LMS J. Comput. Math. 17 (Special issue A) (2014) 36–48
doi:10.1112/S1461157014000205

Computing Galois representations of modular abelian surfaces

Jinxiang Zeng

Abstract

Let $f \in S_2(\Gamma_0(N))$ be a normalized newform such that the abelian variety A_f attached by Shimura to f is the Jacobian of a genus-two curve. We give an efficient algorithm for computing Galois representations associated to such newforms.

1. *Introduction*

Let $f = \sum_{n\geqslant 1} a_n q^n \in S_2(\Gamma_0(N), \epsilon)$ be a normalized newform, $K_f = \mathbb{Q}(\{a_n\}_{n\geqslant 1})$ the number field generated by the coefficients of f. Associated to f there is a modular abelian variety denoted as A_f of dimension $[K_f : \mathbb{Q}]$ constructed by Shimura. Let ℓ be a prime number and $\mathfrak{l}$ a prime ideal of K_f dividing (ℓ) with residue field denoted as $\mathbb{F}$. We denote by $\tilde{f} = \sum_{n\geqslant 1} \tilde{a}_n q^n$ the reduction of f modulo $\mathfrak{l}$. Associated to $\tilde{f}$, there is a continuous representation

$$\rho_{\tilde{f}} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}) \tag{1.1}$$

satisfying the folowing:

(1) $\rho_{\tilde{f}}$ is unramified at prime $p \nmid \ell N$ and

$$\mathrm{Tr}(\rho_{\tilde{f}}(\mathrm{Frob}_p)) = \tilde{a}_p,$$
$$\mathrm{Det}(\rho_{\tilde{f}}(\mathrm{Frob}_p)) = \epsilon(p)p;$$

(2) $V_\ell := A_f[\mathfrak{m}] \subset J_1(N)[\ell]$ is a finite-dimensional $\mathbb{F}$-vector space realizing $\rho_{\tilde{f}}$, where $\mathfrak{m}$ is the kernel of the projection $\mathbb{T}(N, 2) \to \mathbb{F}, T_n \mapsto \tilde{a}_n$ and $\mathbb{T}(N, 2) = \mathbb{Z}[T_n : n \geqslant 1] \subset \mathrm{End}(A_f)$ is the Hecke algebra for A_f.

The fact that this Galois representation (1.1) can be computed in polynomial time, shown in [**6**], is basic for computing coefficients of modular forms of general weights and levels. In particular, by the theory of congruences of modular forms, the computation of mod-ℓ Galois representation associated to modular forms of weight k $(2 < k \leqslant \ell + 1)$ and level 1 can be reduced to the computation of (1.1) with $N = \ell$.

Some progress has been made in designing and implementing practical variants of algorithms for computing coefficients of modular forms of weight $k > 2$ and level 1. All current methods put the main effort into constructing the representation space $V_\ell \subset J_1(\ell)[\ell]$ explicitly. One of the challenges in doing this is that $J_1(\ell)$ as the Jacobian of modular curve $X_1(\ell)$ has dimension quadratic in ℓ ($\dim J_1(\ell) = (\ell-5)(\ell-7)/24$), which is too large to be handled efficiently using current algorithms for computing Riemann–Roch space; see [**2**, **10**, **19**] for the discussion and the computation of $\ell \leqslant 29$ cases. Smarter ways for constructing V_ℓ are also developed, that is, if $d = \gcd(k-2, \ell-1) > 2$ then V_ℓ lies in the Jacobian $J_H(\ell)$ of some modular curve $X_H(\ell)$.

Received 27 February 2014; revised 23 May 2014.

2010 Mathematics Subject Classification 11Y40, 11F80, 11G18, 11G20.

Contributed to the Algorithmic Number Theory Symposium XI, GyeongJu, Korea, 6–11 August 2014.

This work was partially supported by NSFC grant No. 11271212.

This significantly accelerates the calculation, especially when $d = k - 2$; see [4, 16]. Even so, the running time increases dramatically as the level increases. The highest level achieved is $\ell = 43$; see [4].

It seems difficult to investigate higher-level cases using previous methods. For example, let $f_1 = \sum_{n\geqslant 1} a_n q^n$ be the unique (up to Galois conjugacy) newform in $S_{192}(\mathrm{SL}_2(\mathbb{Z}))$. Then we have $[K_{f_1} : \mathbb{Q}] = 16$. The prime 191 is unramified in K_{f_1} and its decomposition can be written as $(191) = \wp_1 \cdot \wp_2 \cdot \wp_3 \cdot \wp_4$, where the residual degrees of prime ideals $\wp_1, \wp_2, \wp_3, \wp_4$ are 1, 1, 2, 12 respectively. Our question is: can we compute $a_p \bmod \wp_i \in \mathbb{F}_{191},\ i = 1, 2$, for large prime p? We cannot use the previous methods, because $J_1(191)$ has dimension equal to 881, which is too large to do any practical calculation.

Using Magma [1], we can check that there is a newform $f = \sum_{n\geqslant 1} b_n q^n \in S_2(\Gamma_0(191))$ with coefficient field $K_f = \mathbb{Q}(\sqrt{5})$, such that $\{f \bmod \mathfrak{l}_i : i = 1, 2\} = \{f_1 \bmod \wp_i : i = 1, 2\}$, where $\mathfrak{l}_i$ are prime ideals of K_f over 191. Moreover, the abelian variety A_f is $\mathbb{Q}$-isomorphic to the Jacobian $\mathrm{Jac}(C)$ of a hyperelliptic curve C (see § 2). So, instead of using $J_1(191)$, we may construct a representation space for each $f \bmod \mathfrak{l}_i$ using $\mathrm{Jac}(C)$ directly.

In general, let A_f be the abelian variety attached to a newform $f \in S_2(\Gamma_1(N))$. If $\dim A_f \geqslant 4$, then it may happen that A_f is not a Jacobian variety. However, if $\dim A_f \leqslant 3$, then there always exists a curve C such that its Jacobian $\mathrm{Jac}(C)$ is isogenous to A_f; see [12, 18]. In this case, instead of A_f, the Jacobian variety $\mathrm{Jac}(C)$ can be used to compute the Galois representations associated to f. In this paper we will study this approach, with an emphasis on the case where A_f has dimension 2 and $\mathrm{Jac}(C)$ is $\mathbb{Q}$-isomorphic to A_f.

The rest of the paper is organized as follows. In § 2 we recall a method for computing an equation for a curve C whose Jacobian is $\mathbb{Q}$-isogenous to modular abelian surface and introduce a method for computing the action of Hecke operators on $\mathrm{Jac}(C)$. We also present a method for computing Galois representations using this curve. In § 3 we focus on an application of computing Galois representations to counting points on modular abelian surfaces. We also present some computational results.

2. *Galois representations and abelian surfaces*

2.1. *Equations for curves with modular Jacobians*

Let C be a non-singular projective curve defined over $\mathbb{Q}$. If there exists a non-constant morphism $\pi : X_1(N) \to C$ defined over $\mathbb{Q}$ for some positive integer N, then C is called modular of level N. A modular curve is called primitive of level N, if it is not modular of level d for any proper divisor $d|N$. The corresponding surjective morphism $\pi_* : J_1(N) \to \mathrm{Jac}(C)$ is defined over $\mathbb{Q}$ and $\mathrm{Jac}(C)$ is called modular of level N as well. Equations for modular curves $C/\mathbb{Q}$ with genus greater than 1 have been studied by some authors. In particular, modular curves with genus 2 have been determined completely; see [8].

