ARNAUD JEHANNE
MICHAEL MÜLLER

Modularity of an odd icosahedral representation


<http://www.numdam.org/item?id=JTNB_2000__12_2_475_0>
Modularity of an odd icosahedral representation

par Arnaud Jehanne et Michael Müller

t à Jacques Martinet

1. Introduction

Consider an irreducible Galois representation

$$\rho : G_Q \rightarrow GL_2(\mathbb{C})$$

and the corresponding induced projective representation

$$\overline{\rho} : G_Q \rightarrow PGL_2(\mathbb{C}),$$

where we denote by $\overline{Q}$ an algebraic closure of $\mathbb{Q}$ and by $G_Q = \text{Gal}(\overline{Q}/\mathbb{Q})$ the absolute Galois group over $\mathbb{Q}$.

Artin has conjectured (for any nontrivial irreducible representation $\rho : G_Q \rightarrow GL_n(\mathbb{C})$), that the analytic continuation of the $L$-series associated to the representation $\rho$ is an entire function. It is known by results of Hecke, Langlands and Tunnel ([Lan], [Tun]) that $\rho$ satisfies Artin’s conjecture, if $\text{Im}(\overline{\rho})$ is solvable. If $\text{Im}(\overline{\rho})$ is isomorphic to $A_5$, this conjecture is not yet proved in general, but it has been proved for particular cases by Buhler ([Buh]) in 1978, and by Kiming and Wang ([K-W]) in 1994. In 1999, Buzzard, Dickinson, Shepherd-Baron and Taylor proved the conjecture for infinitely many icosahedral representations ([B-D-SB-T]). Moreover, in 2000,
Buzzard and Stein gave eight other examples of modular representations in [B-S] and Taylor gave another result that proves the conjecture for infinitely many icosahedral representations ([Tay2]).

In all these examples and theorems one has to assume, that the representation \( \rho \) is odd, that is, \( \det(\rho)(c) = -1 \), where \( c \) denotes the complex conjugation. And for odd representations, Artin's conjecture is equivalent to the fact that the \( L \)-series of this representation coincides with the \( L \)-series \( L(f, s) \) of a weight one modular form \( f \) (see [D-S]).

We give one more example for the Artin conjecture with \( \det(\rho) = \chi_{-43} \) and conductor 5203. With this method one can verify Artin's conjecture for each odd representation with quadratic determinant and conductor lower than 10000. We prove in fact the modularity of this representation by using the computation of its \( L \)-function ([Jeh]) and a basis of the \( \mathbb{C} \)-vector space \( S_2(5203, 1) \) of cusp forms of weight 2, conductor 5203 and nebentype 1.

Note that this representation does not satisfy the hypothesis of the main theorem of [B-D-SB-T]. Indeed, if \( \lambda \) and \( \mu \) are the eigenvalues of the Frobenius element \( \mathrm{Frob}_{p, 2} \) in \( 2 \), then \( \lambda/\mu \) has order 5. We check too that the representation does not satisfy the hypothesis of the theorems of [Tay2].

Acknowledgement. It is a pleasure for the authors to thank Gerhard Frey for fruitful discussions and Kevin Buzzard for useful comments and questions.

2. Modularity of \( \rho \)

We consider the \( L \)-function

\[
L(\rho, s) = \sum_{n=1}^{\infty} a_n n^{-s}
\]

of our irreducible two-dimensional representation \( \rho \). We want to prove that the series deduced formally from \( L(\rho, s) \)

\[
f(z) = \sum_{n=1}^{\infty} a_n q^n
\]

(where \( q = e^{2\pi i z} \)) is a newform of weight one and level equal to the conductor \( \mathfrak{f}(\rho) \) of \( \rho \). We make use of the following proposition (see [Fre1], proposition 1.1).

**Proposition 2.1.** Assume that \( g(z) = \sum b_n q^n \) belongs to the space \( M_k(N, \chi) \) of modular forms of level \( N \) and nebentype \( \chi \), where \( N \) is an integer and \( \chi : (\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^* \) a Dirichlet character. Let \( \mu = N \prod_{p|N} (1 + \frac{1}{p}) \) (where \( p \) runs through the set of prime numbers dividing \( N \)). If \( b_n = 0 \) for \( 0 \leq n \leq \mu k/12 \), then \( g = 0 \).
Let $N = \mathfrak{f}(\rho)$ be the conductor and let $\chi$ be the determinant of $\rho$. Via class field theory, we can consider $\chi$, as a Dirichlet character $(\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*$.

