Realization of modular Galois representations in the Jacobians of modular curves

Peng Tian

Received: 13 October 2020 / Accepted: 22 December 2021 / Published online: 23 March 2022
© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2022

Abstract
In Tian (Acta Arith. 164:399–412, 2014), the author improved the algorithm proposed by Edixhoven and Couveignes for computing mod $\ell$ Galois representations associated to eigenforms $f$ for the cases that $\ell \geq k - 1$ and $f$ has level one, where $k$ is the weight of $f$. In this paper, we generalize the results of Tian (Acta Arith. 164:399–412, 2014) and present a method to find the Jacobians of modular curves of minimal dimensions to realize the modular Galois representations. Our method works for the cases that $\ell \geq 5$ may be any prime without the assumption $\ell \geq k - 1$ and the eigenforms $f$ have arbitrary levels prime to $\ell$. Moreover, if $k > 2$, we give criteria for realizing the mod $\ell$ Galois representations in the Jacobians $J_0$ of $X_0$.

Keywords Modular forms · Modular Galois representations · Jacobians of modular curves

Mathematics Subject Classification Primary 11Fxx · 11G10 · Secondary 11Y10 · 11G30

1 Introduction

In the book [5], Edixhoven and Couveignes proposed a polynomial time algorithm to compute the mod $\ell$ Galois representations $\rho_{f,\ell}$ associated to level one eigenforms. Bruin [1] generalized the algorithm to eigenforms of arbitrary levels.

Let $f \in S_k(\Gamma_0(N), \varepsilon)$ be an eigenform and $\ell$ be a prime with $\ell \geq k - 1$. Let $N' = N\ell$ if $k > 2$ and $N' = N$ if $k = 2$.

This work is supported by NSFC (No: 11601153).

Peng Tian
tianpeng@ecust.edu.cn

1 Department of Mathematics, East China University of Science and Technology, Shanghai 200237, People’s Republic of China
Let $J_1$ denote the Jacobian of the modular curve $X_1(N')$ associated to $\Gamma_1(N')$. Let $\mathbb{T} \subseteq \text{End} J_1$ be the Hecke algebra associated to $S_2(\Gamma_1(N'))$ and $m$ be the maximal ideal associated to $f$. Then it is well known that the $(\mathbb{T}/m)[\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})]$-module $J_1(\overline{\mathbb{Q}})[m]$ is a non-zero finite direct sum of copies of $\rho_{f,m}$. The computations of $\rho_{f,m}$ boil down to producing the representation

$$\rho_{J_1(\overline{\mathbb{Q}})[m]} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{Aut}_{\mathbb{Q}/m}(J_1(\overline{\mathbb{Q}})[m]).$$

Edixhoven and Couveignes [5] proposed a method to efficiently compute $\rho_{J_1(\overline{\mathbb{Q}})[m]}$. They proved that $\rho_f$ can be described by a certain polynomial $P_f \in \mathbb{Q}[x]$ whose splitting field is the fixed field $L$ of $\ker(\rho_f)$. The polynomial can be computed by approximately evaluating the points of $J_1(\overline{\mathbb{Q}})[m]$.

However, in practice, the most time-consuming part of the algorithm is to evaluate $J_1(\overline{\mathbb{Q}})[m]$ and it heavily depends on the dimension of $J_1$. In the paper [10], the author presented an improvement of this algorithm in the cases that $\ell \geq k - 1$ and $f$ has level one. In these cases, one can do the computations with the Jacobian $J_{\Gamma_H}$ of $X_{\Gamma_H}$ rather than $J_1$, where $X_{\Gamma_H}$ is a modular curve of smaller genus with $\Gamma_1(\ell) \leq \Gamma_H \leq \Gamma_0(\ell)$. The explicit computations of evaluating $J_1(\overline{\mathbb{Q}})[m]$ can be greatly reduced by this improved algorithm.

In this paper, we generalize the improved algorithm of [10] to the cases that $\ell \geq 5$ may be any prime without the assumption $\ell \geq k - 1$ and the eigenforms $f$ have arbitrary levels prime to $\ell$.

We firstly propose a method, for a normalized eigenform $f \in S_k(\Gamma_1(N), \varepsilon)$, to find an integer $i$, a congruence subgroup $\Gamma_H$ and a normalized eigenform $f_2 \in S_2(\Gamma_H)$, such that $\rho_{f,\ell}$ is isomorphic to $\rho_{f_2,\ell} \otimes \chi_{\ell}'$. The form $f_2$ given by our method is determined in terms of $\varepsilon, k$ and $i$. Moreover, we prove that the subgroup $\Gamma_H$ produced by this method is the largest possible congruence subgroup with $\Gamma_1(N') \subseteq \Gamma_H \subseteq \Gamma_0(N')$, on which such an eigenform $f_2$ exists. We also give an algorithm for explicitly computing the weight 2 eigenform $f_2$.

Let $J_{\Gamma_H}$ be the Jacobian of the modular curve $X_{\Gamma_H}$ associated to $\Gamma_H$. We then show that $J_1(\overline{\mathbb{Q}})[m]$ is a subspace of $J_{\Gamma_H}[\ell]$ and the representation $\rho_{J_1(\overline{\mathbb{Q}})[m]}$ is a subrepresentation of $J_{\Gamma_H}[\ell]$. This allows us to evaluate the points of $J_1(\overline{\mathbb{Q}})[m]$ by working with the Jacobian $J_{\Gamma_H}$, which has the smallest possible dimension in the sense that $\Gamma_H$ is the largest possible congruence subgroup.

As examples, we do explicit computations to calculate the eigenforms $f_2$ and list the dimensions of $J_1(N')$ and $J_{\Gamma_H}$ in the cases with $\ell$ up to 13 and $N$ up to 6.

In the last section, we discuss the cases with $k > 2$ and $\Gamma_H = \Gamma_0(N\ell)$. To be precise, we first prove that, for a normalized eigenform $f \in S_k(\Gamma_0(N))$, the index $[\Gamma_H : \Gamma_1(N\ell)]$ of $\Gamma_1(N\ell)$ in $\Gamma_H$ is equal to $\phi(N) \cdot \gcd(\ell - 1, k - 2 - 2i)$. It is easy to see that the main theorem (Proposition 4.1) of [10] is a special case of this result with $N = 1$ and $\ell \geq k - 1$. Then we apply this result to give the criteria for the occurrence of $\Gamma_H = \Gamma_0(N\ell)$. As a consequence of the criteria, we show that, for a normalized eigenform $f \in S_{\ell+1}(\Gamma_1(N))$, the existence of a normalized eigenform $f_2 \in S_2(\Gamma_0(N\ell))$ with $\rho_{f,\ell} \cong \rho_{f_2,\ell}$ is equivalent to $f \in S_{\ell+1}(\Gamma_0(N))$. 

\textcopyright Springer
The rest of this paper is organized as follows. In Sect. 2, we recall the computations of modular Galois representations. In Sect. 3, we recall some results on Dirichlet characters and then define Teichmüller lifting of Dirichlet characters. In Sect. 4, we present our methods and algorithm to compute the largest possible congruence subgroups for the weight 2 eigenforms associated to $\rho_{f,\ell}$. In Sect. 5, we give the results on realizing the modular Galois representations in the Jacobians of minimal dimensions. In the last section, we apply our main results to the case of eigenforms on $\Gamma_0(N)$ and obtain the criteria for the occurrence of $\Gamma_H = \Gamma_0(N\ell)$.

2 Computations of modular Galois representations

We let $\ell$ denote a prime with $\ell \geq 5$ and $v$ be a place dividing $\ell$ of the field of algebraic numbers $\overline{\mathbb{Q}}$. The residue field of $v$ is denoted by $\mathbb{F}_\ell$ and it is then the algebraic closure of the prime field $\mathbb{F}_\ell$.

