Dihedral Galois Representations and Katz Modular Forms

Gabor Wiese

Received: February 23, 2004
Revised: March 19, 2004

Communicated by Don Blasius

Abstract. We show that any two-dimensional odd dihedral representation ρ over a finite field of characteristic $p > 0$ of the absolute Galois group of the rational numbers can be obtained from a Katz modular form of level N, character ϵ and weight k, where N is the conductor, ϵ is the prime-to-p part of the determinant and k is the so-called minimal weight of ρ. In particular, $k = 1$ if and only if ρ is unramified at p. Direct arguments are used in the exceptional cases, where general results on weight and level lowering are not available.

2000 Mathematics Subject Classification: 11F11, 11F80, 14G35

1 Introduction

In [S1] Serre conjectured that any odd irreducible continuous Galois representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ for a prime p comes from a modular form in characteristic p of a certain level N_ρ, weight $k_\rho \geq 2$ and character ϵ_ρ. Later Edixhoven discussed in [E2] a slightly modified definition of weight, the so-called *minimal weight*, denoted $k(\rho)$, by invoking Katz' theory of modular forms. In particular, one has that $k(\rho) = 1$ if and only if ρ is unramified at p.
The present note contains a proof of this conjecture for *dihedral representations*. We define those to be the continuous irreducible Galois representations that are induced from a character of the absolute Galois group of a quadratic number field. Let us mention that this is equivalent to imposing that the projective image is isomorphic to a dihedral group D_n with $n \geq 3$.

Theorem 1 *Let p be a prime and $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ an odd dihedral representation. As in [S1] define N_ρ to be the conductor of ρ and ϵ_ρ to be the prime-to-p part of* $\det \circ \rho$ *(considered as a character of $(\mathbb{Z}/(N_\rho p)\mathbb{Z})^*$). Define $k(\rho)$ as in [E2].*
Then there exists a normalised Katz eigenform $f \in \mathcal{S}_{k(\rho)}(\Gamma_1(N_\rho), \epsilon_\rho, \overline{\mathbb{F}_p})_{\mathrm{Katz}}$, whose associated Galois representation ρ_f is isomorphic to ρ.

We will on the one hand show directly that ρ comes from a Katz modular form of level N_ρ, character ϵ_ρ and minimal weight $k(\rho) = 1$, if ρ is unramified at p. If on the other hand ρ is ramified at p, we will finish the proof by applying the fundamental work by Ribet, Edixhoven, Diamond, Buzzard and others on "weight and level lowering" (see Theorem 10).
Let us recall that in weight at least 2 every Katz modular form on Γ_1 is classical, i.e. a reduction from a characteristic zero form of the same level and weight. Hence multiplying by the Hasse invariant, if necessary, it follows from Theorem 1 that every odd dihedral representation as above also comes from a classical modular form of level N_ρ and Serre's weight k_ρ. However, if one also wants the character to be ϵ_ρ, one has to exclude in case $p = 2$ that ρ is induced from $\mathbb{Q}(i)$ and in case $p = 3$ that ρ is induced from $\mathbb{Q}(\sqrt{-3})$ (see [B], Corollary 2.7, and [D], Corollary 1.2).
Edixhoven's theorem on weight lowering ([E2], Theorem 4.5) states that modularity in level N_ρ and the modified weight $k(\rho)$ follows from modularity in level N_ρ and Serre's weight k_ρ, unless one is in a so-called *exceptional case*. A representation $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ is called *exceptional* if the semi-simplification of its restriction to a decomposition group at p is the sum of two copies of an unramified character. Because of work by Coleman and Voloch the only open case left is that of characteristic 2 (see the introduction of [E2]).
Exceptionality at 2 is a common phenomenon for mod 2 dihedral representations. One way to construct examples is to consider the Hilbert class field H of a quadratic field K that is unramified at 2 and has a non-trivial class group. One lets ρ_K be the dihedral representation obtained by induction to $G_{\mathbb{Q}}$ of a mod 2 character of the Galois group of $H|K$. If the prime 2 stays inert in $\mathcal{O}_K$, then $2\mathcal{O}_K$ splits completely in H and the order of $\rho_K(\mathrm{Frob}_2)$ is 2, where Frob_2 is a Frobenius element at 2. Consequently, ρ_K is exceptional. An example for this behaviour is provided by $K = \mathbb{Q}(\sqrt{229})$. If the prime 2 splits in $\mathcal{O}_K$ and the primes of $\mathcal{O}_K$ lying above 2 are principal, then $\rho_K(\mathrm{Frob}_2)$ is the identity and hence ρ_K is exceptional. This happens for example for $K = \mathbb{Q}(\sqrt{2089})$.
Let us point out that some of the weight one forms that we obtain cannot be lifted to characteristic zero forms of weight one and the same level, so that the theory of modular forms by Katz becomes necessary. Namely, if $p = 2$ and the dihedral representation in question has odd conductor N and is induced from a real quadratic field K of discriminant N, whose fundamental units have norm -1, then there does not exist an odd characteristic zero representation with conductor dividing N that reduces to ρ. The representation coming from the quadratic field $\mathbb{Q}(\sqrt{229})$ used above, can also here serve as an example.