**Proposition 2.2.** Let $\theta$ be an element of $M_1(N, \chi)$ and $\mu = N \prod_{p \mid N} (1 + \frac{1}{p})$.

If there are two elements $g_1$ and $g_2$ in $S_2(N, \chi^2)$ such that

$$\theta f \equiv g_1 \mod q^{\frac{\mu}{3} + 1}$$

and

$$f^2 \equiv g_2 \mod q^{\frac{\mu}{3} + 1},$$

then $g_1/\theta$ belongs to $S_1(N, \chi)$.

**Proof.** Since $g_1$ belongs to $S_2(N, \chi)$ and $\theta$ to $M_1(N, \chi)$, it is enough to prove that the meromorphic function $g_1/\theta$ is holomorphic. Moreover we have $g_1^2 \equiv \theta^2 g_2 \mod q^{\mu/3}$. Furthermore $g_1^2$ and $\theta^2 g_2$ are both elements of $S_4(N, \chi^4)$, so we can apply proposition 2.1. This shows that $g_1^2 = \theta^2 g_2$ and therefore that $(g_1/\theta)^2$ is holomorphic. \(\square\)

Now we consider a projective representation $\rho$ given by the polynomial $P(X) = X^5 + 5X^2 - 6X + 27$. It is the example 16 of [B-K]. We consider the lifting $\rho$ of $\rho$ with conductor 5203 and determinant $\chi_{-43}$ (the character associated to $\mathbb{Q}(\sqrt{-43})$) of [Jeh], example 6.

**Theorem 2.3.** The representation $\rho$ is modular.

**Proof.** Let $Q$ be the quadratic form $Q(x, y) = x^2 + xy + 11y^2$; it is known that the associated theta series

$$\Theta_Q = \sum_{(x, y) \in \mathbb{Z}^2} q^{Q(x, y)} = 1 + 2 \sum_{n=1}^{\infty} \left( \sum_{d \mid n} \chi_{-43}(d) \right) q^n$$

belongs to $M_1(43, \chi_{-43})$. We recall that $f$ is the series deduced formally from $L(\rho, s)$. For $N = 5203$, the element $\mu/3$ of proposition 2.2 is equal to 1936. We shall prove in section 3 that there are two elements $g_1$ and $g_2$ such that

$$\Theta_Q f \equiv g_1 \mod q^{2000}$$

and

$$f^2 \equiv g_2 \mod q^{2000}.$$ 

By proposition 2.2, we conclude that $f$ is congruent to an element $g = g_1/\Theta_Q$ in $S_1(5203, \chi_{-43})$ modulo $q^{2000}$. As the series $L(\rho, s)$ has an Euler product, in which the term corresponding to the prime number 2 is

$$(1 - \frac{1}{2} - \sqrt{5} \cdot 2^{-s} - 4^{-s})^{-1},$$
it follows that \( g \mod q^{1000} \) is an eigenvector for the Hecke operator \( T_2 \) and the associated eigenvalue is equal to \( i \frac{1 - \sqrt{5}}{2} \). We obtain that

\[
T_2 g \equiv i \frac{1 - \sqrt{5}}{2} g \mod q^{1000},
\]

and then by proposition 2.1:

\[
T_2 g = i \frac{1 - \sqrt{5}}{2} g.
\]

It proves that there exists an eigenform \( h \) in \( S_1(5203, \chi_{-43}) \) with eigenvalue for \( T_2 \) equal to \( i \frac{1 - \sqrt{5}}{2} \). By [D-S], theorem 4, we obtain a Galois representation

\[
\rho_h : G_Q \rightarrow GL_2(\mathbb{C})
\]

associated to \( h \). The conductor of this representation divides \( 5203 = 11 \cdot 43 \) and its determinant is equal to \( \chi_{-43} \). After [D-S] the eigenvalue of \( T_2 \) is the trace of a Frobenius endomorphism at 2. The trace \( i \frac{1 - \sqrt{5}}{2} \) can be obtained neither by a tetrahedral representation (\( \text{Im}(\overline{\rho}_h) \approx A_4 \)) nor by an octahedral one (\( \text{Im}(\overline{\rho}_h) \approx S_4 \)). Assume that \( \rho_h \) is a dihedral representation. We know that there is a quadratic field \( \mathbb{Q}(\sqrt{d}) \) and a character \( \varphi \) of the absolute Galois group of \( \mathbb{Q}(\sqrt{d}) \) such that \( \rho_h \) is the induction of \( \varphi \). The conductor \( \mathfrak{f}(\rho_h) \) is given by the formula

