Strong multiplicity one for classical modular forms

Saisudharshan Sivakumar

Undergraduate Honors Thesis – Spring 2024
Department of Mathematics, University of Florida
v1.0

Abstract

Classical modular forms are analytic functions of the upper half plane invariant under the action of congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$, up to a factor of automorphy. In this setting, the Hecke operators on the space of modular forms are normal operators on the subspace of cusp forms, the modular forms that vanish at cusps. Cusp forms satisfy the strong multiplicity one property, which roughly says that normalized eigenfunctions of the Hecke operators are uniquely determined by their eigenvalues. Strong multiplicity one, and other multiplicity one results, are often presented in the language of automorphic forms and representation theory. We introduce the theory of classical modular forms and provide a self-contained proof of the strong multiplicity one property for classical modular forms, following the proof in Modular Forms by Toshitsune Miyake. This approach avoids using the language of automorphic forms and representation theory by studying L-functions associated to modular forms, and their Euler products. An application of the strong multiplicity one property yields a basis for the space of cusp forms, which is nice since the space of modular forms decomposes into the direct sum of the space of cusp forms and the space of Eisenstein series.

Acknowledgements

I would like to thank my advisor, Dr. Jeremy Booher, for his guidance as I learned about modular forms and the difficulties of writing mathematics. Prior to his advising, I had not even had the foggiest idea of how to write a thesis, much less of how select a suitable topic. I would like to thank him specifically for reading and commenting on drafts of my thesis. He also helped me greatly in the application process for mathematics graduate school, by writing letters of recommendation, giving advice on my personal statements, and encouraging me to apply to good programs that would fit my interests. He also taught me algebra in a kind manner that reaffirmed my interest in the subject, and provided friendship in difficult times.

I also wish to thank Dr. Sergei Shabanov for his guidance and support throughout my entire time as an undergraduate. I began as a freshman in his Honors Calculus 3 course, and took his courses all the way through his Mathematical Methods in Physics course, all of which were taught at a higher standard that encouraged me to do my best. He had also written many letters of recommendation for REUs and for graduate school. I feel that my attitude towards mathematics was shaped in great part by his, specifically valuing the ability and endurance to do (lengthy) computations and the ability to understand abstract concepts in concrete ways.

Another professor I would like to thank is Dr. Lei Zhang for teaching me Fourier analysis. It was his enthusiastic teaching that made it quite clear to me that it is the most beautiful part of mathematics, and inspired me to do my own reading. The Fourier transform and its avatars have appeared several times during my undergraduate years, in different areas of mathematics (and this thesis!). I have the unshakeable feeling that I will need the rest of my life to meditate on these ideas.

I would like to thank my friends from the math department as well as from the physics department for their company and support. I hope to see them many times in the future. My highschool math teachers, Mrs. Erika Sheehan and Mr. Martin Doherty, and my highschool physics teacher, Dr. Rajasekhar Narisetty, also deserve thanks due to initiating and encouraging my interest in mathematics.

Lastly, I would like to thank my parents for their lifelong support and love for me, and for having faith in me as I progress into the next stages of life.

Contents

Introduction

Modular forms are functions defined on the complex upper half plane that satisfy certain holomorphy conditions, and are invariant under a certain action of so-called *congruence subgroups* of $\mathrm{SL}_2(\mathbb{Z})$, up to some factor. A modular form f admits a Fourier series expansion

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z},$$

where z is in the upper half plane and the a_n are complex numbers. Often, the symbol q is used in place of $e^{2\pi i z}$, so that the Fourier series expansion becomes the q-series expansion $f(z) = \sum_{n=0}^{\infty} a_n q^n$. Each modular form has an associated integer *weight* k and an integer *level* N which characterizes how it transforms under the action of a particular congruence subgroup. There are interesting connections between the theory of modular forms and other areas of mathematics, as we will see in the following examples.

A famous example of a modular form is the weight 12, level 1 *modular discriminant* function Δ given by

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}, \quad q = e^{2\pi i z}.$$

(See LMFDB newform orbit 1.12.a.a.) The *Ramanujan tau function* τ denotes the Fourier coefficients of Δ; that is, $\Delta(z) = \sum_{n=1}^{\infty} \tau(n) q^n$. The tau function satisfies several curious congruence relations, such as:

$$\begin{aligned} \tau(n) &\equiv \sigma_{11}(n) \pmod{2^{11}} \quad \text{for } n \equiv 1 \pmod 8 \\ \tau(n) &\equiv 1217\sigma_{11}(n) \pmod{2^{13}} \quad \text{for } n \equiv 3 \pmod 8 \\ \tau(n) &\equiv 1537\sigma_{11}(n) \pmod{2^{12}} \quad \text{for } n \equiv 5 \pmod 8, \end{aligned}$$

where σ_k is the divisor function given by $\sigma_k(n) = \sum_{d|n} d^k$. In past decades, it was shown that the Fourier coefficients of other modular forms also satisfy similar kinds of congruences. As a result, the theory of congruences of modular forms has garnered significant interest in contemporary number theory.

Another interesting property of the tau function that Ramanujan observed in the early 1900s was that it was a multiplicative function: $\tau(mn) = \tau(m)\tau(n)$ for coprime integers m, n. Mordell gave a proof of this property in 1917, and in the late 1930s, Hecke provided a general theory involving Hecke operators that generalized Mordell's approach to spaces of modular forms and obtained similar results for modular forms.

For another example of a modular form, consider the weight 2, level 11 modular form f given by

$$f(q) = q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2, \quad q = e^{2\pi i z}.$$

(See LMFDB newform orbit 11.2.a.a.) Formally expand this infinite product into the q-series $\sum_{n=1}^{\infty} a_n q^n$. The first few terms of this sum are $q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 + \cdots$. Some interesting facts are that the coefficients a_p for primes $p \neq 11$ satisfy $a_p \equiv p + 1 \pmod 5$, and that the coefficients a_n are multiplicative.

Now consider the *elliptic curve* defined by the equation $y^2 + y = x^3 - x$. For each p, let b_p be p minus the number of solutions in $(\mathbb{Z}/p\mathbb{Z})^2$ to the equation $y^2 + y = x^3 - x$. The first few values of b_p for the primes $2, 3, 5, 7$ are $-2, -1, 1, -2$. But if we compare these values to a_p for the same primes $2, 3, 5, 7$, we find that $a_p = b_p$. Somewhat miraculously, it is true this equality holds for all primes p except for $p = 11$.

The connection between modular forms and elliptic curves is quite profound. The book [DS05] focuses on a result called the *Modularity theorem*, which states that all rational elliptic curves may be obtained from modular forms. This was formerly called the Taniyama-Shimura conjecture, which was posed around 1955. A full proof of the modularity theorem appeared at the turn of the century, but partial progress by Wiles and Taylor on this result led to the proof of Fermat's Last Theorem.

In this thesis, we focus on the Hecke operators and prove the ***strong multiplicity one*** theorem for modular forms. This result is usually stated using the language of *automorphic* forms and representation theory. Automorphic forms are, broadly speaking, a generalization of modular forms in that they are well-behaved functions on the complex upper half plane with respect to the action of some action of a discrete topological (usually matrix) group. We focus on classical modular forms because they are a natural entry point into the theory of automorphic forms, and the strong multiplicity one theorem is essential to the development of the theory of modular forms. ("Classical" modular forms are so named in order to distinguish them from other specialized modular forms appearing in the zoo of almost-invariant functions on the upper half plane with respect to the action of other matrix groups; for example, the Maass forms or the Bianchi modular forms.)

We continue setting the stage for the strong multiplicity one theorem. The collection of all modular forms of a fixed weight and level forms a vector space. This vector space may be decomposed into the direct sum of the space of *cusp forms* and the space of *Eisenstein series*. The space of cusp forms is characterized by the property that the modular forms in this space vanish "at infinity" in a particular way. This property manifests in cusp forms as having constant term zero in their q-series expansions. For example, both the Δ function and f above are cusp forms. An important feature of the space of cusp forms is that we may endow it with the Petersson inner product. The Eisenstein series are well studied modular forms with a number of other properties which we do not discuss.

The *Hecke operators* $\langle n \rangle$ and T_n are certain kinds of "averaging" operators that decompose the spaces of modular forms and cusp forms into the direct sum of what are called χ-*eigenspaces*, which interact nicely with the Hecke operators. The spectral properties of the Hecke operators are of great importance. For starters, the Hecke operators are normal operators on the space of cusp forms, so there exists an orthogonal basis of simultaneous eigenfunctions for the space of cusp forms. More interestingly, we have the following: If the modular form g has Fourier series expansion $\sum_{n=0}^{\infty} t_n e^{2\pi i n z}$ with $t_1 = 1$, and is a simultaneous eigenfunction of the Hecke operators T_n, then

$$T_n g = t_n g$$

for all $n \geq 1$. Hecke eigenvalues are also multiplicative; that is, $t_{mn} = t_m t_n$ for m, n coprime. Thus the Fourier coefficients of f, and the Ramanujan tau function $\tau(n)$, are multiplicative.

The strong multiplicity one property of cusp forms is as follows: Let g be a cusp form at level M that is normalized; that is, g has first Fourier coefficient equal to 1, and is a common eigenfunction of all of the Hecke operators T_n. If there exists a cusp form f that is a normalized eigenfunction f of the Hecke operators T_n at level N (which need not be equal to M) whose Fourier coefficients, that is, its eigenvalues, agree with the Fourier coefficients of g at all indices n coprime to some integer L, we show that g is equal to the cusp form f at level N. In other words, the eigenvalues of g determine the cusp form uniquely.

One elementary application of this result in the theory of modular forms is to determine a basis for the space of cusp forms. In [DS05, Theorem 5.8.3], a particular set of cusp forms, belonging to an even finer collection of cusp forms called *newforms*, is shown to span the space of cusp forms. To obtain the linear independence of these newforms, suppose that there is a nontrivial linear combination of elements in the spanning set that equals zero, $\sum_i c_i f_i = 0$. One can show that this linear combination is of newforms that are eigenfunctions of the Hecke operators, with equal Fourier coefficients away from some fixed integer L. So by strong multiplicity one, each of the f_i are equal, from which linear dependence follows.

We develop the necessary theory of classical modular forms and Hecke operators, mostly following [DS05], and then transition into the proof of strong multiplicity one in [Miy05, Theorem 4.6.19]. This approach avoids the language of automorphic forms and representation theory, and instead obtains the result by studying the L-functions associated to modular forms and their associated Euler products. Almost all of of the results coming from [Miy05] have been reformulated to follow the more modern perspective found in [DS05], especially in the development of the Hecke operators.

0 Preliminaries

In this section, we collect the definitions and results needed to define modular forms. We describe the action of $\mathrm{SL}_2(\mathbb{Z})$ and its congruence subgroups on the upper half plane of the complex plane and introduce the congruence subgroups $\Gamma_0(N)$ and $\Gamma_1(N)$, which will appear in every section thereafter. We discuss modular curves and compactified modular curves briefly.

0.1 The modular group and congruence subgroups

Let R be a unital ring. The ***general linear group*** $\mathrm{GL}_n(R)$ is the group of $n \times n$ invertible matrices with entries from R; that is, matrices with unit determinant, under matrix multiplication. The ***special linear group*** $\mathrm{SL}_n(R)$ is the (normal) subgroup of $\mathrm{GL}_n(R)$ whose matrices have determinant 1_R.

Definition 0.1. The ***modular group*** $\mathrm{SL}_2(\mathbb{Z})$ is the group of 2×2 integer-valued matrices with determinant 1, and is a subgroup of $\mathrm{GL}_2(\mathbb{R})$. †

It is well known (e.g., [Ser78, Chapter 7, Section 1.2, Theorem 2]) that

$$\mathrm{SL}_2(\mathbb{Z}) = \left\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\rangle, \tag{0.1}$$

and that $\mathrm{SL}_2(\mathbb{Z})$ acts on the Riemann sphere $\widehat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ by fractional linear transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az+b}{cz+d}.$$

For $c \neq 0$, $-d/c$ is sent to ∞ and ∞ is sent to a/c; if $c = 0$ then ∞ is sent to ∞. We check that this action defines a group action: It is clear that the identity matrix sends z to itself, and that

$$\begin{pmatrix} q & r \\ s & t \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \begin{pmatrix} q & r \\ s & t \end{pmatrix}\left(\frac{az+b}{cz+d}\right) = \frac{q\frac{az+b}{cz+d}+r}{s\frac{az+b}{cz+d}+t} = \frac{(qa+rc)z+qb+rd}{(sa+tb)z+sb+td} = \begin{pmatrix} qa+rc & qb+rd \\ sa+tb & sb+td \end{pmatrix}(z)$$

for $\left(\begin{smallmatrix} q & r \\ s & t \end{smallmatrix}\right), \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. Similarly, $\mathrm{GL}_2(\mathbb{R})$ acts on $\widehat{\mathbb{C}}$ by fractional linear transformations. It follows that these transformations are (bi)holomorphic and are automorphisms. Furthermore, both I and $-I$ act as the identity on $\widehat{\mathbb{C}}$, so for any $A \in \mathrm{SL}_2(\mathbb{Z})$, the actions of A and $-A$ agree. The generators in (0.1) correspond to the maps

$$z \mapsto z+1 \quad \text{and} \quad z \mapsto -1/z.$$

We consider particular subgroups of the modular group.