The fact that dihedral representations come from *some* modular form is well-known (apparently already due to Hecke). So the subtle issue is to adjust the level, character and weight. It should be noted that Rohrlich and Tunnell solved many cases for $p = 2$ with Serre's weight k_ρ by rather elementary means in [R-T], however, with the more restrictive definition of a dihedral representation to be such that its image in $\mathrm{GL}_2(\overline{\mathbb{F}_2})$, and not in $\mathrm{PGL}_2(\overline{\mathbb{F}_2})$, is isomorphic to a dihedral group.
Let us also mention that it is possible to do computations of weight one forms in positive characteristic on a computer (see [W]) and thus to collect evidence for Serre's conjecture in some cases.
This note is organised as follows. The number theoretic ingredients on dihedral representations are provided in Section 2. In Section 3 some results on oldforms, also in positive characteristic, are collected. Section 4 is devoted to the proof of Theorem 1. Finally, in Section 5 we include a result on the irreducibility of certain mod p representations.

I wish to thank Peter Stevenhagen for helpful discussions and comments and especially Bas Edixhoven for invaluable explanations and his constant support.

2 Dihedral representations

We shall first recall some facts on Galois representations. Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}(V)$ be a continuous representation with V a 2-dimensional vector space over an algebraically closed discrete field k.
Let L be the number field such that $\mathrm{Ker}(\rho) = G_L$ (by the notation G_L we always mean the absolute Galois group of L). Given a prime Λ of L dividing the rational prime l, we denote by $G_{\Lambda,i}$ the i-th ramification group in lower numbering of the local extension $L_\Lambda|\mathbb{Q}_l$. Furthermore, one sets

$$n_l(\rho) = \sum_{i \geq 0} \frac{\dim(V/V^{G_{\Lambda,i}})}{(G_{\Lambda,0} : G_{\Lambda,i})}.$$

This number is an integer, which is independent of the choice of the prime Λ above l. With this one defines the *conductor* of ρ to be $\mathfrak{f}(\rho) = \prod_l l^{n_l(\rho)}$, where the product runs over all primes l different from the characteristic of k. If k is the field of complex numbers, $\mathfrak{f}(\rho)$ coincides with the *Artin conductor*.
Let ρ be a dihedral representation. Then ρ is induced from a character $\chi : G_K \to k^*$ for a quadratic number field K such that $\chi \neq \chi^\sigma$, with $\chi^\sigma(g) = \chi(\sigma^{-1} g \sigma)$ for all $g \in G_K$, where σ is a lift to $G_{\mathbb{Q}}$ of the non-trivial element of $G_{K|\mathbb{Q}}$. For a suitable choice of basis we then have the following explicit description of ρ: If an unramified prime l splits in K as $\Lambda\sigma(\Lambda)$, then $\rho(\mathrm{Frob}_l) = \begin{pmatrix} \chi(\mathrm{Frob}_\Lambda) & 0 \\ 0 & \chi^\sigma(\mathrm{Frob}_\Lambda) \end{pmatrix}$. Moreover, $\rho(\sigma)$ is represented by the matrix $\begin{pmatrix} 0 & 1 \\ \chi(\sigma^2) & 0 \end{pmatrix}$. As ρ is continuous, its image is a finite group, say, of order m.

Lemma 2 *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ be an odd dihedral representation that is unramified at p. Define K, χ, σ and m as above. Let N be the conductor of ρ. Let ζ_m a primitive m-th root of unity and $\mathfrak{P}$ a prime of $\mathbb{Q}(\zeta_m)$ above p.*
Then one of the following two statements holds.

(a) There exists an odd dihedral representation $\widehat{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}[\zeta_m])$, which has Artin conductor N and reduces to ρ modulo $\mathfrak{P}$.

(b) One has that $p = 2$ and K is real quadratic. Moreover, there is an infinite set S of primes such that for each $l \in S$ the trace of $\rho(\mathrm{Frob}_l)$ is zero, and there exists an odd dihedral representation $\widehat{\rho} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}[\zeta_m])$, which has Artin conductor Nl and reduces to ρ modulo $\mathfrak{P}$.

