J. London Math. Soc. (2) 89 (2014) 499–523 © 2014 London Mathematical Society
doi:10.1112/jlms/jdt072

Explicit large image theorems for modular forms

Nicolas Billerey and Luis V. Dieulefait

Abstract

Let f be a (cuspidal) newform of weight $k \geqslant 2$ and level $\Gamma_0(N)$ with $N \geqslant 1$. Ribet proved that, under the assumption that f is non-CM, the residual representations $\bar{\rho}_{f,\lambda}$ attached to f by Deligne have a large image, in a precise sense, for all but finitely many prime ideals λ. In this paper, we make Ribet's theorem explicit by proving that the residue characteristics of these finitely many prime ideals for which the conclusion of Ribet's theorem fails to satisfy some divisibility relation, or are bounded from above by explicit constants, depending on k and N. The results split into different cases according to the possible types for the image, and each of them is illustrated by some numerical examples.

Introduction

Let f be a (cuspidal) newform of weight $k \geqslant 2$, level $N \geqslant 1$ whose Fourier expansion at infinity is given by $f(\tau) = q + \sum_{n \geqslant 2} a_n q^n$, with $q = e^{2i\pi\tau}$ and τ in the complex upper half-plane. We denote by K the number field generated by the coefficients a_n and by $\mathcal{O}$ its ring of integers. Given a prime ideal λ above ℓ in $\mathcal{O}$, we shall denote by $\bar{\rho}_{f,\lambda}$ the unique, up to semi-simplification, mod ℓ Galois representation attached to f by Deligne:

$$\bar{\rho}_{f,\lambda} : \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{GL}(2, \mathbf{F}_\lambda),$$

where $\mathbf{F}_\lambda$ is the residue field of $\mathcal{O}$ at λ. Let us denote by $\bar{G}_\lambda$ its image. Using results of Carayol [1], Ribet [25, Theorem 2.1] proved the following theorem (for a definition of forms with complex multiplication see [24] or Definition 1).

Theorem (Ribet). *Assume that f is not a form with complex multiplication. Then, for almost all λ (that is, all but a finite number), the following assertions hold*:

(i) *the representation $\bar{\rho}_{f,\lambda}$ is irreducible*;
(ii) *the order of the group $\bar{G}_\lambda$ is divisible by the residue characteristic of λ.*

In this paper, we shall say that λ is exceptional if it belongs to the finite set of prime ideals for which one of the assertions of Ribet's theorem does not hold. This theorem is a generalization of [23] in the case of $N = 1$, which itself extends pioneering results of Serre [29] and Swinnerton-Dyer [32] in the case of $N = 1$ and $K = \mathbf{Q}$. Although these latter results provide a precise characterization of exceptional prime ideals, the general theorem of Ribet is however non-effective.

The main goal of this paper is to make Ribet's theorem as effective as possible under the additional assumption that f has trivial Nebentypus. Though this further assumption is used in several places in our paper, we believe that our method generalizes to the case of arbitrary characters. Nevertheless, for the sake of conciseness, this generalization will be considered in

Received 3 April 2013; revised 17 August 2013; published online 8 January 2014.

2010 *Mathematics Subject Classification* 11F80, 11F33 (primary).

Research partially supported by MICINN grant MTM2012-33830 and by an ICREA Academia Research Prize.

another paper. More precisely, we prove that the residue characteristic of an exceptional prime satisfies some divisibility relation, or at least is bounded from above by an explicit constant, depending on k and N.

Before describing our main results, we mention that among the special cases covered are a generalization to arbitrary square-free levels of a result of Mazur [18] on the so-called Eisenstein primes for weight 2 and prime level modular forms, and an explicit version of Serre's theorem on the surjectivity of Galois representations attached to elliptic curves over $\mathbf{Q}$ due to Kraus [14] and Cojocaru [4].

Let us denote by $\mathbf{P}(\bar{\rho}_{f,\lambda})$ the projectivization of $\bar{\rho}_{f,\lambda}$ and by $\mathbf{P}(\bar{G}_\lambda)$ its image in $\mathrm{PGL}(2,\mathbf{F}_\lambda)$. According to Dickson's classification of subgroups of $\mathrm{PGL}(2,\mathbf{F}_\lambda)$ (see [9, II.8.27]), if λ is exceptional (we warn the reader that in the literature, the term 'exceptional' sometimes refers to the last situation below only), then we have that one of the following conditions satisfy us:

(I) $\bar{\rho}_{f,\lambda}$ is reducible;
(II) the image $\mathbf{P}(\bar{G}_\lambda)$ in $\mathrm{PGL}(2,\mathbf{F}_\lambda)$ is dihedral;
(III) $\mathbf{P}(\bar{G}_\lambda)$ is isomorphic to A_4, S_4 or A_5.

Besides, if λ is non-exceptional, then $\mathbf{P}(\bar{\rho}_{f,\lambda})$ is isomorphic to either $\mathrm{PGL}(2,\mathbf{F})$ or $\mathrm{PSL}(2,\mathbf{F})$ for some subfield $\mathbf{F}$ of $\mathbf{F}_\lambda$, and we shall then say that $\bar{\rho}_{f,\lambda}$ has a large image.

In each of the above cases, we thus provide a divisibility relation, or an upper-bound in terms of k and N satisfied by the residue characteristic ℓ of λ. The last case is the simplest one. Namely, we prove the following theorem.

THEOREM (Theorem 4.1). *If $\mathbf{P}(\bar{G}_\lambda)$ is isomorphic to A_4, S_4 or A_5, then either $\ell \mid N$ or $\ell \leqslant 4k-3$.*

In the second case, we give a general upper-bound together with a much finer result in the square-free level case that imply the following theorem.

THEOREM (Theorem 3.2). *Assume $\mathbf{P}(\bar{G}_\lambda)$ to be dihedral. If f does not have complex multiplication, then we have*

$$\ell \leqslant (2(8kN^2(1+\log\log N))^{(k-1)/2})^{g_0^\sharp(k,N)},$$

where $g_0^\sharp(k,N)$ is the number of newforms of weight k and level $\Gamma_0(N)$. Besides, if N is square-free, then either $\ell \mid N$, or $\ell \leqslant k$, or $\ell = 2k-1$.

The first case is by far the most complicated one, and we refer the reader to Theorems 2.4–2.7 for precise and complete statements. Nevertheless, these results, combined with those mentioned in this introduction, yield to (slightly stronger versions of) the following theorems in particular, but important cases where N is square-free and N is a square, respectively.

THEOREM (Square-free level case). *Assume that $N = p_1 \cdots p_t$, where $p_1, \ldots, p_t$ are $t \geqslant 1$ distinct primes, is square-free, and λ is exceptional. Then we have that one of the following is satisfied:*

(i) $\ell \in \{p_1, \ldots, p_t\}$;
(ii) $\ell \leqslant 4k-3$;
(iii) ℓ *divides*

$$\begin{cases} \gcd_{1\leqslant i\leqslant t}(\mathrm{lcm}(p_i^k-1, p_i^{k-2}-1)) & \text{if } k>2, \\ \mathrm{lcm}_{1\leqslant i\leqslant t}(p_i^2-1) & \text{if } k=2. \end{cases}$$

THEOREM (Square level case). *Assume that $N = c^2$ is a square, f does not have complex multiplication and λ is exceptional. Then we have that one of the following is satisfied*:

(i) $\ell \mid N$;
(ii) $\ell \leqslant (2(8kN^2(1+\log\log N))^{(k-1)/2})^{g_0^\sharp(k,N)}$, *where $g_0^\sharp(k,N)$ is the number of (cuspidal) newforms of weight k and level $\Gamma_0(N)$*;
(iii) *there exists a primitive Dirichlet character $\nu : (\mathbf{Z}/c\mathbf{Z})^\times \to \mathbf{C}^\times$ such that*:
  (a) *either ℓ divides the norm of $p^k - \epsilon^{-1}(p)$ for some prime $p \mid c$*;
  (b) *or ℓ divides the numerator of the norm of $B_{k,\epsilon}/2k$*;
  where c_0 divides c, $\epsilon : (\mathbf{Z}/c_0\mathbf{Z})^\times \to \mathbf{C}^\times$ is the inverse of the primitive Dirichlet character attached to ν^2 and $B_{k,\epsilon}$ is the kth Bernoulli number attached to ϵ.

Apart from (III) which is slightly different, the main idea used in proving the results of the paper is to interpret situations (I) and (II) above in terms of congruences between modular forms. In the case of reducible representations $\bar\rho_{f,\lambda}$, the original form f is then shown to be congruent modulo ℓ to a suitable Eisenstein series whose construction depends on the weight and level. The theory of modular forms modulo ℓ of Serre and Katz enables us to interpret this congruence as an equality. The desired bound then follows from a careful study of the constant term of these Eisenstein series at various cusps. Besides, in the case of dihedral projective image, the congruent modular form is a specific twist of the original form f. In that case, the upper-bound follows from those of Sturm and Deligne.

Ghate and Parent recently addressed the question of whether the residual Galois representations attached to rational simple non-CM modular abelian varieties have 'uniform' large images (see [8, Question 1.2] for a precise statement). One of the main results of their paper is that, in the weight 2 situation, there exists a uniform bound (depending on $[K : \mathbf{Q}]$, but not on the level) for the residue characteristic of prime ideals in the A_4, S_4 or A_5 case. While we are in contrary working with a fixed level, their work is still quite relevant for us.

The first section of the paper is devoted to classical facts about modular Galois representations and their local behaviors. The next three sections deal with cases (I), (II) and (III) above, respectively. Finally, some numerical examples illustrating our results are presented in the last section.

1. *Preliminaries*

For simplicity, we shall write $\bar\rho$ for $\bar\rho_{f,\lambda}$. We further denote by $\bar\rho^{ss}$ the semi-simplification of $\bar\rho$. In this section, we also assume $\ell \nmid N$.

1.1. *Local decomposition at Steinberg primes*

Let p be a prime dividing N exactly once. We shall write $p \| N$. Define $\bar\rho_p$ to be the restriction of $\bar\rho$ to a decomposition group G_p at p. For any $x \in \mathcal{O}$, let us denote by $\lambda(x)$ the unramified character of G_p that maps a Frobenius element to $x \pmod\lambda$. Langlands has proved that [16, Proposition 2.8]

$$\bar\rho_p \simeq \begin{pmatrix} \mu\bar\chi_\ell^{k/2-1} & \star \\ 0 & \mu\bar\chi_\ell^{-k/2} \end{pmatrix}, \tag{1.1}$$

where $\mu = \lambda(a_p/p^{k/2-1})$ is trivial or quadratic since $a_p = \pm p^{k/2-1}$ [20, Theorem 4.6.17]. In particular, if $\mathrm{Frob}_p \in G_p$ is a Frobenius element at p, then the roots of the characteristic polynomial of $\bar\rho(\mathrm{Frob}_p)$ are $a_p \pmod\lambda$ and $pa_p \pmod\lambda$.

1.2. *Classification of degenerate cases*

Let $N(\bar{\rho}^{ss})$ be the Artin conductor of $\bar{\rho}^{ss}$. It was proved by Carayol [1] that $N(\bar{\rho}^{ss})$ is a divisor of N. Moreover, Carayol [2, §§ 1.2–1.3] and Livné [15] have (independently) classified the 'degenerate' cases (in Carayol's terminology), that is, when $e_p \overset{\text{def}}{=} v_p(N) - v_p(N(\bar{\rho}^{ss})) > 0$ for some prime p. They proved that when $e_p > 0$, we are in one of the situations described in Table 1.

Moreover, it follows from their classification that, in the first and third cases, p satisfies certain congruences modulo ℓ. Namely, we have the following proposition (which we deduce from [2, § 1.5] using the fact that, in these cases, $\bar{\rho}^{ss}$ is the semi-simplification of the reduction of an ℓ-adic degenerate representation of type (i), (iii) or (iv) with the terminology of [2, Proposition 2]).

PROPOSITION 1.1 (Carayol–Livné). *Assume $e_p > 0$ and $v_p(N) \geqslant 2$. Then we have $p \equiv \pm 1 \pmod{\ell}$.*

1.3. *Local description at ℓ*

Assume $2 \leqslant k \leqslant \ell + 1$. Let G_ℓ be a decomposition group at ℓ and I_ℓ be its inertia subgroup. Then Deligne and Fontaine [7] have, respectively, proved that

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

$$\bar{\rho}_{|I_\ell} \simeq \begin{pmatrix} \bar{\chi}_\ell^{k-1} & \star \\ 0 & 1 \end{pmatrix};$$

(ii) if f is not ordinary at λ, then $\bar{\rho}_{|G_\ell}$ is irreducible and

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

where $\{\psi, \psi'\} = \{\psi, \psi^\ell\}$ is the set of fundamental characters of level 2 ([7, § 2.4]).

The following lemma is immediate.