Definition 0.2. For N a positive integer, the ***principal congruence subgroup of level*** N, $\Gamma(N)$, is given by the subgroup

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

with the matrix congruence interepreted as congruence modulo N entrywise. †

Alternatively, $\Gamma(N) = (I + N\,\mathrm{M}_2(\mathbb{Z})) \cap \mathrm{SL}_2(\mathbb{Z})$. Furthermore, observe that if $N \mid M$, then $\Gamma(M) \subset \Gamma(N)$, since $x \equiv y \pmod{M}$ implies $x \equiv y \pmod{N}$ whenever $N \mid M$.

Lemma 0.3. *The principal congruence subgroup $\Gamma(N)$ is the kernel of the natural homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, so $\Gamma(N)$ is normal in $\mathrm{SL}_2(\mathbb{Z})$; furthermore, the natural homomorphism is surjective.*

Proof. It is clear that $\Gamma(N)$ is the kernel of the natural homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, so we prove that this map is surjective. When $N = 1$, the natural homomorphism is the zero map (so $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$). Let $N > 1$, and consider an element

$$\begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}),$$

so that $\overline{ad-bc} = \overline{1}$ (here $\overline{\cdot}$ denotes reduction modulo N). Then for some integer k, $ad - bc = 1 + kN$. It follows that $1 + kN$ is a multiple of $g = \gcd(c, d)$, so that $\gcd(g, N) = 1$ and $\gcd(c, d, N) = 1$. We show that there exist integers i, j such that $c + iN$ and $d + jN$ are coprime.

If $c \neq 0$, consider a solution j to the system of congruences

$$\begin{cases} j \equiv 1 \pmod{p} & p \mid g \\ j \equiv 0 \pmod{p} & p \nmid g, p \mid c, \end{cases}$$

which may be obtained via the Chinese remainder theorem. Then $\gcd(c, d + jN) = 1$ since any prime p dividing c will not divide $d + jN$ with j chosen as above (of primes p dividing c, when $p \mid g$, we have $p \nmid N$, and when $p \nmid g$, we have $p \nmid d$). If $c = 0$, then $d \neq 0$ and repeat this argument with d, i in place of c, j respectively.

With integers $c + iN$ and $d + jN$ coprime, there exist integers s, t with $s(c + iN) + t(d + jN) = 1$. Then

$$\det \begin{pmatrix} a - (k + aj - bi)tN & b + (k + aj - bi)sN \\ c + iN & d + jN \end{pmatrix} = ad + ajN - (k + aj - bi)tN(d + jN)$$
$$- bc - biN - (k + aj - bi)sN(c + iN) = 1 + kN + ajN - biN - (k + aj - bi)N = 1$$

and

$$\begin{pmatrix} \overline{a - (k + aj - bi)tN} & \overline{b + (k + aj - bi)sN} \\ \overline{c + iN} & \overline{d + jN} \end{pmatrix} = \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$$

as needed. □

Therefore, by the first isomorphism theorem, $\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Lemma 0.4. *The index of* $\Gamma(N)$ *in* $\mathrm{SL}_2(\mathbb{Z})$ *is* $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = N^3 \prod_{p|N}(1 - 1/p^2)$.

Proof. We first show that $|\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})| = p^{3e}(1 - 1/p^2)$ for a prime p by induction on e.

The determinant is a surjective homomorphism from $\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})$ to $(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ with kernel $\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})$. Observe that $|\mathrm{GL}_2(\mathbb{Z}/p\mathbb{Z})|$ is the number of ordered bases of $(\mathbb{Z}/p\mathbb{Z})^2$, given by $(p^2 - 1)(p^2 - p)$. (The first factor counts the number of admissible first basis vectors, and the second factor counts the number of admissible second basis vectors after choosing a first basis vector.) Then by the first isomorphism theorem, $|\mathrm{SL}_2(\mathbb{Z}/p\mathbb{Z})| = (p^2 - 1)(p^2 - p)/(p - 1) = p(p^2 - 1) = p^3(1 - 1/p^2)$.

By Lemma 0.3, the natural homomorphism $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$ is surjective. The surjection $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$ is equal to the composition of the natural homomorphisms $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p^{e+1}\mathbb{Z})$ and $\mathrm{SL}_2(\mathbb{Z}/p^{e+1}\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$, from which it follows that $\mathrm{SL}_2(\mathbb{Z}/p^{e+1}\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$ is surjective also.

Any element γ of $\ker(\mathrm{SL}_2(\mathbb{Z}/p^{e+1}\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z}))$ is of the form

$$\begin{pmatrix} \overline{1 + ip^e} & \overline{rp^e} \\ \overline{sp^e} & \overline{1 + jp^e} \end{pmatrix},$$

for $i, j, r, s \in \{0, \ldots, p-1\}$ and $i = p - j$ (so that $\det \gamma = 1$). Hence $\left|\ker(\mathrm{SL}_2(\mathbb{Z}/p^{e+1}\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z}))\right| = p^3$. Suppose that $|\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})| = p^{3e}(1 - 1/p^2)$. Then by the first isomorphism theorem, $\left|\mathrm{SL}_2(\mathbb{Z}/p^{e+1}\mathbb{Z})\right| = p^3|\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})| = p^3 p^{3e}(1 - 1/p^2) = p^{3(e+1)}(1 - 1/p^2)$ as needed. By induction, $|\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})| = p^{3e}(1 - 1/p^2)$ for any e.

There is an isomorphism of matrix groups $\mathrm{M}_2(\prod_{i=1}^n R_i) \cong \prod_{i=1}^n \mathrm{M}_2(R_i)$ for rings R_i which restricts to the isomorphisms $\mathrm{GL}_2(\prod_{i=1}^n R_i) \cong \prod_{i=1}^n \mathrm{GL}_2(R_i)$ and $\mathrm{SL}_2(\prod_{i=1}^n R_i) \cong \prod_{i=1}^n \mathrm{SL}_2(R_i)$ since $(\prod_{i=1}^n R_i)^\times \cong \prod_{i=1}^n R_i^\times$ and $1_{\prod_{i=1}^n R_i} = \prod_{i=1}^n 1_{R_i}$.

Let N have prime factorization $N = \prod_{p|N} p^e$. By the Chinese remainder theorem, $\mathbb{Z}/N\mathbb{Z} \cong \prod_{p|N} \mathbb{Z}/p^e\mathbb{Z}$. It follows that $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}) \cong \prod_{p|N} \mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})$, from which we have

$$|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})| = \prod_{p|N} |\mathrm{SL}_2(\mathbb{Z}/p^e\mathbb{Z})| = \prod_{p|N} p^{3e}(1 - 1/p^2) = N^3 \prod_{p|N}(1 - 1/p^2)$$

as desired. □

Definition 0.5. A subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ is a ***congruence subgroup (of level*** N**)** if for some positive integer N, $\Gamma(N) \subset \Gamma$. †

Note that congruence subgroups need not be normal in $\mathrm{SL}_2(\mathbb{Z})$.

Let Γ be a level N congruence subgroup. We have $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma][\Gamma : \Gamma(N)]$, and since $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$ is finite, $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$ must also be finite; that is, congruence subgroups have finite index in $\mathrm{SL}_2(\mathbb{Z})$.

Definition 0.6. Frequently used congruence subgroups are

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\} \text{ and}$$
$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\},$$

where $*$ denotes unspecified quantities and the matrix congruences are to be taken entrywise. †

For any positive integer N, the inclusions $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ hold.

Lemma 0.7. *The map* $\Gamma_1(N) \to \mathbb{Z}/N\mathbb{Z}$ *given by* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \bar{b}$ *is surjective with kernel* $\Gamma(N)$.

Proof. For $\bar{b} \in \mathbb{Z}/N\mathbb{Z}$, $\left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right)$ has unit determinant and maps to $\bar{b}$ under the above map. It is clear that the kernel of the above map is $\Gamma(N)$. □

It follows that $\Gamma_1(N)/\Gamma(N) \cong \mathbb{Z}/N\mathbb{Z}$, so that the index of $\Gamma(N)$ in $\Gamma_1(N)$ is N. What follows is a similar result.

Lemma 0.8. *The map* $\Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$ *given by* $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mapsto \bar{d}$ *is surjective with kernel* $\Gamma_1(N)$.

Proof. Let $\bar{d} \in (\mathbb{Z}/N\mathbb{Z})^\times$ be given, and note that $\gcd(d, N) = 1$. Let $c \equiv 0 \pmod{N}$ so that $c = kN$ for some integer k. Choose k coprime to d so that $\gcd(d, kN) = \gcd(d, c) = 1$. Then there exist integers a, b with $ad - bc = 1$. Then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto d \quad \text{and} \quad \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1.$$

If $A \in \Gamma_0(N)$ and

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \bar{1},$$

so $d = jN + 1$ for some integer j. Since $c \equiv 0 \pmod{N}$, $c = kN$ and $\gcd(d, c) = 1$. There exist integers a, b with $1 = ad - bc = a(jN + 1) + bkN = a + (aj + bk)N$. Reducing modulo N gives $a \equiv 1 \pmod{N}$. It follows that $A \in \Gamma_1(N)$. Conversely, if $A \in \Gamma_1(N)$, then $A \mapsto \bar{1}$. □

Hence $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$, so that the index of $\Gamma_1(N)$ in $\Gamma_0(N)$ is $\phi(N) = |(\mathbb{Z}/N\mathbb{Z})^\times| = N \prod_{p|N}(1 - 1/p)$, where ϕ denotes the Euler totient function.

Corollary 0.9. *We obtain*

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]}{[\Gamma_0(N) : \Gamma_1(N)][\Gamma_1(N) : \Gamma(N)]} = \frac{N^3 \prod_{p|N}(1 - 1/p^2)}{N \cdot N \prod_{p|N}(1 - 1/p)} = N \prod_{p|N}(1 + 1/p).$$

0.2 Modular curves

Recall that $\mathrm{SL}_2(\mathbb{Z})$, and more broadly $\mathrm{GL}_2(\mathbb{R})$, acts on the Riemann sphere $\widehat{\mathbb{C}}$ by fractional linear transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \frac{az+b}{cz+d}.$$

If $\gamma \in \mathrm{GL}_2(\mathbb{R})$ with $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $z \in \mathbb{C}$, the computation $(az+b)(c\overline{z}+d) = ac|z|^2 + bd + adz + bc\overline{z} = ac|z|^2 + bd + adz + (ad - \det\gamma)\overline{z} = ac|z|^2 + bd + ad(z+\overline{z}) - \det\gamma\overline{z}$ shows that

$$\text{(0.2)} \qquad \mathrm{Im}(\gamma(z)) = \mathrm{Im}\left(\frac{az+b}{cz+d}\right) = \frac{\mathrm{Im}((az+b)(c\overline{z}+d))}{|cz+d|^2} = \frac{\mathrm{Im}(-\det\gamma\overline{z})}{|cz+d|^2} = \frac{\det\gamma\,\mathrm{Im}(z)}{|cz+d|^2}.$$

From the above calculation it follows that if $\det\gamma > 0$ and z belongs to the ***upper half plane*** $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$, then $\gamma(z) \in \mathcal{H}$. In particular, it follows that $\mathrm{GL}_2^+(\mathbb{R}) = \{\gamma \in \mathrm{GL}_2(\mathbb{R}) : \det\gamma > 0\}$, $\mathrm{SL}_2(\mathbb{Z})$, and any congruence subgroup Γ of $\mathrm{SL}_2(\mathbb{Z})$ act on the upper half plane $\mathcal{H}$ by fractional linear transformations.

Definition 0.10. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. The ***modular curve*** $Y(\Gamma)$ is the orbit space $\Gamma\backslash\mathcal{H} = \{\Gamma z : z \in \mathcal{H}\}$. †

The modular curves for the congruence subgroups $\Gamma_0(N), \Gamma_1(N)$, and $\Gamma(N)$ are denoted by $Y_0(N), Y_1(N)$, and $Y(N)$, respectively.

We topologize modular curves and briefly show they are compact Riemann surfaces. Let Γ be a congruence subgroup. The upper half plane $\mathcal{H}$ is given the Euclidean topology (as a subspace of $\mathbb{C}$ or of $\mathbb{R}^2$), and the natural surjection

$$\pi\colon \mathcal{H} \to Y(\Gamma) \quad \text{defined by} \quad z \mapsto \Gamma z$$

induces the quotient topology on $Y(\Gamma)$ (i.e., the open sets in $Y(\Gamma)$ are those with open preimages under π).