Proof. Suppose that the quadratic field K equals $\mathbb{Q}(\sqrt{D})$ with D square-free. The character $\chi : G_K \to k^*$ can be uniquely lifted to a character $\widetilde{\chi} : G_K \to \mathbb{Z}[\zeta_m]^*$ of the same order, which reduces to χ modulo $\mathfrak{P}$. Denote by $\widetilde{\rho}$ the continuous representation $\mathrm{Ind}_{G_K}^{G_{\mathbb{Q}}} \widetilde{\chi}$. For the choice of basis discussed above the matrices representing ρ can be lifted to matrices representing $\widetilde{\rho}$, whose non-zero entries are in the m-th roots of unity. Then for any open subgroup H of $G_{\mathbb{Q}}$, one has that $(\overline{\mathbb{F}_p}^2)^{\rho(H)}$ is isomorphic to $(\mathbb{Z}[\zeta_m]^2)^{\widetilde{\rho}(H)} \otimes \overline{\mathbb{F}_p}$. Hence the conductor of ρ equals the Artin conductor of $\widetilde{\rho}$, as $\widetilde{\rho}$ is unramified at p. Alternatively, one can first remark that the conductor of χ equals the conductor of $\widetilde{\chi}$ and then use the formulae $\mathfrak{f}(\rho) = \mathrm{Norm}_{K|\mathbb{Q}}(\mathfrak{f}(\chi))D$ and $\mathfrak{f}(\widetilde{\rho}) = \mathrm{Norm}_{K|\mathbb{Q}}(\mathfrak{f}(\widetilde{\chi}))D$.
Thus condition (a) is satisfied if $\widetilde{\rho}$ is odd. Let us now consider the case when $\widetilde{\rho}$ is even. This immediately implies $p = 2$ and that the quadratic field K is real, as is the number field L whose absolute Galois group G_L equals the kernel of ρ, and hence also the kernel of $\widetilde{\chi}$. We shall now adapt "Serre's trick" from [R-T], p. 307, to our situation.
Let $\mathfrak{f}$ be the conductor of $\widetilde{\chi}$. As L is totally real, $\mathfrak{f}$ is a finite ideal of $\mathcal{O}_K$. Via class field theory, $\widetilde{\chi}$ can be identified with a complex character of $\mathrm{CL}_K^{\mathfrak{f}}$, the ray class group modulo $\mathfrak{f}$. Let ∞_1, ∞_2 be the infinite places of K. Consider the class

$$c = [\{(\lambda) \in \mathrm{CL}_K^{4D\mathfrak{f}\infty_1\infty_2} \mid \mathrm{Norm}(\lambda) < 0, \lambda \equiv 1 \bmod 4D\mathfrak{f}\}]$$

in the ray class group of K modulo $4D\mathfrak{f}\infty_1\infty_2$. By Cebotarev's density theorem the primes of $\mathcal{O}_K$ are uniformly distributed over the conjugacy classes of $\mathrm{CL}_K^{4D\mathfrak{f}\infty_1\infty_2}$. Hence, there are infinitely many primes Λ of degree 1 in the class c. Take S to be the set of rational primes lying under them. Let a prime Λ from the class c be given. It is principal, say $\Lambda = (\lambda)$, and coprime to $4D\mathfrak{f}$. By construction we have $c^2 = [\Lambda^2] = 1$. As $\mathrm{CL}_K^{\mathfrak{f}}$ is a quotient of $\mathrm{CL}_K^{4D\mathfrak{f}\infty_1\infty_2}$, the class of Λ in $\mathrm{CL}_K^{\mathfrak{f}}$ has order 1 or 2. Since $p = 2$, the character χ has odd order and we conclude that $\chi(\Lambda) = 1$.
We have $\lambda \equiv 1 \bmod 4D\mathfrak{f}$ and $\mathrm{Norm}(\lambda) = -l$ for some odd prime l. Hence, the extension $K(\sqrt{\lambda})$ has two real and two complex embeddings and is unramified at 2 and at the primes dividing $D\mathfrak{f}$. We represent $K(\sqrt{\lambda})$ by the quadratic character $\xi : G_K \to \{\pm 1\}$. For the complex conjugation, the "infinite Frobenius

element", Frob_{∞_1}, we have that $\xi(\mathrm{Frob}_{\infty_1})\xi^\sigma(\mathrm{Frob}_{\infty_1}) = -1$. We now consider the representation $\widehat{\rho}$ obtained by induction from the character $\widehat{\chi} = \widetilde{\chi}\xi$. Using the same basis as in the discussion at the beginning of this section, an element g of G_K is represented by the matrix $\begin{pmatrix} \widetilde{\chi}(g)\xi(g) & 0 \\ 0 & \widetilde{\chi}^\sigma(g)\xi^\sigma(g) \end{pmatrix}$. In particular, we obtain that the determinant of Frob_∞ over $\mathbb{Q}$ equals -1, whence $\widehat{\rho}$ is odd. Moreover, as l splits in K, one has that $\rho(\mathrm{Frob}_l)$ is the identity matrix, so that the trace of $\rho(\mathrm{Frob}_l)$ is zero.
The reduction of $\widehat{\rho}$ equals ρ, as ξ is trivial in characteristic 2. Moreover, outside Λ the conductor of $\widehat{\chi}$ equals the conductor of $\widetilde{\chi}$. At the prime Λ the local conductor of $\widehat{\chi}$ is Λ, as the ramification is tame. Consequently, the Artin conductor of $\widehat{\rho}$ equals Nl. □

