COMPUTING ACTIONS ON CUSP FORMS

DAVID ZYWINA

ABSTRACT. For positive integers k and N, we describe how to compute the natural action of $\mathrm{SL}_2(\mathbb{Z})$ on the space of cusp forms $S_k(\Gamma(N))$, where a cusp form is given by sufficiently many terms of its q-expansion. This will reduce to computing the action of the Atkin–Lehner operator on $S_k(\Gamma)$ for a congruence subgroup $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$. Our motivating application of such fundamental computations is to compute explicit models of some modular curves X_G.

1. INTRODUCTION

Fix positive integers k and N, and a congruence subgroup $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$. Let $S_k(\Gamma)$ and $M_k(\Gamma)$ be the space of cusp forms and modular forms, respectively, of weight k with respect to Γ. In this article we explain how one can explicitly compute the action of the Atkin–Lehner involution W_N on $S_k(\Gamma)$ and $M_k(\Gamma)$, where we view a modular form as being given by its q-expansion with enough terms known to uniquely determine it (given k and Γ). In §1.4, we will explain how this allows us to compute the natural right action of $\mathrm{SL}_2(\mathbb{Z})$ on $S_k(\Gamma(N))$. In §1.5, we give an application to computing models of modular curves. In §1.7, we recall some related results.

1.1. **Background and notation.** We recall some basic definitions and conventions. Fix a positive integer k.

The group $\mathrm{GL}_2^+(\mathbb{R})$ of 2×2 real matrices with positive determinant acts on the complex upper half plane $\mathfrak{H}$ by linear fractional transformations. For a function $f\colon \mathfrak{H} \to \mathbb{C}$ and a matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{R})$, we define the function $f|_k\gamma\colon \mathfrak{H} \to \mathbb{C}, \tau \mapsto \det(\gamma)^{k/2}(c\tau + d)^{-k} f(\gamma\tau)$. We will simply write $f|\gamma$ when k is fixed or clear from context. We have $f|(\gamma\gamma') = (f|\gamma)|\gamma'$ for all $\gamma, \gamma' \in \mathrm{GL}_2^+(\mathbb{R})$.

For a congruence subgroup Γ, we denote the space of cusp and modular forms by $S_k(\Gamma)$ and $M_k(\Gamma)$, respectively. They consist of holomorphic functions $f\colon \mathfrak{H} \to \mathbb{C}$ that satisfy $f|\gamma = f$ for all $\gamma \in \Gamma$ along with usual conditions at the cusps. Let w be the width of the cusp of Γ at ∞, i.e., the smallest positive integer $w \geq 1$ for which $\left(\begin{smallmatrix} 1 & w \\ 0 & 1 \end{smallmatrix}\right)$ lies in Γ. For each modular form $f \in M_k(\Gamma)$, we have

$$f(\tau) = \sum_{n=0}^{\infty} a_n(f)\, q_w^n$$

for unique $a_n(f) \in \mathbb{C}$, where $q_w := e^{2\pi i\tau/w}$; this is the Fourier series or q-expansion of f. When $w = 1$, we will simply write q for q_1. For a subring of R of $\mathbb{C}$, we denote by $M_k(\Gamma, R)$ and $S_k(\Gamma, R)$ the R-module consisting of modular forms f in $M_k(\Gamma)$ and $S_k(\Gamma)$, respectively, for which all of the coefficients $a_n(f)$ lie in R.

Fix a positive integer N and a congruence subgroup $\Gamma_0(N) \subseteq \Gamma \subseteq \Gamma_1(N)$. Since the matrix $\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ normalizes Γ, we obtain an automorphism

$$M_k(\Gamma) \xrightarrow{\sim} M_k(\Gamma), \quad f \mapsto N^{k/2} \cdot f|\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right) =: f|W_N$$

which we will call the Atkin–Lehner operator of $M_k(\Gamma)$. We have $(f|W_N)(\tau) = \tau^{-k} f(-1/(N\tau))$ and

$$(f|W_N)|W_N = (-1)^k N^k \cdot f.$$

Note that the subspace $S_k(\Gamma)$ is stable under the action of W_N.

Date: February 2, 2021.

2010 *Mathematics Subject Classification.* Primary 11F11; Secondary 11G18.

Remark 1.1. In the literature, our operator W_N is often scaled by a factor of $N^{-k/2}$; in particular, it would then be an involution when k is even. Our version has nicer arithmetic properties when k is odd. For example, $M_k(\Gamma_0(N), \mathbb{Q})$ is always stable under the action of W_N using our normalization.

For $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, the diamond operator $\langle d \rangle$ acts on $M_k(\Gamma)$ and $S_k(\Gamma)$; we have $f|\langle d \rangle := f|\gamma$, where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is any matrix satisfying $\gamma \equiv \left(\begin{smallmatrix} d^{-1} & * \\ 0 & d \end{smallmatrix}\right) \pmod N$.

Take any automorphism σ of the field $\mathbb{C}$ and any modular form $f \in M_k(\Gamma(N))$. Let $\sigma(f)$ be the modular form in $M_k(\Gamma(N))$ whose q-expansion is obtained by applying σ to the coefficients of the q-expansion of f. This defines an action of $\mathrm{Aut}(\mathbb{C})$ on $M_k(\Gamma(N))$. The subspaces $M_k(\Gamma)$ and $S_k(\Gamma)$ are stable under the action of $\mathrm{Aut}(\mathbb{C})$, where $\Gamma = \Gamma(N)$ or $\Gamma_0(N) \subseteq \Gamma \subseteq \Gamma_1(N)$.

Finally, for each positive integer N, we define the N-th root of unity $\zeta_N := e^{2\pi i/N} \in \mathbb{C}^\times$.

1.2. **Setup.** Fix positive integers k and N. Let $\mathcal{M}$ be a subspace of $M_k(\Gamma_1(N))$. For each subring R of $\mathbb{C}$, we define $\mathcal{M}(R) := \mathcal{M} \cap M_k(\Gamma_1(N), R)$, i.e., the R-submodule of $\mathcal{M}$ consisting of modular forms whose Fourier coefficients all lie in R.

Assume that $\mathcal{M}$ satisfies all the following conditions:

(a) $\mathcal{M}$ is stable under the action of W_N.
(b) $\mathcal{M}$ is stable under the action of the diamond operators $\langle d \rangle$ with $d \in (\mathbb{Z}/N\mathbb{Z})^\times$,
(c) $\mathcal{M}(\mathbb{Z})$ spans $\mathcal{M}$ as a $\mathbb{C}$-vector space,
(d) the $\mathbb{Z}$-module $\mathcal{M}(\mathbb{Z})$ has a basis $f_1, \dots, f_g$, where each f_j is given by its q-expansion for which we can compute an arbitrary number of terms.

By our assumptions, $f_1, \dots, f_g$ is a basis of $\mathcal{M}$. The main goal of this paper is explain how to compute the action of the Atkin–Lehner operator W_N on the space $\mathcal{M}$ with respect to a fixed basis $f_1, \dots, f_g$. Equivalently, we will give an algorithm to compute the unique matrix $W \in \mathrm{GL}_g(\mathbb{C})$ satisfying

$$f_j|W_N = \sum_{k=1}^{g} W_{j,k} \cdot f_k$$

for all $1 \le j \le g$. We will see that all the entries of W lie in the cyclotomic field $\mathbb{Q}(\zeta_N)$.

We are motivated by the following examples of spaces $\mathcal{M}$.

Example 1.2. The spaces $M_k(\Gamma)$ and $S_k(\Gamma)$, where Γ is a congruence subgroup with $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$, satisfy conditions (a)–(d). We shall verify these conditions in §4.

Example 1.3. Fix a newform $f \in S_k(\Gamma_1(N))$ of level N. Let $\mathcal{M}_f$ be the $\mathbb{C}$-subspace of $S_k(\Gamma_1(N))$ generated by $\sigma(f)$ with $\sigma \in \mathrm{Aut}(\mathbb{C})$. In §4.5, we will verify that conditions (a)–(d) hold for $\mathcal{M}_f$. There is a unique $c \in \mathbb{C}$ with absolute value $N^{k/2}$ satisfying

$$f|W_N = c\,\overline{f},$$

where $\overline{f}$ is obtained by applying complex conjugation to the coefficients of the q-expansion of f, cf. Proposition 4.4. After expressing f as a linear combination of the cusp forms $f_1, \dots, f_g$, one can use the matrix W to compute the exact value of c.

1.3. **The algorithm.** Fix notation and assumptions as in §1.2. We now describe our algorithm to compute the matrix W; its validity will be proved in §5. The main idea is to use numerical approximations of W to compute the true value. [1]

For a fixed integer $n \ge 1$, let A be the $g \times n$ matrix satisfying $A_{i,j} = a_{j-1}(f_i)$, where $f_i = \sum_{j=0}^{\infty} a_j(f_i) q^j$. By taking n large enough and using that $f_1, \dots, f_g$ is a basis of $\mathcal{M}(\mathbb{Z})$, we may assume that $A \in M_{g,n}(\mathbb{Z})$ has rank g.

Recall that a matrix in $M_{g,n}(\mathbb{Z})$ is in Hermite normal form if it satisfies all the following conditions:

[1] See http://pi.math.cornell.edu/~zywina/papers/AtkinLehner/ for a basic implementation, in Magma, of the algorithms in this paper.

- it is upper triangular and its zero rows lie below all the non-zero rows,
- the *pivot* in each non-zero row, i.e., the first non-zero entry, is positive and strictly to the right of all pivots in rows that lie above it,
- the entries of the matrix above a pivot are all non-negative and smaller than the pivot.

There is a matrix $U \in \mathrm{SL}_g(\mathbb{Z})$ such that $H := UA$ is in Hermite normal form. The matrix H, though not U, is uniquely determined. With a change of basis of $\mathcal{M}(\mathbb{Z})$ given by U, one could take the basis $f_1, \ldots, f_g$ so that A is in Hermite normal form; this would give a distinguished basis of $\mathcal{M}(\mathbb{Z})$ by the uniqueness of H. We define α to be the product of all the pivots of H.

Let Q be the smallest positive divisor N for which the action of the diamond operators $\langle d \rangle$ on $\mathcal{M}$ depends only on the value of d modulo Q. The diamond operators thus give an action of $(\mathbb{Z}/Q\mathbb{Z})^\times$ on $\mathcal{M}$. For each $d \in (\mathbb{Z}/Q\mathbb{Z})^\times$, let $D_d \in M_g(\mathbb{C})$ be the matrix that satisfies $f_j|\langle d \rangle = \sum_{k=1}^{g} (D_d)_{j,k} \cdot f_k$ for all $1 \leq j \leq g$. Moreover, we will see later that $D_d \in \mathrm{GL}_g(\mathbb{Z})$.

For an integer $0 \leq b \leq \varphi(Q) - 1$, where φ is the Euler totient function, define the matrix

$$\beta_b := W \cdot \sum_{d \in (\mathbb{Z}/Q\mathbb{Z})^\times} \zeta_Q^{db} \, D_d.$$

In §5, we will prove that the matrix W lies in $M_g(\mathbb{Q}(\zeta_Q))$ and satisfies $\mathrm{Tr}_{\mathbb{Q}(\zeta_Q)/\mathbb{Q}}(\zeta_Q^b W) = \beta_b$, where the trace of a matrix is taken entry by entry. In particular, $\beta_b \in M_g(\mathbb{Q})$. Define the integer

$$B_{k,N} := \prod_{p|N} p^{\lceil k/(p-1) \rceil},$$

where $\lceil x \rceil$ denotes x rounded up to the nearest integer. We will prove that $B_{k,N}\, \alpha \cdot W$ lies in $M_g(\mathbb{Z}[\zeta_Q])$ and hence $B_{k,N}\, \alpha \cdot \beta_b \in M_g(\mathbb{Z})$.

In §4.8, we will observe that W and D_d can be numerically approximated in $M_g(\mathbb{C})$. By approximating $D_d \in \mathrm{GL}_g(\mathbb{Z})$ to a sufficiently high accuracy, we can compute D_d. By computing W to a sufficiently high accuracy, we can approximate the entries of $B_{k,N}\alpha \cdot \beta_b \in M_g(\mathbb{Z})$ so that they can be explicitly determined. With this approach, we are now able to compute the matrices $\beta_b \in M_g(\mathbb{Q}(\zeta_N))$ for all $0 \leq b \leq \varphi(N) - 1$.

Finally observe that W is the unique matrix in $M_g(\mathbb{Q}(\zeta_Q))$ satisfying $\mathrm{Tr}_{\mathbb{Q}(\zeta_Q)/\mathbb{Q}}(\zeta_Q^b W) = \beta_b$ for all $0 \leq b \leq \varphi(Q) - 1$. Indeed, note that the map

$$\mathcal{T} \colon \mathbb{Q}(\zeta_Q) \to \mathbb{Q}^{\varphi(Q)}, \quad x \mapsto (\mathrm{Tr}_{\mathbb{Q}(\zeta_Q)/\mathbb{Q}}(\zeta_Q^b x))_{0 \leq b \leq \varphi(Q)-1}$$

is an isomorphism of $\mathbb{Q}$-vector spaces (the pairing $\mathbb{Q}(\zeta_Q) \times \mathbb{Q}(\zeta_Q) \to \mathbb{Q}$, $(x, y) \mapsto \mathrm{Tr}_{\mathbb{Q}(\zeta_Q)/\mathbb{Q}}(xy)$ is non-degenerate and $1, \zeta_Q, \ldots, \zeta_Q^{\varphi(Q)-1}$ is a basis for $\mathbb{Q}(\zeta_Q)$ over $\mathbb{Q}$). By computing $\mathrm{Tr}_{\mathbb{Q}(\zeta_Q)/\mathbb{Q}}(\zeta_Q^b \zeta_Q^a)$ with $0 \leq a, b \leq \varphi(Q) - 1$, we can compute $\mathcal{T}$ and its inverse. Using this, we can compute the desired matrix W.

1.4. **Action of $\mathrm{SL}_2(\mathbb{Z})$ on $S_k(\Gamma(N))$.** Fix positive integers k and N. We now explain how, using the algorithm of §1.3, we can compute the natural right action of $\mathrm{SL}_2(\mathbb{Z})$ on $S_k(\Gamma(N))$.

The matrices $S := \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ generate $\mathrm{SL}_2(\mathbb{Z})$, so to describe the action of $\mathrm{SL}_2(\mathbb{Z})$ on $S_k(\Gamma(N))$ it suffices to describe how S and T act. The action of T is straightforward since it fixes the cusp at infinity. For any $h = \sum_{n=1}^{\infty} a_n(h) q_N^n \in S_k(\Gamma(N))$, with $q_N = e^{2\pi i \tau / N}$, we have

$$h|T = \sum_{n=1}^{\infty} a_n(h) \zeta_N^n \cdot q_N^n.$$

Define $\Gamma := \Gamma_0(N^2) \cap \Gamma_1(N)$. Using the algorithm of §1.3 with level N^2 instead of N, we can compute an explicit basis $f_1, \ldots, f_g$ of the $\mathbb{Z}$-module $S_k(\Gamma, \mathbb{Z})$ and a matrix $W \in \mathrm{GL}_g(\mathbb{Q}(\zeta_N))$ satisfying $f_j|W_{N^2} =$

$\sum_{k=1}^{g} W_{j,k} \cdot f_k$. Since $\Gamma(N) = \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right) \Gamma \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}$, we have an isomorphism

$$\beta \colon S_k(\Gamma) \xrightarrow{\sim} S_k(\Gamma(N)), \quad f \mapsto N^{k/2} \cdot f \left| \left(\begin{smallmatrix} 1 & 0 \\ 0 & N \end{smallmatrix}\right) \right.$$

of complex vector spaces which on q-expansions satisfies $\beta(\sum_{n=1}^{\infty} a_n q^n) = \sum_{n=1}^{\infty} a_n q_N^n$. For each $1 \leq j \leq g$, define $h_j := \beta(f_j) = \sum_{n=1}^{\infty} a_n(f_j) q_N^n$. The cusp forms $h_1, \ldots, h_g$ are a basis of the $\mathbb{Z}$-module $S_k(\Gamma(N), \mathbb{Z})$.

