ACTA ARITHMETICA
164.4 (2014)

Computations of Galois representations associated to modular forms of level one

by

Peng Tian (Nanjing and Roma)

1. Introduction. In 1995, René Schoof asked Bas Edixhoven whether given a prime number p, one can compute Ramanujan's tau function $\tau(p)$ defined by

$$\Delta(z) = q\prod_{n\geq 1}(1-q^n)^{24} = \sum_n \tau(n)q^n$$

in time polynomial in $\log p$.

In the book [9], S. J. Edixhoven, J.-M. Couveignes, R. S. de Jong and F. Merkl give an affirmative answer. They generalize Schoof's algorithm [17] and show that

- *There exists a deterministic algorithm that on input a prime number p computes $\tau(p)$ in time polynomial in* $\log p$.

Ramanujan observed the remarkable property of $\tau(p)$:

$$|\tau(p)| \leq 2p^{11/2} \quad \text{for prime } p,$$

which was proved by P. Deligne. In fact, Deligne [6] shows that there exists a continuous semisimple representation

$$\rho_{\Delta,\ell} : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell).$$

This representation is unique up to isomorphism and it has the property that for primes p not dividing $N\ell$ one has

$$\tau(p) \equiv \mathrm{tr}(\rho_{\Delta,\ell}(\mathrm{Frob}_p)) \bmod \ell.$$

In [9], Edixhoven and Couveignes give a polynomial time algorithm to compute the modular Galois representation and thus the value modulo ℓ of Ramanujan's tau function at p. Combining this with the property $|\tau(p)| \leq 2p^{11/2}$ for primes p and the Chinese remainder theorem one can

2010 *Mathematics Subject Classification*: 11-04, 11Fxx, 11G30, 11Y40.
Key words and phrases: modular Galois representations, modular forms, modular curves, Jacobian, Ramanujan's tau function, polynomials.

DOI: 10.4064/aa164-4-5

compute $\tau(p)$. It is well known that the representation appears in the group of ℓ-torsion points of the Jacobian variety of the modular curve $X_1(\ell)$. If the genus g of $X_1(\ell)$ is equal to 1, the question boils down to the case of an elliptic curve, which has been solved by Schoof's algorithm.

Since the Galois representation $\rho_{\Delta,\ell}$ is 2-dimensional, the fixed field of $\ker(\rho_{\Delta,\ell})$ can be described as the splitting field of a certain polynomial $P_{\Delta,\ell} \in \mathbb{Q}[x]$ of degree ℓ^2-1. Moreover, the associated projective representation can be described as the splitting field of a certain polynomial $\tilde{P}_{\Delta,l} \in \mathbb{Q}[x]$ of degree $\ell+1$.

In general, all the discussion above holds for modular forms with level 1.

Unfortunately the algorithm described in [9] is difficult to implement. J. Bosman [2] used this algorithm to approximately evaluate $\tilde{P}_{f,\ell}$ of mod ℓ Galois representations associated to modular forms f of level 1 and of weight $k \le 22$, with $\ell \le 23$. But since the required precision in the calculations grows quite rapidly with ℓ, Bosman did not compute more cases.

In this paper we present an improvement in case $\gcd(k-2, l+1) > 2$. In these cases there is a modular curve X_Γ with $\Gamma_1(\ell) \lneq \Gamma \le \Gamma_0(\ell)$ with the property that the 2-dimensional Galois representation is a subrepresentation of the ℓ-torsion points of the Jacobian of X_Γ. Therefore we can do the computations with the Jacobian of X_Γ rather than of $X_1(\ell)$ that Bosman used. Since the genus of X_Γ is smaller than that of $X_1(\ell)$, the required precision is smaller and the computation is more efficient. This allows us to deal with cases that were inaccessible by Bosman's original algorithm.

As an example, we compute the mod 31 Galois representation associated to the discriminant modular form Δ. For $\ell = 29$ and 31, we also compute the mod ℓ Galois representation associated to the unique normalized cusp forms of level 1 and weights 16, 20 and 22. The correctness of each $\tilde{P}_{f,l}$ is then verified by an application of Serre's conjecture, proved by Khare–Wintenberger [11].

We compute the values modulo 31 of Ramanujan's τ function at some huge primes up to a sign. As a consequence we can verify Lehmer's conjecture up to a large bound. More precisely, we show that

$$\tau(n) \neq 0 \qquad \text{for all } n < 98214982176619929599 9.$$

This improves Bosman's bound by a factor of approximately 43.

2. Outline of the algorithm. Let N be a positive integer. The congruence subgroup $\Gamma_1(N)$ of level N is

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \;\middle|\; c \equiv 0 \bmod N,\ a \equiv b \equiv 1 \bmod N \right\}.$$

Let $k \geq 2$ be an integer. Let $f = \sum_{n>0} a_n(f)q^n \in S_k(\Gamma_1(N)$ be a newform of weight k and level N. Let ε be its nebentypus character. Let K_f be the number field which is obtained by adjoining all coefficients a_n of the q-expansion f to $\mathbb{Q}$. Let ℓ be a prime number. Let λ be a prime of K_f lying over ℓ. Denote by $K_{f,\lambda}$ the completion of K_f at the prime λ. Then thanks to Deligne, we know that there exists an irreducible representation associated to f,

$$\rho_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathrm{GL}_2(K_{f,\lambda}),$$

that is unramified outside $N\ell$. Furthermore, for all primes $p \nmid N\ell$, the characteristic polynomial of the representation at the Frobenius element Frob_p is $x^2 - a_p(f)x + \varepsilon(p)p$. It is possible to reduce the representation modulo λ. We have the following well known theorem:

THEOREM 2.1. *$f \in S_k(N, \varepsilon)$ be a newform. Let λ be as above and let $\mathbb{F}_\lambda$ denote the residue field of λ. Then there exists a continuous semisimple representation*

$$\rho_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\lambda)$$

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

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

Moreover, $\rho_{f,\lambda}$ is unique up to isomorphism.