Also without the condition that it is unramified at p, one can lift a dihedral representation to characteristic zero, however, losing control of the Artin conductor.

Lemma 3 *Let $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ be an odd dihedral representation. Define K, χ, m, ζ_m and $\mathfrak{P}$ as in the previous lemma.*
There exists an odd dihedral representation $\widehat{\rho} : G_\mathbb{Q} \to \mathrm{GL}_2(\mathbb{Z}[\zeta_m])$, whose reduction modulo $\mathfrak{P}$ is isomorphic to ρ.

Proof. We proceed as in the preceding lemma for the definitions of $\widetilde{\chi}$ and $\widetilde{\rho}$. If $\widetilde{\rho}$ is even, then $p = 2$ and K is real. In that case we choose some $\lambda \in \mathcal{O}_K - \mathbb{Z}$, which satisfies $\mathrm{Norm}(\lambda) < 0$. The field $K(\sqrt{\lambda})$ then has two real and two complex embeddings and gives a character $\xi : G_K \to \mathbb{Z}[\zeta_m]^*$. As in the proof of the preceding lemma one obtains that the representation $\widehat{\rho} = \mathrm{Ind}_{G_K}^{G_\mathbb{Q}} \widetilde{\chi}\xi$ is odd and reduces to ρ modulo $\mathfrak{P}$. □

3 On oldforms

In this section we collect some results on oldforms. We try to stay as much as possible in the characteristic zero setting. However, we also need a result on Katz modular forms.

Proposition 4 *Let N, k, r be positive integers, p a prime and ϵ a Dirichlet character of modulus N. The homomorphism*

$$\phi_{p^r}^N : \big(\mathcal{S}_k(\Gamma_1(N), \epsilon, \mathbb{C})\big)^{r+1} \hookrightarrow \mathcal{S}_k(\Gamma_1(Np^r), \epsilon, \mathbb{C}), \;\; (f_0, f_1, \ldots, f_r) \mapsto \sum_{i=0}^{r} f_i(q^{p^i})$$

is compatible with all Hecke operators T_n with $(n, p) = 1$.
Let $f \in \mathcal{S}_k(\Gamma_1(N), \epsilon, \mathbb{C})$ be a normalised eigenform for all Hecke operators. Then the forms $f(q), f(q^{p^2}), \ldots, f(q^{p^r})$ in the image of $\phi_{p^r}^N$ are linearly independent, and on their span the action of the operator T_p in level Np^r is given

by the matrix

$$\begin{pmatrix} a_p(f) & 1 & 0 & 0 & \dots & 0 \\ -\delta p^{k-1}\epsilon(p) & 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ & & \vdots & & & \\ 0 & \dots & 0 & 0 & 0 & 1 \\ 0 & \dots & 0 & 0 & 0 & 0 \end{pmatrix},$$

where $\delta = 1$ if $p \nmid N$ and $\delta = 0$ otherwise.

Proof. The embedding map and its compatibility with the Hecke action away from p is explained in [D-I], Section 6.1. The linear independence can be checked on q-expansions. Finally, the matrix can be elementarily computed. $\square$

Corollary 5 *Let p be a prime, $r \geq 0$ some integer and $f \in \mathcal{S}_k(\Gamma_1(Np^r), \epsilon, \mathbb{C})$ an eigenform for all Hecke operators. Then there exists an eigenform for all Hecke operators $\tilde{f} \in \mathcal{S}_k(\Gamma_1(Np^{r+2}), \epsilon, \mathbb{C})$, which satisfies $a_l(\tilde{f}) = a_l(f)$ for all primes $l \neq p$ and $a_p(\tilde{f}) = 0$.*

Proof. One computes the characteristic polynomial of the operator T_p of Proposition 4 and sees that it has 0 as a root if the dimension of the matrix is at least 3. Hence one can choose the desired eigenform $\tilde{f}$ in the image of $\phi_{p^2}^{Np^r}$. $\square$

As explained in the introduction, Katz' theory of modular forms ought to be used in the study of Serre's conjecture. Following [E3], we briefly recall this concept, which was introduced by Katz in [K]. However, we shall use a "non-compactified" version.

