Trace formulas and class number sums

Nathan Jones

Abstract

We specialize the Eichler-Selberg trace formula to obtain an asymptotic in n for the number of (weighted) $SL_2(\mathbb{Z})$-conjugation orbits of 2×2 matrices of determinant n whose reductions modulo N lie in a given conjugacy class in $GL_2(\mathbb{Z}/N\mathbb{Z})$, for arbitrary level $N \geq 1$ which is relatively prime to n. This generalizes an 1885 result of Hurwitz.

1 Introduction

In [8], Hurwitz writes down formulas for sums of Hurwitz class numbers $H(-\Delta)$ as Δ runs through quadratic progressions to a prime modulus N. He also mentions that these formulas may be generalized to the case where the modulus is not prime. This paper generalizes Hurwitz's result to an arbitrary modulus N, and gives an alternate proof, based on the Eichler-Selberg trace formula. First, we describe all of this more precisely.

For any negative discriminant Δ, recall the Hurwitz class number

$$H(-\Delta) := \sum_{f(x,y)\in \mathcal{Q}_{\mathbb{Z}}^{+}(\Delta)\,//\,SL_2(\mathbb{Z})} \frac{2}{|SL_2(\mathbb{Z})_{f(x,y)}|}.$$

Here we are denoting by

$$\mathcal{Q}_{\mathbb{Z}}^{+}(\Delta) := \{f(x,y) = \alpha x^2 + \beta xy + \gamma y^2 :\ (\alpha,\beta,\gamma) \in \mathbb{Z}_{>0}\times\mathbb{Z}^2,\ \beta^2 - 4\alpha\gamma = \Delta\}$$

the set of positive definite (*not* necessarily primitive) integral binary quadratic forms of discriminant Δ, by $\mathcal{Q}_{\mathbb{Z}}^{+}(\Delta)\,//\,SL_2(\mathbb{Z})$ its orbit space with respect to the classical $SL_2(\mathbb{Z})$-action

$$f\cdot\begin{pmatrix} a & b\\ c & d\end{pmatrix}(x,y) := f(ax+by, cx+dy),$$

and by

$$SL_2(\mathbb{Z})_{f(x,y)} := \{A\in SL_2(\mathbb{Z}) :\ f\cdot A = f\}$$

Mathematics Subject Classification (2000): 11R29, 11F32.
Key words and phrases: Class number, trace formula.

the stabilizer in $SL_2(\mathbb{Z})$ of the form $f(x,y)$. In addition, $H(0)$ is defined to be $-1/12$ and $H(m)=0$ when $m<0$.

Hurwitz shows, for example, that if N is prime, $n>1$ is coprime to N, and a is any integer modulo N with the property that a^2-4n is a quadratic nonresidue modulo N, then

$$(N+1)\sum_{t\equiv a \mod N} H(4n-t^2) = 2\sigma(n)+h_1^{(a)}\psi_1(n)+h_2^{(a)}\psi_2(n)+\cdots+h_\mu^{(a)}\psi_\mu(n),$$

where $\sigma(n)$ is the sum of the divisors of n. The $h_i^{(a)}$'s are coefficients which do not depend on n and the $\psi_i(n)$'s are the Fourier coefficients of the q-expansions of certain weight 2 cusp forms for the modular curve $X(N)$. Thus, if we apply the Ramanujan bound $|\psi_i(p)|\leq 2p^{1/2}$ [3], we obtain

$$\sum_{t\equiv a \mod N} H(4n-t^2) = \frac{2}{N+1}\sigma(n)+O_{N,\varepsilon}(n^{1/2+\varepsilon}). \tag{1}$$

Let us re-interpret this asymptotic. Note that, by pairing the positive definite form $f(x,y)$ with the negative definite form $-f(x,y)$ we have

$$H(-\Delta) = \sum_{f(x,y)\in \mathcal{Q}_{\mathbb{Z}}(\Delta)\,//\,SL_2(\mathbb{Z})} \frac{1}{|SL_2(\mathbb{Z})_{f(x,y)}|},$$

where the sum is now taken over the orbit space of the set of *all* integral binary quadratic forms of discriminant Δ. Let $M_{2\times 2}(\mathbb{Z})$ denote the set of all integral 2 by 2 matrices, and for a fixed pair integers t and n, define

$$\mathcal{T}(t,n) := \{A\in M_{2\times 2}(\mathbb{Z}):\ \operatorname{tr} A = t,\ \det A = n\}.$$

If t and n satisfy $t^2-4n=\Delta$, then there is a bijection

$$\mathcal{Q}_{\mathbb{Z}}(\Delta) \longleftrightarrow \mathcal{T}(t,n) \tag{2}$$

in which

$$\alpha x^2+\beta xy+\gamma y^2 \leftrightarrow \begin{pmatrix} \frac{t+\beta}{2} & -\gamma \\ \alpha & \frac{t-\beta}{2}\end{pmatrix}.$$