Let us first recall the method in [8] for computing an equation for the modular curve C. Let $f = \sum_{n\geqslant 1} a_n q^n \in S_2(\Gamma_1(N))$ be a normalized newform, $S_2(A_f)$ the $\mathbb{C}$-vector space generated by the Galois conjugates of f, and $H^0(A_f, \Omega^1)$ the $\mathbb{C}$-vector space $\{g(q)dq/q : g \in S_2(A_f)\}$. The following proposition in [8] is basic for computing equations for genus-two modular curves.

PROPOSITION 2.1. *Let $f \in S_2(\Gamma_1(N))$ be a normalized newform such that A_f is an abelian surface. Then there exists a primitive modular curve C defined over $\mathbb{Q}$ of level N, such that $\mathrm{Jac}(C)$ is $\mathbb{Q}$-isogenous to A_f, if and only if for every linearly independent pair of modular forms $g_1,\ g_2 \in S_2(A_f)$, there exists $P(X) \in \mathbb{C}[X]$ of degree 5 or 6 without double roots such*

https://doi.org/10.1112/S1461157014000205 Published online by Cambridge University Press

that the functions on $X_1(N)$ given by

$$x = \frac{g_1}{g_2}, \quad y = \frac{q dx/dq}{g_2},$$

satisfy the equation $y^2 = P(x)$.

REMARK 1. The Jacobian $\mathrm{Jac}(C)$ given above is not necessarily $\mathbb{Q}$-isomorphic to A_f. However, if A_f is principally polarized, then there is a general method for finding a curve C such that $\mathrm{Jac}(C) \simeq A_f$; see [9].

Let d be the square-free integer such that $K_f = \mathbb{Q}(\sqrt{d})$ is the coefficient field of $f = \sum_{n\geqslant 1} a_n q^n$. We denote by σ the non-trivial automorphism in $\mathrm{Gal}(\mathbb{Q}(\sqrt{d})/\mathbb{Q})$ and define

$$h_1 := \frac{f+\sigma(f)}{2} = \sum_{n\geqslant 1} \frac{a_n+\sigma(a_n)}{2} q^n, \quad h_2 := \frac{f-\sigma(f)}{2\sqrt{d}} = \sum_{n\geqslant 2} c_n q^n. \tag{2.1}$$

Then $h_1,\ h_2 \in \frac{1}{2}\mathbb{Z}[[q]]$ and $S_2(A_f)$ equals the $\mathbb{C}$-vector space spanned by h_1 and h_2. Hence the coefficients of the polynomial $y^2 = P(x)$ for $x = h_1/h_2,\ y = (q\,dx/dq)/h_2$ are rational numbers.

EXAMPLE 1. Let f be a newform of weight 2 and level 191 with q-expansion

$$f = q + aq^2 - q^3 + (-a-1)q^4 + (-a-1)q^5 - aq^6 + (-a-1)q^7 + \mathrm{O}(q^8), \tag{2.2}$$

where a is a root of $t^2 + t - 1 = 0$. By solving linear equations over $\mathbb{Q}$, we find a hyperelliptic curve C with an affine equation $y^2 = x^6 - 6x^5 + 5x^4 + 2x^3 + 2x^2 + 1$ such that $\mathrm{Jac}(C)$ is $\mathbb{Q}$-isogenous to the abelian surface A_f. In fact, $\mathrm{Jac}(C)$ is $\mathbb{Q}$-isomorphic to A_f, as shown in [9].

2.2. *Computing Galois representations of modular forms*

From now on, we restrict ourselves to newforms with trivial Nebentypus. Let $f = \sum_{n\geqslant 1} a_n q^n \in S_2(\Gamma_0(N))$ be a normalized newform with coefficient field $K_f = \mathbb{Q}(\sqrt{d})$ (d square-free) and ℓ an odd prime that splits in K_f. Assume there is a modular curve $C/\mathbb{Q}$ such that $\mathrm{Jac}(C)$ is $\mathbb{Q}$-isomorphic to A_f. The following paragraphs are devoted to computing the Galois representations $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$ associated to f. By 'computing' we mean determining the fixed field $L := \overline{\mathbb{Q}}^{\ker \rho_f}$ and the image $\rho_f(\sigma)$ for $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ explicitly.

Let $(\ell) = \mathfrak{l}_1\mathfrak{l}_2$ be the factorization of (ℓ) in K_f and $\tilde{f}_i = \sum_{n\geqslant 1} \tilde{a}_{n,i} q^n$ the reduction of f modulo $\mathfrak{l}_i$ for $i = 1, 2$. Associated to each $\tilde{f}_i$, there is a Galois representation $\rho_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$. For any prime $p \neq \ell$ such that $\tilde{a}_{p,1} \neq \tilde{a}_{p,2} \in \mathbb{F}_\ell$, a representation space for ρ_i can be written explicitly by the following lemma.

LEMMA 2.2. *With notation as above, let $\theta_i : \mathbb{T}(N,2) \to \mathbb{F}_\ell,\ T_n \mapsto \tilde{a}_{n,i} = a_n \bmod \mathfrak{l}_i$ be the surjective ring morphism given by $\tilde{f}_i$. Then we have $\ker\theta_i = \langle \ell, T_p - \tilde{a}_{p,i}\rangle$ and $V_i := A_f[\ell, T_p - \tilde{a}_{p,i}]$ is a two-dimensional $\mathbb{F}_\ell$-vector space realizing ρ_i for $i = 1, 2$.*

Proof. The Hecke algebra $\mathbb{T}(N,2)$ on A_f is isomorphic to the ring $\mathbb{Z}[a_n, n \geqslant 1]$ generated by the Fourier coefficients of f, where an algebraic integer a_n acts on A_f as T_n on A_f. So we have $\ker\theta_i = \langle \ell, a_n - \tilde{a}_{n,i}, n \geqslant 1\rangle$. To prove $\ker\theta_i = \langle \ell, T_p - \tilde{a}_{p,i}\rangle$, it suffices to prove that for

https://doi.org/10.1112/S1461157014000205 Published online by Cambridge University Press

any $n \geqslant 1$ there exists an $\alpha \in \mathbb{Z}[a_n, n \geqslant 1]$ such that

$$(a_n - \tilde{a}_{n,i}) = \alpha \cdot (a_p - \tilde{a}_{p,i}) \mod \ell \cdot \mathbb{Z}[a_n, n \geqslant 1].$$

By the Chinese remainder theorem, it suffices to prove

$$(a_n - \tilde{a}_{n,i}) = \alpha_j \cdot (a_p - \tilde{a}_{p,i}) \mod \mathfrak{l}_j, \quad \text{for } j = 1, 2. \tag{2.3}$$

If $i = j$, then (2.3) obviously holds, while if $i \neq j$, (2.3) holds because $(a_p - \tilde{a}_{p,i}) \mod \mathfrak{l}_j = (\tilde{a}_{p,j} - \tilde{a}_{p,i}) \in \mathbb{F}_\ell^\times$.

So we have $A_f[\ker \theta_i] = A_f[\ell, T_p - \tilde{a}_{p,i}]$ realizing ρ_i. That this subspace has dimension 2 follows easily from $\dim_{\mathbb{F}_\ell} A_f[\ker \theta_i] \geqslant 2$, $A_f[\ker \theta_1] \cap A_f[\ker \theta_2] = \{0\}$ and $\dim_{\mathbb{F}_\ell} A_f[\ell] = 4$. □

For each positive integer n, we denote by T_n the operator on $\mathrm{Jac}(C)$ corresponding to the Hecke operator T_n on A_f under the $\mathbb{Q}$-isomorphism $\mathrm{Jac}(C) \simeq A_f$. Then we have $\mathrm{Jac}(C)[\ell, T_p - \tilde{a}_{p,i}])$ (denoted by V_i as well) realizing ρ_i for $i = 1, 2$. The explicit isomorphism $\mathrm{Jac}(C) \simeq A_f$ is not established during computation of the modular curve C, so we cannot expect to compute T_n on $\mathrm{Jac}(C)$ directly without using further techniques.

