Mathematics

http://www.aimspress.com/journal/Math

AIMS Mathematics, 8(12): 28766–28779.
DOI: 10.3934/math.20231473
Received: 25 June 2023
Revised: 22 September 2023
Accepted: 10 October 2023
Published: 23 October 2023

Research article

Computing mod ℓ Galois representations associated to modular forms for small primes

Peng Tian[1,*], **Ha Thanh Nguyen Tran**[2] **and Dung Hoang Duong**[3]

[1] School of Mathematics, East China University of Science and Technology, Shanghai, 200237, China

[2] Department of Mathematical and Physical Sciences, Concordia University of Edmonton, Edmonton, T5B 4E4, Canada

[3] School of Computing and Information Technology, University of Wollongong, Wollongong, NSW 2522, Australia

* **Correspondence:** Email: tianpeng@ecust.edu.cn.

Abstract: In this paper, we propose an algorithm for computing mod ℓ Galois representations associated to modular forms of weight k when $\ell < k - 1$. We also present the corresponding results for the projective Galois representations. Moreover, we apply our algorithms to explicitly compute the mod ℓ projective Galois representations associated to Δ_k for $k = 16, 20, 22, 26$ and all the unexceptional primes ℓ, with $\ell < k - 1$. As an application, for $k = 16, 20, 22, 26$, we obtain the new bounds B_k of n such that $a_n(\Delta_k) \neq 0$ for all $n < B_k$.

Keywords: modular forms; mod ℓ Galois representations; unexceptional primes; polynomials associated to modular Galois representations; Fourier coefficients of modular forms
Mathematics Subject Classification: 11F80, 11F33, 11G30, 11G18

1. Introduction

Let ℓ be a prime number and $f \in S_k(\Gamma_1(N))$ be a cusp form of weight k and level N. Let $\rho_f : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{F}}_\ell)$ be a mod ℓ Galois representation associated to f. Let L be the fixed field of the kernel of ρ_f. Then the representation ρ_f factors through as:

$$\begin{tikzcd}
Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[rr, "\rho_f"] \arrow[dr, "\pi"'] & & GL_2(\overline{\mathbb{F}}_\ell) \\
& Gal(L/\mathbb{Q}) \arrow[ur, "\phi"'] &
\end{tikzcd}$$

where π is the canonical restriction map and ϕ is the isomorphism between $\mathrm{Gal}(L/\mathbb{Q})$ and the image $\mathrm{im}(\rho_f)$ of ρ_f. Thus to compute ρ_f, it suffices to give the Galois extension field L over $\mathbb{Q}$ and the isomorphism ϕ.

In their book [1], Edixhoven et al. propose a polynomial time algorithm to compute ρ_f associated to level one modular forms. They prove that ρ_f can be described by a certain polynomial $P_f \in \mathbb{Q}[x]$ of degree $\ell^2 - 1$ whose splitting field is the fixed field L of $\ker(\rho_f)$. One can obtain L by adjoining the roots of P_f to $\mathbb{Q}$, and the isomorphism ϕ is induced by a bijection between the roots of P_f and a 2-dimensional subspace of the ℓ-torsion of the Jacobian variety $J_1(\ell)$ of the modular curve $X_1(\ell)$ associated to $\Gamma_1(\ell)$. This algorithm has been generalized to modular forms of arbitrary levels by Bruin [2]. Likewise, the associated projective representation $\tilde{\rho}_f : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to PGL_2(\overline{\mathbb{F}}_\ell)$ can be described by a suitable polynomial $\tilde{P}_f \in \mathbb{Q}[x]$ of degree $\ell + 1$.

The computations depend heavily on ℓ and the genus of the modular curve $X_1(\ell)$, which is equal to $(\ell - 5)(\ell - 7)/24$. In practice, the most time-consuming part of the algorithm is to approximate the points of $J_1(\ell)$, and the precision significantly increases when ℓ grows. Consequently, the explicit computations have been done only for the primes no bigger than 43.

Let Δ_k be the unique cusp form of level 1 and weight k with $k = 12, 16, 18, 20, 22, 26$. In practice, this algorithm has been first implemented by Bosman [1, Chapter 7] to evaluate the projective polynomial $\tilde{P}_{\Delta_k}$ for $\ell \leq 23$ and $k \leq \ell + 1$. In [3, 4] and the unpublished paper [5], this algorithm has been improved and more polynomials $\tilde{P}_{\Delta_k}$ have been explicitly computed for $\ell \leq 43$.

However, as far as we know, no one has implemented the algorithm to calculate the polynomials for the cases with $\ell < k - 1$. In this paper, we shall discuss the algorithms for computing mod ℓ Galois representations associated to modular forms of weight k when $\ell < k - 1$. We will propose an algorithm of this case and then do explicit computations of the mod ℓ projective Galois representations $\tilde{\rho}_{\Delta_k}$ for $k = 16, 20, 22, 26$ and all the unexceptional primes ℓ for which $\ell < k - 1$.

In the book [1], the authors deal with the case with $\ell < k - 1$ by twisting the representations and then reduce the computations to the cases with $k \leq \ell + 1$. In fact, for a form of level one and weight k with $\ell < k - 1$, in [1, Proposition 2.5.18] they show a method to obtain a form of weight $k' \leq \ell + 1$, such that the two Galois representations associated to the two forms are isomorphic. In this paper, we will prove this result also holds for modular forms of levels greater than 1.