Let $N \geq 1$ be an integer and R a ring, in which N is invertible. One defines the category $[\Gamma_1(N)]_R$, whose objects are pairs $(E/S/R, \alpha)$, where S is an R-scheme, E/S an elliptic curve (i.e. a proper smooth morphism of R-schemes, whose geometric fibres are connected smooth curves of genus one, together with a section, the "zero section", $0 : S \to E$) and $\alpha : (\mathbb{Z}/N\mathbb{Z})_S \to E[N]$, the *level structure*, is an embedding of S-group schemes. The morphisms in the category are cartesian diagrams

$$\begin{tikzcd} E' \arrow[r] \arrow[d] \arrow[dr, phantom, "\square"] & E \arrow[d] \\ S' \arrow[r] & S, \end{tikzcd}$$

which are compatible with the zero sections and the level structures. For every such elliptic curve $E/S/R$ we let $\underline{\omega}_{E/S} = 0^*\underline{\Omega}_{E/S}$. For every morphism $\pi : E'/S'/R \to E/S/R$ the induced map $\underline{\omega}_{E'/S'} \to \pi^*\underline{\omega}_{E/S}$ is an isomorphism.

A *Katz cusp form* $f \in \mathcal{S}_k(\Gamma_1(N), R)_{\mathrm{Katz}}$ assigns to every object $(E/S/R, \alpha)$ of $[\Gamma_1(N)]_R$ an element $f(E/S/R, \alpha) \in \underline{\omega}_{E/S}^{\otimes k}(S)$, compatibly for the morphisms in

the category, subject to the condition that all q-expansions (which one obtains by adjoining all N-th roots of unity and plugging in a suitable Tate curve) only have positive terms.
For the following definition let us remark that if $m \geq 1$ is coprime to N and is invertible in R, then any morphism of group schemes of the form $\phi_{Nm} : (\mathbb{Z}/Nm\mathbb{Z})_S \to E[Nm]$ can be uniquely written as $\phi_N \times_S \phi_m$ with $\phi_N : (\mathbb{Z}/N\mathbb{Z})_S \to E[N]$ and $\phi_m : (\mathbb{Z}/m\mathbb{Z})_S \to E[m]$.

Definition 6 *A Katz modular form* $f \in \mathcal{S}_k(\Gamma_1(Nm), R)_{\mathrm{Katz}}$ *is called* independent of m *if for all elliptic curves $E/S/R$, all $\phi_N : (\mathbb{Z}/N)_S \hookrightarrow E[N]$ and all $\phi_m, \phi'_m : (\mathbb{Z}/m)_S \hookrightarrow E[m]$ one has the equality*

$$f(E/S/R, \phi_N \times_S \phi_m) = f(E/S/R, \phi_N \times_S \phi'_m) \in \underline{\omega}_{E/S}^{\otimes k}(S).$$

Proposition 7 *Let N, m be coprime positive integers and R a ring, which contains the Nm-th roots of unity and $\frac{1}{Nm}$. A Katz modular form $f \in \mathcal{S}_k(\Gamma_1(Nm), R)_{\mathrm{Katz}}$ is independent of m if and only if there exists a Katz modular form $g \in \mathcal{S}_k(\Gamma_1(N), R)_{\mathrm{Katz}}$ such that*

$$f(E/S/R, \phi_{Nm}) = g(E/S/R, \phi_{Nm} \circ \psi)$$

for all elliptic curves $E/S/R$ and all $\phi_{Nm} : (\mathbb{Z}/Nm\mathbb{Z})_S \hookrightarrow E[Nm]$. Here ψ denotes the canonical embedding $(\mathbb{Z}/N\mathbb{Z})_S \hookrightarrow (\mathbb{Z}/Nm\mathbb{Z})_S$ of S-group schemes. In that case, f and g have the same q-expansion at ∞.

Proof. If $m = 1$, there is nothing to do. If necessary replacing m by m^2, we can hence assume that m is at least 3.
Let us now consider the category $[\Gamma_1(N; m)]_R$, whose objects are triples $(E/S/R, \phi_N, \psi_m)$, where S is an R scheme, E/S an elliptic curve, $\phi_N : (\mathbb{Z}/N\mathbb{Z})_S \hookrightarrow E[N]$ an embedding of group schemes and $\psi_m(\mathbb{Z}/m\mathbb{Z})_S^2 \cong E[m]$ an isomorphism of group schemes. The morphisms are cartesian diagrams compatible with the zero sections, the ϕ_N and the ψ_m as before.
We can pull back the form $f \in \mathcal{S}_k(\Gamma_1(Nm), R)_{\mathrm{Katz}}$ to a Katz form h on $[\Gamma_1(N; m)]_R$ as follows. First let $\beta : (\mathbb{Z}/m\mathbb{Z})_S \hookrightarrow (\mathbb{Z}/m\mathbb{Z})_S^2$ be the embedding of S-group schemes defined by mapping onto the first factor. Using this, f gives rise to h by setting

$$h((E/S/R, \phi_N, \psi_m)) = f((E/S/R, \phi_N, \psi_m \circ \beta)) \in \underline{\omega}_{E/S}^{\otimes k}(S).$$