LEMMA 1.2. *Assume $\ell > k$.*

(i) *The image of $\bar{\chi}_\ell^{k-1}$ is cyclic of order $n = (\ell - 1)/\gcd(\ell - 1, k - 1) \geqslant 2$. In particular, we have $n = 2$ if and only if $\ell = 2k - 1$. Moreover, if $\ell > 4k - 3$, then $n > 5$.*

(ii) *The image of $\psi^{(\ell-1)(k-1)}$ is cyclic of order $m = (\ell + 1)/\gcd(\ell + 1, k - 1) \geqslant 2$. In particular, we have $m = 2$ if and only if $\ell = 2k - 3$. Moreover, if $\ell > 4k - 5$, then $m > 5$.*

TABLE 1. *Classification of the degenerate cases.*

$v_p(N)$	$b + 1 \geqslant 2$	1	2
$v_p(N(\bar{\rho}^{ss}))$	$b \geqslant 1$	0	0
e_p	1	1	2

2. *Reducible representations*

2.1. *Preliminaries: Gauss sums and Bernoulli numbers*

Let $\psi : (\mathbf{Z}/f\mathbf{Z})^\times \to \mathbf{C}^\times$ be a primitive Dirichlet character of modulus $f \geqslant 1$. The Gauss sum attached to ψ is defined by

$$W(\psi) = \sum_{n=1}^{f} \psi(n)\, e^{2i\pi n/f}.$$

LEMMA 2.1. *We have $|W(\psi)| = \sqrt{f}$. Moreover, as an algebraic integer, the norm of $W(\psi)$ is a power of f.*

Proof. The first part of the lemma is [20, Lemma 3.1.1]. Let σ be a $\bar{\mathbf{Q}}$-automorphism and $m \in \mathbf{Z}$ such that $\sigma(e^{2i\pi/f}) = e^{2i\pi m/f}$. Then, by Miyake [20], we have

$$\sigma(W(\psi)) = \sum_{n=1}^{f} \psi^\sigma(n)\, e^{2i\pi nm/f} = \bar{\psi}^\sigma(m) W(\psi^\sigma)$$

and thus $|\sigma(W(\psi))| = |W(\psi^\sigma)| = \sqrt{f}$. This completes the proof of the lemma. □

The Bernoulli numbers attached to ψ are defined by

$$\sum_{n=1}^{f} \psi(n) \frac{t\, e^{nt}}{e^{ft} - 1} = \sum_{m \geqslant 0} B_{m,\psi} \frac{t^m}{m!}.$$

In particular, if ψ is the trivial character, then $B_{m,\psi}$ is the classical Bernoulli number B_m, except when $m = 1$, in which case $B_{1,\psi} = -B_1 = \frac{1}{2}$. The following proposition is a well-known result of van Staudt–Clausen.

PROPOSITION 2.2 (van Staudt–Clausen). *Let $m \geqslant 2$ be an even integer. The denominator of B_m is $\prod_{p-1|m} p$, where the product runs over the primes p such that $p - 1$ divides m.*

The Bernoulli numbers are also related to certain special values of the L-function $L(s, \psi)$ attached to ψ. More precisely, we have the following proposition [34, Chapter 4].

PROPOSITION 2.3. *Assume that ψ to be even. Let $m \geqslant 2$ be an even integer. Then we have*

$$L(m, \psi) = -W(\psi) \frac{C_m}{f^m} \cdot \frac{B_{m,\psi^{-1}}}{2m} \neq 0, \quad \text{where } C_m = \frac{(2i\pi)^m}{(m-1)!}.$$

2.2. *Statement of the results*

THEOREM 2.4. *Assume $\bar{\rho}_{f,\lambda}$ to be reducible. If $v_2(N) = 2$ or $v_2(N) \geqslant 3$ is odd, then either ℓ divides N, or $\ell < k - 1$, or $\ell = 3$.*

Put $c = \max\{d \geqslant 1;\ d^2 \mid N\}$. The following result is a generalization of Ribet's [23, Lemma 5.2] on the level 1 case to higher levels.

THEOREM 2.5 (main result). *Assume $\bar{\rho}_{f,\lambda}$ to be reducible. Then one of the following assertions holds.*

(i) *The prime ℓ divides N or $\ell < k-1$.*
(ii) *The level N is not a square and there exists an even Dirichlet character $\eta : (\mathbf{Z}/c\mathbf{Z})^\times \to \mathbf{C}^\times$ such that, for every prime p dividing N with odd valuation $v_p(N)$, we have:*
  (a) *either $v_p(N) \geqslant 3$ and $p \equiv \pm 1 \pmod{\ell}$;*
  (b) *or $v_p(N) = 1$ and ℓ divides the norm of either $p^k - \eta(p)$, or $p^{k-2} - \eta(p)$.*
(iii) *The level N is a square (that is, $N = c^2$) and one of the following holds:*
  (a) *either there exists a prime p such that $v_p(N) = 2$ and $p \equiv \pm 1 \pmod{\ell}$;*
  (b) *or there exists a primitive Dirichlet character $\nu : (\mathbf{Z}/c\mathbf{Z})^\times \to \mathbf{C}^\times$ such that, for $\ell > k+1$, we have:*
    (1) *either ℓ divides the norm of $p^k - \epsilon^{-1}(p)$ for some prime $p \mid c$;*
    (2) *or ℓ divides the numerator of the norm of $B_{k,\epsilon}/2k$;*
    where c_0 divides c and $\epsilon : (\mathbf{Z}/c_0\mathbf{Z})^\times \to \mathbf{C}^\times$ is the inverse of the primitive Dirichlet character attached to ν^2.

Note that these two results give an effective bound for ℓ in terms of N and k unless $k = 2$ and $N = p_1 \cdots p_t c^2$, where $p_1, \ldots, p_t$ are $t \geqslant 1$ distinct primes not dividing c, and c is odd or divisible by 4 (as in particular condition (2.5) in Theorem 2.5 might be vacuous if $k = 2$). In the square-free level case (namely, when $c = 1$), we, however, have the following theorem whose first part is an immediate corollary of Theorem 2.5, and whose second part follows from a generalization of a result of Mazur on the weight 2 and prime level case (cf. [**18**; **19**, Proposition 1]).

THEOREM 2.6 (Square-free level case). *Assume that $\bar{\rho}_{f,\lambda}$ is reducible and $N = p_1 \cdots p_t$, where $p_1, \ldots, p_t$ are $t \geqslant 1$ distinct primes.*

(i) *If $k > 2$, then one of the following assertions holds:*
  (a) *either ℓ divides N or $\ell < k-1$;*
  (b) *ℓ divides the following non-zero integer*

$$\gcd(\operatorname{lcm}(p_i^k - 1, p_i^{k-2} - 1), 1 \leqslant i \leqslant t).$$

(ii) *If $k = 2$ and $\ell \nmid 6N$, then the following assertions hold:*
  (a) *for any $1 \leqslant i \leqslant t$ with $a_{p_i} = -1$, we have $p_i \equiv -1 \pmod{\ell}$;*
  (b) *we have $(a_{p_1}, \ldots, a_{p_t}) \neq (-1, \ldots, -1)$;*
  (c) *if $(a_{p_1}, \ldots, a_{p_t}) = (+1, \ldots, +1)$, then ℓ divides the non-zero integer $\prod_{i=1}^t (p_i - 1)$.*

We point out that Ribet already proved (but did not publish) the second part of this theorem as well as 'converse results' (see the notes [**27**] on his homepage).

The last theorem of this section deals with the cases not covered by the previous results.

THEOREM 2.7. *Assume that $\bar{\rho}_{f,\lambda}$ is reducible. If $k = 2$ and N is of the form $N = p_1 \cdots p_t c^2$, where $c \neq 1$, $p_1, \ldots, p_t$ are $t \geqslant 1$ distinct primes not dividing c, and c is odd or divisible by 4, then one of the following are satisfied:*

(i) *$\ell \mid N$;*
(ii) *$\ell < k-1$;*
(iii) *there exists a prime p such that $v_p(N) = 2$ and $p \equiv \pm 1 \pmod{\ell}$;*

(iv) *there exists a primitive Dirichlet character* $\nu : (\mathbf{Z}/c\mathbf{Z})^\times \to \mathbf{C}^\times$ *such that, for* $\ell > 3$, *we have that any one of the following is satisfied*:
(a) ℓ *divides the norm of* $p_i^2 - \nu^2(p_i)$ *for some* $1 \leqslant i \leqslant t$;
(b) ℓ *divides the norm of* $p^2 - \epsilon^{-1}(p)$ *for some prime* $p \mid c$;
(c) ℓ *divides* $p_i - 1$ *for some* $1 \leqslant i \leqslant t$;
(d) ℓ *divides the numerator of the norm of* $B_{2,\epsilon}/4$;
where $c_0 \mid c$ *and* $\epsilon : (\mathbf{Z}/c_0\mathbf{Z})^\times \to \mathbf{C}^\times$ *is the inverse of the primitive Dirichlet character attached to* ν^2.

2.3. *The Eisenstein series E*

Assume $\ell \nmid N$. For simplicity, let us denote $\bar\rho$ for $\bar\rho_{f,\lambda}$ and assume $\bar\rho$ to be reducible. The semi-simplification $\bar\rho^{ss}$ of $\bar\rho$ is the direct sum of two characters ϵ_1 and ϵ_2. Each of them may be decomposed as a product $\bar\nu_i\bar\chi_\ell^{\alpha_i}$ with $\bar\nu_i$ unramified at ℓ and $0 \leqslant \alpha_i < \ell - 1$ $(i = 1, 2)$. Using that f has trivial Nebentypus, we obtain that $\bar\rho^{ss}$ has determinant $\bar\chi_\ell^{k-1}$. Hence, we have $\alpha_1 + \alpha_2 \equiv k - 1 \pmod{\ell - 1}$ and $\bar\nu_2 = \bar\nu_1^{-1}$.

Let us further assume that $\ell + 1 \geqslant k$. Using the results of § 1.3, one sees that $\{\alpha_1, \alpha_2\} = \{0, k - 1\}$ and thus

$$\bar\rho^{ss} \simeq \bar\nu \oplus \bar\nu^{-1}\bar\chi_\ell^{k-1}, \tag{2.1}$$

with $\bar\nu \in \{\bar\nu_1, \bar\nu_2\}$. Moreover, according to Carayol's theorem of § 1.2, the conductor $\mathfrak{c}$ of $\bar\nu$ satisfies

$$N(\bar\rho^{ss}) = \mathfrak{c}^2 \mid N. \tag{2.2}$$

In particular, $N(\bar\rho^{ss})$ is a square dividing N.

Let ν be the Teichmüller lift of $\bar\nu$. We may identify it with a primitive Dirichlet character modulo $\mathfrak{c}$. From now on, assume that:

(1) either $k > 2$;
(2) or, $k = 2$ and $\mathfrak{c} \neq 1$.

Under this assumption, we may consider the Eisenstein series in $\mathcal{M}_k(\Gamma_0(\mathfrak{c}^2))$ whose Fourier expansion is given by

$$E(\tau) = -\vartheta(\mathfrak{c})\frac{B_k}{2k} + \sum_{n \geqslant 1} \sigma_{k-1}^{\nu}(n)q^n,$$

where

$$\vartheta(\mathfrak{c}) = \begin{cases} 1 & \text{if } \mathfrak{c} = 1, \\ 0 & \text{otherwise,} \end{cases} \qquad \sigma_{k-1}^{\nu}(n) = \sum_{0<m|n} \nu(n/m)\nu^{-1}(m)m^{k-1}$$

and B_k is the kth Bernoulli number. Note also that our notation E differs from the notation $E_k^{\nu,\nu^{-1}}$ of [5, Chapter 4] by a factor 2: $E_k^{\nu,\nu^{-1}} = 2E$.

The following proposition gives the constant term of the Fourier expansion of E at the various cusps of $\Gamma_0(\mathfrak{c}^2)$.

PROPOSITION 2.8. *The Eisenstein series* E *is defined over* $\mathcal{O}_L$, *where* L *is the field generated by the values of* ν, *unless* $\mathfrak{c} = 1$ *(and* $k > 2$*), in which case* E *is the classical Eisenstein series* $E_k(\tau) = -B_k/2k + \sum_{n \geqslant 1} \sigma_{k-1}(n)q^n$ *of weight* k *and level* 1. *Let* $s = u/v$ *(where* $\gcd(u, v) = 1$, $v \mid \mathfrak{c}^2$ *and* u *varies through a set of representatives of the integers modulo* $\gcd(v, \mathfrak{c}^2/v)$*) be a cusp of* $\Gamma_0(\mathfrak{c}^2)$, *and let* $\gamma \in \mathrm{SL}(2, \mathbf{Z})$ *such that* $\gamma\infty = s$. *Then the constant term* Υ *of* $E|_k\gamma$ *is*

independent of the choice of such a γ and satisfies

$$\Upsilon \neq 0 \Leftrightarrow v = \mathfrak{c}.$$

In that case, we have

$$\Upsilon = -\nu(-u)\left(\frac{\mathfrak{c}}{c_0}\right)^k \frac{W((\nu^2)_0)}{W(\nu)} \frac{B_{k,(\nu^2)_0^{-1}}}{2k} \prod_{p|\mathfrak{c}} (1-(\nu^2)_0(p)p^{-k}),$$

where $(\nu^2)_0$ is the primitive character associated to ν^2 of modulus $c_0 \mid \mathfrak{c}$. Moreover, if $\mathfrak{c} > 1$, then $E|_k\gamma \in \mathcal{O}_L[1/\mathfrak{c}^2](\mu_{\mathfrak{c}^2})[\![q^{1/\mathfrak{c}^2}]\!]$, where $\mu_{\mathfrak{c}^2}$ is the group of $\mathfrak{c}^2$th roots of unity.