(1) \[
\mathfrak{f}(\rho_h) = |\Delta_d| N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(f_{\varphi}),
\]

where \( \Delta_d \) is the discriminant of \( \mathbb{Q}(\sqrt{d})/\mathbb{Q} \) and \( f_{\varphi} \) the conductor of \( \varphi \). Here, \( d \in \{-11, -43, 473\} \).

In \( \mathbb{Q}(\sqrt{-43}) \) and in \( \mathbb{Q}(\sqrt{-11}) \), the prime number 2 is inert and then if \( d = -43 \) or \( -11 \), the trace of the image of a Frobenius at 2 is zero. Hence, we cannot have \( \text{Tr}(\text{Frob}_{\rho_h,2}) = i \frac{1 - \sqrt{5}}{2} \) (where \( \text{Frob}_{\rho_h,2} \) is the Frobenius element of \( \rho_h \) in 2). Because of the formula (1), the only ramified primes for \( \varphi \) are those above 11. We denote by \( \mathfrak{p} \) the only ideal above 11 in the ring of integers of \( \mathbb{Q}(\sqrt{473}) \). By [PARI], we compute that the ray class group of \( \mathfrak{p} \) in \( \mathbb{Q}(\sqrt{473}) \) has order 15. Hence, the eigenvalues of the image of a Frobenius endomorphism at 2 are 15th roots of unity. Therefore the trace of a Frobenius at 2 belongs to the cyclotomic field \( \mathbb{Q}(\mu_{15}) \), which does not contain \( i \frac{1 - \sqrt{5}}{2} \). We conclude that if \( d = 473 \), we cannot have \( \text{Tr}(\text{Frob}_{\rho_h,2}) = i \frac{1 - \sqrt{5}}{2} \). We have now proved that the representation \( \rho_h \) is icosahedral.

Let \( K_h \) be a quintic subfield of \( \mathbb{Q}^{\ker(\rho_h)} \). The only possibilities for the valuations of the discriminant \( d_{K_h} \) of \( K_h \) for prime numbers not dividing 60 are 2 and 4 (see [Ser2], chapter IV, § 1, 2, 3). Since the determinant of \( \rho_h \) is \( \chi_{-43} \), the only possibility for the valuation of \( d_{K_h} \) in 43 is 2. For the valuation of \( d_{K_h} \) in 11, we can have the valuations 4 (if the order of
\(\tilde{\rho}_h(I_{11})\) is equal to 5, where \(I_{11}\) is the inertia in 11, 2 or 0. We check then in table 1 of [B-K] that the only possibilities are \(d_{K_h} = 11^2.43^2\), and then \(\rho_h\) is isomorphic to \(\rho\) or \(d_{K_h} = 11^4.43^2\), that is too large for this table.

Now, we assume that \(d_{K_h} = 11^4.43^2\). In this case, the order of \(\tilde{\rho}_h(I_{11})\) is equal to 5. Since \(\rho_h\) is modular, all the liftings \(\rho_h \otimes \chi\) (where \(\chi\) runs though the Dirichlet characters) are modular. Moreover, there exists such a lifting \(\rho'\) with quadratic nontrivial determinant and such that the order of \(\rho'(I_5)\) is 5 (see [Ser1], theorem 5 p. 228). Since \(\rho'\) is modular, we can assume that \(\rho_h = \rho'\) (but then, the trace of the Frobenius in 2 of \(\rho_h\) is no more \(i\frac{1-\sqrt{5}}{2}\), but \(\frac{1-\sqrt{5}}{2}\), multiplied by an element of \(\{1,-1,i,-i\}\)). We can view \(\rho_h\) as a representation with image in \(GL_2(\mathbb{Z})\), where \(\overline{\mathbb{Z}}\) is the integral closure of \(\mathbb{Z}\) in \(\overline{\mathbb{Q}}\). We choose a place \(v\) in \(\overline{\mathbb{Z}}\) above 11 and we reduce \(\rho_h\) modulo \(v\). We obtain a representation

\[\tilde{\rho}_h : G_{\overline{Q}} \rightarrow GL_2(\overline{\mathbb{F}}_{11}).\]

