduce that p does not divide $\mathfrak{c}_1 \mathfrak{c}_2$. Thus, we are in the first case of Proposition 1.3, and we get an equality of sets of characters of G_p

$$\{\mu(a_p(f)), \mu(a_p(f)) \bar{\chi}_\ell\} = \{\bar{\chi}_\ell^{m_1} \bar{\varepsilon}_1, \bar{\chi}_\ell^{m_2} \bar{\varepsilon}_2\}.$$

There are two cases to look at:

- If $\mu(a_p(f)) = \bar{\chi}_\ell^{m_1} \bar{\varepsilon}_1$, then $a_p(f) \equiv \varepsilon_1(p) p^{m_1} \pmod{\mathfrak{L}}$. In this case, we define $b_p = \varepsilon_1(p)$.
- If $\mu(a_p(f)) = \bar{\chi}_\ell^{m_2} \bar{\varepsilon}_2$, then we have $a_p(f) \equiv \varepsilon_2(p) p^{m_2} \pmod{\mathfrak{L}}$, and we put $b_p = p^{m_2-m_1} \varepsilon_2(p)$.

In both cases we have $a_p(f) \equiv p^{m_1} b_p \pmod{\mathfrak{L}}$ with $b_p \in \{\varepsilon_1(p), p^{m_2-m_1} \varepsilon_2(p)\}$.

- (iii) Finally, if $v_p(N) = v_p(\mathfrak{c})$, we are in the second case of Proposition 1.3, and we get the equality

$$\{\mu(a_p(f)), \mu(a_p(f)^{-1}) \bar{\varepsilon}|_{G_p} \bar{\chi}_\ell^{k-1}\} = \{\bar{\chi}_\ell^{m_1} \bar{\varepsilon}_1, \bar{\chi}_\ell^{m_2} \bar{\varepsilon}_2\}.$$

We again have two cases to consider:

- If $\mu(a_p(f)) = \bar{\chi}_\ell^{m_1} \bar{\varepsilon}_1$, then $a_p(f) \equiv \varepsilon_1(p) p^{m_1} \pmod{\mathfrak{L}}$. Let us put $b_p = \varepsilon_1(p)$.
- If $\mu(a_p(f)) = \bar{\chi}_\ell^{m_2} \bar{\varepsilon}_2$, then $a_p(f) \equiv \varepsilon_2(p) p^{m_2} \pmod{\mathfrak{L}}$. We put $b_p = p^{m_2-m_1} \varepsilon_2(p)$.

In both cases, we again have the congruence $a_p(f) \equiv p^{m_1} b_p \pmod{\mathfrak{L}}$ with $b_p \in \{\varepsilon_1(p), p^{m_2-m_1} \varepsilon_2(p)\}$. \square

Let $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$ and consider k' , r and E as defined in (4.1) and (4.2), respectively. With the notations of Proposition 3.24, we define

$$\begin{cases} f' := f_2^0 \text{ and } N' := \begin{cases} N & \text{if } 2 \mid N \text{ and } a_2(f) = 0; \\ 2N & \text{if } 2 \mid N \text{ and } a_2(f) \neq 0; \\ 4N & \text{if } 2 \nmid N, \end{cases} & \text{if } r = 4; \\ f' := f \text{ and } N' := N, & \text{if } r = 1. \end{cases} \quad (4.3)$$

Proposition 4.12. *The form f' is a normalized eigenform of weight k , level N' , and character ε . Its Fourier coefficients are \mathfrak{L} -integral and if a prime p divides r ,*

then $a_p(f') = a_p(E) = 0$. Moreover, the level $M := \text{lcm}(\mathbf{c}_1\mathbf{c}_2, r)$ of E (see Proposition 4.5) always divides N' , and if $\ell = 2$, then $N' \geq 3$.

Proof. The only facts that do not follow directly from Proposition 3.24 are those on the level N' . First recall that $\mathbf{c}_1\mathbf{c}_2$ always divide N . For $M = \text{lcm}(\mathbf{c}_1\mathbf{c}_2, r)$ to divide N' we thus need to prove that r divides N' . If $r = 1$ this is straightforward. Assume $r = 4$. If $2 \nmid N$, then $N' = 4N$ is divisible by r . If $2 \mid N$ and $a_2(f) \neq 0$, then 4 divides $N' = 2N$. Finally, if $2 \mid N$ and $a_2(f) = 0$, then by Proposition 1.1 we necessarily have $v_2(N) \geq 2$. Therefore $N' = N$ is again divisible by r . In every case, we have $M \mid N'$.

Finally, assume $\ell = 2$. If $\varepsilon_1 = 1$, then we necessarily have $r = 4$ and $N' \geq 4$. Otherwise, if $\varepsilon_1 \neq 1$, we then have $N' \geq \mathbf{c}_1 \geq 3$ because there is no non-trivial primitive character of conductor less than 3. \square

It follows from Lemma 4.11 that if $\bar{\rho}_{f,\lambda}$ is reducible, then there exist \mathbf{P} and \mathbf{b} such that for all primes p , we have $pa_p(f') \equiv p^{m_1+1}a_p(E_{\mathbf{P}}^{\mathbf{b}}) \pmod{\mathfrak{L}}$. In order to use Corollary 3.19 and make these infinite set of congruences equivalent to a finite one, we now need to control the level of $E_{\mathbf{P}}^{\mathbf{b}}$.

Proposition 4.13. *Let $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$, let $p \neq \ell$ be any prime number dividing N , and let $b_p \in \{0, \varepsilon_1(p), p^{k'-1}\varepsilon_2(p)\}$.*

If we have a congruence $a_p(f) \equiv p^{m_1}b_p \pmod{\mathfrak{L}}$, then we have

$$1 \leq v_p(\mathbf{c}_1\mathbf{c}_2) + n_p \leq v_p(N),$$

where n_p is defined as in Proposition 3.24 with respect to $g = E$ and b_p . In particular, those inequalities are independent of the choice of b_p .

Proof. First, we always have $v_p(\mathbf{c}_1\mathbf{c}_2) + n_p \geq 1$, because $n_p = 0$ only if $b_p = a_p(E) = \varepsilon_1(p) + p^{k'-1}\varepsilon_2(p)$, which implies that $v_p(\mathbf{c}_1\mathbf{c}_2) \geq 1$.

Next, we claim the following:

$$b_p = 0 \text{ if and only if } v_p(\mathbf{c}) < v_p(N) \text{ and } v_p(N) \geq 2.$$

Indeed, we have $b_p = 0$ if and only if $a_p(f) \equiv 0 \pmod{\mathfrak{L}}$. Moreover, by Proposition 1.1 we have either $v_p(\mathbf{c}) < v_p(N)$, $v_p(N) \geq 2$ and $a_p(f) = 0$, or $|a_p(f)|^2 = p^s$ with $s \geq 0$. Therefore, we have $a_p(f) \equiv 0 \pmod{\mathfrak{L}}$ if and only if $v_p(\mathbf{c}) < v_p(N)$ and $v_p(N) \geq 2$.

We now prove that $v_p(\mathbf{c}_1\mathbf{c}_2) + n_p \leq v_p(N)$. If $n_p = 0$, it follows from the fact that $\mathbf{c}_1\mathbf{c}_2 \mid N$. If $n_p = 2$, then from Proposition 3.24, we must have $b_p = 0 \notin \{\varepsilon_1(p), p^{k'-1}\varepsilon_2(p)\}$. Therefore, $p \nmid \mathbf{c}_1\mathbf{c}_2$ and from the discussion above we have $v_p(N) \geq 2 = v_p(\mathbf{c}_1\mathbf{c}_2) + n_p$.

Assume finally that $n_p = 1$. We then have $b_p \neq \varepsilon_1(p) + p^{k'-1}\varepsilon_2(p)$ and $b_p \in \{\varepsilon_1(p), p^{k'-1}\varepsilon_2(p)\}$. Therefore, p does not divide both \mathbf{c}_1 and \mathbf{c}_2 . If $p \nmid \mathbf{c}_1\mathbf{c}_2$, we have $v_p(\mathbf{c}_1\mathbf{c}_2) + n_p = 1 \leq v_p(N)$. Otherwise, assume that $p \mid \mathbf{c}_1$ and $p \nmid \mathbf{c}_2$. We then necessarily have $b_p = 0$ and from the discussion above we get $v_p(\mathbf{c}) < v_p(N)$.

Looking at the p -part of the Artin conductor of both sides of the equality $\overline{\chi}_\ell^{k-1}\overline{\varepsilon} = \overline{\chi}_\ell^{m_1+m_2}\overline{\varepsilon_1\varepsilon_2}$, we get $v_p(\overline{\mathfrak{c}}) = v_p(\overline{\mathfrak{c}_1})$ where $\overline{\mathfrak{c}}$ and $\overline{\mathfrak{c}_1}$ denote the conductors of $\overline{\varepsilon}$ and $\overline{\varepsilon_1}$, respectively. Because ε_1 has prime-to- ℓ order, we have $\overline{\mathfrak{c}_1} = \mathfrak{c}_1$. On the other side we always have $\overline{\mathfrak{c}} | \mathfrak{c}$. Therefore, we have $v_p(\mathfrak{c}_1\mathfrak{c}_2) = v_p(\mathfrak{c}_1) \leq v_p(\mathfrak{c})$. Hence, we get $v_p(\mathfrak{c}_1\mathfrak{c}_2) + n_p \leq v_p(N)$. The case $p | \mathfrak{c}_2$ and $p \nmid \mathfrak{c}_1$ is treated in exactly the same way. \square

Corollary 4.14. *Let $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$. Define k' , r and E as in (4.1) and (4.2), respectively. Consider $\mathbf{P} \subseteq \{p \text{ prime}, p | N, p \nmid r\ell\}$ and $\mathbf{b} := (b_p)_{p \in \mathbf{P}} \in \prod_{p \in \mathbf{P}} \{0, \varepsilon_1(p), p^{k'-1}\varepsilon_2(p)\}$ such that for all $p \in \mathbf{P}$, we have $p^{m_1}b_p \equiv a_p(f) \pmod{\mathfrak{L}}$.*

The modular form $E' := E_{\mathbf{P}}^{\mathbf{b}}$ is of weight k' , character $\varepsilon_1\varepsilon_2$, and its level divides N' . It has \mathfrak{L} -integral Fourier coefficients and for every prime p such that either $p \nmid N\ell$ or $p \in \mathbf{P} \cup \{r\}$, E' is a normalized eigenform for the Hecke operator $T_p^{N'}$.

Proof. From Corollary 3.26, the form E' is a normalized eigenform for all the Hecke operators at its level $N_{E'} := M \prod_{p \in \mathbf{P}} p^{n_p}$. Moreover, the action of $T_p^{N'}$ and $T_p^{N_{E'}}$ on E' are the same if p divides both N' and $N_{E'}$ or none of them. If $p \nmid N\ell$, then $p \nmid N_{E'}$. If $p \in \mathbf{P} \cup \{r\}$, by Proposition 4.13, we have

$$1 \leq v_p(N_{E'}) \leq v_p(N').$$

Therefore, $N_{E'}$ divides N' and E' is a normalized eigenform for the announced Hecke operators. The rest of the corollary follows from Corollary 3.26. \square

We now state the first main result of this section. It gives for a given λ , an explicit algorithm to check the reducibility of the representation $\overline{\rho}_{f,\lambda}$.

Theorem 4.15. *Let f be a newform of weight $k \geq 2$, level $N \geq 1$, and character ε . Let λ be a prime ideal of K_f above a prime number ℓ . The following assertions are equivalent:*

- (1) $\overline{\rho}_{f,\lambda}$ is reducible;
- (2) Let \mathfrak{L} be a place of $\overline{\mathbb{Q}}$ above λ . There exists $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$ (see Definition 4.8) such that the following holds. Let k' , r , and N' be as in (4.1), (4.2) and (4.3), respectively. Define

$$a = \begin{cases} 4 & \text{if } \begin{cases} k \equiv m_1 + m_2 + 3 \pmod{4}, \\ \ell = 3 \text{ and } \forall p | N', p \equiv 1 \pmod{9}; \end{cases} \\ 0 & \text{otherwise,} \end{cases}$$

$$b = \begin{cases} 3 & \text{if } \ell | N'; \\ 6 & \text{if } \begin{cases} \ell = 3 \text{ and } \forall p | N', \\ p \equiv 1 \pmod{9}; \end{cases} \\ \ell + 1 & \text{otherwise.} \end{cases} \quad \text{and} \quad \widetilde{k} = a + b + \max(k, k' + bm_1).$$

For every prime $p \leq B := \frac{N'\tilde{k}}{12} \prod_{q|N'}(1 + \frac{1}{q})$ not dividing $r\ell$, we have

- $p \nmid N$ and $a_p(f) \equiv p^{m_1}\varepsilon_1(p) + p^{m_2}\varepsilon_2(p) \pmod{\mathfrak{L}}$;
- or, $p|N$ and $a_p(f) \equiv p^{m_1}b_p \pmod{\mathfrak{L}}$ for some b_p in the set $\{0, \varepsilon_1(p), p^{m_2-m_1}\varepsilon_2(p)\}$.

When this holds, we moreover have $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1}\overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{m_2}\overline{\varepsilon}_2$.