First, in Section 2, we show a generalization of Sturm bound theorem [6, Theorem 2] to mod ℓ modular forms, which gives an explicit method to identify two forms by observing a few coefficients of the q-expansions. Then in Section 3, we use the generalized result to give an explicit method, for a given modular form of type (N, k, ε), to obtain a twist form of type (N, k', ε) with $k' \leq \ell + 1$, such that the two Galois representations associated to the two forms are isomorphic up to twist. In fact this is a generalization of [1, Proposition 2.5.18] to modular forms of arbitrary levels. Consequently, the computations of the cases with $\ell < k - 1$ boil down to the cases with $k \leq \ell + 1$.

In the end of Section 3, we prove the corresponding results for the projective representations and then present the algorithm for the projective case.

In Section 4, we apply the algorithm in Subsection 3.3 to do explicit computations of the mod ℓ projective Galois representations $\tilde{\rho}_{\Delta_k}$ for $k = 16, 20, 22, 26$ and all the unexceptional primes ℓ for which $\ell < k - 1$. Here Δ_k is the normalized cusp form of level one and weight k. The computed projective polynomials $\tilde{P}_{\Delta_k}(x)$ associated to the representations $\tilde{\rho}_{\Delta_k}$ are shown in Table 4.

Lehmer [7] conjectures that Ramanujan's tau function $\tau(n)$ is non-vanishing for all n and shows that

$\tau(n) \neq 0$ for all $n < 3316799$. Serre [8] sums up the congruences of $\tau(p)$ modulo exceptional primes of $\tau(p)$ and obtains a bound of 15 digits for Lehmer's conjecture with respect to $\tau(n)$. Bosman [1] first used the results of modular Galois representations to discuss the non-vanishing coefficients of $\tau(n)$ and then this method was developed by others. So far the bound for Lehmer's conjecture with respect to $\tau(n)$ is up to 24 digits [5].

In [9], the authors discuss non-vanishing Fourier coefficients $a_n(\Delta_k)$ of Δ_k and achieve the bounds B_k of n such that $a_n(\Delta_k) \neq 0$ for all $n < B_k$ in the cases with $k = 16, 18, 20, 22, 26$.

In this paper, as an application, we shall discuss the non-vanishing Fourier coefficients of Δ_k using our results. In fact, for $k = 16, 20, 22, 26$, we obtain higher bounds B_k of n such that $a_n(\Delta_k) \neq 0$ for all $n < B_k$. We demonstrate how much the bounds B_k have been improved for $k = 16, 20, 22, 26$ in Table 1. Note that the last column of Table 1 is the approximate quotients of the new and old bounds.

Table 1. Comparison between the new and old bounds.

k	new bound	old bound	$\frac{\text{new bound}}{\text{old bound}} \approx$
16	169424346446440054199	12604744061516618549	13
20	1222095705994609939349	74201833676082662549	16
22	567829713758553825538049	28265095927027650599999	20
26	3442219356673306598399	818406791865712833299	4

The method in this paper is different with that in the previous papers. In [4], we compute modular Galois representations only when $\ell \geq k - 1$, in which case we say the prime ℓ is "large enough". However, in this paper, we discuss the cases when $\ell < k - 1$, that is, the prime ℓ is small. In this case, we don't have the weight 2 forms by which we can carry out all the computations. Instead, in this paper, we use the twists of the forms by the θ operator. In [9], to obtain the new bounds B_k, we discuss the exceptional primes and observe the congruence formulas, and there is none of new modular Galois representation being computed. In this paper, we do computations in the cases with unexceptional primes by using the new modular Galois representations, which are computed in Subsection 4.2.

Throughout this paper, we suppose $\ell \geq 5$ to be a prime and denote $\overline{\mathbb{F}}_\ell$ the algebraic closure of the finite field $\mathbb{F}_\ell$. All the explicit computations of this paper have been done in the open source software SAGE [10].

2. Mod ℓ modular forms

2.1. Modular forms of type (N, k, ε)

The mod ℓ modular forms were first developed by Serre [11] and Swinnerton-Dyer [12], and generalized by Katz [13]. In this subsection we give a brief review of the theory of mod ℓ modular forms. For the details, we refer to [14] and [15, Section 2].

Let ℓ be a prime and $N \geq 1$ be prime to ℓ. The congruence subgroup $\Gamma_1(N)$ of level N is

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \mid c \equiv 0 \, mod \, N, \quad a \equiv d \equiv 1 \, mod \, N \right\}. \tag{2.1}$$

Let $X_1(\ell)$ be the modular curve associated to $\Gamma_1(\ell)$. Let $k > 0$ be an even integer. Let E be a generalized elliptic curve over a scheme S and $\alpha : (\mathbb{Z}/N\mathbb{Z})_S \hookrightarrow E$ be an embdedding of group schemes. Denote the relative differentials by $\Omega^1_{E/S}$ and zero section by 0. Let $\omega_{E/S} := 0^*\Omega^1_{E/S}$. Then a modular form f of type (N, k) over $\overline{\mathbb{F}}_\ell$ is a law, that assigns to each pair $(E/S, \alpha)$ a section of $\omega^{\otimes k}_{E/S}$.

The q-expansions of mod ℓ modular forms f at cusp ∞ of $\Gamma_1(N)$ have been given by evaluating f on (E_q, α), where $q = e^{2\pi iz}$ and E_q is the Tate curve over $\overline{\mathbb{F}}_\ell[[q]](q^{-1})$. More precisely, the q-expansions of f at ∞ are the the power series $f(E_q, \alpha)/(dt/t)^{\otimes k} \in \overline{\mathbb{F}}_\ell[[q]]$, where dt/t is the standard differential on E_q. This in fact coincides with the usual q-expansions of modular forms, since (E_q, α) corresponds to a neighbourhood of the cusp ∞ in the completed up half plane $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \infty$, where $\mathcal{H}$ is the up half plane. As usual, we denote the n-th coefficient of the q-expansion by $a_n(f)$.