For any $f \in S_k(\Gamma)$, we have

$$\beta(f|W_{N^2}) = N^k \cdot \beta(f) \left| \left(\left(\begin{smallmatrix} 1 & 0 \\ 0 & N \end{smallmatrix}\right)^{-1} \left(\begin{smallmatrix} 0 & -1 \\ N^2 & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} 1 & 0 \\ 0 & N \end{smallmatrix}\right) \right) \right. = N^k \cdot \beta(f) \left| \left(\begin{smallmatrix} 0 & -N \\ N & 0 \end{smallmatrix}\right) \right. = N^k \cdot \beta(f)|S.$$

Therefore,

$$h_j|S = \beta(f_j)|S = N^{-k}\beta(f_j|W_{N^2}) = N^{-k}\beta(\sum_{k=1}^{g} W_{j,k} \cdot f_k) = \sum_{k=1}^{g} N^{-k} W_{j,k} \cdot \beta(f_k) = \sum_{k=1}^{g} N^{-k} W_{j,k} \cdot h_k.$$

So the action of S on the basis $h_1, \ldots, h_g$ of $S_k(\Gamma(N))$ is given by the matrix W. In §1.3, we gave an algorithm to compute W.

1.5. **Modular curves.** Fix an integer $N > 1$ and let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ and $-I \in G$. Associated to the group G, is a modular curve X_G; it is a smooth projective and geometrically irreducible curve X_G defined over $\mathbb{Q}$. In §6, we give a definition of X_G and also give a connection with elliptic curves.

There is a natural right action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the $\mathbb{Q}$-vector space $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))$ characterized by the following properties:

- The group $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ acts via the right action of $\mathrm{SL}_2(\mathbb{Z})$ described in §1.4.
- A matrix $\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$ acts on a cusp form by applying σ_d to the coefficients of its q-expansion, where σ_d is the automorphism of $\mathbb{Q}(\zeta_N)$ satisfying $\sigma_d(\zeta_N) = \zeta_N^d$.

See §3 of [BN19] for an explanation of why this action is well-defined.

From §1.4 and our algorithm in §1.3, we can compute a basis $f_1, \ldots, f_g$ of the $\mathbb{Q}$-vector space $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))^G$, where each f_j is given by its q-expansion for which we can compute arbitrarily many terms. In §6, we will see that $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))^G$ is naturally isomorphism to $H^0(X_G, \Omega_{X_G})$. Let $\omega_1, \ldots, \omega_g$ be the basis of $H^0(X_G, \Omega_{X_G})$ corresponding to $f_1, \ldots, f_g$. In particular, the genus of X_G is g.

Now assume that $g \geq 2$. The morphism

$$\varphi \colon X_G \to \mathbb{P}^{g-1}_{\mathbb{Q}}, \quad P \mapsto [\omega_1(P), \ldots, \omega_g(P)]$$

is called the canonical map and it is uniquely determined up to an automorphism of $\mathbb{P}^{g-1}_{\mathbb{Q}}$. The image $C := \varphi(X_G)$ is the canonical curve of X_G.

We will see that the homogenous ideal $I(C) \subseteq \mathbb{Q}[x_1, \ldots, x_g]$ of the curve C is generated by the homogeneous polynomials $F \in \mathbb{Q}[x_1, \ldots, x_g]$ for which $F(f_1, \ldots, f_g) = 0$. In §6, we describe how to find a set of generators of the ideal $I(C)$ from enough terms of the q-expansions of the cusp forms $f_1, \ldots, f_g$, and hence compute the curve C.

If X_G is (geometrically) hyperelliptic, then C has genus 0 and φ has degree 2. If X_G is not hyperelliptic, then φ is an embedding and hence X_G and C are isomorphic curves.

Remark 1.4. The bottleneck in the above approach to computing modular curves is that $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))$ with its $\mathrm{SL}_2(\mathbb{Z})$-action becomes harder to compute as N grows. In particular, note that $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))^G$ often has much smaller dimension than $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))$. The original goal of this paper was to show that this obvious and direct approach is actually computable.

1.6. **Examples.** We now give a few basic examples.

Example 1.5. Define the congruence subgroup $\Gamma := \Gamma_0(49) \cap \Gamma_1(7)$; it has level $N = 49$. Then there is a unique basis $\{f_1, f_2, f_3\}$ of the $\mathbb{Z}$-module $S_2(\Gamma, \mathbb{Z})$ satisfying:

$$f_1 = q - 3q^8 + 4q^{22} + \dots, \quad f_2 = q^2 - 3q^9 - q^{16} + \dots, \quad f_3 = q^4 - 4q^{11} + 3q^{18} + \dots.$$

We have $f_j|\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) = \sum_{k=1}^{3} W_{j,k} \cdot f_k$ for a unique matrix $W \in \mathrm{GL}_3(\mathbb{C})$. Using the algorithm of §1.3, we find that

$$W = 7 \cdot \begin{pmatrix} -3\xi^2 - 2\xi + 2 & 2\xi^2 - \xi - 6 & -\xi^2 - 3\xi + 3 \\ 2\xi^2 - \xi - 6 & \xi^2 + 3\xi - 3 & 3\xi^2 + 2\xi - 2 \\ -\xi^2 - 3\xi + 3 & 3\xi^2 + 2\xi - 2 & 2\xi^2 - \xi - 6 \end{pmatrix},$$

where $\xi := \zeta_7 + \zeta_7^{-1}$.

Now consider the modular curve $X(7) := X_G$ over $\mathbb{Q}$, where G is the subgroup of $\mathrm{GL}_2(\mathbb{Z}/7\mathbb{Z})$ consisting of matrices of the form $\pm\left(\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right)$. For $1 \le j \le 3$, let h_j be the cusp form in $S_2(\Gamma(7), \mathbb{Z})$ with the same q-expansion as f_j except q is replaced by q_7. From the discussion in §1.4, we find that h_1, h_2, h_3 is a basis of the $\mathbb{Q}$-vector space $S_2(\Gamma(7), \mathbb{Q}) = S_2(\Gamma(7), \mathbb{Q})^G$. Applying the methods of §6, we find that $X(7)$ has genus 3 and $F(h_1, h_2, h_3) = 0$, where $F(x, y, z) = x^3z - xy^3 + yz^3$. In particular, we deduce that the curve $X(7)$ is isomorphic to the curve in $\mathbb{P}^2_{\mathbb{Q}}$ defined by the equation $x^3z - xy^3 + yz^3 = 0$ (which up to changing the sign of z is the Klein quartic). For more on the curve $X(7)$, see [Elk99].

Example 1.6. Let G be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/13\mathbb{Z})$ generated by $\left(\begin{smallmatrix} 2 & 0 \\ 0 & 2 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 5 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 1 \\ -1 & 1 \end{smallmatrix}\right)$. The group G contains the scalar matrices in $\mathrm{GL}_2(\mathbb{Z}/13\mathbb{Z})$ and its image in $\mathrm{PGL}_2(\mathbb{Z}/13\mathbb{Z})$ is isomorphic to the symmetric group S_4; these properties uniquely characterize G up to conjugation in $\mathrm{GL}_2(\mathbb{Z}/13\mathbb{Z})$. A model for X_G was first computed by Banwait and Cremona in [BC14].

Set $\zeta := \zeta_{13}$. The $\mathbb{Q}(\zeta)$-vector space $S_2(\Gamma(N), \mathbb{Q}(\zeta))$ has dimension 50. Using the algorithm from §1.3 and §1.4, we can find a basis of this space as well as the natural $\mathrm{SL}_2(\mathbb{Z})$-action. A computation then shows that the $\mathbb{Q}$-vector space $S_2(\Gamma(N), \mathbb{Q}(\zeta))^G$ has dimension 3 and there is a basis f_1, f_2, f_3 characterized by the following q-expansions:

$$\begin{aligned} f_1 =& q_{13} + (\zeta^{11} + \zeta^{10} + \zeta^3 + \zeta^2)q_{13}^2 + (-\zeta^{11} - \zeta^{10} + \zeta^9 + \zeta^7 + \zeta^6 + \zeta^4 - \zeta^3 - \zeta^2 + 2)q_{13}^3 + \cdots, \\ f_2 =& (\zeta^{11} + \zeta^{10} + \zeta^3 + \zeta^2)q_{13} + (-4\zeta^{11} - 4\zeta^{10} - \zeta^9 - \zeta^7 - \zeta^6 - \zeta^4 - 4\zeta^3 - 4\zeta^2 - 3)q_{13}^2 \\ &+ (3\zeta^{11} + 3\zeta^{10} - 3\zeta^9 - 3\zeta^7 - 3\zeta^6 - 3\zeta^4 + 3\zeta^3 + 3\zeta^2 - 5)q_{13}^3 + \cdots, \\ f_3 =& (\zeta^9 + \zeta^7 + \zeta^6 + \zeta^4)q_{13} + (4\zeta^{11} + 4\zeta^{10} + 2\zeta^9 + 2\zeta^7 + 2\zeta^6 + 2\zeta^4 + 4\zeta^3 + 4\zeta^2 + 5)q_{13}^2 \\ &+ (-\zeta^{11} - \zeta^{10} + 2\zeta^9 + 2\zeta^7 + 2\zeta^6 + 2\zeta^4 - \zeta^3 - \zeta^2 + 4)q_{13}^3 + \cdots. \end{aligned}$$

Moreover, we have chosen f_1, f_2, f_3 so that it is a basis of the $\mathbb{Z}$-module $S_2(\Gamma(N), \mathbb{Q}(\zeta))^G \cap S_2(\Gamma(N), \mathbb{Z}[\zeta])$. Applying the methods of §6, we find that $F(f_1, f_2, f_3) = 0$, where $F(x, y, z)$ is the polynomial

$$\begin{aligned} &13x^4 + 13x^3y + 25x^3z - 8x^2y^2 + 9x^2yz + 3x^2z^2 - 20xy^3 \\ &- 39xy^2z - 34xyz^2 - 12xz^3 - 6y^4 - 15y^3z - 14y^2z^2 - 5yz^3. \end{aligned}$$

We deduce that X_G is isomorphic to the curve in $\mathbb{P}^2_{\mathbb{Q}}$ defined by the equation $F(x, y, z) = 0$.

We have also used our methods to verify models of various modular curves arising from non-split Cartans that occur in the literature; see [Bar14, MS18, DMS19]. One benefit of our approach is that it works for general G and does not require any special representation theory.

1.7. **Some related results.** There is an alternate method using Eisenstein series to compute the $\mathrm{SL}_2(\mathbb{Z})$-action on the full space $M_k(\Gamma(N))$ where $k \ge 2$; this was not known to the author until after the first draft of this paper was completed. For simplicity, assume that $N \ge 3$. In [BN19], Brunault and Neururer considered the $\mathbb{C}$-subalgebra $\mathcal{R}_N$ of $M_*(\Gamma(N)) := \bigoplus_{k \ge 1} M_k(\Gamma(N))$ generated by certain Eisenstein series $E^{(1)}_{a,b}$ with $a, b \in \mathbb{Z}/N\mathbb{Z}$. Citing

work of Khuri–Makdisi, they observe that the k-th graded part of $\mathcal{R}_N$ agrees with $M_k(\Gamma(N))$ for all $k \geq 2$. The q-expansion of the $E^{(1)}_{a,b}$ lie in $\mathbb{Q}(\zeta_N)$ and the right action of $\mathrm{SL}_2(\mathbb{Z})$ on them is explicit. So for $k \geq 2$, we obtain a basis of $M_k(\Gamma(N), \mathbb{Q}(\zeta_N))$ along with the action of $\mathrm{SL}_2(\mathbb{Z})$ with respect to this basis.

It would be interesting to compare the efficiency of our algorithm versus an Eisenstein series approach to computing the action of $\mathrm{SL}_2(\mathbb{Z})$ on $M_k(\Gamma(N))$. In §2.3 of [Coh19], Cohen (who is using Eisenstein series to computing the q-expansion of a modular form at all cusps) notes that for large N, one needs to work numerically in $\mathbb{C}$ and then if desired use LLL-type algorithms to recognize the coefficients. So a reasonable approach would be to use Eisenstein series to do numerical approximations and then the methods of this paper to determine coefficients precisely. Since the algorithm of §1.3 requires only recognizing rational integers, it should not need as much accuracy as an LLL-type algorithm. We will study the Eisenstein series approach in future work.

Collins and Cohen [Col18, Coh19] have both recently described how to numerically compute the q-expansion of a modular form at all of its cusps (both of these papers are interested in numerically computing Petersson inner products). In private communications, David Loeffler has observed that there is a purely algebraic approach to computing Atkin–Lehner operators using modular symbols.

1.8. **Acknowledgements.** Thanks to Jeremy Rouse for corrections to an earlier version.

2. Arithmetic of the Atkin–Lehner operator

Fix positive integers k and N. In this section, we prove some arithmetic facts about the action of the Atkin–Lehner operator W_N and the diamond operators on the space of modular forms $M_k(\Gamma_1(N))$.

For each automorphisms σ of $\mathbb{C}$, we have $\sigma(\zeta_N) = \zeta_N^{\chi_N(\sigma)}$ for a unique $\chi_N(\sigma) \in (\mathbb{Z}/N\mathbb{Z})^\times$.

Theorem 2.1. *Take any congruence subgroup $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$.*

(i) *Let B be a $\mathbb{Z}[1/N, \zeta_N]$-subalgebra of $\mathbb{C}$. The map $M_k(\Gamma, B) \to M_k(\Gamma, B)$, $f \mapsto f|W_N$ is an isomorphism of B-modules.*

(ii) *Let B be a subring of $\mathbb{C}$. For any $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, the map $M_k(\Gamma, B) \to M_k(\Gamma, B)$, $f \mapsto f|\langle d\rangle$ is an isomorphism of B-modules.*

(iii) *For any modular form $f \in M_k(\Gamma_1(N))$ and automorphism σ of the field $\mathbb{C}$, we have*

$$\sigma(f|W_N) = (\sigma(f)|W_N)|\langle\chi_N(\sigma)\rangle,$$

Proof. We first prove (i). We will make use of Katz's algebraic theory of modular forms, cf. Chapter II of [Kat76]. Almost everything we will require is summarized in §3.6 of [Oht95]. Fix a $\mathbb{Z}[1/N, \zeta_N]$-subalgebra B of $\mathbb{C}$. With definitions as in §2.1 of [Kat76], let $R^k(B, \Gamma_{00}(N)^{\mathrm{arith}})$ and $R^k(B, \Gamma_{00}(N)^{\mathrm{naive}})$ be the B-modules consisting of $\Gamma_{00}(N)^{\mathrm{arith}}$ and $\Gamma_{00}(N)^{\mathrm{naive}}$ modular forms, respectively, of weight k defined over B.

We claim that $f|W_N \in M_k(\Gamma_1(N), B)$ for any modular form $f \in M_k(\Gamma_1(N), B)$. Fix a modular form $f \in M_k(\Gamma_1(N), B)$. Since $B \subseteq \mathbb{C}$, associated to f is a modular form $F \in R^k(B, \Gamma_{00}(N)^{\mathrm{arith}})$, cf. §2.4 of [Kat76]. The two modular forms f and F each have the notion of a q-expansion and they agree with each other. Using the isomorphisms in (2.3.6) of [Kat76], we obtain from F a modular form $G \in R^k(B, \Gamma_{00}(N)^{\mathrm{naive}})$. Since B is a $\mathbb{Z}[1/N, \zeta_N]$-algebra, we have a unique isomorphism $\mathbb{Z}/N\mathbb{Z} \xrightarrow{\sim} \mu_N$ of group schemes over $\operatorname{Spec} B$ satisfying $1 \mapsto \zeta_N$. Using this isomorphism $\mathbb{Z}/N\mathbb{Z} \cong \mu_N$, we can view G as a modular form in $R^k(B, \Gamma_{00}(N)^{\mathrm{arith}})$. Associated to G, there is a classical weakly modular form g on $\Gamma_1(N)$; *weakly* meaning that it is meromorphic, and not necessarily holomorphic, at the cusps. A straightforward computation shows that $f|W_N = g$; for example, see Lemma 3.6.5 of [Oht95] (note that $N^{-1} \cdot f|\tau$ in the notation of [Oht95] agrees with our $N^{-k} \cdot f|W_N$). Since G is defined over B, the q-expansion of G, and hence also of $g = f|W_N$, has coefficients in B. This completes the proof of the claim.