For any positive integer $n$, the congruence subgroups $\Gamma_0(n)$ and $\Gamma_1(n)$ respectively are

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}) \mid c \equiv 0 \pmod{n} \right\}$$

and

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, \mathbb{Z}) \mid c \equiv 0 \pmod{n} \text{ and } d \equiv 1 \pmod{n} \right\}.$$

Now let $N > 0$ and $k \geq 2$ be integers. Let $q = q(z) = e^{2\pi iz}$ and $f(z) = \sum_{n>0} a_n(f) q^n \in S_k(\Gamma_1(N), \varepsilon)$ be a normalized eigenform of weight $k$ and level $N$, with nebentypus character $\varepsilon$. Let $K_f$ be the coefficient number field of $f$, which is obtained by adjoining all the Fourier coefficients $a_n(f)$ of the $q$-expansion of $f$ to $\mathbb{Q}$. Let $\lambda$ be a prime of $K_f$ lying over $\ell$. Then Deligne [3] proves the following well known theorem:

**Theorem 1** There exists a unique (up to isomorphism) continuous semi-simple representation

$$\rho_{f,\lambda} : \text{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to GL_2(\mathbb{F}_\ell).$$

which is unramified outside $N\ell$ and such that for all primes $p \nmid N\ell$ the characteristic polynomial of $\rho_{f,\lambda}(\text{Frob}_p)$ satisfies

$$\text{charpol}(\rho_{f,\lambda}(\text{Frob}_p)) \equiv x^2 - a_p(f)x + \varepsilon(p)p^{k-1} \pmod{\lambda}. \quad (2.1)$$

We also let $\rho_{f,\ell}$ denote the representation $\rho_{f,\lambda}$ when the prime $\lambda$ is not involved in our discussion.

In the book [5], Edixhoven and Couveignes proposed a polynomial time algorithm to compute $\rho_{f,\ell}$ for level one eigenforms. In his PhD thesis [1], Bruin generalized the algorithm to eigenforms of arbitrary levels.
Let $f \in S_k(\Gamma_1(N), \varepsilon)$ be a normalized eigenform. Suppose $\ell \geq k - 1$. Let $N' = N \ell$ if $k > 2$ and $N' = N$ if $k = 2$. We let $J_1$ be the Jacobian of the modular curve $X_1(N')$ associated to $\Gamma_1(N')$. Let $T \subseteq \text{End} J_1$ be the Hecke algebra generated by the diamond and Hecke operators over $\mathbb{Z}$ and let $I_f$ be the ring homomorphism $I_f : T \to \mathbb{F}_\ell$, given by $\langle d \rangle \mapsto \varepsilon(d)$ and $T_n \mapsto a_n(f) \mod v$. Let $m_f$ denote the kernel of $I_f$ and if we put $V_f = J_1(\mathbb{Q})[m_f] = \{ x \in J_1(\overline{\mathbb{Q}}) \mid tx = 0 \text{ for all } t \in m_f \}$, then $V_f$ is a non-zero finite direct sum of copies of $\rho_{f,\ell}$. The number of the copies of $\rho_{f,\ell}$ is called multiplicity of $\rho_{f,\ell}$. For details, we refer to [8, Sects. 3.2 and 3.3].

Thus, to compute modular Galois representation $\rho_{f,\ell}$, it suffices to compute the representation $\rho_{V_f} : \text{Gal}(\overline{\mathbb{Q}}) \to \text{Aut}_{T/m_f}(V_f)$ (in the case that the multiplicities are larger than one, it is in fact sufficient to compute any simple constituent of $\rho_{V_f}$).

The method provided by Edixhoven and Couveignes to compute $\rho_{V_f}$ is to evaluate a suitable polynomial $P_{V_f} \in \mathbb{Q}[x]$ whose splitting field is the fixed field of $\rho_{V_f}$. More precisely, we can take the polynomial to be

$$P_{V_f}(x) = \prod_{Q \in V_f - \{0\}} (x - \sum_{i=1}^{g} h(Q_i)),$$

for some suitable function $h(x)$ in the function field of $X_1(N')$, where $g$ is the genus of $X_1(N')$ and $Q_i$ are the points on $X_1(N')$ such that $Q = \sum_{i=1}^{g} (Q_i) - g \cdot (O)$ as divisors on $X_1(N')$ via the Abel-Jacobi map.

In [5], the authors proposed two methods to efficiently evaluate the points $Q \in V_f - \{0\}$, either over complex numbers or modulo sufficiently many small prime numbers to reconstruct $V_f$. In each of the methods, however, it requires high precisions to approximate the points of $V_f$. Consequently, it always takes quite much time to obtain the polynomial $P_{V_f}$ in practice. It is known that the required precisions and calculations increase very rapidly with the growth of the dimension of the Jacobian. Therefore, the calculations can be largely decreased if we can work with a Jacobian which has a smaller dimension.

### 3 Dirichlet characters and Teichmüller lifting

Let $n$ be a positive integer and $\varepsilon : (\mathbb{Z}/n\mathbb{Z})^* \to \mathbb{C}^*$ be a Dirichlet character modulo $n$. For any positive divisor $d$ of $n$, we let $\pi_{n,d}$ be the canonical projection

$$\pi_{n,d} : (\mathbb{Z}/n\mathbb{Z})^* \to (\mathbb{Z}/d\mathbb{Z})^*, \ x \mod n \mapsto x \mod d.$$ 

Then we know $\pi_{n,d}$ is surjective.
Each Dirichlet character \( \varepsilon \) modulo \( d \) can lift to a unique Dirichlet character \( \varepsilon_{\text{ind}} \) modulo \( n \) such that
\[
\varepsilon_{\text{ind}} = \varepsilon \circ \pi_{n,d},
\]
and the character \( \varepsilon_{\text{ind}} \) is said to be induced by \( \varepsilon \).

For a positive integer \( n \), we let \( \zeta_n \) denote a primitive \( n \)-th root of unity. To give the definition of Teichmüller lifting of Dirichlet character, we need

**Lemma 1** Let \( n \) be a positive integer. Let \( \ell \) be a prime number with \( \ell \nmid n \) and \( v \) be a place dividing \( \ell \) of \( \overline{\mathbb{Q}} \). Then the \( n \)-th roots of unity are distinct modulo \( v \).

**Proof** Since \( \ell \nmid n \), it is easy to see that \( x^n - 1 \) and its derivative \( nx^{n-1} \) are coprime mod \( \ell \). It follows that \( x^n - 1 \) has no double roots in \( \mathbb{F}_\ell \). \( \square \)

Let \( \ell \) be a prime number and \( v \) be a place dividing \( \ell \) of \( \overline{\mathbb{Q}} \). Let \( n \) be a positive integer and \( \varepsilon \) be a Dirichlet character modulo \( n \). Let \( E \) denote the number field which is obtained by adjoining all the values of \( \varepsilon \) to \( \mathbb{Q} \). For a prime \( \lambda \) of \( E \) lying over \( \ell \), let \( \bar{\varepsilon} \) denote the reduction of \( \varepsilon \) mod \( \lambda \). Then we have

**Proposition 1** There exists a Dirichlet character \( T(\bar{\varepsilon}) \) modulo \( n \) which satisfies:
1. \( T(\bar{\varepsilon}) \equiv \varepsilon \mod v \); and
2. \( \ker(T(\bar{\varepsilon})) = \ker(\bar{\varepsilon}) \).