As f is independent of m, it is clear that h is independent of ψ_m and thus invariant under the natural $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$-action.
As $m \geq 3$, one knows that the category $[\Gamma_1(N; m)]_R$ has a final object $(E^{\mathrm{univ}}/Y_1(N; m)_R/R, \alpha^{\mathrm{univ}})$. In other words, h is an $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$-invariant global section of $\underline{\omega}_{E^{\mathrm{univ}}/Y_1(N;m)_R}^{\otimes k}$. Since this R-module is equal to $\mathcal{S}_k(\Gamma_1(N), R)_{\mathrm{Katz}}$ (see e.g. Equation 1.2 of [E3], p. 210), we find some $g \in \mathcal{S}_k(\Gamma_1(N), R)_{\mathrm{Katz}}$ such that $f(E/S/R, \phi_{Nm}) = g(E/S/R, \phi_{Nm} \circ \psi)$ for all $(E/S/R, \phi_{Nm})$.

Plugging in the Tate curve, one sees that the standard q-expansions of f and g coincide. $\square$

Corollary 8 *Let N, m be coprime positive integers, p a prime not dividing Nm and $\epsilon : (\mathbb{Z}/N\mathbb{Z})^* \to \overline{\mathbb{F}_p}$ a character. Let $f \in \mathcal{S}_k(\Gamma_1(Nm), \epsilon, \overline{\mathbb{F}_p})_{\mathrm{Katz}}$ be a Katz cuspidal eigenform for all Hecke operators.*
If f is independent of m, then there exists an eigenform for all Hecke operators $g \in \mathcal{S}_k(\Gamma_1(N), \epsilon, \overline{\mathbb{F}_p})_{\mathrm{Katz}}$ such that the associated Galois representations ρ_f and ρ_g are isomorphic.

Proof. From the preceding proposition we get a modular form $g \in \mathcal{S}_k(\Gamma_1(N), \epsilon, \overline{\mathbb{F}_p})_{\mathrm{Katz}}$, noting that the character is automatically good. Because of the compatibility of the embedding map with the operators T_l for primes $l \nmid m$, we find that g is an eigenform for these operators. As the operators T_l for primes $l \nmid m$ commute with the others, we can choose a form of the desired type. $\square$

4 Proof of the principal result

We first cover the weight one case.

Theorem 9 *Let p be a prime and $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ an odd dihedral representation of conductor N, which is unramified at p. Let ϵ denote the character* $\det \circ \rho$.
Then there exists a Katz eigenform f in $\mathcal{S}_1(\Gamma_1(N), \epsilon, \overline{\mathbb{F}_p})_{\mathrm{Katz}}$, whose associated Galois representation is isomorphic to ρ.

Proof. Assume first that part (a) of Lemma 2 applies to ρ, and let $\widehat{\rho}$ be a lift provided by that lemma. A theorem by Weil-Langlands (Theorem 1 of [S2]) implies the existence of a newform g in $\mathcal{S}_1(\Gamma_1(N), \det \circ \widehat{\rho}, \mathbb{C})$, whose associated Galois representation is isomorphic to $\widehat{\rho}$. Now reduction modulo a suitable prime above p yields the desired modular form. In particular, one does not need Katz' theory in this case.
If part (a) of Lemma 2 does not apply, then part (b) does, and we let S be the infinite set of primes provided. For each $l \in S$ the theorem of Weil-Langlands yields a newform $f^{(l)}$ in $\mathcal{S}_1(\Gamma_1(Nl), \mathbb{C})$, whose associated Galois representation reduces to ρ modulo $\mathfrak{P}$, where $\mathfrak{P}$ is the ideal from the lemma. Moreover, the congruence $a_q(f^{(l)}) \equiv 0 \bmod \mathfrak{P}$ holds for all primes $q \in S$ different from l.
From Corollary 5 we obtain Hecke eigenforms $\widetilde{f}^{(l)} \in \mathcal{S}_1(\Gamma_1(Nl^3), \mathbb{C})$ such that $a_l(\widetilde{f}^{(l)}) = 0$ and $a_q(\widetilde{f}^{(l)}) = a_q(f^{(l)}) \equiv 0 \bmod \mathfrak{P}$ for all primes $q \in S$, $q \neq l$. Reducing modulo the prime ideal $\mathfrak{P}$, we get eigenforms $g^{(l)} \in \mathcal{S}_1(\Gamma_1(Nl^3), \epsilon, \overline{\mathbb{F}_p})$, whose associated Galois representations are isomorphic to ρ. One also has $a_q(g^{(l)}) = 0$ for all $q \in S$.
The coefficients $a_q(f^{(l)})$ for all primes $q \mid N$ appear in the L-series of the complex representation $\rho_{f^{(l)}}$ associated to $f^{(l)}$. As the image of $\rho_{f^{(l)}}$ is isomorphic