The above claim shows that the function $\alpha\colon M_k(\Gamma, B) \to M_k(\Gamma, B)$, $f \mapsto f|W_N$ is well-defined; it is clearly a homomorphism of B-modules. For any $f \in M_k(\Gamma, B)$, we have $\alpha(\alpha(f)) = (f|W_N)|W_N = (-N)^k \cdot f$. Since $N \in B^\times$, this proves that α is an isomorphism of B-modules. This completes the proof of part (i).

Now fix a subring B of $\mathbb{C}$ and take any $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. Take any modular form $f \in M_k(\Gamma, B)$. We have $f|\langle d\rangle \in M_k(\Gamma)$. As above, associated to f is a modular form $F \in R^k(B, \Gamma_{00}(N)^{\mathrm{arith}})$. With notation as in Chapter II of [Oht95], there is a modular form $F' \in R^k(B, \Gamma_{00}(N)^{\mathrm{arith}})$ that satisfies $F'(E, \omega, i) = F(E, \omega, di)$ for all $\Gamma_{00}(N)^{\mathrm{arith}}$-test objects (E, ω, i). There is a classical weakly modular form f' on $\Gamma_1(N)$ that corresponds to F' and the coefficients of its q-expansions all lie in B. It is straightforward to show that $f' = f|\langle d\rangle$; this is equation (3.6.7) of [Oht95]. So the q-expansion of $f|\langle d\rangle$ has coefficients in B and thus $f|\langle d\rangle \in M_k(\Gamma, B)$. Therefore, the map

$$\alpha_d \colon M_k(\Gamma, B) \to M_k(\Gamma, B), \quad f \mapsto f|\langle d\rangle$$

is well-defined; it is clearly a homomorphism of B-modules. The map α_d is invertible and its inverse is $\alpha_{d^{-1}}$.

Part (iii) follows from Lemma 3.5.2 of [Oht95]. Note that this lemma is stated for cusp forms, but this assumption is not used in the proof. The lemma is also stated for modular forms with coefficients in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$, say in $\mathbb{C}$; this is not a problem since $M_k(\Gamma_1(N))$ has a basis consisting of modular forms with algebraic Fourier coefficients. □

Corollary 2.2. *Fix a number field $K \subseteq \mathbb{C}$ and a modular form $f \in M_k(\Gamma_0(N), K)$. Then $f|W_N$ also lies in $M_k(\Gamma_0(N), K)$.*

Proof. We have $f|W_N$ in $M_k(\Gamma_0(N))$. Take any automorphism σ of $\mathbb{C}$ that fixes K. We have $\sigma(f) = f$ since f has coefficients in K. By Theorem 2.1(iii), we have $\sigma(f|W_N) = (f|W_N)|\langle \chi_N(\sigma)\rangle = f|W_N$. Since σ was an arbitrary automorphism of $\mathbb{C}$ that fixes K, we deduce that $f|W_N$ has coefficients in K. □

Lemma 2.3. *We have $(f|\langle d\rangle)|W_N = (f|W_N)|\langle d^{-1}\rangle$ for all $f \in M_k(\Gamma_1(N))$ and $d \in (\mathbb{Z}/N\mathbb{Z})^\times$.*

Proof. Take any $f \in M_k(\Gamma_1(N))$ and $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. Choose a matrix $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ that is congruent to $\left(\begin{smallmatrix} d & 0 \\ 0 & d^{-1}\end{smallmatrix}\right)$ modulo N. One can check that $\gamma' := \left(\begin{smallmatrix} 0 & -1 \\ N & 0\end{smallmatrix}\right)\gamma\left(\begin{smallmatrix} 0 & -1 \\ N & 0\end{smallmatrix}\right)^{-1}$ is in $\mathrm{SL}_2(\mathbb{Z})$ and is congruent to $\left(\begin{smallmatrix} d^{-1} & 0 \\ 0 & d\end{smallmatrix}\right)$ modulo N. Therefore,

$$(f|W_N)|\langle d^{-1}\rangle = N^{k/2} \cdot (f|\left(\begin{smallmatrix} 0 & -1 \\ N & 0\end{smallmatrix}\right))|\gamma = N^{k/2} \cdot (f|\gamma')|\left(\begin{smallmatrix} 0 & -1 \\ N & 0\end{smallmatrix}\right) = (f|\langle d\rangle)|W_N. \qquad \square$$

3. Integrality of coefficients

Fix positive integers k and N. For a modular form $f \in M_k(\Gamma_1(N))$ whose Fourier coefficients are algebraic integers, the coefficients of the modular form $f|W_N$ are algebraic but need not be integral.

The goal of this section is to show that the coefficients of $f|W_N$ times an explicit positive integer are all algebraic integers. Define the integers

$$B_{k,N} := \prod_{p|N} p^{\lceil k/(p-1)\rceil} \quad \text{and} \quad C_{k,N} := \prod_{p|N} p^{\lfloor k/(p-1)\rfloor},$$

where $\lceil x\rceil$ and $\lfloor x\rfloor$ are the values of x rounded up and down, respectively, to the nearest integer. Note that $C_{k,N}$ divides the integer $C_k := \prod_{p\le k+1} p^{\lfloor k/(p-1)\rfloor}$ which depends only on k.

Theorem 3.1.

(i) *If $f \in M_k(\Gamma_1(N))$ is a modular form whose Fourier coefficients are algebraic integers, then the coefficients of $B_{k,N} \cdot f|W_N$ are also algebraic integers.*

(ii) *If $f \in M_k(\Gamma_0(N))$ is a modular form whose Fourier coefficients are algebraic integers, then the coefficients of $C_{k,N} \cdot f|W_N$ are also algebraic integers.*

3.1. **Valuations.** Take any number field $K \subseteq \mathbb{C}$ that contains ζ_N. For a non-zero prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$, let $v_\mathfrak{p}\colon K^\times \to \mathbb{Q}$ be the valuation corresponding to $\mathfrak{p}$ normalized so that $v_\mathfrak{p}(p) = 1$, where p is the rational prime divisible by $\mathfrak{p}$. We set $v_\mathfrak{p}(0) = +\infty$. For each modular form $f \in M_k(\Gamma(N), K)$, define

$$v_\mathfrak{p}(f) = \inf_{n \geq 0} v_\mathfrak{p}(a_n(f)),$$

where f has q-expansion $\sum_{n=0}^{\infty} a_n(f) q_N^n$. Note that $v_\mathfrak{p}(f) \neq -\infty$ since the q-expansion of f actually lies in $K \otimes_{\mathbb{Z}} \mathbb{Z}[\![q_N]\!] \subseteq K[\![q_N]\!]$. Similarly, we can define $v_\mathfrak{p}(f)$ for any power series $f \in K \otimes_{\mathbb{Z}} \mathbb{Z}[\![q_N]\!]$. For a modular form $f \in M_k(\Gamma_1(N), K)$, we have $f|W_N \in M_k(\Gamma_1(N), K)$ by Theorem 2.1(i).

Lemma 3.2. *Let $\mathfrak{p}$ be a non-zero prime ideal of $\mathcal{O}_K$ that does not divide N. Then $v_\mathfrak{p}(f|W_N) = v_\mathfrak{p}(f)$ for all $f \in M_k(\Gamma_1(N), K)$.*

Proof. We claim that $v_\mathfrak{p}(f|W_N) \geq v_\mathfrak{p}(f)$ holds for any non-zero $f \in M_k(\Gamma_1(N), K)$. After scaling f by an appropriate non-zero element of K, we may assume without loss of generality that $v_\mathfrak{p}(f) = 0$. So $f \in M_k(\Gamma_1(N), B)$, where B is the subring of K consisting of $x \in K$ satisfying $v_\mathfrak{p}(x) \geq 0$. Since $\mathfrak{p} \nmid N$, we find that B is a $\mathbb{Z}[1/N, \zeta_N]$-subalgebra of $\mathbb{C}$. By Theorem 2.1(i), we deduce that $f|W_N$ also has coefficients in B and hence $v_\mathfrak{p}(f|W) \geq 0$. This proves the claim.

We now prove the lemma. We may assume that f is non-zero since otherwise the lemma is trivial. Applying the claim to $f|W_N$ gives $v_\mathfrak{p}((f|W_N)|W_N) \geq v_\mathfrak{p}(f|W_N)$. Since $(f|W_N)|W_N = \pm N^k f$ and $\mathfrak{p} \nmid N$, this implies that $v_\mathfrak{p}(f) \geq v_\mathfrak{p}(f|W_N)$. This proves the lemma since the claim gives the other inequality $v_\mathfrak{p}(f|W_N) \geq v_\mathfrak{p}(f)$. □

Note that the $\mathfrak{p}$-adic valuations of f and $f|W_N$ need not agree for primes $\mathfrak{p}$ dividing N. The following theorem bounds the difference between these two valuations.

Theorem 3.3. *Take any prime p that divides N and any prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ that divides p. Then*

$$\left| v_\mathfrak{p}(f|W_N) - v_\mathfrak{p}(f) - k/2 \cdot v_p(N) \right| \leq \frac{k}{2} v_p(N) + \frac{k}{p-1}$$

for any non-zero $f \in M_k(\Gamma_1(N), K)$.

Remark 3.4. In the special case where $f \in M_k(\Gamma_0(p), \mathbb{Q})$, Theorem 3.3 was proved by Deligne and Rapoport, cf. Proposition 3.20 in Chapter VII of [DR73]. We prove Theorem 3.3 by reducing to this special case.

3.2. **Proof of Theorem 3.3.** We claim that the inequality

$$v_\mathfrak{p}(f|W_N) - v_\mathfrak{p}(f) \geq -\frac{k}{p-1} \tag{3.1}$$

holds for all non-zero $f \in M_k(\Gamma_1(N), K)$.

Assume that the claim holds. Take any non-zero $f \in M_k(\Gamma_1(N), K)$. Applying (3.1) to the modular function $f|W_N$ gives $v_\mathfrak{p}((f|W_N)|W_N) - v_\mathfrak{p}(f|W_N) \geq -\frac{k}{p-1}$. Since $(f|W_N)|W_N = \pm N^k f$, we deduce that

$$v_\mathfrak{p}(f|W_N) - v_\mathfrak{p}(f) - k v_p(N) \leq \frac{k}{p-1}. \tag{3.2}$$

The theorem follows from the inequalities (3.1) and (3.2).

We will prove (3.1) by considering various cases. Take any non-zero $f \in M_k(\Gamma_1(N), K)$. Note that there is no harm in scaling f by a non-zero element of K since the value $v_\mathfrak{p}(f|W_N) - v_\mathfrak{p}(f)$ will not change. In particular, we may assume that $v_\mathfrak{p}(f) = 0$ when desired.

Different weights will arise in the proof, so we will add subscripts to slash and Atkin–Lehner operators to indicate the weight involved if it is not k. Let B be the subring of K consisting of $x \in K$ satisfying $v_\mathfrak{p}(x) \geq 0$. For later, note that the power series ring $B[\![q]\!]$ is integrally closed since B is a PID, cf. [Bou98, Ch. V §4 Prop. 14].

• **Case 1**: *Suppose that $N = p$ and that $f \in M_k(\Gamma_0(N), \mathbb{Q})$.*

The claim in this case follows from Proposition 3.20 in Chapter VII of [DR73].

• **Case 2**: *Suppose that* $N = p$ *and that* $f \in M_k(\Gamma_0(N), K)$.

After scaling f by an appropriate non-zero element of K, we may assume that $f \in M_k(\Gamma_0(N), \mathcal{O}_K)$ and $v_{\mathfrak{p}}(f) = 0$. We have $M_k(\Gamma_0(N), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathcal{O}_K = M_k(\Gamma_0(N), \mathcal{O}_K)$, cf. section B.1.2 in Appendix B of [BDP17]. So there are $f_1, \ldots, f_d \in M_k(\Gamma_0(N), \mathbb{Z})$ and $c_1, \ldots, c_d \in \mathcal{O}_K$ such that $f = \sum_{i=1}^{d} c_i f_i$. Therefore, $v_{\mathfrak{p}}(f|W_N) \geq \min_i v_{\mathfrak{p}}(f_i|W_N)$. By Case 1, we have $v_{\mathfrak{p}}(f_i|W_N) \geq v_{\mathfrak{p}}(f_i) - k/(p-1) \geq -k/(p-1)$ for all $1 \leq i \leq d$. We deduce that $v_{\mathfrak{p}}(f|W_N) \geq -k/(p-1)$. This proves the claimed inequality (3.1) in this case.

• **Case 3**: *Suppose that* $N = p^{r+1}$ *for an integer* $r \geq 1$ *and that* $f \in M_k(\Gamma_0(N), K)$.

After possibly replacing K by a larger number field, we may assume without loss of generality that there is an element $\pi \in K$ satisfying $v_{\mathfrak{p}}(\pi) = k/(p-1)$. Define $g := p^{rk/2} \cdot f| \left(\begin{smallmatrix} p^r & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}$. The function g is a modular form on the congruence subgroup

$$\Gamma := \left(\begin{smallmatrix} p^r & 0 \\ 0 & 1 \end{smallmatrix}\right) \Gamma_0(p^{r+1}) \left(\begin{smallmatrix} p^r & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1} = \left\{ \left(\begin{smallmatrix} a & p^r b \\ pc & d \end{smallmatrix}\right) : a, b, c, d \in \mathbb{Z} \text{ such that } ad - p^{r+1}bc = 1 \right\}.$$

We have $g \in M_k(\Gamma, B)$ since $g(\tau) = f(\tau/p^r)$ and $v_{\mathfrak{p}}(f) = 0$.

With the matrix $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, define the polynomial

$$P(x) := \prod_{j=0}^{p^r - 1} (x - g|T^j).$$

The q-expansion of $g|T^j$ has coefficients in B; they are obtained by scaling the coefficients of g by suitable N-th roots of unity. Therefore, $P(x) = \sum_{i=0}^{p^r} b_i \cdot x^{p^r - i}$ with $b_i \in B[\![q]\!]$. Since the matrices $\{T^j : 0 \leq j \leq p^r - 1\}$ represent the right cosets of Γ in $\Gamma_0(p)$, we find that b_i is a modular form for $\Gamma_0(p)$ of weight ki and hence $b_i \in M_{ki}(\Gamma_0(p), B)$. By Case 2 applied to b_i, we have

$$v_{\mathfrak{p}}(b_i|_{ki} W_p) \geq -ki/(p-1)$$

and hence $v_{\mathfrak{p}}(\pi^i \cdot b_i|_{ki} W_p) \geq 0$. Therefore, $\pi^i \cdot b_i|_{ki} W_p$ is an element of $B[\![q]\!]$.

Now define the polynomial

$$Q(x) := \prod_{j=0}^{p^r - 1} (x - \pi \cdot p^{k/2} (g|T^j)| \left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right)) = \sum_{i=0}^{p^r} \pi^i \cdot p^{ki/2} b_i|_{ki} \left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right) \cdot x^{p^r - i} = \sum_{i=0}^{p^r} \pi^i \cdot b_i|_{ki} W_p \cdot x^{p^r - i};$$

it is a monic polynomial with coefficients in $B[\![q]\!]$. We have

$$f|W_N = N^{k/2} f| \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right) = N^{k/2} \cdot p^{-rk/2}\, g| \left(\left(\begin{smallmatrix} p^r & 0 \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right) \right) = p^{k/2} g| \left(\begin{smallmatrix} 0 & -p^r \\ N & 0 \end{smallmatrix}\right) = p^{k/2} g| \left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right)$$

and hence $\pi \cdot f|W_N$ is a root of $Q(x)$. Since $B[\![q]\!]$ is integrally closed and since $\pi \cdot f|W_N$ is a root of $Q(x) \in (B[\![q]\!])[x]$ that lies in the fraction field of $B[\![q]\!]$, we deduce that $\pi \cdot f|W_N$ lies in $B[\![q]\!]$. Therefore, $v_{\mathfrak{p}}(\pi \cdot f|W_N) \geq 0$ and hence $v_{\mathfrak{p}}(f|W_N) \geq -v_{\mathfrak{p}}(\pi) = -k/(p-1)$. This proves the claimed inequality (3.1) in this case.

• **Case 4**: *Suppose that* $f \in M_k(\Gamma_0(N), K)$.