**Proof** Let \( O_E \) be the integer ring of \( E \) and \( \mathbb{F}_\lambda = O_E / \lambda \) be the residue field. We let \( q = \#\mathbb{F}_\lambda \) and \( \mu_{q-1} = \{\zeta_{q-1}^j | 0 \leq j \leq q - 2\} \) be the group of \( (q - 1) \)-st roots of unity. Since both \( \mu_{q-1} \) and \( \mathbb{F}_\lambda^* \) have \( q - 1 \) elements, it follows from Lemma 1 that the reduction modulo \( \lambda \) restricted on \( \mu_{q-1} \)
\[
\begin{align*}
\rightarrow: \mu_{q-1} &\longrightarrow \mathbb{F}_\lambda^*, \\
a &\mapsto \bar{a} = a \mod \lambda,
\end{align*}
\]
is a group isomorphism. We denote its inverse by
\[
\omega: \mathbb{F}_\lambda^* \longrightarrow \mu_{q-1}.
\]
Then it satisfies \( \omega(x) \equiv x \mod v \). Composing \( \omega \) with \( \bar{\varepsilon} \), we obtain a Dirichlet character \( T(\bar{\varepsilon}) = \omega \circ \bar{\varepsilon} \) modulo \( n \) which satisfies:
1. \( \omega \circ \bar{\varepsilon} \equiv \varepsilon \mod v \); and
2. \( \ker(\omega \circ \bar{\varepsilon}) = \ker(\bar{\varepsilon}) \).

**Definition 1** The Dirichlet character \( T(\bar{\varepsilon}) \) given in Proposition 1 is called a Teichmüller lifting of \( \bar{\varepsilon} \).
The largest possible congruence subgroups of the weight 2 eigenforms associated to $\rho_{f,\ell}$

Let $N > 0$ be an integer and $f$ be an eigenform of level $N$. In this section, we present our method to obtain a largest possible congruence subgroup $\Gamma_H$, on which there exists a weight 2 eigenform $f_2$ such that $\rho_{f,\ell}$ is isomorphic to a twist of $\rho_{f_2,\ell}$. We also give an algorithm for explicitly computing the eigenform $f_2$.

We follow the notation of Sect. 2. Moreover, the following notations are used in the rest of this paper.

Let $n$ be a positive integer and $H$ be a subgroup of $(\mathbb{Z}/n\mathbb{Z})^*$. Then we let $\Gamma_H(n)$ denote the congruence subgroup

$$\Gamma_H(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbb{Z}) \mid c \equiv 0 \pmod{n} \text{ and } d \pmod{n} \in H \right\}.$$

Let $\varphi_n$ denote the surjection:

$$\varphi_n : \Gamma_0(n) \twoheadrightarrow (\mathbb{Z}/n\mathbb{Z})^*, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d.$$

Then the kernel of $\varphi_n$ is $\Gamma_1(n)$ and the preimage $\varphi_n^{-1}(H)$ of $H$ under $\varphi_M$ is $\Gamma_H(n)$.

4.1 Twists of modular Galois representations

In order to discuss the case with $\ell < k - 1$, we first give some results on the twists of modular Galois representations by the cyclotomic character.

Let $\chi_\ell$ denote the mod $\ell$ cyclotomic character. The following proposition, which is a corollary of [4, Theorem 3.4], allows us to reduce the case $\ell < k - 1$ to $\ell \geq k - 1$ by twisting.

**Proposition 2** Let $\ell \geq 5$ be a prime number, $N > 0$ an integer prime to $\ell$, and $k \geq 2$. Let $f \in S_k(\Gamma_1(N), \varepsilon)$ be an eigenform and $\lambda$ be a prime of $K_f$ lying over $\ell$. Suppose the representation $\rho_{f,\lambda}$ is irreducible and $a_1(f) \not\equiv 0 \pmod{\lambda}$. Then there exist integers $i$ and $k'$ with $0 \leq i \leq \ell - 1$, $2 \leq k' \leq \ell + 1$, a normalized eigenform $g \in S_{k'}(\Gamma_1(N), \varepsilon)$ and a prime $\ell$ of $K_g$ lying over $\ell$, such that $\rho_{f,\lambda}$ is isomorphic to $\rho_{g,\ell} \otimes \chi_\ell^i$.

**Proof** By [4, Theorem 3.4], we have $i$ and $k'$ with $0 \leq i \leq \ell - 1$, $k' \leq \ell + 1$, and an eigenform $g'$ which has level $N$ and Nebentypus character $\varepsilon$, and a prime $\ell$ of $K_{g'}$ lying over $\ell$, such that $\rho_{f,\lambda}$ is isomorphic to $\rho_{g',\ell} \otimes \chi_\ell^i$.

Since the representation $\rho_{f,\lambda}$ is irreducible, so is $\rho_{g',\ell} \cong \rho_{f,\lambda} \otimes \chi_\ell^{-i}$. It follows that $g'$ is a cuspidal eigenform. By $a_1(f) \not\equiv 0 \pmod{\lambda}$, we know $g'$ is nonzero, and thus we have $a_1(g') \neq 0$. Let $g = (a_1(g'))^{-1}g'$ be the normalized eigenform and then we have $g \in S_{k'}(\Gamma_1(N), \varepsilon)$ and $\rho_{f,\lambda} \cong \rho_{g,\ell} \otimes \chi_\ell^i$. 

Springer
4.2 Computing the largest possible congruence subgroups of the weight 2 eigenforms associated to $\rho_{f,\ell}$

Now we can give our main results on computing the largest possible congruence subgroup of the weight 2 eigenform associated to $\rho_{f,\ell}$.

First we state the following result without proof, which has been obtained independently by H. Carayol and J-P. Serre, and is usually called Carayol’s Lemma.

**Lemma 2** (Carayol’s Lemma) Let $\ell \geq 5$ be a prime and $v$ be a place dividing $\ell$ of $\overline{\mathbb{Q}}$. Let $f \in S_k(\Gamma_1(N), \varepsilon)$ be a normalized eigenform. Suppose the representation $\rho_{f,\ell}$ is irreducible. Let $\varepsilon'$ be a Dirichlet character which is congruent to $\varepsilon \mod v$. Then there exists a normalized eigenform $f' \in S_k(\Gamma_1(N), \varepsilon')$ such that $\rho_{f,\ell}$ and $\rho_{f',\ell}$ are isomorphic.

**Proof** See [2, Proposition 3].

Then for $k > 2$, we have the following result and we treat the case $k = 2$ later in Theorem 4.

**Theorem 2** Let $\ell \geq 5$ be a prime number, $N > 0$ an integer prime to $\ell$, and $k > 2$. Let $f \in S_k(\Gamma_1(N), \varepsilon)$ be a normalized eigenform and $\lambda$ be a prime of $K_f$ lying over $\ell$. Suppose the representation $\rho_{f,\lambda}$ is irreducible. Then there exist an integer $i$ with $0 \leq i \leq \ell - 1$, a normalized eigenform $f_2 \in S_2(\Gamma_H)$, and a prime $\lambda_2$ lying over $\ell$ in the field $K_{f_2}$, such that $\rho_{f,\lambda}$ is isomorphic to $\rho_{f_2,\lambda_2} \otimes \chi_{\ell}^i$. Here $H = \{ x \in (\mathbb{Z}/N\ell\mathbb{Z})^* \mid \varepsilon(x)x^{k-2-2i} \equiv 1 \mod \lambda \}$ and $\Gamma_H = \Gamma_H(N\ell)$.