The discriminant modular form is given by

$$\Delta(z) = q\prod_{n\geq 1}(1-q^n)^{24} = \sum_n \tau(n)q^n,$$

and its Fourier coefficients define the Ramanujan's tau function $\tau(n)$.

In the book [9], S. Edixhoven and J.-M. Couveignes generalize Schoof's algorithm [17] and show that

- *There exists a deterministic algorithm that computes the* $\bmod \ell$ *Galois representation associated to level one modular forms in time polynomial in ℓ.*

Since we have the congruence relation

$$\tau(p) \equiv \mathrm{tr}(\rho_{\Delta,\ell}(\mathrm{Frob}_p)) \bmod \ell,$$

this algorithm can be used to compute $\tau(p) \bmod \ell$ in time polynomial in $\log p$ and ℓ.

Fix a prime number ℓ and let λ be a prime lying over ℓ. The residue field of the ring of integers of $\overline{\mathbb{Q}}_\ell$ is isomorphic to $\overline{\mathbb{F}}_\ell$. And then since $\mathbb{F}_\lambda \subset \overline{\mathbb{F}}_\ell$, we can view our representation $\rho_{f,\lambda}$ as taking values in $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$. In [14, Theorem 2.2], the author shows that if $2 < k \leq \ell + 1$ and $\rho_{f,\lambda}$ is irreducible, then there is a newform $f_2 \in S_2(\Gamma_1(N\ell))$, together with a prime λ_2

lying over ℓ of the coefficient field K_{f_2}, such that ρ_{f_2,λ_2} is isomorphic to $\rho_{f,\lambda}$. Therefore, for any $p \nmid N\ell$, the matrices $\rho_{f,\lambda}(\mathrm{Frob}_p)$ and $\rho_{f_2,\lambda_2}(\mathrm{Frob}_p)$ have the same characteristic polynomial in $\overline{\mathbb{F}}[x]$. This allows Edixhoven and Couveignes to reduce the questions to the weight 2 cases.

Now we suppose that $\rho_{f,\lambda}$ is a mod ℓ Galois representation associated to a newform $f \in S_2(\Gamma_1(\ell))$ with character ε. Let $X_1(\ell)$ be the modular curve associated to $\Gamma_1(\ell)$ and $J_1(\ell)$ denote its Jacobian. Denoting by $\mathbb{T}$ the Hecke algebra generated by the diamond and Hecke operators over $\mathbb{Z}$, i.e. $\mathbb{T} = \mathbb{Z}[T_n, \langle n\rangle : n \in \mathbb{Z}_+ \text{ and } (n,\ell) = 1]$, we have $\mathbb{T} \subset \mathrm{End}\, J_1(\ell)$ and there is a ring homomorphism $\theta : \mathbb{T} \to \mathbb{F}_\lambda$, given by $\langle d\rangle \mapsto \varepsilon(d)$ and $T_n \mapsto a_n(f)$. Let $\mathfrak{m}$ denote the kernel of θ and put

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

This is a 2-dimensional $\mathbb{T}/\mathfrak{m}$-linear subspace of $J_1(\ell)(\overline{\mathbb{Q}})[\ell]$, and the semisimplification of the representation

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

is isomorphic to $\rho_{f,\lambda}$ (see [15, Sections 3.2 and 3.3]).

If $\#\,\mathbb{T}/\mathfrak{m} = \ell$, then the fixed field of $\rho_{f,\lambda}$ is naturally the splitting field of a suitable polynomial $P_{f,\lambda} \in \mathbb{Q}[X]$ of degree $\ell^2 - 1$. More precisely, we can take

$$P_{f,\lambda}(x) = \prod_{P \in V_\lambda - \{0\}} (x - h(P)) \tag{2.2}$$

for some suitable function h in the function field of $X_1(\ell)$. Here $h(P)$ has the following meaning. If g is the genus of $X_1(\ell)$, then we can write each divisor $P \in V_\lambda - \{0\}$ as $\sum_{i=1}^{g}(P_i) - gO)$ for certain points P_i on $X_1(\ell)$. We put $h(P) = \sum_{i=1}^{g} h(P_i)$.

Composed with the canonical projection map $\mathrm{GL}_2(\mathbb{F}_\lambda) \to \mathrm{PGL}_2(\mathbb{F}_\lambda)$, the representation $\rho_{f,\lambda}$ gives a projective representation $\tilde{\rho}_{f,\lambda} : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\lambda)$.