After scaling f by a non-zero element of K, we may assume that $v_{\mathfrak{p}}(f) = 0$. Let p^r be the largest power of p that divides N. Set $M := N/p^r$. Let $R \subseteq \mathrm{SL}_2(\mathbb{Z})$ be a set of representatives of the right cosets of $\Gamma_0(M)$ in $\mathrm{SL}_2(\mathbb{Z})$ chosen so that each $A \in R$ is congruent to the identity matrix modulo p^r. Define

$$g := \prod_{A \in R} f|A.$$

The function g is an element of $M_{km}(\Gamma_0(p^r), K)$ with $m := |R|$. We have $v_{\mathfrak{p}}(f|A) = v_{\mathfrak{p}}(f)$ for all $A \in R$ by [DR73, VII Corollaire 3.12] and our assumption that all $A \in R$ are congruent modulo p^r to the identity matrix.

Therefore, $v_{\mathfrak{p}}(g) = \sum_{A\in R} v_{\mathfrak{p}}(f|A) = mv_{\mathfrak{p}}(f)$. We have $v_{\mathfrak{p}}(g) = m\cdot 0 = 0$ since $v_{\mathfrak{p}}(f) = 0$, so g is an element of $M_{k'}(\Gamma_0(p^r), B)$ with $k' := km$. By Case 2 or Case 3 applied to g, we have

$$v_{\mathfrak{p}}(g|_{k'}W_{p^r}) \geq -km/(p-1). \tag{3.3}$$

Define the matrix $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$. Take any $A \in R$. Since $S^{-1}AS \in \mathrm{SL}_2(\mathbb{Z})$ is congruent to the identity matrix modulo p^r, we have

$$v_{\mathfrak{p}}(f|S) = v_{\mathfrak{p}}((f|S)|(S^{-1}AS)) = v_{\mathfrak{p}}((f|A)|S)$$

by [DR73, VII Corollaire 3.12]. Therefore, $v_{\mathfrak{p}}(g|_{k'}S) = \sum_{A\in R} v_{\mathfrak{p}}((f|A)|S) = m\cdot v_{\mathfrak{p}}(f|S)$. We have

$$f|W_N = N^{k/2}f|\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right) = N^{k/2}(f|S)|\left(S^{-1}\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)\right) = N^{k/2}(f|S)|\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

So $(f|W_N)(\tau) = N^k(f|S)(N\tau)$ and hence $v_{\mathfrak{p}}(f|W_N) = k\cdot v_{\mathfrak{p}}(N) + v_{\mathfrak{p}}(f|S)$. Similarly, $v_{\mathfrak{p}}(g|_{k'}W_{p^r}) = k'\cdot v_{\mathfrak{p}}(p^r) + v_{\mathfrak{p}}(g|_{k'}S)$. Therefore,

$$m\cdot v_{\mathfrak{p}}(f|W_N) = kmv_{\mathfrak{p}}(N) + mv_{\mathfrak{p}}(f|S) = k'v_{\mathfrak{p}}(p^r) + v_{\mathfrak{p}}(g|_{k'}S) = v_{\mathfrak{p}}(g|_{k'}W_{p^r}).$$

By (3.3), we deduce that $v_{\mathfrak{p}}(f|W_N) \geq -k/(p-1)$. This proves the claimed inequality (3.1) in this case.

• **Case 5**: *General case.*

We may assume that $v_{\mathfrak{p}}(f) = 0$. Take any $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. By Theorem 2.1(ii), the diamond operator $\langle d\rangle$ acts as an automorphism on $M_k(\Gamma_1(N), B)$. This implies that $v_{\mathfrak{p}}(h|\langle d\rangle) = v_{\mathfrak{p}}(h)$ for all $h \in M_k(\Gamma_1(N), K)$.

Define

$$g := \prod_{d\in(\mathbb{Z}/N\mathbb{Z})^\times} f|\langle d\rangle;$$

it is a modular form on $\Gamma_0(N)$ of weight $k' := k\varphi(N)$. Therefore, $v_{\mathfrak{p}}(g) = \sum_d v_{\mathfrak{p}}(f|\langle d\rangle) = \varphi(N)v_{\mathfrak{p}}(f) = 0$. We have

$$g|_{k'}W_N = \prod_{d\in(\mathbb{Z}/N\mathbb{Z})^\times} (f|\langle d\rangle)|W_N = \prod_{d\in(\mathbb{Z}/N\mathbb{Z})^\times} (f|W_N)|\langle d^{-1}\rangle,$$

where the last equality uses Lemma 2.3. Therefore, $v_{\mathfrak{p}}(g|_{k'}W_N) = \sum_d v_{\mathfrak{p}}((f|W_N)|\langle d^{-1}\rangle) = \varphi(N)v_{\mathfrak{p}}(f|W_N)$ and hence

$$v_{\mathfrak{p}}(f|W_N) = \varphi(N)^{-1}\cdot v_{\mathfrak{p}}(g|_{k'}W_N) \geq -\varphi(N)^{-1}\cdot k'/(p-1) = -k/(p-1),$$

where the inequality uses Case 4 applied to g. This completes the proof of the claimed inequality (3.1).

3.3. **Proof of Theorem 3.1.** Take any $f \in M_k(\Gamma_1(N))$ whose Fourier coefficients are algebraic integers. There is a number field $K \subseteq \mathbb{C}$ that contains the coefficients of f and the N-th root of unity ζ_N. We thus have $f \in M_k(\Gamma_1(N), \mathcal{O}_K)$. We have $f|W_N \in M_k(\Gamma_1(N), K)$ by Theorem 2.1(i). So to prove that $B_{k,N}\cdot f|W_N$ has coefficients in $\mathcal{O}_K$, it suffices to show that $v_{\mathfrak{p}}(B_{k,N}\cdot f|W_N) \geq 0$ for all non-zero primes $\mathfrak{p}$ of $\mathcal{O}_K$. Take any non-zero prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$. If $\mathfrak{p} \nmid N$, then

$$v_{\mathfrak{p}}(B_{k,N}\cdot f|W_N) = v_{\mathfrak{p}}(f|W_N) = v_{\mathfrak{p}}(f) \geq 0,$$

where we have used Lemma 3.2 and that f has coefficients in $\mathcal{O}_K$.

Now suppose that $\mathfrak{p}$ divides N. We have $v_{\mathfrak{p}}(B_{k,N}) = \lceil k/(p-1)\rceil$. By Theorem 3.3 with $v_{\mathfrak{p}}(f) \geq 0$, we have $v_{\mathfrak{p}}(f|W_N) \geq -k/(p-1)$. Therefore, $v_{\mathfrak{p}}(B_{k,N}\cdot f|W_N) \geq \lceil k/(p-1)\rceil - k/(p-1) \geq 0$. This completes the proof of part (i).

We now prove (ii). Take any $f \in M_k(\Gamma_0(N))$ whose Fourier coefficients are algebraic integers. Choose a number field $K \subseteq \mathbb{C}$ for which $f \in M_k(\Gamma_0(N), \mathcal{O}_K)$. Without loss of generality, we may assume that $f \in M_k(\Gamma_0(N), \mathbb{Z})$ since $M_k(\Gamma_0(N), \mathcal{O}_K) = M_k(\Gamma_0(N), \mathbb{Z}) \otimes_{\mathbb{Z}} \mathcal{O}_K$, cf. section B.1.2 in Appendix B of [BDP17]. We have $f|W_N \in M_k(\Gamma_0(N), \mathbb{Q})$ by Corollary 2.2.

Take any prime p. If $p \nmid N$, then $v_p(C_{k,N} \cdot f|W_N) = v_p(f|W_N) = v_p(f) \geq 0$, where we have used Lemma 3.2 and that f has coefficients in $\mathbb{Z}$. Now suppose that p divides N. By Theorem 3.3 and $v_p(f) \geq 0$, we have $v_p(f|W_N) \geq -k/(p-1)$. Therefore,

$$v_p(C_{k,N} \cdot f|W_N) = \lfloor k/(p-1) \rfloor + v_p(f|W_N) \geq \lfloor k/(p-1) \rfloor - k/(p-1) > -1.$$

The coefficients of $C_{k,N} \cdot f|W_N$ lie in $\mathbb{Q}$ so $v_p(C_{k,N} \cdot f|W_N)$ is an integer. Therefore, $v_p(C_{k,N} \cdot f|W_N) \geq 0$ since $v_p(C_{k,N} \cdot f|W_N)$ is an integer strictly larger than -1. We have $C_{f,N} \cdot f|W_N \in M_k(\Gamma_0(N), \mathbb{Z})$ since its coefficients are rational and have non-negative valuation at all non-zero primes p. This proves (ii).

4. Spaces of modular forms

Fix positive integers k and N. In this section, we verify that several subspaces $\mathcal{M}$ of $M_k(\Gamma_1(N))$ satisfy conditions (a)–(d) of §1.2. In §4.8, we explain how to numerically approximate the action of W_N and diamond operators on $M_k(\Gamma_1(N))$.

4.1. **Generators.** Recall that for a subspace $\mathcal{M} \subseteq M_k(\Gamma_1(N))$ and a subring $R \subseteq \mathbb{C}$, we defined $\mathcal{M}(R)$ to be $\mathcal{M} \cap M_k(\Gamma_1(N), R)$.

Lemma 4.1. *Let $\{h_1, \ldots, h_r\}$ be a set that generates a finite index subgroup of $\mathcal{M}(\mathbb{Z})$. Assume further that one can compute an arbitrary number of terms in the q-expansion of each h_i. Then one can find a basis $f_1, \ldots, f_g$ of the $\mathbb{Z}$-module $\mathcal{M}(\mathbb{Z})$ for which one can compute an arbitrary number of terms in the q-expansion of each f_i.*

Proof. Let L be the subgroup of $\mathcal{M}(\mathbb{Z})$ generated by $\{h_1, \ldots, h_r\}$. Let s be the largest integer for which $s \leq k/12 \cdot [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)]$. For each $f \in \mathcal{M}$, we have a q-expansion $\sum_{i=0}^{\infty} a_i(f) q^i$. For a prime p, Sturm's bound (Theorem 9.18 of [Ste07]) says that if $f \in \mathcal{M}(\mathbb{Z})$ satisfies $a_i(f) \equiv 0 \pmod{p}$ for all $i \leq s$, then $a_i(f) \equiv 0 \pmod{p}$ for all i. In particular, if $f \in \mathcal{M}(\mathbb{Z})$ satisfies $a_i(f) = 0$ for all $i \leq s$, then $a_i(f) = 0$ for all i.

Let g be the rank of the $\mathbb{Z}$-module $\mathcal{M}(\mathbb{Z})$. So by replacing $\{h_i\}$ by a suitable subset, we may assume that $r = g$ and that the modular forms $h_1, \ldots, h_g$ are a basis for L (Sturm's bound ensures that we can check linear independence by only considering a finite number of terms of the q-expansions).

Let A be the $g \times s$ matrix satisfying $A_{i,j} = a_{j-1}(h_i)$. Since the $h_1, \ldots, h_g$ are linearly independent in $\mathcal{M}(\mathbb{Z})$, Sturm's bound implies that $A \in M_{g,s}(\mathbb{Z})$ has rank g. Recall that there are unique positive integers $b_1, \ldots, b_g$ satisfying $b_i | b_{i+1}$ for all $1 \leq i < g$ such that there are matrices $U \in \mathrm{GL}_g(\mathbb{Z})$ and $V \in \mathrm{GL}_s(\mathbb{Z})$ with $(UAV)_{i,j}$ equal to b_i when $i = j$ and 0 otherwise. This is the *Smith normal form* of A and is straightforward to compute.

First suppose that $b_1 \neq 1$. Choose a prime p dividing b_1. Then A modulo p has rank strictly less than g. So there are $c_1, \ldots, c_g \in \mathbb{Z}$, not all divisible by p, such that $c_1 a_i(h_1) + \cdots + c_g a_i(h_g) \equiv 0 \pmod{p}$ for all $i \leq s$. By Sturm's bound, all the coefficients of the q-expansion of $c_1 a_i(h_1) + \cdots + c_g a_i(h_g)$ are divisible by p. So $f := c_1/p \cdot h_1 + \cdots + c_g/p \cdot h_g$ is an element of $\mathcal{M}(\mathbb{Z})$. We have $f \notin L$ since not all of the c_i are divisible by p. Let L' be the subgroup of $\mathcal{M}(\mathbb{Z})$ generated by $h_1, \ldots, h_g$ and f. By replacing L by L' and choosing a new basis $h_1, \ldots, h_g$ of L', we can repeat this process until $b_1 = 1$.

Now suppose that $b_1 = 1$. We claim that $L = \mathcal{M}(\mathbb{Z})$ and hence $h_1, \ldots, h_g$ is a basis of $\mathcal{M}(\mathbb{Z})$. Suppose on the contrary that $L \neq \mathcal{M}(\mathbb{Z})$ and hence there is a prime p and a modular form $f \in \mathcal{M}(\mathbb{Z})$ such that $pf \in L$ and $f \notin L$. We have $pf = c_1 h_1 + \cdots c_g h_g$ for unique $c_i \in \mathbb{Z}$. If not all the c_i are divisible by p, then we find that A modulo p has rank strictly less than g. However, A modulo p has rank g since $p \nmid b_1 = 1$. This contradicts proves the claim.

Once we have found a basis of $\mathcal{M}(\mathbb{Z})$, the parts of the lemma concerning arbitrarily many terms is immediate. □

Lemma 4.2. *Assume that $\mathcal{M} = \bigoplus_{i=1}^{m} \mathcal{M}_i \subseteq M_k(\Gamma_1(N))$, where each $\mathcal{M}_i$ is a subspace of $M_k(\Gamma_1(N))$ satisfying conditions (a)–(d) of §1.2. Then $\mathcal{M}$ also satisfies conditions (a)–(d).*

Proof. Define $L := \oplus_{i=1}^{m} \mathcal{M}_i(\mathbb{Z}) \subseteq \mathcal{M}(\mathbb{Z})$. Conditions (a)–(c) for $\mathcal{M}$ are immediate consequences of those from the $\mathcal{M}_i$. Since L spans $\mathcal{M}$, we find that L is a finite index subgroup of $\mathcal{M}(\mathbb{Z})$. Condition (d) for $\mathcal{M}$ follows from condition (d) of the $\mathcal{M}_i$ and Lemma 4.1. □

Let $\mathcal{M}$ be a subspace of $M_k(\Gamma_1(N))$ that is stable under the $\mathrm{Aut}(\mathbb{C})$-action. For a number field $L \subseteq \mathbb{C}$ and modular form $f \in \mathcal{M}(L)$, we define

$$\mathrm{Tr}_{L/\mathbb{Q}}(f) = \sum_{\sigma\colon L \hookrightarrow \mathbb{C}} \sigma(f),$$

where σ varies over the field embeddings $L \hookrightarrow \mathbb{C}$. We have $\mathrm{Tr}_{L/\mathbb{Q}}(f) \in \mathcal{M}$ since $\mathcal{M}$ is stable under the action of $\mathrm{Aut}(\mathbb{C})$. The q-expansion of $\mathrm{Tr}_{L/\mathbb{Q}}(f)$ is obtained from the q-expansion of f by taking the trace of the coefficients and hence $\mathrm{Tr}_{L/\mathbb{Q}}(f) \in \mathcal{M}(\mathbb{Q})$. If $f \in \mathcal{M}(\mathcal{O}_L)$, then $\mathrm{Tr}_{L/\mathbb{Q}}(f) \in \mathcal{M}(\mathbb{Z})$.

The following lemma is useful for finding a set of modular forms that generate a finite index subgroup of $\mathcal{M}(\mathbb{Z})$. Choosing a linear independent subset, one can then use Lemma 4.1 to compute a basis of $\mathcal{M}(\mathbb{Z})$.

Lemma 4.3. *Let $\mathcal{M}$ be a subspace of $M_k(\Gamma_1(N))$ that is stable under the $\mathrm{Aut}(\mathbb{C})$-action. Let $\{h_1, \ldots, h_s\}$ be a subset of $\mathcal{M}$ that is not contained in any proper subspace of $\mathcal{M}$ stable under the $\mathrm{Aut}(\mathbb{C})$-action. Further assume that for each $1 \leq i \leq s$, we have $h_i \in \mathcal{M}(\mathcal{O}_{L_i})$ for a number field $L_i \subseteq \mathbb{C}$.*

For each $1 \leq i \leq s$, choose an $a_i \in \mathcal{O}_{L_i}$ such that $L = \mathbb{Q}[a_i]$. Then the set

$$\left\{ \mathrm{Tr}_{L_i/\mathbb{Q}}(a_i^{j-1} h_i) : 1 \leq i \leq s,\ 1 \leq j \leq [L_i : \mathbb{Q}] \right\} \tag{4.1}$$

spans $\mathcal{M}$ and generates a finite index subgroup of $\mathcal{M}(\mathbb{Z})$.