Proof. The proposition is immediate when $\mathfrak{c} = 1$. Assume therefore $\mathfrak{c} > 1$. Then, by construction, the Fourier expansion of E has coefficients in $\mathcal{O}_L$, and therefore E is defined over $\mathcal{O}_L[1/\mathfrak{c}^2](\mu_{\mathfrak{c}^2})$ (see [**11**, § 1.6]).

Let $s = u/v$ as in the proposition be a cusp of $\Gamma_0(\mathfrak{c}^2)$ (for the description of a set of representatives of the cusps of $\Gamma_0(\mathfrak{c}^2)$, see [**10**, Proposition 2.6]) and $\gamma \in \mathrm{SL}(2,\mathbf{Z})$ such that $\gamma\infty = s$. The last assertion follows from the q-expansion principle, and the fact that the Fourier expansion of E at ∞ has coefficients in $\mathcal{O}_L$ (see [**11**, Corollary 1.6.2.]).

Since k is even, the constant term of E at s is well defined (that is, it does not depend on the choice of such a γ). Put

$$\gamma = \begin{pmatrix} u & \beta \\ v & \delta \end{pmatrix} \in \mathrm{SL}(2,\mathbf{Z}) \quad \text{and} \quad G = \frac{C_k W(\nu)}{\mathfrak{c}^k} E, \ \text{where } C_k = \frac{(2i\pi)^k}{(k-1)!}. \tag{2.3}$$

The constant part of $G|_k\gamma$ is then given by the following sum (see [**5**, Chapter 4] and [**28**, § VII.3] for a justification in the weight 2 case; the factor $\frac{1}{2}$ comes from our normalization for E):

$$\Upsilon_0 = \frac{1}{2} \sum_{i,j,l=0}^{\mathfrak{c}-1} \nu(ij)\vartheta(\overline{i\mathfrak{c}u + v(j+l\mathfrak{c})})\zeta^{\overline{\mathfrak{c}i\beta+(j+l\mathfrak{c})\delta}}(k),$$

where the bar means reduction modulo $\mathfrak{c}^2$,

$$\vartheta(\bar{n}) = \begin{cases} 1 & \text{if } n \equiv 0 \pmod{\mathfrak{c}^2}, \\ 0 & \text{otherwise,} \end{cases} \qquad \zeta^{\bar{n}}(k) = \sum_{m \equiv n \pmod{\mathfrak{c}^2}}{}' \frac{1}{m^k},$$

and the primed summation notation means to sum over non-zero integers.

Assume Υ_0 to be non-zero. Then there exist $i,j,l \in \{0,\dots,\mathfrak{c}-1\}$ such that

$$\nu(ij)\vartheta(\overline{i\mathfrak{c}u + v(j+l\mathfrak{c})}) \neq 0.$$

In other words, $\gcd(ij,\mathfrak{c}) = 1$ and $i\mathfrak{c}u + v(j+l\mathfrak{c}) \equiv 0 \pmod{\mathfrak{c}^2}$. It follows that $vj \equiv 0 \pmod{\mathfrak{c}}$. But j is co-prime to $\mathfrak{c}$ by assumption. So $v \equiv 0 \pmod{\mathfrak{c}}$ and u is invertible modulo $\mathfrak{c}$. The congruence $i \equiv -(j/u)(v/\mathfrak{c}) \pmod{\mathfrak{c}}$ follows easily and, therefore, we have

$$\nu(ij) = \nu\left(-\frac{vj^2}{u\mathfrak{c}}\right) = \nu\left(-\frac{j^2}{u}\right)\nu\left(\frac{v}{\mathfrak{c}}\right) \neq 0.$$

So $\gcd(v/\mathfrak{c},\mathfrak{c}) = 1$ and since $\mathfrak{c} \mid v$ and $v \mid \mathfrak{c}^2$, we obtain $v = \mathfrak{c}$.

Conversely, assume $v = \mathfrak{c} > 1$. Then $\gcd(u,\mathfrak{c}) = 1$ and, on one hand, we have

$$i\mathfrak{c}u + v(j+l\mathfrak{c}) \equiv 0 \pmod{\mathfrak{c}^2} \Longleftrightarrow i \equiv -j/u \pmod{\mathfrak{c}};$$

on the other hand

$$\begin{aligned}\mathfrak{c}i\beta+(j+l\mathfrak{c})\delta&=\frac{1}{u}(u\mathfrak{c}i\beta+(j+l\mathfrak{c})u\delta)\\&\equiv\frac{1}{u}(-vj\beta+(j+l\mathfrak{c})(1+\beta v))\ (\mathrm{mod}\,\mathfrak{c}^2)\\&\equiv\frac{1}{u}(j+l\mathfrak{c})\ (\mathrm{mod}\,\mathfrak{c}^2).\end{aligned}$$

Combining these two facts, we find that

$$\begin{aligned}2\Upsilon_0&=\sum_{l=0}^{\mathfrak{c}-1}\sum_{\substack{j=0\\ \gcd(j,\mathfrak{c})=1}}^{\mathfrak{c}-1}\nu(-j^2/u)\zeta^{\overline{(j+l\mathfrak{c})/u}}(k)\\&=\nu(-u)\sum_{l=0}^{c-1}\sum_{\substack{j=0\\ \gcd(j,\mathfrak{c})=1}}^{\mathfrak{c}-1}\nu(j^2/u^2)\sum_{m\equiv(j+l\mathfrak{c})/u\ (\mathrm{mod}\,\mathfrak{c}^2)}{}'\frac{1}{m^k}\\&=\nu(-u)\sum_{\substack{j=0\\ \gcd(j,\mathfrak{c})=1}}^{\mathfrak{c}-1}\sum_{m\equiv j/u\ (\mathrm{mod}\,\mathfrak{c})}{}'\frac{\nu^2(m)}{m^k}\\&=2\nu(-u)\sum_{m\geqslant 1}\frac{\nu^2(m)}{m^k}=2\nu(-u)L(k,\nu^2),\end{aligned}\tag{2.4}$$

where ν^2 is viewed as a character modulo $\mathfrak{c}$. Let $(\nu^2)_0$ be the primitive Dirichlet character attached to ν^2. It is an even character modulo $c_0 \mid \mathfrak{c}$ and we have

$$L(k,\nu^2)=L(k,(\nu^2)_0)\prod_{p\mid\mathfrak{c}}(1-(\nu^2)_0(p)p^{-k}).\tag{2.5}$$

Applying Proposition 2.3 to $\psi=(\nu^2)_0$ and $m=k$, we obtain

$$L(k,(\nu^2)_0)=-W((\nu^2)_0)\frac{C_k}{c_0^k}\frac{B_{k,(\nu^2)_0^{-1}}}{2k}\neq 0.\tag{2.6}$$

According to Equations (2.4)–(2.6) together with (2.3), when $v=\mathfrak{c}$, the constant term of the Fourier expansion of E at s is thus the non-zero algebraic number

$$\Upsilon=\frac{\mathfrak{c}^k}{C_kW(\nu)}\Upsilon_0=-\nu(-u)\left(\frac{\mathfrak{c}}{c_0}\right)^k\frac{W((\nu^2)_0)}{W(\nu)}\frac{B_{k,(\nu^2)_0^{-1}}}{2k}\prod_{p\mid\mathfrak{c}}(1-(\nu^2)_0(p)p^{-k}),$$

as claimed. □

2.4. *Proof of Theorems* 2.4 *and* 2.5

Assume $\bar\rho$ to be reducible with $\ell\nmid N$ and $\ell+1\geqslant k$. We keep the notation of § 2.3. In particular, we have (cf. (2.1) and (2.2))

$$\bar\rho^{ss}\simeq\bar\nu\oplus\bar\nu^{-1}\bar\chi_\ell^{k-1},\tag{2.7}$$

where $\bar\nu$ is a character of conductor $\mathfrak{c}$ such that $\mathfrak{c}^2\mid N$. So, in particular, we have $\mathfrak{c}\mid c$.

Assume $v_2(N)=2$. Then $v_2(c)=1$ and $\mathfrak{c}$ is odd since there is no primitive Dirichlet character modulo twice an odd integer. Therefore, we are in a degenerate case at $p=2$ as described in § 1.2. By Proposition 1.1, we have $2\equiv\pm1\ (\mathrm{mod}\,\ell)$, namely $\ell=3$.

If N is not a square, then let us consider a prime p dividing N with odd valuation $v_p(N)$. Once again, we necessarily are in one of the degenerate cases. If $v_p(N)\geqslant 3$, then, by Proposition 1.1, we obtain $p\equiv\pm1\ (\mathrm{mod}\,\ell)$. This completes the proof of Theorem 2.4.

Assume now that, for some prime p, we have $v_p(N) = 1$ and let us denote by η the Teichmüller lift of $\bar{\nu}^2$. Since $\mathfrak{c}$ is a divisor of c, we may identify η with an even Dirichlet character modulo c. Comparing the restriction to a decomposition group at p of $\bar{\rho}^{ss}$ given by (2.1) with the local representation given by (1.1), we obtain the following equality between sets of characters of G_p:

$$\{\bar{\nu}, \bar{\nu}^{-1}\bar{\chi}_\ell^{k-1}\} = \{\mu\bar{\chi}_\ell^{k/2}, \mu\bar{\chi}_\ell^{k/2-1}\},$$

where $\mu = \lambda(a_p/p^{k/2-1})$ is the at most quadratic character defined in § 1.1. We thus are in one of the following situations:

(1) either $\bar{\nu} = \mu\bar{\chi}_\ell^{k/2}$ and then $\bar{\nu}^2 = \bar{\chi}_\ell^k$. Applying this equality to a Frobenius element at p, we obtain that $\bar{\nu}^2(\mathrm{Frob}_p) = p^k \pmod{\ell}$ and therefore ℓ divides the norm of $p^k - \eta(p)$;

(2) or $\bar{\nu} = \mu\bar{\chi}_\ell^{k/2-1}$ and then $\bar{\nu}^2 = \bar{\chi}_\ell^{k-2}$. Again we have $\bar{\nu}^2(\mathrm{Frob}_p) = p^{k-2} \pmod{\ell}$ and we conclude as before that ℓ divides the norm of $p^{k-2} - \eta(p)$.

It remains to prove Theorem 2.5 when N is a square, namely, when $N = c^2$. Assume first that $\mathfrak{c} \neq c$. Then we are in a degenerate case as described in § 1.2 for some prime number p. Moreover, $N(\bar{\rho}^{ss}) = \mathfrak{c}^2$ is a square and therefore we have $v_p(N) = 2$ and $v_p(N(\bar{\rho}^{ss})) = 0$. By Proposition 1.1, it follows that $p \equiv \pm 1 \pmod{\ell}$.

In other words, if, for every prime p dividing N with valuation 2, we have $p \not\equiv \pm 1 \pmod{\ell}$, then $\mathfrak{c} = c$, $N = \mathfrak{c}^2$ and there is no degeneration at all. Assume now that we are in this situation. Since the space of weight 2 and level 1 modular forms are trivial, it follows that either $k > 2$, or $k = 2$ and $\mathfrak{c} \neq 1$. Therefore, we may consider the Eisenstein series E of § 2.3. Let M denote the compositum of K and L (the field generated by the values of ν).

LEMMA 2.9. *The Eisenstein series E is a normalized eigenform for all the Hecke operators at level $\Gamma_0(N)$. Moreover, there exists a prime ideal $\mathcal{L}$ above ℓ in the integer ring of M such that*

$$a_r \equiv a_r(E) \pmod{\mathcal{L}} \quad \textit{for all primes } r \neq \ell.$$

Proof. The fact that E is a normalized eigenform for all the Hecke operators at level $\Gamma_0(N)$ follows, for instance, from [**5**, Proposition 5.2.3]. Moreover, by isomorphism (2.7) there exists a prime ideal $\mathcal{L}$ above ℓ in the integer ring of M such that

$$a_r \equiv a_r(E) \pmod{\mathcal{L}} \quad \text{for all primes } r \nmid \ell N.$$

If now r is a prime dividing N, then $r^2 \mid N$ and $a_r = 0$ (see [**20**, Theorem 4.6.17]). Besides, $\nu(r) + \nu^{-1}(r)r^{k-1} = 0$. Hence, $a_r = 0 = a_r(E)$. This proves the lemma. □

Let now Θ be the Katz's operator on modular forms over $\bar{\mathbf{F}}_\ell$, whose action on q-expansions is given by $q(d/dq)$ (denoted by $A\theta$ in [**12**]). Assume $\ell > k + 1$. Then the constant term of E at ∞ is non-zero only if $\mathfrak{c} = 1$ and $k > 2$. In that case it is $-B_k/2k$, which is ℓ-integral by Proposition 2.2. We denote by $\bar{f}$ and $\bar{E}$ the modular forms over $\bar{\mathbf{F}}_\ell$ obtained by reduction modulo $\mathcal{L}$ of f and E, respectively. Lemma 2.9 implies that $\Theta(\bar{f}) = \Theta(\bar{E})$. Moreover, Katz has proved that if $\ell > k + 1$, then Θ is injective [**12**, Corollary (3)]. Under this assumption, it thus follows that the Eisenstein series E becomes cuspidal after reduction.