Since the projective line $\mathbb{P}(V_\lambda)$ has $\ell + 1$ points, the fixed field of $\tilde{\rho}_{f,\lambda}$ is naturally the splitting field of a suitable polynomial $\tilde{P}_{f,\lambda} \in Q[X]$ of degree $\ell + 1$. More precisely, we can take

$$\tilde{P}_{f,\lambda}(x) = \prod_{L \subset \mathbb{P}(V_\lambda)} \Big(x - \sum_{P \in L - \{0\}} h(P)\Big). \tag{2.3}$$

J. Bosman first uses a complex approximation approach to compute the points in V_ℓ over $\mathbb{C}$ and then from these computed points evaluates approximately $\tilde{P}_{f,\ell}$. In the end, he explicitly computes mod ℓ Galois projective representations associated to modular forms of level 1 and weight up to 22, with $\ell \leq 23$. For details, we refer to [3, Chapter 2].

3. Galois theory of modular curves. Let ℓ be a prime number and Γ be a congruence subgroup of level ℓ. Let $\mathfrak{h}$ denote the upper half-plane and $X_\Gamma = (\Gamma\backslash\mathfrak{h}) \cup (\Gamma\backslash(\mathbb{Q}\cup\infty))$ be the modular curve for Γ. The function field of the modular curve X_Γ is denoted by $\mathbb{C}(X_\Gamma)$. Then from [7, Section 7.5] we know that the function field extension $\mathbb{C}(X(\ell))|\mathbb{C}(X(1))$ is Galois with Galois group

$$\mathrm{Gal}(\mathbb{C}(X(\ell))|\mathbb{C}(X(1))) \cong \mathrm{SL}_2(\mathbb{Z}/\ell\mathbb{Z})/\{\pm I\},$$

and the extension $\mathbb{C}(X_1(\ell))|\mathbb{C}(X_0(\ell))$ is Galois with Galois group

$$\mathrm{Gal}(\mathbb{C}(X_1(\ell))|\mathbb{C}(X_0(\ell))) \cong \{\pm I\}\Gamma_0/\{\pm I\}\Gamma_1 \cong (\mathbb{Z}/\ell\mathbb{Z})^*/\{\pm 1\}. \tag{3.1}$$

Definition 3.1. Let $\Gamma_1 \le \Gamma_2$ be congruence subgroups. The natural morphism $X_{\Gamma_1} \to X_{\Gamma_2}$ is said to be *Galois* if the extension $\mathbb{C}(X_{\Gamma_1})|\mathbb{C}(X_{\Gamma_2})$ is Galois. The *Galois group of* $X_{\Gamma_1} \to X_{\Gamma_2}$ is defined to be $\mathrm{Gal}(\mathbb{C}(X_{\Gamma_1})|\mathbb{C}(X_{\Gamma_2}))$.

This allows us to speak of the Galois theory of modular curves over $\mathbb{C}$ via the Galois theory of their function fields. Let $G = \mathrm{Gal}(\mathbb{C}(X_\Gamma)|\mathbb{C}(X_0(\ell)))$. Since the meromorphic differentials of the modular curve X_Γ form a 1-dimensional vector space over $\mathbb{C}(X_\Gamma)$ generated by df for a non-constant function $f \in \mathbb{C}(X_\Gamma)$ that is Γ-invariant, the space of differentials is isomorphic to $\mathbb{C}(X_\Gamma)$ as a G-module.

4. Algorithm for our cases. In this section we will explain how to compute the polynomial $P_{f,\lambda}$ in (2.2), the splitting field of which is the fixed field of the Galois representations $\rho_{f,\lambda}$ associated to a modular form f of level 1. All the discussion in this section also holds for the case of projective polynomial $\tilde{P}_{f,\lambda}$ in (2.3). As explained in Section 2, our main task is then to compute the 2-dimensional $\mathbb{F}_\lambda$-linear space V_λ. We will follow Bosman except that we work with a modular curve that sometimes has smaller genus than $X_1(\ell)$.

4.1. Finding modular curves. Let $k > 0$ be an even integer and let ℓ be a prime number with $k \le \ell + 1$. Let $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$ be a newform of level 1. In general, the modular curve to realize the representation $\rho_{f,\lambda}$ is $X_1(\ell)$, which has genus $(\ell-5)(\ell-7)/24$, but we have

Proposition 4.1. *Let $k > 0$ be an even integer and $f \in S_k(\mathrm{SL}_2(\mathbb{Z}))$ be a newform of level 1 and weight k. Let $\ell \ge k-1$ be a prime number and λ be a prime lying over ℓ. Let Γ be the unique group*

$$\Gamma_1(\ell) \subset \Gamma \subset \Gamma_0(\ell)$$

with $[\Gamma : \Gamma_1(\ell)] = \frac{1}{2}\gcd(k-2, \ell-1)$. Then there exists a newform $f_2 \in S_2(\Gamma)$ and a prime λ_2 lying over ℓ in the field K_{f_2} such that $\rho_{f,\lambda}$ is isomorphic to ρ_{f_2,λ_2}.

Proof. It follows from [14, Theorem 2.2] that there exists $f_2 \in S_2(\Gamma_1(\ell))$ and a prime $\lambda_2 \mid \ell$ such that $\rho_{f,\lambda}$ is isomorphic to ρ_{f_2,λ_2}. Since the character of f is trivial in our case, for any $p \nmid \ell$ by (2.1) we have the equalities in $\overline{\mathbb{F}}$:

$$a_p(f_2) = a_p(f) \quad \text{and} \quad \varepsilon_2(p) = p^{k-2} \tag{4.1}$$

Here ε_2 is the nebentypus character of f_2, which is a Dirichlet character of the cyclic group $(\mathbb{Z}/\ell\mathbb{Z})^*$. Let ω be the cyclotomic character; it follows from the second equation in (4.1) that $\varepsilon_2 = \omega^{k-2}$.