Proof. Let S be the set (4.1) and let W be the span of S in $\mathcal{M}$. The set W is stable under the action of $\mathrm{Aut}(\mathbb{C})$ since $S \subseteq \mathcal{M}(\mathbb{Z})$. So to prove that S spans $\mathcal{M}$, it suffices to show that each h_e is in W for each $1 \leq e \leq s$.

Fix $1 \leq e \leq s$. Set $d = [L_e : \mathbb{Q}]$ and let $\sigma_1, \ldots, \sigma_d\colon L_e \hookrightarrow \mathbb{C}$ be the distinct complex embeddings of L_e. For any $1 \leq j \leq d$, we have

$$\mathrm{Tr}_{L_e/\mathbb{Q}}(a_e^{j-1} h_e) = \sum_{i=1}^{d} \sigma_i(a_e)^{j-1} \cdot \sigma_i(h_e). \tag{4.2}$$

The $d \times d$ matrix B with $B_{i,j} = \sigma_i(a_e)^{j-1}$ has determinant $\prod_{1 \leq i < j \leq d}(\sigma_j(a_e) - \sigma_i(a_e)) \neq 0$. Therefore from (4.2), we find that each $\sigma_i(h_e)$ is in the complex vector space spanned by $\{\mathrm{Tr}_{L_e/\mathbb{Q}}(a_e^{j-1} h_e) : 1 \leq j \leq d\}$. In particular, h_e is an element of W. Since we took any $1 \leq e \leq s$, this proves that S spans W. □

4.2. **Newforms.** A newform of weight k and level N is a cusp form $f \in S_k(\Gamma_1(N))$ that is an eigenform for all the Hecke operators T_n and satisfies $a_1(f) = 1$. We have $T_n(f) = a_n(f) f$ for all $n \geq 1$. Let $\mathcal{N}(k, N)$ be the set of newforms of level N. The set $\mathcal{N}(k, N) \subseteq S_k(\Gamma_1(N))$ is stable under the action of $\mathrm{Aut}(\mathbb{C})$.

Fix a newform $f \in \mathcal{N}(k, N)$. The coefficients of the q-expansion of f generate a number field L whose degree we will denote by g. One can compute the field L and can also compute an arbitrary number of terms of the q-expansion of f, see Algorithm 9.14 in [Ste07] when $k \geq 2$ for an algorithm using modular symbols.

We now briefly discuss the harder excluded $k = 1$ case. For an odd character $\varepsilon\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, one can compute a basis of

$$M_1(\Gamma_1(N))(\varepsilon) := \{f \in M_1(\Gamma_1(N)) :\ f|\langle d \rangle = \varepsilon(d) f \text{ for all } d \in (\mathbb{Z}/N\mathbb{Z})^\times\}$$

for which we can determine arbitrarily many terms of their q-expansions and all the coefficients lie in a cyclotomic extension; for example, see [Sch15]. The action of the Hecke operators T_n on a modular form in $M_1(\Gamma_1(N))(\chi)$ can be computed from its q-expansion. From this, we can compute a basis of $M_1(\Gamma_1(N)) = \oplus_\varepsilon M_1(\Gamma_1(N))(\varepsilon)$ for which we can determine arbitrarily many terms of their q-expansions (and all the coefficients lie in a cyclotomic extension) and we know the action of the diamond and Hecke operators with respect to this basis. By simultaneously diagonalizing the action of T_p for several small primes p, we can compute the newforms in $\mathcal{N}(1, N)$ (we can check that a modular form $f \in M_1(\Gamma_1(N))$ is a cusp form by verifying that $f^2 \in S_2(\Gamma_1(N))$).

4.3. **Pseudo-eigenvalues.** We now describe how the Atkin–Lehner operator W_N acts on a newform $f \in \mathcal{N}(k, N)$.

Proposition 4.4. *For $f \in \mathcal{N}(k, N)$, we have*

$$f|W_N = \lambda_N(f) \cdot (-1)^k N^{k/2} \cdot \overline{f},$$

where $\lambda_N(f) \in \mathbb{C}$ is an algebraic number with absolute value 1 and $\overline{f} \in \mathcal{N}(k, N)$ is obtained by applying complex conjugation to the coefficients of the q-expansion of f.

Proof. See §1 and Theorem 1.1 of [AL78]. Note that our Atkin–Lehner operators are normalized differently and the proposition is stated so that $\lambda_N(f)$ agrees with the value from [AL78]. □

The number $\lambda_N(f)$ is called the pseudo-eigenvalue of f. In special cases, one has a closed expression for $\lambda_N(f)$. For example, if N is squarefree, then an expression for $\lambda_N(f)$ in terms of Gauss sums can be found in [Asa76].

Let $\varepsilon_f \colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$ be the nebentypus of f; it is the unique such Dirichlet character satisfying $f|\langle d\rangle = \varepsilon_f(d) f$ for all $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. Note that one can determine ε_f from the q-expansion of f since $a_{p^2}(f) = a_p(f)^2 - \varepsilon_f(p)p^{k-2}$ for all primes $p \nmid N$.

4.3.1. *Approximating pseudo-eigenvalues.* For a fixed newform $f \in \mathcal{N}(k, N)$, we now describe how to numerically approximate $\lambda_N(f) \in \mathbb{C}$ from enough terms of the q-expansion of f.

For a real number $b > 0$, substituting $\tau = i \cdot b/N^{1/2}$ into the equation from Proposition 4.4 gives

$$(i \cdot b/N^{1/2})^{-k} \cdot f(i \cdot b^{-1}/N^{1/2}) = \lambda_N(f) \cdot (-1)^k N^{k/2} \cdot \overline{f}(i \cdot b/N^{1/2})$$

and hence

$$i^k b^{-k} \sum_{n=1}^{\infty} a_n(f)\,(e^{-2\pi/(bN^{1/2})})^n = \lambda_N(f) \sum_{n=1}^{\infty} \overline{a_n(f)}\,(e^{-2\pi b/N^{1/2}})^n. \tag{4.3}$$

If we know the coefficient $a_n(f)$ for all $n \le N$, then we can compute the sums $\sum_{n=1}^{N} a_n(f)\,(e^{-2\pi/(bN^{1/2})})^n$ and $\sum_{n=1}^{N} \overline{a_n(f)}\,(e^{-2\pi b/N^{1/2}})^n$. We can then approximate the series in (4.3); the error terms of these approximations can be bounded using that $|a_n(f)| \le d(n)n^{k/2}$ by Deligne, where $d(n)$ is the number of divisors of n.

If $\overline{f}(i \cdot b/N^{1/2})$ is non-zero, then (4.3) gives a formula for $\lambda_N(f)$ that can be used to approximate it by computing enough terms of each series. Note that we have $\overline{f}(i \cdot b/N^{1/2}) \neq 0$ away from a discrete set of $b > 0$ since $\overline{f}$ is non-zero and holomorphic. In practice, one wants to choose b close to 1; this ensure that both series converge absolutely at a similar rate.

4.4. **Atkin–Lehner–Li theory.** For background, see §9.2 of [Ste07]. For positive divisors M of N and d of N/M, we have a degeneracy map

$$\alpha_d \colon S_k(\Gamma_1(M)) \hookrightarrow S_k(\Gamma_1(N)), \quad f(\tau) \mapsto f(d\tau).$$

On q-expansions, we have $\alpha_d(\sum_{n=1}^{\infty} a_n q^n) = \sum_{n=1}^{\infty} a_n q^{dn}$.

The old subspace of $S_k(\Gamma_1(N))$ is the subspace generated by $\alpha_d(S_k(\Gamma_1(M)))$ for all positive divisors $M|N$ with $M \neq N$ and $d|(N/M)$; we denote it by $S_k(\Gamma_1(N))_{\text{old}}$. The new subspace of $S_k(\Gamma_1(N))$, which we denote by $S_k(\Gamma_1(N))_{\text{new}}$, is the orthogonal complement of the subspace $S_k(\Gamma_1(N))_{\text{old}}$ of $S_k(\Gamma_1(N))$ with respect to the Petersson inner product. The set $\mathcal{N}(k, N)$ of newforms is a basis of $S_k(\Gamma_1(N))_{\text{new}}$. We have a decomposition

$$S_k(\Gamma_1(N)) = \bigoplus_{M|N} \bigoplus_{d|\frac{N}{M}} \alpha_d(S_k(\Gamma_1(M))_{\text{new}}). \tag{4.4}$$

Lemma 4.5. *Take any positive divisors $M|N$ and $d|(N/M)$, and set $e := N/(dM)$. For any $f \in S_k(\Gamma_1(M))_{\text{new}}$ and $m \in (\mathbb{Z}/N\mathbb{Z})^\times$, we have*

$$\alpha_d(f)|W_N = e^k\, \alpha_e(f|W_M) \quad \textit{and} \quad \alpha_d(f)|\langle m\rangle = \alpha_d(f|\langle m\rangle).$$

Proof. We have

$$\begin{aligned}\alpha_d(f)|W_N &= d^{-k/2}N^{k/2}(f|\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right))|\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)\\ &= d^{-k/2}N^{k/2}M^{-k/2}(f|W_M)|(\left(\begin{smallmatrix} 0 & -1 \\ M & 0 \end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right))\\ &= e^{k/2}(f|W_M)|(\left(\begin{smallmatrix} 0 & -1 \\ M & 0 \end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right))\\ &= e^{k/2}(f|W_M)|\begin{pmatrix} N/M & 0 \\ 0 & d \end{pmatrix} = e^{k/2}(f|W_M)|\left(\begin{smallmatrix} e & 0 \\ 0 & 1 \end{smallmatrix}\right) = e^k\alpha_e(f|W_M).\end{aligned}$$

Now take any $m \in (\mathbb{Z}/N\mathbb{Z})^\times$ and choose an $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ satisfying $\gamma \equiv \left(\begin{smallmatrix} m^{-1} & 0 \\ 0 & m \end{smallmatrix}\right) \pmod N$. We have

$$\alpha_d(f|\langle m\rangle) = d^{-k/2}\, f|(\gamma\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)) = \alpha_d(f)|(\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}\gamma\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)) = \alpha_d(f)|\langle m\rangle,$$

where the last equality uses that $\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)^{-1}\gamma\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)$ is in $\mathrm{SL}_2(\mathbb{Z})$ and is congruent to $\left(\begin{smallmatrix} m^{-1} & * \\ 0 & m \end{smallmatrix}\right)$ modulo N. □

4.5. **The space $\mathcal{M}_f$.** Fix a newform $f \in \mathcal{N}(k, N)$. The coefficients of the q-expansion of f generate a number field L whose degree we will denote by g. As noted in §4.2, one can compute the field L and arbitrarily many terms of the q-expansion of f. Fix an $a \in \mathcal{O}_L$ satisfying $L = \mathbb{Q}[a]$.

We define $\mathcal{M}_f$ to be the subspace of $S_k(\Gamma_1(N))$ generated by $\sigma(f)$ with $\sigma \in \mathrm{Aut}(\mathbb{C})$. Moreover, the set $\{\sigma_1(f), \dots, \sigma_g(f)\}$ is a basis of $\mathcal{M}_f$, where $\sigma_1, \dots, \sigma_g \colon L \hookrightarrow \mathbb{C}$ are the distinct complex embeddings of L. By Lemma 4.3, the set

$$\left\{ \mathrm{Tr}_{L/\mathbb{Q}}(a^{j-1}f) : 1 \le j \le g \right\} \tag{4.5}$$

spans $\mathcal{M}_f$ and generates a finite index subgroup of $\mathcal{M}_f(\mathbb{Z})$. Moreover, the set (4.5) is a basis of the g-dimensional vector space $\mathcal{M}_f$. In particular, $\mathcal{M}_f(\mathbb{Z})$ spans $\mathcal{M}_f$. Since we can compute arbitrarily many terms of the q-expansion of f, we can compute arbitrarily many terms of the q-expansion of the modular forms in the set (4.5). By Lemma 4.1, we can find a basis $f_1, \dots, f_g$ of the $\mathbb{Z}$-module $\mathcal{M}_f(\mathbb{Z})$ such that an arbitrary number of terms in the q-expansion of each f_i can be computed.

The space $\mathcal{M}_f$ is stable under the action of W_N since by Proposition 4.4, we have

$$\sigma(f)|W_N = \lambda_N(\sigma(f)) \cdot (-1)^k N^{k/2} \cdot \overline{\sigma(f)}$$

for each $\sigma \in \mathrm{Aut}(\mathbb{C})$. The space $\mathcal{M}_f$ is stable under the action of $\langle d\rangle$, with $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, since $\sigma(f)|\langle d\rangle = \varepsilon_{\sigma(f)}(d)\,\sigma(f)$ for each $\sigma \in \mathrm{Aut}(\mathbb{C})$.

We have now verified the following.

Lemma 4.6. *For each $f \in \mathcal{N}(k, N)$, $\mathcal{M}_f$ satisfies the conditions (a)–(d) from §1.2.*

4.6. **Cusp forms.** Since $\mathcal{N}(k, N)$ is a basis of $S_k(\Gamma_1(N))_{\mathrm{new}}$, we have

$$S_k(\Gamma_1(N))_{\mathrm{new}} = \bigoplus_{f \in \mathcal{N}'(k,N)} \mathcal{M}_f,$$

where $\mathcal{N}'(k, N)$ is a set of representatives of the $\mathrm{Aut}(\mathbb{C})$-orbits on $\mathcal{N}(k, N)$. By (4.4), we have

$$S_k(\Gamma_1(N)) = \bigoplus_{M|N} \bigoplus_{f \in \mathcal{N}'(k,M)} \bigoplus_{d|\frac{N}{M}} \alpha_d(\mathcal{M}_f) = \bigoplus_{f \in \mathcal{N}'(k,M)} \bigoplus_{M|N} \bigoplus_{de=N/M,\, d \le e} \mathcal{M}_{f,d}, \tag{4.6}$$

where for $d|(N/M)$ and $e = (N/M)/d$ we define

$$\mathcal{M}_{f,d} := \begin{cases} \alpha_d(\mathcal{M}_f) \oplus \alpha_e(\mathcal{M}_f) & \text{if } d \ne e, \\ \alpha_d(\mathcal{M}_f) & \text{if } d = e. \end{cases}$$

Lemma 4.7. *Take any positive divisors $M|N$ and $d|(N/M)$, and set $e := (N/M)/d$. Then for any newform $f \in \mathcal{N}(k, M)$, $\mathcal{M}_{f,d}$ satisfies conditions (a)–(d) of §1.2.*

Proof. From Lemma 4.6, $\mathcal{M}_f$ satisfies the conditions (a)–(d) from §1.2 with N replaced by M. There is a basis $f_1, \dots, f_g$ of the $\mathbb{Z}$-module $\mathcal{M}_f(\mathbb{Z})$ that is a basis of $\mathcal{M}_f$ and for which arbitrary number of terms of the q-expansion of each f_i can be computed.

Since $\mathcal{M}_f$ is stable under the action of W_M and the diamond operators, Lemma 4.5 implies that $\mathcal{M}_{f,d}$ is stable under the action of W_N and the diamond operators. The set $\{\alpha_d(f_1), \dots, \alpha_d(f_g), \alpha_e(f_1), \dots, \alpha_e(f_g)\}$ generates a finite index subgroup of $\mathcal{M}_{f,d}(\mathbb{Z})$ and spans $\mathcal{M}_{f,d}$. By Lemma 4.1, we can find a basis of $\mathcal{M}_{f,d}(\mathbb{Z})$ for which an arbitrary number of terms of the q-expansions can be computed. We have thus verified that $\mathcal{M}_{f,d}$ satisfies conditions (a)–(d). □

Now take any congruence subgroup $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$. Let H be the subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ such that Γ consists of the matrices in $\mathrm{SL}_2(\mathbb{Z})$ whose image modulo N is of the form $\left(\begin{smallmatrix} h^{-1} & * \\ 0 & h \end{smallmatrix}\right)$ for some $h \in H$. By (4.6), we have

$$S_k(\Gamma) = \bigoplus_{M \mid N} \bigoplus_{\substack{f \in \mathcal{N}'(k,M) \\ \varepsilon_f(H)=1}} \bigoplus_{\substack{d \mid \frac{N}{M} \\ d \le (N/M)^{1/2}}} \mathcal{M}_{f,d}.$$

The following proposition is now an immediate consequence of Lemmas 4.7 and 4.2.