If $\mathfrak{c} = 1$, then we immediately obtain that ℓ divides the numerator of $B_k/2k$ as stated in the theorem. Assume therefore that $\mathfrak{c} > 1$. Then ℓ divides the numerator of the norm of the constant term of E at each cusp of $\Gamma_0(\mathfrak{c}^2)$, namely by Proposition 2.8:

$$\Upsilon = \pm\left(\frac{\mathfrak{c}}{c_0}\right)^k \frac{W(\epsilon^{-1})}{W(\nu)} \frac{B_{k,\epsilon}}{2k} \prod_{p\mid\mathfrak{c}} (1 - \epsilon^{-1}(p)p^{-k}),$$

where $\epsilon : (\mathbf{Z}/c_0\mathbf{Z})^\times \to \mathbf{C}^\times$ is the inverse of the primitive Dirichlet character attached to ν^2. By Lemma 2.1, the prime divisors of the norm of $W(\epsilon^{-1})/W(\nu)$ divide N and therefore are co-prime to ℓ. The same obviously holds for $\mathfrak{c}/c_0$. Therefore, we eventually obtain that ℓ divides the norm of either $p^k - \epsilon^{-1}(p)$ for some p dividing $\mathfrak{c}$ (and thus c) or the norm of the numerator of $B_{k,\epsilon}/2k$. This completes the proof of Theorem 2.5.

2.5. *Proof of Theorem* 2.6

As already mentioned, the first part of Theorem 2.6 is a direct corollary of Theorem 2.5. So let us assume $k = 2$ and $\ell \nmid 6N$. By the reasoning at the beginning of § 2.3, we may write

$$\bar{\rho}^{ss} \simeq \mathbf{1} \oplus \bar{\chi}_\ell, \tag{2.8}$$

where $\mathbf{1}$ is the trivial character of $\mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$. In particular, we have $\mathfrak{c}^2 = N(\bar{\rho}^{ss}) = 1$, hence $\mathfrak{c} = 1$. Let now $p \in \{p_1, \ldots, p_t\}$ be a prime dividing N. By § 1.1, the local representation $\bar{\rho}_p$ at p semi-simplifies to

$$\lambda(a_p) \oplus \lambda(a_p)\bar{\chi}_\ell. \tag{2.9}$$

Comparing (2.8) and (2.9), we obtain the following equality between sets of characters of G_p:

$$\{\mathbf{1}, \bar{\chi}_\ell\} = \{\lambda(a_p)\bar{\chi}_\ell, \lambda(a_p)\}.$$

Moreover, if $a_p = -1$, then the character $\lambda(a_p)$ is non-trivial and, therefore, we must have $\lambda(a_p) = \bar{\chi}_\ell$ as characters of G_p. In other words, $p \equiv -1 \pmod{\ell}$. This proves assertion ((ii)(a)) of Theorem 2.6.

Before proving the next two assertions, note that we precisely are in the excluded situation of § 2.3, namely $k = 2$ and $\mathfrak{c} = 1$. For that reason, we cannot use the Eisenstein series E as in the proof of Theorem 2.5 (cf. § 2.4).

To circumvent the lack of weight 2 level 1 Eisenstein series, it will be more convenient to directly work with modular forms over $\bar{\mathbf{F}}_\ell$. Let E_2 be the classical series in characteristic 0 defined by

$$E_2(\tau) = -\frac{1}{24} + \sum_{n \geqslant 1} \sigma_1(n) q^n.$$

Recall that E_2 is not a modular form (it is a quasi-modular form). However, its reduction modulo ℓ (recall that $\ell \geqslant 5$), denoted by $\bar{E}_2$, is a well-defined modular form over $\bar{\mathbf{F}}_\ell$. Moreover, as a modular form over $\bar{\mathbf{F}}_\ell$ of level N (which is co-prime to ℓ by assumption), $\bar{E}_2$ has filtration $\ell + 1$ (see [**29**]). Put

$$E' = \left[\prod_{p|N} (a_p U_p - p\mathrm{Id})\right] \bar{E}_2,$$

where U_p denotes the usual Hecke operator at p. The following proposition summarizes the main properties of E'.

PROPOSITION 2.10. *As a modular form over $\bar{\mathbf{F}}_\ell$, E' is a well-defined normalized $(a_1(E') = 1)$ eigenform for all the Hecke operators at level $\Gamma_0(N)$ such that*

$$\begin{cases} T_r E' = (1 + r)E' & \text{for all primes } r \nmid N, \\ U_p E' = a_p E' & \text{for any prime } p \mid N. \end{cases}$$

Moreover, E' has filtration 2 unless $(a_{p_1}(f),\dots,a_{p_t}(f))=(-1,\dots,-1)$ when it has filtration $\ell+1$. The constant term of its Fourier expansion at infinity is given by

$$a_0(E')=\begin{cases}(-1)^{t+1}\dfrac{(p_1-1)\cdots(p_t-1)}{24} & \text{if } (a_{p_1}(f),\dots,a_{p_t}(f))=(+1,\dots,+1),\\ 0 & \text{otherwise.}\end{cases}$$

Proof. By the commutativity of the Hecke algebra, E' is a well-defined modular form over $\bar{\mathbf{F}}_\ell$ of level N. Let r be a prime not dividing N. Since $T_r\bar{E}_2=(1+r)\bar{E}_2$, we obtain that $T_rE'=(1+r)E'$, as claimed.

Let $u\neq 1$ be an integer dividing N. We denote by $\bar{E}_{2,u}$ the reduction modulo ℓ of the classical characteristic-0 Eisenstein series $E_{2,u}\in\mathcal{M}_2(\Gamma_0(u))$ defined by

$$E_{2,u}(\tau)=E_2(\tau)-uE_2(u\tau)=\frac{u-1}{24}+\sum_{n\geqslant 1}\left(\sum_{\substack{0<m|n\\ u\nmid m}}m\right)q^n. \tag{2.10}$$

If p is a prime divisor of N, then recall that we have

$$U_p\bar{E}_2=\bar{E}_{2,p}+p\bar{E}_2;$$
$$U_p\bar{E}_{2,u}=\begin{cases}\bar{E}_{2,p}+(1+p)\bar{E}_{2,u}-\bar{E}_{2,pu} & \text{if } p\nmid u,\\ \bar{E}_{2,p}+p\bar{E}_{2,u/p} & \text{if } p\mid u \text{ and } p\neq u,\\ \bar{E}_{2,p} & \text{if } p=u.\end{cases}$$

So let p be a prime divisor of N. We have

$$\begin{aligned}(a_pU_p-p\mathrm{Id})U_p\bar{E}_2&=((a_pU_p-p\mathrm{Id}))(\bar{E}_{2,p}+p\bar{E}_2)\\ &=p^2(a_p-1)\bar{E}_2+(a_p-p+pa_p)\bar{E}_{2,p}.\end{aligned}$$

If $a_p=+1$, then we obtain $(a_pU_p-p\mathrm{Id})U_p\bar{E}_2=\bar{E}_{2,p}=(a_pU_p-p\mathrm{Id})\bar{E}_2$, which is the desired result. On the other hand, if $a_p=-1$, then, by the assertion ((ii)(a)) proved above, we have $p\equiv -1\pmod{\ell}$ and the previous equality between forms over $\bar{\mathbf{F}}_\ell$ thus gives

$$(a_pU_p-p\mathrm{Id})U_p\bar{E}_2=-2\bar{E}_2+\bar{E}_{2,p}=-(a_pU_p-p\mathrm{Id})\bar{E}_2.$$

To complete the proof, it now remains to compute the filtration of E' and the first two terms of its Fourier expansion at infinity. Let $s=\sharp\{1\leqslant i\leqslant t\mid a_{p_i}(f)=+1\}$. If $0<s<t$, then we may assume, without loss of generality, that

$$N=p_1\cdots p_s\cdot p_{s+1}\cdots p_t\quad\text{with}\quad\begin{cases}U_{p_i}f=f & \text{for all } 1\leqslant i\leqslant s,\\ U_{p_i}f=-f & \text{for all } s+1\leqslant i\leqslant t.\end{cases}$$

By induction on t, we prove that

$$E'=\delta_{(s=0)}2^t\bar{E}_2+\sum_{\substack{(k,l)\in\{0,\dots,s\}\times\{0,\dots,t-s\}\\ (k,l)\neq(0,0)}}(-1)^{k+1}\sum_{\substack{1\leqslant i_1<\cdots<i_k\leqslant s\\ s+1\leqslant j_1<\cdots<j_l\leqslant t}}\bar{E}_{2,p_{i_1}\cdots p_{i_k}\cdot p_{j_1}\cdots p_{j_l}},$$

where

$$\delta_{(s=0)}=\begin{cases}1 & \text{if } s=0,\\ 0 & \text{otherwise,}\end{cases}$$

and the condition $1\leqslant i_1<\cdots<i_k\leqslant s$ or $s+1\leqslant j_1<\cdots<j_l\leqslant t$ is empty if $s=0$ or $s=t$, respectively. From this equality the assertion about the filtration follows. Moreover, an easy computation using Newton's binomial theorem and (2.10) proves the assertions about the first two Fourier coefficients. □

Let us now complete the proof of Theorem 2.6. According to (2.8) and the previous proposition, we have

$$a_n(\bar{f}) = a_n(E') \quad \text{for all prime-to-}\ell \text{ integers } n,$$

where $\bar{f}$ denotes the modular form over $\bar{\mathbf{F}}_\ell$ obtained by reduction of f modulo λ. Since $\ell \geqslant 5 > k+1 = 3$, Katz's theory [**12**, Corollary (3)] actually shows that $\bar{f} = E'$. Thus, E' has filtration 2 and we cannot have $(a_{p_1}(f), \dots, a_{p_t}(f)) = (-1, \dots, -1)$. Moreover, the constant term of E' at infinity must vanish and when $(a_{p_1}(f), \dots, a_{p_t}(f)) = (+1, \dots, +1)$, this gives the congruence stated in the theorem.

2.6. *Proof of Theorem* 2.7

Assume $\bar{\rho}$ to be reducible with $\ell \nmid N$ and $\ell + 1 \geqslant k$. As in § 2.4, we have

$$\bar{\rho}^{ss} \simeq \bar{\nu} \oplus \bar{\nu}^{-1}\bar{\chi}_\ell, \tag{2.11}$$

where $\bar{\nu}$ is a character of conductor $\mathfrak{c}$ such that $N(\bar{\rho}^{ss}) = \mathfrak{c}^2 \mid N$. So, in particular, we have $\mathfrak{c} \mid c$.

If $\mathfrak{c} \neq c$, then we necessarily are in a degenerate case as described in § 1.2, with $e_p = 2$ at some prime divisor p of c. Therefore, $v_p(N) = 2$ and, by Proposition 1.1, we have $p \equiv \pm 1 \pmod{\ell}$.

We can thus assume, from now on, that $\mathfrak{c} = c$. Let us denote by ν the Teichmüller lift of $\bar{\nu}$, viewed as a primitive Dirichlet character modulo c.

Let $1 \leqslant i \leqslant t$. Comparing the restriction to a decomposition group at p_i of $\bar{\rho}^{ss}$ with the local representation given by (1.1), we obtain the following equality between sets of characters of G_{p_i}:

$$\{\bar{\nu}, \bar{\nu}^{-1}\bar{\chi}_\ell\} = \{\lambda(a_{p_i})\bar{\chi}_\ell, \lambda(a_{p_i})\},$$

where $\lambda(a_{p_i})$ is the quadratic character defined in § 1.1.

Assume that, for some $1 \leqslant i \leqslant t$, we have $\bar{\nu} = \lambda(a_{p_i})\bar{\chi}_\ell$ (again, as characters of G_{p_i}). Since $a_{p_i} = \pm 1$, it then follows that ℓ divides the norm of $\nu(p_i)^2 - p_i^2$.

From now on, we will therefore assume that $\bar{\nu} = \lambda(a_{p_i})$ for every $1 \leqslant i \leqslant t$. It then follows that $\bar{\nu}(p_i) = a_{p_i} \pmod{\ell}$. Since $\mathfrak{c} > 1$, we may consider the Eisenstein series

$$E(\tau) = \sum_{n \geqslant 1} \sigma_1^\nu(n) q^n \in \mathcal{M}_2(\Gamma_0(\mathfrak{c}^2))$$

introduced in § 2.3. This is an eigenform for all the Hecke operators at level $\Gamma_0(\mathfrak{c}^2)$.

2.6.1. *The Eisenstein series* E'

Put

$$E'(\tau) = \left[\prod_{i=1}^{t} (U_{p_i} - p_i \nu^{-1}(p_i)\mathrm{Id})\right] E(p_1 \cdots p_t \tau) \in \mathcal{M}_2(\Gamma_0(N)),$$

where U_{p_i} denotes the p_ith Hecke operator acting on $\mathcal{M}_2(\Gamma_0(N))$. In expanded form, we have

$$E'(\tau) = E + \sum_{j=1}^{t} (-1)^j \sum_{1 \leqslant i_1 < \cdots < i_j \leqslant t} p_{i_1} \cdots p_{i_j} \nu^{-1}(p_{i_1} \cdots p_{i_j}) E(p_{i_1} \cdots p_{i_j} \tau). \tag{2.12}$$

As before, let us denote by L the field generated by the values of ν and by M the compositum of L and K. The following lemma is crucial.