By (3.1), the map $X_1(\ell) \to X_0(\ell)$ is Galois and its Galois group is $(\mathbb{Z}/\ell\mathbb{Z})^*/\{\pm 1\}$. Now let H denote the normal subgroup $\ker(\omega^{k-2})/\{\pm 1\}$ of $(\mathbb{Z}/\ell\mathbb{Z})^*/\{\pm 1\}$. By the Galois theory of function fields of modular curves, we have an intermediate curve X of $X_1(\ell) \to X_0(\ell)$ such that the Galois group of $X_1(\ell) \to X$ is H. Let φ denote the surjection

$$\varphi : \ \Gamma_0(\ell) \twoheadrightarrow (\mathbb{Z}/\ell\mathbb{Z})^*, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \overline{d}, \tag{4.2}$$

whose kernel is $\Gamma_1(\ell)$. Let Γ_H be the preimage of $\{\pm 1\}H$ under φ. Then we have $X = X_{\Gamma_H}$ and $\ker(\varphi) \subseteq \Gamma_H$, since $\#H = \frac{1}{2}\gcd(k-2, \ell-1)$.

To complete the proof we only need to check that $f_2 \in S_2(\Gamma_1(\ell))$ also lies in $S_2(\Gamma_H)$. In fact, for all $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_H$, it follows from the definition of Γ_H that $\varphi(\gamma)$ is in $\ker(\omega^{k-2})$ and thus $f_2|_2\gamma = \omega^{k-2}(\varphi(\gamma))f_2 = f_2$, which implies $f_2 \in S_2(\Gamma_H)$. ∎

Once we find a congruence subgroup Γ_H of level ℓ with $\Gamma_1(\ell) \subset \Gamma \subset \Gamma_0(\ell)$ such that the associated newform $f_2 \in S_2(\Gamma_1(\ell))$ lies in $S_2(\Gamma_H)$, then X_{Γ_H} can be taken as the modular curve to realize the representations. The proof implies that $X_1(\ell) \to X_{\Gamma_H}$ is Galois with Galois group H.

Now, $\gcd(\ell-1, k-2)$ cannot be larger than $\ell-1$ or $k-2$. If it is equal to $\ell-1$, the character ω^{k-2} is trivial and the representation is actually a subrepresentation of the ℓ-torsion of the Jacobian of $X_0(\ell)$. This happens for instance for $k = 12$ and $\ell = 11$, reducing the computation to a calculation on the genus 1 curve $X_0(11)$. If the gcd equals $k-2$, we have $\ell \geq k-1$ with $\ell \equiv 1 \bmod k-2$. This happens for instance for $k = 12$ and $\ell = 31$.

4.2. Realization of ρ in the Jacobian of a modular curve. Let $k > 0$ be an even integer. Suppose $H = \ker(\omega^{k-2})/\{\pm 1\}$. In this subsection, we assume that $\ell \geq k-1$ is a prime number and $f \in S_2(\Gamma_1(\ell))$ has character ω^{k-2} and so lies in $S_2(\Gamma_H)$ where Γ_H corresponds to H via φ in (4.2). Let X_{Γ_H} be the modular curve of the subgroup Γ_H and denote by J_{Γ_H} its Jacobian. Then $X_1(\ell) \to X_{\Gamma_H}$ is Galois with Galois group H. As discussed in Section 3, the meromorphic differential space over $X_1(\ell)$ is isomorphic to $\mathbb{C}(X_1(\ell))$ as a $\mathrm{Gal}(\mathbb{C}(X_1(\ell))|\mathbb{C}(X_0(\ell)))$-module; it follows that the holomorphic differential space $\Omega^1_{\mathrm{hol}}(X_{\Gamma_H})$ is the H-invariant part of $\Omega^1_{\mathrm{hol}}(X_1(\ell))$. By

taking duals of these spaces, we get

$$J_{\Gamma_H}(\overline{\mathbb{Q}})[\ell] = J_1(\ell)(\overline{\mathbb{Q}})[\ell]^H := \{x \in J_1(\ell)(\overline{\mathbb{Q}})[\ell] \mid \sigma(x) = x \text{ for all } \sigma \in H\}.$$

As discussed in Section 2, the representation associated to f is a subrepresentation of the ℓ-torsion points of $J_1(\ell)$. However, in our cases one can work with J_{Γ_H} instead of $J_1(\ell)$:

PROPOSITION 4.2. *The torsion space V_λ is a 2-dimensional subspace of $J_{\Gamma_H}(\overline{\mathbb{Q}})[\ell]$.*

Proof. It follows from the definition of H that each $\sigma \in H$ acts on $J_1(\ell)(\overline{\mathbb{Q}})[\ell]$ just as the diamond operator $\langle d\rangle$ for some $d \in (\mathbb{Z}/\ell\mathbb{Z})^*$ with $d^{k-2} = 1$. This implies that $\sigma - id$ is an element of $\mathfrak{m} = \ker(\theta)$ and thus $V_\lambda \subset J_1(\ell)(\overline{\mathbb{Q}})[\ell]^H = J_{\Gamma_H}(\overline{\mathbb{Q}})[\ell]$. ∎