Proposition 4.8. *The space $S_k(\Gamma)$ satisfies conditions (a)–(d) of §1.2.*

4.7. **Eisenstien series.** Fix a congruence subgroup $\Gamma_1(N) \subseteq \Gamma \subseteq \Gamma_0(N)$ and let H be a subgroup of $(\mathbb{Z}/N\mathbb{Z})^\times$ associated to Γ as in §4.6. Let $E_k(\Gamma)$ be the Eisenstein subspace of $M_k(\Gamma)$. We have

$$M_k(\Gamma) = E_k(\Gamma) \oplus S_k(\Gamma).$$

Let χ_1 and χ_2 be primitive Dirichlet characters modulo N_1 and N_2, respectively, satisfying $(\chi_1\chi_2)(-1) = (-1)^k$. For each integer $e \ge 1$, define the Eisenstein series

$$F_k(\chi_1, \chi_2, e)(\tau) = c_0 + \sum_{n=1}^{\infty} \sigma_{k-1}(\chi_1, \chi_2, n) q^{ne},$$

where

$$\sigma_{k-1}(\chi_1, \chi_2, n) := \sum_{d \mid n, d \ge 1} d^{k-1} \chi_1(d) \chi_2(n/d),$$

$c_0 = 0$ if $N_2 \neq 1$, and $c_0 = -B_{k,\chi_1}/(2k)$ if $N_2 = 1$ (where $B_{k,\chi}$ is a generalized Bernoulli number, cf. §5 of [Ste07]).

Except for the case with $k = 2$ and $\chi_1 = \chi_2 = 1$, $F_k(\chi_1, \chi_2, e)$ is an element of $M_k(\Gamma_1(N_1N_2e))$. Note that $F_k(\chi_1, \chi_2, e)$ satisfies $F_k(\chi_1, \chi_2, e)|\langle d \rangle = (\chi_1\chi_2)(d) \cdot F_k(\chi_1, \chi_2, e)$ for all $d \in (\mathbb{Z}/N_1N_2e\mathbb{Z})^\times$. If $k = 2$, $\chi_1 = \chi_2 = 1$ and $e > 1$, then $F_k(\chi_1, \chi_2, 1) - eF_k(\chi_1, \chi_2, e)$ is an element of $M_2(\Gamma_0(e))$.

The set B of Eisenstein series as above with N_1N_2e dividing N and $(\chi_1\chi_2)(H) = 1$ form a basis of $E_k(\Gamma)$; this follows from Theorem 5.9 of [Ste07].

We can compute an arbitrary number of terms of the q-expansion of modular forms in B. We also know the action of the diamond operators with respect to the basis B. For each $f \in B$, we can also compute arbitrarily many terms in the q-expansion of $f|W_N$; for example, see §2.2 of [Coh19].

Proposition 4.9. *The space $M_k(\Gamma)$ satisfies conditions (a)–(d) of §1.2.*

Proof. The space $M_k(\Gamma)$ is indeed stable under the actions of W_N and the diamond operators. By Proposition 4.8, there is a basis B' of $S_k(\Gamma, \mathbb{Z})$ that spans $S_k(\Gamma)$ and for which we can compute arbitrarily many terms of their q-expansions. The set $B \cup B'$ spans $M_k(\Gamma)$. By Lemmas 4.3 and 4.1, we can find a basis of $M_k(\Gamma, \mathbb{Z})$ that spans $M_k(\Gamma)$ and for which we can compute arbitrarily many terms of their q-expansions. □

4.8. **Numerically approximations for the Atkin–Lehner action.** Take any modular form $h \in M_k(\Gamma_1(N), \mathbb{Z})$ for which we can compute arbitrarily many terms of its q-expansion. We now explain how we can approximate each coefficient of $h|W_N$ to arbitrary accuracy in $\mathbb{C}$. In the setting of §1.2, this will allow us to approximate the entries of the matrix W to arbitrary accuracy.

Let B be the basis of $E_k(\Gamma_1(N))$ from §4.7. Define

$$B' := \bigcup_{M|N,\, d|(N/M)} \{\alpha_d(f) : f \in \mathcal{N}(k, M)\};$$

The set B' is a basis of $S_k(\Gamma_1(N))$ from (4.7) and hence $B \cup B'$ is a basis of $M_k(\Gamma_1(N))$. For each $f \in B \cup B'$, every coefficient $a_n(f)$ in $\mathbb{C}$ is algebraic and can be computed to arbitrary accuracy. Expressing h in terms of the basis $B \cup B'$, it suffices to explain how for each $f \in B \cup B'$ we can approximate any coefficient of $f|W_N$ to arbitrary accuracy in $\mathbb{C}$.

If $f \in B$, we can compute arbitrarily many terms of the q-expansion of $f|W_N$, cf. §2.2 of [Coh19]. Finally consider any element in B'; it is of the form $\alpha_d(f)$ with $f \in \mathcal{N}(k, M)$. We can compute any coefficient of $\alpha_d(f)$ to arbitrary accuracy in $\mathbb{C}$ by using Lemma 4.5 and Proposition 4.4 (approximations of $\lambda_M(f)$ can be found as in §4.3.1).

5. Verification of the algorithm

We now verify the validity of the algorithm from §1.3. Recall that Q is the smallest positive divisor of N for which the action of $\langle d \rangle$ on $\mathcal{M}$ depends only on the value of d modulo Q. By Theorem 2.1(ii), we find that $\langle d \rangle$ acts on $\mathcal{M}(\mathbb{Z})$ with inverse $\langle d^{-1} \rangle$. Therefore, each D_d lies in $\mathrm{GL}_g(\mathbb{Z})$.

Lemma 5.1. *For any $f \in \mathcal{M}(\mathbb{Z})$, the modular form $B_{k,N} \cdot f|W_N$ has Fourier coefficients in $\mathbb{Z}[\zeta_Q]$.*

Proof. Fix a modular form $f \in \mathcal{M}(\mathbb{Z})$. Take any automorphism σ of $\mathbb{C}$ that fixes $\mathbb{Q}(\zeta_Q)$. By Theorem 2.1(iii) and using that f has rational coefficients, we find that

$$\sigma(f|W_N) = (f|W_N)|\langle \chi_N(\sigma) \rangle = f|W_N,$$

where the last equality uses that $f|W_N \in \mathcal{M}$ and that $\chi_N(\sigma) \equiv 1 \pmod{Q}$ since σ fixes ζ_Q. We deduce that $f|W_N$, and hence also $B_{k,N} \cdot f|W_N$, has coefficients in $\mathbb{Q}(\zeta_Q)$ since σ is an arbitrary automorphism of $\mathbb{C}$ that fixes $\mathbb{Q}(\zeta_Q)$. By Theorem 3.1(i), the Fourier coefficients of $B_{k,N} \cdot f|W_N$ are algebraic integers. We deduce that $B_{k,N} \cdot f|W_N$ has coefficients in $\mathbb{Z}[\zeta_Q]$ which is the ring of integers of $\mathbb{Q}(\zeta_Q)$. □

Lemma 5.2. *For any $f \in \mathcal{M}(\mathbb{Z}[\zeta_Q])$, we have $\alpha f = b_1 f_1 + \cdots b_g f_g$ with $b_i \in \mathbb{Z}[\zeta_Q]$.*

Proof. There is no harm in changing the basis $f_1, \ldots, f_g$ of $\mathcal{M}(\mathbb{Z})$. In particular, we may assume $f_1, \ldots, f_g$ are chosen so that the matrix A of §1.3 is in Hermite normal form. Let a_j be the leading coefficient of the q-expansion of f_j. The pivots of the matrix A are $a_1, \ldots, a_g$ and hence $\alpha = a_1 \cdots a_g$. We have $f = c_1 f_1 + \cdots + c_g f_g$ for unique $c_i \in \mathbb{Q}(\zeta_Q)$.

We claim that $a_1 \cdots a_i \cdot c_i$ is an element of $\mathbb{Z}[\zeta_Q]$ for all $1 \le i \le g$. Suppose that the claim is false and let $1 \le j \le g$ be the minimal value for which $a_1 \cdots a_j \cdot c_j \notin \mathbb{Z}[\zeta_Q]$. Therefore,

$$\sum_{i=j}^{g} (a_1 \cdots a_{j-1}\, c_i)\, f_i = a_1 \cdots a_{j-1} \cdot f - \sum_{i=1}^{j-1} (a_1 \cdots a_{j-1}\, c_i)\, f_i \tag{5.1}$$

has coefficients in $\mathbb{Z}[\zeta_Q]$, where we have used that f and the f_i have coefficients in $\mathbb{Z}[\zeta_Q]$ and the minimality of j. The leading coefficients of (5.1) is $a_1 \cdots a_{j-1} c_j \cdot a_j$ since we have chosen the basis $f_1, \ldots, f_g$ so that A is in Hermite normal form. So $a_1 \cdots a_j \cdot c_j \in \mathbb{Z}[\zeta_Q]$ which contradicts the choice of j and thus proves the claim.

By the above claim, we have $\alpha c_i \in \mathbb{Z}[\zeta_Q]$ for all $1 \le i \le g$ since $\alpha = a_1 \cdots a_g$. This proves the lemma with $b_i = \alpha c_i$. □

Lemma 5.3. *The matrix $B_{k,N}\alpha \cdot W$ lies in $M_g(\mathbb{Z}[\zeta_Q])$.*

Proof. Take any $1 \le j \le g$. By Lemma 5.1 and our assumption that $\mathcal{M}$ is stable under the action of W_N, we have $B_{k,N} \cdot f_j|W_N \in \mathcal{M}(\mathbb{Z}[\zeta_Q])$. By Lemma 5.2, we deduce that $B_{k,N}\alpha \cdot f_j|W_N = \sum_{i=1}^{g} b_{j,i} f_i$ with $b_{j,i} \in \mathbb{Z}[\zeta_Q]$. From the definition of the matrix W, we find that $B_{k,N}\alpha \cdot W_{j,i} = b_{j,i}$ for all $1 \le i \le g$. Since j was arbitrary, we deduce that the entries of $B_{k,N}\alpha \cdot W$ lies in $\mathbb{Z}[\zeta_Q]$. □

We now describe the natural Galois action on the matrix W.

Lemma 5.4. *For each $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_Q)/\mathbb{Q})$, we have $\sigma(W) = W \cdot D_{\chi_Q(\sigma)}$.*

Proof. Take any $1 \le j \le g$. By the definition of the matrix W, we have $f_j|W_N = \sum_{k=1}^{g} W_{j,k} \cdot f_k$. Therefore,

$$\sigma(f_j|W_N) = \sum_{k=1}^{g} \sigma(W_{j,k}) \cdot \sigma(f_k) = \sum_{k=1}^{g} \sigma(W_{j,k}) \cdot f_k,$$

where we have used that each f_k has coefficients in $\mathbb{Z}$. Set $d := \chi_N(\sigma) \in (\mathbb{Z}/N\mathbb{Z})^\times$. By Theorem 2.1(iii) and using that f_j has integer coefficients, we have $\sigma(f_j|W_N) = (f_j|W_N)|\langle d\rangle$. Using the definition of W and D_d, we deduce that

$$\sigma(f_j|W_N) = (f_j|W_N)|\langle d\rangle = \sum_{i=1}^{g} W_{j,i} \cdot f_i|\langle d\rangle = \sum_{i=1}^{g} W_{j,i} \cdot \sum_{k=1}^{g} (D_d)_{i,k} \cdot f_k = \sum_{k=1}^{g} (W D_d)_{j,k} \cdot f_k.$$

By comparing our two expressions for $\sigma(f_j|W_N)$, we find that $\sigma(W)_{j,k} = (W D_d)_{j,k}$ for all $1 \le k \le g$. Since $1 \le j \le g$ was arbitrary, we conclude that $\sigma(W) = W D_d$. Finally, we note that D_d depends only on d modulo Q and $d \equiv \chi_Q(\sigma) \pmod{Q}$. □

We have $W \in M_g(\mathbb{Q}(\zeta_Q))$ by Lemma 5.3. For each integer $0 \le b \le \varphi(Q) - 1$, define the matrix

$$\beta_b := \mathrm{Tr}_{\mathbb{Q}(\zeta_Q)/\mathbb{Q}}(\zeta_Q^b W) \in M_g(\mathbb{Q}). \tag{5.2}$$

By Lemma 5.3, we have $B_{k,N}\alpha\, W \in M_g(\mathbb{Z}[\zeta_Q])$ and hence $B_{k,N}\alpha \cdot \beta_b \in M_g(\mathbb{Z})$. We have

$$\beta_b = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_Q)/\mathbb{Q})} \sigma(\zeta_Q)^b \cdot \sigma(W) = \sum_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_Q)/\mathbb{Q})} \zeta_Q^{\chi_Q(\sigma)\cdot b} \cdot W \cdot D_{\chi_Q(\sigma)},$$

where the last equality uses Lemma 5.4. Therefore,

$$\beta_b = W \cdot \sum_{d \in (\mathbb{Z}/Q\mathbb{Z})^\times} \zeta_Q^{db} D_d$$

which agrees with the definition of β_b given in §1.3.

In §4.8, we explained how to numerical approximate the matrices W and D_d in $M_g(\mathbb{C})$. Since D_d has integer entries, it can be determined by a sufficiently accurate approximation. So an approximation of W gives an approximation of the matrix β_b. Since $N_{k,N}\alpha\, \beta_b$ has integer entries, we can thus determine β_b from a sufficiently accurate approximation of W in $M_g(\mathbb{C})$.

Finally, in §1.3, we observed that W is the unique matrix in $M_g(\mathbb{Q}(\zeta_Q))$ that satisfies $\mathrm{Tr}_{\mathbb{Q}(\zeta_Q)/\mathbb{Q}}(\zeta_Q^b W) = \beta_b$ for all $0 \le b \le \varphi(Q) - 1$. Moreover, it is straightforward to compute W given the matrices β_b.

6. Modular curves

Fix a positive integer $N \ge 1$. The group $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper half plane $\mathfrak{H}$ via linear fractional transformations. The quotient $\Gamma(N)\backslash\mathfrak{H}$ is a Riemann surface and can be completed to a compact and smooth Riemann surface $\mathcal{X}_N$.

Every meromorphic function f on $\mathcal{X}_N$ has a q-expansion $\sum_{n\in\mathbb{Z}} c_n(f) q_N^n$, where the $c_n(f) \in \mathbb{C}$ are 0 for all but finitely many negative $n \in \mathbb{Z}$. Let $\mathcal{F}_N$ be the field consisting of all meromorphic functions f on $\mathcal{X}_N$ for which $c_n(f)$ lies in $\mathbb{Q}(\zeta_N)$ for all n. For example, $\mathcal{F}_1 = \mathbb{Q}(j)$, where j is the modular j-invariant.

Lemma 6.1. *There is a unique right action $*$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on the field $\mathcal{F}_N$ such that the following hold for all $f \in \mathcal{F}_N$:*

(a) *For $A \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, we have $(f * A)(\tau) = f(\gamma\tau)$, where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is any matrix congruent to A modulo N.*

(b) *For $A = \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, the q-expansion of $f * A$ is $\sum_{n\in\mathbb{Z}} \sigma_d(c_n(f))q_N^n$, where σ_d is the automorphism of the field $\mathbb{Q}(\zeta_N)$ that satisfies $\sigma_d(\zeta_N) = \zeta_N^d$.*

Proof. This follows from Theorem 6.6 and Proposition 6.9 of [Shi94]. □

For a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, let $\mathcal{F}_N^G$ be the subfield of $\mathcal{F}_N$ fixed by G under the action of Lemma 6.1.

Lemma 6.2.