Lemma 0.11. *The quotient map $\pi\colon \mathcal{H} \to Y(\Gamma)$ is an open map.*

Proof. It suffices to show that the projection π takes an open disk B in $\mathcal{H}$ to an open set in $Y(\Gamma)$; that is, to show that

$$\bigcup_{\gamma\in\Gamma} \gamma(B)$$

is open. Since each γ^{-1} is continuous, each $\gamma(B)$ is open, so π is an open map. □

Proposition 0.12. *The action of the modular group $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ is properly discontinuous; that is, for $z_1, z_2 \in \mathcal{H}$, (including the case $z_1 = z_2$) there exist neighborhoods U_1 of z_1 and U_2 of z_2 in $\mathcal{H}$ such that for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, if $\gamma(U_1) \cap U_2 \neq \emptyset$, then $\gamma(z_1) = z_2$. Equivalently, for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, if $\gamma(z_1) \neq z_2$, then $\gamma(U_1) \cap U_2 = \emptyset$.*

Proof. Let V_1 and V_2 be neighborhoods of z_1 and z_2, respectively, with compact closure (e.g. open disks or bounded open sets). Let $y_1 = \sup_{z\in V_1}\{\mathrm{Im}(z)\}$, $Y_1 = \sup_{z\in V_1}\{\mathrm{Im}(z)\}$, and $y_2 = \inf_{z\in V_2}\{\mathrm{Im}(z)\}$. Then from (0.2), we have for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ not equal to $\pm I$ (i.e., $c \neq 0$) and $z \in V_1$ that

$$\mathrm{Im}(\gamma(z)) = \frac{\mathrm{Im}(z)}{|cz+d|^2} \leq \frac{\mathrm{Im}(z)}{c^2|z|^2} \leq \frac{1}{c^2\,\mathrm{Im}(z)} \leq \frac{1}{c^2 y_1}$$

and

$$\mathrm{Im}(\gamma(z)) = \frac{\mathrm{Im}(z)}{|cz+d|^2} \leq \frac{Y_1}{\mathrm{Re}(cz+d)^2} = \frac{Y_1}{(c\,\mathrm{Re}(z)+d)^2},$$

so that $\mathrm{Im}(\gamma(z)) \leq \min\left\{1/c^2 y_1, Y_1/(c\,\mathrm{Re}(z)+d)^2\right\}$. All but finitely many integers c may be chosen so that $1/c^2 y_1 < y_2$, and of the finitely many c where this inequality does not hold, we may choose all but finitely many d such that $Y_1/(c\,\mathrm{Re}(z)+d)^2 < y_2$ uniformly in z (since V_1 has compact closure). Thus for all but finitely many integers c, d, if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$, then

$$\sup_{z\in V_1} \{\mathrm{Im}(\gamma(z))\} < \inf_{z\in V_2} \{\mathrm{Im}(z)\}. \tag{0.3}$$

Thus for $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ satisfying (0.3), $\gamma(V_1) \cap V_2 = \emptyset$. We show that there are only finitely many $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ for which $\gamma(V_1) \cap V_2 \neq \emptyset$.

We determine the matrices in $\mathrm{SL}_2(\mathbb{Z})$ which have fixed bottom row (c, d). This is equivalent to finding all matrices $\eta = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ such that $\eta\gamma$ has bottom row (c, d), where $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is a fixed matrix with bottom row (c, d). Evidently $C = 0$ and $D = 1$, and since $1 = AD - BC = A$, we have that η must have the form $\left(\begin{smallmatrix} 1 & B \\ 0 & 1 \end{smallmatrix}\right)$, and B may be taken to be any integer. Explicitly, the matrices in $\mathrm{SL}_2(\mathbb{Z})$ with bottom row (c, d) are

$$\left\{ \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} : k \in \mathbb{Z} \right\},$$

where (a, b) is one such pair such that $ad - bc = 1$. Thus for $\gamma \in \left\{ \left(\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) : k \in \mathbb{Z} \right\}$, the intersection $\gamma(V_1) \cap V_2 = \left(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)V_1 + k\right) \cap V_2 = \emptyset$ for all but finitely many k; that is, for finitely many γ. So of the finitely many pairs of integers (c, d) for which (0.3) does not hold, only finitely many matrices $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with bottom row (c, d) exist with $\gamma(V_1) \cap V_2 \neq \emptyset$.

Let $F = \{\gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma(V_1) \cap V_2 \neq \emptyset, \gamma(z_1) \neq z_2\}$, which is finite by the above argument. For each $\gamma \in F$ there exist disjoint neighborhoods $V_{1,\gamma}$ of $\gamma(z_1)$ and $V_{2,\gamma}$ of z_2 in $\mathcal{H}$. Let

$$U_1 = V_1 \cap \left(\bigcap_{\gamma\in F} \gamma^{-1}(V_{1,\gamma}) \right) \quad \text{and} \quad U_2 = V_2 \cap \left(\bigcap_{\gamma\in F} V_{2,\gamma} \right),$$

and note that U_1, U_2 are open, as elements of $\mathrm{SL}_2(\mathbb{Z})$ are open maps on $\mathcal{H}$ by Lemma 0.11. Then take any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma(U_1) \cap U_2 \neq \emptyset$. If $\gamma \notin F$, then we must have $\gamma(z_1) = z_2$. Suppose that $\gamma \in F$. Then $U_1 \subset \gamma^{-1}(U_{1,\gamma})$ and $U_2 \subset U_{2,\gamma}$ so that $\gamma(U_1) \cap U_2 \subset U_{1,\gamma} \cap U_{2,\gamma}$. But $\gamma(U_1) \cap U_2 \neq \emptyset$, which is in contradiction with $U_{1,\gamma}$ and $U_{2,\gamma}$ chosen to be disjoint. Hence $\gamma \notin F$, so that $\gamma(z_1) = z_2$. ☐

The equality

$$\begin{aligned} \emptyset = \pi^{-1}(\pi(U_1) \cap \pi(U_2)) &= \left(\bigcup_{\gamma\in\Gamma} \gamma(U_1) \right) \cap \left(\bigcup_{\gamma\in\Gamma} \gamma(U_2) \right) = \bigcup_{\gamma,\eta\in\Gamma} \gamma(U_1) \cap \eta(U_2) \\ &= \bigcup_{\eta\in\Gamma} \eta \left[\left(\bigcup_{\gamma\in\Gamma} (\eta^{-1}\gamma)(U_1) \right) \cap U_2 \right] = \bigcup_{\eta\in\Gamma} \eta \left[\left(\bigcup_{\gamma'\in\Gamma} \gamma'(U_1) \right) \cap U_2 \right] \end{aligned} \tag{0.4}$$

implies that $\left(\bigcup_{\gamma'\in\Gamma} \gamma'(U_1)\right) \cap U_2$ must be empty, which proves the following: $\pi(U_1) \cap \pi(U_2) = \emptyset$ in $Y(\Gamma)$ is equivalent to $\left(\bigcup_{\gamma\in\Gamma} \gamma(U_1)\right) \cap U_2 = \emptyset$ in $\mathcal{H}$.

Proposition 0.13. *The space $Y(\Gamma)$ is second-countable, connected, and Hausdorff.*

Proof. Since π is open and $\mathcal{H}$ is second-countable, $Y(\Gamma)$ is second-countable. As $\mathcal{H}$ is connected and π is continuous, $Y(\Gamma)$ is connected.

Let $\pi(z_1)$ and $\pi(z_2)$ be distinct points in $Y(\Gamma)$ (so that $\gamma(z_1) \neq z_2$ for any $\gamma \in \Gamma$), and take neighborhoods U_1 of z_1 and U_2 of z_2 such that for any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, if $\gamma(U_1) \cap U_2 \neq \emptyset$, then $\gamma(z_1) = z_2$, as per the previous result. Then $\left(\bigcap_{\gamma\in\Gamma} \gamma(U_1)\right) \cap U_2 = \emptyset$ since $\gamma(z_1) \neq z_2$ for every $\gamma \in \Gamma$. From the discussion surrounding (0.4), we have that $\pi(U_1) \cap \pi(U_2) = \emptyset$ as needed, with $\pi(U_1), \pi(U_2)$ open since π is an open mapping. ☐

What remains is to compactify $Y(\Gamma)$ and to put charts on the resulting compact space, which we do without verifying the details.

The group $\mathrm{GL}_2^+(\mathbb{Q}) = \{\gamma \in \mathrm{GL}_2(\mathbb{Q}) : \det \gamma > 0\}$ acts on $\mathbb{Q} \cup \{\infty\}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \left(\frac{r}{s}\right) = \frac{ar + bs}{cr + ds},$$

taking ∞ to a/c and $-d/c$ to ∞ when $c \neq 0$, and taking ∞ to ∞ when $c = 0$. Since $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is invertible, the action above never produces indeterminate forms like $0/0$. Furthermore, $\mathrm{SL}_2(\mathbb{Z})$ acts transitively: Any rational number is of the form a/c, where a and c are coprime. Choose b, d so that $ad - bc = 1$, from which we have $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(\infty) = a/c$.

Let $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$ and define the ***compactified modular curve*** $X(\Gamma)$ as a set by

$$X(\Gamma) = \Gamma \backslash \mathcal{H}^* = Y(\Gamma) \cup \Gamma \backslash (\mathbb{Q} \cup \{\infty\}).$$

Call the points $\Gamma s \in \Gamma \backslash (\mathbb{Q} \cup \{\infty\})$ ***cusps*** of $X(\Gamma)$ (or of Γ). Denote by $X_0(N)$, $X_1(N)$, and $X(N)$ the modular curves $X(\Gamma_0(N))$, $X(\Gamma_1(N))$, and $X(\Gamma(N))$ respectively.

Lemma 0.14. *The modular curve $X(\Gamma)$ has finitely many cusps for any congruence subgroup Γ.*

Proof. The number of cusps of $X(\Gamma)$ is equal to the index of Γ in $\mathrm{SL}_2(\mathbb{Z})$. Let $\mathrm{SL}_2(\mathbb{Z})$ act on $\Gamma \backslash (\mathbb{Q} \cup \{\infty\})$ by $\gamma(\Gamma s) = \Gamma(\gamma s)$. The action is well defined: If $\Gamma s = \Gamma t$, then $s = \gamma' t$ for some $\gamma' \in \Gamma$. Then $\Gamma \gamma \gamma' s = \Gamma \gamma'' \gamma s = \Gamma s$ for some $\gamma'' \in \Gamma$. This group action is transitive since $\mathrm{SL}_2(\mathbb{Z})$ acts transitively on $\mathbb{Q} \cup \{\infty\}$, and the isotropy group of $\Gamma \backslash (\mathbb{Q} \cup \{\infty\})$ is Γ. Thus $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma] = |\Gamma \backslash (\mathbb{Q} \cup \{\infty\})|$. □

It follows that the modular curve $X(1) = \mathrm{SL}_2(\mathbb{Z}) \backslash \mathcal{H}^*$ has one cusp, namely, ∞.

A base for the topology of $\mathcal{H}^*$ consists of open disks centered at elements of $\mathcal{H}$ and the neighborhoods

$$\alpha(\{z \in \mathcal{H} : \mathrm{Im}(z) > M\} \cup \{\infty\}) \quad \text{for } M > 0, \alpha \in \mathrm{SL}_2(\mathbb{Z}),$$

images of disks centered at ∞ under elements of $\mathrm{SL}_2(\mathbb{Z})$. Give $\mathcal{H}$ the topology these sets generate. As fractional linear transformations are conformal maps, for elements $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ with $\gamma(\infty) \in \mathbb{Q}$, a disk centered at ∞ is mapped to a disk that is tangent to the real axis, containing one rational number.

Choosing this base ensures that $X(\Gamma)$ is Hausdorff (whereas taking open disks at each point in $\mathbb{Q} \cup \{\infty\}$ would not since $\mathbb{Q}$ is dense in the real line). Furthermore, every $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is a homeomorphism of $\mathcal{H}^*$ with itself. Give $X(\Gamma)$ the quotient topology with the quotient map $\pi \colon \mathcal{H}^* \to X(\Gamma)$ defined by extending the natural projection.

Proposition 0.15. *The modular curve $X(\Gamma)$ is Hausdorff, connected, and compact.*

Proof. See [DS05, Proposition 2.4.2]. □

Before defining charts on $X(\Gamma)$, we collect some results about elliptic points.

Definition 0.16. Let Γ be a congruence subgroup. For $z \in \mathcal{H}$ let $\Gamma_z = \{\gamma \in \Gamma : \gamma(z) = z\}$, the isotropy subgroup of z. Call $z \in \mathcal{H}$ (and the corresponding point $\pi(z) \in X(\Gamma)$) an ***elliptic point*** of Γ if Γ_z is nontrivial; that is, if the containment $\{\pm I\} \subset \{\pm I\}\Gamma_z$ is proper. †

Proposition 0.17. *Let Γ be a congruence subgroup. Then $X(\Gamma)$ has finitely many elliptic points, and for each elliptic point z of Γ, its isotropy subgroup Γ_z is finite cyclic.*

Proof. See [DS05, Proposition 2.3.3, Corollaries 2.3.4, 2.3.5]. □

It follows that every point $z \in \mathcal{H}$ has an associated positive integer

$$h_z = |\{\pm I\}\Gamma_z / \{\pm I\}| = \begin{cases} |\Gamma_z|/2 & \text{if } -I \in \Gamma_z \\ |\Gamma_z| & \text{if } -I \notin \Gamma_z \end{cases}$$

called the period of z. Note that $h_z > 1$ when z is an elliptic point, and that for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the period of $\gamma(z)$ under $\gamma\Gamma\gamma^{-1}$ is the same as the period of z under Γ. As a result, $h_z = h_{\gamma z}$ for all $\gamma \in \Gamma$, so that the period of $\Gamma z \in Y(\Gamma) \subset X(\Gamma)$ is well defined.