This bijection is a map of $SL_2(\mathbb{Z})$-sets, where $SL_2(\mathbb{Z})$ operates by conjugation on $\mathcal{T}(t,n)$. Thus we may re-write the Hurwitz class number as

$$H\left(-(t^2-4n)\right) = \sum_{A\in \mathcal{T}(t,n)\,//\,SL_2(\mathbb{Z})} \frac{1}{|SL_2(\mathbb{Z})_A|}$$

where $\mathcal{T}(t,n)\,//\,SL_2(\mathbb{Z})$ denotes the set of $SL_2(\mathbb{Z})$-conjugation orbits in $\mathcal{T}(t,n)$ and

$$SL_2(\mathbb{Z})_A := \{B\in SL_2(\mathbb{Z}) : B^{-1}AB = A\}.$$

In this paper we prove

Theorem 1. *Let $N \geq 1$ be any integer level, $n \geq 1$ a non-square integer coprime to N and $\mathcal{A} \subset GL_2(\mathbb{Z}/N\mathbb{Z})$ any $SL_2(\mathbb{Z}/N\mathbb{Z})$-conjugation orbit with*

$$\det \mathcal{A} \equiv n \mod N.$$

Then,

$$\sum_{A \in \mathcal{T}_{\mathcal{A}}^e(n) \,//\, SL_2(\mathbb{Z})} \frac{1}{|SL_2(\mathbb{Z})_A|} = \frac{2|\mathcal{A}|}{|SL_2(\mathbb{Z}/N\mathbb{Z})|}\sigma(n) + O_\varepsilon(|\mathcal{A}|n^{1/2+\varepsilon}),$$

where

$$\mathcal{T}_{\mathcal{A}}^e(n) := \{A \in M_{2\times 2}(\mathbb{Z}) : \ A \mod N \in \mathcal{A}, \det A = n \text{ and } (tr\, A)^2 < 4n\}.$$

Note that this theorem specializes to (1) in the case where N is prime and $\mathcal{A}$ is the $SL_2(\mathbb{Z}/N\mathbb{Z})$-conjugation orbit of trace a and determinant n.

The case where $n = p$ is prime is of particular interst. The work of Deuring [4] (see also [2, Theorem 14.18]) interprets the left-hand side of (1) as essentially counting the number of isomorphism classes of elliptic curves over $\mathbb{Z}/p\mathbb{Z}$ whose Frobenius endomorphism has trace congruent to a modulo N. Duke [5] uses this observation to unconditionally bound the mean-square error in the Chebotarev density theorem for the N-th division fields of elliptic curves over $\mathbb{Q}$, for N prime. In a forthcoming paper we will use Theorem 1 to strengthen Theorem 2 of [5].

2 Acknowledgment

This paper comprises a portion of my Ph. D. dissertation. I would like to express gratitude to my advisor William Duke for his guidance.

3 General framework

Let

$$\mathcal{A} =: SL_2(\mathbb{Z}/N\mathbb{Z})aSL_2(\mathbb{Z}/N\mathbb{Z})^{-1}, \qquad a \in GL_2(\mathbb{Z}/N\mathbb{Z})$$

be as in Theorem 1, and define the subgroup $\mathcal{D} \subset GL_2(\mathbb{Z}/N\mathbb{Z})$ to be the subgroup generated by a and the negative of the identity:

$$\mathcal{D} = \mathcal{D}_a := \left\langle a, -\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\rangle \subset GL_2(\mathbb{Z}/N\mathbb{Z})$$

In order to obtain the theorem using trace formulas, we will make use of the following properties of $\mathcal{D}$:

1. The group $\mathcal{D}$ intersects $\mathcal{A}$ nontrivially:

$$\mathcal{D} \cap \mathcal{A} \neq \emptyset.$$

2. The group $\mathcal{D}$ is abelian, so that its space of class functions is spanned by its multiplicative characters χ.

3. The negative of the identity matrix belongs to $\mathcal{D}$:

$$-\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathcal{D}$$

We will employ a trace formula for the action of $T_{\mathcal{D}}(n)$, the associated degree n Hecke operator, on the space $S_2(\Gamma_{\mathcal{D}}, \chi)$ of weight 2 cusps forms with character χ relative to the associated congruence group $\Gamma = \Gamma_{\mathcal{D}}$ (for definitions, see Section 4).

We remark that any other group $\mathcal{D}$ satisfying properties 1, 2 and 3 could be used in our proof in place of $\mathcal{D}_a$. In fact, one need not assume $\mathcal{D}$ to be abelian, although it is conveniently simplifies the proof. All that is really necessary is that the multiplicative characters on $\mathcal{D}$ distinguish the $SL_2(\mathbb{Z}/N\mathbb{Z})$ conjugation orbits in $\mathcal{D}$. For example, if

$$\mathcal{A} \cap \left\{ \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \mod N \right\} \neq \emptyset,$$

then one could use the trace formula for $\Gamma_0(N)$ with character as developed in [10] or [7] to prove Theorem 1. Otherwise, we must use other congruence groups. Chen [1] has also used trace formulas for groups other than $\Gamma_0(N)$ (in the case of prime level and trivial character) to deduce the existence of isogenies between the jacobians of certain modular curves.