Proof. Assertion (2) is weaker than the second part of Lemma 4.11. Therefore, (1) implies (2).

Assume that (2) holds. Consider again k', r, E, N' , and f' defined in (4.1), (4.2) and (4.3), respectively. Define $\mathbf{P} := \{p \text{ prime, } p|N, p \nmid \ell r, p \leq B\}$, and $\mathbf{b} := (b_p)_{p \in \mathbf{P}}$. Finally, with the notation of Corollary 3.26, consider the form $E' := E_{\mathbf{P}}^{\mathbf{b}}$.

We wish to apply Corollary 3.19 with $f = f', g = E', m_f = 1$ and $m_g = m_1 + 1$. By Corollary 4.14, we have $E' \in \mathbf{M}_{k'}(N', \varepsilon_1\varepsilon_2)$, it has \mathfrak{L} -integral Fourier coefficients, and it is an eigenform for all the Hecke operators at level N' of index less than B , except maybe at ℓ . Moreover, from the identity $\overline{\chi}_\ell^{m_1+m_2}\overline{\varepsilon}_1\overline{\varepsilon}_2 = \overline{\chi}_\ell^{k-1}\overline{\varepsilon}$, we have

$$\overline{\chi}_\ell^{k'+2(m_1+1)}\overline{\varepsilon}_1\overline{\varepsilon}_2 = \overline{\chi}_\ell^{(m_2-m_1+1)+2(m_1+1)}\overline{\varepsilon}_1\overline{\varepsilon}_2 = \overline{\chi}_\ell^{m_1+m_2+3}\overline{\varepsilon}_1\overline{\varepsilon}_2 = \overline{\chi}_\ell^{k+2}\overline{\varepsilon}.$$

Let p be a prime number less than B . If $p|\ell r$, then we have

$$p^{m_1+1}a_p(E') \equiv 0 \equiv pa_p(f') \pmod{\mathfrak{L}}.$$

Otherwise, by Corollary 3.26 we have $p^{m_1+1}a_p(E') \equiv p^{m_1+1}b_p \equiv pa_p(f') \pmod{\mathfrak{L}}$. The definitions of a, b and \tilde{k} correspond to those of a, b and k in Proposition 3.17 (the case $\ell = 2$ and $N' \leq 2$ never occurs as proved in Proposition 4.12). By Corollary 3.19, we therefore obtain the congruence $na_n(f') \equiv n^{m_1+1}a_n(E') \pmod{\mathfrak{L}}$ for every non-negative integer n . By Lemma 4.11, we thus have $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1}\overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{m_2}\overline{\varepsilon}_2$. \square

Remark 4.16. From this theorem, we can deduce an algorithm that takes a prime ideal λ as input and decides whether the representation $\overline{\rho}_{f,\lambda}$ is reducible or not, and computes the representation if it is reducible. In particular, it justifies the reducibility modulo 11 of the representation treated in [3, 5.1.2]. We give further details on how to explicitly do this in PARI/GP in Sec. 6. Moreover, the theorem extends the case $m = 1$ of [18, Proposition 2].

The previous theorem holds without any restriction on ℓ , but the result depends on ℓ through

- (1) the set $R_{N,k,\varepsilon}(\mathfrak{L})$;
- (2) the integer B that bounds the number of congruences to check.

We first remove the dependency in ℓ in the set $R_{N,k,\varepsilon}(\mathfrak{L})$.

Definition 4.17. Define $R_{N,\varepsilon}$ as the set of pairs $(\varepsilon_1, \varepsilon_2)$ of primitive Dirichlet characters such that $\varepsilon_1\varepsilon_2 = \varepsilon$ and for every prime number p , we have $v_p(\frac{N}{c_1c_2}) \in \{0, 1, 2\}$, where c_i is the conductor of ε_i .

Proposition 4.18. *Assume $\ell \geq k - 1$ and $\ell \nmid N\varphi(N)$. The representation $\bar{\rho}_{f,\lambda}$ is reducible if and only if there exists $(\varepsilon_1, \varepsilon_2) \in R_{N,\varepsilon}$ such that $\bar{\rho}_{f,\lambda} \cong \bar{\varepsilon}_1 \oplus \bar{\chi}_\ell^{k-1} \bar{\varepsilon}_2$. We moreover have $a_\ell(f) \equiv \varepsilon_1(\ell) + \ell^{k-1} \varepsilon_2(\ell) \pmod{\mathfrak{L}}$.*

Proof. From Proposition 4.10, if $\bar{\rho}_{f,\lambda}$ is reducible, then there exists a quadruple $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$ such that $\bar{\rho}_{f,\lambda} \cong \bar{\chi}_\ell^{m_1} \bar{\varepsilon}_1 \oplus \bar{\chi}_\ell^{m_2} \bar{\varepsilon}_2$. By the assumptions $\ell \nmid N$ and $\ell \geq k - 1$, together with Proposition 1.2, f must be ordinary at λ , and we have an equality of sets

$$\left\{ \mu(a_\ell(f)), \bar{\chi}_\ell^{k-1} \mu\left(\frac{\varepsilon(\ell)}{a_\ell(f)}\right) \right\} = \{ \bar{\chi}_\ell^{m_1} \bar{\varepsilon}_1, \bar{\chi}_\ell^{m_2} \bar{\varepsilon}_2 \}.$$

It follows that $(m_1, m_2) = (0, k - 1)$ and $a_\ell(f) \equiv \varepsilon_1(\ell) \equiv \varepsilon_1(\ell) + \ell^{k-1} \varepsilon_2(\ell) \pmod{\mathfrak{L}}$. Finally, the character $\varepsilon(\varepsilon_1 \varepsilon_2)^{-1}$ reduces to the trivial character modulo \mathfrak{L} , and because $\ell \nmid \varphi(N)$, it must have prime-to- ℓ order. Using Lemma 2.7, it must be trivial, and we get $\varepsilon = \varepsilon_1 \varepsilon_2$. \square

The following result will allow us to both remove the dependency in ℓ in the bound B of Theorem 4.15, and bound the set of ℓ such that $\bar{\rho}_{f,\lambda}$ is reducible.

Proposition 4.19. *Assume $\ell > k + 1$ and $\ell \nmid N\varphi(N)$. The representation $\bar{\rho}_{f,\lambda}$ is reducible if and only if there exist a pair $(\varepsilon_1, \varepsilon_2) \in R_{N,\varepsilon}$, and $\mathbf{b} \in \prod_{p \in \mathbf{P}} \{0, \varepsilon_1(p), p^{k-1} \varepsilon_2(p)\}$, with $\mathbf{P} := \{p \text{ prime}, p \mid N, p \nmid \ell r\}$, such that $f' \equiv E' \pmod{\mathfrak{L}}$, with f' defined as in (4.3) and $E' := E_{\mathbf{P}}^{\mathbf{b}}$.*

Proof. If we have $f' \equiv E' \pmod{\mathfrak{L}}$, then in particular for all primes $p \nmid N\ell r$, we have

$$a_p(f) = a_p(f') \equiv a_p(E') \equiv \varepsilon_1(p) + p^{k-1} \varepsilon_2(p) \pmod{\mathfrak{L}}.$$

By Lemma 4.11, $\bar{\rho}_{f,\lambda}$ is therefore reducible.

Assume that $\bar{\rho}_{f,\lambda}$ is reducible. The existence of $(\varepsilon_1, \varepsilon_2)$ is granted by Proposition 4.18. Moreover, by Lemma 4.11 there exists $\mathbf{b} \in \prod_{p \in \mathbf{P}} \{0, \varepsilon_1(p), p^{k-1} \varepsilon_2(p)\}$ such that for every prime number p , we have a congruence $a_p(f') \equiv a_p(E') \pmod{\mathfrak{L}}$. By Corollary 4.14, $E' \in M_k(N', \varepsilon)$ has \mathfrak{L} -integral Fourier coefficients and is an eigenform for all the Hecke operators at level N' . By Proposition 4.12, f' has the same properties and therefore the modular form $f' - E'$ is constant modulo \mathfrak{L} .

By the assumptions $\ell > k + 1$ and $\ell \nmid N\varphi(N)$, we have $\ell \geq 5$ and $\ell \nmid N$. Therefore, we know from [12, Theorem 12.3.7] that Katz' modular form spaces with coefficients in $\overline{\mathbb{F}}_\ell$ are isomorphic to the spaces of reduction modulo \mathfrak{L} of modular forms with \mathfrak{L} -integral coefficients. Therefore, from [15, Corollary 4.4.2], for $f' - E'$ to be congruent to a non-zero constant we must have $k \equiv 0 \pmod{\ell - 1}$. This cannot hold under the assumption $\ell > k + 1$, and we get $f' \equiv E' \pmod{\mathfrak{L}}$. \square

We now state our second main result. It is analogous to Theorem 4.15 for the prime numbers $\ell > k + 1$ and $\ell \nmid N\varphi(N)$.

Theorem 4.20. *Let f be a newform of weight $k \geq 2$, level $N \geq 1$, and character ε . Let λ be a prime ideal of K_f above a prime number ℓ . Assume $\ell > k + 1$ and $\ell \nmid N\varphi(N)$. The following assertions are equivalent.*

- (1) $\overline{\rho}_{f,\lambda}$ is reducible.
- (2) Let \mathfrak{L} be a place of $\overline{\mathbb{Q}}$ above λ . There exists $(\varepsilon_1, \varepsilon_2) \in R_{N,\varepsilon}$ such that the following holds. Let r be as in (4.2) (recall that $(m_1, m_2) = (0, k - 1)$) and let N' be as in (4.3). Define

$$C = \begin{cases} 0 & \text{if } r > 1 \text{ or } \varepsilon_1 \neq \mathbb{1}; \\ -\frac{B_{k,\varepsilon_0}}{2k} \prod_{p|N} a_p(f)(a_p(f) - p^{k-1}\varepsilon_0(p)) & \text{otherwise,} \end{cases}$$

where ε_0 is the primitive character associated to ε .

We have $C \equiv 0 \pmod{\mathfrak{L}}$, and for all primes $p \leq B := \frac{N'k}{12} \prod_{q|N'} (1 + \frac{1}{q})$, we have either $p \nmid r$ or

- $a_p(f) \equiv \varepsilon_1(p) + p^{k-1}\varepsilon_2(p) \pmod{\mathfrak{L}}$, if $p \nmid N$;
- $a_p(f) \equiv b_p \pmod{\mathfrak{L}}$ for some $b_p \in \{0, \varepsilon_1(p), p^{k-1}\varepsilon_2(p)\}$, if $p \mid N$.

When this holds, we moreover have $\overline{\rho}_{f,\lambda} \cong \overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{k-1} \overline{\varepsilon}_2$.

Proof. Assume $\overline{\rho}_{f,\lambda}$ to be reducible. Introduce f' and E' as in Proposition 4.19. The congruences for $a_p(f)$ follow from the congruence $f' \equiv E' \pmod{\mathfrak{L}}$. It only remains to prove that $C \equiv 0 \pmod{\mathfrak{L}}$. Because f' is cuspidal, its constant coefficient at infinity is equal to 0. Therefore, the one of E' must be congruent to 0 modulo \mathfrak{L} .

The congruence $C \equiv 0 \pmod{\mathfrak{L}}$ is non-trivial only if $r = 1$ and $\varepsilon_1 = \mathbb{1}$. In this case, we have $\varepsilon_2 = \varepsilon_0$, the set \mathbf{P} of Proposition 4.19 is the set of prime divisors of N and for all $p \in \mathbf{P}$ we have $b_p \equiv a_p(f) \pmod{\mathfrak{L}}$. Therefore, the constant coefficient of E' is equal to

$$\begin{aligned} -\frac{B_{k,\varepsilon_2}}{2k} \prod_{p \in \mathbf{P}} b_p(b_p - p^{k-1}\varepsilon_2(p)) &\equiv -\frac{B_{k,\varepsilon_0}}{2k} \prod_{p|N} a_p(f)(a_p(f) - p^{k-1}\varepsilon_0(p)) \pmod{\mathfrak{L}} \\ &\equiv C \pmod{\mathfrak{L}}. \end{aligned}$$

This proves that (1) implies (2).

Assume now that the second part of the theorem holds. Consider again the modular forms E and f' , and define $\mathbf{P}_{\leq B} := \{p \text{ prime}, p \mid N, p \leq B\}$ and $\mathbf{b}_{\leq B} := (b_p)_{p \in \mathbf{P}_{\leq B}}$, and let $E' := E_{\mathbf{P}_{\leq B}}^{\mathbf{b}_{\leq B}}$. By Corollary 4.14, we have $E' \in M_k(N', \varepsilon)$, it has \mathfrak{L} -integral coefficients, and it is an eigenform for all the Hecke operators at level N' of index less than B . The form f' has moreover the same properties and for all prime numbers $p \leq B$, we have by assumption $a_p(f') \equiv a_p(E') \pmod{\mathfrak{L}}$. In order to apply Corollary 3.19 to $f = f'$, $g = E'$, $m_f = m_g = 0$, we need to have $a_0(E') \equiv 0 \pmod{\mathfrak{L}}$. From Proposition 3.29, we have $a_0(E') = 0$ if $\varepsilon_1 \neq \mathbb{1}$ or $r > 1$.