(i) *The matrix $-I$ acts trivially on $\mathcal{F}_N$ and the right action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ on $\mathcal{F}_N$ is faithful.*

(ii) *We have $\mathcal{F}_N^{\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})} = \mathcal{F}_1 = \mathbb{Q}(j)$ and $\mathcal{F}_N^{\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})} = \mathbb{Q}(\zeta_N)(j)$.*

(iii) *The field $\mathbb{Q}(\zeta_N)$ is algebraically closed in $\mathcal{F}_N$.*

Proof. This also follows from Theorem 6.6 and Proposition 6.9 of [Shi94]. □

Let G be a subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ and $-I \in G$. By Lemma 6.2, the field $\mathcal{F}_N^G$ has transcendence degree 1 and $\mathbb{Q}$ is algebraically closed in $\mathcal{F}_N^G$.

We define the modular curve X_G to be the smooth, projective and geometrically irreducible curve over $\mathbb{Q}$ with function field $\mathcal{F}_N^G$. We can identify $X_G(\mathbb{C})$ with the compact and smooth Riemann surface that completes $\Gamma_G\backslash\mathfrak{H}$, where Γ_G is the congruence subgroup consisting of matrices in $\mathrm{SL}_2(\mathbb{Z})$ whose image modulo N lies in G.

We now describe how the modular curves X_G are related to understanding the Galois action on the torsion points of elliptic curves; this is given for background purposes and will not be used elsewhere in the paper. Let $\pi_G\colon X_G \to \operatorname{Spec}\mathbb{Q}[j] \cup \{\infty\} = \mathbb{P}^1_{\mathbb{Q}}$ be the morphism arising from the inclusion $\mathbb{Q}(j) \subseteq \mathcal{F}_N^G$. In particular, we may view $\pi_G(X_G(\mathbb{Q}))$ as a subset of $\mathbb{Q} \cup \{\infty\}$.

Consider an elliptic curve $E/\mathbb{Q}$ whose j-invariant we denote by $j_E \in \mathbb{Q}$. Let $E[N]$ be the N-torsion subgroup of $E(\overline{\mathbb{Q}})$, where $\overline{\mathbb{Q}}$ is a fixed algebraic closure of $\mathbb{Q}$. The group $E[N]$ is a free $\mathbb{Z}/N\mathbb{Z}$-module of rank 2 and has a natural action of $\mathrm{Gal}_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ that respects the group structure. By choosing a basis for $E[N]$, the Galois action can be expressed by a representation

$$\rho_{E,N}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

The subgroup $\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}})$ of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ is uniquely defined up to conjugacy.

Let G^t be the subgroup of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ obtained by taking the transpose of the elements of G. Suppose further that $j_E \notin \{0, 1728\}$; equivalently, the automorphism group of the elliptic curve $E_{\overline{\mathbb{Q}}}$ is cyclic of order 2. Then $\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}})$ is conjugate in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ to a subgroup of G^t if and only if j_E is an element of $\pi_G(X_G(\mathbb{Q}))$, cf. Proposition 3.3 of [Zyw15] (the transpose arises because the action in Proposition 3.1 of [Zyw15] is slightly different than ours). So the modular curves X_G, and their morphisms π_G, contain information about the images of $\rho_{E,N}$ for elliptic curves $E/\mathbb{Q}$ with $j_E \notin \{0, 1728\}$.

Remark 6.3.

(i) The assumptions $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$ and $-I \in G$ are natural in this elliptic curve setting. We have $\det(\rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}})) = (\mathbb{Z}/N\mathbb{Z})^\times$ and the group $\langle \rho_{E,N}(\mathrm{Gal}_{\mathbb{Q}}), -I\rangle$, up to conjugacy in $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$, depends only on j_E.

(ii) The occurrence of G^t is due to the fact that in this paper we have natural right actions while we usually view the action of $\mathrm{Gal}_{\mathbb{Q}}$ on $E[N]$ as a left action. Sometimes in the literature, for example in [Zyw15], the modular curve corresponding to the group G agrees with our X_{G^t}.

6.1. **The canonical ring.** This section is dedicated to describing the canonical ring $R_{X_G} := \bigoplus_{k\geq 0} H^0(X_G, \Omega_{X_G}^{\otimes k})$ of X_G, and in particular $H^0(X_G, \Omega_{X_G})$, in terms of cusps forms. This is certainly well-known, but lacking a reference we give a quick demonstration.

We now fix an integer $k \geq 0$. Take any $\omega \in H^0(X_G, \Omega_{X_G}^{\otimes k})$. The form ω induces a differential k-form on $X_G(\mathbb{C})$; on $\mathfrak{H}$ it equals $(2\pi i)^k f(\tau)\,(d\tau)^k$ for a unique cusp form $f \in S_{2k}(\Gamma_G, \mathbb{C})$. We define $\alpha_k(\omega) := f$.

In §1.5, we defined a right action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $S_{2k}(\Gamma(N), \mathbb{Q}(\zeta_N))$; we also denote it by $*$.

Lemma 6.4. *The cusp form $\alpha_k(\omega)$ lies in $S_{2k}(\Gamma(N), \mathbb{Q}(\zeta_N))^G$ for all $\omega \in H^0(X_G, \Omega_{X_G}^{\otimes k})$.*

Proof. Take any $\omega \in H^0(X_G, \Omega_{X_G}^{\otimes k})$ and set $f := \alpha_k(\omega) \in S_{2k}(\Gamma_G, \mathbb{C})$. Choose a non-constant $u \in \mathcal{F}_N^G$. We have $\omega = v(du)^k$ for a unique modular function $v \in \mathcal{F}_N^G$. The form ω on $X_G(\mathbb{C})$ arises from the form $v(\tau)u'(\tau)^k(d\tau)^k$ on $\mathfrak{H}$. Therefore, $f(\tau) = (2\pi i)^{-k} v(\tau)u'(\tau)^k$.

We claim that the coefficients of the q-expansion of f lie in $\mathbb{Q}(\zeta_N)$. The coefficients of the q-expansion of v are in $\mathbb{Q}(\zeta_N)$ since $v \in \mathcal{F}_N$. So to prove the claim, it suffices to show that $(2\pi i)^{-1}u'(\tau)$ has a q-expansion with coefficients in $\mathbb{Q}(\zeta_N)$. Since $u \in \mathcal{F}_N$, we have $u = \sum_{n\in\mathbb{Z}} c_n(u) q_N^n$ with $c_n(u) \in \mathbb{Q}(\zeta_N)$ that are 0 for all but finitely many negative n. Therefore, $(2\pi i)^{-1}u'(\tau) = \sum_{n\in\mathbb{Z}} n/N \cdot c_n(u) q_N^n$ which has coefficients in $\mathbb{Q}(\zeta_N)$. This proves the claim.

Now take any $A \in G$. Set $d = \det(A)$ and choose $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ so that $A \equiv \gamma \left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right) \pmod N$. Since $u \in \mathcal{F}_N^G$, we have $u(\tau) = (u * A)(\tau) = \sigma_d(u(\gamma\tau))$. The coefficients of $u(\gamma\tau)$ lie in $\mathbb{Q}(\zeta_N)$ since $u \in \mathcal{F}_N$ and $\mathcal{F}_N$ is stable under the right action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$. We have $u(\gamma\tau) = \sum_n b_n q_N^n$ with $b_n \in \mathbb{Q}(\zeta_N)$. Taking derivatives gives

$$(2\pi i)^{-1}u'(\tau) = (2\pi i)^{-1}\frac{d}{d\tau}\sigma_d(u(\gamma\tau)) = (2\pi i)^{-1}\frac{d}{d\tau}\sum_n \sigma_d(b_n)q_N^n = \sum_n n/N \cdot \sigma_d(b_n)q_N^n.$$

Therefore,

$$(2\pi i)^{-1}u'(\tau) = \sigma_d\Big(\sum_n n/N \cdot b_n q_N^n\Big) = \sigma_d\Big((2\pi i)^{-1}\frac{d}{d\tau}u(\gamma\tau)\Big) = \sigma_d\Big((2\pi i)^{-1}(u'|_2\gamma)(\tau)\Big). \tag{6.1}$$

Since $v \in \mathcal{F}_N^G$, we have $v(\tau) = (v*A)(\tau) = \sigma_d(v(\gamma\tau))$. Taking the k-power of both sides of (6.1) and multiplying by $v(\tau)$ gives

$$(2\pi i)^{-k}v(\tau)u'(\tau)^k = \sigma_d\big((2\pi i)^{-k}v(\tau)(u'|_2\gamma)^k(\tau)\big) = \sigma_d\Big(\big(((2\pi i)^{-k}v\,(u')^k)|_{2k}\gamma\big)(\tau)\Big);$$

equivalently, $f = \sigma_d(f|_{2k}\gamma)$. Therefore, $f = f * A$. Since A was an arbitrary element of G, we deduce that $f \in S_{2k}(\Gamma(N), \mathbb{Q}(\zeta_N))^G$. □

Using Lemma 6.4, we have a linear map

$$\alpha_k \colon H^0(X_G, \Omega_{X_G}^{\otimes k}) \to S_{2k}(\Gamma(N), \mathbb{Q}(\zeta_N))^G$$

of $\mathbb{Q}$-vector spaces.

Lemma 6.5. *The linear map α_k is injective for all k. The linear map α_1 is an isomorphism.*

Proof. Define $H = G \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Since H is the image of Γ_G modulo N, we have $S_{2k}(\Gamma(N), \mathbb{Q}(\zeta_N))^H = S_{2k}(\Gamma_G, \mathbb{Q}(\zeta_N))$. In particular, $S_{2k}(\Gamma(N), \mathbb{Q}(\zeta_N))^G \subseteq S_{2k}(\Gamma_G, \mathbb{C})$. Let

$$\iota \colon S_{2k}(\Gamma(N), \mathbb{Q}(\zeta_N))^G \otimes_{\mathbb{Q}} \mathbb{C} \to S_{2k}(\Gamma_G, \mathbb{C})$$

be the $\mathbb{C}$-linear map induced by the inclusion.

We claim that ι is an isomorphism. The group H is normal in G, so we obtain a right action of G/H on $S_{2k}(\Gamma_G, \mathbb{Q}(\zeta_N))$. Let $\varphi \colon G \to \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ be the homomorphism satisfying $\varphi(A)(\zeta_N) = \zeta_N^{\det A}$; it is surjective since $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$. We obtain an action of $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ on $S_{2k}(\Gamma_G, \mathbb{Q}(\zeta_N))$ by using the

action of G/H and the isomorphism $G/H \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ induced by φ; note that we can view this as a left action $\bullet$ since G/H is abelian. With this new action, we have $\sigma \bullet (cf) = \sigma(c)\,(\sigma \bullet f)$ for all $c \in \mathbb{Q}(\zeta_N)$, $f \in S_{2k}(\Gamma_G, \mathbb{Q}(\zeta_N))$ and $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$. By Galois descent for vector spaces (see the corollary to Proposition 6 in Chapter V §10 of [Bou03]), the natural homomorphism

$$S_{2k}(\Gamma(N), \mathbb{Q}(\zeta_N))^G \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_N) = S_{2k}(\Gamma_G, \mathbb{Q}(\zeta_N))^{\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})} \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_N) \to S_{2k}(\Gamma_G, \mathbb{Q}(\zeta_N)) \tag{6.2}$$

is an isomorphism of $\mathbb{Q}(\zeta_N)$-vector spaces. Since $S_{2k}(\Gamma_G, \mathbb{C})$ has a basis with coefficients in $\mathbb{Q}(\zeta_N)$, we deduce that ι is an isomorphism by tensoring (6.2) up to $\mathbb{C}$.

By tensoring α_k up to $\mathbb{C}$ and composing with ι, we obtain a $\mathbb{C}$-linear map

$$\beta_k \colon H^0(X_G(\mathbb{C}), \Omega^{\otimes k}_{X_G(\mathbb{C})}) = H^0(X_G, \Omega^{\otimes k}_{X_G}) \otimes_{\mathbb{Q}} \mathbb{C} \to S_{2k}(\Gamma_G, \mathbb{C}).$$

Since ι is an isomorphism, it suffices to prove that β_k is injective and that β_1 is an isomorphism. For any holomorphic k-form ω on $X_G(\mathbb{C})$, $f := \beta_k(\omega)$ is the *unique* cusp form in $S_{2k}(\Gamma_G, \mathbb{C})$ such that the form on $\mathfrak{H}$ induced by ω equals $(2\pi i)^k f(\tau)(d\tau)^k$. So β_k is indeed injective. The linear map β_1 is an isomorphism, cf. Corollary 2.17 of [Shi94]. □

Let $R_{X_G} = \bigoplus_{k\geq 0} H^0(X_G, \Omega^{\otimes k}_{X_G})$ be the canonical ring of X_G. Using the linear maps α_k, we obtain a homomorphism

$$\alpha \colon R_X \to \bigoplus_{k\geq 0} S_{2k}(\Gamma_G, \mathbb{Q}(\zeta_N))^G \tag{6.3}$$

of graded rings, where multiplication on the right hand side is multiplication of functions. From Lemma 6.5, the homomorphism α is injective, and $\alpha_1 \colon H^0(X_G, \Omega_{X_G}) \to S_2(\Gamma_G, \mathbb{Q}(\zeta_N))^G$ is an isomorphism.

7. Canonical map

7.1. **Setup.** Fix an integer $N \geq 1$ and a subgroup G of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ that satisfies $-I \in G$ and $\det(G) = (\mathbb{Z}/N\mathbb{Z})^\times$.

From §1.4, and the algorithm of §1.3, we can compute a basis of the $\mathbb{Q}$-vector space $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))$ and, with respect to this basis, compute the right action of $\mathrm{SL}_2(\mathbb{Z})$. Using the action of $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ on $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))$ from §1.5, one can then compute a basis $f_1, \ldots, f_g$ of the $\mathbb{Q}$-vector space $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))^G$. Each f_j is given by a q-expansion for which an arbitrary number of its coefficients can be computed.

Let $\omega_1, \ldots, \omega_g$ be the basis of the $\mathbb{Q}$-vector space $H^0(X_G, \Omega^1_{X_G})$ that satisfies $\alpha_1(\omega_j) = f_j$, where α_1 is the isomorphism $H^0(X_G, \Omega_{X_G}) \xrightarrow{\sim} S_2(\Gamma(N), \mathbb{Q}(\zeta_N))^G$ from §6. Observe that g is the genus of the modular curve X_G. We shall assume that $g \geq 2$.

Let

$$\varphi \colon X_G \to \mathbb{P}^{g-1}_{\mathbb{Q}}$$

be the canonical morphism corresponding to the basis $\omega_1, \ldots, \omega_g$ and denote its image by C. The goal of §7 is to describe how to compute the ideal $I(C) \subseteq \mathbb{Q}[x_1, \ldots, x_g]$ of C, and hence the curve $C \subseteq \mathbb{P}^{g-1}_{\mathbb{Q}}$, from the cusps forms $f_1, \ldots, f_g$. If X_G is not hyperelliptic, then φ will be an embedding and hence we will have found a model for X_G.

7.2. **Background.** Let X be a smooth, projective and geometrically irreducible curve defined over a field k. In our application, the curve X will be the modular curve X_G defined over $\mathbb{Q}$. Denote the genus of X by g and assume that $g \geq 2$. Fix a basis $\omega_1, \ldots, \omega_g$ of the k-vector space $H^0(X, \Omega^1_X)$; it gives rise to a non-constant morphism

$$\varphi \colon X \to \mathbb{P}^{g-1}_k.$$

Define the curve $C := \varphi(X)$ and let $I(C) \subseteq k[x_1, \ldots, x_g]$ be the homogeneous ideal of C. We have $I(C) = \oplus_{d\geq 0} I_d(C)$, where $I_d(C)$ consists of the homogeneous polynomials in $I(C)$ of degree d.

We say that X is *hyperelliptic* if there is a morphism $X_{\bar{k}} \to \mathbb{P}^1_{\bar{k}}$ of degree 2 (by the following lemmas, this is equivalent to there being a morphism $X \to Y$ of degree 2 with Y a curve of genus 0). We first consider the case where X is not hyperelliptic.