4 Notation and Background

Throughout this paper we use the standard notation:

$$\Gamma(N) := \{\gamma \in SL_2(\mathbb{Z}) : \ \gamma \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod N\}.$$

In particular, $\Gamma(1)$ denotes the full modular group $SL_2(\mathbb{Z})$. For any subset $S \subseteq M_{2\times 2}(\mathbb{Z}/N\mathbb{Z})$ we put

$$\mathcal{T}_S := \{A \in M_{2\times 2}(\mathbb{Z}) : \ A \mod N \in S\},$$

Further we define, for any integers t and n,

$$\mathcal{T}_S(n) = \{A \in \mathcal{T}_S : \ \det A = n\} \quad \text{and} \quad \mathcal{T}_S(t,n) = \{A \in \mathcal{T}_S(n) : \ \operatorname{tr} A = t\}.$$

We abbreviate $\mathcal{T} := \mathcal{T}_{M_{2\times 2}(\mathbb{Z}/N\mathbb{Z})}$, so that our previous notation $\mathcal{T}(t,n)$ is consistent.

If X is any set of matrices stable by left (resp. right) multiplication by a group Γ of matrices, we use the usual notation

$$\Gamma \setminus X \quad (\text{ resp. } \ X / \Gamma)$$

to denote the left (resp. right) coset space, whereas $X\,//\,\Gamma$ denotes the space of conjugation orbits, if Γ acts on X by conjugation. We denote by

$$\Gamma_x := \{\gamma \in \Gamma : \gamma x \gamma^{-1} = x\}$$

the centralizer in Γ of $x \in X$. Finally, $Z(\Gamma)$ denotes the center of the group Γ, and I denotes the 2×2 identity matrix.

4.1 Preliminaries

We now briefly set up the background, following [9], where full details (of the weight $k > 2$ case) may be found. For an even positive integer weight $k \geq 2$ and a function f on the upper half-plane we denote

$$\left(f|_k \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)(z) := (ad - bc)^{k/2}(cz + d)^{-k} f\left(\frac{az + b}{cz + d}\right).$$

Suppose Γ is any Fuchsian group of the first kind and that

$$\chi : \Gamma \longrightarrow \mathbb{C}^*$$

is a multiplicative character whose kernel has finite index in Γ. We consider the space of holomorphic weight k modular forms with character χ for Γ

$$\mathcal{M}_k(\Gamma, \chi) = \{f : \mathbb{H} \to \mathbb{C}, f \text{ holomorphic (at cusps too)}, \forall \gamma \in \Gamma, f|_k\gamma = \chi(\gamma)f\}.$$

Note that, if $-I \in \Gamma$ we have

$$\chi(-I) \neq (-1)^k \implies \mathcal{M}_k(\Gamma, \chi) = \{0\}. \tag{3}$$

The subspace of cusp forms is defined by

$$\mathcal{S}_k(\Gamma, \chi) = \{f \in \mathcal{M}_k(\Gamma, \chi) : f \equiv 0 \text{ at the cusps of } \Gamma\}.$$

We recall the action of Hecke operators on these spaces. Define the semigroup

$$\tilde{\Gamma} := \{g \in GL_2^+(\mathbb{R}) : \ [\Gamma : g\Gamma g^{-1} \cap \Gamma] < \infty \ \text{ and } \ [g\Gamma g^{-1} : g\Gamma g^{-1} \cap \Gamma] < \infty\}.$$

Let Υ be any subsemigroup satisfying

$$\Gamma \subseteq \Upsilon \subseteq \tilde{\Gamma}$$

and assume that χ extends to a multiplicative character of Υ so that for $\alpha \in \Upsilon$ and $\gamma \in \Gamma$ we have

$$\alpha\gamma\alpha^{-1} \in \Gamma \Longrightarrow \chi(\alpha\gamma\alpha^{-1}) = \chi(\gamma). \tag{4}$$

Given any finite union of double cosets

$$\mathcal{T} = \bigsqcup_{\alpha \in \Upsilon'} \Gamma\alpha\Gamma \qquad\qquad (\Upsilon' \subset \Upsilon),$$

denote by T (or by T^χ, when we wish to emphasize the character χ) the Hecke operator

$$T : \mathcal{S}_k(\Gamma, \chi) \to \mathcal{S}_k(\Gamma, \chi),$$

defined by the finite sum

$$T(f) = \sum_{\alpha \in \Upsilon'} \det(\alpha)^{k/2-1} \sum_{\alpha_1 \in \Gamma \backslash \Gamma \alpha \Gamma} \overline{\chi(\alpha_1)} f|_k \alpha_1.$$

We refer to this situation by saying that the double coset space $\mathcal{T}$ *defines* the Hecke operator T.

4.2 The Eichler-Selberg Trace formula

We use the following trace formula due originally to Eichler [6] (see also [11], which works out the $\chi|_\Gamma$ = non-trivial case). The set-up is as follows. Let $T = T^\chi$ be any Hecke operator (defined by the double-coset space $\mathcal{T}$) acting on the space $\mathcal{S}_k(\Gamma, \chi)$ of cusp forms for Γ with character χ. Let

$$\mathcal{T}^h := \{\alpha \in \mathcal{T} : \ \mathrm{tr}\,(\alpha)^2 > 4\det(\alpha) \text{ and } \alpha\text{'s fixed points are cusps of } \Gamma\}$$

and

$$\mathcal{T}^e := \{\alpha \in \mathcal{T} : \ \mathrm{tr}\,(\alpha)^2 < 4\det(\alpha)\}.$$

denote the subsets of hyperbolic and elliptic matrices, respectively. If the matrix α is hyperbolic, then let η_α and ζ_α be its real eigenvalues, taken in either order, and define