Assume A_f and $\mathrm{Jac}(C)$ both have good reduction at p. Then we have a commutative diagram

$$\begin{array}{ccc} \mathrm{End}_{\mathbb{Q}}(A_f) & \hookrightarrow & \mathrm{End}_{\mathbb{F}_p}(A_f \otimes \mathbb{F}_p) \\ \downarrow \simeq & \circlearrowright & \downarrow \simeq \\ \mathrm{End}_{\mathbb{Q}}(\mathrm{Jac}(C)) & \hookrightarrow & \mathrm{End}_{\mathbb{F}_p}(\mathrm{Jac}(C) \otimes \mathbb{F}_p) \end{array}$$

The Eichler–Shimura relation asserts that $T_p = \mathrm{Frob}_p + p\mathrm{Frob}_p^{-1}$ on $A_f \otimes \mathbb{F}_p$. Using the commutative diagram above, we have $T_p = \mathrm{Frob}_p + p\mathrm{Frob}_p^{-1}$ on $\mathrm{Jac}(C) \otimes \mathbb{F}_p$ as well. In other words, $V_i(\overline{\mathbb{F}}_p) = \mathrm{Jac}(C)(\overline{\mathbb{F}}_p)[\ell, \mathrm{Frob}_p + p\mathrm{Frob}_p^{-1} - \tilde{a}_{p,i}]$ can be computed just by exploring the Frobenius endomorphism and multiplication on $\mathrm{Jac}(C)(\overline{\mathbb{F}}_p)$.

In order to construct $V_i/\mathbb{Q}$, we first compute sufficiently many $V_i(\overline{\mathbb{F}}_p)$ for small primes p and then reconstruct it by the Chinese remainder theorem.

More precisely, let τ be the hyperelliptic involution on C. Assume C is imaginary (the real case is similar). Then there is a single $\mathbb{Q}$-rational point ∞ at infinity and each point $D \in \mathrm{Jac}(C)$ has a unique reduced representation, that is, $D = D_x - r \cdot \infty$, where $D_x = \sum_{i=1}^{r} P_i$, $P_i \neq \infty$, $P_j \neq \tau(P_{j'})$ if $j \neq j'$, and $0 \leqslant r \leqslant 2$. Using these representations of points on $\mathrm{Jac}(C)$, we have a well-defined map (see [**13**])

$$\iota : \mathrm{Jac}(C) \setminus \{0\} \to \overline{\mathbb{Q}}, \quad D \mapsto \sum_{P \in D_x} y(P),$$

where each point P is on the affine part of C, so it can be represented by coordinates $(a, b, 1)$, and $y(P)$ is the y-coordinate b. By the uniqueness of the representation, we have $\sigma(\iota(D)) = \iota(\sigma(D))$ for all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ and $D \in \mathrm{Jac}(C)(\overline{\mathbb{Q}}) \setminus \{0\}$.

Let $P_i(X)$ be the polynomial defined as

$$P_i(X) = \prod_{D \in V_i(\overline{\mathbb{Q}}) \setminus \{0\}} (X - \iota(D)), \quad i = 1, 2. \tag{2.4}$$

Then $P_i(X) \in \mathbb{Q}[X]$ and $\deg P_i(X) = \ell^2 - 1$. The splitting field of $P_i(X)$ is the fixed field $L_i := \overline{\mathbb{Q}}^{\ker \rho_i}$ and the Galois representation ρ_i factors as $\rho_i : \mathrm{Gal}(L_i/\mathbb{Q}) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_\ell)$.

https://doi.org/10.1112/S1461157014000205 Published online by Cambridge University Press

LEMMA 2.3. *The logarithmic heights of coefficients of $P_i(X)$, $i = 1, 2$, are in $\mathrm{O}(\ell^2)$.*

Proof. Let $h : \mathrm{Jac}(\overline{\mathbb{Q}}) \to \mathbb{R}$ be the naive height function defined in [17]. For each ℓ-torsion point $D \in V_i(\overline{\mathbb{Q}}) \setminus \{0\}$, we have $h(D) \leqslant \frac{1}{3}\log(d) + \frac{4}{3}\log 2$ [17, Theorem 6.4], where d is the discriminant of the hyperelliptic curve C. So, there is an absolute constant c such that the logarithmic heights of roots (that is, $\iota(D)$) of $P_i(X)$ are bounded above by c. Hence the logarithmic heights of coefficients of $P_i(X)$ are bounded above by $\mathrm{O}(\ell^2)$. □

We now turn to the object $\mathrm{Jac}(C) \otimes \mathbb{F}_p$. For simplicity, the reduction of the $\mathbb{Q}$-rational point ∞ is denoted by ∞ as well.

DEFINITION 1. Let p be a prime such that $\tilde{a}_{p,1} \neq \tilde{a}_{p,2}$. If for all $D \in \mathrm{Jac}(C)(\overline{\mathbb{Q}}) \setminus \{0\}$ with reduced representation $D = D_x - r \cdot \infty$, its reduction $\tilde{D} = \tilde{D}_x - r \cdot \infty$ is the reduced representation for $\tilde{D} \in \mathrm{Jac}(\overline{\mathbb{F}}_p) \setminus \{0\}$, then p is called a good prime.

REMARK 2. It is shown in [13] that if C is imaginary then r always equals 2 in the reduced representation. As a consequence, every prime p such that $\tilde{a}_{p,1} \neq \tilde{a}_{p,2}$, A_f and $\mathrm{Jac}(C)$ have good reduction at p is a good prime.

Now let p be a good prime and $\mathbb{F}_q$ the minimal extension of $\mathbb{F}_p$ such that $V_i(\overline{\mathbb{F}}_p) = V_i(\mathbb{F}_q)$. Then we have a projection

$$\pi_i : \mathrm{Jac}(C)(\mathbb{F}_q)[\ell] \to V_i(\mathbb{F}_q), \quad D \mapsto (\mathrm{Frob}_p + p\mathrm{Frob}_p^{-1} - \tilde{a}_{p,i'})(D), \quad i = 1, 2; \tag{2.5}$$

here $i' = 2$ if $i = 1$ and $i' = 1$ if $i = 2$. The strategy to find a basis for $V_i(\mathbb{F}_q)$ can be formulated as follows:

(1) Compute $n = |\mathrm{Jac}(C)(\mathbb{F}_q)|$ and factor n as $n = \ell^e \cdot m$ with $\ell \nmid m$.
(2) Construct ℓ-torsion points by picking random points on $\mathrm{Jac}(C)(\mathbb{F}_q)$ and multiplying these points by m and proper powers of ℓ.
(3) Project the ℓ-torsion points to $V_i(\mathbb{F}_q)$ using the map π_i (2.5).