4.3. Description of the computations. Now we show how to explicitly compute the polynomial

$$P_{f,\lambda}(x) = \prod_{P \in V_\lambda - \{0\}} (x - h(P)).$$

First of all, $J_\Gamma(\mathbb{C})[\ell]$ can be described in terms of modular symbols by the isomorphisms

$$J_\Gamma(\mathbb{C})[\ell] \cong H_1(X_\Gamma, \mathbb{F}_\ell) \cong \mathbb{S}_2(\Gamma) \otimes \mathbb{F}_\ell.$$

Let g be the genus of J_Γ. Taking a basis $f_1, \dots, f_g$ of $S_2(\Gamma)$, we can compute the period lattice $\Lambda \subset \mathbb{C}^g$ by integrating $(f_1, \dots, f_g)$ along elements of $H_1(X_\Gamma, \mathbb{F}_\ell)$. Let $\mathbb{T}'$ be the the Hecke algebra over $S_2(\Gamma)$. Since the action of $\mathbb{T}' \subset \mathrm{End}(J_\Gamma)$ on $\mathbb{S}_2(\Gamma)$ can be numerically computed [21], we thus obtain approximations of the torsion points of $V_\lambda \subset (1/\ell)\Lambda/\Lambda$. Then using the Newton iteration approximation method, we can find torsion divisors via the Abel–Jacobi map and finally compute the polynomial in (2.2).

This approximation method requires very high precision even when ℓ is quite small. But since the precision depends on the dimension of the Jacobian J_Γ, replacing by J_Γ whose dimension is smaller than $J_1(\ell)$ reduces a large number of calculations and therefore we can compute the cases for larger ℓ.

5. Examples. For $k = 12, 14, 16, 18, 20$ and 22, let Δ_k denote the unique cusp form of level 1 and weight k. In [2], Bosman computed the modular projective polynomials $\tilde{P}_{\Delta_k,\ell}$ for several values of ℓ and k. We add a few more polynomials to this list using the algorithm described in Section 4.

We first give a list of (k, ℓ) with $\gcd(k-2, \ell-1) > 2$ for which we have computed the polynomials $\tilde{P}_{\Delta_k,\ell}$ together with the dimensions of $J_1(l)$ and J_{Γ_H}:

(k,ℓ)	$\gcd(k-2,\ell-1)$	Dimension of $J_1(\ell)$	Dimension of J_{Γ_H}
(12, 31)	10	26	6
(16, 29)	14	22	4
(20, 31)	6	26	6
(22, 31)	10	26	6

The corresponding polynomials are given in Table 1.

Table 1. Polynomials

(k,ℓ)	$\tilde{P}_{\Delta_k,\ell}$
$(12,31)$	$x^{32}-4x^{31}-155x^{28}+713x^{27}-2480x^{26}+9300x^{25}-5921x^{24}+24707x^{23}+127410x^{22}-646195x^{21}+747906x^{20}-7527575x^{19}+4369791x^{18}-28954961x^{17}-40645681x^{16}+66421685x^{15}-448568729x^{14}+751001257x^{13}-1820871490x^{12}+2531110165x^{11}-4120267319x^{10}+4554764528x^{9}-5462615927x^{8}+4607500922x^{7}-4062352344x^{6}+2380573824x^{5}-1492309000x^{4}+521018178x^{3}-201167463x^{2}+20505628x-1261963$
$(16,29)$	$x^{30}-13x^{29}+116x^{28}-899x^{27}+6003x^{26}-33002x^{25}+142158x^{24}-437871x^{23}+599981x^{22}+3161522x^{21}-30157709x^{20}+149069425x^{19}-545068137x^{18}+1602112888x^{17}-3929042061x^{16}+8240756348x^{15}-15020495335x^{14}+23992472995x^{13}-33394267804x^{12}+40034881756x^{11}-40888329774x^{10}+35730188833x^{9}-27316581262x^{8}+17713731976x^{7}-7068248851x^{6}-1463296732x^{5}+4054490087x^{4}-2555610007x^{3}+2573924261x^{2}+2363203645x-261910751$
$(20,31)$	$x^{32}-4x^{31}-62x^{30}+558x^{29}-248x^{28}-23560x^{27}+143499x^{26}+59489x^{25}-4280108x^{24}+17190864x^{23}+12517459x^{22}-344750256x^{21}+1225662500x^{20}-278789479x^{19}-14790203106x^{18}+64357190741x^{17}-83774789980x^{16}-406418167694x^{15}+2480836111912x^{14}-5273524311353x^{13}-3257558862543x^{12}+54285321863574x^{11}-162450534558477x^{10}+197719989210108x^{9}+250865100757790x^{8}-1714511602191278x^{7}+4206562171750919x^{6}-6661579151098950x^{5}+7460752526582377x^{4}-5959749341609879x^{3}+3269911760551427x^{2}-1113936554991727x+178725601175511$
$(22,31)$	$x^{32}-3x^{31}-124x^{30}+651x^{29}+5797x^{28}-44020x^{27}-46593x^{26}+1523309x^{25}-4960682x^{24}-28562129x^{23}+205283395x^{22}+345367838x^{21}-3865963779x^{20}-5281917640x^{19}+35629245810x^{18}+95827452774x^{17}+227525150938x^{16}-1735983387875x^{15}-9952753525850x^{14}+15867354189588x^{13}+146446287180279x^{12}-99789981007214x^{11}-1135328992145553x^{10}-171825071648506x^{9}+7446294546204081x^{8}+2945308331901 47x^{7}-24397472702475140x^{6}-9976638213111902x^{5}+61714590456038129x^{4}+16902762581347117x^{3}-13833080015551423x^{2}-202960986205176103x+187532019539254309$