Else, if $\varepsilon_1 = 1$ and $r = 1$, we have $\varepsilon_2 = \varepsilon_0$ and

$$\begin{aligned} a_0(E') &= -\frac{B_{k,\varepsilon_2}}{2k} \prod_{p|N, p \leq B} b_p(b_p - p^{k-1}\varepsilon_2(p)) \\ &\equiv -\frac{B_{k,\varepsilon_0}}{2k} \prod_{p|N, p \leq B} a_p(f)(a_p(f) - p^{k-1}\varepsilon_0(p)) \pmod{\mathfrak{L}}. \end{aligned}$$

By the assumption $C \equiv 0 \pmod{\mathfrak{L}}$, we have either $a_0(E') \equiv 0 \pmod{\mathfrak{L}}$, or there exists $p_0 | N$, $p_0 > B$, such that $a_{p_0}(f)(a_{p_0}(f) - p_0^{k-1}\varepsilon_0(p_0)) \equiv 0 \pmod{\mathfrak{L}}$. Define then

$$\begin{aligned} E'' &:= \begin{cases} E' & \text{if } a_0(E') \equiv 0 \pmod{\mathfrak{L}}; \\ E'^{b_{p_0}}_{p_0} & \text{otherwise} \end{cases} \quad \text{with} \\ b_{p_0} &= \begin{cases} 0 & \text{if } a_{p_0}(f) \equiv 0 \pmod{\mathfrak{L}}; \\ p_0^{k-1}\varepsilon_0(p_0) & \text{if } a_{p_0}(f) \equiv p_0^{k-1}\varepsilon_0(p_0) \pmod{\mathfrak{L}}. \end{cases} \end{aligned}$$

By Corollary 4.14, E'' still lies in $M_k(N', \varepsilon)$, has \mathfrak{L} -integral Fourier coefficients, is an eigenform for the Hecke operators at level N' of index less than B , for any prime $p \leq B$, we have $a_p(E'') \equiv a_p(f') \pmod{\mathfrak{L}}$, and its constant Fourier coefficient vanishes modulo \mathfrak{L} . By Corollary 3.19, we finally get $E'' \equiv f' \pmod{\mathfrak{L}}$, and we therefore have $\overline{\rho}_{f,\lambda} \cong \overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{k-1} \overline{\varepsilon}_2$. \square

Remark 4.21. Notice that we could have always taken $r = 4$ from the start (i.e. from (4.2)) without modifying any of the results of Sec. 4. The version of Theorems 4.15 and 4.20 we exposed in the introduction assumed that. The coefficient C is then equal to zero, and we get back the results announced previously.

From Theorem 4.20 we also deduce a bound for the reducible primes in terms of N , k and ε only.

Theorem 4.22. *Assume that $\overline{\rho}_{f,\lambda}$ is reducible, then one of the following conditions holds.*

- $\ell \leq k + 1$;
- $\ell | N\varphi(N)$;
- *there exists $(\varepsilon_1, \varepsilon_2) \in R_{N,\varepsilon}$ such that ℓ divides the algebraic norm of one the following nonzero quantities*

- (1) $B_{k,(\varepsilon_1^{-1}\varepsilon_2)_0}$;
- (2) $p^k - (\varepsilon_1\varepsilon_2^{-1})_0(p)$ for a prime p such that $p | \mathfrak{c}_1\mathfrak{c}_2$, $p \nmid \mathfrak{c}_0$ with \mathfrak{c}_0 the conductor of $(\varepsilon_1\varepsilon_2^{-1})_0$.

Proof. Assume $\ell > k + 1$ and $\ell \nmid N\varphi(N)$. From Proposition 4.19, if $\overline{\rho}_{f,\lambda}$ is reducible, we have a congruence modulo \mathfrak{L} between the cuspidal modular form f' , and the

Eisenstein series E' . Therefore, by Katz' q -expansion principle (see [15]) the constant coefficient of E' must be congruent to 0 modulo \mathfrak{L} at every cusp. By Proposition 3.30, the constant coefficient of E' at the cusp $\frac{1}{\mathfrak{c}_2}$ divides the quantity

$$-\varepsilon_1(-1) \frac{W((\varepsilon_1 \varepsilon_2^{-1})_0)}{W(\varepsilon_2^{-1})} \frac{B_{k,(\varepsilon_1^{-1} \varepsilon_2)_0}}{2k} \left(\frac{\mathfrak{c}_2}{\mathfrak{c}_0} \right)^k \\ \times \prod_{p|\mathfrak{c}_1 \mathfrak{c}_2} \left(1 - \frac{(\varepsilon_1 \varepsilon_2^{-1})_0(p)}{p^k} \right) \prod_{p|N'} \left(1 - \frac{\varepsilon_1(p) \varepsilon_2^{-1}(p)}{p^k} \right) \left(1 - \frac{1}{p} \right).$$

Let us look at the prime factors of the norm of this coefficient.

- The number $-\varepsilon_1(-1)$ is a unit. Its norm has no prime factor.
- By Proposition 2.6, the prime factors of the norm of $\frac{W((\varepsilon_1 \varepsilon_2^{-1})_0)}{W(\varepsilon_2^{-1})} \left(\frac{\mathfrak{c}_2}{\mathfrak{c}_0} \right)^k$ are only powers of prime factors of N . By assumption, ℓ does not divide them.
- For $p|N'$, we have $1 - \frac{1}{p} = \frac{p-1}{p}$. By the assumption $\ell \nmid N\varphi(N)$, this cannot vanish modulo \mathfrak{L} .
- For $p|N'$ again, let us prove that the prime factors of the norm of $\left(1 - \frac{\varepsilon_1(p) \varepsilon_2^{-1}(p)}{p^k} \right)$ are redundant with the ones of N and $(p^k - (\varepsilon_1 \varepsilon_2^{-1})_0(p))$. Note that we either have $p = 2$ and $(k, \varepsilon_1, \varepsilon_2) = (2, 1, 1)$, or $N' = N$. In the first case we have $1 - \frac{\varepsilon_1(p) \varepsilon_2^{-1}(p)}{p^k} = \frac{3}{4}$. This cannot vanish modulo \mathfrak{L} by assumption because 2 and 3 are less or equal to $k + 1 = 3$. Otherwise, we have $p|N$, then either $p|\mathfrak{c}_0$ and $1 - \frac{\varepsilon_1(p) \varepsilon_2^{-1}(p)}{p^k} = 1 \not\equiv 0 \pmod{\mathfrak{L}}$, or $p \nmid \mathfrak{c}_0$ and $1 - \frac{\varepsilon_1(p) \varepsilon_2^{-1}(p)}{p^k} = \frac{p^k - (\varepsilon_1 \varepsilon_2^{-1})_0(p)}{p^k}$. Therefore, ℓ must divide the algebraic norm of $p^k - (\varepsilon_1 \varepsilon_2^{-1})_0(p)$.
- Finally ℓ divides either the norm of $\frac{B_{k,(\varepsilon_1^{-1} \varepsilon_2)_0}}{2k}$ and thus $B_{k,(\varepsilon_1^{-1} \varepsilon_2)_0}$ because $2k$ is nonzero modulo \mathfrak{L} by assumption, or $p^k - (\varepsilon_1 \varepsilon_2^{-1})_0(p)$ for $p|\mathfrak{c}_1 \mathfrak{c}_2$. This final quantity contains only prime factors of N if $p|\mathfrak{c}_0$. We can therefore consider only the primes $p \nmid \mathfrak{c}_0$. \square

5. Dihedral Representations

Let $k \geq 2$, $N \geq 1$ be two integers, and ε be a Dirichlet character modulo N of conductor \mathfrak{c} . Let $f \in S_k^{\text{new}}(N, \varepsilon)$ be a newform. We study in this section the case where $\overline{\rho}_{f,\lambda}$ has projective dihedral image. The main result of this section is Theorem 5.10. The strategy used to prove this result is similar to the one of [3, Theorem 3.2] but several technicalities arise when dealing with forms with non-trivial characters. However, our method is based on a more refined use of the local description of $\overline{\rho}_{f,\lambda}$ at the prime dividing the level, leading to an improved bound in the trivial character case.

5.1. CM forms

Let φ be a Dirichlet character of modulus M . We define the twist of f by φ as the only newform $f \otimes \varphi$ such that $a_p(f \otimes \varphi) = \varphi(p)a_p(f)$ for all but finitely many primes p . We have the following result from [2, §§1–3].

Proposition 5.1. *With the above notations $f \otimes \varphi \in S_k(\text{lcm}(N, M^2, \mathfrak{c}M), \varphi^2\varepsilon)$. For all primes $p \nmid M$, we have $a_p(f \otimes \varphi) = \varphi(p)a_p(f)$ and the p -part of the level of $f \otimes \varphi$ is equal to $p^{v_p(N)}$.*

Moreover, if $v_p(N) = v_p(\mathfrak{c})$ and $\varphi_p = \varepsilon_p^{-1}$, where φ_p and ε_p denote the p -parts of φ and ε , respectively, then the p -parts of the levels of $f \otimes \varphi$ and f are equal, and we have $a_p(f \otimes \varphi) = \varepsilon'_p(p)\varphi'_p(p)\overline{a_p(f)}$, with $\overline{a_p(f)}$ the complex conjugate of $a_p(f)$ and ε'_p and φ'_p are the prime-to- p part of ε and φ , respectively.

We take this definition of CM forms from [28, p. 34].

Definition 5.2. Suppose φ is not the trivial character. The form f is said to have complex multiplication by φ if $\varphi(p)a_p(f) = a_p(f)$ for all primes p in a set of primes of density 1.

5.2. Study of the ramification of a character

Let ℓ be a prime number and let λ be a prime ideal of \mathcal{O}_f above ℓ . We assume for the rest of the section that $\ell \neq 2$. Consider the projectivization

$$\mathbb{P}\overline{\rho}_{f,\lambda} : G_{\mathbb{Q}} \xrightarrow{\overline{\rho}_{f,\lambda}} \text{GL}_2(\mathbb{F}_{\lambda}) \rightarrow \text{PGL}_2(\mathbb{F}_{\lambda})$$

and assume that $\mathbb{P}\overline{\rho}_{f,\lambda}(G_{\mathbb{Q}})$ is a dihedral group D_{2n} of order $2n$ with $\ell \nmid n$. Let C be the unique cyclic subgroup of order n in $\mathbb{P}\overline{\rho}_{f,\lambda}(G_{\mathbb{Q}})$. It is a normal subgroup, and we get a quadratic character

$$\theta_{f,\lambda} : G_{\mathbb{Q}} \xrightarrow{\mathbb{P}\overline{\rho}_{f,\lambda}} D_{2n} \rightarrow D_{2n}/C \cong \mathbb{Z}/2\mathbb{Z}.$$

Recall that the elements in $D_{2n} \setminus C$ are of order 2 and hence have all trace 0. Let us focus on the ramification of the character $\theta_{f,\lambda}$. Let $\mathfrak{c}_{f,\lambda}$ be the conductor of $\theta_{f,\lambda}$ seen as a Dirichlet character. Because $\overline{\rho}_{f,\lambda}$ is unramified outside $N\ell$, the prime factors of $\mathfrak{c}_{f,\lambda}$ are among the ones of $N\ell$. Let $K_{f,\lambda}$ be the number field fixed by the kernel of $\theta_{f,\lambda}$. It is a quadratic extension of \mathbb{Q} , and we can write $K_{f,\lambda} = \mathbb{Q}(\sqrt{d_{f,\lambda}})$ with $d_{f,\lambda} \in \mathbb{Z}$ square-free. By the conductor-discriminant formula [26, VII. (11.9)], we have

$$\mathfrak{c}_{f,\lambda} = \begin{cases} |d_{f,\lambda}| & \text{if } d_{f,\lambda} \equiv 1 \pmod{4}, \\ 4|d_{f,\lambda}| & \text{if } d_{f,\lambda} \equiv 2, 3 \pmod{4}. \end{cases}$$

We thus have the following result.

Proposition 5.3. *Let p be a prime number dividing $\mathfrak{c}_{f,\lambda}$. Then we have either $p \neq 2$, $p \mid N\ell$ and $v_p(\mathfrak{c}_{f,\lambda}) = 1$, or $p = 2$, $p \mid N$ and $v_p(\mathfrak{c}_{f,\lambda}) \in \{2, 3\}$.*

We now prove the following lemma.

Lemma 5.4. *Let G be a finite group and let K be a field of positive characteristic ℓ . Let $\rho : G \rightarrow \mathrm{GL}_2(K)$ be a morphism with values in the subgroup of $\mathrm{GL}_2(K)$ of upper triangular matrices. Put $\rho = \begin{pmatrix} \chi_1 & c \\ 0 & \chi_2 \end{pmatrix}$. If the order of $\mathbb{P}\rho$ is prime to ℓ , then $\mathrm{Im}(\mathbb{P}\rho) \cong \mathrm{Im}(\chi_1\chi_2^{-1})$.*

Proof. From the isomorphisms $G/\ker(\chi_1\chi_2^{-1}) \cong \mathrm{Im}(\chi_1\chi_2^{-1})$ and $G/\ker(\mathbb{P}\rho) \cong \mathrm{Im}(\mathbb{P}\rho)$, it suffices to prove that $\ker(\mathbb{P}\rho) = \ker(\chi_1\chi_2^{-1})$.