Using general algorithms for computing zeta functions of hyperelliptic curves, the zeta function for $C/\mathbb{F}_p$ can be computed in $\mathrm{O}(\log^\omega p)$ time for some constant ω. In fact, the explicit value of ω is not required in the following complexity analysis. Using Cantor's algorithm, addition in the Jacobian $\mathrm{Jac}(C)(\mathbb{F}_q)$ can be done in $\tilde{\mathrm{O}}(\log q)$ time. Moreover, $|\mathrm{Jac}(C)(\mathbb{F}_q)|$ is bounded above by $\mathrm{O}(q^2)$. So the complexity of constructing an ℓ-torsion point is bounded above by $\tilde{\mathrm{O}}(\log q^2 \cdot \log q) = \tilde{\mathrm{O}}(\log^2 q)$, which is bounded by $\tilde{\mathrm{O}}(\ell^4 \log^2 p)$, since $[\mathbb{F}_q : \mathbb{F}_p] < \ell^2$. Since $\dim_{\mathbb{F}_\ell}(V_i) = 2$, a basis for it can often be found from several random points on $V_i(\mathbb{F}_q)$, with a complexity

$$\mathrm{O}(\log^\omega p) + \tilde{\mathrm{O}}(\ell^4 \log^2 p). \tag{2.6}$$

By the uniqueness property, $P_i(X) \bmod p$ can be computed as

$$P_i(X) \bmod p = \prod_{\tilde{D} \in V_i(\mathbb{F}_q) \setminus \{0\}} (X - \tilde{\iota}(\tilde{D})) \in \mathbb{F}_p[X], \tag{2.7}$$

where $\tilde{\iota} : \mathrm{Jac}(C)(\overline{\mathbb{F}}_p) \setminus \{0\} \to \overline{\mathbb{F}}_p$ is the reduction of ι. Given $V_i(\mathbb{F}_q)$, we can compute the polynomial $P_i(X) \bmod p$ in $\tilde{\mathrm{O}}(\ell^2 \log q) = \tilde{\mathrm{O}}(\ell^3 \log p)$ time. By Lemma 2.3 and the Chinese remainder theorem, to reconstruct $P_i(X) \in \mathbb{Q}[X]$ it suffices to compute $P_i(X) \bmod p$ for primes p bounded above by $\mathrm{O}(\ell^2)$. So the complexity of computing $P_i(X)$ is

$$\sum_{\text{prime } p \leqslant \mathrm{O}(\ell^2)} \mathrm{O}(\log^\omega p) + \tilde{\mathrm{O}}(\ell^4 \log^2 p) + \tilde{\mathrm{O}}(\ell^3 \log p) = \tilde{\mathrm{O}}(\ell^6). \tag{2.8}$$

https://doi.org/10.1112/S1461157014000205 Published online by Cambridge University Press

REMARK 3. (1) The complexity of computing zeta functions of $C/\mathbb{F}_p$ for primes p in $\mathrm{O}(\ell^2)$ is $\mathrm{O}(\ell^2 \log^{\omega} \ell)$, which becomes a minor term in the overall complexity of computing $P_i(X)$. Therefore, as mentioned above, the explicit value of the constant ω is not required.

(2) If ℓ is inert in K_f, then the reduction of f modulo the prime ideal (ℓ) gives a representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_{\ell^2})$. And the two-dimensional $\mathbb{F}_{\ell^2}$-vector space $\mathrm{Jac}(C)[\ell]$ realizes ρ.

(3) Similarly, we can compute a polynomial $Q_i(X)$ of degree $\ell+1$ describing the projective representation $\tilde{\rho}_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell) \twoheadrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)$, where $Q_i(X)$ is defined as

$$Q_i(X) = \prod_{L \in \mathbb{P}^1(V_i(\overline{\mathbb{Q}}))} \left(X - \sum_{D \in L \setminus \{0\}} \iota(D) \right), \quad i = 1, 2. \tag{2.9}$$

Similar to Lemma 2.3, the logarithmic heights of coefficients of $Q_i(X)$ are bounded above by $\mathrm{O}(\ell^2)$. It turns out that these polynomials can be reduced to polynomials with small coefficients; see Table 2 (a reduced polynomial for $Q_i(X)$ is denoted by $Q_{\ell,i}^{\mathrm{red}}(x)$).

We are mainly interested in the image of Frobenius elements in the Galois group. The following theorem [**5**, Theorem 1.1] will help us in determining the matrix $\rho_i(\mathrm{Frob}_p)$.

THEOREM 2.4. *Let K be a global field and $f(x) \in K[x]$ a separable polynomial with Galois group G and roots $a_1, \ldots, a_n$ in some splitting field. There is a polynomial $h(x) \in K[x]$ and polynomials $\Gamma_C \in K[X]$ indexed by the conjugacy classes C of G, defined as*

$$\Gamma_C(X) = \prod_{\sigma \in C} \left(X - \sum_{j=1}^{n} h(a_j)\sigma(a_j) \right),$$

such that

$$\mathrm{Frob}_\wp \in C \iff \Gamma_C\left(\mathrm{Tr}_{\frac{\mathbb{F}_q[x]}{f(x)}/\mathbb{F}_q}(h(x)x^q) \right) = 0 \mod \wp$$

for almost all primes $\wp$ of K, where $\mathbb{F}_q$ is the residue field at $\wp$.

The 'almost all primes' in the theorem are those not dividing the denominators of the coefficients of f, its leading coefficient and the resultants of $\Gamma_C(X)$ and $\Gamma_{C'}(X)$ for all $C \neq C'$. Usually one can take $h(x) = x^2$; see [**5**].

In our case, for each conjugacy class $C \subset \mathrm{GL}_2(\mathbb{F}_\ell)$ the corresponding polynomial $\Gamma_C(X)$ is defined as

$$\Gamma_C(X) = \prod_{\sigma \in C} \left(X - \sum_{D \in V_i(\overline{\mathbb{Q}}) \setminus \{0\}} h(\iota(D)) \cdot \iota(\sigma(D)) \right). \tag{2.10}$$

We choose a small prime p such that the points of $V_i(\overline{\mathbb{F}}_p)$ are defined over a small extension field $\mathbb{F}_q$ of $\mathbb{F}_p$, and then Hensel lift each $\tilde{\iota}(\tilde{D}) \in \mathbb{F}_q$ for $\tilde{D} \in V_i(\mathbb{F}_q)$ to $\iota(D) \in \mathbb{Q}_q$ with high p-adic precision. Then we can recover $\Gamma_C(X)$ using formula (2.10).

PROPOSITION 2.5. *With notation as above, we assume p, $[\mathbb{F}_q : \mathbb{F}_p]$, $\deg h(X)$ and coefficients of the auxiliary polynomial $h(X)$ are all in $O(1)$. Given $P_i(X) \in \mathbb{Q}[X]$ and $V_i(\mathbb{F}_q)$. Then for any conjugacy class $C \subset \mathrm{GL}_2(\mathbb{F}_\ell)$, the polynomial $\Gamma_C(X) \in \mathbb{Q}[X]$ can be computed in $\tilde{O}(\ell^8)$ time.*

Proof. Similar to the proof of [**19**, Proposition 4.6]. □

https://doi.org/10.1112/S1461157014000205 Published online by Cambridge University Press

DEFINITION 2. Fixing an auxiliary polynomial $h(x)$, a representation datum for ρ_i is defined as

$$S_i(\ell) := \{\mathfrak{l}_i, P_i(X), \Gamma_C(X) \text{ for all conjugacy classes } C \subset \mathrm{GL}_2(\mathbb{F}_\ell)\}, \quad i = 1, 2.$$

Similarly, a representation datum for $\tilde{\rho}_i$ is defined as

$$\tilde{S}_i(\ell) := \{\mathfrak{l}_i, Q_i(X), \Gamma_C(X) \text{ for all conjugacy classes } C \subset \mathrm{PGL}_2(\mathbb{F}_\ell)\}, \quad i = 1, 2.$$

There are $\ell^2 - 1$ conjugacy classes in $\mathrm{GL}_2(\mathbb{F}_\ell)$. So the complexity of computing each datum $S_i(\ell)$ is

$$\tilde{\mathrm{O}}(\ell^6) + (\ell^2 - 1) \cdot \tilde{\mathrm{O}}(\ell^8) = \tilde{\mathrm{O}}(\ell^{10}). \tag{2.11}$$

Let m be a generator for the maximal order of K_f ($m = (1+\sqrt{d})/2$ if $d = 1 \bmod 4$, $m = \sqrt{d}$ otherwise), then the pth coefficient a_p of f can be written as $a_p = a + bm$ with $a, b \in \mathbb{Z}$. We can determine $a \bmod \ell, b \bmod \ell$ easily using the data $S_1(\ell)$ and $S_2(\ell)$.