**Proof** Let $v$ be a place dividing $\lambda$ of $\overline{\mathbb{Q}}$. By Proposition 2, there exist $i$ and $k'$ with $0 \leq i \leq \ell - 1$, $k' \leq \ell + 1$, a normalized eigenform $g \in S_k'(\Gamma_1(M_1), \varepsilon)$, and a prime $l$ of $K_g$ lying over $\ell$, such that $\rho_{f,\lambda}$ is isomorphic to $\rho_{g,1} \otimes \chi_{\ell}^{i}$. Then by (2.1) we have the equality in $\overline{\mathbb{F}}$:

$$\chi_{\ell}^{k-1} = \chi_{\ell}^{k'-1+2i}. \tag{4.1}$$

It follows from [6, Proposition 9.3] that there exist a normalized eigenform $g_2 \in S_2(\Gamma_1(N\ell), \psi)$ and a prime $l_2|\ell$, such that $\rho_{g,1}$ is isomorphic to $\rho_{g_2,l_2}$. Again by (2.1) we have the equality in $\overline{\mathbb{F}}$:

$$\overline{\psi} \chi_{\ell} = \overline{\varepsilon} \chi_{\ell}^{k'-1}, \tag{4.2}$$

where the bar denotes reduction modulo $v$. Therefore we have that $\rho_{f,\lambda}$ is isomorphic to $\rho_{g_2,l_2} \otimes \chi_{\ell}^{i}$ and it follows from (4.1) and (4.2) that

$$\overline{\psi} = \overline{\varepsilon} \chi_{\ell}^{k-2-2i}. \tag{4.3}$$

Let $\varepsilon_2$ be a Teichmüller lifting of $\overline{\psi}$ as in Definition 1. By Lemma 2, we have a normalized eigenform $f_2 \in S_2(\Gamma_1(N\ell), \varepsilon_2)$, and a prime $\lambda_2$ lying over $\ell$ in the field $K_{f_2}$, such that $\rho_{f_2,\lambda_2}$ is isomorphic to $\rho_{g_2,l_2}$, therefore, isomorphic to $\rho_{f,\lambda}$. 
Theorem 3 Let $\ell \geq 5$ be a prime number, $N > 0$ an integer prime to $\ell$, and $k > 2$. Let $f \in S_k(\Gamma_1(N), \psi)$ be a normalized eigenform and $\lambda$ be a prime of $K_f$ lying over $\ell$. Suppose the representation $\rho_{f, \lambda}$ is irreducible. Suppose we have a congruence subgroup $\Gamma$ with $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$ and a normalized eigenform $g_2 \in S_2(\Gamma)$ with $\rho_{f, \ell} \cong \rho_{g_2, \ell} \otimes \chi_\ell^i$ for some integer $i$ with $0 \leq i \leq \ell - 1$. Let $H = \{x \in (\mathbb{Z}/N \mathbb{Z})^* | \varepsilon(\lambda)x^{k-2-2i} \equiv 1 \mod N\}$ and $\Gamma_H = \Gamma_H(N \ell)$. Then we have $\Gamma \subseteq \Gamma_H$.

Moreover, there exists a normalized eigenform $f_2 \in S_2(\Gamma_H)$ such that $\rho_{f, \ell}$ is isomorphic to $\rho_{f_2, \ell} \otimes \chi_\ell^i$.

Proof Since $g_2 \in S_2(\Gamma)$ and $\Gamma_1(N \ell) \subseteq \Gamma$, the form $g_2$ can be naturally seen as a form on $\Gamma_1(N \ell)$ with a modulo $N \ell$ nebentypus character $\psi$.

Let $\varphi_{N \ell}$ denote the surjection:

$$\varphi_{N \ell} : \Gamma_0(N \ell) \twoheadrightarrow (\mathbb{Z}/N \ell \mathbb{Z})^*, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \mod N \ell.$$ 

For any $\gamma \in \Gamma \subseteq \Gamma_0(N \ell)$, we have that $g_2 = g_2|_{2 \gamma} = \psi(\varphi_{N \ell}(\gamma)) \cdot g_2$, which implies that $\varphi_{N \ell}(\gamma) \in \ker(\psi)$.

Since $\rho_{f, \ell} \cong \rho_{g_2, \ell} \otimes \chi_\ell^i$, by (2.1) we have the equality in $\mathbb{F}$:

$$\overline{\psi} = \varepsilon\chi_\ell^{k-2-2i}.$$ 

Note $H$ actually is the kernel of $\varepsilon\chi_\ell^{k-2-2i}$. It follows that $\varphi_{N \ell}(\gamma) \in \ker(\psi) \subseteq \ker(\overline{\psi}) = \ker(\varepsilon\chi_\ell^{k-2-2i}) = H$. By the definition of $\Gamma_H = \Gamma_H(N \ell)$, we have $\gamma \in \Gamma_H$, and therefore $\Gamma \subseteq \Gamma_H$.

Let $\varepsilon_2$ be a Teichmüller lifting of $\overline{\psi}$ as in Definition 1. By Lemma 2, we have a normalized eigenform $f_2 \in S_2(\Gamma_1(N \ell), \varepsilon_2)$ such that $\rho_{f_2, \ell}$ is isomorphic to $\rho_{g_2, \ell}$. Then we know that $\rho_{f, \ell}$ is isomorphic to $\rho_{f_2, \ell} \otimes \chi_\ell^i$ and it follows

$$\overline{\varepsilon_2} = \varepsilon_2\chi_\ell^{k-2-2i}.$$ 

(4.4)

Now we show $f_2 \in S_2(\Gamma_H)$. Since $\varepsilon_2$ is a Teichmüller lifting of $\overline{\psi}$, it follows from (4.4) that $\ker(\varepsilon_2) = \ker(\overline{\varepsilon_2}) = \ker(\varepsilon\chi_\ell^{k-2-2i}) = H$. Then for any $\gamma \in \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_H$, we have $\varphi_{N \ell}(\gamma) \in \ker(\psi)$ and thus $f_2|_{2 \gamma} = \varepsilon_2(\varphi_{N \ell}(\gamma)) \cdot f_2 = f_2$, which implies $f_2 \in S_2(\Gamma_H)$. □

\[ Springer \]
If the weight $k$ of $f$ is 2, we have the following results.

**Theorem 4** Let $\ell \geq 5$ be a prime number and $N > 0$ an integer prime to $\ell$. Let $f \in S_2(\Gamma_1(N), \varepsilon)$ be a normalized eigenform and $\lambda$ be a prime of $K_f$ lying over $\ell$. Suppose the modular Galois representation $\rho_{f, \lambda}$ is irreducible. Let $H = \ker(\bar{\varepsilon})$ be the kernel of the reduction of $\varepsilon$ modulo $\lambda$ and $\Gamma_H = \Gamma_H(N)$. Then there exists a normalized eigenform $f_2 \in S_2(\Gamma_H)$ such that $\rho_{f, \ell} \cong \rho_{f_2, \ell}$.

Moreover, the group $\Gamma_H$ is the largest possible congruence subgroup with $\Gamma_1(N) \subseteq \Gamma_H \subseteq \Gamma_0(N)$, on which such eigenform $f_2$ exists.

**Proof** We take a Teichmüller lifting of $\bar{\varepsilon}$, and the existence of $f_2$ follows from Lemma 2.

Let $g_2 \in S_2(\Gamma)$ be a normalized eigenform, such that $\rho_{f, \ell} \cong \rho_{g_2, \ell}$ for some congruence subgroup $\Gamma$ with $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$. We will show $\Gamma \subseteq \Gamma_H(N)$.

Let $\psi$ be the nebentypus character of $g_2$. Let $\varphi_N$ denote the surjection:

$$\varphi_N : \Gamma_0(N) \twoheadrightarrow (\mathbb{Z}/N\mathbb{Z})^*, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \text{ (mod } N).$$

For any $\gamma \in \Gamma$, we have that $g_2|_{\gamma} = \psi(\varphi_N(\gamma)) \cdot g_2$ and hence $\varphi_N(\gamma) \in \ker(\psi)$. Since $\rho_{f, \ell} \cong \rho_{g_2, \ell}$, by (2.1) we have $\bar{\psi} = \bar{\varepsilon}$. It follows that $\varphi_N(\gamma) \in \ker(\psi) \subseteq \ker(\bar{\varepsilon}) = H$. By the definition of $\Gamma_H(N)$, we have $\gamma \in \Gamma_H(N)$, and therefore $\Gamma \subseteq \Gamma_H(N)$. \qed

**Remark 1** It follows from [7, Theorem 1.2] that the eigenform $f_2$ as given in Theorem 2 and 4 can be replaced by a newform (normalized eigenform with primitive eigenvalues system) of weight 2 and level $M$ for some divisor $M$ of $N$.