We now define charts for $X(\Gamma)$, starting by defining them on $Y(\Gamma)$. Since $\mathrm{SL}_2(\mathbb{Z})$ acts properly discontinuously on $\mathcal{H}$, we have the following:

Corollary 0.18 (to Proposition 0.12)**.** *Let Γ be a congruence subgroup. Then each point $z \in \mathcal{H}$ is contained in a neighborhood $U \subset \mathcal{H}$ such that for all $\gamma \in \Gamma$, if $\gamma(U) \cap U \neq \emptyset$ then $\gamma \in \Gamma_z$. Furthermore, U has no elliptic points except possibly z.*

Given a point $\pi(z) \in Y(\Gamma)$, take a neighborhood U for z as in the corollary above. Let $\delta_z = \left(\begin{smallmatrix} 1 & -z \\ 1 & -\overline{z} \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{C})$ be the map from $\mathcal{H}$ (or U by restriction) to $\mathbb{C}$ which takes z to 0 and $\overline{z}$ to ∞. Note that the isotropy subgroup of 0 in the transformation group $(\delta_z \{\pm I\} \Gamma \delta_z^{-1})_0 / \{\pm I\}$ is the conjugate $\delta_z(\{\pm I\} \Gamma / \{\pm I\})\delta_z^{-1}$ of the isotropy subgroup of z, hence is cyclic of order h_z as a group of transformations by Proposition 0.17 (note h_z may be equal to 1). Since this group of fractional linear transformations fixes 0 and ∞, these maps are given by $w \mapsto aw$, which are rotations about the origin through angular multiples of $2\pi/h_z$. We call δ_z a "straightening map" since it takes neighborhoods of z to neighborhoods of the origin for which equivalent points are evenly spaced apart angularly. (See [DS05, Figures 2.1, 2.2].)

Let $\rho\colon \mathbb{C} \to \mathbb{C}$ be given by $\rho(w) = w^{h_z}$. Then $\psi = \rho \circ \delta_z \colon U \to V = \psi(U)$ given by $\psi(w) = (\delta(w))^{h_z}$ straightens then "wraps" around the neighborhood into a disk. By the open mapping theorem V is an open subset of $\mathbb{C}$. There exists an bijection $\varphi\colon \pi(U) \to V$ such that $\varphi \circ \pi = \psi$ (see [DS05, Section 2.2]), which is a homeomorphism as well. The maps φ and open sets U for each z are indeed charts for $Y(\Gamma)$.

For neighborhoods containing points in $\mathbb{Q} \cup \{\infty\}$, we specify charts as follows. Let $s \in \mathbb{Q} \cup \{\infty\}$ be a cusp. There exists some $\delta_s \in \mathrm{SL}_2(\mathbb{Z})$ that maps s to ∞. We define the width of s to be

$$h_s = \left|\mathrm{SL}_2(\mathbb{Z})_\infty / (\delta_s \{\pm I\} \Gamma \delta_s^{-1})_\infty\right|.$$

Where the period of an elliptic point is the number of sectors of the disk containing the point that are identified under isotropy, the width of a cusp is the number of sectors (of the infinitely many that come together to s) that are distinct under isotropy (see [DS05, Figure 2.6]). The width of s is finite and independent of the choice of δ_s, and similarly to elliptic points, for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, the width of $\gamma(s)$ under $\gamma\Gamma\gamma^{-1}$ is the same as the width of s under Γ. Thus h_s is the same for all the cusps in Γs, making the width well defined on $X(\Gamma)$.

Let $U = \delta_s^{-1}(\{z \in \mathcal{H} : \mathrm{Im}(z) > 2\} \cup \{\infty\})$ and let $\psi = \rho \circ \delta_s$ where $\rho\colon \mathbb{C} \to \mathbb{C}$ is given by $\rho(z) = e^{2\pi i z/h_s}$. With $V = \psi(U)$ (an open subset of $\mathbb{C}$), obtain $\psi\colon U \to V$ with $\psi(z) = e^{2\pi i \delta_s(z)/h_s}$. The effect of ψ is to straighten U by making identified points differ by a constant, and the exponential map wraps the upper half plane into a disk centered at 0 (where ∞ maps to). Similarly, there exists a homeomorphism $\varphi\colon \pi(U) \to V$ such that $\varphi \circ \pi = \psi$ that gives the chart as desired. Hence the maps ϕ and open sets U for each s give charts on the rest of $X(\Gamma)$.

We briefly define fundamental domains obtained from $X(\Gamma)$, without proofs of claims. We first consider the case $\Gamma = \mathrm{SL}_2(\mathbb{Z})$. Consider the set $\mathcal{D} = \{z \in \mathcal{H} : |\mathrm{Re}(z)| \leq 1/2, |z| \geq 1\}$. The map $\pi\colon \mathcal{D} \to Y(1) = Y(\mathrm{SL}_2(\mathbb{Z}))$ given by the natural projection $z \mapsto \mathrm{SL}_2(\mathbb{Z})z$ is a surjection, and is not injective since the boundary half lines where $\mathrm{Re}(z) = \pm 1/2$ are identified by the translation $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ which takes z to $z+1$ (similarly, the two halves of the boundary arc where $|z| = 1$ are identified by the inversion $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ taking z to $-1/z$). (See [DS05, Section 2.3]) In fact, if two distinct points in $\mathcal{D}$ are $\mathrm{SL}_2(\mathbb{Z})$-equivalent, then the points lie on the boundary of $\mathcal{D}$ and are either translates or inverses of each other by the aforementioned maps. So by a suitable identification of points on the boundary of $\mathcal{D}$ the map π can be made a bijection. We say that $\mathcal{D}$ is a ***fundamental domain*** for $\mathcal{H}$ under the action of $\mathrm{SL}_2(\mathbb{Z})$. A similar procedure may be done for $\mathcal{D}^* = \mathcal{D} \cup \{\infty\}$ and $X(1) = X(\mathrm{SL}_2(\mathbb{Z}))$, by which $\mathcal{D}^*$ becomes a fundamental domain for $\mathcal{H}^*$ under the action of $\mathrm{SL}_2(\mathbb{Z})$.

For other congruence subgroups Γ, write $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_j \{\pm I\} \Gamma \gamma_j$ for some set of representatives γ_j of the coset space $\Gamma \backslash \mathrm{SL}_2(\mathbb{Z})$, and consider the surjection $\pi\colon \bigcup_j \gamma_j \mathcal{D} \to Y(\Gamma)$ given by $z \mapsto \Gamma z$. By identifying the appropriate boundary points of $\bigcup_j \gamma_j \mathcal{D}$, π may be regarded as a bijection, and so $\bigcup_j \gamma_j \mathcal{D}$ becomes a fundamental domain for $\mathcal{H}$ under the action of Γ. A similar procedure for $X(\Gamma)$ produces fundamental domains of $\mathcal{H}^*$ under the action of Γ.

1 Modular forms

In this section, we define modular forms and discuss the growth of their Fourier coefficients. Then we provide dimension formulas for various spaces of modular forms as well as definitions of Eisenstein series as examples of modular forms. We conclude by discussing Dirichlet characters and L-functions corresponding to modular forms.

1.1 Definitions

Definition 1.1. For an integer k and a congruence subgroup Γ, a meromorphic function $f\colon \mathcal{H} \to \mathbb{C}$ is ***weakly modular of weight*** k (with respect to Γ) if

$$f(\gamma(z)) = (cz+d)^k f(z) \quad \text{for any} \quad \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,\ z \in \mathcal{H}. \qquad \dagger$$

Sometimes we will say that a meromorphic function $f\colon \mathcal{H} \to \mathcal{C}$ is just "weakly modular" if the weight k and congruence subgroup Γ are irrelevant or clear from context.

Definition 1.2. For any matrix $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{R})$ the ***factor of automorphy*** $j(\gamma, z)$ for $z \in \mathbb{C}$ is defined by

$$j(\gamma, z) = cz + d.$$

For any integer k and $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$ define the ***weight-k γ operator*** $|_k[\gamma]$ on functions $f\colon \mathcal{H} \to \mathbb{C}$ by

$$(f|_k[\gamma])(z) = (\det\gamma)^{k/2} j(\gamma, z)^{-k} f(\gamma(z)), \quad \text{for } z \in \mathcal{H}. \qquad \dagger$$

Note that $|_k[\gamma]$ composes left to right with other weight-k operators. Since the factor of automorphy $j(\gamma, z) = cz + d$ cannot be zero or infinity (as $z \in \mathcal{H}$), if f is meromorphic on $\mathcal{H}$, then so is $f|_k[\gamma]$, and the number of poles and zeroes of $f|_k[\gamma]$ and f are the same.

So for an integer k and a congruence subgroup Γ, a meromorphic function $f\colon \mathcal{H} \to \mathbb{C}$ is weakly modular of weight k (with respect to Γ) if

$$f|_k[\gamma] = f \quad \text{for all } \gamma \in \Gamma,$$

and this is equivalent to the original definition above. Note that if f is weakly modular with respect to Γ, then the zeroes of f and poles of f are Γ-invariant sets.

Lemma 1.3. *For any $\gamma, \eta \in \mathrm{GL}_2^+(\mathbb{R})$ and $z \in \mathcal{H}$, we have $j(\gamma\eta, z) = j(\gamma, \eta(z)) j(\eta, z)$. For any function $f\colon \mathcal{H} \to \mathbb{C}$, we have $f|_k[\gamma\eta] = (f|_k[\gamma])|_k[\eta]$.*

Proof. Elements of $\mathrm{GL}_2^+(\mathbb{Q})$ act on column vectors in $\mathbb{C}^2$ by matrix multiplication, and act on points in $\mathbb{C}$ by fractional linear transformations. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2^+(\mathbb{Q})$ and observe that for $z \in \mathbb{C}$ we have

$$\gamma \begin{pmatrix} z \\ 1 \end{pmatrix} = \begin{pmatrix} az+b \\ cz+d \end{pmatrix} = \begin{pmatrix} \gamma(z) \\ 1 \end{pmatrix} j(\gamma, z).$$

Then for $\eta \in \mathrm{SL}_2(\mathbb{Z})$ we have

$$\begin{aligned} \gamma\eta \begin{pmatrix} z \\ 1 \end{pmatrix} &= \begin{pmatrix} (\gamma\eta)(z) \\ 1 \end{pmatrix} j(\gamma\eta, z) \quad \text{and} \\ \gamma\eta \begin{pmatrix} z \\ 1 \end{pmatrix} &= \gamma \begin{pmatrix} \eta(z) \\ 1 \end{pmatrix} j(\eta, z) = \begin{pmatrix} \gamma(\eta(z)) \\ 1 \end{pmatrix} j(\gamma, \eta(z)) j(\eta, z). \end{aligned}$$

It follows that $j(\gamma\eta, z) = j(\gamma, \eta(z)) j(\eta, z)$. Then for $f\colon \mathcal{H} \to \mathbb{C}$,

$$\begin{aligned} (f|_k[\gamma\eta])(z) &= (\det(\gamma\eta))^{k/2} j(\gamma\eta, z)^{-k} f((\gamma\eta)(z)) \\ &= (\det\eta)^{k/2} j(\eta, z)^{-k} (\det\gamma)^{k/2} j(\gamma, \eta(z))^{-k} f(\gamma(\eta(z))) \\ &= (\det\eta)^{k/2} j(\eta, z)^{-k} (f|_k[\gamma])(\eta(z)) \\ &= ((f|_k[\gamma])|_k[\eta])(z). \end{aligned}$$

□

From the lemma it follows that if $f\colon \mathcal{H} \to \mathbb{C}$ is weakly modular with respect to some set of matrices A, then f is weakly modular with respect to the group generated by A. So with $\mathrm{SL}_2(\mathbb{Z}) = \left\langle \left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right), \left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)\right\rangle$, a function $f\colon \mathcal{H} \to \mathbb{C}$ is weakly modular of weight k with respect to $\mathrm{SL}_2(\mathbb{Z})$ if

$$(1.1) \qquad f(z+1) = f\left(\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)z\right) = (0z+1)^k f(z) = f(z) \quad \text{and} \quad f(-1/z) = f\left(\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)z\right) = z^k f(z).$$

It follows that weakly modular functions of weight k with respect to $\mathrm{SL}_2(\mathbb{Z})$ are $\mathbb{Z}$-periodic. A similar phenomenon happens for weakly modular functions of weight k with respect to congruence subgroups. If Γ is a congruence subgroup of level N, then $\Gamma(N) \subset \Gamma$, so that Γ contains a translation matrix of the form $\left(\begin{smallmatrix}1&h\\0&1\end{smallmatrix}\right)$ for some minimal positive integer h dividing N. To see that h necessarily divides N, observe that if

$$\begin{pmatrix}1 & b_1\\ 0 & 1\end{pmatrix}, \begin{pmatrix}1 & b_2\\ 0 & 1\end{pmatrix} \in \Gamma, \quad \text{then} \quad \begin{pmatrix}1 & \gcd(b_1,b_2)\\ 0 & 1\end{pmatrix} \in \Gamma.$$

By a similar computation to (1.1), it follows that weakly modular functions with respect to Γ are $h\mathbb{Z}$-periodic. Weakly modular functions with respect to $\Gamma(N)$ are $N\mathbb{Z}$-periodic, and weakly modular functions with respect to $\Gamma_1(N)$ are $\mathbb{Z}$-periodic.