$$\mathrm{sgn}(\alpha) := \text{ the sign of either eigenvalue.}$$

If α is elliptic, then choose $\sigma \in SL_2(\mathbb{R})$ so that

$$\sigma\alpha\sigma^{-1} = r \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} \qquad (r > 0)$$

and define

$$\eta_\alpha := re^{i\theta}, \qquad \zeta_\alpha := re^{-i\theta}.$$

Theorem 2. *Suppose that the double-coset space $\mathcal{T} \subset GL_2^+(\mathbb{R})$ defining T contains no scalar or parabolic elements. If $-I \in \Gamma$, then assume also that $\chi(-I) = (-1)^k$. Then the trace $tr(T)$ of the Hecke operator T is given by*

$$tr(T) = -t_e - t_h + \delta(\chi, k) \sum_{\alpha \in \Gamma \backslash \mathcal{T}} \overline{\chi}(\alpha), \tag{5}$$

where

$$\delta(\chi, k) := \begin{cases} 1 & \text{if } k = 2 \text{ and } \chi|_\Gamma \equiv 1 \\ 0 & \text{otherwise,} \end{cases} \tag{6}$$

$$t_e := \sum_{\alpha \in \mathcal{T}^e \,//\, \Gamma} \frac{\overline{\chi(\alpha)}}{|\Gamma_\alpha|} \frac{\eta_\alpha^{k-1}}{\eta_\alpha - \zeta_\alpha}.$$

and

$$t_h := \frac{1}{|Z(\Gamma)|} \sum_{\alpha \in \mathcal{T}^h /\!/ \Gamma} \overline{\chi(\alpha)} sgn(\alpha)^k \frac{\min\{|\eta_\alpha|, |\zeta_\alpha|\}^{k-1}}{|\eta_\alpha - \zeta_\alpha|}$$

Theorem 1 is obtained by using a particular case of Theorem 2. We now specify the Fuchsian group Γ and Hecke operator T we will use. Given the discussion in Section 4.1, it remains to define Γ and Υ and describe the characters χ of Γ and how they extend to Υ, as well as the double coset spaces $\mathcal{T}$ defining our Hecke operators.

Given any subgroup

$$\mathcal{D} \subset GL_2(\mathbb{Z}/N\mathbb{Z})$$

which satisfies properties 1, 2 and 3 from Section 3, we take

$$\Gamma = \Gamma_{\mathcal{D}} := \mathcal{T}_{\mathcal{D}}(1) = \{\gamma \in \Gamma(1) : \gamma \mod N \in \mathcal{D}\}$$

and Υ to be the semigroup $\mathcal{T}_{\mathcal{D}}$. We fix a group homomorphism

$$\chi : \mathcal{D} \cap SL_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathbb{C}^*.$$

Since $\mathcal{D}$ is abelian, it is not hard to show that any such character may be extended (in $|\mathcal{D}/(\mathcal{D} \cap SL_2(\mathbb{Z}/N\mathbb{Z}))|$ different ways) to a character

$$\chi : \mathcal{D} \longrightarrow \mathbb{C}^*. \tag{7}$$

Pre-composition with reduction modulo N then defines a character

$$\chi : \Gamma_{\mathcal{D}} \longrightarrow \mathcal{D} \longrightarrow \mathbb{C}^*$$

satisfying $\Gamma(N) \subseteq \ker \chi$. By (7), χ extends to a semigroup homomorphism

$$\chi : \mathcal{T}_{\mathcal{D}} \longrightarrow \mathcal{D} \longrightarrow \mathbb{C}^*,$$

and one verifies (4) immediately. We take our Hecke operators $T = T_{\mathcal{D}}(n)$ to be those defined by the double coset space $\mathcal{T}_{\mathcal{D}}(n)$.

Note that, by property 3, we have

$$-\mathcal{T}_{\mathcal{D}}(n) = \mathcal{T}_{\mathcal{D}}(n).$$

If in addition $\chi(-I) \neq (-1)^k$, then by (3) we see that the left-hand side of (5) must be zero. Pairing α with $-\alpha$ in the various sums and using the identities

$$\eta_{-\alpha} = -\eta_\alpha \quad \text{and} \quad \zeta_{-\alpha} = -\zeta_\alpha,$$

we see that in this case the right hand side of (5) is also zero. This shows

Remark 3. *The formula* (5)*, applied with* $\Gamma = \Gamma_{\mathcal{D}}$ *and* $T = T_{\mathcal{D}}(n)$*, is still valid if* $\chi(-I) \neq (-1)^k$*.*

We will also use (5) with $\mathcal{D}$ replaced by its "twin" $\mathcal{D}'$, defined by

$$\mathcal{D}' := g\mathcal{D}g^{-1}, \qquad g := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{Z}/N\mathbb{Z}),$$

together with χ's twin

$$\chi' : \mathcal{D}' \longrightarrow \mathbb{C}^*, \qquad \chi'(A) := \chi(g^{-1}Ag)$$

The group $\Gamma' := \Gamma_{\mathcal{D}'}$, the double-coset space $\mathcal{T}_{\mathcal{D}'}(n)$ and Hecke operator $T_{\mathcal{D}'}(n)$ are defined just as for $\mathcal{D}$.

5 Proof of Theorem 1

Having set up all the specifics, we are now ready to prove Theorem 1.