The computations done to obtain these polynomials required a precision of about 4200 bits for $\ell = 31$ and 3500 bits for $\ell = 29$. The calculations have been done in SAGE [16]. They took about 10 days for each of the cases with

$\ell = 31$ and one week for the case $\ell = 29$. The polynomial $\tilde{P}_{\Delta_{12},31}$ has also been obtained by Zeng [22]. His method avoids high precision computations and is based on p-adic computations. Mascot [13] claims to have computed $P_{\Delta_{12},29}$, but unfortunately he has not provided the polynomial.

It is difficult to rigorously prove that the computations have been done with sufficient accuracy and that therefore the results are correct. However, once the polynomial is computed, one can verify that it is correct using Serre's conjecture.

Let ℓ be a prime. A Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ has a Serre level $N(\rho)$ and a Serre weight $k(\rho)$. See [20] for Serre's definition and [8] for a reformulation. Then we have the following famous theorem which was fully proved by C. Khare and J. P. Wintenberger in 2008:

THEOREM 5.1 (Serre's Conjecture). *Let ℓ be a prime and let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q}) \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be a representation that is irreducible and odd. Then there exists a newform f of level $N(\rho)$ and weight $k(\rho)$ and a prime λ of K_f above ℓ such that ρ is isomorphic to $\overline{\rho}_{f,\lambda}$.*

Proof. See [11]. ∎

Now we have

PROPOSITION 5.2. *For each pair (k, ℓ) in Table* 1*, we denote by Δ_k the normalized newform of weight k and level* 1*. Then the polynomial $\tilde{P}_{\Delta_k,\ell}$ in Table* 1 *is irreducible. The Galois group of its splitting field is isomorphic to* $\mathrm{PGL}_2(\mathbb{F}_\ell)$*. Moreover, the subgroup of* $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ *fixing a root of $\tilde{P}_{\Delta_k,\ell}$ corresponds via $\tilde{\rho}_{\Delta,\ell}$ to the subgroup of* $\mathrm{PGL}_2(\mathbb{F}_\ell)$ *fixing a point of* $\mathbb{P}^1(\mathbb{F}_\ell)$*.*

Proof. First, the algorithm in [10, Algorithm 6.1] which has been implemented in MAGMA [1] was used to compute the Galois group $\mathrm{Gal}(\tilde{P}_{\Delta_k,\ell})$ of the polynomials in Table 1 as a permutation group acting on the roots. The practical calculations can be done in several seconds. This provides us with an isomorphism

$$\mathrm{Gal}(\tilde{P}_{\Delta_k,\ell}) \cong \mathrm{PGL}_2(\mathbb{F}_\ell). \tag{5.1}$$

Then we have a projective representation $\tilde{\rho}_{k,\ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)$ by composing the canonical map $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\tilde{P}_{\Delta_k,\ell})$ with the isomorphism in (5.1). Since the group $\mathrm{PGL}_2(\mathbb{F}_\ell)$ has no outer automorphisms, up to isomorphism $\tilde{\rho}_{k,\ell}$ is uniquely determined by $\tilde{P}_{\Delta_k,\ell}$.

We denote by $K_{k,\ell} := \mathbb{Q}[x]/(\tilde{P}_{\Delta_k,\ell})$ the number field defined by $\tilde{P}_{\Delta_k,\ell}$, and the integer ring of $K_{k,\ell}$ is denoted by $\mathcal{O}_{k,\ell}$.

Let G be the subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ fixing a root of $\tilde{P}_{\Delta_k,\ell}$. By the canonical map $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \twoheadrightarrow \mathrm{Gal}(\tilde{P}_{\Delta_k,\ell})$, the group G corresponds to a subgroup of $\mathrm{Gal}(\tilde{P}_{\Delta_k,\ell})$ of index $[K_{k,\ell} : \mathbb{Q}] = \deg(\tilde{P}_{\Delta_k,\ell}) = \ell + 1$, and thus the image of G via $\tilde{\rho}_{k,\ell}$ is a subgroup of $\mathrm{PGL}_2(\mathbb{F}_\ell)$ of index $\ell + 1$, which by [9, Lemma 7.3.2]

is the stabiliser subgroup of a point in $\mathbb{P}^1(\mathbb{F}_\ell)$. Therefore, via Galois theory $K_{k,\ell}$ is the fixed field of a subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}|\mathbb{Q})$ fixing a root of $\tilde{P}_{\Delta_k,\ell}$, which corresponds to the stabiliser subgroup of a point in $\mathbb{P}^1(\mathbb{F}_\ell)$.