LEMMA 2.11. *The Eisenstein series E' is a normalized eigenform for all the Hecke operators at level $\Gamma_0(N)$. Moreover, there exists a prime ideal $\mathcal{L}$ above ℓ in the integer ring of M such that*

$$a_r \equiv a_r(E') \pmod{\mathcal{L}} \quad \textit{for all primes } r \neq \ell.$$

Proof. The Eisenstein series E' is clearly normalized and, since ℓ is co-prime to N, this is an eigenfunction for the T_ℓ-operator acting on $\mathcal{M}_2(\Gamma_0(N))$. By isomorphism (2.11) and assumption $\bar{\nu}(p_i) = a_{p_i} \pmod{\ell}$, $1 \leqslant i \leqslant t$, there exists a prime ideal $\mathcal{L}$ above ℓ in the integer ring of M such that

$$\nu(r) + \nu^{-1}(r)r \equiv a_r \pmod{\mathcal{L}} \quad \text{for every prime } r \nmid \ell N$$

and $\nu(p_i) \equiv a_{p_i} \pmod{\mathcal{L}}$ for any $1 \leqslant i \leqslant t$. Let r be a prime. If r does not divide ℓN, then E' is a T_r-eigenfunction with eigenvalue $a_r(E') = \nu(r) + \nu^{-1}(r)r$, which is congruent to a_r modulo $\mathcal{L}$. Otherwise, if r divides c (and thus N), then E' is a U_r-eigenfunction with corresponding eigenvalue $0 = a_r$. Finally, if $r = p_j \in \{p_1, \dots, p_t\}$, then we have

$$(U_{p_j}E')(\tau) = \left(\prod_{\substack{i=1 \\ i \neq j}}^{t} (U_{p_i} - p_i\nu^{-1}(p_i)\mathrm{Id}) \right) \cdot (U_{p_j}^2 - p_j\nu^{-1}(p_j)U_{p_j})E(p_1 \cdots p_t\tau).$$

Besides, according to [**5**, Proposition 5.2.2], we have

$$\begin{aligned}
&(U_{p_j}^2 - p_j\nu^{-1}(p_j)U_{p_j})E(p_1 \cdots p_t\tau) \\
&\quad = (\nu(p_j) + \nu^{-1}(p_j)p_j)E(\widehat{p_1 \cdots p_t}\tau) - p_jE(p_1 \cdots p_t\tau) - p_j\nu^{-1}(p_j)E(\widehat{p_1 \cdots p_t}\tau) \\
&\quad = \nu(p_j)(U_{p_j} - p_j\nu^{-1}(p_j)\mathrm{Id})E(p_1 \cdots p_t\tau),
\end{aligned}$$

where $\widehat{p_1 \cdots p_t} = \prod_{\substack{i=1 \\ i \neq j}}^{t} p_i$. This equality proves that E' is a U_{p_j}-eigenfunction with corresponding eigenvalue $\nu(p_j)$ and the congruence $\nu(p_j) \equiv a_{p_j} \pmod{\mathcal{L}}$ eventually completes the proof of the lemma. □

2.6.2. *Constant term at $1/\mathfrak{c}$ and end of the proof of Theorem* 2.7 Since E' vanishes at ∞, we compute its constant term at another specific cusp, where it is non-vanishing, namely $1/\mathfrak{c}$. Put

$$\gamma = \begin{pmatrix} 1 & 0 \\ \mathfrak{c} & 1 \end{pmatrix} \in \mathrm{SL}(2, \mathbf{Z}).$$

We postpone the proof of the following proposition to § 2.6.3.

Proposition 2.12. *The constant term of the Fourier expansion of $E'|_2\gamma$ is the non-zero algebraic number in $\mathcal{O}_L[1/\mathfrak{c}^2](\mu_{\mathfrak{c}^2})$:*

$$\Upsilon' = -\nu(-1)\left(\frac{\mathfrak{c}}{c_0}\right)^2 \frac{W((\nu^2)_0)}{W(\nu)} \frac{B_{2,(\nu^2)_0^{-1}}}{4} \left(\prod_{i=1}^{t} (1 - p_i^{-1}) \right) \cdot \left(\prod_{p \mid \mathfrak{c}} (1 - (\nu^2)_0(p)p^{-2}) \right),$$

where the second product runs over the primes and $(\nu^2)_0$ is the primitive Dirichlet character associated to ν^2 of modulus $c_0 \mid \mathfrak{c}$.

Using this proposition, we now complete the proof of Theorem 2.7. Let Θ be the Katz's operator on modular forms over $\bar{\mathbf{F}}_\ell$, whose action on q-expansions is given by $q(d/dq)$ (denoted by $A\theta$ in [**12**]). Assume $\ell > k + 1 = 3$. Lemma 2.11 implies that $\Theta(\bar{f}) = \Theta(\bar{E})$, where $\bar{f}$ and $\overline{E'}$ are the modular forms over $\bar{\mathbf{F}}_\ell$ obtained by reduction modulo $\mathcal{L}$ of f and E', respectively. Moreover, Katz has proved that if $\ell > 3$, then Θ is injective [**12**, Corollary (3)]. Under this assumption, it thus follows that the Eisenstein series E' becomes cuspidal after reduction.

Put $\epsilon = (\nu^2)_0^{-1}$. By Proposition 2.12 and using the assumption $\mathfrak{c} = c$, we therefore have that ℓ divides the numerator of the norm of

$$\Upsilon' = \pm \left(\frac{c}{c_0}\right)^2 \frac{W(\epsilon^{-1})}{W(\nu)} \frac{B_{2,\epsilon}}{4} \left(\prod_{i=1}^{t}(1-p_i^{-1})\right) \cdot \left(\prod_{p|c}(1-\epsilon^{-1}(p)p^{-2})\right).$$

By Lemma 2.1, the prime divisors of the norm of $W(\epsilon^{-1})/W(\nu)$ divide N and therefore are co-prime to ℓ. The same obviously holds for c/c_0. It thus follows that either $p_i \equiv 1 \pmod{\ell}$ for some $1 \leqslant i \leqslant t$, or ℓ divides the norm of either $p^2 - \epsilon^{-1}(p)$ for some p dividing c, or the norm of the numerator of $B_{2,\epsilon}/4$. This completes the proof of Theorem 2.7.

2.6.3. *Proof of Proposition* 2.12 Let us first introduce notation as in the proof of Proposition 2.8. Put

$$G = \frac{C_2 W(\nu)}{\mathfrak{c}^2} E, \quad \text{where } C_2 = -4\pi^2,$$

and similarly

$$G' = \frac{C_2 W(\nu)}{\mathfrak{c}^2} E'.$$

For simplicity, we shall denote by $\underline{i}$ the elements of

$$\mathcal{N} = \{(i_1, \ldots, i_j) \text{ such that } j \in \{1, \ldots, t\} \text{ and } 1 \leqslant i_1 < \cdots < i_j \leqslant t\}.$$

If $\underline{i} = (i_1, \ldots, i_j) \in \mathcal{N}$, we put

$$p_{\underline{i}} = p_{i_1} \cdots p_{i_j} \quad \text{and} \quad a_{\underline{i}} = a_{p_{i_1}} \cdots a_{p_{i_j}}.$$

Let $v = \overline{(c_v, d_v)} \in (\mathbf{Z}/\mathfrak{c}^2\mathbf{Z})^2$ of order $\mathfrak{c}^2$. Following [5, § 4.6], define

$$G_2^v(\tau) = \frac{1}{(c_v\tau + d_v)^2} + \frac{1}{\mathfrak{c}^4} \sum_{d \in \mathbf{Z}}{}' \frac{1}{((c_v\tau + d_v)/\mathfrak{c}^2 - d)^2} + \frac{1}{\mathfrak{c}^4} \sum_{c \neq 0} \sum_{d \in \mathbf{Z}} \frac{1}{((c_v\tau + d_v)/\mathfrak{c}^2 - c\tau - d)^2}, \tag{2.13}$$

where the primed summation notation means to sum over non-zero integers. For any $\underline{i} \in \mathcal{N}$ and any $v \in (\mathbf{Z}/\mathfrak{c}^2\mathbf{Z})^2$ of order $\mathfrak{c}^2$, put

$$G_2^{v,p_{\underline{i}}}(\tau) = G_2^v(p_{\underline{i}}\tau) \quad \text{and} \quad G^{p_{\underline{i}}}(\tau) = G(p_{\underline{i}}\tau).$$

According to [5, § 4.2] and the definition of E (cf. § 2.3), we have

$$G = \frac{1}{2} \sum_{i,j,l=0}^{\mathfrak{c}-1} \nu(ij) G_2^{\overline{(i\mathfrak{c}, j+l\mathfrak{c})}}$$

and therefore

$$G^{p_{\underline{i}}} = \frac{1}{2} \sum_{i,j,l=0}^{\mathfrak{c}-1} \nu(ij) G_2^{\overline{(i\mathfrak{c}, j+l\mathfrak{c})}, p_{\underline{i}}}. \tag{2.14}$$

Lemma 2.13. *Let $v = \overline{(c_v, d_v)} \in (\mathbf{Z}/\mathfrak{c}^2\mathbf{Z})^2$ of order $\mathfrak{c}^2$. The constant term of $G_2^{v,p_{\underline{i}}}|_2\gamma$ is*

$$\Upsilon_{v,\underline{i}} = \vartheta(\overline{c_v p_{\underline{i}} + d_v \mathfrak{c}}) \left(\frac{1}{p_{\underline{i}}}\right)^2 \zeta^{\overline{d_v/p_{\underline{i}}}}(2),$$

where the bar means reduction modulo $\mathfrak{c}^2$,

$$\vartheta(\bar{n}) = \begin{cases} 1 & \text{if } n \equiv 0 \pmod{\mathfrak{c}^2}, \\ 0 & \text{otherwise,} \end{cases} \qquad \zeta^{\bar{n}}(2) = \sum_{m \equiv n \pmod{\mathfrak{c}^2}}{}' \frac{1}{m^2},$$

and the primed summation notation means to sum over non-zero integers.

Proof. We first compute $G_2^{v,p_{\underline{i}}}|_2\gamma$ using (2.13). We find

$$(G_2^{v,p_{\underline{i}}}|_2\gamma)(\tau) = \frac{1}{(c_v p_{\underline{i}}\tau + d_v(\mathfrak{c}\tau+1))^2} + \sum_{d\in\mathbf{Z}}{}' \frac{1}{(c_v p_{\underline{i}}\tau + d_v(\mathfrak{c}\tau+1) - \mathfrak{c}^2 d(\mathfrak{c}\tau+1))^2} + \sum_{c\neq 0}\sum_{d\in\mathbf{Z}} \frac{1}{(c_v p_{\underline{i}}\tau + d_v(\mathfrak{c}\tau+1) - \mathfrak{c}^2(cp_{\underline{i}}\tau + d(\mathfrak{c}\tau+1)))^2}.$$

In other words, we have $(G_2^{v,p_{\underline{i}}}|_2\gamma)(\tau) = A + B$, where

$$A = \frac{1}{((c_v p_{\underline{i}} + d_v\mathfrak{c})\tau + d_v)^2} + \sum_{d\in\mathbf{Z}}{}' \frac{1}{((c_v p_{\underline{i}} + d_v\mathfrak{c} - \mathfrak{c}^2 d\mathfrak{c})\tau + d_v - \mathfrak{c}^2 d)^2}$$

and

$$B = \sum_{c\neq 0}\sum_{d\in\mathbf{Z}} \frac{1}{((c_v p_{\underline{i}} + d_v\mathfrak{c} - \mathfrak{c}^2(cp_{\underline{i}} + d\mathfrak{c}))\tau + d_v - \mathfrak{c}^2 d)^2}.$$

Since $\gcd(p_{\underline{i}}, \mathfrak{c}) = 1$, we may assume, without loss of generality, that $0 \leqslant c_v p_{\underline{i}} + d_v\mathfrak{c} < \mathfrak{c}^2$. Therefore, the constant term of A is given by

$$\vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}})\frac{1}{d_v^2}$$

and the one of B by

$$\vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}})\sum_{c\neq 0}\sum_{\substack{d\in\mathbf{Z} \\ cp_{\underline{i}}+d\mathfrak{c}=0}} \frac{1}{(d_v - \mathfrak{c}^2 d)^2}.$$

Therefore, the constant term of $G_2^{v,p_{\underline{i}}}|_2\gamma$ is

$$\Upsilon_{v,\underline{i}} = \vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}})\sum_{c\in\mathbf{Z}}\sum_{\substack{d\in\mathbf{Z} \\ cp_{\underline{i}}+d\mathfrak{c}=0}} \frac{1}{(d_v - \mathfrak{c}^2 d)^2}.$$

Note that if $\vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}}) = 1$, then $d_v \not\equiv 0 \pmod{\mathfrak{c}^2}$ since v is of order $\mathfrak{c}^2$. A change of variable yields

$$\Upsilon_{v,\underline{i}} = \vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}})\sum_{c\in\mathbf{Z}}\sum_{\substack{d\in\mathbf{Z} \\ cp_{\underline{i}}+d\mathfrak{c}=0 \\ (c,d)\equiv v \ (\mathfrak{c}^2)}} \frac{1}{d^2}$$

and thus

$$\Upsilon_{v,\underline{i}} = \vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}})\sum_{\substack{d\neq 0 \\ d\equiv d_v \ (\mathfrak{c}^2) \\ p_{\underline{i}}|d}} \frac{1}{d^2} = \vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}})\sum_{\substack{m\neq 0 \\ m\equiv d_v/p_{\underline{i}} \ (\mathfrak{c}^2)}} \frac{1}{(p_{\underline{i}} m)^2}.$$

Finally, we obtain $\Upsilon_{v,\underline{i}} = \vartheta(\overline{c_v p_{\underline{i}} + d_v\mathfrak{c}})/p_{\underline{i}}^2 \cdot \zeta^{\overline{d_v/p_{\underline{i}}}}(2)$, as asserted. □

Using this lemma and formula (2.14), we are now able to compute the constant term of $G^{p_{\underline{i}}}|_2\gamma$.