5.1 Eliminating the weights from the elliptic term

We begin by using the twin group $\mathcal{D}'$ to obtain (in the weight $k = 2$ case) an expression involving the simpler elliptic term

$$\sum_{\alpha \in \mathcal{T}^e_{\mathcal{D}}(n) \,//\, \Gamma} \frac{\overline{\chi(\alpha)}}{|\Gamma_\alpha|} \quad \text{in place of} \quad \sum_{\alpha \in \mathcal{T}^e_{\mathcal{D}}(n) \,//\, \Gamma} \frac{\overline{\chi(\alpha)}}{|\Gamma_\alpha|} \frac{\eta_\alpha}{\eta_\alpha - \zeta_\alpha}.$$

To do this, we express the sum of the traces

$$\mathrm{tr}\,(T^{\chi}_{\mathcal{D}}(n)) + \mathrm{tr}\,(T^{\chi'}_{\mathcal{D}'}(n)),$$

using Theorem 2. (Note, since we assume n is not a square, the double coset space $\mathcal{T}_{\mathcal{D}}(n)$ (resp. $\mathcal{T}_{\mathcal{D}'}(n)$) doesn't have any scalar or parabolic elements). First, note that the map

$$\mathcal{T}_{\mathcal{D}}(n) \longrightarrow \mathcal{T}_{\mathcal{D}'}(n), \qquad \alpha \mapsto g\alpha g^{-1}, \qquad g = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{Z})$$

allows us to write the elliptic term of $\mathrm{tr}\,(\mathcal{T}^{\chi'}_{\mathcal{D}'}(n))$ as

$$\begin{aligned} \sum_{\alpha \in \mathcal{T}^e_{\mathcal{D}'}(n) \,//\, \Gamma'} \frac{\overline{\chi'(\alpha)}}{|\Gamma_\alpha|} \frac{\eta_\alpha^{k-1}}{\eta_\alpha - \zeta_\alpha} &= \sum_{\alpha \in \mathcal{T}^e_{\mathcal{D}}(n) \,//\, \Gamma} \frac{\overline{\chi'(g\alpha g^{-1})}}{|\Gamma_{g\alpha g^{-1}}|} \frac{\eta_{g\alpha g^{-1}}^{k-1}}{\eta_{g\alpha g^{-1}} - \zeta_{g\alpha g^{-1}}} \\ &= - \sum_{\alpha \in \mathcal{T}^e_{\mathcal{D}}(n) \,//\, \Gamma} \frac{\overline{\chi(\alpha)}}{|\Gamma_\alpha|} \frac{\zeta_\alpha^{k-1}}{\eta_\alpha - \zeta_\alpha}, \end{aligned}$$

where the second equality follows from the identities

$$\eta_{g\alpha g^{-1}} = \zeta_\alpha \quad \text{and} \quad \zeta_{g\alpha g^{-1}} = \eta_\alpha.$$

Thus, if $k = 2$, we see that $\mathrm{tr}\,(T_{\mathcal{D}}^{\chi}(n)) + \mathrm{tr}\,(T_{\mathcal{D}'}^{\chi'}(n))$ is equal to

$$-\sum_{\alpha \in \mathcal{T}_{\mathcal{D}}^{e}(n)//\Gamma} \frac{\overline{\chi(\alpha)}}{|\Gamma_\alpha|} - \sum_{\alpha \in \mathcal{T}_{\mathcal{D}}^{h}(n)//\Gamma} \overline{\chi(\alpha)} \frac{\min\{|\eta_\alpha|, |\zeta_\alpha|\}}{|\eta_\alpha - \zeta_\alpha|} + 2 \cdot \delta(\chi, 2) \sum_{\alpha \in \Gamma \backslash \mathcal{T}_{\mathcal{D}}(n)} \overline{\chi}(\alpha). \tag{8}$$

5.2 Using orthogonality to pick out residue classes

We will now use the orthogonality relations of the characters χ in such a way that our sums will be over matrices α which are congruent modulo N to a prescribed matrix. Using property 1 of Section 3, we may choose $a \in \mathcal{D} \cap \mathcal{A}$. We compute

$$\frac{1}{|\mathcal{D}^*|} \sum_{\chi \in \mathcal{D}^*} \chi(a) \left(\mathrm{tr}\,(T_{\mathcal{D}}^{\chi}(n)) + \mathrm{tr}\,(T_{\mathcal{D}'}^{\chi'}(n)) \right).$$

Using the orthogonality relations

$$\frac{1}{|\mathcal{D}^*|} \sum_{\chi \in \mathcal{D}^*} \chi(a)\overline{\chi}(\alpha) = \begin{cases} 1 & \text{if } \alpha \equiv a \mod N \\ 0 & \text{otherwise,} \end{cases}$$

together with (8), we find that the sum

$$\frac{1}{|\mathcal{D}^*|} \sum_{\chi \in \mathcal{D}^*} \chi(a) \left(t_e(T_{\mathcal{D}}^{\chi}(n)) + t_e(T_{\mathcal{D}'}^{\chi'}(n)) + t_h(T_{\mathcal{D}}^{\chi}(n)) + t_h(T_{\mathcal{D}'}^{\chi'}(n)) \right)$$

of the elliptic and hyperbolic terms is equal to

$$\sum_{\alpha \in \mathcal{T}_{\{a\}}^{e}(n)//\Gamma} \frac{1}{|\Gamma_\alpha|} + \sum_{\alpha \in \mathcal{T}_{\{a\}}^{h}(n)//\Gamma} \frac{\min\{|\eta_\alpha|, |\zeta_\alpha|\}}{|\eta_\alpha - \zeta_\alpha|}.$$