Let $D = \{q \in \mathbb{C} : |q| < 1\}$ be the open unit disk in $\mathbb{C}$ and let $D' = D\backslash\{0\}$ denote the punctured open unit disk in $\mathbb{C}$. The exponential map $z \mapsto e^{2\pi i z/h} = q$ is a $h\mathbb{Z}$-periodic holomorphic map which maps $\mathcal{H}$ to D'. Since f is $h\mathbb{Z}$-periodic, it follows that the function $\tilde{f}\colon D' \to \mathbb{C}$ corresponding to f defined by $\tilde{f}(q) = f(h\log(q)/2\pi i)$ (so $f(z) = \tilde{f}(e^{2\pi i z/h})$) is well defined because a branch of the logarithm is determined up to integral multiples of $2\pi i$.

The logarithm can be defined holomorphically about each $q \in D'$. It follows that $\tilde{f}$ is meromorphic on D' since f is meromorphic on $\mathcal{H}$, and so $\tilde{f}$ has a Laurent expansion $\tilde{f}(q) = \sum_{n\in\mathbb{Z}} a_n q^n$ at each q in a punctured neighborhood of $q = 0$ (and $a_n = 0$ for all n sufficiently small). Moreover, if f is holomorphic on $\mathcal{H}$, it follows that $\tilde{f}$ is also holomorphic on D'.

From $|q| = e^{-2\pi \operatorname{Im} z/h}$, it follows that q tends to zero as $\operatorname{Im} z$ tends to infinity. We define f to be meromorphic (respectively holomorphic) at ∞ if $\tilde{f}$ has a meromorphic (respectively holomorphic) extension to $q = 0$. The Laurent series of $\tilde{f}$ about $q = 0$ is used to obtain a Fourier series expansion of f about ∞, given by

$$f(z) = \sum_{n\in\mathbb{Z}} a_n q^n, \quad q = e^{2\pi i z/h},$$

which converges absolutely and uniformly on compact subsets of the half plane $\{z \in \mathbb{Z} : \operatorname{Im} z > \tau\}$ for some large enough τ (so that q lies in a punctured neighborhood of zero). When referring to a Fourier series of a $h\mathbb{Z}$-periodic meromorphic function on $\mathcal{H}$, we mean the expansion obtained in the above manner. If f is holomorphic on $\mathcal{H}$ and is holomorphic at ∞, the Fourier series expansion becomes $f(z) = \sum_{n=0}^{\infty} a_n q^n$, $q = e^{2\pi i z/h}$, valid for $z \in \mathcal{H}$. To see that a weakly modular holomorphic function $f\colon \mathcal{H} \to \mathbb{C}$ is holomorphic at ∞, it suffices to show that $\lim_{\operatorname{Im} z\to\infty} f(z)$ exists or that $f(z)$ is bounded as $\operatorname{Im} z$ grows unboundedly.

Definition 1.4. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and let k be an integer. A function $f\colon \mathcal{H} \to \mathbb{C}$ is a ***modular form of weight*** k (with respect to Γ) if it satisfies the following:

(1) f is holomorphic on $\mathcal{H}$,

(2) f is weakly modular of weight k with respect to Γ, and

(3) $f|_k[\alpha]$ is holomorphic at ∞ for all $\alpha \in \mathrm{SL}_2(\mathbb{Z})$.

Furthermore, if for every $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, the coefficient a_0 vanishes in the Fourier series expansion of $f|_k[\alpha]$, then we call f a ***cusp form of weight*** k (with respect to Γ). The set of modular forms (respectively cusp forms) of weight k with respect to Γ is denoted by $\mathcal{M}_k(\Gamma)$ (respectively $\mathcal{S}_k(\Gamma)$).

Define also the ***weight*** k ***Eisenstein space*** (of Γ) by the quotient of the space of modular forms by the space of cusp forms; that is, $\mathcal{E}_k(\Gamma) = \mathcal{M}_k(\Gamma)/\mathcal{S}_k(\Gamma)$. It can be shown that the Eisenstein space may be obtained as a complement of $\mathcal{S}_k(\Gamma)$ in $\mathcal{M}_k(\Gamma)$ under the Petersson inner product (we define the Petersson inner product in Section 2.3, but do not prove this result). We briefly discuss the Eisenstein space at the end of Section 1.2. †

Later on, for example in Section 3.2, we specify the congruence subgroup that a modular form is with respect to by its level; that is, we say that a modular form with respect to Γ is "at level N" if Γ is of level N.

Recall that the Γ-equivalence classes of points in $\mathbb{Q} \cup \infty$ are the cusps of Γ. There are finitely many cusps, at most the index of Γ in $\mathrm{SL}_2(\mathbb{Z})$, which we showed was finite in the discussion following Definition 0.5. Write a cusp s as $\alpha(\infty)$ for some $\alpha \in \mathrm{SL}_2(\mathbb{Z})$. We say that f is holomorphic at s $f|_k[\alpha]$ is holomorphic at ∞, where $f|_k[\alpha]$ is viewed as a modular form of weight k with respect to $\alpha^{-1}\Gamma\alpha$. In view of this definition, condition (3) of Definition 1.4 says that f must be holomorphic at the cusps of Γ. The group $\alpha^{-1}\Gamma\alpha$ is a congruence subgroup since for some $N > 0$, the principal congruence subgroup $\Gamma(N)$ is contained in Γ and is normal in $\mathrm{SL}_2(\mathbb{Z})$, so that $\Gamma(N) = \alpha^{-1}\Gamma(N)\alpha \subset \alpha^{-1}\Gamma\alpha$.

As congruence subgroups have finite index in $\mathrm{SL}_2(\mathbb{Z})$, only finitely many coset representatives α_j in a decomposition $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_j \Gamma\alpha_j$ are needed to verify condition (3) in the definition above, and in verifying that the term a_0 vanishes for all Fourier series expansions for cusp forms: we have by condition (2) of the above definition that $f|_k[\gamma\alpha_j] = f|_k[\alpha_j]$ for all $\gamma \in \Gamma$.

Lemma 1.5. (a) *For any $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$, there exists $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, $r \in \mathbb{Q}^+$, and $a, b, d \in \mathbb{Z}$ relatively prime such that $\gamma = r\alpha\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$.*

It follows that for $f \in \mathcal{M}_k(\Gamma)$ and γ with $\gamma = r\alpha\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$, since $f|_k[\alpha]$ has a Fourier expansion, so does $f|_k[\gamma]$. Moreover, if the constant term in the Fourier expansion for $f|_k[\alpha]$ is 0, the same holds for the Fourier expansion for $f|_k[\gamma]$.

(b) *Let Γ_1, Γ_2 be congruence subgroups with $\gamma\Gamma_2\gamma^{-1} \subset \Gamma_1$ for some $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$. If $f \in \mathcal{M}_k(\Gamma_1)$, then $f|_k[\gamma] \in \mathcal{M}_k(\Gamma_2)$, and the same result holds for cusp forms.*

Proof. Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be an element of $\mathrm{GL}_2^+(\mathbb{Q})$. If $c = 0$, there is nothing to show. So assume that $c \neq 0$. Then write $a/c = a'/c'$ with a' and c' coprime integers; that is, write a/c in lowest terms. Then choose integers s, t such that $sa' + tc' = 1$, from which it follows that $\left(\begin{smallmatrix} s & t \\ -c' & a' \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$. We have

$$\begin{pmatrix} s & t \\ -c' & a' \end{pmatrix}\gamma = c\begin{pmatrix} s & t \\ -c' & a' \end{pmatrix}\begin{pmatrix} a'/c' & b/c \\ 1 & d/c \end{pmatrix} = \begin{pmatrix} sa + tc & sb + tc \\ 0 & a'd - c'b \end{pmatrix} = A$$

There exists an integer $r > 0$ such that $rA \in \mathrm{M}_2(\mathbb{Z})$, from which we can divide through by the greatest common divisor g of the (three) nonzero entries of rA to find that the nonzero entries of $\frac{r}{g}A$ are coprime to each other. Rearranging, we obtain $\gamma = \frac{g}{r}\left(\begin{smallmatrix} s & t \\ -c' & a' \end{smallmatrix}\right)^{-1}\left(\frac{r}{g}A\right)$, which proves the first part of (a).

To see the second part of (a), observe that if $\gamma = r\alpha\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)$, then $f|_k[\gamma] = f|_k[r\alpha\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)] = (f|_k[\alpha])|_k[\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)]$. Since f is a modular form, $f|_k[\alpha]$ is holomorphic at ∞ and hence admits a Fourier series expansion of the form $(f|_k[\alpha])(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z/h}$ for some positive integer h. Thus the Fourier series expansion for $(f|_k[\alpha])|_k[\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)]$ is of the form $(f|_k[\alpha\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right)])(z) = \sum_{n=0}^{\infty} b_n e^{2\pi i a z/dh}$. Observe that b_0 is proportional to a_0.

Part (b) is clear from the following observation. For any $\alpha \in \mathrm{SL}_2(\mathbb{Z})$ we have that $\gamma\alpha\gamma^{-1} \in \mathrm{SL}_2(\mathbb{Z})$ and

$$(f|_k[\gamma])|_k[\alpha] = (f|_k[\gamma\alpha\gamma^{-1}])|_k[\gamma].$$

If $\alpha \in \Gamma_2$, then $\gamma\alpha\gamma^{-1} \in \Gamma_1$ so that $(f|_k[\gamma\alpha\gamma^{-1}])|_k[\gamma] = f|_k[\gamma]$. From part (a) deduce the holomorphicity of $(f|_k[\gamma\alpha\gamma^{-1}])|_k[\gamma]$ for any $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, and that the result in part (b) is true for cusp forms. □

It is possible to determine if a weakly modular holomorphic function on $\mathcal{H}$ is a modular form by investigating the growth of its Fourier coefficients. First, we prove a few lemmas.

Lemma 1.6. *If x is a cusp of a congruence subgroup Γ and $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ sends x to ∞, then*

$$\sigma\Gamma_x\sigma^{-1} \cdot \{\pm I\} = \left\{ \pm \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m : m \in \mathbb{Z} \right\}$$

for some integer $h > 0$.

Proof. Without loss of generality take $x = \infty$ by taking $\sigma\Gamma\sigma^{-1}$ in place of Γ. By a computation, we have

$$\Gamma_\infty \subset \left\{ \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}$$

We obtain the result by observing that $\left\{ \pm \left(\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right) : b \in \mathbb{Z} \right\} / \{\pm I\} \cong \mathbb{Z}$. □

Lemma 1.7. *Let f be a weakly modular holomorphic function on $\mathcal{H}$ of weight k with respect to some congruence subgroup Γ. If there exists a real number v such that $f(z) = O(\mathrm{Im}(z)^{-v})$ as $\mathrm{Im}(z) \to \infty$ uniformly with respect to $\mathrm{Re}(z)$, then f is a modular form of weight k. Moreover, if v may be chosen so that $v < k$, then f is a cusp form.*

Proof. Let x be a cusp of Γ. If $x = \infty$, then we may send it to a rational cusp via an element of Γ since $\Gamma \neq \Gamma_\infty$, and repeat the above argument. So suppose x is rational. Then there exists $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\sigma(x) = \infty$. Let $h > 0$ be an integer satisfying the result of the previous lemma. Then the Fourier series expansion of $f|_k[\sigma^{-1}]$ is

$$(f|_k[\sigma^{-1}])(z) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n z/h},$$

with

$$a_n = \frac{1}{h} \int_{z_0}^{z_0+h} (f|_k[\sigma^{-1}])(z) e^{-2\pi i n z/h} \mathrm{d}z, \quad \text{for any fixed } z_0 \in \mathcal{H}. \tag{1.2}$$

Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \sigma^{-1}$, and note that $c \neq 0$, since σ^{-1} does not fix ∞. We have that $\mathrm{Im}(\sigma^{-1}(z)) = \mathrm{Im}(z)/|cz+d|^2 = O(1/\mathrm{Im}(z))$ as $\mathrm{Im}(z) \to \infty$, uniformly on $|\mathrm{Re}(z)| \leq h/2$. Then by assumption,

$$(f|_k[\sigma^{-1}])(z) = f(\sigma^{-1}(z)) j(\sigma^{-1}, z)^{-k} = O(\mathrm{Im}(z)^{v-k}) \quad (\text{as } \mathrm{Im}(z) \to \infty),$$

uniformly on $|\mathrm{Re}(z)| \leq h/2$. Choosing $z_0 = iy - h/2$ in (1.2), we have that $|a_n| = O(y^{v-k} e^{2\pi n y/h})$ as $y \to \infty$.