Consider the Eisenstein series \(E_{10}\) normalized such that its constant term is equal to 1. Then the coefficients of the \(q\)-expansion of \(E_{10}\) are 11-integers and \(E_{10} \equiv 1\) mod 11. Moreover, the reduction \(S = \sum b_nq^n\) of \(hE_{10}\) modulo \(v\) is a cusp form with coefficients in \(\overline{\mathbb{F}}_{11}\) of weight 11, level 5203 and determinant \(\overline{\chi}_{-43}\) (the reduction of \(\chi_{-43}\) modulo \(v\)), that is an eigenform for the Hecke operators and such that

\[\text{Tr}(F_{\tilde{\rho}_h,p}) = b_p \quad \text{and} \quad \det(F_{\tilde{\rho}_h,p}) = \overline{\chi}_{-43}(p)p^{10}\]

for all prime number \(p \not\in \{11,43\}\) (see [D-S] p. 520 and 521). Then, \(\tilde{\rho}_h\) satisfies Serre’s conjecture (3.2.3) of [Ser3], that is, \(\tilde{\rho}_h\) arises from a cusp form with coefficients in \(\overline{\mathbb{F}}_{11}\). The level of this cusp form is equal to \(11^2.43\). In this case, we know that we can “take off” the 11-part of this level. This representation arises from a cusp form with level 43 (see theorem (2.1) p. 643 of [Rib]). Finally, by theorem 4.5 p. 572 of [Edi], we obtain that \(\tilde{\rho}_h\) arises from a cusp form with the weight predicted by Serre. We conclude that \(\tilde{\rho}_h\) satisfies Serre’s conjecture (3.2.4), that is, with the level and weight predicted by Serre. Then this representation arises from a cusp form with coefficients in \(\overline{\mathbb{F}}_{11}\) of level 43, character \(\overline{\chi}_{-43}\) and weight \(k\) as in [Ser3], § 2. To compute this weight, we consider the restriction of \(\tilde{\rho}_h\) to the inertia group \(I_{11}\). We denote by \(\phi\) the cyclotomic character. Since \(\tilde{\rho}_h|_{I_{11}}\) has order 5 and has a trivial determinant, then \(\tilde{\rho}_h|_{I_{11}}\) is conjugated to

\[\begin{pmatrix} \phi^4 & 0 \\ 0 & \phi^6 \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \phi^2 & 0 \\ 0 & \phi^8 \end{pmatrix},\]

and we obtain \(k = 51\) or 31, using the recipe of [Ser3]. By theorem 3.4 of [Edi], that we recall below (theorem 2.4), we see that we only have to deal with the spaces of cusp forms with coefficients in \(\overline{\mathbb{F}}_{11}\) of level 43, character \(\overline{\chi}_{-43}\) and weight 3 (resp. 7). We compute a basis for each of
these spaces and check that no eigenform of these spaces corresponds to $\tilde{\rho}_k$.

Indeed, we know that the values of the trace of Frobenius span $\mathbb{Q}(i, \sqrt{5})$. And the values of the reductions modulo 11 span $\mathbb{F}_{121}$. Now if we look at $S_3(43, \chi_{-43})$, we see that the coefficients of an eigenform of this space span the root field of the polynomial $X^6 + 20X^4 + 121X^2 + 214$, that is congruent modulo 11 to $(X + 3)(X + 8)(X^4 + 7X + 8)$. Then we don’t have an eigenform in $S_3(43, \chi_{-43})$ modulo 11 such that its eigenvalues span $\mathbb{F}_{121}$.

For $S_7(43, \chi_{-43})$, the Hecke operator $T_2$ has the polynomial characteristic

$$X(X^{20} + 1038X^{18} + 455829X^{16} + 110435384X^{14} + 16133606976X^{12}$$
$$+ 1458210485616X^{10} + 80362197690736X^8 + 2545997652841536X^6$$
$$+ 40210452531479040X^4 + 212033222410436608X^2$$
$$+ 64236717122519040).$$