Let $\varepsilon : (\mathbb{Z}/(N\ell)\mathbb{Z})^* \to \overline{\mathbb{F}}_\ell$ be a Dirichlet character. Define an action of $\mathbb{Z}/(N\ell)\mathbb{Z})^*$ on mod ℓ form f by

$$(\langle a\rangle^*)(E/S, \alpha) = f(E/S, a\alpha), \quad a \in \mathbb{Z}/(N\ell)\mathbb{Z})^*. \tag{2.2}$$

A modular form f of type (N, k) is called a form of type (N, k, ε) if it satisfies

$$(\langle a\rangle^*)(E/S, \alpha) = \varepsilon(a)f. \tag{2.3}$$

One can also define Hecke operators T_p that are coincide with the usual Hecke operators. For instance, we have that all the T_p commute with each other and the eigenvalues determine the q-expansions of f up to a constant factor.

A modular form f is called cusp form if $a_0(f) = 0$. A modular form f of type (N, k, ε) is said to be an eigenform if it is an eigenvector for all the Hecke operators T_p with $p \nmid N\ell$. An eigenform f is said to be normalized if $a_1(f) = 1$.

2.2. *Operator θ and Hasse invariant A*

Let $\theta = q\frac{d}{dq}$ be the classical differential operator $\sum_{n>0} a_n(f)q^n \mapsto \sum_{n>0} na_n(f)q^n$. If f is an eigenform of type (N, k, ε), in [16, Section 2.1], it is shown that θf is an eigenform of type $(N, k + \ell + 1, \varepsilon)$.

Let A be the Hasse invariant of the Tate curve E_q over $\overline{\mathbb{F}}_\ell[[q]](q^{-1})$, then we have:

Lemma 2.1. *The Hasse invariant A is given by $A = (dt/t)^{\otimes \ell-1}$. Hence, A is a mod ℓ modular form of type* $(1, \ell - 1, 1)$.

Proof. This is Proposition 1.9 *c*) of [14]. □

From this lemma, we know the q-expansion of A is 1. For two forms of types (N, k_1, ε) and (N, k_2, ε) with $k_1 \equiv k_2 \mod \ell - 1$, we can view the two forms as forms of the same type by multiplying one form by suitable powers of A. This can be used to prove the following proposition, which is a generalization of Sturm bound theorem to modular forms of different weights:

Proposition 2.2. *Let f_1 and f_2 be two normalized eigenforms of type (N, k_1, ε) and (N, k_2, ε), respectively. Let $k = max\{k_1, k_2\}$. Suppose that $k_1 \equiv k_2 \mod \ell - 1$ and $a_m(f_1) = a_m(f_2)$ in $\overline{\mathbb{F}}_\ell$ for all m with $m \leq \frac{k[SL_2(\mathbb{Z}):\Gamma_1(N)]}{12}$. Then $f_1 = f_2$.*

Proof. Let A be the Hasse invariant. Without loss of generality, we suppose $k_1 \leq k_2$. Then by Lemma 2.1, the form $A^{(k_2-k_1)/(\ell-1)}f_1$ is an eigenform of type (N, k_2, ε). We know $A = 1$, and this implies that the form f_1 is also a form of type (N, k_2, ε). Since we have $a_m(f_1) = a_m(f_2)$ in $\overline{\mathbb{F}}_\ell$ for all m with $m \leq \frac{k[SL_2(\mathbb{Z}):\Gamma_1(N)]}{12}$, it follows from Sturm's theorem that $f_1 = f_2$. □

A proof of this result for classical modular forms can be found in [17].

The following well-known theorem takes an important role for our computations:

Theorem 2.3. *Let f be a normalized eigenform of type (N, k, ε), then there exist i and k' with $0 \leq i \leq \ell - 1$, $k' \leq \ell + 1$, and a normalized eigenform of type (N, k', ε), such that $f = \theta^i g$.*

Proof. See [15, Theorem 3.4]. □

3. Computing mod ℓ Galois representations for small ℓ

In this section, we shall describe the algorithm for computing mod ℓ Galois representations associated to modular forms of weight k when $\ell < k - 1$. We also prove the corresponding results for the projective representations and then present the algorithm for the projective case.

3.1. Modular Galois representations and θ twists

Deligne [18] proves the following well known theorem:

Theorem 3.1 (Deligne). *Let f be an eigenform of type (N, k, ε). Then there exists a continuous semi-simple representation*

$$\rho_f : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to GL_2(\overline{\mathbb{F}}_\ell), \tag{3.1}$$

which is unramified outside $N\ell$, and for all primes $p \nmid N\ell$ the characteristic polynomial of $\rho_f(Frob_p)$ satisfies in $\overline{\mathbb{F}}_\ell$

$$charpol(\rho_f(Frob_p)) = x^2 - a_p(f)x + \varepsilon(p)p^{k-1}. \tag{3.2}$$

Moreover, ρ_f is unique up to isomorphism.