2.3. *Verification of projective representation datum*

Recall that the logarithmic heights of coefficients of $Q_i(X)$ are bounded above by $\mathrm{O}(\ell^2)$. However, the implied constant is not given. We should prove that the polynomial recovered from $Q_i(X) \bmod p$ for small primes p is indeed correct. More precisely, let $\tilde{S}_i(\ell)$ be a projective representation datum for $\tilde{\rho}_i$. We would like to verify that the projective representation given by $\tilde{\rho}_i' : \mathrm{Gal}(Q_i(X)) \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)$ is isomorphic to $\tilde{\rho}_i : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$ given by the newform f_i. This is accomplished by using Serre's conjecture on modular forms.

Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ be an irreducible Galois representation and V a two-dimensional $\mathbb{F}_\ell$-vector space realizing ρ. The Serre level $N(\rho)$ of ρ is defined as

$$N(\rho) = \prod_{p \neq \ell} p^{n(p,\rho)}. \tag{2.12}$$

The exponent $n(p, \rho)$ is defined as

$$n(p, \rho) = \sum_{i=0}^{\infty} \frac{\dim(V/V_i)}{[\rho(G_0) : \rho(G_i)]}, \tag{2.13}$$

where G_i is the ith ramification group of the fixed field $\overline{\mathbb{Q}}^{\ker \rho}$ at p and V_i is the subspace of V fixed by $\rho(G_i)$. It is easy to see that $n(p, \rho) = 0$ if and only if $V_0 = V$ (ρ is unramified at p) and $n(p, \rho) = \dim(V/V_0)$ if and only if $V_1 = V$ (ρ is tamely ramified at p).

The Serre weight $k(\rho)$ is defined in terms of the local representation $\rho|_{D_\ell}$, where D_ℓ is the decomposition group of $\overline{\mathbb{Q}}^{\ker \rho}$ at ℓ. See [7] for the explicit definition.

Let $\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$ be the projective representation associated to ρ. By Tate's lifting theorem, there exists a lifting ρ' of $\tilde{\rho}$ with minimal Serre weight and minimal Serre level as well. The Serre weight $k(\tilde{\rho})$ and Serre level $N(\tilde{\rho})$ of $\tilde{\rho}$ are defined to be $k(\rho')$ and $N(\rho')$, respectively.

If ρ is wildly ramified at ℓ, a theorem of Moon and Taguchi [11] relates $k(\rho)$ to the discriminant of certain number field. The following proposition can be found in [6, Chapter 7].

PROPOSITION 2.6. *Let $\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$ be an irreducible projective representation that is wildly ramified at ℓ. Take a point in $\mathbb{P}^1(\mathbb{F}_\ell)$, let $H \subset \mathrm{PGL}_2(\mathbb{F}_\ell)$ be its stabilizer subgroup and let K be the number field defined as*

$$K = \overline{\mathbb{Q}}^{\tilde{\rho}^{-1}(H)}.$$

https://doi.org/10.1112/S1461157014000205 Published online by Cambridge University Press

Let $k \geqslant 1$ be an integer. Then

$$k(\tilde{\rho}) = k \iff v_\ell(\mathrm{Disc}K/\mathbb{Q}) = k + \ell - 2.$$

It would be nice to have similar results for the Serre level $N(\tilde{\rho})$. In one direction, we have the following result [**3**, Proposition 2].

PROPOSITION 2.7. *Let $\mathbb{F}/\mathbb{F}_\ell$ be a finite extension and $\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F})$ a projective representation with $\mathrm{im}(\tilde{\rho}) \supset \mathrm{PSL}_2(\mathbb{F})$ and let K be the number field defined as Proposition 2.6 with constant field $\mathbb{F}_\ell$ replaced by $\mathbb{F}$. Let $p \neq \ell$ be a prime above which $K/\mathbb{Q}$ is at most tamely ramified. Then the valuation $v_p(N(\tilde{\rho}))$ is at most 2 and can be expressed as follows:*

$$v_p(N(\tilde{\rho})) = \begin{cases} 0, & \text{if } K \text{ is unramified at } p, \\ 1, & \text{if } K \text{ is ramified at } p \text{ but also has an unramified prime above } p, \\ 2, & \text{if } K \text{ has no unramified prime above } p. \end{cases}$$

In the other direction, we prove that, in some cases, the valuation of the discriminant of K at prime $p|N(\tilde{\rho})$ is equal to $\ell - 1$. More precisely, we have the following result.

PROPOSITION 2.8. *Let $\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$ be a projective representation with $\mathrm{im}(\tilde{\rho}) \supset \mathrm{PSL}_2(\mathbb{F}_\ell)$ and $\det(\tilde{\rho})|_{D_p}$ be unramified at prime $p \neq \ell$, where D_p is the decomposition group of $\overline{\mathbb{Q}}^{\ker\tilde{\rho}}$ at p. Let K be the number field defined as Proposition 2.6. Then*

$$v_p(N(\tilde{\rho})) = 1 \Rightarrow v_p(\mathrm{Disc}(K/\mathbb{Q})) = \ell - 1 \quad \text{and} \quad (p) = \wp_1^\ell \cdot \wp_2,$$

where $\wp_1$ and $\wp_2$ are two different prime ideals of K.

Note that the condition that $\det(\tilde{\rho})|_{D_p}$ is unramified at prime $p \neq \ell$ is equivalent to requiring that the modular form corresponding to $\tilde{\rho}$ has trivial Nebentypus. To prove Proposition 2.8, we first prove a lemma on the order of $\tilde{\rho}(I_p)$.

LEMMA 2.9. *Let $\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$ be a projective representation and $\det(\tilde{\rho})|_{D_p}$ be unramified at prime $p \neq \ell$. Then $\tilde{\rho}(I_p)$ is unipotent and non-trivial if and only if $v_p(N(\tilde{\rho})) = 1$.*

Proof. If $\tilde{\rho}(I_p)$ is unipotent and non-trivial then $\tilde{\rho}(I_p) = \left\langle \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \right\rangle$. Let $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_\ell)$ be a Tate lifting of $\tilde{\rho}$ with $\rho(I_p) = \tilde{\rho}(I_p)$. Then $n(p, \rho) = 1$ follows easily by (2.13). Since $\tilde{\rho}$ is ramified at p, we have that $v_p(N(\tilde{\rho})) \geqslant 1$. By the definition of $N(\tilde{\rho})$, we have $v_p(N(\tilde{\rho})) = 1$.