Using the classical set bijections

$$\Gamma \backslash \mathcal{T}_{\mathcal{D}}(n) \longleftrightarrow \Gamma(1) \backslash \mathcal{T}(n) \longleftrightarrow \left\{ \begin{pmatrix} d & b \\ 0 & n/d \end{pmatrix} : d \mid n,\ b \mod (n/d) \right\},$$

as well as

$$\{\chi \in \mathcal{D}^* : \chi|_{\mathcal{D} \cap SL_2(\mathbb{Z}/N\mathbb{Z})} \equiv 1\} \longleftrightarrow (\det(\mathcal{D}))^*$$

and the exact sequence

$$1 \longrightarrow \mathcal{D} \cap SL_2(\mathbb{Z}/N\mathbb{Z}) \longrightarrow \mathcal{D} \longrightarrow \det(\mathcal{D}) \longrightarrow 1,$$

we find that the remaining term

$$\frac{1}{|\mathcal{D}^*|} \sum_{\chi \in \mathcal{D}^*} \chi(a) \cdot 2 \cdot \delta(\chi, 2) \sum_{\alpha \in \Gamma \backslash \mathcal{T}_{\mathcal{D}}(n)} \overline{\chi}(\alpha)$$

is equal to

$$\frac{2}{|\mathcal{D} \cap SL_2(\mathbb{Z}/N\mathbb{Z})|} |\Gamma \backslash \mathcal{T}_{\mathcal{D}}(n)| = \frac{2}{[\Gamma : \Gamma(N)]} \sigma(n)$$

5.3 Passing from Γ to $\Gamma(1)$

We have now expressed the trace $\mathrm{tr}\,(T_{\mathcal{D}}^{\chi}(n)) + \mathrm{tr}\,(T_{\mathcal{D}'}^{\chi'}(n))$ in terms of a sum over Γ-conjugation orbits. We will now convert this into a sum over $\Gamma(1)$-conjugation orbits.

Lemma 4. *We have*

$$\sum_{\alpha \in \mathcal{T}^e_{\{a\}}(n)//\Gamma} \frac{1}{|\Gamma_\alpha|} \;=\; [\Gamma(1)_{a,N} : \Gamma] \sum_{\beta \in \mathcal{T}^e_{\mathcal{A}}(n)//\Gamma(1)} \frac{1}{|\Gamma(1)_\beta|} \tag{9}$$

and

$$\sum_{\alpha \in \mathcal{T}^h_{\{a\}}(n)//\Gamma} \frac{\min\{|\eta_\alpha|, |\zeta_\alpha|\}}{|\eta_\alpha - \zeta_\alpha|} \;=\; O_\varepsilon([\Gamma(1)_{a,N} : \Gamma] n^{1/2+\varepsilon}), \tag{10}$$

where

$$\Gamma(1)_{a,N} := \{\gamma \in \Gamma(1) : (\gamma \mod N)a = a(\gamma \mod N)\}.$$

Proof. First note that, if $\beta \in \mathcal{T}_{\mathcal{A}}(n)$, then $\Gamma(1)\beta\Gamma(1)^{-1} \cap \mathcal{T}_{\{a\}}(n) \neq \emptyset$, and so we may take such a β to belong to $\mathcal{T}_{\{a\}}(n)$. Thus, we may write the elliptic term as

$$\begin{aligned}\sum_{\alpha \in \mathcal{T}^e_{\{a\}}(n)//\Gamma} \frac{1}{|\Gamma_\alpha|} &= \sum_{\beta \in \mathcal{T}^e_{\mathcal{A}}(n)//\Gamma(1)} \left(\sum_{\alpha \in (\Gamma(1)\beta\Gamma(1)^{-1} \cap \mathcal{T}^e_{\{a\}}(n))//\Gamma} \frac{1}{|\Gamma_\alpha|} \right) \\ &= \sum_{\beta \in \mathcal{T}^e_{\mathcal{A}}(n)//\Gamma(1)} \left(\sum_{\alpha \in \Gamma(1)_{a,N}\beta\Gamma(1)^{-1}_{a,N}//\Gamma} \frac{1}{|\Gamma_\alpha|} \right)\end{aligned}$$

and likewise with the hyperbolic term: $\sum_{\alpha \in \mathcal{T}^h_{\{a\}}(n)//\Gamma} \frac{\min\{|\eta_\alpha|,|\zeta_\alpha|\}}{|\eta_\alpha - \zeta_\alpha|}$ is equal to

$$\begin{aligned}&\sum_{\substack{0<d<\sqrt{n} \\ d|n}} \frac{d}{n/d-d} \sum_{\beta \in \mathcal{T}^h_{\mathcal{A}}(\pm(n/d+d),n)//\Gamma(1)} \left(\sum_{\alpha \in (\Gamma(1)\beta\Gamma(1)^{-1} \cap \mathcal{T}^h_{\{a\}}(n))//\Gamma} 1 \right) \\ \leq &\sum_{\substack{0<d<\sqrt{n} \\ d|n}} \frac{d}{n/d-d} \sum_{\beta \in \mathcal{T}(\pm(n/d+d),n)//\Gamma(1)} \left(\sum_{\alpha \in \Gamma(1)_{a,N}\beta\Gamma(1)^{-1}_{a,N}//\Gamma} 1 \right).\end{aligned}$$