Let $\sigma \in \ker(\mathbb{P}\rho)$. There exists $\lambda \in K$ such that $\rho(\sigma) = \lambda I_2$, and we immediately have $\chi_1(\sigma) = \chi_2(\sigma)$. Therefore, $\sigma \in \ker(\chi_1\chi_2^{-1})$.

Let $\sigma \in \ker(\chi_1\chi_2^{-1})$ and let $\lambda := \chi_1(\sigma) = \chi_2(\sigma)$. We then have

$$\rho(\sigma) = \begin{pmatrix} \lambda & c(\sigma) \\ 0 & \lambda \end{pmatrix}.$$

The order of $\rho(\sigma)$ in $\mathrm{PGL}_2(K)$ is equal to 1 if $c(\sigma) = 0$ and to ℓ if not. By assumption, the image of $\mathbb{P}\rho$ is of order prime to ℓ . Thus $c(\sigma) = 0$ and $\sigma \in \ker(\mathbb{P}\rho)$. \square

We first study the ramification of $\theta_{f,\lambda}$ at ℓ .

Proposition 5.5. *Assume $\ell \nmid N$ and $\ell > k$. Then, with the terminology of Proposition 1.2, we have the following.*

- (1) *If f is ordinary at λ and $\ell \neq 2k - 1$, then $\theta_{f,\lambda}$ is unramified at ℓ ;*
- (2) *If f is not ordinary at λ and $\ell \neq 2k - 3$, then $\theta_{f,\lambda}$ is unramified at ℓ .*

Proof. We are under the hypotheses of Proposition 1.2.

- If f is ordinary at λ , then we have

$$\bar{\rho}_{f,\lambda|I_\ell} \cong \begin{pmatrix} \bar{\chi}_\ell^{k-1} & \star \\ 0 & 1 \end{pmatrix}.$$

The order of the image of $\mathbb{P}\bar{\rho}_{f,\lambda}$ is prime to ℓ . Therefore, so is the one of $\bar{\rho}_{f,\lambda|I_\ell}$. By Lemma 5.4, we have $\mathrm{Im}(\mathbb{P}\bar{\rho}_{f,\lambda}) \cong \mathrm{Im}(\bar{\chi}_\ell^{k-1})$. The image of $\bar{\chi}_\ell^{k-1}$ is a cyclic group of order $\frac{\ell-1}{\gcd(\ell-1, k-1)}$. If $\ell > k$ and $\ell \neq 2k - 1$, it is greater than 2. Therefore, the image of $\mathbb{P}\bar{\rho}_{f,\lambda}$ is necessarily included in C and $\theta_{f,\lambda}$ is unramified at ℓ .

- If f is not ordinary at λ , then we have

$$\bar{\rho}_{f,\lambda|I_\ell} \cong \begin{pmatrix} \psi^{k-1} & 0 \\ 0 & \psi^{\ell(k-1)} \end{pmatrix}.$$

By Lemma 5.4, $\text{Im}(\mathbb{P}\bar{\rho}_{f,\lambda})$ is isomorphic to the image of $\psi^{(k-1)(\ell-1)}$. It is of order $\frac{\ell+1}{\gcd(\ell+1, k-1)}$ which is again greater than 2 if we assume $\ell > k$ and $\ell \neq 2k-3$. We conclude as before. \square

We now look at the ramification at the primes $p \mid N$, $p \neq \ell$.

Proposition 5.6. *Let p be a prime number dividing N and different from ℓ .*

- (1) *If $v_p(N) = 1$ and $v_p(\mathfrak{c}) = 0$, then $\theta_{f,\lambda}$ is unramified at p .*
- (2) *Assume $v_p(N) = v_p(\mathfrak{c})$. If $\theta_{f,\lambda}$ is ramified at p , then the p -parts of ε and $\theta_{f,\lambda}$ are equal modulo λ (in particular, ε_p has order 2 modulo λ).*

Proof. (1) By Proposition 1.3, the restriction of $\bar{\rho}_{f,\lambda}$ at an inertia subgroup I_p at p , is given by

$$\bar{\rho}_{f,\lambda|I_p} \cong \begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix}.$$

By assumption, the order of image of $\mathbb{P}\bar{\rho}_{f,\lambda}$ is prime to ℓ . Therefore, by Lemma 5.4 $\text{Im}(\mathbb{P}\bar{\rho}_{f,\lambda})$ is trivial, and $\mathbb{P}\bar{\rho}_{f,\lambda}$ is unramified at p , as well as $\theta_{f,\lambda}$.

- (2) By Proposition 1.3, we have

$$\bar{\rho}_{f,\lambda|I_p} \cong 1 \oplus \bar{\varepsilon}_{|I_p}.$$

As a character of $G_{\mathbb{Q}}$, ε factors through the group $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. Moreover, an inertia subgroup at p in $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ is given by the group $\text{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q}(\zeta_{p^{v_p(N)}})) \cong (\mathbb{Z}/p^{v_p(N)}\mathbb{Z})^\times$. Thus, as a Dirichlet character, the restriction of ε to I_p is ε_p . By Lemma 5.4, we thus have $\mathbb{P}\bar{\rho}_{f,\lambda}(I_p) \cong \bar{\varepsilon}_p(I_p)$. If $\theta_{f,\lambda}$ is ramified at p , then its image must have a non-trivial intersection with $D_{2n} \setminus C$. Therefore, it is isomorphic to $\mathbb{Z}/2\mathbb{Z}$. We deduce that the reduction of ε_p modulo λ is of order 2, and that the p -part of $\theta_{f,\lambda}$ corresponds to the reduction of ε_p . \square

5.3. Proof of the main result

In order to prove the main result of this section, consider the form

$$g = f \otimes \theta_{f,\lambda}.$$

It is by construction a newform of weight k , character ε , and we have the following.

Proposition 5.7. *The Galois representations $\bar{\rho}_{f,\lambda}$ and $\bar{\rho}_{g,\lambda}$ are isomorphic.*

Proof. Because f and g have same weight and character, the determinants of $\bar{\rho}_{f,\lambda}$ and $\bar{\rho}_{g,\lambda}$ are the same. Let p be a prime not dividing $N\ell$. By Propositions 5.1 and 5.3, the representations are both unramified at p and their traces at a Frobenius element at p are the reductions modulo λ of $a_p(f)$ and $a_p(g) = \theta_{f,\lambda}(p)a_p(f)$, respectively. If $\theta_{f,\lambda}(p) = 1$, then the traces agree. Else, if $\theta_{f,\lambda}(p) = -1$, then by definition of

$\theta_{f,\lambda}$ we have $\text{Tr}(\overline{\rho}_{f,\lambda}(\text{Frob}_p)) = 0$ and the traces agree again. By Brauer–Nesbitt theorem [11, Lemme 3.2], we have $\overline{\rho}_{f,\lambda} \cong \overline{\rho}_{g,\lambda}$. \square

From now on, let assume that $\ell > k$, $\ell \notin \{2k-1, 2k-3\}$. From Proposition 5.5, it means that the character $\theta_{f,\lambda}$ is unramified at ℓ . The following proposition contains many information about the level and the Fourier coefficients of g .

Proposition 5.8. *Assume that $\ell \nmid N\varphi(N)$. Write N_g for the level of g and let p be a prime number.*

- (i) *If either $p \nmid N$, or $v_p(N) = 1$ and $v_p(\mathfrak{c}) = 0$, then $v_p(N_g) = v_p(N)$ and $a_p(g) = \theta_{f,\lambda}(p)a_p(f)$.*
- (ii) *If $v_p(N) = v_p(\mathfrak{c}) \geq 1$, then $v_p(N_g) = v_p(N)$ and $a_p(g) = \theta_{f,\lambda}(p)a_p(f)$ if $\theta_{f,\lambda}$ is unramified at p , and $a_p(g) = a_p(f)\varepsilon'_p(p)(\theta_{f,\lambda})'_p(p)$ otherwise, where ε'_p and $(\theta_{f,\lambda})'_p$ are the prime-to- p parts of ε and $\theta_{f,\lambda}$, respectively.*
- (iii) *If $v_p(N) \geq 2$ and $v_p(\mathfrak{c}) < v_p(N)$, then $v_p(N_g) \leq v_p(N) + 2\min(v_p(N), v_p(2))$.*

In particular, we have $N_g \mid N \gcd(N, 2)^2$.

Proof. (i) If $p \nmid N$ then $\theta_{f,\lambda}$ is unramified at p by construction if $p \neq \ell$, and by Proposition 5.5 if $p = \ell$. If $v_p(N) = 1$ and $v_p(\mathfrak{c}) = 0$, then by Proposition 5.6, $\theta_{f,\lambda}$ is also unramified at p . By Proposition 5.1, we therefore have $v_p(N_g) = v_p(N)$ and $a_p(g) = \theta_{f,\lambda}(p)a_p(f)$.

(ii) If $v_p(N) = v_p(\mathfrak{c})$. Then either $\theta_{f,\lambda}$ is unramified at p , and we again have $v_p(N_g) = v_p(N)$ and $a_p(g) = \theta_{f,\lambda}(p)a_p(f)$, or it is ramified. In this latter case, by Proposition 5.6, we have $\varepsilon_p \equiv (\theta_{f,\lambda})_p \pmod{\lambda}$. As we assumed $\ell \nmid \varphi(N)$, by Lemma 2.7, we get that ε_p has order 2 and that $(\theta_{f,\lambda})_p = \varepsilon_p = \varepsilon_p^{-1}$. Therefore, by Proposition 5.1, we have $v_p(N_g) = v_p(N)$ and $a_p(g) = \overline{a_p(f)\varepsilon'_p(p)(\theta_{f,\lambda})'_p(p)}$.

(iii) Finally assume $v_p(N) \geq 2$ and $v_p(\mathfrak{c}) < v_p(N)$. If $p \neq 2$, then we have $v_p(\mathfrak{c}_{f,\lambda}) = 1$ and by Proposition 5.1 we find that $v_p(N_g) \leq v_p(N)$. Assume that $p = 2$ and let us look at the Artin conductors of $\overline{\rho}_{f,\lambda}$ and $\overline{\rho}_{g,\lambda}$. By Proposition 5.7, they are equal. Moreover, by Proposition 1.4 the difference between the 2-adic valuations of N and $N(\overline{\rho}_{f,\lambda})$, and of N_g and $N(\overline{\rho}_{g,\lambda})$, respectively, cannot be greater than 2. Therefore, we have

$$v_2(N_g) \leq v_2(N(\overline{\rho}_{g,\lambda})) + 2 = v_2(N(\overline{\rho}_{f,\lambda})) + 2 \leq v_2(N) + 2. \quad \square$$

Finally, consider the set $\mathbf{P} = \{p \text{ prime}, v_p(N) \geq 2 \text{ and } v_p(\mathfrak{c}) < v_p(N)\}$, and with the notations of Corollary 3.26, define

$$h := g_{\mathbf{P}}^{(0)}_{p \in \mathbf{P}}.$$

Proposition 5.9. *Assume that $\ell \nmid N\varphi(N)$. The form h is of weight k , character ε , and level dividing $N \gcd(N, 2)^2$. Moreover, it is a normalized eigenform for all the*

Hecke operators at level $N \gcd(N, 2)^2$ and for all prime numbers p , we have

$$a_p(h) = \begin{cases} a_p(g) & \text{if } p \notin \mathbf{P}, \\ 0 & \text{if } p \in \mathbf{P}. \end{cases}$$

Proof. The computation of the weight and the character of h follows from Corollary 3.26 as well as Fourier coefficients of h . Write N_h for the level of h and N_g for the level of g . With the notations of Corollary 3.26, we have $N_h = N_g \prod_{p \in \mathbf{P}} p^{n_p}$ and h is an eigenform for all the Hecke operators at level N_h . Let us prove that N_h divides $N \gcd(N, 2)^2$.

If $n_p = 0$, there is nothing to do. If $n_p = 2$, then p does not divide the level of g . By definition of \mathbf{P} we have $v_p(N_h) = v_p(N_g) + 2 = 2 \leq v_p(N)$. If $n_p = 1$, then we have $p \mid N_g$ and $a_p(g) \neq 0$. Moreover, the character of g is ε . Therefore, by Proposition 1.1 we cannot have $v_p(N_g) \geq 2$ and $v_p(N_g) > v_p(\mathfrak{c})$. However, by assumption we have $v_p(N) \geq 2$ and $v_p(N) > v_p(\mathfrak{c})$. We conclude that either $v_p(N_g) = v_p(\mathfrak{c}) < v_p(N)$, or $v_p(N_g) \leq 1 < v_p(N)$. In every case we have $v_p(N_h) = v_p(N_g) + 1 \leq v_p(N)$.

Finally, to prove that h is an eigenform for all the Hecke operators at level $N \gcd(N, 2)^2$, we just have to prove that the prime divisors of N_h and $N \gcd(N, 2)^2$ are the same. This is clear from Proposition 5.8 for the prime numbers outside \mathbf{P} . If $p \in \mathbf{P}$, then the p -adic valuation of the level of h is also positive by Corollary 3.26. This finishes the proof. \square

We now prove our main result.