If $v_p(N(\tilde{\rho})) = 1$, then a Tate lifting ρ of $\tilde{\rho}$ with $n(\rho, p) = 1$ satisfies $\dim V_0 = 1$ and $V_1 = V$, where V is a representation for ρ and V_i, $i \geqslant 0$, are defined as before. So $\rho(I_p)$ has the form $\left\langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \right\rangle$ or $\left\langle \left(\begin{smallmatrix} 1 & 0 \\ 0 & x \end{smallmatrix}\right) \right\rangle$ with $1 \neq x \in \mathbb{F}_\ell^\times$. Since $\det(\tilde{\rho})|_{D_p}$ is unramified, we have that $\det(\rho)|_{D_p}$ is unramified as well, that is, $\det(\rho)|_{I_p} = 1$. Hence we have $\rho(I_p) = \left\langle \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \right\rangle$, so $\tilde{\rho}(I_p)$ is unipotent and non-trivial. □

Proof of Proposition 2.8. Let $L := \overline{\mathbb{Q}}^{\ker\tilde{\rho}}$ be the number field cut out by $\tilde{\rho}$. Then L is the normal closure of K. By the lemma above, $\tilde{\rho}(I_p)$ is unipotent of order ℓ, so p is tamely ramified in L with ramification index equal to ℓ. Since L is the normal closure of K, the prime p is ramified (tamely) in K as well. Write its prime ideal factorization as $(p) = \prod_{i=1}^g \wp_i^{e_i}$.

https://doi.org/10.1112/S1461157014000205 Published online by Cambridge University Press

Then e_i divides ℓ and there exists at least one e_i greater than 1. On the other hand, we have $\sum_{i=1}^{g} e_i \cdot f_i = [K:\mathbb{Q}] = \ell + 1$, where f_i is the residue degree of $\wp_i$. Hence the factorization must be of the form $(p) = \wp_1^{\ell} \cdot \wp_2$, with $f_1 = f_2 = 1$. Since K is tamely ramified at p, the valuation of $\mathrm{Disc}(K/\mathbb{Q})$ at p is equal to $(\ell+1) - (f_1 + f_2) = \ell - 1$. □

Combining the relation between $k(\tilde{\rho})$ and $v_\ell(\mathrm{Disc}(K/\mathbb{Q}))$, we have the following theorem.

THEOREM 2.10. *Let $N > 1$ be a square-free integer, $k \geqslant 2$ an even integer and $\ell \geqslant k-1$ an odd prime not dividing N. Let $\tilde{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$ be a projective representation wildly ramified at ℓ with $\mathrm{im}(\tilde{\rho}) \supset \mathrm{PSL}_2(\mathbb{F}_\ell)$ and $\det(\tilde{\rho})|_{D_p}$ be unramified at prime $p|N$. Then $\tilde{\rho}$ is odd with $k(\tilde{\rho}) = k$ and $N(\tilde{\rho}) = N$ if and only if K is not totally real with discriminant $\mathrm{Disc}(K/\mathbb{Q}) = (-1)^{(\ell-1)/2} \cdot \ell^{k+\ell-2} \cdot N^{\ell-1}$ and each prime p dividing N can be factored as $(p) = \wp_1^{\ell} \cdot \wp_2$ in K with $\wp_1 \neq \wp_2$.*

Proof. Here, we say that a projective representation $\tilde{\rho}$ is odd if $\tilde{\rho}(c)$ is non-scalar, where c is the complex conjugation. It can be easily checked that $\tilde{\rho}$ is odd if and only if each Tate lifting of $\tilde{\rho}$ is odd.

By Propositions 2.6–2.8, we have

$$k(\tilde{\rho}) = k \quad \text{and} \quad N(\tilde{\rho}) = N,$$

if and only if

$$|\mathrm{Disc}(K/\mathbb{Q})| = \ell^{k+\ell-2} \cdot N^{\ell-1} \text{ and } (p) = \wp_1^{\ell} \cdot \wp_2 \text{ with } \wp_1 \neq \wp_2 \text{ for all } p|N.$$

Therefore, it remains to check that $\tilde{\rho}$ is odd if and only if K is not totally real and the sign of $\mathrm{Disc}(K/\mathbb{Q})$ is $(-1)^{(\ell-1)/2}$.

Now, assume $\tilde{\rho}$ is odd. Then up to conjugation, we have $\tilde{\rho}(c) = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, the orbits of $\tilde{\rho}(c)$ on $\mathbb{P}^1(\mathbb{F}_\ell)$ have length $\{1, 1, 2, \ldots, 2\}$, that is, K has two real embeddings and $\ell - 1$ complex embeddings.

Conversely, if K is not totally real, then $\tilde{\rho}(c)$ is non-scalar, so $\tilde{\rho}$ is odd. □

REMARK 4. If $k \geqslant 3$, then $v_\ell(\mathrm{Disc}(K/\mathbb{Q})) = k + \ell - 2$ implies the assumption, that is, $\tilde{\rho}$ is wildly ramified at ℓ. However, if $k = 2$, we need to consider the factorization of (ℓ) in K to check this assumption. In this case, assume K is given by $\mathbb{Q}[x]/(P(x))$ and $v_\ell(\mathrm{Disc}(P(x))) = v_\ell(\mathrm{Disc}(K/\mathbb{Q})) = \ell$. Then the assumption can be verified by considering the factorization of $P(x)$ over $\mathbb{F}_\ell[x]$.

Now, let $\tilde{S}_i(\ell)$ be a projective representation datum for $\tilde{\rho}_i$. We first compute the Galois group of the polynomial $Q_i(X) \in \tilde{S}_i(\ell)$ using Magma [1]. This establishes an embedding $\mathrm{Gal}(Q_i(X)) \hookrightarrow \mathrm{PGL}_2(\mathbb{F}_\ell)$ and defines a projective representation $\tilde{\rho}_i' : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_\ell)$. Then we use Theorem 2.10 to determine $k(\tilde{\rho}_i')$ and $N(\tilde{\rho}_i')$. It turns out that $\tilde{\rho}_i'$ is surjective for each case in Table 1 and $k(\tilde{\rho}_i') = 2$, $N(\tilde{\rho}_i') = 191$ as expected. By Serre's conjecture on modular forms, there exists a newform g_i of weight $k(\tilde{\rho}_i')$ and level $N(\tilde{\rho}_i')$ with projective representation $\tilde{\rho}_i'$. Using Sturm's bound (see [15]), g_i is determined by its first few coefficients, which can be computed using $\tilde{S}_i(\ell)$ as well. The last step of the verification process is to verify that g_i is congruent to the original newform f_i.

3. *Applications*

Let A_f be the abelian surface attached to a newform $f \in S_2(\Gamma_0(N))$. Let p be a prime such that A_f has good reduction at p. The characteristic polynomial of a Frobenius element Frob_p

https://doi.org/10.1112/S1461157014000205 Published online by Cambridge University Press

on A_f is

$$P(t) = (t^2 - a_p \cdot t + p)(t^2 - \sigma(a_p) \cdot t + p),$$

where $\sigma \in \mathrm{Gal}(K_f/\mathbb{Q})$ is the non-identity element. Since $|A_f(\mathbb{F}_p)| = P(1)$, to count the number of points on $A_f(\mathbb{F}_p)$ it suffices to compute the pth Fourier coefficient of f, and this can be reduced to computing the mod-ℓ Galois representations associated to $\mathrm{Jac}(C)$.

ALGORITHM 1. Counting points on modular abelian surface.
Input: A normalized newform $f \in S_2(\Gamma_0(N))$ with $K_f = \mathbb{Q}(\sqrt{d})$ (d square-free), hyperelliptic curve $C : y^2 = F(x)$ for A_f and a prime number p.
Output: $|A_f(\mathbb{F}_p)|$.