to a fixed finite group G, not depending on l, there are only finitely many possibilities for the value of $a_q(f^{(l)})$. Hence the same holds for the $g^{(l)}$. Consequently, there are two forms $g_1 = g^{(l_1)}$ and $g_2 = g^{(l_2)}$ for $l_1 \neq l_2$ that have the same coefficients at all primes $q \mid N$. For primes $q \nmid Nl_1l_2$ one has that the trace of $\rho_{f^{(l_1)}}(\mathrm{Frob}_q)$ is congruent to the trace of $\rho_{f^{(l_2)}}(\mathrm{Frob}_q)$, whence $a_q(g_1) = a_q(g_2)$. Let us point out that this includes the case $q = p = 2$, as the complex representation is unramified at p.
In the next step we embed g_1 and g_2 into $\mathcal{S}_1(\Gamma_1(Nl_1^3l_2^3), \epsilon, \overline{\mathbb{F}_p})_{\mathrm{Katz}}$ via the method in the statement of Proposition 7. As the q-expansions coincide, g_1 and g_2 are mapped to the same form h. But as h comes from g_2, it is independent of l_1 and analogously also of l_2. Since $\rho_h = \rho$, Theorem 9 follows immediately from Corollary 8. $\square$

We will deduce the cases of weight at least two from general results. The current state of the art in "level and weight lowering" seems to be the following theorem.

Theorem 10 *[Ribet, Edixhoven, Diamond, Buzzard,...] Let p be a prime and $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ a continuous irreducible representation, which is assumed to come from some modular form. Define k_ρ and N_ρ as in [S1]. If $p = 2$, additionally assume either (i) that the restriction of ρ to a decomposition group at 2 is not contained within the scalar matrices or (ii) that ρ is ramified at 2. Then there exists a normalised eigenform $f \in \mathcal{S}_{k_\rho}(\Gamma_1(N_\rho), \overline{\mathbb{F}_p})$ giving rise to ρ.*

Proof. The case $p \neq 2$ is Theorem 1.1 of [D], and the case $p = 2$ with condition (i) follows from Propositions 1.3 and 2.4 and Theorem 3.2 of [B], multiplying by the Hasse invariant if necessary.
We now show that if $p = 2$ and ρ restricted to a decomposition group $G_{\mathbb{Q}_2}$ at 2 is contained within the scalar matrices, then ρ is unramified at 2. Let $\phi : G_{\mathbb{Q}} \to \overline{\mathbb{F}_2}^*$ be the character such that $\phi^2 = \det \circ \rho$. As ϕ has odd order, it is unramified at 2 because of the Kronecker-Weber theorem. If ρ restricted to $G_{\mathbb{Q}_2}$ is contained within the scalar matrices, then we have that $\rho|_{G_{\mathbb{Q}_2}}$ is $\begin{pmatrix} \phi|_{G_{\mathbb{Q}_2}} & 0 \\ 0 & \phi|_{G_{\mathbb{Q}_2}} \end{pmatrix}$, whence ρ is unramified at 2. $\square$

Proof of theorem 1. Let ρ be the dihedral representation from the assertion. If ρ is unramified at p, one has $k(\rho) = 1$, and Theorem 1 follows from Theorem 9.
If ρ is ramified at p, then let $\widehat{\rho}$ be a characteristic zero representation lifting ρ, as provided by Lemma 3. The theorem by Weil-Langlands already used above (Theorem 1 of [S2]) implies the existence of a newform in weight one and characteristic zero giving rise to $\widehat{\rho}$. So from Theorem 10 we obtain that ρ comes from a modular form of Serre's weight k_ρ and level N_ρ. Let us note that using Katz modular forms the character is automatically the conjectured one ϵ_ρ.
The weights k_ρ and $k(\rho)$ only differ in two cases (see [E2], remark 4.4). The first case is when $k(\rho) = 1$. The other case is when $p = 2$ and ρ is not finite

at 2. Then one has $k(\rho) = 3$ and $k_\rho = 4$. In that case one applies Theorem 3.4 of [E2] to obtain an eigenform of the same level and character in weight 3, or one applies Theorem 3.2 of [B] directly. $\square$

5 An irreducibility result

We first study the relation between the level of an eigenform in characteristic p and the conductor of the associated Galois representation.