### 4.3 An algorithm for computing the eigenforms of weight 2 associated to $\rho_{f, \ell}$

In this subsection, we give an algorithm for explicitly computing the weight 2 eigenform $f_2$ as given in Theorems 2 and 4.

First we note that in the proof of Theorem 2, the integer $i$ is determined by Proposition 2. Consequently, in the case with $\ell \geq k - 1$, Theorem 2 boils down to the following corollary.

**Corollary 1** Let $\ell \geq 5$ be a prime number, $N > 0$ an integer prime to $\ell$, and $k > 2$. Let $f \in S_k(\Gamma_1(N), \varepsilon)$ be a normalized eigenform and $\lambda$ be a prime of $K_f$ lying over $\ell$. Suppose the representation $\rho_{f, \lambda}$ is irreducible and $\ell \geq k - 1$. Then there exist a normalized eigenform $f_2 \in S_2(\Gamma_H)$ and a prime $\lambda_2$ lying over $\ell$ in the field $K_{f_2}$, such that $\rho_{f, \lambda}$ is isomorphic to $\rho_{f_2, \lambda_2}$. Here $H = \{ x \in (\mathbb{Z}/N\ell\mathbb{Z})^* | \varepsilon(x)x^{k-2} \equiv 1 \pmod{\lambda} \}$ and $\Gamma_H = \Gamma_H(N\ell)$.

Moreover, the group $\Gamma_H$ is the largest possible congruence subgroup with $\Gamma_1(N\ell) \subseteq \Gamma_H \subseteq \Gamma_0(N\ell)$, on which such eigenform $f_2$ exists.

**Proof** If $\ell \geq k - 1$, the integer $i$ in Proposition 2 can be taken to be 0. Therefore, in Theorem 2 we have $i = 0$ and $H = \{ x \in (\mathbb{Z}/N\ell\mathbb{Z})^* | \varepsilon(x)x^{k-2} \equiv 1 \pmod{\lambda} \}$. The last statement just follows from Theorem 3. \qed
Let $\ell \geq 5$ be a prime number, $N > 0$ an integer prime to $\ell$, and $k \geq 2$. Let $f \in S_k(\Gamma_1(N), \varepsilon)$ be a normalized eigenform and $\lambda$ be a prime of $K_f$ lying over $\ell$. Suppose the representation $\rho_{f,\lambda}$ is irreducible. Let $v$ be a place dividing $\lambda$ of $\mathbb{Q}$.

Now we can describe the algorithm.

If $k = 2$ or $\ell \geq k - 1$, by Theorem 4 and Corollary 1, we take $H = \ker(\bar{\varepsilon} \chi_k^{k-2})$ and it suffices to compute $f_2 \in S_2(H(N\ell))$ with $\rho_{f,\lambda} \cong \rho_{f_2,\lambda_2}$. This can be done by verifying

$$a_p(f) \equiv a_p(f_2) \mod v$$

for the first few primes $p$.

If $k > 2$ and $\ell < k - 1$, according to [5, Proposition 2.5.18] and [1, Theorem 3.5], one can explicitly compute $i, k'$ and $g$ as given in Proposition 2 and then obtain $f_2$ by verifying

$$a_p(f) \equiv p^i a_p(f_2) \mod v$$

for the first few primes $p$.

By the above discussions and Remark 1, we have

**Algorithm 5** Let $\ell \geq 5$ be a prime number, $N > 0$ an integer prime to $\ell$, and $k \geq 2$. Let $f \in S_k(\Gamma_1(N), \varepsilon)$ be a normalized eigenform and $\lambda$ be a prime of $K_f$ lying over $\ell$. Suppose the representation $\rho_{f,\lambda}$ is irreducible. Let $N' = N$ if $k = 2$ and $N' = N\ell$ if $k > 2$. This algorithm outputs an integer $i$ with $0 \leq i \leq \ell - 1$, a normalized eigenform $f_2 \in S_2(H(N\ell))$, and a prime $\lambda_2$ lying over $\ell$ in the field $K_{f_2}$, such that $\rho_{f,\lambda}$ is isomorphic to $\rho_{f_2,\lambda_2} \otimes \chi_k^i$. Here $H = \{ x \in (\mathbb{Z}/N'\mathbb{Z})^* \mid \varepsilon(x)x_k^{k-2} \equiv 1 \mod \lambda \}$ and $\Gamma_H = \Gamma_H(N')$.

1. Set $i \leftarrow 0$ if $k = 2$ or $\ell \geq k - 1$. Otherwise compute $i$ as given in Proposition 2.
2. Compute the set $S$ consisting of all the divisors of $N'$.
3. Take $M$ in $S$ and do:
   (a) Compute the group $H' = \{ x \pmod{M} \mid \gcd(x, N'\ell) = 1 \text{ with } 0 < x < N'\ell \}$ and $\varepsilon(x)x_k^{k-2} \equiv 1 \mod \lambda$).
   (b) Compute the congruence subgroup $\Gamma_H'(M)$
   (c) Compute $B = \frac{[S_L(\mathbb{Z});\Gamma_1(M)]^2}{12} \cdot (\ell^2 - 1 + k)$ and $a_p(f)$ for all primes $p$ with $p \leq B$.
   (d) Compute all newforms $F$ in $S_2(\Gamma_H'(M))$ using modular symbols.
   (e) For each $f_2$ in $F$, do:
      (i) Compute $p^i a_p(f_2)$ for all primes $p$ with $p \leq B$ and compute the primes $P$ of the composed field $K_f K_{f_2}$ lying over $\ell$.
      (ii) If there is a prime $l \in P$ such that $a_p(f) \equiv p^i a_p(f_2) \mod l$ for all primes $p$ with $p \leq B$, put $\lambda_2 = l \cap K_{f_2}$ and then output $i$, $f_2$, $\lambda_2$, and terminate.
   (f) Set $S \leftarrow S - \{ M \}$ and go to step 3.
5 Realizing modular Galois representations in the Jacobians of minimal dimensions

In this section, we describe the method to find the Jacobians of modular curves that can be used to realize the modular Galois representations and have the smallest possible dimensions in the sense that the associated congruence subgroups are largest as shown in Theorem 3 and 4.

Let $N > 0$ and $k \geq 2$ be integers. Let $f \in S_k(\Gamma_1(N), \varepsilon)$ be a normalized eigenform. Let $\ell \geq 5$ be a prime number with $\ell \nmid N$ and $\lambda$ be a prime of $K_f$ lying over $\ell$. Let $N' = N$ if $k = 2$ and $N' = N\ell$ if $k > 2$. Let $H = \{ x \in (\mathbb{Z}/N'\mathbb{Z})^* \mid \varepsilon(x)\lambda^{k-2-2i} \equiv 1 \text{ mod } \lambda \}$ and $\Gamma_H = \Gamma_H(N')$. If the representation $\rho_{f, \lambda}$ is irreducible, Algorithm 5 gives an integer $i$ with $0 \leq i \leq \ell - 1$, a normalized eigenform $f_2 \in S_2(\Gamma_H, \varepsilon_2)$, and a prime $\lambda_2$ lying over $\ell$ in the field $K_{f_2}$, such that $\rho_{f, \lambda}$ is isomorphic to $\rho_{f_2, \lambda_2} \otimes \chi_\ell^i$.