Theorem 5.10. Assume $\bar{\rho}_{f,\lambda}$ has dihedral projective image. If $N = 1$, then we have $\ell \leq k$ or $\ell \in \{2k - 1, 2k - 3\}$. Else, if $N \geq 2$ and f does not have complex multiplication, then we have

$$\ell \leq \left(2N^{\frac{k-1}{2}}\right)^{[K_f:\mathbb{Q}]} \times \max \left(\left(\frac{k}{3} (2 \log \log(N) + 2.4) \right)^{\frac{k-1}{2}}, \left(\frac{5}{2} N^{\frac{k-1}{2}} \right) \right)^{[K_f:\mathbb{Q}]}.$$

Proof. Assume that $\ell > k$, $\ell \notin \{2k - 1, 2k - 3\}$ and $\ell \nmid N\varphi(N)$. If $N = 1$, then $\theta_{f,\lambda}$ is unramified everywhere and thus trivial, which is a contradiction. Assume now that $N \geq 2$. Because f does not have complex multiplication, there exists some prime number p such that $a_p(f) \neq a_p(h)$. Moreover, from Proposition 5.9, f and h are both modular forms of weight k , level $N \gcd(N, 2)^2$, and character ε , that are eigenforms for all the Hecke operators at this level. Therefore, p must be less than $B = \frac{kN \gcd(N, 2)^2}{12} \prod_{q \mid N} \left(1 + \frac{1}{q}\right)$. Indeed, because f and h are cusp eigenforms of the same weight, level and character, if $a_q(f) = a_q(h)$ for all primes $q \leq B$, then we would get $a_n(f) = a_n(h)$ for all integers $n \leq B$, and by Proposition 3.20, $f = h$.

We treat various cases for p .

- If $p = \ell$, then we have $\ell \leq B$.

- If $p \nmid N\ell$, then from Propositions 5.8 and 5.9, we have $a_p(h) = a_p(g) = \theta_{f,\lambda}(p)a_p(f)$. This implies that $\theta_{f,\lambda}(p) = -1$ and by Proposition 5.7, we get $a_p(f) \equiv 0 \pmod{\lambda}$.
- If $v_p(N) \geq 2$ and $v_p(N) > v_p(\mathfrak{c})$, then by Propositions 1.1 and 5.9, we have $a_p(f) = 0 = a_p(h)$. We cannot have $a_p(f) \neq a_p(h)$ in this situation.
- If $v_p(N) = 1$ and $v_p(\mathfrak{c}) = 0$, then by Propositions 5.8 and 5.9, we have $a_p(h) = a_p(g) = \theta_{f,\lambda}(p)a_p(f)$ and $v_p(N_g) = 1$. Therefore, we have $\theta_{f,\lambda}(p) = -1$ and by Propositions 1.3 and 5.7, we get

$$\begin{pmatrix} pa_p(f) & \star \\ 0 & a_p(f) \end{pmatrix} \cong \begin{pmatrix} -pa_p(f) & \star \\ 0 & -a_p(f) \end{pmatrix}.$$

Hence, we either have $a_p(f) \equiv 0 \pmod{\lambda}$, or $p+1 \equiv 0 \pmod{\ell}$.

- Finally, assume that $v_p(N) = v_p(\mathfrak{c})$. By Propositions 5.8 and 5.9, we have $a_p(h) = a_p(g)$ and $v_p(N_g) = v_p(N)$. Therefore, by Propositions 5.7 and 1.3, we have an isomorphism of representations of G_p :

$$\mu(a_p(f)) \oplus \mu(a_p(f))\overline{\chi_\ell^{k-1}\varepsilon_{|G_p}} \cong \mu(a_p(h)) \oplus \mu(a_p(h))\overline{\chi_\ell^{k-1}\varepsilon_{|G_p}}.$$

The second character of each representation is ramified at p , while the first is not. We deduce that we have $a_p(f) \equiv a_p(h) \pmod{\mathfrak{L}}$.

If $\theta_{f,\lambda}$ is unramified at p , we have by Proposition 5.8, $a_p(h) = \theta_{f,\lambda}(p)a_p(f)$, and therefore $\theta_{f,\lambda}(p) = -1$ and $a_p(f) \equiv 0 \pmod{\lambda}$.

If $\theta_{f,\lambda}$ is ramified at p , we have from Propositions 5.8 and 5.9,

$$a_p(h) = \varepsilon'_p(p)(\theta_{f,\lambda})'_p(p)\overline{a_p(f)} \equiv a_p(f) \pmod{\lambda}.$$

We moreover know from Proposition 1.1 that $a_p(f)\overline{a_p(f)} = p^{k-1}$. Therefore, we get that $a_p(f)^2 \equiv \varepsilon'_p(p)(\theta_{f,\lambda})'_p(p)p^{k-1} \pmod{\lambda}$.

To sum up, we have either $\ell \leq B$, or $a_p(f) \equiv 0 \pmod{\lambda}$, or $p \mid N$ and $p+1 \equiv 0 \pmod{\ell}$, or $p \mid N$ and $a_p(f)^2 \equiv \varepsilon'_p(p)^2(\theta_{f,\lambda})'_p(p)p^{k-1} \pmod{\lambda}$. Using Deligne's bounds for the coefficients of a newform (see [10, Théorème 8.2]) and Lemma 3.22, this means that either $\ell \leq N+1$, or

$$\begin{aligned} \ell \mid |\text{Norm}(a_p(f))| &= \prod_{\sigma: K_f \hookrightarrow \mathbb{C}} |\sigma(a_p(f))| \\ &\leq (2p^{\frac{k-1}{2}})^{[K_f:\mathbb{Q}]} \\ &\leq (2N^{\frac{k-1}{2}})^{[K_f:\mathbb{Q}]} \left(\frac{k}{3} (2 \log \log(N) + 2.4) \right)^{\frac{k-1}{2} [K_f:\mathbb{Q}]}, \end{aligned}$$

or

$$\begin{aligned} \ell \mid |\text{Norm}(a_p(f)^2 - \varepsilon'_p(p)^2(\theta_{f,\lambda})'_p(p)p^{k-1})| \\ \leq \prod_{\sigma: K_f \hookrightarrow \mathbb{C}} (|\sigma(a_p(f)^2)| + p^{k-1}) \end{aligned}$$

$$\begin{aligned} &\leq (5p^{k-1})^{[K_f:\mathbb{Q}]} \\ &\leq (5N^{k-1})^{[K_f:\mathbb{Q}]} \\ &\leq (2N^{\frac{k-1}{2}})^{[K_f:\mathbb{Q}]} \times \left(\frac{5}{2}N^{\frac{k-1}{2}}\right)^{[K_f:\mathbb{Q}]} . \end{aligned}$$

We therefore get the wanted result. \square

6. Numerical Applications

6.1. Checking the reducibility

We explain here how to use Theorems 4.15 and 4.20 to explicitly compute the prime ideals λ for which the representation $\bar{\rho}_{f,\lambda}$ is reducible. We begin by discussing the dependency of the set $R_{N,k,\varepsilon}(\mathfrak{L})$ (see Definition 4.8) in the place \mathfrak{L} .

Proposition 6.1. *Let $N \geq 1$ and $k \geq 2$ be integers, and let ε be a Dirichlet character modulo N . Let ℓ be a prime number and let \mathfrak{L} be a place of $\overline{\mathbb{Q}}$ above ℓ . The set $R_{N,k,\varepsilon}(\mathfrak{L})$ depends only on $\mathfrak{L} \cap \mathbb{Q}(\varepsilon)$ (and on N , k and ε).*

Proof. Write $\pi_{\mathfrak{L}}$ for the projection modulo \mathfrak{L} , and $T_{\mathfrak{L}}$ for the associated Teichmüller lift (see Sec. 2.2). Recall that for $x \in \overline{\mathbb{F}}_{\ell}^{\times}$, $T_{\mathfrak{L}}(x)$ is the only root of unity of order prime to ℓ and such that $\pi_{\mathfrak{L}}(T_{\mathfrak{L}}(x)) = x$.

We first prove that the map $T_{\mathfrak{L}} \circ \pi_{\mathfrak{L}}$ depends only on ℓ . Let ζ be a root of unity of order $n = \ell^m q$ with $m \geq 0$ and $\ell \nmid q$. We can then write $\zeta = \zeta^{\ell^m a} \cdot \zeta^{qb}$, with $\ell \nmid b$ and a prime to q . Because ζ is a root of unity of order n , $\zeta^{\ell^m a}$ is a root of unity of order q and ζ^{qb} is a root of unity of order ℓ^m . From Lemma 2.7, we get $\zeta \equiv \zeta^{\ell^m a} \pmod{\mathfrak{L}}$, and $T_{\mathfrak{L}} \circ \pi_{\mathfrak{L}}(\zeta) = \zeta^{\ell^m a}$. Therefore, it depends only on ℓ .

Let $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\mathfrak{L})$. The only dependency on the place \mathfrak{L} is the congruence

$$\overline{\chi}_{\ell}^{k-1} \varepsilon \equiv \overline{\chi}_{\ell}^{m_1+m_2} \varepsilon_1 \varepsilon_2 \pmod{\mathfrak{L}}.$$

Decompose ε as $\varepsilon_{\ell} \varepsilon'$, where ε_{ℓ} is the ℓ -part of ε , and ε' is unramified at ℓ . Looking at the ℓ -part of the congruence in one hand, and at the prime-to- ℓ part in another hand, the congruence is equivalent to

$$\overline{\chi}_{\ell}^{k-1} \varepsilon_{\ell} \equiv \overline{\chi}_{\ell}^{m_1+m_2} \pmod{\mathfrak{L}} \quad \text{and} \quad \varepsilon' \equiv \varepsilon_1 \varepsilon_2 \pmod{\mathfrak{L}}. \quad (6.1)$$

Applying $T_{\mathfrak{L}}$ to the second equation, we get $T_{\mathfrak{L}} \circ \pi_{\mathfrak{L}}(\varepsilon') = T_{\mathfrak{L}} \circ \pi_{\mathfrak{L}}(\varepsilon_1 \varepsilon_2)$. We have seen that this depends only on ℓ . Let us look at the first equation. The projection of ε_{ℓ} modulo \mathfrak{L} depends only on $\mathfrak{L} \cap \mathbb{Q}(\varepsilon)$. Moreover, $\pi_{\mathfrak{L}}(\varepsilon_{\ell})$ is a character modulo \mathfrak{L} of conductor ℓ . Therefore, there exists an integer k_{ℓ} between 0 and $\ell - 1$, depending only on $\mathfrak{L} \cap \mathbb{Q}(\varepsilon)$, such that $\pi_{\mathfrak{L}}(\varepsilon_{\ell}) = \overline{\chi}_{\ell}^{k_{\ell}}$. The equation $\overline{\chi}_{\ell}^{k-1} \varepsilon_{\ell} \equiv \overline{\chi}_{\ell}^{m_1+m_2} \pmod{\mathfrak{L}}$ is therefore equivalent to $k + k_{\ell} - 1 \equiv m_1 + m_2 \pmod{\ell - 1}$ and depends only on $\mathfrak{L} \cap \mathbb{Q}(\varepsilon)$. \square

Notice that we have in fact proved that $R_{N,k,\varepsilon}(\mathfrak{L})$ depends only on $\mathfrak{L} \cap \mathbb{Q}(T_{\mathfrak{L}} \circ \pi_{\mathfrak{L}}(\varepsilon_{\ell}))$ but we will only use what we have stated. A practical application of this result is that we can compute the set $R_{N,k,\varepsilon}(\mathfrak{L})$ while knowing only a prime ideal λ below \mathfrak{L} in a finite extension of $\mathbb{Q}(\varepsilon)$, like K_f for example. For λ a prime ideal in an extension of $\mathbb{Q}(\varepsilon)$, we will freely write $R_{N,k,\varepsilon}(\lambda)$ for the set $R_{N,k,\varepsilon}(\mathfrak{L})$ for any place \mathfrak{L} above λ . We also deduce from Proposition 6.1, a procedure to compute $R_{N,k,\varepsilon}(\lambda)$:

Algorithm 6.2. Input: Two integers $N \geq 1$, $k \geq 2$, a Dirichlet character ε modulo N , and a prime ideal λ in a finite extension of $\mathbb{Q}(\varepsilon)$ above a prime number ℓ .

Output: The set $R_{N,k,\varepsilon}(\lambda)$.