So if $n < 0$, then $a_n = 0$; moreover, if $v < k$, then $a_0 = 0$. It follows that f is holomorphic at all cusps of Γ, and has a zero at any cusp if $v < k$. □

Lemma 1.8. *Let $\{a_n\}_{n=0}^{\infty}$ be a sequence of complex numbers, and let $f \colon \mathcal{H} \to \mathbb{C}$ be given by $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$. If $a_n = O(n^v)$ for some $v > 0$, then $\sum_{n=0}^{\infty} a_n e^{2\pi i n z}$ is convergent absolutely and uniformly on compact subsets of $\mathcal{H}$. Moreover,*

$$\begin{aligned} f(z) &= O(\mathrm{Im}(z)^{-v-1}) \quad (\mathrm{Im}(z) \to 0), \text{ and} \\ f(z) - a_0 &= O(e^{-2\pi \mathrm{Im}(z)}) \quad (\mathrm{Im}(z) \to \infty), \end{aligned}$$

uniformly on $\mathrm{Re}(z)$.

Proof. From $\Gamma(s) = \lim_{n\to\infty} \frac{n! n^s}{s(s+1)\cdots(s+n)}$ for real $s > 0$ (Euler-Gauss), we have for $v > 0$ that

$$\lim_{n\to\infty} n^v / (-1)^n \binom{-v-1}{n} = \Gamma(v).$$

Thus there exists $L > 0$ such that

$$|a_n| \leq L(-1)^n \binom{-v-1}{n}$$

for all $n \geq 0$. Let $z = x + iy$, so that

$$\begin{aligned} \sum_{n=0}^{\infty} |a_n||e^{2\pi i n z}| &\leq L\left(\sum_{n=0}^{\infty} (-1)^n \binom{-v-1}{n} e^{-2\pi n y} \right) \\ &= L(1 - e^{-2\pi y})^{-v-1}. \end{aligned} \tag{1.3}$$

It follows that f is convergent absolutely and uniformly on compact subsets of $\mathcal{H}$. Since $1 - e^{-2\pi y} = O(y)$ as $y \to 0$, we have that $|f(z)| = O(y^{-v-1})$. Furthermore, (1.3) implies that f is bounded as y tends to ∞.

Let $g\colon \mathcal{H} \to \mathbb{C}$ be given by $g(z) = \sum_{n=0}^{\infty} a_{n+1} e^{2\pi i n z}$, and observe that g also satisfies the hypotheses of the lemma. It follows that g is also bounded on a neighborhood of ∞. Therefore

$$f(z) - a_0 = e^{2\pi i z} g(z) = O(e^{-2\pi y}) \quad (y \to \infty). \qquad \square$$

Combining the previous few lemmas, we obtain the following:

Proposition 1.9. *Let f be a weakly modular holomorphic function on $\mathcal{H}$ with respect to some congruence subgroup Γ. If in a Fourier expansion of f given by $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z/h}$, the coefficients a_n are of order $O(n^v)$ for some $v > 0$, then f is a modular form.*

The following result describes the growth of cusp forms:

Proposition 1.10. *Let f be a weakly modular holomorphic function on $\mathcal{H}$. Then f is a cusp form if and only if $f(z)\operatorname{Im}(z)^{k/2}$ is bounded on $\mathcal{H}$.*

Proof. We may assume that k is even, and observe that Lemma 1.7 provides the 'if' direction of the result. So assume that f is a cusp form and let g be given by $g(z) = |f(z)| \operatorname{Im}(z)^{k/2}$. Since $g(\gamma(z)) = g(z)$ for any $\gamma \in \Gamma$, view g as a continuous function on $Y(\Gamma)$. Since Γ has only finitely many inequivalent cusps, it suffices to show that g is bounded on a neighborhood of a cusp of Γ. Let x be a cusp of Γ, and let $\sigma \in \mathrm{SL}_2(\mathbb{Z})$ take x to ∞. Choose a positive integer h so that $\sigma \Gamma_x \sigma^{-1} \cdot \{\pm I\} = \left\{ \pm \left(\begin{smallmatrix} 1 & h \\ 0 & 1 \end{smallmatrix}\right)^m : m \in \mathbb{Z} \right\}$, and let $(f|_k[\sigma^{-1}])(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z/h}$ be the Fourier expansion of f at x. Then

$$\begin{aligned} g(\sigma^{-1}(z)) &= \left|(f|_k[\sigma^{-1}])(z)\right| \operatorname{Im}(z)^{k/2} \\ &= \left| \sum_{n=1}^{\infty} a_n e^{2\pi i n z/h} \right| \operatorname{Im}(z)^{k/2} \quad (\text{as } \operatorname{Im}(z) \to \infty). \end{aligned}$$

Hence g is bounded on a neighborhood of x. $\square$

Corollary 1.11. *Let f be an element of $\mathcal{S}_k(\Gamma)$, let x be a cusp of Γ, and let σ be an element of $\mathrm{SL}_2(\mathbb{Z})$ that maps x to ∞. Let $(f|_k[\sigma^{-1}])(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z/h}$ be the Fourier expansion of f at x. Then $a_n = O(n^{k/2})$.*

Proof. Let $g = f|_k[\sigma^{-1}]$, so that $g \in \mathcal{S}_k(\sigma\Gamma\sigma^{-1})$. By Proposition 1.10, there exists a constant $M > 0$ such that $|g(z)| \leq M \operatorname{Im}(z)^{-k/2}$. Thus

$$\begin{aligned} |a_n| &= \frac{1}{h} \left| \int_0^h g(x+iy) e^{-2\pi i n (x+iy)/h} \mathrm{d}x \right| \\ &\leq M y^{-k/2} e^{2\pi n y/h}. \end{aligned}$$

By taking $y = 2/n$, it follows that $|a_n| \leq (M e^{4\pi/h} 2^{-k/2}) n^{k/2}$. $\square$

Lastly, we record the dimensions of various spaces of modular forms below, without proof (See [DS05, Chapter 3]). These dimension formulas are obtained via Riemann surface theory. In particular, the Riemann-Roch theorem is used, in combination with the geometric data of $X(\Gamma)$: its genus, number of cusps, number of elliptic points, and more.

Theorem 1.12. *Let k be an even integer and let Γ be a congruence subgroup. Let g be the genus of $X(\Gamma)$, let $\varepsilon_2, \varepsilon_3$ be the number of elliptic points with period 2, 3 respectively, and let ε_∞ be the number of cusps. Then*

$$\dim \mathcal{M}_k(\Gamma) = \begin{cases} (k-1)(g-1) + \lfloor \frac{k}{4} \rfloor \varepsilon_2 + \lfloor \frac{k}{3} \rfloor \varepsilon_3 + \frac{k}{2}\varepsilon_\infty & \text{if } k \geq 2, \\ 1 & \text{if } k = 0, \\ 0 & \text{if } k < 0, \end{cases} \quad \text{and}$$

$$\dim \mathcal{S}_k(\Gamma) = \begin{cases} (k-1)(g-1) + \lfloor \frac{k}{4} \rfloor \varepsilon_2 + \lfloor \frac{k}{3} \rfloor \varepsilon_3 + (\frac{k}{2} - 1)\varepsilon_\infty & \text{if } k \geq 4, \\ g & \text{if } k = 2, \\ 0 & \text{if } k < 0, \end{cases}$$

In particular, the space of modular forms of weight 0, $\mathcal{M}_0(\mathrm{SL}_2(\mathbb{Z}))$, is isomorphic to $\mathbb{C}$ since the genus of $X(1)$ is 0. Furthermore, $\mathcal{M}_2(\mathrm{SL}_2(\mathbb{Z})) = 0$ and $\mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z})) = 0$ for $k = 0, 2$. For any even integer $k \geq 4$, $\mathcal{M}_k(\mathrm{SL}_2(\mathbb{Z})) = \mathcal{S}_k(\mathrm{SL}_2(\mathbb{Z})) \oplus \mathbb{C}E_k$ where E_k is the normalized weight k Eisenstein series, which we will define in Section 1.2, and

$$\dim S_k(\mathrm{SL}_2(\mathbb{Z})) = \begin{cases} \lfloor \frac{k}{12} \rfloor - 1 & \text{if } k \equiv 2 \pmod{12}, \\ \lfloor \frac{k}{12} \rfloor & \text{otherwise.} \end{cases}$$

Theorem 1.13. *Let k be an odd integer and let Γ be a congruence subgroup. If $-I \in \Gamma$, then both $\mathcal{M}_k(\Gamma)$ and $\mathcal{S}_k(\Gamma)$ are zero. Otherwise, let g be the genus of $X(\Gamma)$, ε_3 be the number of elliptic points with period 3, $\varepsilon_\infty^{\mathrm{reg}}, \varepsilon_\infty^{\mathrm{irr}}$ be the number of regular and irregular cusps, respectively (see* [DS05, Section 3.6]*). Then*

$$\dim \mathcal{M}_k(\Gamma) = \begin{cases} (k-1)(g-1) + \lfloor \frac{k}{3} \rfloor \varepsilon_3 + \frac{k}{2}\varepsilon_\infty^{\mathrm{reg}} + \frac{k-1}{2}\varepsilon_\infty^{\mathrm{irr}} & \text{if } k \geq 3, \\ 0 & \text{if } k < 0, \end{cases} \quad \text{and}$$

$$\dim \mathcal{S}_k(\Gamma) = \begin{cases} (k-1)(g-1) + \lfloor \frac{k}{3} \rfloor \varepsilon_3 + (\frac{k}{2} - 1)\varepsilon_\infty^{\mathrm{reg}} + \frac{k-1}{2}\varepsilon_\infty^{\mathrm{irr}} & \text{if } k \geq 3, \\ 0 & \text{if } k < 0. \end{cases}$$

If $\varepsilon_\infty^{\mathrm{reg}} > 2g-2$, then $\dim \mathcal{M}_1(\Gamma) = \varepsilon_\infty^{\mathrm{reg}}/2$ and $\dim \mathcal{S}_1(\Gamma) = 0$. If $\varepsilon_\infty^{\mathrm{reg}} \leq 2g-2$, then $\dim \mathcal{M}_1(\Gamma) \geq \varepsilon_\infty^{\mathrm{reg}}$ and $\dim \mathcal{S}_1(\Gamma) = \dim \mathcal{M}_1(\Gamma) - \varepsilon_\infty^{\mathrm{reg}}/2$.

Dimension formulas for other spaces of modular forms (varying k, N, Γ) may be found in [DS05, Section 3.9].

Let k be an integer and Γ a congruence subgroup. Then the dimensions of the Eisenstein spaces are given by

$$\dim \mathcal{E}_k(\Gamma) = \begin{cases} \varepsilon_\infty & \text{if } k \geq 4 \text{ is even}, \\ \varepsilon_\infty^{\mathrm{reg}} & \text{if } k \geq 3 \text{ is odd and } -I \notin \Gamma, \\ \varepsilon_\infty - 1 & \text{if } k = 2, \\ \varepsilon_\infty^{\mathrm{reg}}/2 & \text{if } k = 1 \text{ and } -I \notin \Gamma, \\ 1 & \text{if } k = 0, \\ 0 & \text{if } k < 0, \text{ or if } k > 0 \text{ is odd and } -I \in \Gamma. \end{cases}$$

1.2 Eisenstein series

We define the Eisenstein series for a number of spaces of modular forms to provide some examples of modular forms. We do not verify any claims in this section.

Elementary Eisenstein series for $\mathrm{SL}_2(\mathbb{Z})$ are defined for even weights $k \geq 4$, by

$$G_k(z) = {\sum_{(c,d)}}' \frac{1}{(cz+d)^k}, \quad z \in \mathcal{H},$$

where the notation $\sum'_{(c,d)}$ denotes summation over all nonzero integer pairs $(c,d) \in \mathbb{Z}^2$. This sum is absolutely convergent, and converges uniformly on compact subsets of $\mathcal{H}$. It follows that G_k is holomorphic on $\mathcal{H}$ and we may rearrange the terms of the sum defining G_k. A Fourier series for G_k is given by

$$G_k(z) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)e^{2\pi i z},$$

where σ_{k-1} is the arithmetic function $\sigma_{k-1}(n) = \sum_{\substack{m|n \\ m>0}} m^{k-1}$. (See [DS05, Section 1.1]) Obtain the normalized Eisenstein series $E_k(z) = G_k(z)/(2\zeta(k))$, which can be shown to be given by

$$E_k(z) = \frac{1}{2}\sum_{\substack{(c,d)\in\mathbb{Z}^2 \\ \gcd(c,d)=1}}\frac{1}{(cz+d)^k} \quad \text{or} \quad E_k(z) = \frac{1}{2}\sum_{\gamma\in P_+\backslash \mathrm{SL}_2(\mathbb{Z})}\frac{1}{j(\gamma,z)^k},$$

where $P_+ = \left\{\left(\begin{smallmatrix}1 & n\\ 0 & 1\end{smallmatrix}\right) : n \in \mathbb{Z}\right\}$ is the positive part of the parabolic subgroup of $\mathrm{SL}_2(\mathbb{Z})$. It is more elegant to verify that the normalized Eisenstein series is weakly modular of weight k using the last equality above.