LEMMA 2.14. *The constant term of* $G^{p_{\underline{i}}}|_2\gamma$ *is*

$$\Upsilon_{\underline{i}} = \nu(p_{\underline{i}})\frac{1}{p_{\underline{i}}^2}\cdot\Upsilon_0, \quad \text{with } \Upsilon_0 = -\nu(-1)W((\nu^2)_0)\frac{C_2}{c_0^2}\frac{B_{2,(\nu^2)_0^{-1}}}{4}\prod_{p\mid\mathfrak{c}}(1-(\nu^2)_0(p)p^{-2}),$$

where $(\nu^2)_0$ *is the primitive Dirichlet character associated to* ν^2 *of modulus* $c_0 \mid \mathfrak{c}$.

Proof. The proof of this lemma is quite similar to the proof of Proposition 2.8. According to (2.14), we have

$$\Upsilon_{\underline{i}} = \frac{1}{2}\sum_{i,j,l=0}^{\mathfrak{c}-1}\nu(ij)\Upsilon_{\overline{(i\mathfrak{c},j+l\mathfrak{c})},\underline{i}}$$

and thus, by Lemma 2.13,

$$\Upsilon_{\underline{i}} = \frac{1}{2}\cdot\frac{1}{p_{\underline{i}}^2}\sum_{i,j,l=0}^{\mathfrak{c}-1}\nu(ij)\vartheta(\overline{i\mathfrak{c}p_{\underline{i}}+\mathfrak{c}(j+l\mathfrak{c})})\zeta^{\overline{d_v/p_{\underline{i}}}}(2).$$

This yields

$$\begin{aligned}\Upsilon_{\underline{i}} &= \frac{1}{2}\cdot\frac{1}{p_{\underline{i}}^2}\sum_{l=0}^{\mathfrak{c}-1}\sum_{\substack{j=0\\ \gcd(j,\mathfrak{c})=1}}^{\mathfrak{c}-1}\nu\left(-\frac{j^2}{p_{\underline{i}}}\right)\zeta^{\overline{d_v/p_{\underline{i}}}}(2)\\ &= \frac{1}{2}\cdot\frac{1}{p_{\underline{i}}^2}\nu(p_{\underline{i}})\nu(-1)\sum_{l=0}^{\mathfrak{c}-1}\sum_{\substack{j=0\\ \gcd(j,\mathfrak{c})=1}}^{\mathfrak{c}-1}\nu((j^2/p_{\underline{i}})^2)\sum_{m\equiv(j+l\mathfrak{c})/p_{\underline{i}}\ (\mathfrak{c}^2)}{}'\frac{1}{m^2}\\ &= \frac{1}{p_{\underline{i}}^2}\nu(p_{\underline{i}})\nu(-1)L(2,\nu^2).\end{aligned}$$

Let $(\nu^2)_0$ be the primitive character associated to ν^2 of modulus $c_0 \mid \mathfrak{c}$. We have

$$L(2,\nu^2) = L(2,(\nu^2)_0)\prod_{p\mid\mathfrak{c}}(1-(\nu^2)_0(p)p^{-2}).$$

Applying Proposition 2.3 to $\psi = (\nu^2)_0$ and $m = k$, we obtain

$$L(2,(\nu^2)_0) = -W((\nu^2)_0)\frac{C_2}{c_0^2}\frac{B_{2,(\nu^2)_0^{-1}}}{4} \neq 0$$

and thus

$$\Upsilon_{\underline{i}} = -\frac{1}{p_{\underline{i}}^2}\nu(p_{\underline{i}})\nu(-1)W((\nu^2)_0)\frac{C_2}{c_0^2}\frac{B_{2,(\nu^2)_0^{-1}}}{4}\prod_{p\mid\mathfrak{c}}(1-(\nu^2)_0(p)p^{-2}),$$

as claimed. □

Let us now complete the proof of Proposition 2.12. With the notation introduced at the beginning of this paragraph and Equation (2.12), we have

$$G'|_2\gamma = G|_2\gamma + \sum_{\underline{i}\in\mathcal{N}}(-1)^{\sharp\underline{i}}p_{\underline{i}}\nu^{-1}(p_{\underline{i}})G^{p_{\underline{i}}}|_2\gamma.$$

Therefore, according to Proposition 2.8 and Lemma 2.14, the constant term of $G'|_2\gamma$ is

$$\Upsilon_0 + \sum_{\underline{i}\in\mathcal{N}}(-1)^{\sharp\underline{i}}p_{\underline{i}}\nu^{-1}(p_{\underline{i}})\Upsilon_{\underline{i}} = \Upsilon_0\left(1+\sum_{\underline{i}\in\mathcal{N}}(-1)^{\sharp\underline{i}}p_{\underline{i}}\nu^{-1}(p_{\underline{i}})\nu(p_{\underline{i}})\frac{1}{p_{\underline{i}}^2}\right) = \Upsilon_0\prod_{i=1}^{t}(1-p_i^{-1}),$$

where $(\nu^2)_0$ is the primitive character associated to ν^2 of modulus $c_0 \mid \mathfrak{c}$. Proposition 2.12 now follows from the normalization $E' = (\mathfrak{c}^2/(C_2 W(\nu)))G'$.

3. *Dihedral representations*

3.1. *Preliminaries: twisting and CM forms*

Let M be an integer, $F(\tau) = \sum_{n\geqslant 1} a_n(F)q^n \in \mathcal{S}_k(\Gamma_0(M))$ and ψ be a Dirichlet character of modulus $f \geqslant 1$. Define

$$(F \otimes \psi)(\tau) = \sum_{n\geqslant 1} a_n(F)\psi(n)q^n.$$

The following result is a special case of [**30**, Proposition 3.64].

LEMMA 3.1. *With the notation above, assume ψ to be a quadratic primitive Dirichlet character. Then $F \otimes \psi$ belongs to $\mathcal{S}_k(\Gamma_0(\mathrm{lcm}(M, f^2)))$. Moreover, if F is a normalized Hecke eigenform for the Hecke operators $\{T_p\}_{p\nmid M}$, then $F \otimes \psi$ is a normalized Hecke eigenform for the Hecke operators $\{T_p\}_{p\nmid fM}$ with corresponding eigenvalues $\{a_p(F)\psi(p)\}_{p\nmid fM}$.*

We take the following definition for CM forms [**24**].

DEFINITION 1. Assume that ψ is not the trivial character. The form F has complex multiplication (or, F is a CM form) by ψ if $a_p(F) = a_p(F)\psi(p)$ for all p in a set of primes of density 1.

3.2. *Statement of the result*

Recall that

$$\mathbf{P}(\bar{\rho}_{f,\lambda}) : G_{\mathbf{Q}} \xrightarrow{\bar{\rho}_{f,\lambda}} \mathrm{GL}(2, \mathbf{F}_\lambda) \longrightarrow \mathrm{PGL}(2, \mathbf{F}_\lambda),$$

where $G_{\mathbf{Q}} = \mathrm{Gal}(\bar{\mathbf{Q}}/\mathbf{Q})$, and put $\mathbf{P}(\bar{G}_\lambda) = \mathbf{P}(\bar{\rho}_{f,\lambda})(G_{\mathbf{Q}})$.

The following result is a generalization to arbitrary weights and fields of coefficients of a theorem on the surjectivity of Galois representations attached to elliptic curves over $\mathbf{Q}$ independently proved by Kraus [**14**] and Cojocaru [**4**]. In particular, it implies that, in the case of dihedral projective image, ℓ is explicitly bounded in terms of k and N.

THEOREM 3.2. *Assume that $\mathbf{P}(\bar{G}_\lambda)$ is dihedral. If f does not have complex multiplication, then we have*

$$\ell \leqslant (2(8kN^2(1 + \log\log N))^{(k-1)/2})^{[K:\mathbf{Q}]}.$$

Besides, if N is square-free, then either $\ell \mid N$, or $\ell \leqslant k$, or $\ell = 2k - 1$.

REMARK 1. (i) The integer $[K : \mathbf{Q}]$ is bounded from above by the dimension $g_0^\sharp(k, N)$ of the new subspace of $\mathcal{S}_k(\Gamma_0(N))$. A closed formula in terms of k and N for $g_0^\sharp(k, N)$ as well as asymptotic estimates can be found in [**17**].

(ii) When $N = 1$, the result goes back to Ribet (see the proof of (ii) p. 264 and the remark after [**23**, Corollary 4.5]). Moreover, our argument for the case of arbitrary square-free level is a combination of tricks from [**25**, **26**].

(iii) A newform of square-free level and trivial Nebentypus is automatically non-CM (see, for example, [**33**, § 4]).

3.3. *Proof of Theorem* 3.2

Assume $\ell \nmid N$ and $\mathbf{P}(\bar{G}_\lambda)$ dihedral. Then $\mathbf{P}(\bar{G}_\lambda)$ is an extension of $\{\pm 1\}$ by a cyclic group C, and every element of $\bar{G}_\lambda$ that does not map to C has trace 0. Hence, we may consider the following quadratic character:

$$\epsilon_\lambda : G_{\mathbf{Q}} \overset{\mathbf{P}(\bar{\rho}_{f,\lambda})}{\longrightarrow} \mathbf{P}(\bar{G}_\lambda) \longrightarrow \{\pm 1\}.$$

Let L_λ be the number field cut out by $\mathbf{P}(\bar{\rho}_{f,\lambda})$ and $K_\lambda/\mathbf{Q}$ its quadratic subextension fixed by the kernel of ϵ_λ. The extension $L_\lambda/\mathbf{Q}$ has Galois group isomorphic to $\mathbf{P}(\bar{G}_\lambda)$ while $C \simeq \mathrm{Gal}(L_\lambda/K_\lambda)$. Clearly, ϵ_λ is unramified outside ℓN. The following proposition describes more precisely the ramification set of ϵ_λ.

PROPOSITION 3.3. *Assume* $2 < \ell \nmid N$.

(i) *Let* $p \neq \ell$ *be a ramified prime for* ϵ_λ. *Then* $p^2 \mid N$.
(ii) *Assume* $\ell > k$ *and*
  (a) *either* f *is ordinary at* λ *and* $\ell \neq 2k-1$;
  (b) *or* f *is not ordinary at* λ *and* $\ell \neq 2k-3$.

Then ϵ_λ *is unramified at* ℓ.

Proof. Let p be a prime dividing N exactly once. By § 1.1, we know that the inertia subgroup I_p at p acts unipotently in $\bar{\rho}$. Since $\bar{G}_\lambda$ has prime-to-ℓ order, it follows that I_p acts trivially. So $\bar{\rho}$ and, hence, ϵ_λ are unramified at p. This proves the first part of the proposition.

Assume now $\ell > k$. Let I_ℓ be the inertia group of a decomposition subgroup at ℓ and recall that $\ell \nmid N$. We prove that ϵ_λ is unramified at ℓ under conditions (a) and (b) in turn.

(a) Assume that f is ordinary at λ and $\ell \neq 2k-1$. By § 1.3, we have

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

But $\bar{G}_\lambda$ has prime-to-ℓ order and therefore $\star = 0$. In particular, $\mathbf{P}(\bar{\rho}_{f,\lambda})(I_\ell)$ is isomorphic to the image of $\bar{\chi}_\ell^{k-1}$ which is, by Lemma 1.2, cyclic of order $(\ell-1)/\gcd(\ell-1, k-1) > 2$. Therefore, it has to be included in C, and hence ϵ_λ is unramified at ℓ.

(b) Assume that f is not ordinary at λ and $\ell \neq 2k-3$. By § 1.3, $\mathbf{P}(\bar{\rho}_{f,\lambda})(I_\ell)$ is isomorphic to the image of I_ℓ under $\psi^{(\ell-1)(k-1)}$, where ψ is a fundamental character of level 2. By the assumption $\ell \neq 2k-3$ and Lemma 1.2, it is therefore cyclic of order $(\ell+1)/\gcd(\ell+1, k-1) > 2$. We conclude as before. □

Assume N to be square-free and $\ell > k$. Then, by the above proposition, K_λ is the unique quadratic extension of $\mathbf{Q}$ ramified at ℓ only and $\ell \in \{2k-1, 2k-3\}$. The case $\ell = 2k-3$, however, does not occur. This is proved in [**6**, Lemma 3.2]. Hence, Theorem 3.2 in the square-free level case.