Lemma 7.1. *Suppose that X is not hyperelliptic.*

(i) *The morphism φ is an embedding. In particular, X and C are isomorphic.*
(ii) *We have* $\dim_k I_2(C) = (g-2)(g-3)/2$ *and* $\dim_k I_3(C) = (g-3)(g^2+6g-10)/6$.
(iii) *If $g \geq 4$, then the ideal I is generated by $I_2(C)$ and $I_3(C)$.*
(iv) *If $g = 3$, then the ideal I is generated by $I_4(C)$ and* $\dim_k I_4(C) = 1$.

Proof. First assume that k is algebraically closed. The morphism φ is an embedding and the curve $C \subseteq \mathbb{P}^{g-1}_k$ has degree $2g-2$, cf. [Har77, IV §5]. Let H be a hyperplane section of $C \subseteq \mathbb{P}^{g-1}_k$. Fix an integer $d \geq 2$. We have $\deg(dH) = d(2g-2) > 2g-2$ and hence $l(dH) = d(2g-2)-g+1$ by Riemann–Roch. The d-th component of the graded ring $k[x_1,\dots,x_g]/I(C)$ has dimension $l(dH)$ and hence $\dim_k I_d(C) = \binom{g-1+d}{d} - l(dH) = \binom{g-1+d}{d} - d(2g-2) + g - 1$. The claimed dimensions in the lemma are now immediate. Part (iii) is a theorem of Petri, cf. [SV88]. Finally suppose that $g = 3$ and let F be a generator of the vector space $I_4(C)$. Since C is a smooth curve of genus 3, this implies that C is defined by $F = 0$ and hence $I(C)$ is generated by F.

Now consider a general field k. The forms $\omega_1,\dots,\omega_g$ are also a basis of $H^0(X_{\bar{k}}, \Omega^1_{X_{\bar{k}}}) = H^0(X, \Omega^1_X) \otimes_k \bar{k}$. With this basis fixed, the natural map $I_d(C) \otimes_k \bar{k} \to I_d(C_{\bar{k}})$ is an isomorphism for all $d \geq 0$. It is now easy to deduce the lemma from the algebraically closed case. □

Lemma 7.2. *Suppose that X is hyperelliptic.*

(i) *The curve C has genus 0 and $X \xrightarrow{\varphi} C$ has degree 2.*
(ii) *The ideal $I(C)$ is generated by $I_2(C)$ and* $\dim_k I_2(C) = (g-1)(g-2)/2$.

Proof. As in the proof of Lemma 7.1, the natural map $I_d(C) \otimes_k \bar{k} \to I_d(C_{\bar{k}})$ is an isomorphism for all $d \geq 0$. It is now easy to show that the general case reduced to the case where k is algebraically closed.

Assume k is algebraically closed. The morphism $\varphi\colon X \to C$ has degree 2 and the curve $C \subseteq \mathbb{P}^{g-1}_k$ is a rational normal curve of degree $g-1$, cf. [Har77, IV §5]. Since C is a rational normal curve, it is of genus 0 and $I(C)$ is generated by $I_2(C)$.

Let H be a hyperplane section of $C \subseteq \mathbb{P}^{g-1}_k$. Fix an integer $d \geq 2$. We have $\deg(dH) = d(g-1) > 0$ and hence $l(dH) = d(g-1)-0+1$ by Riemann–Roch. The d-th component of the graded ring $k[x_1,\dots,x_g]/I(C)$ has dimension $l(dH)$ and hence $\dim_k I_d(C) = \binom{g-1+d}{d} - l(dH) = \binom{g-1+d}{d} - d(g-1) - 1$. The claimed dimension for $I_2(C)$ is now immediate. □

7.3. **Computing $I_d(C)$.** Fix notation and assumptions as in §7.1. In this section, we describe how to compute $I_d(C)$ for a fixed integer $d \geq 0$. We may assume that $d \geq 2$ since $I_0(C) = I_1(C) = 0$.

Let Γ_G be the congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ from §6 and let w be the width of Γ_G at ∞. Note that w is the smallest positive integer for which $\left(\begin{smallmatrix}1 & w\\ 0 & 1\end{smallmatrix}\right)$ modulo N lies in G. The q-expansion of any cusp form $f \in S_k(\Gamma(N), \mathbb{Q}(\zeta_N))^G \subseteq S_k(\Gamma_G, \mathbb{C})$ is a power series in $q_w := e^{2\pi i\tau/w}$ since $f|\left(\begin{smallmatrix}1 & w\\ 0 & 1\end{smallmatrix}\right) = f$.

Let M_d be the set of monomials in $\mathbb{Q}[x_1,\dots,x_g]$ of degree d. For each $m \in M_d$, we have $m(f_1,\dots,f_g) \in S_{2d}(\Gamma(N), \mathbb{Q}(\zeta_N))^G$ and hence

$$m(f_1,\dots,f_g) = \sum_{n=0}^{\infty} a_{m,n} q_w^n$$

for unique $a_{m,n} \in \mathbb{Q}(\zeta_N)$.

Lemma 7.3. *Consider a homogeneous polynomial $F \in \mathbb{Q}[x_1, \dots, x_g]$ of degree d; we have $F = \sum_{m \in M_d} c_m m$ for unique $c_m \in \mathbb{Q}$. Then F is an element of $I_d(C)$ if and only if*

$$\sum_{m \in M_d} a_{m,n}\, c_m = 0 \tag{7.1}$$

holds for all $0 \le n \le d(2g-1)$.

Proof. From the injective homomorphism (6.3) of graded rings, we find that F lies in $I_d(C)$ if and only if $F(f_1, \dots, f_g) = 0$. We have

$$F(f_1, \dots, f_g) = \sum_{m \in M_d} c_m m(f_1, \dots, f_g) = \sum_{n=0}^{\infty} \Big(\sum_{m \in M_d} a_{m,n} c_m \Big) q_w^n.$$

So F lies in $I_d(C)$ if and only if (7.1) holds for all $n \ge 0$. One implication of the lemma is now immediate.

Now suppose that $F \notin I_d(C)$; equivalently, $F(f_1, \dots, f_g) \ne 0$. Let ν be the smallest integer for which the coefficient of q_w^ν in the q-expansion of $F(f_1, \dots, f_g)$ is non-zero. It thus suffices to prove that $\nu \le d(2g-1)$.

The differential form $f_j(\tau) d\tau$ on $\Gamma_G \backslash \mathfrak{H}$ extends to a holomorphic differential 1-form on $X_G(\mathbb{C})$ for each $1 \le j \le g$. Define $\omega := F(f_1(\tau), \dots, f_g(\tau))\, (d\tau)^d$. Since F is homogeneous of degree d, $F(f_1(\tau), \dots, f_g(\tau))\, (d\tau)^d$ gives rise to a holomorphic differential d-form ω on $X_G(\mathbb{C})$. We have $\omega \ne 0$ since $F(f_1, \dots, f_g) \ne 0$.

The divisor of ω is effective and has degree $d(2g-2)$. Therefore, $v_P(\omega) \le d(2g-2)$, where $P \in X_G(\mathbb{C})$ is the cusp at infinity and $v_P(\omega)$ is the order of vanishing of ω at P. One can verify that $v_P(\omega) = \nu - d$. Therefore, $\nu \le d(2g-2) + d = d(2g-1)$. □

By the above lemma, $I_d(C)$ consists of the polynomials $\sum_{m \in M_d} c_m m$ with $c_m \in \mathbb{Q}$ such that (7.1) holds for all $0 \le n \le d(2g-1)$. So given the values $a_{m,n} \in \mathbb{Q}(\zeta_N)$ with $m \in M_d$ and $0 \le n \le d(2g-1)$, computing a basis of $I_d(C)$ is basic linear algebra (note that since $\mathbb{Q}(\zeta_N)$ over $\mathbb{Q}$ has basis $1, \zeta_N, \dots, \zeta_N^{\varphi(N)-1}$, each equation (7.1) can be replaced by $\varphi(N)$ linear equations with rational coefficients).

It remains to explain how $a_{m,n}$ can be computed for fixed $m \in M_d$ and $0 \le n \le d(2g-1)$; recall that the f_j are given by their q-expansions and we can compute an arbitrary number of terms. The q-expansion of each cusp form f_j lies in $q_w \cdot \mathbb{Q}(\zeta_N)[\![q_w]\!]$. Using this and that m is homogeneous of degree d, one can check that $a_{m,n}$ is determined by the coefficients of q_w^i in the q-expansion of f_j for all $0 \le i \le n - d$ and $1 \le j \le g$.

In particular, we deduce that $I_d(C)$ can be computed from the coefficients of q_w^i in the q-expansion of f_j for all $0 \le i \le d(2g-1) - d = d(2g-2)$ and $1 \le j \le g$.

7.4. **Computing the curve C.** Fix notation and assumptions as in §7.1. To compute the curve $C \subseteq \mathbb{P}^{g-1}_{\mathbb{Q}}$, it suffices to find a set of generators of the ideal $I(C) \subseteq \mathbb{Q}[x_1, \dots, x_g]$. We have assumed that $g \ge 2$. We may further assume that $g \ge 3$ since $C = \mathbb{P}^1_{\mathbb{Q}}$ and $I(C) = 0$ if $g = 2$.

From §7.3, we can compute the $\mathbb{Q}$-vector space $I_2(C)$ from the cusps forms $f_1, \dots, f_g$; let $F_1, \dots, F_r$ be a basis. By Lemmas 7.1 and 7.2, and using $g \ge 3$, we find that X_G is hyperelliptic if and only if $r = (g-1)(g-2)/2$. If X_G is hyperelliptic, Lemma 7.2 implies that the curve C has genus 0 and the ideal $I(C)$ is generated by $F_1, \dots, F_r$. We may now assume that X_G is not hyperelliptic.

Suppose $g = 3$. By Lemma 7.1, $I_4(C)$ has dimension 1 and generates the ideal $I(C)$. From §7.3, we can compute the $\mathbb{Q}$-vector space $I_4(C)$; let F be a basis. The ideal $I(C)$ is thus generated by F and hence $C \subseteq \mathbb{P}^2$ is the smooth plane quartic defined by $F = 0$.

Now assume that $g \ge 4$. By Lemma 7.1, the ideal $I(C)$ is generated by $I_2(C)$ and $I_3(C)$, and $I_3(C)$ has dimension $(g-3)(g^2+6g-10)/6$. Let W be the subspace of $I_3(C)$ generated by $x_i F_j$ with $1 \le i \le g$ and $1 \le j \le r$. If W has dimension $(g-3)(g^2+6g-10)/6$, then $W = I_3(C)$ and hence $I(C)$ is generated by $F_1, \dots, F_r$.

Finally suppose that the dimension of W is not $(g-3)(g^2+6g-10)/6$. From §7.3, we can compute the $\mathbb{Q}$-vector space $I_3(C)$. Let $G_1, \dots, G_s$ be polynomials in $I_3(C)$ that give rise to a basis in $I_3(C)/W$. The ideal

$I(C)$ is thus generated by $F_1, \dots, F_r, G_1, \dots, G_s$. It is not needed for our purposes, but one can further show that $s = g - 3$.

Remark 7.4. One can choose $f_1, \dots, f_g$ to be a basis of the $\mathbb{Z}$-module $S_2(\Gamma(N), \mathbb{Q}(\zeta_N))^G \cap S_2(\Gamma(N), \mathbb{Z}[\zeta_N])$. We can choose $F_1, \dots, F_r$ to be basis of the $\mathbb{Z}$-module $I_2(C) \cap \mathbb{Z}[x_1, \dots, x_g]$. The LLL-algorithm can be used to makes such choices with relatively small coefficients.

References

[Asa76] Tetsuya Asai, *On the Fourier coefficients of automorphic forms at various cusps and some applications to Rankin's convolution*, J. Math. Soc. Japan **28** (1976), no. 1, 48–61. MR0427235 ↑4.3

[AL78] A. O. L. Atkin and Wen Ch'ing Winnie Li, *Twists of newforms and pseudo-eigenvalues of W-operators*, Invent. Math. **48** (1978), no. 3, 221–243. MR508986 ↑4.3

[BC14] Barinder S. Banwait and John E. Cremona, *Tetrahedral elliptic curves and the local-global principle for isogenies*, Algebra Number Theory **8** (2014), no. 5, 1201–1229. MR3263141 ↑1.6

[Bar14] Burcu Baran, *An exceptional isomorphism between modular curves of level 13*, J. Number Theory **145** (2014), 273–300, DOI 10.1016/j.jnt.2014.05.017. MR3253304 ↑1.6

[BDP17] Massimo Bertolini, Henri Darmon, and Kartik Prasanna, *p-adic L-functions and the coniveau filtration on Chow groups*, J. Reine Angew. Math. **731** (2017), 21–86. With an appendix by Brian Conrad. ↑3.2, 3.3

[BN19] François Brunault and Michael Neururer, *Fourier expansions at cusps*, The Ramanujan Journal (2019). ↑1.5, 1.7

[Bou98] Nicolas Bourbaki, *Commutative algebra. Chapters 1–7*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 1998. Translated from the French; Reprint of the 1989 English translation. MR1727221 ↑3.2

[Bou03] ———, *Algebra II. Chapters 4–7*, Elements of Mathematics (Berlin), Springer-Verlag, Berlin, 2003. Translated from the 1981 French edition by P. M. Cohn and J. Howie; Reprint of the 1990 English edition [Springer, Berlin; MR1080964 (91h:00003)]. MR1994218 ↑6.1

[Coh19] Henri Cohen, *Expansions at cusps and Petersson products in Pari/GP*, Elliptic integrals, elliptic functions and modular forms in quantum field theory, Texts Monogr. Symbol. Comput., Springer, Cham, 2019, pp. 161–181. MR3889557 ↑1.7, 4.7, 4.8

[Col18] Dan Collins, *Numerical computation of Petersson inner products and q-expansions*, 2018. arXiv:1802.09740. ↑1.7

[DR73] P. Deligne and M. Rapoport, *Les schémas de modules de courbes elliptiques*, Modular functions of one variable, II (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, pp. 143–316. Lecture Notes in Math., Vol. 349 (French). MR0337993 ↑3.4, 3.2, 3.2

[DMS19] Valerio Dose, Pietro Mercuri, and Claudio Stirpe, *Double covers of Cartan modular curves*, J. Number Theory **195** (2019), 96–114. MR3867436 ↑1.6

[Elk99] Noam D. Elkies, *The Klein quartic in number theory*, The eightfold way, Math. Sci. Res. Inst. Publ., vol. 35, Cambridge Univ. Press, Cambridge, 1999, pp. 51–101. MR1722413 ↑1.5

[Har77] Robin Hartshorne, *Algebraic geometry*, Springer-Verlag, New York-Heidelberg, 1977. Graduate Texts in Mathematics, No. 52. MR0463157 ↑7.2, 7.2

[Kat76] Nicholas M. Katz, *p-adic interpolation of real analytic Eisenstein series*, Ann. of Math. (2) **104** (1976), no. 3, 459–571. MR506271 ↑2

[MS18] Pietro Mercuri and René Schoof, *Modular forms invariant under non-split Cartan subgroups*, 2018. arXiv:1805.06873. ↑1.6

[Oht95] Masami Ohta, *On the p-adic Eichler-Shimura isomorphism for Λ-adic cusp forms*, J. Reine Angew. Math. **463** (1995), 49–98. ↑2

[Sch15] George J. Schaeffer, *Hecke stability and weight 1 modular forms*, Math. Z. **281** (2015), no. 1-2, 159–191. MR3384865 ↑4.2

[Shi94] Goro Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Mathematical Society of Japan, vol. 11, Princeton University Press, Princeton, NJ, 1994. Reprint of the 1971 original; Kanô Memorial Lectures, 1. ↑6, 6, 6.1

[Ste07] William Stein, *Modular forms, a computational approach*, Graduate Studies in Mathematics, vol. 79, American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells. MR2289048 ↑4.1, 4.2, 4.4, 4.7

[SV88] Karl-Otto Stöhr and Paulo Viana, *A variant of Petri's analysis of the canonical ideal of an algebraic curve*, Manuscripta Math. **61** (1988), no. 2, 223–248. MR943539 ↑7.2

[Zyw15] David Zywina, *On the possible images of the mod ℓ representations associated to elliptic curves over* $\mathbb{Q}$, 2015. arXiv:1508.07660. ↑6, ii

Department of Mathematics, Cornell University, Ithaca, NY 14853, USA
Email address: zywina@math.cornell.edu
URL: http://www.math.cornell.edu/~zywina