1. Enumerate the first n primes ℓ_j such that $(d/\ell_j) = 1$, $1 \leqslant j \leqslant n$, and $\prod_{j=1}^{n} \ell_j > c\sqrt{p}$, where the constant $c = 4(1 + 1/\sqrt{d})$ if $d \equiv 1 \bmod 4$ and $c = 4$ otherwise. Set $\mathcal{M} = \emptyset$.
2. Compute the representation datum $S_i(\ell_j)$ for $1 \leqslant j \leqslant n$, $i = 1, 2$.
3. For each datum $S_i(\ell_j)$, compute the trace $t_i = \mathrm{Tr}_{\mathbb{F}_p[x]/P_i(x)}(x^{p+2}), P_i(X) \in S_i(\ell_j)$. Find the polynomial $\Gamma_{C_i}(X) \in S_i(\ell_j)$ such that $\Gamma_{C_i}(t_i) \bmod p = 0$. Set $\mathcal{M} := \mathcal{M} \cup \{(\ell_j, C_i)\}$.
4. Reconstruct $a_p \in K_f$ from $\mathcal{M}$ by the Chinese remainder theorem.
5. Output $P(1) = (p + 1 - a_p) \cdot (p + 1 - \sigma(a_p))$.

Notice that the auxiliary polynomial for the representation datum is set to be $h(x) = x^2$. Asymptotically, half of all primes ℓ satisfy $(d/\ell) = 1$. So all primes ℓ_j found in Step 1 are bounded above by $\tilde{\mathrm{O}}(\log p)$. Each representation datum $S_i(\ell_j)$ can be computed in $\tilde{\mathrm{O}}(\ell_j^{10})$ time. Hence Step 2 can be completed in

$$\sum_{\ell_j \leqslant \tilde{\mathrm{O}}(\log p)} \tilde{\mathrm{O}}(\ell_j^{10}) = \tilde{\mathrm{O}}(\log^{11} p)$$

time. The complexity of computing $x^{p+2} \in \mathbb{F}_p[x]/P_i(x)$ is $\tilde{\mathrm{O}}(\ell_j^2 \log^2 p)$ ($\tilde{\mathrm{O}}(\log p)$ multiplications in a finite field of degree $\leqslant \ell_j^2 - 1$) and its trace can be computed in time $\tilde{\mathrm{O}}(\ell_j^2 \log^2 p)$ as well. It takes $\tilde{\mathrm{O}}(\ell_j^2 \log p)$ to compute a single $\Gamma_C(t_i) \bmod p$, and the one with zero value can be found after at most $\ell_j + 2$ attempts. Therefore it takes $\tilde{\mathrm{O}}(\ell_j^3 \log p)$ to find the conjugacy class C_i. In summary, Step 3 takes

$$\sum_{1 \leqslant j \leqslant n} \tilde{\mathrm{O}}(\ell_j^2 \log^2 p) + \tilde{\mathrm{O}}(\ell_j^3 \log p) = \tilde{\mathrm{O}}(\log^5 p).$$

Since the representation datum can be used to compute $A_f(\mathbb{F}_{p'})$ for primes $p' \leqslant p$ as well, Step 2 can be viewed as a precomputation. Then we have an algorithm of complexity $\tilde{\mathrm{O}}(\log^5 p)$ for counting points on a special class of modular abelian surfaces.

REMARK 5. The computation of representation data is rather time-consuming, but once we have these data, it is straightforward to obtain the zeta functions of $C/\mathbb{F}_p$ for primes p. There are Schoof-type point-counting algorithms for general curves over $\mathbb{F}_p$ of genus 2 with complexity $\tilde{\mathrm{O}}(\log^8 p)$. If, in addition, the curves have explicit and efficient real multiplication then the complexity can be reduced to $\tilde{\mathrm{O}}(\log^5 p)$; see [13, 14]. Compared with these methods, the main advantage of our approach is that we do not need to assume the efficiently computable of certain $\phi \in \mathrm{End}(\mathrm{Jac}(C))$ on generic elements of $\mathrm{Jac}(C)$, and our approach can be easily generalized to higher-genus cases.

https://doi.org/10.1112/S1461157014000205 Published online by Cambridge University Press

In fact, while computing the representation datum $S_i(\ell)$, we can use a modular symbol algorithm for computing coefficients of modular forms to compute the zeta function for $C/\mathbb{F}_p$, with a complexity polynomial in p. We can use general algorithms for function fields to perform addition in $\mathrm{Jac}(C)(\mathbb{F}_q)$. Therefore, even for higher-genus cases, the representation datum $S_i(\ell)$ can be computed in time polynomial in ℓ. Similarly, the zeta function for $C/\mathbb{F}_p$ can be computed easily from $S_i(\ell)$ for sufficiently many small primes ℓ.

Let $f \in S_2(\Gamma_0(191))$ be the newform as in Example 1. The first five primes split in $K_f = \mathbb{Q}(\sqrt{5})$ are 11, 19, 29, 31 and 41. For each $\ell \in \{11, 19, 29, 31, 41\}$, denote by $(\ell) = \mathfrak{l}_1 \cdot \mathfrak{l}_2$ its prime decomposition. The first few coefficients of $\tilde{f}_i := f \bmod \mathfrak{l}_i$ are listed in Table 1. The entry corresponding to each $Q_i(X)$ ($P_i(X)$) is the number of decimal digits of the maximal coefficient of $Q_i(X)$ ($P_i(X)$). The reduction of each $Q_i(X)$ to a polynomial $Q_{\ell,i}^{\mathrm{red}}(x)$ with small coefficients is listed in Table 2. Using this much simpler polynomial $Q_{\ell,i}^{\mathrm{red}}(x)$, we can compute the maximal order of number field $K_{\ell,i} := \mathbb{Q}[x]/(Q_{\ell,i}^{\mathrm{red}}(x))$. Its discriminant is listed in Table 1 as well.

We take $p = 2^{38} + 2^{34} + 6713075$ for example. Since $11 \cdot 19 \cdot 29 \cdot 31 \cdot 41 > 4 \cdot (1 + 1/\sqrt{5}) \cdot \sqrt{p}$, we can recover a_p from $a_p \bmod \ell$ for $\ell \in \{11, 19, 29, 31, 41\}$ by the Chinese remainder theorem, which is $a_p = 374306 - 146389 \cdot ((-1 + \sqrt{5})/2)$. So the characteristic polynomial of Frob_p on A_f is

$$\begin{aligned} P(t) &= (t^2 - a_p t + p) \cdot (t^2 - \sigma(a_p) t + p) \\ &= t^4 - 895001 \cdot t^3 + 757598501755 \cdot t^2 \\ &\quad - 261398009901174203 \cdot t + 85301665853409303575209. \end{aligned} \tag{3.1}$$

As a consequence, we have $|A_f(\mathbb{F}_p)| = P(1) = 85301404456157000007761 \approx 2^{76}$, which is a prime.