For each (k,ℓ) in Table 1, the discriminant of the field $K_{k,\ell}$ over $\mathbb{Q}$ is $(-1)^{(\ell-1)/2}\ell^{k+\ell-2}$. This can be shown as follows. One can compute the discriminant $\mathcal{D}(\tilde{P}_{\Delta_k,\ell})$ of $\tilde{P}_{\Delta_k,\ell}$, and the discriminant $\mathcal{D}_{k,\ell}$ of the number field $K_{k,\ell}$ divides $\mathcal{D}(\tilde{P}_{\Delta_k,\ell})$. Then for each prime divisor q of the discriminant of $\mathcal{D}(\tilde{P}_{\Delta_k,\ell})$ one can efficiently compute the power of q that divides the discriminant of $K_{k,\ell}$ using the algorithms in [4, Section 6]. In the cases with $\ell = 31$ it is easy to factorize the discriminants of the polynomials $\tilde{P}_{\Delta_k,31}$ and then the discriminant of $K_{k,31}$ turns out to be ℓ^{k+l-2}. In the case $\ell = 29$, the discriminant of $\tilde{P}_{\Delta_k,\ell}$ can be factorized as $3^6 \cdot 19^4 \cdot 29^{43} \cdot 12653^2 \cdot 19387^2 \cdot B^2$ where B is a product of large primes and has about 162 decimal digits. We have failed to factorize B, but checked that it is not divisible by any prime $< 10^6$. However, we expect that the prime divisors of B do not divide the discriminant $\mathcal{D}_{16,29}$ of $K_{16,29}$ and fortunately we can check this with the algorithm of Buchmann–Lenstra without knowing its factorization. In fact, this boils down to the following computation: Let P' be the derivative of $\tilde{P}_{\Delta_{16},29}$; then in $\mathbb{Z}/B\mathbb{Z}$ we compute $h = \tilde{P}_{\Delta_{16},29}/\gcd(\tilde{P}_{\Delta_{16},29}, P')$. Now we take a lift $\tilde{h}$ of h. The fact that the minimal polynomial of $\tilde{h}/B$ is a divisor of the resultant $R(X)$ of $(X - \tilde{h}(x))/B$ and $\tilde{P}_{\Delta_{16},29}(x)$ with respect to x allows us to show that $\tilde{h}/B$ is an algebraic integer. Therefore no prime divisor of B can be a factor of $\mathcal{D}_{16,29}$. Then it follows from [4, Section 6] that $\mathcal{D}_{16,29} = 29^{43}$. All the explicit computations involved here are trivial.

Now each prime $p \neq \ell$ is unramified in $K_{k,\ell}$ and in all four cases it follows that $\tilde{\rho}_{k,\ell}$ is unramified at all $p \neq \ell$. By a lifting of $\tilde{\rho}_{k,\ell}$ we mean a representation $\rho_{k,\ell} : G \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ that makes the following diagram commute:

$$\begin{array}{ccc} G & \xrightarrow{\tilde{\rho}_{k,\ell}} & \mathrm{PGL}_2(\mathbb{F}_\ell) \\ {\scriptstyle \rho_{k,\ell}}\downarrow & & \downarrow \\ \mathrm{GL}_2(\overline{\mathbb{F}}_\ell) & \twoheadrightarrow & \mathrm{PGL}_2(\overline{\mathbb{F}}_\ell) \end{array}$$

where the bottom and right maps are the canonical ones. Then from [18, Section 6], we know $\tilde{\rho}_{k,\ell}$ has a lifting which is unramified outside ℓ and therefore has Serre level 1. By [9, Corollary 7.2.10] the minimal weight of a lifting of $\tilde{\rho}_{k,\ell}$ equals $v_\ell(\mathrm{Disc}(K_{k,\ell}|\mathbb{Q})) - \ell + 2 = k$. This shows that $\tilde{\rho}_{k,\ell}$ has a lifting $\rho_{k,\ell}$ with weight k and level 1.

The representation $\rho_{k,\ell}$ is odd in all four cases. Indeed, suppose not. Then the image under $\rho_{k,l}$ of a complex conjugation ι is $\pm\mathrm{Id} \in \mathrm{GL}_2(\mathbb{F}_\ell)$. This implies that $\tilde{\rho}_{k,l}(\iota)$ is trivial. It follows that $K_{\ell,k}$ is totally real. However,

this cannot be true. Indeed, for $\ell = 31$ the discriminant of $K_{k,\ell}$ is negative, while for $\ell = 29$ the polynomial $\tilde{P}_{\Delta_{16},29}(x) = \sum_{i=1}^{30} a_i X^i$ has the property that $a_1^2 - 2a_0a_2 < 0$, which implies that the sum of the reciprocals of its roots is negative.

The fact that $\operatorname{Im}\tilde{\rho}_{k,\ell} = \mathrm{PGL}_2(\mathbb{F}_\ell)$ implies that $\rho_{k,\ell}$ is absolutely irreducible. For each (k,ℓ) in Table 1, the cuspidal space $S_k(\mathrm{SL}_2(\mathbb{Z}))$ has dimension 1 and Serre's conjecture ensures that $\rho_{k,\ell} \cong \rho_{\Delta_k,\ell}$, and hence $\tilde{\rho}_{k,\ell} \cong \tilde{\rho}_{\Delta_k,\ell}$. ∎

As an example we also computed the following congruence relations in $\mathbb{Z}/31\mathbb{Z}$:

$$\begin{aligned}\tau(10^{1000} + 4351) &= \pm 8,\\ \tau(10^{1000} + 10401) &= 0,\\ \tau(10^{1000} + 11979) &= \pm 11,\\ \tau(10^{1000} + 17557) &= \pm 8.\end{aligned}$$

To obtain these relations, it took about half an hour in SAGE.