Assume now that N is any integer not divisible by ℓ, and that $\ell > k$ satisfies $\ell \neq 2k-1$ and $\ell \neq 2k-3$. We may identify ϵ_λ with a Dirichlet character. Let us denote by $\mathfrak{c}$ its conductor. It is co-prime to ℓ by the above proposition. We then have $\mathfrak{c} = |D_{K_\lambda}|$, where D_{K_λ} is the fundamental discriminant of the quadratic field K_λ fixed by the kernel of ϵ_λ (see [**22**, VII. § 11]). In particular, if $K_\lambda = \mathbf{Q}(\sqrt{D_0})$ with D_0 square-free, then $\mathfrak{c} = D_0$ or $4D_0$ depending on whether

$D_0 \equiv 1 \pmod 4$ or not. Moreover, if $\ell > 2k-1$, then by the proposition above, $\mathfrak{c}^2 \mid 2^4 N$. Put $g = f \otimes \epsilon_\lambda$. By the Lemma 3.1, $g \in \mathcal{S}_k(\Gamma_0(2^4 N))$ and, for any prime $p \nmid 2N$, g is an eigenform for the T_p Hecke operator with corresponding eigenvalue $a_p(g) = a_p \epsilon_\lambda(p)$. Let $D_0' = \varepsilon \prod_{3 \leqslant p \mid N} p$ be the product of all odd primes dividing N with a sign $\varepsilon \in \{\pm 1\}$ chosen so that $D_0' \equiv 3 \pmod 4$. Then $4D_0'$ is a fundamental discriminant and the Kronecker symbol $\psi = (4D_0'/\cdot)$ is a primitive quadratic Dirichlet character of modulus $4D_0'$ (see [**3**, Theorem 2.2.15]) precisely ramified at the primes dividing $2N$. Put

$$\tilde{f} = f \otimes \psi \quad \text{and} \quad \tilde{g} = g \otimes \psi.$$

Since $(4D_0')^2 \mid 2^4 N^2$, it follows from Lemma 3.1 that $\tilde{f}, \tilde{g} \in \mathcal{S}_k(\Gamma_0(2^4 N^2))$ and, for any integer n, we have

$$\begin{cases} a_n(\tilde{f}) = a_n \psi(n), \\ a_n(\tilde{g}) = a_n \epsilon_\lambda(n) \psi(n). \end{cases} \tag{3.1}$$

Since f is assumed to be non-CM (in the sense of Definition 1), we have $\tilde{f} \neq \tilde{g}$ and by Murty [**21**, Theorem 1], there exists an integer

$$n \leqslant \frac{4k}{3} N^2 \prod_{p \mid 2N} \left(1 + \frac{1}{p}\right) \leqslant 2kN^2 \prod_{p \mid N} \left(1 + \frac{1}{p}\right) \tag{3.2}$$

such that $a_n(\tilde{f}) \neq a_n(\tilde{g})$. According to (3.1), it follows that we have

$$\psi(n) \neq 0, \quad a_n \neq 0 \text{ and } \epsilon_\lambda(n) = -1.$$

From the condition $\epsilon_\lambda(n) = -1$, we deduce that there exists a prime divisor q of n together with an odd integer t such that $q^t \mid n$, but $q^{t+1} \nmid n$ and $\epsilon_\lambda(q) = -1$. If $q = \ell$, then we are done in bounding ℓ in terms of k and N. Assume therefore $q \neq \ell$. The multiplicativity of the Fourier coefficients of f gives that $a_{q^t} \mid a_n$, and hence (since t is odd) that $a_q \neq 0$. Besides, since $\epsilon_\lambda(q) = -1$, the image under $\bar{\rho}_{f,\lambda}$ of a Frobenius at q has trace 0 modulo λ. In other words, ℓ divides the norm of the non-zero algebraic integer a_q. Applying Deligne's estimate on the Fourier coefficients of f and its Galois conjugates by $\bar{\mathbf{Q}}$-automorphisms, we obtain that

$$\ell \leqslant \mathrm{N}_{K/\mathbf{Q}}(a_q) = \prod_{\sigma : K \hookrightarrow \mathbf{C}} |\sigma(a_q)| \leqslant (2q^{(k-1)/2})^{[K:\mathbf{Q}]}. \tag{3.3}$$

Besides, using [**14**, Lemma 2] and inequality (3.2), we obtain the following estimate for q:

$$q \leqslant 8kN^2(1 + \log\log N). \tag{3.4}$$

The theorem follows from (3.3) and (3.4).

4. *Projective image isomorphic to A_4, S_4 or A_5*

The following result is proved in a different way in [**25**].

THEOREM 4.1. *If $\mathbf{P}(\bar{G}_\lambda)$ is isomorphic to A_4, S_4 or A_5, then either $\ell \mid N$ or $\ell \leqslant 4k-3$.*

Proof. Assume that $\ell \nmid N$ and $\ell > k$. Then, by § 1.3, $\mathbf{P}(\bar{G}_\lambda)$ has a cyclic subgroup given the image of inertia at ℓ. In the case of ordinariness, this cyclic subgroup is isomorphic to the image of $\bar{\chi}_\ell^{k-1}$ which has order > 5 if $\ell > 4k-3$ by Lemma 1.2. Else, if f is not ordinary at λ, then it has order $(\ell+1)/\gcd(\ell+1, k-1)$ which is also > 5 if $\ell > 4k-3$.

In any case, if $\ell > 4k-3$, then $\mathbf{P}(\bar{G}_\lambda)$ has an element of order > 5. This rules out the possibility for $\mathbf{P}(\bar{G}_\lambda)$ to be isomorphic to A_4, S_4 or A_5. □

REMARK 2. In [8, Theorem 1.4(a)], Ghate and Parent give an explicit upper-bound in the weight 2 case and projective image isomorphic to A_4, S_4 or A_5, depending only (and necessarily) on $[K : \mathbf{Q}]$, but *not* on the level.

5. *Numerical examples*

In this section, we give some examples illustrating the theorems of the paper. All the computations were performed on SAGE [31].

5.1. *Reducible representations*

Before dealing with examples, let us first recall that, for the representations $\bar{\rho}_{f,\lambda}$, irreducibility is equivalent to absolute irreducibility.

5.1.1. *Square level case* Fix $(k, N) = (6, 81)$. The new subspace in $\mathcal{S}_6(\Gamma_0(81))$ is eighteen-dimensional and splits into five Galois conjugacy classes labeled 81.6a,...,81.6e in SAGE [31]. According to Theorem 2.5, the prime ideals λ such that $\bar{\rho}_{f,\lambda}$ is reducible for some newform $f \in \mathcal{S}_6(\Gamma_0(81))$ have residue characteristic ℓ in $\{2, 3, 5, 7, 43, 1171\}$. Let us first show that 2, 3, 7, 43 and 1171 are indeed the residue characteristics of some prime ideals λ, for which $\bar{\rho}_{f,\lambda}$ is reducible for the specific (up to Galois conjugacy) modular form f labeled 81.6c. We have

$$f(\tau) = q + \alpha q^2 + (\alpha^2 - 32)q^4 + (-\tfrac{1}{4}\alpha^3 - \tfrac{9}{4}\alpha^2 + \tfrac{25}{2}\alpha + 54)q^5 + O(q^5),$$

where α is a root of $X^4 + 3X^3 - 84X^2 - 72X + 792$.

Let us denote by K the number field generated by α. We call ν the primitive Dirichlet character modulo 9 sending 2 to ζ_3, where ζ_3 is a primitive third root of unity and $L = \mathbf{Q}(\zeta_3)$. Since ν has order 3, we have $\epsilon = \nu$ with the notation of Theorem 2.5. Moreover, we have $B_{6,\nu}/12 = (751\zeta_3 + 1172)/3$, which has norm $3^{-1} \cdot 7 \cdot 43 \cdot 1171$.

Then we show more precisely that, for each $\ell \in \{2, 3, 7, 43, 1171\}$, there are prime ideals λ_ℓ and $\mathfrak{p}_\ell$ above ℓ in $\mathcal{O}$ and $\mathbf{Z}[\zeta_3]$, respectively, such that $\bar{\rho}^{ss}_{f,\lambda_\ell} \simeq \bar{\rho}_{E,\mathfrak{p}_\ell}$, where E is the following Eisenstein series:

$$E(\tau) = \sum_{n \geqslant 1} \sigma_5^\nu(n)q^n = q - (31\zeta_3 + 32)q^2 + (1023\zeta_3 + 31)q^4 + (3124\zeta_3 - 1)q^5 + O(q^5).$$

Such an isomorphism is proved to hold by checking that, for all integers n up to the Sturm bound (which, here, equals 54), we have a congruence

$$a_n \equiv a_n(E) \pmod{\mathcal{L}_\ell},$$

for some prime ideal $\mathcal{L}_\ell$ above ℓ in the integer ring of the compositum KL. For instance, if $\ell = 43$, we can take

$$\mathcal{L}_{43} = (43, \alpha + \zeta_3 - 6).$$

Therefore, we have $\bar{\rho}^{ss}_{f,\lambda_\ell} \simeq \bar{\nu}_\ell \oplus \bar{\nu}_\ell^{-1}\bar{\chi}_\ell^5$ where

$$\bar{\nu}_\ell \ : G_{\mathbf{Q}} \twoheadrightarrow (\mathbf{Z}/9\mathbf{Z})^\times \xrightarrow{\nu} \mathbf{Z}[\zeta_3] \twoheadrightarrow \mathbf{Z}[\zeta_3]/\mathfrak{p}_\ell$$

is ν modulo $\mathfrak{p}_\ell$ viewed as a character of $G_{\mathbf{Q}}$. For each ℓ as above, the corresponding ideals λ_ℓ and $\mathfrak{p}_\ell$ are listed in Table 2 (as given in SAGE).

Let us now see what happens for the remaining prime, namely $\ell = 5$. For the specific newform above with coefficients field K, we have $5\mathcal{O} = \lambda_5\lambda_5'$, where $\lambda_5 = (5, \alpha + 4)$ and $\lambda_5' = (5, \alpha^3 + 4\alpha^2 + 3)$. Then λ_5 and λ_5' have inertia degree 1 and 3, respectively. Besides, if Frob_2 denotes a Frobenius at 2, the characteristic polynomial of $\bar{\rho}_{f,\lambda_5}(\mathrm{Frob}_2)$ and $\bar{\rho}_{f,\lambda_5'}(\mathrm{Frob}_2)$ is $X^2 - \alpha X + 2^5$.

TABLE 2. *Congruence primes between f and E.*

ℓ	λ_ℓ	$\mathfrak{p}_\ell$
2	$(2, \alpha^3/36 + \alpha^2/4 - 7\alpha/6 - 7)$	(2)
3	$(3, -\alpha^3/36 + \alpha^2/12 + 7\alpha/6 - 7)$	$(2\zeta_3 + 1)$
7	$(7, \alpha^3/36 + \alpha^2/12 - 5\alpha/3 + 2)$	$(3\zeta_3 + 1)$
43	$(43, \alpha^3/36 + \alpha^2/12 - 5\alpha/3 - 20)$	$(7\zeta_3 + 6)$
1171	$(1171, \alpha^3/36 + \alpha^2/12 - 5\alpha/3 - 586)$	$(39\zeta_3 + 25)$

TABLE 3. *Smallest prime $p \neq 3, 5$ and $\leqslant 100$ such that $\bar{\rho}_{f,\lambda}(\mathrm{Frob}_p)$ acts irreducibly.*

f	$K = \mathbf{Q}(\alpha)$	λ	p
81.6a	$\alpha^2 + 3\alpha - 30 = 0$	$(-6\alpha + 25)$	2
		$(-6\alpha - 43)$	7
81.6b	$\alpha^2 - 3\alpha - 30 = 0$	$(-6\alpha - 25)$	2
		$(-6\alpha + 43)$	7
81.6c	$\alpha^4 + 3\alpha^3 - 84\alpha^2 - 72\alpha + 792 = 0$	$(5, \alpha + 4)$	2
		$(5, \alpha^3 + 4\alpha^2 + 3)$	2
81.6d	$\alpha^4 - 3\alpha^3 - 84\alpha^2 + 72\alpha + 792 = 0$	$(5, \alpha + 1)$	2
		$(5, \alpha^3 + \alpha^2 + 2)$	2
81.6e	$\alpha^6 - 171\alpha^4 + 7128\alpha^2 - 432 = 0$	$(5, \alpha^2 + 1)$	$\emptyset$
		$(5, \alpha^2 + 3\alpha + 3)$	7
		$(5, \alpha^2 + 2\alpha + 3)$	7

Such a polynomial being irreducible modulo λ_5 and λ_5' as one checks, we obtain that $\bar{\rho}_{f,\lambda_5}$ and $\bar{\rho}_{f,\lambda_5'}$ are both irreducible.

For each pair (f, λ), where f is a newform in $\mathcal{S}_6(\Gamma_0(81))$ and λ is a prime ideal in $\mathcal{O}$ above 5, we give in Table 3 the smallest prime number $p \neq 3, 5$ and $\leqslant 100$ for which the characteristic polynomial of $\bar{\rho}_{f,\lambda}(\mathrm{Frob}_p)$ is irreducible.