TABLE 1. *Summary of representation data for ρ_i.*

ℓ	$\tilde{f}_i$	$Q_i(X)$	$P_i(X)$	$\mathrm{Disc}(K_{\ell,i})$	$\tilde{a}_{p,i}$	$a_p \bmod \ell$
11	$q + 7q^2 + 10q^3 + \ldots$	17	102	$-11^{11} \cdot 191^{10}$	7	$9 + 10 \cdot ((-1 + \sqrt{5})/2)$
	$q + 3q^2 + 10q^3 + \ldots$	15	87	$-11^{11} \cdot 191^{10}$	3	
19	$q + 14q^2 + 18q^3 + \ldots$	47	275	$-19^{19} \cdot 191^{18}$	14	$6 + 6 \cdot ((-1 + \sqrt{5})/2)$
	$q + 4q^2 + 18q^3 + \ldots$	48	276	$-19^{19} \cdot 191^{18}$	4	
29	$q + 23q^2 + 28q^3 + \ldots$	99	639	$29^{29} \cdot 191^{28}$	23	$3 + 3 \cdot ((-1 + \sqrt{5})/2)$
	$q + 5q^2 + 28q^3 + \ldots$	100	641	$29^{29} \cdot 191^{28}$	5	
31	$q + 18q^2 + 30q^3 + \ldots$	111	740	$-31^{31} \cdot 191^{30}$	18	$12 + 24 \cdot ((-1 + \sqrt{5})/2)$
	$q + 12q^2 + 30q^3 + \ldots$	109	730	$-31^{31} \cdot 191^{30}$	12	
41	$q + 34q^2 + 40q^3 + \ldots$	181	1289	$41^{41} \cdot 191^{40}$	34	$17 + 22 \cdot ((-1 + \sqrt{5})/2)$
	$q + 6q^2 + 40q^3 + \ldots$	180	1293	$41^{41} \cdot 191^{40}$	6	

https://doi.org/10.1112/S1461157014000205 Published online by Cambridge University Press

TABLE 2. *Polynomials corresponding to projective representations.*

$Q^{\mathrm{red}}_{11,1}(x)$	$x^{12} - 2x^{11} + 99x^{10} + 1496x^9 - 7161x^8 - 77660x^7 + 535128x^6$ $- 1759912x^5 + 9071854x^4 - 29111269x^3 + 35167605x^2 - 118403833x + 283431617$
$Q^{\mathrm{red}}_{11,2}(x)$	$x^{12} - 4x^{11} - 11x^{10} - 484x^9 - 165x^8 + 215666x^7 + 1463286x^6 + 16446562x^5$ $+ 45871815x^4 + 171307389x^3 + 360521777x^2 + 765979601x + 372355371$
$Q^{\mathrm{red}}_{19,1}(x)$	$x^{20} - 9x^{19} - 361x^{18} + 7068x^{17} - 52288x^{16} + 697851x^{15} + 9227673x^{14}$ $- 984175566x^{13} + 22938549919x^{12} - 156485353104x^{11} - 283331301915x^{10}$ $- 5671765761816x^9 + 139391174142417x^8 - 491377289503645x^7 + 1223873060235593x^6$ $- 1559067235168012x^5 + 2162497369354741 4x^4 + 8859188863932123x^3$ $+ 350580422723685512x^2 + 3513186138698590635x - 20425396511439477376$
$Q^{\mathrm{red}}_{19,2}(x)$	$x^{20} - 7x^{19} - 323x^{18} + 11039x^{17} - 50350x^{16} + 981407x^{15} - 13332338x^{14} - 163266905x^{13}$ $+ 5247983350x^{12} - 148140809984x^{11} + 2184669800102x^{10} - 2498380187197x^9$ $- 247124344515040x^8 + 3667970283360225x^7 - 23893750621974781x^6$ $+ 88140463317813945x^5 - 609337375211152 57x^4 - 374960886922014111x^3$ $+ 1527817807625237133x^2 + 3080602038292235873x + 2159967343611754103$

Acknowledgement. I would like to thank the referees for their constructive comments and helpful suggestions.

References

1. W. BOSMA, J. CANNON and C. PLAYOUST, 'The Magma algebra system I: The user language', *J. Symbolic Comput.* 24 (1997) no. 3–4, 235–265.
2. J. BOSMAN, 'Explicit computations with modular Galois representations', PhD Thesis, Universiteit Leiden, December 2008, available at https://openaccess.leidenuniv.nl/.
3. J. BOSMAN, 'Modular forms applied to the computational inverse Galois problem', Preprint, 2011, arXiv:1109.6879v1 [math.NT].
4. M. DERICKX, M. VAN HOEIJ and J. ZENG, 'Computing Galois representations and equations for modular curves $X_H(\ell)$', Preprint, 2013, arXiv:1312.6819v1 [math.NT].
5. T. DOKCHITSER and V. DOKCHITSER, 'Identifying Frobenius elements in Galois groups', *Algebra Number Theory* 7 (2013) no. 6, 1325–1352.
6. S. J. EDIXHOVEN and J.-M. COUVEIGNES, *Computational aspects of modular forms and Galois representations*, Annals of Mathematical Studies 176 (Princeton University Press, 2011) (with R. S. de Jong, F. Merkl and J. G. Bosman).
7. S. J. EDIXHOVEN, 'The weight in Serres conjectures on modular forms', *Invent. Math.* 109 (1992) no. 3, 563–594.
8. E. GONZÁLEZ-JIMÉNEZ and J. GONZÁLEZ, 'Modular curves of genus 2', *Math. Comp.* 72 (2003) no. 241, 397–418.
9. E. GONZÁLEZ-JIMÉNEZ, J. GONZÁLEZ and J. GUÁRDIA, 'Computations on modular Jacobian surfaces', *Algorithmic number theory*, Lecture Notes in Computer Science 2369 (Springer, Berlin, 2002) 189–197.
10. N. MASCOT, 'Computing modular Galois representations', *Rend. Circ. Mat. Palermo* (2) 62 (2013) 451–476.
11. H. MOON and Y. TAGUCHI, 'Refinement of Tate's discriminant bound and non-existence theorems for mod p Galois representations', *Doc. Math. Extra Volume Kato* (2003) 641–654.
12. F. OORT and K. UENO, 'Principally polarized abelian varieties of dimension two or three are Jacobian varieties', *J. Fac. Sci. Univ. Tokyo, Sec. IA* 20 (1973) 377–381.
13. P. GAUDRY and É. SCHOST, 'Modular equations for hyperelliptic curves', *Math. Comp.* 74 (2005) no. 249, 397–418.
14. P. GAUDRY, D. KOHEL and B. SMITH, 'Counting points on genus 2 curves with real multiplication', *Advances in Cryptology-Asiacrypt 2011*, Lecture Notes in Computer Science 7073 (eds D. H. Lee and H. Wang; Springer, Berlin, 2011) 504–519.

https://doi.org/10.1112/S1461157014000205 Published online by Cambridge University Press

15. J. Sturm, 'On the congruence of modular forms', *Number theory (New York, 1984–1985)*, Lecture Notes in Mathematics 1240 (Springer, Berlin, 1987) 275–280.
16. P. Tian, 'Further computations of Galois representations associated to modular forms', Preprint, 2013, arXiv:1311.0577v1 [math.NT].
17. Y. Uchida, 'Canonical local heights and multiplication formulas for the Jacobians of curves of genus 2', *Acta Arith.* 149 (2011) 111–130.
18. A. Weil, 'Zum Beweis des Torellischen Satzes', *Nachr. Akad. Wiss. Göttingen Math.-Phys. Kl.* (1957) 33–53.
19. J. Zeng and L. Yin, 'On the computation of coefficients of modular forms: the reduction modulo p approach', *Math. Comp.*, to appear.

Jinxiang Zeng
Department of Mathematical Sciences
Tsinghua University
Beijing 100084
PR China

cengjx09@mails.tsinghua.edu.cn

https://doi.org/10.1112/S1461157014000205 Published online by Cambridge University Press