Let $X_{\Gamma_H}$ be the modular curve of the subgroup $\Gamma_H$ and $J_{\Gamma_H}$ its Jacobian. Let $\mathbb{T}_{\Gamma_H}$ be the Hecke algebra of weight 2 for $\Gamma_H$ and let $\mathcal{I}_{f_2}$ be the ring homomorphism

$$\mathcal{I}_{f_2} : \mathbb{T}_{\Gamma_H} \to \overline{\mathbb{F}}_\lambda, \quad (d) \mapsto \varepsilon_2(d), \quad T_n \mapsto a_n(f_2) \mod \lambda_2.$$ 

Let $m_{f_2}$ denote the kernel of $\mathcal{I}_{f_2}$ and we put

$$V_{f_2} = J_{\Gamma_H}[m_{f_2}] = \{ x \in J_{\Gamma_H} \mid tx = 0 \text{ for all } t \text{ in } m_{f_2} \}.$$ 

Then by the arguments of [8, Sects. 3.2 and 3.3] we know that $V_{f_2}$ is a non-zero finite direct sum of copies of $\rho_{f_2, \lambda_2}$.

Therefore, to compute modular Galois representation $\rho_{f, \lambda}$, it suffices to compute the representation $\rho_{V_{f_2}} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \to Aut_{\mathbb{T}_{\Gamma_H}/m_{f_2}}(V_{f_2})$. Moreover we have

**Theorem 6** The torsion space $V_{f_2}$ is a subspace of $J_{\Gamma_H}[\ell]$. Therefore, the representation $\rho_{V_{f_2}}$ is a subrepresentation of $J_{\Gamma_H}[\ell]$.

**Proof** Since $m_{f_2}$ is the kernel of $\mathcal{I}_{f_2}$, it implies that $V_{f_2} = J_{\Gamma_H}[m_{f_2}] \subseteq J_{\Gamma_H}[\ell]$. □

By the argument at the end of Sect. 2, we know that the calculations can be largely decreased if we can realize the modular Galois representation $\rho_{V_{f_2}}$ in a Jacobian which has a smaller dimension. Theorem 6 allows us to work with $J_{\Gamma_H}$ instead of $J_1(N')$ to compute $\rho_{V_{f_2}}$. Since the dimension of $J_{\Gamma_H}$ is the same as the dimension of the $\mathbb{C}$-vector space $S_2(\Gamma_H)$, it follows from Theorem 3 and 4 that the Jacobian $J_{\Gamma_H}$ produced by our method has the smallest possible dimension, in the sense that $\Gamma_H$ is the largest possible congruence subgroup with $\Gamma_1(N') \subseteq \Gamma_H \subseteq \Gamma_0(N')$ associated to the representation $\rho_{f, \lambda}$.

At the end of this section, we give examples to demonstrate our results. In Tables 1, 2, 3, 4 and 5, we take newforms $f \in S_{12}(\Gamma_1(N))$, and output the associated eigenforms $f_2$ produced by our algorithm in the cases of $\ell$ up to 13 and $N$ up to 6. We also list the dimensions of $J_1(N')$ and $J_{\Gamma_H}$, which are denoted by $d_1$ and $d_H$, respectively.
In Sect. 4, we show the maximality of the congruence subgroup $\Gamma H$ with $\Gamma_1(N\ell) \subseteq \Gamma_H \subseteq \Gamma_0(N\ell)$. It is natural for us to consider when $\Gamma_H = \Gamma_0(N\ell)$ may happen. In this section, as applications of our previous results, we discuss the cases with $\Gamma_H = \Gamma_0(N\ell)$.

Now let $\phi(n)$ be the Euler totient function. We first show the following lemma.

Lemma 3 Let $k \geq 0$ and $m > 0$ be integers, and $\ell$ a prime factor of $m$. Then the kernel of the homomorphism

$$
\vartheta : (\mathbb{Z}/m\mathbb{Z})^* \mapsto (\mathbb{Z}/\ell\mathbb{Z})^*, \quad x \mod m \mapsto x^k \mod \ell
$$

has order $\frac{\phi(m) \cdot \gcd(\ell-1,k)}{\ell-1}$.

Proof Since $\ell$ is a prime factor of $m$, the homomorphism $\vartheta$ factors as:

$$
\begin{array}{ccc}
(\mathbb{Z}/m\mathbb{Z})^* & \xrightarrow{\alpha} & (\mathbb{Z}/\ell\mathbb{Z})^* \\
\downarrow \vartheta & & \downarrow \beta \\
(\mathbb{Z}/\ell\mathbb{Z})^* & &
\end{array}
$$

6 Reduction to the cases of eigenforms on $\Gamma_0$
Table 4  \( N = 5 \),  
\( f = q + a \cdot q^2 + \left( -\frac{1}{12} a^3 - \frac{725}{28} a \right) \cdot q^3 + O(q^4) \) and  
\( K_f \) is the number field defined by  
\( x^4 + 4132x^2 + 2496256 \)

| \( \ell \) | \( \lambda \) | \( \lambda_2 \) | \( i \) | \( f_2 \) | \( K_{f_2} \) | \( d_1 \) | \( d_H \) |
|---|---|---|---|---|---|---|---|
| 7 | \((7, \frac{1}{60} a^2 + \frac{494}{15})\) | \((7, -\frac{a^3}{4} + (-\frac{a^2}{120} - \frac{217}{15}) \cdot a^2 + \frac{5a^4}{4} - \frac{a^2}{60} - \frac{524}{15})\) | 0 |  
\(+ q + a \cdot q^2 + (a^3 - a) \cdot q^3 + O(q^4)\)  
\(+ x^4 - x^2 + 1\) | 25 | 13 |
| 11 | \((11, \frac{1}{60} a^2 + \frac{434}{15})\) | \((11, (\frac{a^3}{120} - \frac{a^2}{120} - \frac{1711a}{1220}) \cdot a^3 + (\frac{1033}{60} \cdot a^3 + (-\frac{a^2}{440} + \frac{599}{110}) \cdot a^2 + (\frac{5a^4}{6} - \frac{a^2}{4} - \frac{27037a}{12320}) \cdot a + \frac{a^2}{2240} + \frac{a^2}{220} + \frac{1369}{560} + \frac{373}{110})\) | 0 |  
\(+ q + a \cdot q^2 + (\frac{1}{2} a^3 - \frac{7}{2} a) \cdot q^3 + O(q^4)\)  
\(+ x^4 + 7x^2 + 4\) | 81 | 9 |
| 13 | \((13, -\frac{1}{360} a^3 + \frac{1048}{15})\) | \((13, (\frac{a^3}{26880} + \frac{10517a}{1220}) \cdot a^3 + (\frac{13}{5040} \cdot a^3 + \frac{20517a}{1220} - \frac{20}{7} \cdot a^5 + \frac{241a^3}{20160} + \frac{199823a}{5040} - \frac{24}{7} \cdot a^3 + \frac{403a^3}{80640} + \frac{258707a}{20160} - \frac{355}{24}) \cdot a^2 + (\frac{403a^3}{80640} + \frac{258707a}{20160} - \frac{355}{24}) \cdot a + \frac{a^2}{12} + \frac{5a^4}{4} - \frac{406}{3})\) | 0 |  
\(+ q + a \cdot q^2 + (-\frac{13}{24} a^3 - \frac{38}{3} a^3 - \frac{11}{8} a) \cdot q^3 + O(q^4)\)  
\(+ x^8 + 5x^6 + 24x^4 + 5x^2 + 1\) | 121 | 25 |
Table 5 \( N = 6 \), \( f = q - 32q^2 - 243q^3 + O(q^4) \) and \( K_f = \mathbb{Q} \)