- (1) Compute ε_{ℓ} and ε' , the ℓ -part and prime-to- ℓ part of ε , respectively.
- (2) Compute the unique Dirichlet character ε'' modulo N such that ε'' has prime-to- ℓ order, is unramified at ℓ and $\varepsilon'\varepsilon''^{-1}$ has order a power of ℓ . This corresponds to the character $T_{\mathfrak{L}} \circ \pi_{\mathfrak{L}}(\varepsilon')$ for any place \mathfrak{L} above λ .
- (3) Compute the integers k_{ℓ} such that $0 \leq k_{\ell} \leq \ell - 2$ and for all integer $1 \leq n \leq N$ prime to N , $\varepsilon_{\ell}(n) \equiv n^{k_{\ell}} \pmod{\lambda}$. We then have $\varepsilon_{\ell} \equiv \overline{\chi}_{\ell}^{k_{\ell}} \pmod{\lambda}$.
- (4) Compute the set $M_{N,k,\varepsilon}(\lambda)$ of pairs of integers (m_1, m_2) such that $0 \leq m_1 \leq m_2 < \ell - 1$ and $m_1 + m_2 \equiv k + k_{\ell} - 1 \pmod{\ell - 1}$.
- (5) Compute the set $E_{N,k,\varepsilon}(\lambda)$ of pairs of Dirichlet characters $(\varepsilon_1, \varepsilon_2)$ of conductor (c_1, c_2) and such that ε_1 and ε_2 have prime-to- ℓ order, are unramified at ℓ , satisfy $\varepsilon_1 \varepsilon_2 = \varepsilon''$ and for all primes $p \neq \ell$, we have $v_p(\frac{N}{c_1 c_2}) \in \{0, 1, 2\}$.
- (6) Return the set $E_{N,k,\varepsilon}(\lambda) \times M_{N,k,\varepsilon}(\lambda) = R_{N,k,\varepsilon}(\lambda)$.

We now give the two main algorithms that follows from Theorems 4.20 and 4.15, respectively. The first algorithm computes the prime ideals λ of \mathcal{O}_f , of residual characteristic ℓ such that $\ell > k + 1$ and $\ell \nmid N\varphi(N)$, for which $\overline{\rho}_{f,\lambda}$ is reducible, together with the description of $\overline{\rho}_{f,\lambda}$. The correctness of the algorithm is granted by Theorem 4.20.

Algorithm 6.3. Input: A newform f , described by its Fourier coefficients $(a_n(f))_{n \geq 0}$ as elements of the number field K_f , together with its level N , weight k , and character ε .

Output: The set of prime ideals λ of \mathcal{O}_f of residual characteristic ℓ such that $\ell > k + 1$ and $\ell \nmid N\varphi(N)$, for which $\overline{\rho}_{f,\lambda}$ is reducible, together with the shape of $\overline{\rho}_{f,\lambda}$.

- (1) Set $\text{Red}(f) = \emptyset$.
- (2) Compute the set $R_{N,\varepsilon}$ (see Definition 4.17).
- (3) For $(\varepsilon_1, \varepsilon_2) \in R_{N,\varepsilon}$,
 - (a) Compute r , C , and B defined in (4.2), and Theorem 4.20, respectively.
 - (b) Compute the set $P(\varepsilon_1, \varepsilon_2)$ of prime divisors of the gcd of the algebraic norms of
 - C ;

- $a_p(f) - \varepsilon_1(p) - p^{k-1}\varepsilon_2(p)$, for $p \nmid Nr$, $p \leq B$;
- and $a_p(f)(a_p(f) - \varepsilon_1(p))(a_p(f) - p^{k-1}\varepsilon_2(p))$, for $p \mid N$, $p \nmid r$, $p \leq B$,

that are bigger than $k+1$ and do not divide $N\varphi(N)$. By Theorem 4.20, these are the only prime numbers bigger than $k+1$ and not dividing $N\varphi(N)$ for which $\overline{\rho}_{f,\lambda}$ can be reducible.

- (4) For $(\varepsilon_1, \varepsilon_2) \in R_{N,\varepsilon}$ and for $\ell \in P(\varepsilon_1, \varepsilon_2)$,
 - (a) Compute the prime ideals λ of \mathcal{O}_f above ℓ .
 - (b) For each such λ , compute a prime ideal \mathfrak{L} in the ring of integers of $K_f(\varepsilon_1, \varepsilon_2)$ above λ .
 - (c) For each such \mathfrak{L} , check the following congruences.
 - $C \equiv 0 \pmod{\mathfrak{L}}$;
 - $a_p(f) \equiv \varepsilon_1(p) + p^{k-1}\varepsilon_2(p) \pmod{\mathfrak{L}}$ for all $p \nmid Nr$, $p \leq B$;
 - $a_p(f)(a_p(f) - \varepsilon_1(p))(a_p(f) - p^{k-1}\varepsilon_2(p)) \equiv 0 \pmod{\mathfrak{L}}$ for all $p \mid N$, $p \nmid r$, $p \leq B$.

If they all hold, add $(\lambda, \varepsilon_1, \varepsilon_2, 0, k-1)$ to $\text{Red}(f)$. By Theorem 4.20, $\overline{\rho}_{f,\lambda}$ is reducible and we have $\overline{\rho}_{f,\lambda} \cong \overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{k-1}\overline{\varepsilon}_2$.

- (5) Return $\text{Red}(f)$.

We now turn to the computation of the reducible primes of residue characteristic ℓ such that $\ell \leq k+1$ or $\ell \mid N\varphi(N)$. The correctness of the following algorithm follows by Theorem 4.15.

Algorithm 6.4. Input: A newform f , described by its Fourier coefficients $(a_n(f))_{n \geq 0}$ as elements of the number field K_f , together with its level N , weight k , and character ε .

Output: The set of prime ideals λ of \mathcal{O}_f of residual characteristic ℓ such that $\ell \leq k+1$ or $\ell \mid N\varphi(N)$, for which $\overline{\rho}_{f,\lambda}$ is reducible, together with the shape of $\overline{\rho}_{f,\lambda}$.

- (1) Set $\text{Red}(f) = \emptyset$.
- (2) Compute the set P of prime numbers ℓ such that $\ell \leq k+1$ or $\ell \mid N\varphi(N)$.
- (3) For each $\ell \in P$, compute the set $P(\ell)$ of prime ideals λ in \mathcal{O}_f above ℓ .
- (4) For each $\ell \in P$ and for each $\lambda \in P(\ell)$, compute $R_{N,k,\varepsilon}(\lambda)$ using Algorithm 6.2.
We can do this because we have $\mathbb{Q}(\varepsilon) \subset K_f$.
- (5) For each $\ell \in P$, for each $\lambda \in P(\ell)$, and for each $(\varepsilon_1, \varepsilon_2, m_1, m_2) \in R_{N,k,\varepsilon}(\lambda)$,
 - (a) Compute a prime ideal \mathfrak{L} in the ring of integers of $K_f(\varepsilon_1, \varepsilon_2)$ above λ .
 - (b) Compute r and B defined in (4.2) and Theorem 4.15, respectively.
 - (c) Check the following congruences.
 - $a_p(f) \equiv p^{m_1}\varepsilon_1(p) + p^{m_2}\varepsilon_2(p) \pmod{\mathfrak{L}}$ for all $p \nmid Nr$, $p \leq B$;
 - $a_p(f)(a_p(f) - p^{m_1}\varepsilon_1(p))(a_p(f) - p^{m_2}\varepsilon_2(p)) \equiv 0 \pmod{\mathfrak{L}}$ for all $p \mid N$, $p \nmid r$, $p \leq B$.

If they all hold, add $(\lambda, \varepsilon_1, \varepsilon_2, m_1, m_2)$ to $\text{Red}(f)$. By Theorem 4.15, $\overline{\rho}_{f,\lambda}$ is reducible and we have $\overline{\rho}_{f,\lambda} \cong \overline{\chi}_\ell^{m_1} \overline{\varepsilon}_1 \oplus \overline{\chi}_\ell^{m_2} \overline{\varepsilon}_2$.

(6) Return $\text{Red}(f)$.

The correctness of Algorithms 6.3 and 6.4 follows directly from Theorems 4.20 and 4.15, respectively. The most time-consuming computation is step 3(b) of Algorithm 6.3. This depends on the size of the “big” reducible primes. We have implemented these algorithms in PARI/GP [36], and we have been able to execute them as long as the degree of K_f keeps reasonable (say $[K_f : \mathbb{Q}] \leq 20$). The second limiting factor being the weight k that controls the size of the Fourier coefficients of f . Our code is available on GitHub at the following address:

<https://github.com/bpeaucelle/mfreducible>

6.2. Numerical examples

We present here some examples of applications of the algorithms described above to compute the reducible primes of a given newform. Throughout this section, we use the Conrey representation $(\varepsilon_a(b))_{b \wedge a=1}$ for the Dirichlet characters of modulus a . This is the way they are described in the LMFDB for example (and in some extent in PARI/GP). Notice that there would be no possible confusion with the characters $\varepsilon_1, \varepsilon_2$ from the algorithms above.

6.2.1. A concrete example

Consider the space $S_7^{\text{new}}(7, \varepsilon_7(3))$. It has dimension 6 over \mathbb{C} and is generated by 2 newforms, f_1 and f_2 , up to conjugation by $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\varepsilon_7(3)))$. We have $K_{f_1} = \mathbb{Q}[t]/(t^2 - t + 1)$ and $K_{f_2} = \mathbb{Q}[x]/(x^4 + 2x^2 + 4)$. Notice that $(1, x, \frac{x^2}{2}, \frac{x^3}{2})$ is an integer basis of \mathcal{O}_{f_2} , and that $\varepsilon_7(3)$ sends 3 to t in K_{f_1} and to $-\frac{x^2}{2}$ in K_{f_2} . The q -expansions of f_1 and f_2 are given by

$$\begin{aligned} f_1 &= q + 12tq^2 + (-7t - 7)q^3 + (80t - 80)q^4 + (-105t + 210)q^5 \\ &\quad + (-168t + 84)q^6 - 343q^7 + O(q^8), \\ f_2 &= q + \left(\frac{3}{2}x^3 + 2x^2 + 3x\right)q^2 + \left(13x^3 - \frac{3}{2}x^2 + 13x + 3\right)q^3 \\ &\quad + (15x^2 - 24x + 30)q^4 + \left(-25x^3 - \frac{25}{2}x^2 + 50x - 50\right)q^5 + O(q^6). \end{aligned}$$

The set of prime numbers less than $k + 1 = 8$ or dividing $N\varphi(N) = 42$ is therefore $\{2, 3, 5, 7\}$. We treat those primes separately in what follows.

- $\ell = 2$: The ideal $2\mathcal{O}_{f_1}$ is prime and we have $2\mathcal{O}_{f_2} = ((x, 2)\mathcal{O}_{f_2})^2$. Because, the ideal generated by 2 in $\mathbb{Z}[\varepsilon_7(3)]$ is prime, we have

$$R_{7,7,\varepsilon_7(3)}(2\mathcal{O}_{f_1}) = R_{7,7,\varepsilon_7(3)}((2, x)\mathcal{O}_{f_2}) = \{(\mathbb{1}, \varepsilon_7(4), 0, 0); (\varepsilon_7(4), \mathbb{1}, 0, 0)\}.$$

In fact, the two elements of this set give rise to the same representation. We only study the case $(\varepsilon_1, \varepsilon_2, m_1, m_2) = (\varepsilon_7(4), \mathbb{1}, 0, 0)$. According to Theorem 4.15, we have

$$k' = 2, \quad r = 1, \quad N' = 7, \quad a = 0, \quad b = 3, \quad \tilde{k} = 10, \quad B = 6 + \frac{2}{3}.$$

To check the reducibility of $\bar{\rho}_{f_1, (2)}$ and $\bar{\rho}_{f_2, (2, x)}$ we only have to check the third and fifth coefficients of f_1 and f_2 . The table below shows the reduction modulo the prime ideals above of $a_p(f_i) - 1 - \varepsilon_7(4)(p)$ for $i = 1, 2$, and $p = 3, 5$. From Theorem 4.15, we know that $\bar{\rho}_{f_i, \lambda}$ is reducible if and only if the row corresponding to f_i contains only zeros.

p	3	5
$a_p(f_1) - (1 + \varepsilon_7(4)(p)) \pmod{2}$	0	0
$a_p(f_2) - (1 + \varepsilon_7(4)(p)) \pmod{(2, x)}$	0	0

Therefore, we have $\bar{\rho}_{f_1, (2)} \cong \mathbb{1} \oplus \overline{\varepsilon_7(4)}$ and $\bar{\rho}_{f_2, (2, x)} \cong \mathbb{1} \oplus \overline{\varepsilon_7(4)}$.