Let $f = \sum_{n>0} a_n(f)q^n$ be an eigenform. Then by definition, the eigenform θf has q-expansion $\sum_{n>0} na_n(f)q^n$. It follows from the above theorem that

$$\rho_{\theta f} = \rho_f \otimes \chi_\ell,$$

where χ is the mod ℓ cyclotomic character. Then for an eigenform f of type (N, k, ε) with $\ell < k - 1$, it follows from Theorem 2.3 that there exist an integer i and an eigenform g of type (N, k', ε) with $k' \leq \ell + 1$, such that ρ_f is a twist of ρ_g by χ_ℓ^i, i. e.,

$$\rho_f \cong \rho_g \otimes \chi_\ell^i. \tag{3.3}$$

Moreover, we have the following theorem to determine such i and k':

Theorem 3.2. *Let f_1 and f_2 be two normalized eigenforms of type (N, k_1, ε) and (N, k_2, ε), respectively. Let i be an integer with $0 \leq i \leq \ell - 1$. Then $f_1 = \theta^i f_2$ if and only if $k_1 \equiv k_2 + 2i$* mod $\ell - 1$ *and $a_p(f_1) = p^i a_p(f_2)$ in $\overline{\mathbb{F}}_\ell$ for all primes p with $p \leq \frac{\ell(\ell+1)[SL_2(\mathbb{Z}):\Gamma_1(N)]}{12}$.*

Proof. We first assume that $f_1 = \theta^i f_2$. By the argument above, it follows that ρ_{f_1} and $\rho_{f_2} \otimes \chi_\ell^i$ are isomorphic. Then by (3.2), we have

$$\varepsilon\chi_\ell^{k_1-1} = \varepsilon\chi_\ell^{k_2-1+2i}.$$

Hence we have $k_1 \equiv k_2 + 2i \mod \ell - 1$. Since $a_p(\theta^i f_2) = p^i a_p(f_2)$ for all primes p, in $\overline{\mathbb{F}}_\ell$ we have

$$a_p(f_1) = p^i a_p(f_2)$$

for all primes p with $p \leq \frac{\ell(\ell+1)[SL_2(\mathbb{Z}):\Gamma_1(N)]}{12}$.

For the other direction, we assume that

$$k_1 \equiv k_2 + 2i \mod \ell - 1,$$

and $a_p(f_1) = p^i a_p(f_2)$ for all primes p with $p \leq \frac{\ell(\ell+1)[SL_2(\mathbb{Z}):\Gamma_1(N)]}{12}$.

It follows from Theorem 2.3 that there exist an integer j with $0 \leq j \leq \ell - 1$ and a normalized eigenform g_1 of type $(N, k_{g_1}, \varepsilon)$ with $k_{g_1} \leq \ell + 1$ such that $f_1 = \theta^j g_1$ in $\overline{\mathbb{F}}_\ell$. This implies that $f_1 = \theta^j g_1$ is a form of type (N, k_1, ε) with $k_1 \leq \ell(\ell + 1)$.

We set $f_2' = \theta^i f_2$. Then for the same reason as above, the form f_2' is of type (N, k_2', ε) with $k_2' \leq \ell(\ell + 1)$. Moreover, we have that $\rho_{f_2'}$ is isomorphic to $\rho_{f_2} \otimes \chi_\ell^i$. By the argument in the first paragraph of the proof, we have

$$k_2' \equiv k_2 + 2i \mod \ell - 1. \tag{3.4}$$

Then by the assumption and (3.4), we have

$$k_1 \equiv k_2 + 2i \equiv k_2' \mod \ell - 1,$$

and

$$a_p(f_1) = p^i a_p(f_2) = a_p(f_2')$$

for all primes p with $p \leq \frac{\ell(\ell+1)[SL_2(\mathbb{Z}):\Gamma_1(N)]}{12}$.

Since f_1 and f_2' are normalized eigenforms, this implies that $a_m(f_1) = a_m(f_2')$ for all $m \in \mathbb{Z}$ with $m \leq \frac{\ell(\ell+1)[SL_2(\mathbb{Z}):\Gamma_1(N)]}{12}$. By Proposition 2.2, we then have that $f_1 = f_2'$ and therefore $f_1 = \theta^i f_2$. This completes the proof. □

This theorem also provides a method to calculate the values of i and k' for which (3.3) is satisfied. From this point of view, this theorem is a generalization of [1, Proposition 2.5.18] from level one to arbitrary levels. In [2, Theorem 3.5], the author gives an elaborate result of the generalization of [1, Proposition 2.5.18], which is used to theoretically prove that the algorithm described in [2] is in polynomial time. However, it is quite convenient to apply Theorem 3.2 when we do explicit computations.

3.2. *The algorithm*

In this subsection, we shall describe the algorithm for computing the mod ℓ Galois representations associated to modular forms. This algorithm was first proposed by Edixhoven and Couveignes [1] for modular forms of level one and then generalized to forms of arbitrary levels by Bruin [2]. The algorithm that we shall present is slightly different. In fact, we shall apply Theorem 3.2 instead when we reduce the computations to the cases with $2 \leq k \leq \ell + 1$.

Now let f be a cuspidal normalized eigenform of type (N, k, ε) with $\ell < k - 1$. Theorem 2.3 and 3.2 allow us to explicitly obtain a normalized eigenform f' of type (N, k', ε) with $2 \leq k' \leq \ell + 1$ such that ρ_f and $\rho_{f'} \otimes \chi_\ell^i$ are isomorphic. Thus it suffices to compute $\rho_{f'}$ and the question boils down to the case with $2 \leq k' \leq \ell + 1$.

In [19, Theorem 2.2], the author shows that if $2 < k \leq \ell + 1$ and $\rho_{f,\lambda}$ is ireducible, then there is a cuspidal normalized eigenform f_2 of type $(N\ell, 2, \varepsilon_2)$ such that ρ_f is isomorphic to ρ_{f_2}. Therefore, for any $p \nmid N\ell$, this reduces the questions to the case with $k = 2$.