Into how many Γ-conjugation orbits does $\Gamma(1)_{a,N}\beta\Gamma(1)^{-1}_{a,N}$ decompose? Writing a right coset decomposition

$$\Gamma(1)_{a,N} = \bigsqcup_{b \in B} \Gamma b,$$

we have

$$\Gamma(1)_{a,N}\beta\Gamma(1)^{-1}_{a,N} = \bigcup_{b \in B} \Gamma b \beta b^{-1} \Gamma^{-1}. \tag{11}$$

If β is hyperbolic, then the centralizer $\Gamma(1)_\beta = \{\pm I\}$, and so, by property 3 of the group $\mathcal{D}$, the union (11) is disjoint. Thus, there are exactly $[\Gamma(1)_{a,N} : \Gamma]$ Γ-conjugation orbits in $\Gamma(1)_{a,N}\beta\Gamma(1)_{a,N}^{-1}$, and so $\sum_{\alpha\in\mathcal{T}^h_{\{a\}}(n)//\Gamma} \frac{\min\{|\eta_\alpha|,|\zeta_\alpha|\}}{|\eta_\alpha-\zeta_\alpha|}$ is less than or equal to

$$2\cdot[\Gamma(1)_{a,N}:\Gamma]\sum_{\substack{0<d<\sqrt{n}\\ d|n}}\frac{d}{n/d-d}\left|\mathcal{T}(n/d+d,n)//\Gamma(1)\right|.$$

One can show that there is a bijection

$$\mathcal{T}(n/d+d,n)\,//\,\Gamma(1)\longleftrightarrow\left\{\begin{pmatrix}d & x\\ 0 & n/d\end{pmatrix}:\ x \mod (n/d-d)\right\},$$

upon which (10) follows from

$$\sum_{\substack{0<d<\sqrt{n}\\ d|n}} d\le\sqrt{n}\sum_{d|n}1=O_\varepsilon(n^{1/2+\varepsilon}).$$

If β is elliptic and $\Gamma(1)_\beta=\{\pm I\}$, then again (11) is disjoint and (9) follows. Otherwise, $\Gamma(1)_\beta$ is a group of order 4 or 6, and in that case we decompose the set B of coset representatives into two subsets

$$B=B_1\sqcup B_2,$$

where

$$B_1=\{b\in B:\Gamma(1)_{b\beta b^{-1}}\subseteq\Gamma\}$$

and

$$B_2=\{b\in B:\Gamma(1)_{b\beta b^{-1}}\not\subseteq\Gamma\}$$

and note that, for $b\in B_2$, $\Gamma(1)_{b\beta b^{-1}}\cap\Gamma=\{\pm I\}$. We then observe that, for any $b,b'\in\Gamma(1)_{a,N}$ we have

$$\Gamma b\beta b^{-1}\Gamma^{-1}=\Gamma b'\beta b'^{-1}\Gamma^{-1}$$

if and only if the equivalent conditions

$$b'b^{-1}\in\Gamma(1)_{b'\beta(b')^{-1}}\Gamma\iff b'\in\Gamma\Gamma(1)_{b\beta b^{-1}}b$$

hold. The first condition shows that unless $b,b'\in B_2$ we must have

$$\Gamma b\beta b^{-1}\Gamma^{-1}\cap\Gamma b'\beta b'^{-1}\Gamma^{-1}=\emptyset,$$

and when $b,b'\in B_2$ the second condition shows that the number of conjugation orbits in

$$\bigcup_{b\in B_2}\Gamma b\beta b^{-1}\Gamma^{-1}$$

collapses by a factor of $\frac{2}{|\Gamma(1)_\beta|}$. In this case we have

$$\sum_{\alpha\in\Gamma(1)_{a,N}\beta\Gamma(1)_{a,N}^{-1}//\Gamma}\frac{1}{|\Gamma_\alpha|}=\sum_{b\in B_1}\frac{1}{|\Gamma(1)_\beta|}+\frac{2}{|\Gamma(1)_\beta|}\sum_{b'\in B_2}\frac{1}{2}$$
$$=\frac{[\Gamma(1)_{a,N}:\Gamma]}{|\Gamma(1)_\beta|},$$

upon which (9) follows, concluding the proof of Lemma 4. □

5.4 Finishing the proof

We have now shown that when $k=2$, the trace $\frac{1}{|\mathcal{D}|}\sum_{\chi\in\mathcal{D}^*}\left(\mathrm{tr}\,(T_{\mathcal{D}}^{\chi}(n))+\mathrm{tr}\,(T_{\mathcal{D}'}^{\chi'}(n))\right)$ is equal to

$$-[\Gamma(1)_{a,N}:\Gamma]\sum_{\beta\in\mathcal{T}_{\mathcal{A}}^{\epsilon}(n)//\Gamma(1)}\frac{1}{|\Gamma(1)_\beta|}+\frac{2}{[\Gamma:\Gamma(N)]}\sigma(n)+O_\varepsilon([\Gamma(1)_{a,N}:\Gamma]n^{1/2+\varepsilon}).$$