- $\ell = 3$: We have $3\mathcal{O}_{f_1} = ((3, t+1)\mathcal{O}_{f_1})^2$ and $3\mathcal{O}_{f_2} = ((3, x^2+1)\mathcal{O}_{f_2})^2$. As for $\ell = 2$, the ideal generated by 3 in $\mathbb{Z}[\varepsilon_7(3)]$ is prime. Therefore, we have

$$\begin{aligned} R_{7, 7, \varepsilon_7(3)}((3, t+1)\mathcal{O}_{f_1}) &= R_{7, 7, \varepsilon_7(3)}((3, x^2+1)\mathcal{O}_{f_2}) \\ &= \{(\mathbb{1}, \varepsilon_7(6)); (\varepsilon_7(6), \mathbb{1})\} \times \{(0, 0); (1, 1)\}. \end{aligned}$$

As above, we treat only the cases $(\varepsilon_1, \varepsilon_2, m_1, m_2) = (\varepsilon_7(6), \mathbb{1}, 0, 0)$ and $(\varepsilon_7(6), \mathbb{1}, 1, 1)$. According to Theorem 4.15, we have in both cases

$$k' = 1, \quad r = 1, \quad N' = 7, \quad a = 0, \quad b = 4, \quad \tilde{k} = 11, \quad B = 7 + \frac{1}{3}.$$

We have to look at the second, fifth and seventh coefficients of f_1 and f_2 . Let look at the second and fifth first.

p	2	5
$a_p(f_1) - (1 + \varepsilon_7(6)(p)) \pmod{(3, t+1)}$	1	0
$a_p(f_1) - (p + p\varepsilon_7(6)(p)) \pmod{(3, t+1)}$	2	0
$a_p(f_2) - (1 + \varepsilon_7(6)(p)) \pmod{(3, x^2+1)}$	2	0
$a_p(f_2) - (p + p\varepsilon_7(6)(p)) \pmod{(3, x^2+1)}$	0	0

From these computations, we deduce that the only representation that can be reducible is $\bar{\rho}_{f_2, (3, x^2+1)}$, and that it can only be isomorphic to $\overline{\chi_3} \oplus \overline{\chi_3 \varepsilon_7(6)}$. To confirm this isomorphism, we finally have to check that there exists some $b_7 \in \{0, 7, 7\varepsilon_7(6)(7)\} = \{0, 7\}$ such that $a_7(f_2) \equiv 7b_7 \pmod{(3, x^2+1)}$.

We find that we have $a_7(f_2) \equiv 7 \pmod{(3, x^2 + 1)}$. Therefore, the representation $\bar{\rho}_{f_1, (3, t+1)}$ is irreducible, and we have $\bar{\rho}_{f_2, (3, x^2+1)} \cong \bar{\chi}_3 \oplus \bar{\chi}_3 \overline{\varepsilon_7(6)}$.

- $\ell = 5$: We have that 5 is prime in \mathcal{O}_{f_1} and $5\mathcal{O}_{f_2} = (5, x^2 - 2x - 2)(5, x^2 + 2x - 2)$. There is again only one prime ideal above 5 in $\mathbb{Z}[\varepsilon_7(3)]$ and we have

$$\begin{aligned} R_{7,7,\varepsilon_7(3)}(5\mathcal{O}_{f_1}) &= R_{7,7,\varepsilon_7(3)}(5, x^2 \pm 2x - 2) \\ &= \{(\mathbf{1}, \varepsilon_7(3)); (\varepsilon_7(3), \mathbf{1})\} \times \{(0, 2); (1, 1)\}. \end{aligned}$$

Looking at the congruences at $p = 3$ for f_1 and $p = 2$ for f_2 , we have

$$\begin{aligned} a_3(f_1) - (1 + 3^2\varepsilon_7(3)(3)) &\equiv 4t + 2 \pmod{5}, \\ a_3(f_1) - (\varepsilon_7(3)(3) + 3^2) &\equiv 2t + 4 \pmod{5}, \\ a_2(f_2) - (1 + 2^2\varepsilon_7(3)(2)) &\equiv \begin{cases} 2 & \pmod{(5, x^2 - 2x - 2)}, \\ 4x & \pmod{(5, x^2 + 2x - 2)}, \end{cases} \\ a_2(f_2) - (\varepsilon_7(3)(2) + 2^2) &\equiv \begin{cases} 2x + 3 & \pmod{(5, x^2 - 2x - 2)}, \\ 2x + 1 & \pmod{(5, x^2 + 2x - 2)}, \end{cases} \\ a_2(f_2) - (2 + 2\varepsilon_7(3)(2)) &\equiv \begin{cases} 3x + 2 & \pmod{(5, x^2 - 2x - 2)}, \\ x & \pmod{(5, x^2 + 2x - 2)}. \end{cases} \end{aligned}$$

The only candidate remaining is $(\varepsilon_7(3), \mathbf{1}, 1, 1)$ for $\bar{\rho}_{f_1, (5)}$ (and $(\mathbf{1}, \varepsilon_7(3), 1, 1)$ which gives the same representation). We have

$$k' = 1, \quad r = 1, \quad N' = 7, \quad a = 0, \quad b = 6, \quad \tilde{k} = 13, \quad B = 8 + \frac{2}{3}.$$

We check the second, third and seventh coefficients, and we get

$$\begin{aligned} a_2(f_1) &\equiv 2 + 2\varepsilon_7(3)(2) \pmod{5}, \\ a_3(f_1) &\equiv 3 + 3\varepsilon_7(3)(3) \pmod{5}, \\ a_7(f_1) &\equiv 7 \pmod{5}. \end{aligned}$$

Therefore, the representations $\bar{\rho}_{f_2, (5, x^2 - 2x - 2)}$ and $\bar{\rho}_{f_2, (5, x^2 + 2x - 2)}$ are irreducible, and we have an isomorphism $\bar{\rho}_{f_1, (5)} \cong \bar{\chi}_5 \oplus \bar{\chi}_5 \overline{\varepsilon_7(3)}$.

- $\ell = 7$: We have $7\mathcal{O}_{f_1} = (7, t - 5)(7, t - 3)$ and $7\mathcal{O}_{f_2} = (7, x - 1)(7, x - 2)(7, x + 2)(7, x + 1)$. This time 7 decomposes in $\mathbb{Z}[\varepsilon_7(3)]$ and we have

$$\begin{aligned} R_{7,7,\varepsilon_7(3)}(7, t - 3) &= R_{7,7,\varepsilon_7(3)}(7, x \pm 1) \\ &= \{(\mathbf{1}, \mathbf{1})\} \times \{(0, 1); (2, 5); (3, 4)\} \quad \text{and} \\ R_{7,7,\varepsilon_7(3)}(7, t - 5) &= R_{7,7,\varepsilon_7(3)}(7, x \pm 2) \\ &= \{(\mathbf{1}, \mathbf{1})\} \times \{(0, 5); (1, 4); (2, 3)\}. \end{aligned}$$

For f_1 , looking at $p = 2$ leaves us only with $(\varepsilon_1, \varepsilon_2, m_1, m_2) = (1, 1, 2, 5)$ for the ideal $(7, t - 3)$ and $(1, 1, 1, 4)$ for $(7, t - 5)$. In both cases we have to look at congruences up to $p = 5$, and we get

$$\bar{\rho}_{f_1, (7, t-3)} \cong \bar{\chi}_7^2 \oplus \bar{\chi}_7^5 \quad \text{and} \quad \bar{\rho}_{f_1, (7, t-5)} \cong \bar{\chi}_7 \oplus \bar{\chi}_7^4.$$

For f_2 , looking at $p = 3$ leaves us with $(1, 1, 2, 5)$ for $(7, x + 1)$, $(1, 1, 1, 4)$ for $(7, x + 2)$, $(1, 1, 2, 3)$ for $(7, x - 2)$, and $(1, 1, 3, 4)$ for $(7, x - 1)$. In the first two cases we have $r = 1$, and we have to look at congruences up to $p = 5$. In the last two cases we have $r = 4$, and we have to check congruences up to $p = 53$ and $p = 67$, respectively. In every case, Theorem 4.15 shows that the corresponding representation is reducible. To sum up we have

$$\begin{aligned} \bar{\rho}_{f_2, (7, x-1)} &\cong \bar{\chi}_7^3 \oplus \bar{\chi}_7^4, & \bar{\rho}_{f_2, (7, x+1)} &\cong \bar{\chi}_7^2 \oplus \bar{\chi}_7^5, \\ \bar{\rho}_{f_2, (7, x-2)} &\cong \bar{\chi}_7^2 \oplus \bar{\chi}_7^3, & \bar{\rho}_{f_2, (7, x+2)} &\cong \bar{\chi}_7 \oplus \bar{\chi}_7^4. \end{aligned}$$

We finally look at the prime numbers $\ell > 7$. We have

$$R_{7, \varepsilon_7(3)} = \{(\mathbf{1}, \varepsilon_7(3)), (\varepsilon_7(3), \mathbf{1})\}.$$

Let $(\varepsilon_1, \varepsilon_2) \in R_{7, \varepsilon_7(3)}$. We have $r = 1$, $N' = 1$, $B = 4 + \frac{1}{3}$, and

$$C(\varepsilon_1, \varepsilon_2) = \begin{cases} 0 & \text{if } (\varepsilon_1, \varepsilon_2) = (\varepsilon_7(3), \mathbf{1}); \\ -\frac{B_{7, \varepsilon_7(3)}}{14} a_7(f_i)^2 & \text{if } (\varepsilon_1, \varepsilon_2) = (\mathbf{1}, \varepsilon_7(3)). \end{cases}$$

We first look at f_1 . We find that 43 is the only prime factor greater than 7 of the gcd of the algebraic norms of $C(\varepsilon_1, \varepsilon_2)$ and $a_p(f_1) - \varepsilon_1(p) - p^6 \varepsilon_2(p)$, for $p = 2, 3$. In \mathcal{O}_{f_1} we have $43\mathcal{O}_{f_1} = (43, t - 7)(43, t + 6)$ and we get the following table.

$(\varepsilon_1, \varepsilon_2)$	$(\mathbf{1}, \varepsilon_7(3))$		$(\varepsilon_7(3), \mathbf{1})$	
	$C(\mathbf{1}, \varepsilon_7(3))$	$a_p(f_1) - 1 - p^6 \varepsilon_7(3)(p)$		$a_p(f_1) - \varepsilon_7(3)(p) - p^6$
		$p = 2$	$p = 3$	$p = 2$ $p = 3$
$(43, t - 7)$	0	0	0	14 25
$(43, t + 6)$	40	31	22	0 0

Therefore, we get $\bar{\rho}_{f_1, (43, t-7)} \cong \mathbf{1} \oplus \overline{\chi_{43}^6 \varepsilon_7(3)}$ and $\bar{\rho}_{f_1, (43, t+6)} \cong \overline{\varepsilon_7(3)} \oplus \bar{\chi}_{43}^6$.

We now turn to f_2 . Computing again the gcd of the algebraic norm of $C(\varepsilon_1, \varepsilon_2)$ and $a_p(f_2) - \varepsilon_1(p) - p^7 \varepsilon_2(p)$, for $p = 2, 3$, we find that the only possible residue characteristics are 97 and 3919. We have the following decompositions in \mathcal{O}_{f_2} :

$$97\mathcal{O}_{f_2} = (97, x - 19)(97, x - 5)(97, x + 5)(97, x + 19),$$

$$3919\mathcal{O}_{f_2} = (3919, x - 934)(3919, x - 621)(3919, x + 621)(3919, x + 934).$$

$(\varepsilon_1, \varepsilon_2)$	$(\mathbb{1}, \varepsilon_7(3))$			$(\varepsilon_7(3), \mathbb{1})$	
	$C(\mathbb{1}, \varepsilon_7(3))$	$a_p(f_2) - 1 - p^6 \varepsilon_7(3)(p)$		$a_p(f_2) - \varepsilon_7(3)(p) - p^6$	
		$p = 2$	$p = 3$	$p = 2$	$p = 3$
$(97, x - 19)$	9	33	75	30	57
$(97, x - 5)$	0	0	0	8	66
$(97, x + 5)$	0	80	15	88	81
$(97, x + 19)$	11	3	18	0	0
$(3919, x - 934)$	3160	3231	1337	0	0
$(3919, x - 621)$	0	0	0	3042	609
$(3919, x + 621)$	0	1685	2010	808	2619
$(3919, x + 934)$	1455	3038	3047	3726	1710

Therefore, the representations $\overline{\rho}_{f_2, (97, x-19)}$, $\overline{\rho}_{f_2, (97, x+5)}$, $\overline{\rho}_{f_2, (3919, x+621)}$ and $\overline{\rho}_{f_2, (3919, x+934)}$ are irreducible, and we have

$$\begin{aligned} \overline{\rho}_{f_2, (97, x-5)} &\cong \mathbb{1} \oplus \overline{\chi_{97}^6 \varepsilon_7(3)}, & \overline{\rho}_{f_2, (97, x+19)} &\cong \overline{\varepsilon_7(3)} \oplus \overline{\chi_{97}^6}, \\ \overline{\rho}_{f_2, (3919, x-934)} &\cong \overline{\varepsilon_7(3)} \oplus \overline{\chi_{3919}^6}, & \overline{\rho}_{f_2, (3919, x-621)} &\cong \mathbb{1} \oplus \overline{\chi_{3919}^6 \varepsilon_7(3)}. \end{aligned}$$

The following table sums up all the cases for which $\overline{\rho}_{f_i, \lambda}$ is reducible.