Now suppose that ρ_f is a mod ℓ Galois representation associated to a cuspidal normalized eigenform of type $(N, 2, \varepsilon)$. Let $X_1(\ell)$ be the modular curve associated to $\Gamma_1(\ell)$ and let $J_1(\ell)$ denote its Jacobian. Denote $\mathbb{T}$ the subring of $\mathrm{End}(J_1(\ell))$ generated by the Hecke operators T_p over $\mathbb{Z}$. Then

$$\mathbb{T} = \mathbb{Z}[T_n, \langle n \rangle : n \in \mathbb{Z}_+ \text{ and } (n, \ell) = 1].$$

Define a ring homomorphism

$$\theta : \mathbb{T} \to \mathbb{F}_\lambda,$$

given by

$$\langle d \rangle \mapsto \varepsilon(d) \quad \textit{and} \quad T_n \mapsto a_n(f).$$

Let $\mathfrak{m}$ denote the maximal ideal $\ker\theta$ and then $\mathbb{T}/\mathfrak{m} \subset \overline{\mathbb{F}}_\ell$. Moreover, we let

$$V = J_1(\ell)(\overline{\mathbb{Q}})[\mathfrak{m}] = \{x \in J_1(\ell)(\overline{\mathbb{Q}}) \mid tx = 0 \text{ for all } t \text{ in } \mathfrak{m}\}.$$

Then we have:

Theorem 3.3. *The set V is a 2-dimensional $\mathbb{T}/\mathfrak{m}$-linear subspace of $J_1(\ell)(\overline{\mathbb{Q}})[\ell]$. Moreover, the representation*

$$\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(V)$$

is isomorphic to the modular Galois representation ρ_f.

Proof. See [20, Section 3.2 and 3.3]). □

Let L be the fixed field of $\ker(\rho_f)$ of the Galois representation ρ_f. Then the representation ρ_f can factor through as:

$$\begin{tikzcd}
Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[rr, "\rho_f"] \arrow[dr, "\pi"'] & & GL_2(\overline{\mathbb{F}}_\ell) \\
& Gal(L/\mathbb{Q}) \arrow[ur, "\phi"'] &
\end{tikzcd}$$

where π is the canonical restriction map and ϕ is the isomorphism between $\mathrm{Gal}(L/\mathbb{Q})$ and the image $\mathrm{im}(\rho_f)$ of ρ_f. It can be shown that, to compute ρ_f, it suffices to compute a suitable polynomial $P_f(x) \in \mathbb{Q}[x]$ of degree $\ell^2 - 1$ with

$$P_f(x) = \prod_{P \in V - \{0\}} (x - h(P))$$

for some suitable function h in the function field of $X_1(\ell)$. Here $h(P) = \sum_{i=1}^{g} h(P_i)$ where g is the genus of $X_1(\ell)$, and P_i are the points on $X_1(\ell)$ such that each divisor $P \in V - \{0\}$ can be written as $\sum_{i=1}^{g}(P_i) - gO$.

In fact, it can be shown that the fixed field of ρ_f is actually the splitting field of $P_f \in \mathbb{Q}[x]$. Then one can obtain L by adjoining the roots of P_f to $\mathbb{Q}$, and the isomorphism ϕ is induced by the bijection between the roots of P_f and the points of the 2-dimensional $\mathbb{T}/\mathfrak{m}$-linear subspace V of $J_1(\ell)(\overline{\mathbb{Q}})[\ell]$.

3.3. Computations of projective Galois representations

Composed with the canonical projection map $GL_2(\mathbb{F}_\lambda) \to PGL_2(\mathbb{F}_\lambda)$, the representation ρ_f in (3.1) gives a projective representation

$$\tilde{\rho}_f : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to PGL_2(\overline{\mathbb{F}}_\ell).$$

Now we apply Theorem 3.2 to the projective representation cases and then we have:

Theorem 3.4. *Let f_1 and f_2 be two normalized eigenforms of type (N, k_1, ε) and (N, k_2, ε), respectively. Let i be an integer with $0 \le i \le \ell - 1$. Suppose that $k_1 \equiv k_2 + 2i \mod \ell - 1$ and $a_p(f_1) = p^i a_p(f_2)$ in $\overline{\mathbb{F}}_\ell$ for all primes p with $p \le \frac{\ell(\ell+1)[SL_2(\mathbb{Z}):\Gamma_1(N)]}{12}$. Then $\tilde{\rho}_{f_1}$ and $\tilde{\rho}_{f_2}$ are isomorphic.*

Proof. It follows from Theorem 3.2 that $\tilde{\rho}_{f_1}$ and $\tilde{\rho}_{f_2} \otimes \chi_\ell^i$ are isomorphic. For any $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, we have

$$\rho_{f_2} \otimes \chi_\ell^i(\sigma) = \rho_{f_2}(\sigma) \cdot \chi_\ell^i(\sigma).$$

In $PGL_2(\mathbb{F}_\lambda)$, we have

$$\overline{\rho_{f_2}(\sigma)} = \overline{\rho_{f_2}(\sigma) \cdot \chi_\ell^i(\sigma)},$$

where, as usual, the bar denotes the quotient by the subgroup of $GL_2(\overline{\mathbb{F}}_\ell)$ consisting of scalar matrices. Hence we have $\tilde{\rho}_{f_2} \otimes \chi_\ell^i = \tilde{\rho}_{f_2}$ and this implies $\tilde{\rho}_{f_1}$ and $\tilde{\rho}_{f_2}$ are isomorphic. □

Now we can describe the algorithm for computing the projective Galois representation $\tilde{\rho}_f$ associated to an normalized eigenform of type (N, k, ε) with $\ell < k - 1$.