The reduction of this polynomial modulo 11 has two factors of degree 2: $X^2 + X - 3$ and $X^2 - X - 3$. The roots of $X^2 + X - 3$ are $6(-1 + \sqrt{2})$ and $6(-1 - \sqrt{2})$. If the derivation application acts twice on the corresponding eigenforms (see theorem 2.4 below), we obtain the eigenvalues $2(-1 + \sqrt{2})$ and $2(-1 - \sqrt{2})$. These values cannot correspond with an eigenvalue $\frac{-1 + \sqrt{5}}{2}$, multiply by an element of $\{1, -1, i, -i\}$. We solve the case of the polynomial $X^2 - X - 3$ by the same way. $\square$

In order to write theorem 2.4, we have to introduce the derivation $\theta$. If $f = \sum a_n q^n$ is a formal series, we define the series $\theta f$ by setting $\theta f = \sum n a_n q^n$. If $f$ is a modular form with coefficients in $\overline{\mathbb{F}}_p$, then $\theta f$ is such a modular form too. Moreover, the application $\theta$ does neither change the level nor the character, but it increases the weight by $p + 1$ (see [Edi]).

**Theorem 2.4** (Edixhoven). Let $f$ be an eigenform in a space $\tilde{S}_k(N, \chi)$ of modular forms with coefficients in $\overline{\mathbb{F}}_p$. Then there exists integers $n$ and $k'$ with $0 \leq n \leq p - 1$, $k' \leq p + 1$, and an eigenform $g$ in $\tilde{S}_{k'}(N, \chi)$ such that $f$ and $\theta^n g$ have the same eigenvalues for all $\tilde{T}_L$ ($L \neq p$).

3. **Existence of $g_1$ and $g_2$**

In this section we describe very briefly (since we use only standard techniques in computational number theory) how one can show, that there are two cusp forms $g_1, g_2 \in S_2(5203, 1)$ which satisfies

$$\Theta Q f \equiv g_1 \mod q^{2000}$$

$$f^2 \equiv g_2 \mod q^{2000}$$

with

$$\Theta Q f = t_1 + i.t_2 + \sqrt{5}.t_3 + i\sqrt{5}.t_4$$
$$f^2 = f_1 + i.f_2 + \sqrt{5}.f_3 + i\sqrt{5}.f_4$$
with $t_i = \sum_{n=1}^{\infty} t_{i,n}q^n$, $f_i = \sum_{n=1}^{\infty} f_{i,n}q^n$ and $t_{i,n}, f_{i,n} \in \mathbb{Q}$ for $i \in \{1, 2, 3, 4\}$ and $n \in \mathbb{N}$ as in section 2.

The method is as follows: We compute a basis $\{h_1, \ldots, h_g\}$ of $S_2(5203, 1)$ with

$$h_m = \sum_{n=1}^{\infty} h_{m,n}q^n, \ h_{m,n} \in \mathbb{Z}, m = 1, \ldots, g$$

(It is enough for us to compute the first 2000 coefficients of the $q$-expansion of the $h_m$). Here $g = \dim S_2(5203, 1) = 473$ is the dimension of the space of cusp forms of level 5203. Such a basis exists due to results of [Shi], see also [D-D-T]. To compute the basis we use the modular symbol method (introduced by Birch) and the explicit knowledge of the action of the Hecke algebra on the modular symbols. For a description of this method see for example [Cre] or [Mer].

The rest is linear algebra. After computing such a basis we have to check, that there exists two cuspforms $g_1, g_2$ which satisfies 2. Let

$$A = \begin{pmatrix} h_{m,n} \\ 2f_{1,n} \\ \vdots \\ 2f_{4,n} \\ 2t_{1,n} \\ \vdots \\ 2t_{4,n} \end{pmatrix} \in \text{Mat}^{481 \times 2000}(\mathbb{Z})$$

be the matrix of the coefficients of the basis $\{h_1, \ldots, h_g\}$ and the coefficients of the $t_i$ and the $f_i$. Then one has to show that

$$\text{rank}(A) = \dim S_2(5203, 1) = 473.$$ 

(We multiply $f_i, t_i$ by 2 to get a $q$-expansion with integral coefficients for $n \leq 2000$.) To compute the rank we reduce the matrix $A$ modulo different prime numbers $p$ and check that $\text{rank}(A \mod p) = 473$. Hadamard’s inequality gives us a bound for the number of primes $p$ that guarantee that $\text{rank}(A) = 473$ over $\mathbb{Q}$ (we need 380 prime numbers $p$ with $p > 2 \cdot 10^9$; it is clear that these bounds are not good, but the computation takes only 20 hours on a PII 450MHz Linux-PC, so we did not try to improve them).

References