| \( \ell \) | \( \lambda \) | \( \lambda_2 \) | \( i \) | \( f_2 \) | \( K_{f_2} \) | \( d_1 \) | \( d_H \) |
|---|---|---|---|---|---|---|---|
| 5 | (5) | \( (2\alpha + 1) \) | 0 | \( q + \alpha \cdot q^2 - \alpha \cdot q^3 + O(q^4) \) | \( x^2 + 1 \) | 9 | 5 |
| 7 | (7) | \( (3\alpha - 2) \) | 4 | \( q + \alpha \cdot q^2 + (\alpha - 1) \cdot q^3 + O(q^4) \) | \( x^2 - x + 1 \) | 25 | 13 |
| 11 | (11) | (11) | 0 | \( q + q^2 - q^3 + O(q^4) \) | \( \mathbb{Q} \) | 81 | 9 |
| 13 | (13) | \( (-\alpha^3 - \alpha - 1) \) | 0 | \( q + \alpha \cdot q^2 + (1 - \alpha^2) \cdot q^3 + O(q^4) \) | \( x^4 - x^2 + 1 \) | 121 | 61 |

where \( \alpha \) is the canonical homomorphism

\[
(\mathbb{Z}/m\mathbb{Z})^* \to (\mathbb{Z}/\ell\mathbb{Z})^*, \quad x \mod m \mapsto x \mod \ell,
\]

and \( \beta \) is the homomorphism

\[
(\mathbb{Z}/\ell\mathbb{Z})^* \to (\mathbb{Z}/\ell\mathbb{Z})^*, \quad x \mod \ell \mapsto x^k \mod \ell.
\]

Since \( \alpha \) is surjective, the image \( \text{Im}(\alpha) \) of \( \beta \) is the same as the image \( \text{Im}(\beta) \) of \( \beta \). Let \( g \) be a generator of the cyclic group \( (\mathbb{Z}/m\mathbb{Z})^* \) and then we know it has order \( \ell - 1 \). It follows that \( \text{Im}(\beta) = \langle g^k \rangle \) has order \( \frac{\ell - 1}{\gcd(\ell - 1, k)} \), which implies that the order of \( \text{Im}(\alpha) \) is also equal to \( \frac{\ell - 1}{\gcd(\ell - 1, k)} \).

Since \( (\mathbb{Z}/m\mathbb{Z})^*/\ker(\alpha) \cong \text{Im}(\alpha) \) and \( (\mathbb{Z}/m\mathbb{Z})^* \) has order \( \phi(m) \), it follows that the kernel of \( \alpha \) has order \( \frac{\phi(m) \cdot \gcd(\ell - 1, k)}{\ell - 1} \).

**Theorem 7** Let \( \ell \geq 5 \) be a prime number, \( N > 0 \) an integer prime to \( \ell \), and \( k > 2 \). Let \( f \in S_k(\Gamma_0(N)) \) be a normalized eigenform and \( \lambda \) be a prime of \( K_f \) lying over \( \ell \). Suppose the representation \( \rho_{f, \lambda} \) is irreducible. Let \( i \) be the integer with \( 0 \leq i \leq \ell - 1 \) and \( \Gamma_H \) be the congruence subgroup as given in Theorem 2. Then the index \( [\Gamma_H : \Gamma_1(N\ell)] \) of \( \Gamma_1(N\ell) \) in \( \Gamma_H \) is \( \phi(N) \cdot \gcd(\ell - 1, k - 2 - 2i) \).

**Proof** By Theorem 2, there exists a normalized eigenform \( f_2 \in S_2(\Gamma_H, \varepsilon_2) \), such that \( \rho_{f_2, \ell} \otimes \chi_\ell^i \). Here \( H = \{ x \in (\mathbb{Z}/N\ell\mathbb{Z})^* | \varepsilon(x) x^{k-2-2i} \equiv 1 \mod \lambda \} \) and \( \Gamma_H = \Gamma_H(\mathbb{N}). \)

Since the nebentypus character of \( f \in S_k(\Gamma_0(N)) \) is trivial, it follows that \( H = \{ x \in (\mathbb{Z}/N\ell\mathbb{Z})^* | x^{k-2-2i} \equiv 1 \mod \ell \} \). Let \( \vartheta \) be the homomorphism:

\[
\vartheta : (\mathbb{Z}/N\ell\mathbb{Z})^* \to (\mathbb{Z}/\ell\mathbb{Z})^*, \quad x \mod (N\ell) \mapsto x^{k-2-2i} \mod \ell.
\]

Then it is evident that \( H = \ker(\vartheta) \). It follows from Lemma 3 and \( \gcd(N, \ell) = 1 \) that

\[
\#H = \frac{\phi(N) \cdot \gcd(\ell - 1, k - 2 - 2i)}{\ell - 1} = \phi(N) \cdot \gcd(\ell - 1, k - 2 - 2i).
\]

Let \( \varphi_{N\ell} \) denote the surjective homomorphism:

\[
\varphi_{N\ell} : \Gamma_0(N\ell) \to (\mathbb{Z}/N\ell\mathbb{Z})^*, \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \mod (N\ell).
\]
Then $\Gamma_1(N\ell)$ is the kernel of $\varphi_{N\ell}$ and $\Gamma_H$ is the preimage $\varphi_{N\ell}^{-1}(H)$ of $H$ under $\varphi_{N\ell}$. It follows that $\Gamma_H/\Gamma_1(N\ell) \cong H$, and hence, the index $[\Gamma_H : \Gamma_1(N\ell)] = \#(\Gamma_H/\Gamma_1(N\ell)) = \#H = \phi(N) \cdot \gcd(\ell - 1, k - 2 - 2i).$ \hfill \Box

**Remark 2** It is easy to see that the main theorem (Proposition 4.1) of [10] is a special case of Theorem 7 with $N = 1$ and $\ell \geq k - 1$.

**Remark 3** By Theorem 7, if $f \in S_k(\Gamma_0(N))$, the computations of $H'$ in Algorithm 5 can be reduced. To be precise, the Step (a) in Step 3 of Algorithm 5 can be replaced by

(a') Compute $t = \frac{N' - 1}{\phi(N) \cdot \gcd(\ell - 1, k - 2 - 2i)}$ and the group $H' = \{x^t \pmod{M} | \gcd(x, N'\ell) = 1 \text{ with } 0 < x < N'\ell\}$.

If $f$ is an eigenform on $\Gamma_0(N)$, Theorem 7 implies the following corollary, which shows when the group $\Gamma_H$ equals $\Gamma_0(N\ell)$.

**Corollary 2** Let $\ell \geq 5$ be a prime number, $N > 0$ an integer prime to $\ell$, and $k > 2$. Let $f \in S_k(\Gamma_0(N))$ be a normalized eigenform. Suppose the representation $\rho_{f,\ell}$ is irreducible. Let $i$ be the integer with $0 \leq i \leq \ell - 1$ and $\Gamma_H$ be the congruence subgroup as given in Theorem 2. Then $\Gamma_H = \Gamma_0(N\ell)$ if and only if $\ell - 1|k - 2 - 2i$.

**Proof** It follows from Theorem 7 that $[\Gamma_H : \Gamma_1(N\ell)] = \phi(N) \cdot \gcd(\ell - 1, k - 2 - 2i)$. Then $\Gamma_H = \Gamma_0(N\ell)$ if and only if $[\Gamma_H : \Gamma_1(N\ell)] = [\Gamma_0(N\ell) : \Gamma_1(N\ell)] = \phi(N\ell) = \phi(N) \cdot (\ell - 1)$, and hence if and only if $k - 2 - 2i$ is divisible by $\ell - 1$. \hfill \Box

If we suppose $\ell \geq k - 1$, the integer $i$ as given in Corollary 2 can be taken to be 0, and hence $\Gamma_H = \Gamma_0(N\ell)$ if and only $\ell = k - 1$. Thus we can show

**Corollary 3** Let $\ell \geq 5$ be a prime number, $N > 0$ an integer prime to $\ell$, and $k > 2$. Let $f \in S_k(\Gamma_0(N))$ be a normalized eigenform. Suppose $\ell \geq k - 1$ and the representation $\rho_{f,\ell}$ is irreducible. Then there exists a normalized eigenform $f_2 \in S_2(\Gamma_0(N\ell))$ with $\rho_{f,\ell} \cong \rho_{f_2,\ell}$ if and only if $\ell = k - 1$.