First, by Theorems 2.3 and 3.4, we can explicitly obtain a normalized eigenform f' of type (N, k', ε) with $2 \le k' \le \ell + 1$ such that $\tilde{\rho}_f$ and $\tilde{\rho}_{f'}$ are isomorphic. Thus our computations boil down to the case with $2 \le k' \le \ell + 1$. Then again we can reduce the question to the weight 2 case using the same arguments in the previous subsection. Finally, we can compute a suitable polynomial instead for the following reason:

Let K be the fixed field of $\ker(\tilde{\rho}_f)$, then the representation $\tilde{\rho}_f$ can factor through as:

$$\begin{tikzcd}
 & GL_2(\mathbb{F}_\lambda) \arrow[dr] & \\
Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[ur, "\rho_{f,\lambda}"] \arrow[rr, "\tilde{\rho}_{f,\lambda}"] \arrow[dr, "\pi"'] & & PGL_2(\mathbb{F}_\lambda) \\
 & Gal(K/\mathbb{Q}) \arrow[ur, "\varphi"'] &
\end{tikzcd}$$

where π is the canonical restriction map and φ is the isomorphism between $\mathrm{Gal}(\overline{L/\mathbb{Q}})$ and $\mathrm{im}(\tilde{\rho}_f)$. Let $V = J_1(\ell)(\overline{\mathbb{Q}})[\mathfrak{m}]$ be the 2-dimensional $\mathbb{T}/\mathfrak{m}$-linear subspace of $J_1(\ell)(\overline{\mathbb{Q}})[\ell]$ as in Theorem 3.3. Then the projective line $\mathbb{P}(V)$ has $\ell + 1$ points, and it follows that the fixed field of $\tilde{\rho}_f$ is in fact the splitting field K of a certain polynomial $\tilde{P}_f \in Q[x]$ of degree $\ell + 1$, which is given by

$$\tilde{P}_f(x) = \prod_{A \subset \mathbb{P}(V)} (x - \sum_{P \in A - \{0\}} h(P)). \tag{3.5}$$

Moreover, one can obtain K by adjoining the roots of $\tilde{P}_{f,\ell}$ to $\mathbb{Q}$ and, the isomorphism φ is induced by the bijection between the roots of $\tilde{P}_f$ and the points of the projective line $\mathbb{P}(V)$. This implies that the projective representation $\tilde{\rho}_f$ can be described by the polynomial $\tilde{P}_f$.

4. Explicit computations

For $k = 16, 18, 20, 22$ and 26, let $\Delta_k = \sum_{n>0}^{\infty} a_n q^n$ denote the unique cusp form of level 1 and weight k. A prime ℓ is said to be *exceptional* if the image of $\rho_{\Delta_k,\ell}$ does not contain $SL_2(\mathbb{F}_\ell)$. Otherwise, a prime ℓ is called *unexceptional.*

Bosman [1] first does practical computations and obtains $\tilde{P}_{\Delta_k}$ for modular forms Δ_k of level 1 and of weight $k \leq 22$, with $\ell \leq 23$. Others improve the algorithm and computed the polynomials for more cases. See [4] and [5] for instance. As far as we know, all the polynomials $\tilde{P}_{\Delta_k}$ that have been computed in this method are shown in [1, Section 7.5] and [5, Table 4].

Note that all the computed polynomials are of the cases with $k \leq \ell+1$. In this section, we shall apply the algorithm described in Subsection 3.3 to explicitly compute the polynomials $\tilde{P}_{\Delta_k}$ associated to the mod ℓ projective Galois representations $\tilde{\rho}_{\Delta_k}$ for $k = 16, 20, 22, 26$ and all the unexceptional primes ℓ, with $\ell < k - 1$.

As an application, we shall discuss the non-vanishing Fourier coefficients of Δ_k using our results.

4.1. Reducing to the cases with $k \leq \ell + 1$.

For a prime ℓ, we let $\tilde{\Delta}_k = \sum_{n>0}^{\infty} \tilde{a}_n q^n$, where $\tilde{a}_n$ means the reduction of a_n mod ℓ. Then $\tilde{\Delta}_k$ is a normalized cuspidal eigenform of type $(1, k, 1)$. We denote by $\tilde{P}_{\Delta_k,\ell}$ the polynomial $\tilde{P}_{\Delta_k}(x)$ defined in (3.5) which describes the mod ℓ projective Galois representation $\tilde{\rho}_{\Delta_k}$ associated to $\tilde{\Delta}_k$.

A prime ℓ is said to be exceptional if the image of ρ_f does not contain $SL_2(\mathbb{F}_\ell)$. In Table 2 we list the all unexceptional primes for Δ_k with $\ell < k - 1$. Then for the (k, ℓ) in Table 2, we shall compute the polynomials $\tilde{P}_{\Delta_k,\ell}$.

Table 2. Small unexceptional primes for Δ_k.

k	ℓ
16	13
20	17
22	11 19
26	13 23

For Δ_k and unexceptional prime ℓ, with (k, ℓ) in Table 2, we apply Theorem 3.4 to find normalized eigenforms f of type $(1, k', 1)$ with $k' < \ell - 1$ such that $\tilde{\rho}_{\Delta_k}$ and $\tilde{\rho}_f$ are isomorphic. More precisely, we first obtain all pairs (i, k') such that

$$k \equiv k' + 2i \mod \ell - 1.$$

Then we take a pair (i, k') such that $a_p(f_1) \equiv p^i a_p(f_2) \mod \ell$ for all primes p with $p \leq \frac{\ell(\ell+1)}{12}$. This condition can be verified quickly in SAGE. In fact, by Theorem 2.3, such k' and i do exist and after doing some simple calculations we explicitly obtain the forms that satisfy the conditions in Theorem 3.2. Then by Theorem 3.4, we finally reduce the computations to the cases with $k \leq \ell + 1$. Thus it gives:

Proposition 4.1. *We take values of k, ℓ, i, k' in each row of Table 3. Then we have the congruences*

$$\Delta_k \equiv \theta^i \Delta_{k'} \mod \ell,$$

and moreover, we have $\tilde{\rho}_{\Delta_k} \cong \tilde{\rho}_{\Delta_{k'}}$.