ℓ	f_1		f_2			
2	(2) $\mathbb{1} \oplus \overline{\varepsilon_7(4)}$		(2, x) $\mathbb{1} \oplus \overline{\varepsilon_7(4)}$			
3	Irreducible		(3, $x^2 + 1$) $\overline{\chi}_3 \oplus \overline{\chi}_3 \overline{\varepsilon_7(6)}$			
5	(5) $\overline{\chi}_5 \oplus \overline{\chi}_5 \overline{\varepsilon_7(3)}$		Irreducible			
7	(7, $t - 3$) $\overline{\chi}_7^2 \oplus \overline{\chi}_7^5$	(7, $t - 5$) $\overline{\chi}_7 \oplus \overline{\chi}_7^4$	(7, $x - 2$) $\overline{\chi}_7^2 \oplus \overline{\chi}_7^3$	(7, $x - 1$) $\overline{\chi}_7^3 \oplus \overline{\chi}_7^4$	(7, $x + 1$) $\overline{\chi}_7^2 \oplus \overline{\chi}_7^5$	(7, $x + 2$) $\overline{\chi}_7 \oplus \overline{\chi}_7^4$
$\ell > k + 1$	(43, $t - 7$) $\mathbb{1} \oplus \overline{\chi}_{47}^6 \overline{\varepsilon_7(3)}$	(43, $t + 6$) $\overline{\varepsilon_7(3)} \oplus \overline{\chi}_{43}^6$	(97, $x - 5$) $\mathbb{1} \oplus \overline{\chi}_{97}^6 \overline{\varepsilon_7(3)}$		(97, $x + 19$) $\overline{\varepsilon_7(3)} \oplus \overline{\chi}_{97}^6$	
$\ell \nmid N\varphi(N)$			(3919, $x - 934$) $\overline{\varepsilon_7(3)} \oplus \overline{\chi}_{3919}^6$		(3919, $x - 621$) $\mathbb{1} \oplus \overline{\chi}_{3919}^6 \overline{\varepsilon_7(3)}$	

6.2.2. Irreducible everywhere representation

We present an example of a form which all residual representations are irreducible. Fix $(N, k, \varepsilon) = (35, 4, \mathbb{1})$. The space $S_4^{\text{new}}(35, \mathbb{1})$ has dimension 6 over \mathbb{C} and contains 3 newforms up to conjugation by $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Let f be the newform of this space which q -expansion is

$$f = q + (y + 4)q^2 + (1 - 4y)q^3 + O(q^4),$$

where y is a root of $X^2 - 2$, and generates K_f . We have in this case

$$R_{35, \mathbb{1}} = \{(\mathbb{1}, \mathbb{1})\}.$$

Therefore, by Theorem 4.22 the only prime ideals λ of \mathcal{O}_f for which $\overline{\rho}_{f, \lambda}$ can be reducible are of residue characteristic $\ell \in \{2, 3, 5, 7\}$ (because we have $B_{4, \mathbb{1}} = -\frac{1}{30}$). Let us look at each of these cases.

- $\ell = 2$: We have $2\mathcal{O}_f = (2, y)^2$ and $R_{35, 4, \mathbb{1}}(2, y) = \{(\mathbb{1}, \mathbb{1}, 0, 0)\}$. However, we have

$$\text{Tr}(\overline{\rho}_{f, (2, y)}(\text{Frob}_3)) \equiv a_3(f) \equiv 1 \pmod{(2, y)} \quad \text{and}$$

$$\text{Tr}((\mathbb{1} \oplus \mathbb{1})(\text{Frob}_3)) \equiv 0 \pmod{(2, y)}.$$

Therefore $\overline{\rho}_{f, (2, y)}$ is irreducible.

- $\ell = 3$: The ideal $3\mathcal{O}_f$ is prime, and we have $R_{35, 4, \mathbb{1}}(3) = \{(\mathbb{1}, \mathbb{1}, 0, 1)\}$. However, we have

$$\text{Tr}(\overline{\rho}_{f, (3)}(\text{Frob}_2)) \equiv a_2(f) \equiv y + 1 \pmod{3} \quad \text{and}$$

$$\text{Tr}((\mathbb{1} \oplus \overline{\chi}_3)(\text{Frob}_2)) \equiv 0 \pmod{3}.$$

Therefore, $\overline{\rho}_{f, (3)}$ is irreducible.

- $\ell = 5$: Again, 5 is prime in \mathcal{O}_f , and we have $R_{35, 4, \mathbb{1}}(5) = \{(\mathbb{1}, \mathbb{1}, 0, 3); (\mathbb{1}, \mathbb{1}, 1, 2)\}$. Looking at a Frobenius element at 2, we have

$$\text{Tr}(\overline{\rho}_{f, (5)}(\text{Frob}_2)) \equiv a_2(f) \equiv y + 4 \pmod{5}$$

and

$$\text{Tr}((\mathbb{1} \oplus \overline{\chi}_5^3)(\text{Frob}_2)) \equiv 4 \pmod{5},$$

$$\text{Tr}((\overline{\chi}_5 \oplus \overline{\chi}_5^2)(\text{Frob}_2)) \equiv 0 \pmod{5}.$$

Therefore, $\overline{\rho}_{f, (5)}$ is irreducible.

- $\ell = 7$: We have $7\mathcal{O}_f = (7, y - 3)(7, y + 3)$ and $R_{35, 7, \mathbb{1}}(7, y \pm 3) = \{(\mathbb{1}, \mathbb{1})\} \times \{(0, 3); (1, 2); (4, 5)\}$. However, for a Frobenius element at 7 we have

$$\begin{cases} \text{Tr}(\overline{\rho}_{f, (7, y-3)}(\text{Frob}_3)) \equiv 3 \pmod{(7, y-3)}, \\ \text{Tr}(\overline{\rho}_{f, (7, y+3)}(\text{Frob}_3)) \equiv 6 \pmod{(7, y+3)}, \end{cases}$$

and

$$\text{Tr}((\mathbb{1} \oplus \overline{\chi}_7^3)(\text{Frob}_3)) \equiv 0 \pmod{7},$$

$$\mathrm{Tr}((\overline{\chi}_7 \oplus \overline{\chi}_7^2)(\mathrm{Frob}_3)) \equiv 5 \pmod{7},$$

$$\mathrm{Tr}((\overline{\chi}_7^4 \oplus \overline{\chi}_7^5)(\mathrm{Frob}_3)) \equiv 2 \pmod{7}.$$

Therefore, the representations $\overline{\rho}_{f,(7,y-3)}$ and $\overline{\rho}_{f,(7,y+3)}$ are irreducible.

Thus, for all prime ideals λ in \mathcal{O}_f , the representation $\overline{\rho}_{f,\lambda}$ is irreducible.

Acknowledgments

The author really wants to thank Nicolas Billerey for his great advice during the redaction of this paper. The author also wishes to thank Samuele Anni for stimulating discussions at Grenoble, and Bill Allombert and Karim Belabas for the fruitful exchanges about PARI/GP and the numerical implementation of this work. Finally, one is also grateful to the referee that gave many comments on various points of the present paper and helped to clarify some arguments of the proofs.

References

- [1] S. Anni, Images des représentations galoisiennes (2013), <https://tel.archives-ouvertes.fr/tel-00903800>.
- [2] A. O. L. Atkin and W. C. W. Li, Twists of newforms and pseudo-eigenvalues of w -operators, *Inventiones Mathematicae* **48**(3) (1978) 221–243.
- [3] N. Billerey and L. V. Dieulefait, Explicit large image theorems for modular forms, *J. Lond. Math. Soc.* **89**(2) (2014) 499–523.
- [4] N. Billerey and R. Menares, Strong modularity of reducible Galois representations, *Trans. Amer. Math. Soc.* **370**(2) (2018) 967–986.
- [5] H. Carayol, Sur les représentations l -adiques associées aux formes modulaires de Hilbert, *Annales Scientifiques de l'École Normale Supérieure* **19**(3) (1986) 409–468.
- [6] H. Carayol, Sur les représentations galoisiennes modulo l attachées aux formes modulaires, *Duke Math. J.* **59**(3) (1989) 785–801.
- [7] L. Carlitz, Arithmetic properties of generalized Bernoulli numbers, *J. für Die Reine und Angewandte Mathematik (Crelles Journal)* **202** (1959) 174–182.
- [8] H. Cohen, Sums involving the values at negative integers of l -functions of quadratic characters, *Mathematische Annalen* **217**(3) (1975) 271–285.
- [9] H. Cohen, *Number Theory. Vol. I. Tools and Diophantine Equations*, Graduate Texts in Mathematics, Vol. 239 (Springer, New York, 2007).
- [10] P. Deligne, La conjecture de weil : I, *Publications Mathématiques de l'IHÉS* **43** (1974) 273–307.
- [11] P. Deligne and J.-P. Serre, Formes modulaires de poids 1, *Annales Scientifiques de l'École Normale Supérieure, Série 4* **7**(4) (1974) 507–530.
- [12] F. Diamond and J. Im, Modular forms and modular curves, in *Seminar on Fermat's Last Theorem (Toronto, ON, 1993)*, CMS Conference Proceedings, Vol. 17 (American Mathematical Society, Providence, RI, 1995), pp. 39–133.
- [13] B. Edixhoven, The weight in Serre's conjectures on modular forms, *Inventiones Mathematicae* **109** (1992) 563–594.

- [14] B. Huppert, *Endliche Gruppen. I*. Die Grundlehren Der Mathematischen Wissenschaften, Vol. 134 (Springer-Verlag, Berlin, New York, 1967).
- [15] N. M. Katz, p -adic properties of modular schemes and modular forms, in *Modular Functions of One Variable III*, Lecture Notes in Mathematics, Vol. 350 (Springer, Berlin Heidelberg, 1973), pp. 69–190.
- [16] N. M. Katz, A result on modular forms in characteristic p , in *Modular Functions of One Variable V*, Lecture Notes in Mathematics, Vol. 601 (Springer, Berlin Heidelberg, 1977), pp. 53–61.
- [17] A. Kraus, Une remarque sur les points de torsion des courbes elliptiques, *Comptes Rendus de l'Académie des Sciences, Paris, Série I, Mathématiques* **321**(9) (1995) 1143–1146.
- [18] A. Kraus, Majorations effectives pour l'équation de fermat généralisée, *Canadian Journal of Mathematics* **49**(6) (1997) 1139–1161.
- [19] R. Livné, On the conductors of mod l Galois representations coming from modular forms, *Journal of Number Theory* **31**(2) (1989) 133–141.
- [20] D. Loeffler and J. Weinstein, On the computation of local components of a newform, *Mathematics of Computation* **81** (2012) 1179–1200.
- [21] D. Loeffler and J. Weinstein, Erratum: “on the computation of local components of a newform”, *Mathematics of Computation* **84** (2014) 355–356.
- [22] G. Martink, Dimensions of the spaces of cusp forms and newforms on $\gamma_0(n)$ and $\gamma_1(n)$, *Journal of Number Theory* **112** (2005) 298–331.
- [23] L. Meier, Topological modular forms with level structures: decompositions and duality (2017), arxiv preprint: <https://arxiv.org/abs/1609.09264>.
- [24] T. Miyake, *Modular Forms*, Springer Monographs in Mathematics, English edn. (Springer-Verlag, Berlin, 2006).
- [25] M. R. Murty, Congruences between modular forms, in *Analytic Number Theory*, London Mathematical Society Lecture Note Series, Vol. 247 (Cambridge University Press, Cambridge, 1997), pp. 309–320.
- [26] J. Neukirch, *Algebraic Number Theory*, Grundlehren Der Mathematischen Wissenschaften, Vol. 322 (Springer-Verlag, Berlin, 1999).
- [27] K. A. Ribet, On l -adic representations attached to modular forms, *Inventiones Mathematicae* **28** (1975) 245–275.
- [28] K. A. Ribet, Galois representations attached to eigenforms with nebentypus, in *Modular Functions of One Variable V*, Lecture Notes in Mathematics, Vol. 601 (1977), pp. 17–51.
- [29] K. A. Ribet, On l -adic representations attached to modular forms II, *Glasgow Mathematical Journal* **27** (1985) 185–194.
- [30] K. A. Ribet, Report on mod l representations of $\text{Gal}(\overline{\mathbf{q}}/\mathbf{q})$, in *Motives*, Proceedings of Symposia in Pure Mathematics, Vol. 55 (American Mathematical Society, Providence, RI, 1994), pp. 639–676.
- [31] J. B. Rosser and L. Schoenfeld, Approximate formulas for some functions of prime numbers, *Illinois Journal of Mathematics* **6** (1962) 64–94.
- [32] J.-P. Serre, Congruences et formes modulaires, in *Séminaire Bourbaki Vol. 1971/72 Exposés 400–417*, eds. A. Dold and B. Eckmann, Lecture Notes in Mathematics (Springer, 1973), pp. 319–338.
- [33] K. G. C. Staudt, Beweis eines lehrrsatzes, die bernoullischen zahlen betreffen, *Journal für die reine und angewandte Mathematik (Crelles Journal)* **21** (1840) 372–374.
- [34] J. Sturm, On the congruence of modular forms, in *Number Theory*, Lecture Notes in Mathematics, Vol. 1240 (Springer, Berlin, 1987), pp. 275–280.

- [35] H. P. F. Swinnerton-Dyer, On ℓ -adic representations and congruences for coefficients of modular forms, in *Modular Functions of One Variable III*, eds. W. Kuyk and J.-P. Serre, Lecture Notes in Mathematics, (Springer, 1973), pp. 1–55.
- [36] The PARI Group, Univ. Bordeaux. *PARI/GP version 2.13.0*, 2020, [tt http://pari.math.u-bordeaux.fr/](http://pari.math.u-bordeaux.fr/).
- [37] D. Zagier, Elliptic modular forms and their applications, in *The 1-2-3 of Modular Forms: Lectures at a Summer School in Nordfjordeid, Norway*, eds. J. H. Bruinier, G. van der Geer, G. Harder, D. Zagier and K. Ranestad, Universitext (Springer, 2008).