Therefore, all the representations $\bar{\rho}_{f,\lambda}$ are irreducible unless perhaps if f is the form 81.6e and $\lambda = (5, \alpha^2 + 1)$. But this latter representation is also proved to be irreducible by noting that the eigenvalues of $\bar{\rho}_{f,\lambda}(\mathrm{Frob}_2)$ and $\bar{\rho}_{f,\lambda}(\mathrm{Frob}_{19})$ in $\mathbf{F}_\lambda$ are $\{3\beta, 3\beta\}$ and $\{2\beta + 1, 3\beta + 1\}$, respectively, where β is the image of α in $\mathbf{F}_\lambda$ (since if it were reducible, we would have $\bar{\rho}_{f,\lambda}^{ss} \simeq \epsilon_1 \oplus \epsilon_2$, where both ϵ_1 and ϵ_2 factor through $(\mathbf{Z}/45\mathbf{Z})^\times$). This eventually proves the following proposition.

PROPOSITION 5.1. *There exists a newform $f \in \mathcal{S}_6(\Gamma_0(81))$ together with a prime ideal λ in $\mathcal{O}$ such that $\bar{\rho}_{f,\lambda}$ is reducible if and only if ℓ belongs to $\{2, 3, 7, 43, 1171\}$.*

5.1.2. *Square-free level case* Fix $(k, N) = (4, 11)$. The new subspace in $\mathcal{S}_4(\Gamma_0(11))$ is two-dimensional and generated by one Galois orbit labeled 11.4a in SAGE [31]. Let f be a representative of this Galois orbit. We have

$$f(\tau) = q + \alpha q^2 + (-4\alpha + 3)q^3 + (2\alpha - 6)q^4 + (8\alpha - 7)q^5 + O(q^5),$$

where α is a root of $X^2 - 2X - 2$. The field $K = \mathbf{Q}(\alpha)$ is the coefficients field of f. According to Theorem 2.6, if $\bar{\rho}_{f,\lambda}$ is reducible, then λ has residue characteristic ℓ in the set $\{2, 3, 5, 11, 61\}$.

For each prime ℓ in $\{2,3,5,11,61\}$, we give in Table 4 the smallest prime $p \neq 11, \ell$ and $p \leqslant 100$ such that the characteristic polynomial of $\bar{\rho}_{f,\lambda}(\mathrm{Frob}_p)$ is irreducible.

Therefore, all such Galois representations are irreducible, except perhaps $\bar{\rho}_{f,(2\alpha-1)}$ and $\bar{\rho}_{f,(\alpha-9)}$. These latter representations turn out to be reducible and we have

$$\bar{\rho}^{ss}_{f,(2\alpha-1)} \simeq \bar{\chi}_{11} \oplus \bar{\chi}_{11}^2 \quad \text{and} \quad \bar{\rho}^{ss}_{f,(\alpha-9)} \simeq \mathbf{1} \oplus \bar{\chi}_{61}^3 \simeq \bar{\rho}_{E_4,61}.$$

This eventually proves the following proposition.

PROPOSITION 5.2. *There exists a newform $f \in \mathcal{S}_4(\Gamma_0(11))$ together with a prime ideal λ in $\mathcal{O}$ such that $\bar{\rho}_{f,\lambda}$ is reducible if and only if $\ell = 11$ or $\ell = 61$.*

5.2. *Dihedral representation*

In this section, we discuss an example of dihedral projective representation attached to some specific newform. The new subspace in $\mathcal{S}_2(\Gamma_0(1888))$ has dimension 58 and is split into 16 Galois orbits. Among them let us consider the newform f (up to Galois conjugacy) labeled 1888.10a whose first terms in its Fourier expansion at infinity are

$$f(\tau) = q + \tfrac{1}{2}\alpha q^3 + (-\tfrac{1}{16}\alpha^4 + \tfrac{3}{2}\alpha^2 - \alpha - 2)q^5 + O(q^6),$$

where α is a root of $X^5 + 6X^4 - 20X^3 - 128X^2 + 48X + 320$. The prime 5 is definitely smaller than the (huge) bound given in Theorem 3.2 and one proves that there is a mod 5 representation attached to f which has dihedral projective image. Namely, let us consider the prime ideal $\lambda = (5, \alpha/2)$ above 5 in $\mathcal{O}$. Then one checks that the representation $\bar{\rho}_{f,\lambda}$ is isomorphic to $\bar{\rho}_{\mathcal{E},5}$ where $\mathcal{E}$ is the rational CM elliptic curve of conductor 32 given by the equation $y^2 = x^3 - x$. Since $5 \equiv 1 \pmod 4$, one knows by the theory of complex multiplication that $\bar{\rho}_{\mathcal{E},5}$ has image included in the normalizer of a split Cartan subgroup of $\mathrm{GL}(2, \mathbf{F}_5)$. The same conclusion for $\bar{\rho}_{f,\lambda}$ thus follows.

5.3. *Projective image isomorphic to A_4, S_4 or A_5*

As an illustration of Theorem 4.1, we report here on an example due to Ribet [**26**, Remark 2, p. 283] and recalled in [**13**, Example 3.2, p. 244] (we warn the reader that the term 'exceptional' therein refers to a modular representation with projective image isomorphic to A_4, S_4 or A_5). The new subspace in $\mathcal{S}_2(\Gamma_0(23))$ is two-dimensional and generated by one Galois orbit labeled 23.4a in SAGE, with coefficients field $K = \mathbf{Q}(\alpha)$, where α is a root of $X^2 + X - 1$. Let λ be the unique prime ideal above 3 in $\mathcal{O}$. It is shown in [**13**] that the corresponding projective representation has image isomorphic to A_5 and that the field cut out by its kernel is the A_5-extension of $\mathbf{Q}$ given as the splitting field of the polynomial $X^5 + 3X^3 + 6X^2 + 9$.

Several other examples may also be found in [**13**] such as a mod 19 representation of projective image isomorphic to S_4 attached to the unique cusp form of weight 6, level 4 and trivial Nebentypus. The authors also discuss an effective procedure that, given a newform f and a prime ℓ, determines whether some mod ℓ representation attached to f has projective image isomorphic to A_4, S_4 or A_5.

TABLE 4. *Smallest prime $p \neq 11, \ell$ and $\leqslant 100$ such that $\bar{\rho}_{f,\lambda}(\mathrm{Frob}_p)$ acts irreducibly.*

ℓ	2	3	5	11		61	
λ	(α)	$(\alpha-1)$	(5)	$(2\alpha-3)$	$(2\alpha-1)$	$(\alpha-9)$	$(\alpha+7)$
p	3	2	2	2	$\emptyset$	$\emptyset$	2

Acknowledgements. The first-named author is indebted to Mladen Dimitrov, David Loeffler, Filippo Nuccio, Nick Ramsey and Panagiotis Tsaknias for helpful conversations. Gabor Wiese deserves special thanks for his constant support and advice, as well as for invaluable comments and suggestions. Part of this work was done when Nicolas Billerey was a postdoc at the Institut für Experimentelle Mathematik in Essen. He is grateful to its members for a pleasant and stimulative working environment.

References

1. H. Carayol, 'Sur les représentations l-adiques associées aux formes modulaires de Hilbert', *Ann. Sci. École Norm. Sup.* (4) 19 (1986) 409–468.
2. H. Carayol, 'Sur les représentations galoisiennes modulo l attachées aux formes modulaires', *Duke Math. J.* 59 (1989) 785–801.
3. H. Cohen, *Number theory. Vol. I. Tools and diophantine equations*, Graduate Texts in Mathematics 239 (Springer, New York, 2007).
4. A. C. Cojocaru, 'On the surjectivity of the Galois representations associated to non-CM elliptic curves', *Canad. Math. Bull.* 48 (2005) 16–31. With an appendix by Ernst Kani.
5. F. Diamond and J. Shurman, *A first course in modular forms*, Graduate Texts in Mathematics 228 (Springer, New York, 2005).
6. L. V. Dieulefait, 'Automorphy of $\mathrm{Symm}^5(\mathrm{GL}(2))$ and base change', Preprint, 2012, arXiv:1208.3946.
7. B. Edixhoven, 'The weight in Serre's conjectures on modular forms', *Invent. Math.* 109 (1992) 563–594.
8. E. Ghate and P. Parent, 'On uniform large Galois images for modular abelian varieties', *Bull. London Math. Soc.* 44 (2012) 1169–1181.
9. B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134 (Springer, Berlin, 1967).
10. H. Iwaniec, *Topics in classical automorphic forms*, Graduate Studies in Mathematics 17 (American Mathematical Society, Providence, RI, 1997).
11. N. M. Katz, 'p-adic properties of modular schemes and modular forms', *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, Lecture Notes in Mathematics 350 (Springer, Berlin, 1973) 69–190.
12. N. M. Katz, 'A result on modular forms in characteristic p', *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, Lecture Notes in Mathematics 601 (Springer, Berlin, 1977) 53–61.
13. I. Kiming and H. A. Verrill, 'On modular mod l Galois representations with exceptional images', *J. Number Theory* 110 (2005) 236–266.
14. A. Kraus, 'Une remarque sur les points de torsion des courbes elliptiques', *C. R. Acad. Sci. Paris Sér. I Math.* 321 (1995) 1143–1146.
15. R. Livné, 'On the conductors of mod l Galois representations coming from modular forms', *J. Number Theory* 31 (1989) 133–141.
16. D. Loeffler and J. Weinstein, 'On the computation of local components of a newform', *Math. Comp.* 81 (2012) 1179–1200.
17. G. Martin, 'Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$', *J. Number Theory* 112 (2005) 298–331.
18. B. Mazur, 'Modular curves and the Eisenstein ideal', *Inst. Hautes Études Sci. Publ. Math.* 47 (1977/78) 33–186.
19. B. Mazur and J.-P. Serre, 'Points rationnels des courbes modulaires $X_0(N)$ (d'après A. Ogg)', *Séminaire Bourbaki (1974/1975), Exp. No. 469*, Lecture Notes in Mathematics 514 (Springer, Berlin, 1976) 238–255.
20. T. Miyake, *Modular forms*, Springer Monographs in Mathematics (Springer, Berlin, English edition, 2006). Translated from the 1976 Japanese original by Yoshitaka Maeda.
21. M. R. Murty, 'Congruences between modular forms', *Analytic number theory (Kyoto, 1996)*, London Mathematical Society Lecture Note Series 247 (Cambridge University Press, Cambridge, 1997) 309–320.
22. J. Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences] 322 (Springer, Berlin, 1999). Translated from the 1992 German original and with a note by Norbert Schappacher, with a foreword by G. Harder.
23. K. A. Ribet, 'On l-adic representations attached to modular forms', *Invent. Math.* 28 (1975) 245–275.
24. K. A. Ribet, 'Galois representations attached to eigenforms with Nebentypus', *Modular functions of one variable, V (Proc. Second Internat. Conf., Univ. Bonn, Bonn, 1976)*, Lecture Notes in Mathematics 601 (Springer, Berlin, 1977) 17–51.
25. K. A. Ribet, 'On l-adic representations attached to modular forms. II', *Glasgow Math. J.* 27 (1985) 185–194.
26. K. A. Ribet, 'Images of semistable Galois representations', *Pacific J. Math.* (Special Issue) (1997) 277–297. Olga Taussky-Todd: in memoriam.
27. K. A. Ribet, 'Non-optimal levels of mod l reducible Galois representations or Modularity of residually reducible representations', 9 July 2010. Notes of a talk given at the Centre de Recerca Matemàtica (Barcelona).

28. B. Schoeneberg, *Elliptic modular functions: an introduction* (Springer, 1974). Translated from the German by J. R. Smart and E. A. Schwandt; Die Grundlehren der mathematischen Wissenschaften, Band 203.
29. J.-P. Serre, 'Congruences et formes modulaires [d'après H. P. F. Swinnerton-Dyer]', *Séminaire Bourbaki, 24e année (1971/1972), Exp. No. 416*, Lecture Notes in Mathematics 317 (Springer, Berlin, 1973) 319–338.
30. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan 11 (Princeton University Press, Princeton, NJ, 1994). Reprint of the 1971 original, Kanô Memorial Lectures, 1.
31. W. A. Stein *et al. Sage Mathematics Software (Version 5.2)*. The Sage Development Team, 2012. http://www.sagemath.org.
32. H. P. F. Swinnerton-Dyer, 'On l-adic representations and congruences for coefficients of modular forms', *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, Lecture Notes in Mathematics 350 (Springer, Berlin, 1973) 1–55.
33. P. Tsaknias, 'A possible generalization of Maeda's conjecture', Preprint, 2012, arXiv:1205.3420.
34. L. C. Washington, *Introduction to cyclotomic fields*, 2nd edn. Graduate Texts in Mathematics 83 (Springer, New York, 1997).

Nicolas Billerey
Laboratoire de Mathématiques
Université Blaise Pascal – Clermont-Ferrand 2
Campus Universitaire des Cézeaux
63177 Aubière cedex
France
nicolas.billerey@math.univ-bpclermont.fr

Luis V. Dieulefait
Departament d'Àlgebra i Geometria
Facultat de Matemàtiques
Universitat de Barcelona
Gran Via de les Corts Catalanes, 585
08007 Barcelona
Spain
ldieulefait@ub.edu