Table 3. The values of k, ℓ, i, k'.

k	ℓ	i	k'
16	13	2	12
20	17	2	16
22	11	1	12
	19	2	18
26	13	1	12
	23	2	22

4.2. The polynomials $\tilde{P}_{\Delta_k,\ell}$

We take values of k, ℓ, i, k' in each row of Table 3. Since $\tilde{\rho}_{\Delta_k}$ and $\tilde{\rho}_{\Delta_{k'}}$ are isomorphic, we have

$$\tilde{P}_{\Delta_k,\ell}(x) = \tilde{P}_{\Delta_{k'},\ell}(x).$$

Fortunately, all the corresponding polynomials $\tilde{P}_{\Delta_{k'},\ell}(x)$ have been computed and shown in [1, Section 7.5]. As a result, the polynomials $\tilde{P}_{\Delta_k,\ell}(x)$ associated to the mod ℓ projective Galois representation $\tilde{\rho}_{\Delta_k}$ are shown in Table 4.

Table 4. The polynomials $\tilde{P}_{\varDelta_k,\ell}$ associated to $\tilde{\rho}_{\Delta_k}$.

(k, ℓ)	$\tilde{P}_{\varDelta_k,\ell}$
(16, 13)	$x^{14}+7x^{13}+26x^{12}+78x^{11}+169x^{10}+52x^9-702x^8-1248x^7+494x^6+2561x^5+312x^4-2223x^3+169x^2+506x-215$
(20, 17)	$x^{18}-2x^{17}-17x^{15}+204x^{14}-1904x^{13}+3655x^{12}+5950x^{11}-3672x^{10}-38794x^9+19465x^8+95982x^7-280041x^6-206074x^5+455804x^4+946288x^3-1315239x^2+606768x-378241$
(22, 11)	$x^{12}-4x^{11}+55x^9-165x^8+264x^7-341x^6+330x^5-165x^4-55x^3+99x^2-41x-111$
(22, 19)	$x^{20}+10x^{19}+57x^{18}+228x^{17}-361x^{16}-3420x^{15}+23446x^{14}+88749x^{13}-333526x^{12}-1138233x^{11}+1629212x^{10}+13416014x^9+7667184x^8-208954438x^7+95548948x^6+593881632x^5-1508120801x^4-1823516526x^3+2205335301x^2+1251488657x-8632629109$
(26, 13)	$x^{14}+7x^{13}+26x^{12}+78x^{11}+169x^{10}+52x^9-702x^8-1248x^7+494x^6+2561x^5+312x^4-2223x^3+169x^2+506x-215$
(26, 23)	$x^{24}-11x^{23}+46x^{22}-1127x^{20}+6555x^{19}-7222x^{18}-140737x^{17}+1170700x^{16}-2490371x^{15}-16380692x^{14}+99341324x^{13}+109304533x^{12}-2612466661x^{11}+4265317961x^{10}+48774919226x^9-244688866763x^8-88695572727x^7+4199550444457x^6-10606348053144x^5-25203414653024x^4+185843346182048x^3-228822955123883x^2-1021047515459130x+2786655204876088$

4.3. *An application for the non-vanishing Fourier coefficients of Δ_k*

In [9], the authors discuss the non-vanishing Fourier coefficients of Δ_k with $k = 16, 18, 20, 22, 26$ and achieve the explicit bounds B_k of n such that the Fourier coefficients $a_n(\Delta_k) \neq 0$ for all $n < B_k$. They first prove that the smallest n for which $a_n(\Delta_k) = 0$ must be a prime. Then, for each prime p with $a_p(\Delta_k) = 0$, they obtain the formulations that such p must satisfy. In addition, the congruence

$$a_p(\Delta_k) \equiv 0 \mod \ell$$

can be verified by the polynomials $\tilde{P}_{\Delta_k,\ell}$ associated to the projective Galois representations. Precisely, when the polynomial $\tilde{P}_{\Delta_k,\ell} \in \mathbb{Z}[x]$, it can be shown that $a_p(\Delta_k) \equiv 0 \mod \ell$ is equivalent to $\tilde{P}_{\Delta_k,\ell} \mod p$ having an irreducible factor of degree 2 in $\mathbb{F}_p[x]$. Consequently, one can systematically search for the smallest prime p satisfying the formulations, as well as $a_p(\Delta_k) \equiv 0 \mod \ell$.

Now we can add the polynomials $\tilde{P}_{\Delta_k,\ell}$ in Table 4 to the searching computations. That is, for $k = 16, 20, 22, 26$ and all the small unexceptional primes ℓ in Table 2, we can efficiently verify the additional searching conditions

$$a_p(\Delta_k) \equiv 0 \mod \ell.$$

As a result, for $k = 16, 20, 22, 26$, we are able to obtain the new bounds B_k of n such that $a_n(\Delta_k) \neq 0$ for all $n < B_k$.

Proposition 4.2. *Let the pair (k, B_k) take the values as in Table 5. Then the coefficients $a_n(\Delta_k)$ are non-vanishing for all n with $n < B_k$ in Table 5.*

Table 5. The bounds B_k.

k	B_k
16	169424346446440054199
20	1222095705994609939349
22	567829713758553825538049
26	3442219356673306598399

5. Further work and applications

The computational results of modular Galois representations can be applied to compute the Fourier coefficients of modular forms f according to (3.2). More precisely, if we can calculate mod ℓ Galois representations for enough primes ℓ whose product exceeds $4p^{(k-1)/2}$, the coefficient $a_p(f)$ can be easily computed by Chinese Remainder Theorem. Our results in this paper add the small primes to the list and can be applied to the computations of the Fourier coefficients of modular forms. Besides, for many groups $\mathrm{SL}_2(\mathbb{F}_{\ell^k})$ and $\mathrm{GL}_2(\mathbb{F}_{\ell^k})$, it is still unknown whether they are Galois groups of number fields over rational field $\mathbb{Q}$. Our results are expected to answer some of these questions, since our computations also provide number fields and their Galois groups, namely $\mathrm{SL}_2(\mathbb{F}_{\ell^k})$ and $\mathrm{GL}_2(\mathbb{F}_{\ell^k})$.