**Proof** Let $\Gamma_H$ be the congruence subgroup as given in Corollary 1. By the maximality of $\Gamma_H$ and $\Gamma_H \subseteq \Gamma_0(N\ell)$, we know that a normalized eigenform $f_2 \in S_2(\Gamma_0(N\ell))$ with $\rho_{f,\ell} \cong \rho_{f_2,\ell}$ exists if and only if $\Gamma_H = \Gamma_0(N\ell)$. This corollary immediately follows from Corollary 2 since we can take $i$ to be 0 in this case. \hfill \Box

For an eigenform $f \in S_k(\Gamma_1(N))$, let $i$ be the integer with $0 \leq i \leq \ell - 1$ and $\Gamma_H$ be the congruence subgroup as given in Theorem 2. Suppose $\gcd(\ell, \phi(N)) = 1$ and $\ell - 1|k - 2 - 2i$. Then we can show that the condition $\Gamma_H = \Gamma_0(N\ell)$ conversely implies that $f$ is an eigenform on $\Gamma_0(N)$. In fact, in the following theorem, we will show that the form $f_2$ as given in Theorem 2 is a form on $\Gamma_0(N\ell)$ if and only if $f$ is a form on $\Gamma_0(N)$.

**Theorem 8** Let $\ell \geq 5$ be a prime number, $N > 0$ an integer prime to $\ell$, and $k > 2$. Let $f \in S_k(\Gamma_1(N))$ be a normalized eigenform. Suppose the representation $\rho_{f,\ell}$ is irreducible. Let $i$ be the integer with $0 \leq i \leq \ell - 1$ and $\Gamma_H$ be the congruence subgroup as given in Theorem 2. Suppose $\ell \nmid \phi(N)$ and $\ell - 1|k - 2 - 2i$. Then $\Gamma_H = \Gamma_0(N\ell)$ if and only if $f \in S_k(\Gamma_0(N))$. \hfill \Box
The sufficiency follows from the sufficiency of Corollary 2. Now we prove the necessity.

By Theorem 2, there exists a normalized eigenform \( f_2 \in S_2(\Gamma_H, \varepsilon_2) \), such that \( \rho_{f, \ell} \) is isomorphic to \( \rho_{f_2, \ell} \otimes \chi^i_\ell \). Let \( \varepsilon \) be the nebentypus character of \( f \). Then we have

\[
\bar{\varepsilon}_2 \equiv \bar{\varepsilon}_{\text{ind}} \cdot \chi^k_\ell - 2 - 2i \quad \text{mod } v, \tag{6.1}
\]

where \( \varepsilon_{\text{ind}} \) is the mod \( N\ell \) character induced by \( \varepsilon \).

Suppose \( \Gamma_H = \Gamma_0(N\ell) \) and then \( \varepsilon_2 \) is a trivial character. Note \( \ell - 1 | k - 2 - 2i \), and it implies that the congruence (6.1) reduces to

\[
\bar{\varepsilon}_{\text{ind}} \equiv 1 \quad \text{mod } v.
\]

By (3.1), we have \( \varepsilon_{\text{ind}} = \varepsilon \circ \pi_{N\ell, N} \). Since \( \pi_{N\ell, N} \) is surjective, we therefore have

\[
\bar{\varepsilon} \equiv 1 \quad \text{mod } v.
\]

Since \( \varepsilon \) is a Dirichlet character of \( (\mathbb{Z}/N\mathbb{Z})^\ast \), each element of its image is a \( \phi(N) \)-th root of unity. It follows from \( \ell \nmid \phi(N) \) and Lemma 1 that the image of \( \varepsilon \) does not contain any other \( \phi(N) \)-th root of unity except 1. Hence \( \varepsilon \) is the trivial character and this shows \( f \in S_k(\Gamma_0(N)) \).

If we suppose \( \ell \geq k - 1 \), the integer \( i \) can be taken to be 0 and then Theorem 8 is reduced to the following corollary.

**Corollary 4** Let \( \ell \geq 5 \) be a prime number and \( N > 0 \) an integer prime to \( \ell \). Let \( f \in S_{\ell+1}(\Gamma_1(N)) \) be a normalized eigenform. Suppose \( \ell \nmid \phi(N) \) and the representation \( \rho_{f, \ell} \) is irreducible. Then there exists a normalized eigenform \( f_2 \in S_2(\Gamma_0(N\ell)) \) with \( \rho_{f, \ell} \cong \rho_{f_2, \ell} \) if and only if \( f \in S_{\ell+1}(\Gamma_0(N)) \).

**Proof** Let \( k = \ell + 1 \) denote the weight of \( f \). Then we have \( \ell \geq k - 1 \) and \( \ell - 1 | k - 2 \). Let \( \Gamma_H \) be the congruence subgroup as given in Corollary 1. Then by the proof of Corollary 3, we know that a normalized eigenform \( f_2 \in S_2(\Gamma_0(N\ell)) \) with \( \rho_{f, \ell} \cong \rho_{f_2, \ell} \) exists if and only if \( \Gamma_H = \Gamma_0(N\ell) \). This corollary immediately follows from Theorem 8 since we can take \( i \) to be 0 in this case.

**Acknowledgements** Our deepest gratitude goes to the anonymous reviewers for their careful work and thoughtful suggestions that have helped improve this paper substantially.

**References**

1. Bruin, P.: Modular Curves, Arakelov Theory, Algorithmic Applications. Ph.D. thesis, Universiteit Leiden (2010)
2. Carayol, H.: Sur les représentations Galoisiennes modulo \( \ell \) attachées aux formes modulaires. Duke Math. J. 59, 785–801 (1989)
3. Deligne, P.: Formes modulaires et représentations \( \ell \)-adiques. Lecture Notes in Mathematics, vol. 179, pp. 139–172. Springer, Berlin (1971)
4. Edixhoven, S.J.: The weight in Serre’s conjectures on modular forms. Invent. Math. 109(3), 563–594 (1992)
5. Edixhoven, S.J., Couveignes, J.-M. et. al.: Computational Aspects of Modular Forms and Galois Representations. Annals of Mathematics Studies, vol. 176. Princeton University Press, Princeton (2011)
6. Gross, B.H.: A tameness criterion for Galois representations associated to modular forms (mod $p$). Duke Math. J. 61, 445–517 (1990)
7. Ribet, K.A.: Galois representations attached to eigenforms with nebentypus. In: Serre, J.-P., Zagier, D.B. (eds.) Modular Functions of One Variable, V (Proceedings of Second International Conference, University of Bonn, Bonn, 1976), pp. 18–52. Springer, Berlin (1977)
8. Ribet, K.A., Stein, W.A.: Lectures on Serre’s Conjectures. Arithmetic Algebraic Geometry (Park City, UT, 1999), pp. 143–232. American Mathematical Society, Providence (2001)
9. Stein, W.A.: Modular Forms, A Computational Approach. Graduate Studies in Mathematics, vol. 79. American Mathematical Society, Providence (2007)
10. Tian, P.: Computations of Galois representations associated to modular forms of level one. Acta Arith. 164, 399–412 (2014)

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.