On the other hand, writing the trace of each $T_{\mathcal{D}}^{\chi}(n)$ with respect to a basis $\{f_1,f_2,\ldots,f_g\}\subset\mathcal{S}_2(\Gamma)$ of Hecke eigenforms, together with

$$S_2(\Gamma(N))=\bigoplus_{\chi\in(\Gamma/\Gamma(N))^*}S_2(\Gamma,\chi)$$

and the Ramanujan bound

$$|\lambda_i(n)|=O_\varepsilon(n^{1/2+\varepsilon})\qquad\qquad(T_{\mathcal{D}}^{\chi}(n)f_i=\lambda_i(n)f_i)$$

for the Hecke eigenvalues, we see also that

$$\frac{1}{|\mathcal{D}|}\sum_{\chi\in\mathcal{D}^*}\left(\mathrm{tr}\,(T_{\mathcal{D}}^{\chi}(n))+\mathrm{tr}\,(T_{\mathcal{D}'}^{\chi'}(n))\right)=O_\varepsilon\left(\frac{\text{genus of }X(N)}{[\Gamma:\Gamma(N)]}n^{1/2+\varepsilon}\right).$$

Thus,

$$\sum_{\beta\in\mathcal{T}_{\mathcal{A}}^{\epsilon}(n)//\Gamma(1)}\frac{1}{|\Gamma(1)_\beta|}=\frac{2}{[\Gamma(1)_{a,N}:\Gamma(N)]}\sigma(n)+O_\varepsilon\left(\frac{\text{genus of }X(N)}{[\Gamma(1)_{a,N}:\Gamma(N)]}n^{1/2+\varepsilon}\right)$$
$$=\frac{2|\mathcal{A}|}{|SL_2(\mathbb{Z}/N\mathbb{Z})|}\sigma(n)+O_\varepsilon\left(\frac{|SL_2(\mathbb{Z}/N\mathbb{Z})||\mathcal{A}|}{|SL_2(\mathbb{Z}/N\mathbb{Z})|}n^{1/2+\varepsilon}\right),$$

finishing the proof of Theorem 1. For the genus of $X(N)$, see [9, Theorem 4.2.11], for example. Note that in case $n=p$ is prime we obtain the sharper error term $O(|\mathcal{A}|p^{1/2})$, with an absolute constant.

Corollary 5. *Suppose $\mathcal{B}$ is any subset of $GL_2(\mathbb{Z}/N\mathbb{Z})$ which is stable by $SL_2(\mathbb{Z}/N\mathbb{Z})$-conjugation and which has constant determinant, i.e.*

$$\forall b,\,b'\in\mathcal{B},\quad \det b=\det b'.$$

Then, the result of Theorem 1 holds when one replaces $\mathcal{A}$ by $\mathcal{B}$, namely

$$\sum_{A \in \mathcal{T}_{\mathcal{B}}^{e}(n) \,//\, SL_2(\mathbb{Z})} \frac{1}{|SL_2(\mathbb{Z})_A|} = \frac{2|\mathcal{B}|}{|SL_2(\mathbb{Z}/N\mathbb{Z})|}\sigma(n) + O_{\varepsilon}(|\mathcal{B}|n^{1/2+\varepsilon}),$$

with the sharper error term $O(|\mathcal{B}|p^{1/2})$ (with an absolute implied constant) if $n = p$ is prime.

Proof. Write

$$\mathcal{B} = \bigsqcup_i \mathcal{A}_i,$$

where $\mathcal{A}_i$ are $SL_2(\mathbb{Z}/N\mathbb{Z})$-conjugation orbits, and apply Theorem 1. □

References

[1] I. Chen, *The Jacobians of non-split Cartan modular curves*, Proc. London Math. Soc. (3) no. 1 (1998), 1–38.

[2] D. A. Cox, *Primes of the form $x^2 + ny^2$*, Wiley, 1989.

[3] P. Deligne, *La conjecture de Weil I*, Publ. Math. Inst. Hautes Études Sci. No. 43 (1974), 273–307.

[4] M. Deuring, *Die typen der Multiplikationenringe der elliptischen Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg 14 (1941), 197–272.

[5] W. D. Duke, *Elliptic curves with no exceptional primes*, C. R. Math. Acad. Sci. Paris Sér. I 325 (1997), 813–818.

[6] M. Eichler, *Eine verallgemeinerung der abelschen integrale*, Math. Z. 67 (1957), 267–289.

[7] H. Hijikata, *Explicit formula of the traces of Hecke operators for $\Gamma_0(N)$*, J. Math. Soc. Japan 26 (1974), 56–82.

[8] A. Hurwitz, *Über die Klassenzahlrelationen und Modularkorrespondenzen primzahliger Stufe*, in: Werke Bd. II, Birkhäuser Verlag, 1963, 51–67.

[9] T. Miyake, *Modular Forms*, Springer-Verlag, 1989.

[10] J. Oesterle, *Sur la trace des opérateurs de Hecke*, Ph.D. Thesis, L'Université de Paris-Sud, Centre d'Orsay, 1977.

[11] M. Saito, *On Eichler's trace formula*, J. Math. Soc. Japan, 24 (2) (1971), 333–340.

Centre de Recherches Mathématiques
Université de Montréal
P.O. Box 6128,
Centre-ville Station
Montréal, Québec H3C 3J7, Canada.
E-mail: jones@dms.umontreal.ca