6. Conclusions

In this paper, we give an explicit method, for a given modular form of type (N, k, ε), to obtain a twist form of type (N, k', ε) with $k' \leq \ell + 1$, such that the two Galois representations associated to the two forms are isomorphic up to twist. Then we prove the corresponding results for the projective representations and present the algorithm for the projective case. Moreover, we apply the algorithm in Subsection 3.3 to do explicit computations of the mod ℓ projective Galois representations $\tilde{\rho}_{\Delta_k}$ for $k = 16, 20, 22, 26$ and all the unexceptional primes ℓ for which $\ell < k - 1$. The computed projective polynomials $\tilde{P}_{\Delta_k}(x)$ associated to the representations $\tilde{\rho}_{\Delta_k}$ are shown in Table 4.

In the end, as an application, we discuss the non-vanishing Fourier coefficients of Δ_k using our results. In fact, for $k = 16, 20, 22, 26$, we obtain new higher bounds B_k of n such that $a_n(\Delta_k) \neq 0$ for all $n < B_k$, which are shown in Table 5.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgements

Peng Tian is supported by NSFC (NOs: 11601153) and Ha T. N. Tran was supported by the Natural Sciences and Engineering Research Council of Canada (NSERC) (funding RGPIN-2019-04209 and

DGECR-2019-00428).

Conflict of interest

The authors declare that they have no conflicts of interest.

References

1. S. J. Edixhoven, J. M. Couveignes, R. S. de Jong, F. Merkl, J. G. Bosman, *Computational Aspects of Modular Forms and Galois Representations*, Ann. of Math. Stud., 176, Princeton Univ. Press, Princeton, 2011.
2. P. Bruin, *Modular curves, Arakelov theory, algorithmic applications*, Ph.D. thesis, Universiteit Leiden, 2008.
3. N. Mascot, Computing modular Galois representations, *Rendiconti del Circolo Matematico di Palermo*, **62** (2013), 451–476. https://doi.org/10.1007/s12215-013-0136-4
4. P. Tian, Computations of Galois representations associated to modular forms of level one, *Acta Arith.*, **164** (2014), 399–412. https://doi.org/10.4064/aa164-4-5
5. M. Derickx, M. van Hoeij, J. Zeng, *Computing Galois representations and equations for modular curves $X_H(\ell)$*, `http://arxiv.org/abs/1312.6819`
6. J. Sturm, On the congruence of modular forms, *Lect. Notes Math.*, **1240** (1987), 275–280. https://doi.org/10.1007/BFb0072985
7. D. H. Lehmer, The vanishing of Ramanujan's function $\tau(n)$, *Duke Math. J.*, **10** (1947), 429–433. https://doi.org/10.1215/S0012-7094-47-01436-1
8. J. P. Serre, *Une interprétation des congruences relatives à la fonction de Ramanujan*, Séminaire Delange-Pisot-Poitiou, 14, 1968.
9. P. Tian, H. Qin, Non-vanishing Fourier coefficients of Δ_k, *Appl. Math. Computat.*, **339** (2018), 507–515. https://doi.org/10.1016/j.amc.2018.07.022
10. *SAGE, Open source mathematics software,* `http://sagemath.org`
11. J. P. Serre, Formes modulaires et fonctions zêta p-adiques, *Lect. Notes Math.*, **350** (1973), 191–268. https://doi.org/10.1007/978-3-540-37802-0_4
12. H. P. F. Swinnerton-Dyer, On ℓ-adic representations and congruences for coefficients of modular forms (I), *Lect. Notes Math.*, **350** (1973), 1–55. https://doi.org/10.1007/BFb0072985
13. N. M. Katz, p-adic properties of modular schemes and modular forms, *Lect. Notes Math.*, **350** (1973), 69–190. https://doi.org/10.1007/978-3-540-37802-0_3
14. B. H. Gross, A tameness criterion for Galois representations associated to modular forms (MOD p), *Duke Math. J.*, **61** (1990), 445–517. https://doi.org/10.1215/S0012-7094-90-06119-8
15. S. J. Edixhoven, The weight in Serre's conjectures on modular forms, *Invent. Math.*, **109** (1992), 563–594. https://doi.org/10.1007/BF01232041
16. N. M. Katz, A result on modular forms in characteristic p, *Lect. Notes Math.*, **601** (1976), 53–61. https://doi.org/10.1007/BFb0063944

17. W. Kohnen, On Fourier coefficients of modular forms of different weights, *Acta Arith.*, **113** (1971), 57–67.

18. P. Deligne, Formes modulaires et représentations ℓ-adiques, *Lect. Notes Math.*, **179** (1971), 139–172. https://doi.org/10.1007/BFb0058810

19. K. A. Ribet, Report on mod ℓ representations of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, Motives (Seattle, WA, 1991), *Amer. Math. Soc., Providence, RI*, 1994, 639–676.

20. K. A. Ribet, W. A. Stein, Lectures on Serre's conjectures, Arithmetic algebraic geometry (Park City, UT, 1999), *Amer. Math. Soc., Providence, RI*, 2001, 143–232.