In 1947, D. H. Lehmer conjectured that $\tau(n) \neq 0$ for all n. In [12, Theorem 2] he proved that the smallest n for which $\tau(n) = 0$ must be a prime. J.-P. Serre [19] showed that if $\tau(p) = 0$ for a prime p, then

$$\begin{aligned}p &\equiv -1 \bmod 2^{11}3^7 5^3 691,\\ p &\equiv -1, 19, 31 \bmod 7^2,\\ p &\equiv \text{a non-square mod } 23.\end{aligned}$$

We systematically searched for the smallest prime p in these congruence classes for which in addition $\tau(p) \equiv 0 \bmod 11 \cdot 13 \cdot 17 \cdot 19 \cdot 31$. The smallest prime we found is

$$p = 982149821766199295999.$$

Thus we have

COROLLARY 5.3. *$\tau(n) \neq 0$ for all*

$$n < 982149821766199295999.$$

We did the searching computations in PARI and they took around one hour. In [9, Corollar 7.4], Bosman's bound is 22798241520242687999 and our bound improves his by a factor of approximately 43. In [22], Zeng and Yin also obtained the same prime.

Acknowledgements. The author is partly supported by China Scholarship Council (CSC). The author sincerely thanks his advisor René Schoof for proposing this exciting topic, as well as for his many critical sugges-

tions and comments on this paper. The author is grateful to Johan Bosman for his continuous assistance throughout this work. Also, thanks to Bas Edixhoven for his enlightening explanation and comments on the original algorithm. Thanks also go to Mark van Hoeij who explained to the author the algorithm to compute the discriminant of the number field for the case $(k, \ell) = (16, 29)$.

References

[1] W. Bosma, J. J. Cannon and C. E. Playoust, *The Magma algebra system I: the user language*, J. Symbolic Comput. 24 (1997), 235–265.

[2] J. Bosman, *On the computation of Galois representations associated to level one modular forms*, arXiv:0710.1237 (2007).

[3] J. Bosman, *Explicit computations with modular Galois representations*, Ph.D. thesis, Univ. Leiden, 2008.

[4] J. A. Buchmann and H. W. Lenstra, Jr., *Approximating rings of integers in number fields*, J. Théor. Nombres Bordeaux 6 (1994), 221–260.

[5] H. Cohen, *A Course in Computational Algebraic Number Theory*, Grad. Texts in Math. 138, Springer, Berlin, 1993.

[6] P. Deligne, *Formes modulaires et représentations ℓ-adiques*, in: Lecture Notes in Math. 179, Springer, 1971, 139–172.

[7] F. Diamond and J. Shurman, *A First Course in Modular Forms*, Grad. Texts in Math. 228, Springer, New York, 2005.

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

[9] S. J. Edixhoven, J.-M. Couveignes, R. S. de Jong, F. Merkl and J. G. Bosman, *Computational Aspects of Modular Forms and Galois Representations*, Ann. of Math. Stud. 176, Princeton Univ. Press, Princeton, 2011.

[10] K. Geissler and J. Klüners, *Galois group computation for rational polynomials*, J. Symbolic Comput. 30 (2000), 653–674.

[11] C. Khare and J.-P. Wintenberger, *Serre's modularity conjecture (I), (II)*, Invent. Math. 178 (2009), 485–586.

[12] D. H. Lehmer, *The vanishing of Ramanujan's function $\tau(n)$*, Duke Math. J. 10 (1947), 429-433.

[13] N. Mascot, *Computing modular Galois representations*, Rend. Circ. Mat. Palermo 62 (2013), 451–476; arXiv:1211.1635v5 (2013).

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

[15] K. A. Ribet and W. A. Stein, *Lectures on Serre's conjectures*, in: Arithmetic Algebraic Geometry (Park City, UT, 1999), Amer. Math. Soc., Providence, RI, 2001, 143–232.

[16] SAGE, *open source mathematics software*, http://sagemath.org/.

[17] R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. 44 (1985), 483–494.

[18] J.-P. Serre, *Modular forms of weight one and Galois representations*, in: Algebraic Number Fields: L-functions and Galois Properties, A. Fröhlich (ed.), Academic Press, London, 1977, 193–268.

[19] J.-P. Serre, *Sur la lacunarité des puissances de* η, Glasgow Math. J. 27 (1985). 203–221.

[20] J.-P. Serre, *Sur les représentations modulaires de degré 2 de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987), 179–230.

[21] W. A. Stein, *Modular Forms, a Computational Approach*, Grad. Stud. Math. 79, Amer. Math. Soc., Providence, RI, 2007.

[22] J. X. Zeng and L. S. Yin, *On the computation of coefficients of modular forms: the reduction modulo p approach*, arXiv:1211.1124v4 (2013).

Peng Tian
Department of Mathematics
Nanjing University
210093, Nanjing, P.R. China
and
Dipartimento di Matematica
Università di Roma "Tor Vergata"
00133 Roma, Italy
E-mail: tianpeng.china@gmail.com

Received on 22.10.2013
and in revised form on 14.3.2014 (7623)