Let $g_2(z) = 60G_4(z)$ and $g_3(z) = 140G_6(z)$, and define the ***discriminant function*** $\Delta\colon \mathcal{H} \to \mathbb{C}$ by $\Delta(z) = (g_2(z))^3 - 27(g_3(z))^2$. The discriminant function is a nonzero cusp form of weight 12, with Fourier coefficients $a_0 = 0$, $a_1 = (2\pi)^{12}$. In fact, the only zero of Δ is at ∞. It follows that the ***j-invariant*** $j\colon \mathcal{H} \to \mathbb{C}$ given by $j(z) = 1728(g_2(z))^3/\Delta(z)$ is holomorphic on $\mathcal{H}$. The j-invariant is $\mathrm{SL}_2(\mathbb{Z})$-invariant, is a surjection, and has a simple pole at ∞ with residue 1.

We summarize what the Eisenstein series for $\Gamma(N)$ look like for weights $k \geq 3$. Let N be a positive integer and let $\overline{v} \in (\mathbb{Z}/N\mathbb{Z})^2$ be an element of order 2 written as a row vector, where v is some lift of $\overline{v}$ to $\mathbb{Z}^2$ (so $\bar{\cdot}$ denotes reduction modulo N). Let $\delta = \left(\begin{smallmatrix}a & b\\ c_v & d_v\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with (c_v, d_v) a lift of $\overline{v}$ to $\mathbb{Z}^2$, and let $k \geq 3$ be an integer. Lastly, let ϵ_N be $1/2$ if $N = 1, 2$ and 1 otherwise.

Define the Eisenstein series $E_k^{\overline{v}}(z)\colon \mathcal{H} \to \mathbb{C}$ by

$$E_k^{\overline{v}}(z) = \epsilon_N \sum_{\substack{(c,d)\equiv v \pmod{N} \\ \gcd(c,d)=1}}\frac{1}{(cz+d)^k},$$

and it can be shown that

$$E_k^{\overline{v}}(z) = \sum_{\gamma\in(P_+\cap\Gamma(N)\backslash\Gamma(N)\delta)}\frac{1}{j(\gamma,z)^k}.$$

Note that when $N = 1$, we have from this definition that $E_k^{\overline{v}} = E_k$ since there is only one choice of $\overline{v}$.

A computation yields the fact that for $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, $E_k^{\overline{v}}|_k[\gamma] = E_k^{\overline{v\gamma}}$, from which it follows that these series are elements of $\mathcal{M}_k(\Gamma(N))$. By symmetrizing, one can define Eisenstein series for any congruence subgroup Γ by

$$E_{k,\Gamma}^{\overline{v}} = \sum_{\gamma_j\in\Gamma(N)\backslash\Gamma} E_k^{\overline{v}}|_k[\gamma_j],$$

where the γ_j constitute a set of coset representatives for $\Gamma(N)\backslash\Gamma$.

For odd weights k and $N = 1, 2$, the Eisenstein space $\mathcal{E}_k(\Gamma(N))$ has dimension 0, since $-I \in \Gamma(N)$. For k even or for $N > 2$, $E_k^{\overline{v}}$ vanishes at ∞ for all $\overline{v}$ except for $\pm\overline{(0,1)}$. One can show that $E_k^{\overline{(c,d)}}$ is nonvanishing on points in the set $\Gamma(N)(-d/c)$ and vanishes on the other cusps of $\Gamma(N)$. A basis of $\mathcal{E}_k(\Gamma(N))$ may be formed by choosing a set of vectors $\{\overline{v}\} = \{\overline{(c,d)}\}$ for which the quotients $-d/c$ represent the cusps of $\Gamma(N)$; it follows from the previous sentence that $\{E_k^{\overline{v}}\}$ is linearly independent. The number of elements in this set is ε_∞ (for $\Gamma(N)$). Thus for all $k \geq 3$, it is possible to obtain bases for the Eisenstein spaces (recall that for odd weights and $N = 1, 2$ the spaces are zero). The basis elements are given by the reductions modulo $\mathcal{S}_k(\Gamma(N))$ of the modular forms $E_k^{\overline{v}}$, but it is possible to redefine the Eisenstein spaces $\mathcal{E}_k(\Gamma(N))$ as subspaces of $\mathcal{M}_k(\Gamma(N))$ so that the basis elements are the Eisenstein series themselves (see [DS05, Section 5.11]).

In view of the definition of the normalized Eisenstein series for $N = 1$, define for any $\overline{v} \in (\mathbb{Z}/N\mathbb{Z})^2$ of order N

$$G_k^{\overline{v}}(z) = \sum_{(c,d)\equiv v \pmod{N}}{}' \frac{1}{(cz+d)^k}.$$

It can be shown that (see [DS05, Section 4.2])

$$G_k^{\overline{v}}(z) = \frac{1}{\epsilon_N} \sum_{n \in (\mathbb{Z}/N\mathbb{Z})^\times} \zeta_+^n(k) E_k^{n^{-1}\overline{v}}(z),$$

where

$$\zeta_+^n(k) = \sum_{\substack{m=1 \\ m \equiv n \pmod{N}}}^{\infty} \frac{1}{m^k} \quad \text{for } n \in (\mathbb{Z}/N\mathbb{Z})^\times.$$

The Fourier series expansion of $G_k^{\overline{v}}(z)$ for $k \geq 3$ and $\overline{v} \in (\mathbb{Z}/N\mathbb{Z})^2$ of order N is given by

$$G_k^{\overline{v}}(z) = \delta(\overline{c}_v)\zeta^{\overline{d}_v}(k) + \frac{(-2\pi i)^k}{N^k(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}^{\overline{v}}(n) e^{2\pi i n t/N},$$

where

$$\delta(\overline{c}_v) = \begin{cases} 1 & \text{if } \overline{c}_v = \overline{0}, \\ 0 & \text{otherwise,} \end{cases} \qquad \zeta^{\overline{d}_v}(k) = \sum_{d \equiv d_v \pmod{N}}{}' \frac{1}{d^k},$$

and

$$\sigma_{k-1}^{\overline{v}}(n) = \sum_{\substack{m \mid n \\ n/m \equiv c_v \pmod{n}}} \operatorname{sgn}(m) m^{k-1} \mu_N^{d_v m}.$$

In the sum for $\zeta^{\overline{d}_v}(k)$, we sum over positive and negative d, and similarly for m in the sum for $\sigma_{k-1}^{\overline{v}}$. Similarly to the Eisenstein series, one may form a basis $\left\{G_k^{\overline{v}}\right\}$ of the Eisenstein space $\mathcal{E}_k(\Gamma(N))$ (using the same choice of $\{\overline{v}\}$ as before). Since the n-th Fourier coefficient is of the order n^k, it follows from Proposition 1.9 that $E_k^{\overline{v}}$ is a modular form.

1.3 Dirichlet characters and L-functions

For any positive integer N, denote by Z_N the group $\mathbb{Z}/N\mathbb{Z}$.

Definition 1.14. A ***Dirichlet character modulo*** N is a homomorphism

$$\chi\colon Z_N^\times \to \mathbb{C}^\times.$$

(We will sometimes suppress "Dirichlet" when referring to Dirichlet characters.) †

The product of two Dirichlet characters χ, ψ, defined by pointwise multiplication $(\chi\psi)(n) = \chi(n)\psi(n)$ for $n \in Z_N^\times$, is a Dirichlet character. The trivial map is a Dirichlet character, called the trivial character. Hence the set of Dirichlet characters of $Z_N^\times$ forms a group called the ***dual group*** of $Z_N^\times$, denoted $\widehat{Z_N^\times}$. Since $Z_N^\times$ is a finite group, the image of any character lies in the roots of unity. Thus the inverse of a Dirichlet character is its complex conjugate character $\overline{\chi}$, defined by taking the complex conjugate pointwise: $\overline{\chi}(n) = \overline{\chi(n)}$ for $n \in Z_N^\times$, where $\overline{\cdot}$ denotes complex conjugation. Note that the only Dirichlet character of $Z_1^\times$ is the trivial character $\mathbf{1}_1$.

Proposition 1.15. *The dual group $\widehat{Z_N^\times}$ is (noncanonically) isomorphic to $Z_N^\times$; it follows that the number of Dirichlet characters modulo N is $\phi(N)$.*

Proof. This is [DF04, Exercise 5.2.14], which states that finite Abelian groups are (noncanonically) self-dual.

Let $G = \langle x_1\rangle \times \cdots \times \langle x_r\rangle$ be a finite Abelian group (recall the structure theorem for finitely generated Abelian groups). Define characters $\chi_i\colon \langle x_i\rangle \to \mathbb{C}^\times$ by $x_i \mapsto e^{2\pi i/|x_i|}$ for $1 \le i \le r$, which have order $|x_i|$ in $\widehat{\langle x_i\rangle}$. It is evident that the group $G' = \langle \chi_1\rangle \times \cdots \times \langle \chi_r\rangle$ is isomorphic to G.

Define the homomorphism $\rho\colon G' \to \widehat{G}$ by $(\chi_1^{e_1}, \ldots, \chi_r^{e_r}) \mapsto \chi_1^{e_1}\pi_1 \cdots \chi_r^{e_r}\pi_r$, where π_i denotes the projection $G \to \langle x_i\rangle$. It is evident that $\ker\rho$ is trivial. Let $f\colon G \to \mathbb{C}^\times$ be a character of $\widehat{G}$, and let $\iota_i\colon \langle x_i\rangle \to G$ denote the inclusion $x_i \mapsto (1, \ldots, 1, x_i, 1, \ldots, 1)$. Then $f\iota_i \in \widehat{\langle x_i\rangle}$, and a preimage of f under ρ is $(f\iota_1, \ldots, f\iota_r)$. The result follows. □

Proposition 1.16. *The groups $Z_N^\times$ and $\widehat{Z_N^\times}$ satisfy the following orthogonality relations:*

$$\sum_{n\in Z_N^\times} \chi(n) = \begin{cases} \phi(N) & \text{if } \chi = \mathbf{1}, \\ 0 & \text{if } \chi \neq \mathbf{1}, \end{cases} \qquad \sum_{\chi\in \widehat{Z_N^\times}} \chi(n) = \begin{cases} \phi(N) & \text{if } n = 1, \\ 0 & \text{if } n \neq 1. \end{cases} \tag{1.4}$$

Proof. Let χ be a Dirichlet character. If $\chi = \mathbf{1}$, then $\sum_{n\in Z_N^\times} \chi(n) = \phi(N)$. Suppose $\chi \neq \mathbf{1}$, so that there exists $m \in Z_N^\times$ for which $\chi(m) \neq 1$. Then $\sum_{n\in Z_N^\times} \chi(n) = \sum_{n\in Z_N^\times} \chi(mn) = \chi(m)\sum_{n\in Z_N^\times} \chi(n)$, so that $\sum_{n\in Z_N^\times} \chi(n) = 0$.

Similarly, let $n \in Z_N^\times$. If $n = 1$, $\sum_{\chi\in\widehat{Z_N^\times}} \chi(n) = \phi(N)$. If $n \neq 1$, there exists a character η that is not 1 on n, and similarly obtain the equality $\sum_{\chi\in\widehat{Z_N^\times}} \chi(n) = \sum_{\chi\in\widehat{Z_N^\times}} (\eta\chi)(n) = \eta(n)\sum_{\chi\in\widehat{Z_N^\times}} \chi(n)$, from which $\sum_{\chi\in\widehat{Z_N^\times}} \chi(n) = 0$ follows. □

Any Dirichlet character χ modulo d may be lifted to a character χ_N modulo N when $d \mid N$, by the rule $\chi_N(n \pmod N) = \chi(n \pmod d)$ for all $n \in \mathbb{Z}$ coprime to N. In other words, if $\pi_{N,d}\colon Z_N^\times \to Z_d^\times$ is the natural projection, then $\chi_N = \chi \circ \pi_{N,d}$.

However, given positive N, d with $d \mid N$ and χ a character modulo N, it is not always possible to find a character χ_d modulo d such that $\chi = \chi_d \circ \pi_{N,d}$. But for every character modulo N there exists a divisor d of N and a character χ_d modulo d such that $\chi = \chi_d \circ \pi_{N,d}$.

Definition 1.17. The ***conductor*** m_χ of a Dirichlet character χ modulo N is the smallest positive divisor d of N such that there exists a Dirichlet character χ_d modulo d such that $\chi = \chi_d \circ \pi_{N,d}$, equivalently, such that χ is trivial on the normal subgroup

$$\ker(\pi_{N,d}) = \{n \in Z_N^\times : n \equiv 1 \pmod d\}.$$

A Dirichlet character modulo N is called a ***primitive character*** if its conductor is N. †

Note that the only character modulo N with conductor 1 is the trivial character $\mathbf{1}_N$, so that the trivial character $\mathbf{1}_N$ is primitive only for $N = 1$.