Lemma 11 *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}_p})$ be a continuous representation of conductor N, and let k be a positive integer. If $f \in \mathcal{S}_k(\Gamma_1(M), \epsilon, \overline{\mathbb{F}_p})_{\mathrm{Katz}}$ is a Hecke eigenform giving rise to ρ, then N divides M.*

Proof. By multiplying with the Hasse invariant, if necessary, we can assume that the weight is at least 2. Hence the form f can be lifted to characteristic zero (see e.g. [D-I], Theorem 12.3.2) in the same level. Thus there exists a newform g, say of level L, whose Galois representation ρ_g reduces to ρ. Now Proposition 0.1 of [L] yields that N divides L. As L divides M, the lemma follows. $\square$

We can derive the following proposition, which is of independent interest.

Proposition 12 *Let $f \in \mathcal{S}_k(\Gamma_0(N), \overline{\mathbb{F}_p})_{\mathrm{Katz}}$ be a normalised Hecke eigenform for a square-free level N with $p \nmid N$ in some weight $k \geq 1$.*

(a) If $p = 2$, the associated Galois representation is either irreducible or trivial.

(b) For any prime p the associated Galois representation is either irreducible or corresponds to a direct sum $\alpha \oplus \chi_p^{k-1}\alpha^{-1}$, where χ_p is the mod p cyclotomic character and α is a character factoring through $G(\mathbb{Q}(\zeta_p)|\mathbb{Q})$ for a primitive p-th root of unity ζ_p.

Proof. Let us assume that the representation ρ associated to f is reducible. Since ρ is semi-simple, it is isomorphic to the direct sum of two characters $\alpha \oplus \beta$. As the determinant is the $(k-1)$-th power of the mod p cyclotomic character χ_p, we have that $\beta = \chi_p^{k-1}\alpha^{-1}$. Since the conductor of χ_p^{k-1} is 1, it follows that the conductor of α equals that of β. Consequently, the conductor of ρ is the square of the conductor of α. Lemma 11 implies that the conductor of ρ divides N. As we have assumed this number to be square-free, we have that ρ can only ramify at p.
The number field L with $G_L = \mathrm{Ker}(\rho)$ is abelian. As only p can be ramified, it follows that L is contained in $\mathbb{Q}(\zeta_{p^n})$ for some p^n-th root of unity. Since the order of α is prime to p, we conclude that α factors through $G(\mathbb{Q}(\zeta_p)|\mathbb{Q})$. In characteristic $p = 2$ this implies that ρ is the trivial representation, as χ_2 is the trivial character. $\square$

References

[B] K. Buzzard. *On level lowering for mod 2 representations.* Mathematical Research Letters 7 (2000). 95-110.

[D] F. Diamond *The refined conjecture of Serre.* Elliptic curves, modular forms, & Fermat's last theorem (Hong Kong, 1993), Internat. Press, Cambridge, MA, 1995. 22-37.

[D-I] F. Diamond and J. Im. *Modular forms and modular curves.* Seminar on Fermat's Last Theorem (Toronto, ON, 1993-1994), CMS Conf. Proc., 17, Amer. Math. Soc., Providence, RI, 1995. 39-133.

[E1] S. J. Edixhoven. *Comparison of integral structures on spaces of modular forms of weight two, and computation of spaces of forms mod* 2 *of weight one.* Accepted for publication in the Journal de l'Institut de Mathmatiques de Jussieu. `http://arxiv.org/abs/math.NT/0312019`

[E2] S. J. Edixhoven. *The weight in Serre's conjectures on modular forms.* Invent. Math. 109 (1992). 563-594.

[E3] S. J. Edixhoven. *Serre's conjecture.* Modular Forms and Fermat's Last Theorem (Gary Cornell, Joseph Silverman and Glenn Stevens, editors). Springer-Verlag, 1997. 209-242.

[K] 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, Vol. 350, Springer, Berlin, 1973. 69-190.

[L] R. Livn. *On the conductors of mod l Galois representations coming from modular forms.* J. of Number Theory 31 (1989). 133-141.

[R-T] D. E. Rohrlich, J. B. Tunnell. *An elementary case of Serre's conjecture.* Pacific Journal of Mathematics 181, No. 3 (1997). 299-309.

[S1] J.-P. Serre. *Sur les reprsentations de degr* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. Duke Mathematical Journal 54, No. 1 (1987). 179-230.

[S2] J.-P. Serre. *Modular forms of weight one and Galois representations.* Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977. 193-268.

[W] G. Wiese. *Computing Hecke algebras of weight* 1 *in MAGMA.* Appendix B of [E1].

Gabor Wiese
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden
The Netherlands
gabor@math.leidenuniv.nl