Any Dirichlet character χ modulo N extends to a function (abusing notation) $\chi\colon Z_N \to \mathbb{C}$ by the rule $\chi(n) = 0$ for noninvertible elements n of the ring Z_N. Further extend χ to a function $\chi\colon \mathbb{Z} \to \mathbb{C}$ by the rule $\chi(n) = \chi(n \pmod N)$. The resulting map $\chi\colon \mathbb{Z} \to \mathbb{C}$ is a totally multiplicative (set) function; that is, $\chi(nm) = \chi(n)\chi(m)$ for all $n, m \in \mathbb{Z}$.

For example, the extension of the trivial character $\mathbf{1}_N$ to a function on $\mathbb{Z}$ is given by

$$\mathbf{1}_N(n) = \begin{cases} 1 & \text{if } \gcd(n, N) = 1, \\ 0 & \text{if } \gcd(n, N) \neq 1. \end{cases}$$

Also note that the extension of any Dirichlet character χ satisfies

$$\chi(0) = \begin{cases} 1 & \text{if } N = 1, \\ 0 & \text{if } N > 1. \end{cases}$$

Obtain new orthogonality relations from the ones appearing in (1.4) by summing from 0 to $N-1$ in the first orthogonality relation and by taking $n \in \mathbb{Z}$ in the second:

$$\sum_{n=0}^{N-1} \chi(n) = \begin{cases} \phi(N) & \text{if } \chi = \mathbf{1}, \\ 0 & \text{if } \chi \neq \mathbf{1}, \end{cases} \qquad \sum_{\chi \in \widehat{Z_N^\times}} \chi(n) = \begin{cases} \phi(N) & \text{if } n \equiv 1 \pmod{N}, \\ 0 & \text{if } n \not\equiv 1 \pmod{N}. \end{cases} \tag{1.5}$$

Lemma 1.18. *Let N be a positive integer. If $N = 1, 2$, then every Dirichlet character χ modulo N satisfies $\chi(-1) = 1$. If $N > 2$, then the number of Dirichlet characters modulo N is even, of which half satisfy $\chi(-1) = 1$ and the other half satisfy $\chi(-1) = -1$.*

Proof. The extensions of a Dirichlet character to functions on $\mathbb{Z}$ are unique, so it suffices to study Dirichlet characters given by homomorphisms $Z_N^\times \to \mathbb{C}^\times$. For $N = 1, 2$, $\phi(N) = 1$ so that the only Dirichlet character is the trivial one. For $N > 2$, $\phi(N)$ is even, so there are an even number of characters modulo N.

For $N > 2$, the map $\widehat{Z_N^\times} \to Z_2$ given by evaluation at $N-1$ (which corresponds to evaluation at -1) is a nontrivial homomorphism since there exists a character which is not 1 on $N-1$. By the first isomorphism theorem, the result follows. □

Dirichlet characters are used to decompose the vector spaces $\mathcal{M}_k(\Gamma_1(N)), \mathcal{S}_k(\Gamma_1(N)), \mathcal{E}_k(\Gamma_1(N))$ into direct sums of interesting subspaces.

For a character χ, define the character (using the same symbol) $\chi\colon \Gamma_0(N) \to \mathbb{C}^\times$ by $\chi(\gamma) = \chi(d_\gamma)$, where d_γ denotes the lower right entry of $\gamma \in \Gamma_0(N)$. (We can also define χ on any other group of matrices with positive determinant and lower left entry a multiple of N.)

Proposition 1.19. *For each Dirichlet character χ modulo N, define the **χ-eigenspace** of $\mathcal{M}_k(\Gamma_1(N))$ by*

$$\mathcal{M}_k(N, \chi) = \{f \in \mathcal{M}_k(\Gamma_1(N)) : f|_k[\gamma] = \chi(\gamma) f \text{ for all } \gamma \in \Gamma_0(N)\}.$$

Similarly define χ-eigenspaces of $\mathcal{S}_k(\Gamma_1(N))$. Then the following decompositions hold:

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_\chi \mathcal{M}_k(N, \chi), \quad \mathcal{S}_k(\Gamma_1(N)) = \bigoplus_\chi \mathcal{S}_k(N, \chi).$$

We prove this result at the beginning of Section 2.2.

Before defining L-functions for modular forms, we make a few observations. Let Γ be a congruence subgroup, so that by definition there exists a positive integer N such that $\Gamma(N) \subset \Gamma$, from which it follows that $\mathcal{M}_k(\Gamma) \subset \mathcal{M}_k(\Gamma(N))$. Furthermore, $\Gamma_1(N^2)$ is contained in

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma(N) \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N^2},\ a \equiv d \equiv 1 \pmod{N} \right\},$$

from which we have

$$\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(N^2) \subset \Gamma(N) \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}.$$

So if $f \in \mathcal{M}_k(\Gamma(N))$,

$$f(Nz) = f\left(\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right) z\right) = N^{-k/2} \left(f|_k[\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)] \right)(z)$$

and $N^{-k/2} f|_k[\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)] \in \mathcal{M}_k(\Gamma_1(N^2))$. Indeed, $f(Nz)$ is holomorphic on $\mathcal{H}$ since f is holomorphic on $\mathcal{H}$. For $\gamma \in \Gamma_1(N^2)$, $\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)\gamma \in \Gamma(N)\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$ so that

$$N^{-k/2} f|_k[\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)]|_k[\gamma] = N^{-k/2} f|_k[\gamma' \left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)] = N^{-k/2} f|_k[\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)],$$

where γ' is an element of $\Gamma(N)$. Lastly, let $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, and note that $\mathrm{SL}_2(\mathbb{Z})$ is normal in $\mathrm{GL}_2(\mathbb{Z})$ so that $\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)\alpha = \alpha'\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for some $\alpha' \in \mathrm{SL}_2(\mathbb{Z})$. Then

$$N^{-k/2}\Big(f|_k[\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)]|_k[\alpha]\Big)(z) = N^{-k/2}\Big(f|_k[\alpha'\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right)]\Big)(z) = j\big(\alpha'\left(\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right), z\big)^{-k} f(\alpha'(Nz)) = (f|_k[\alpha'])(Nz),$$

which is holomorphic at ∞ since $f \in \mathcal{M}_k(\Gamma(N))$. If the series expansion of f at ∞ is $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z/N}$, we have the Fourier expansion

$$f(Nz) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z},$$

and vice versa. So for the purposes of defining L-functions for modular forms, it suffices to define them for modular forms in $\mathcal{M}_k(\Gamma_1(N))$. We require a few preliminary results about Dirichlet series:

Lemma 1.20. *Assume that both $\sum_{n=1}^{\infty} a_n n^{-s}$ and $\sum_{n=1}^{\infty} b_n n^{-s}$ are absolutely convergent at $s = \sigma_0$ with $\sigma_0 > 0$ real. If $\sum_{n=1}^{\infty} a_n n^{-s} = \sum_{n=1}^{\infty} b_n n^{-s}$ on $\mathrm{Re}(s) \geq \sigma_0$, then $a_n = b_n$ for all n.*

Proof. By taking differences, it suffices to show that if $\sum_{n=1}^{\infty} a_n n^{-s} = 0$, then $a_n = 0$ for all n. Since $\sum_{n=1}^{\infty} a_n n^{-s}$ is absolutely convergent at $s = \sigma_0$, it is absolutely and uniformly convergent on $\mathrm{Re}(s) \geq \sigma_0$. Suppose there exists a smallest integer m such that $a_m \neq 0$.

By hypothesis, $-a_m = \sum_{n=m+1}^{\infty} a_n (n/m)^{-\sigma}$. Let $\sigma = \mathrm{Re}(s) \geq \sigma_0$, and note that for $n > m^2$, we have $(n/m)^{-\sigma} < n^{-\sigma/2}$. It follows that

$$\begin{aligned} |a_m| &\leq \sum_{n=m+1}^{\infty} |a_n|(n/m)^{-\sigma} \\ &\leq \sum_{n=m+1}^{m^2} |a_n|(n/m)^{-\sigma} + \sum_{n=m^2+1}^{\infty} |a_n| n^{-\sigma/2}. \end{aligned}$$

Choose N large enough so that

$$\sum_{n=N+1}^{\infty} |a_n| n^{-\sigma_0} \leq |a_m|/3,$$

and choose $\sigma > 2\sigma_0$ large enough so that

$$\sum_{n=m+1}^{m^2} |a_n|(n/m)^{-\sigma} + \sum_{n=m^2+1}^{N} |a_n| n^{-\sigma/2} \leq |a_m|/3.$$

With these choices, $|a_m| \leq 2|a_m|/3$, which is a contradiction. □

Proposition 1.21. *Let f be a holomorphic function on $\mathcal{H}$ such that:*

(1) *The Fourier expansion for f,*

$$f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z},$$

converges absolutely and uniformly on compact subsets of $\mathcal{H}$, and

(2) *there exists $v > 0$ such that*

$$f(z) = O(\mathrm{Im}(z)^{-v}) \quad (\mathrm{Im}(z) \to 0)$$

uniformly on $\mathrm{Re}(z)$.

Then $a_n = O(n^v)$.

Proof. By hypothesis, there exists a constant $M > 0$ such that $|f(z)| \le M\,\mathrm{Im}(z)^{-v}$. Then

$$\begin{aligned}|a_n| &= \left|\int_0^1 f(x+iy)e^{-2\pi i n(x+iy)}\mathrm{d}x\right| \\ &\le My^{-v}e^{2\pi ny}.\end{aligned}$$

By taking $y = 2/n$, it follows that $|a_n| \le (Me^{4\pi}2^{-v})n^v$. □

A converse to the above proposition is Lemma 1.8.

Lemma 1.22 (Phragmen-Lindelöf). *For two real numbers v_1, v_2 with $v_1 < v_2$, let*

$$F = \{s \in \mathbb{C} : v_1 \le \mathrm{Re}(s) \le v_2\}.$$

Let ϕ be a holomorphic function on a domain containing F satisfying

$$|\phi(s)| = O\big(e^{|\tau|^\delta}\big) \quad (|\tau| \to \infty, \text{with } s = \sigma + i\tau),$$

uniformly on F with $\delta > 0$. For a real number b, if

$$|\phi(s)| = O(|\tau|^b) \quad (|\tau| \to \infty) \quad \text{on } \mathrm{Re}(s) = v_1 \text{ and } \mathrm{Re}(s) = v_2,$$

then $|\phi(s)| = O(|\tau|^b)$ as $|\tau| \to \infty$ uniformly on F.

Proof. By hypothesis, there exists $L > 0$ such that $|\phi(s)| \le Le^{|\tau|^\delta}$. Suppose first that $b = 0$. Then there exists $M > 0$ such that $|\phi(s)| \le M$ on $\mathrm{Re}(s) = v_1$ and on $\mathrm{Re}(s) = v_2$. Let m be a positive integer with $m \equiv 2 \pmod 4$ and let $s = \sigma + i\tau$. Since $\mathrm{Re}(s^m) = \mathrm{Re}((\sigma + i\tau)^m)$ is a polynomial of σ and τ with highest term of τ given by $-\tau^m$, we have

$$\mathrm{Re}(s^m) = -\tau^m + O(|\tau|^{m-1}) \quad (|\tau| \to \infty),$$

uniformly on F. With m even, $\mathrm{Re}(s^m)$ has an upper bound on F. Choose m and N so that $m > \delta$ and $\mathrm{Re}(s^m) < N$, so that for any $\varepsilon > 0$,

$$\left|\phi(s)e^{\varepsilon s^m}\right| \le Me^{\varepsilon N} \quad \text{on } \mathrm{Re}(s) = v_1 \text{ and } \mathrm{Re}(s) = v_2,$$

and

$$\left|\phi(s)e^{\varepsilon s^m}\right| = O\big(e^{|\tau|^\delta - \varepsilon\tau^m + K|\tau|^{m-1}}\big) \quad (|\tau| \to \infty, \text{so this quantity tends to zero in the limit}),$$

uniformly on F. By the maximum principle, it follows that $\left|\phi(s)e^{\varepsilon s^m}\right| \le Me^{\varepsilon N}$ for $s \in F$. Let ε tend to 0 so that $|\phi(s)| \le M$, that is, $\phi(s) = O(|\tau|^0)$.

Now let $b \ne 0$. Let $\psi(s) = (s - v_1 + 1)^b = e^{b\log(s - v_1 + 1)}$ (using the principal branch of the logarithm); note that ψ is holomorphic. Since $\mathrm{Re}(\log(s - v_1 + 1)) = \log|s - v_1 + 1|$, we have

$$|\psi(s)| = |s - v_1 + 1|^b \sim |\tau|^b \quad (|\tau| \to \infty),$$

uniformly on F (the notation $|s - v_1 + 1|^b \sim |\tau|^b$ means that $\lim_{|\tau|\to\infty} |s - v_1 + 1|^b/|\tau|^b = 1$).

Let $\phi_1(s) = \phi(s)/\psi(s)$. The function ϕ_1 satisfies the same assumptions as ϕ with $b = 0$, so by repeating the above argument with $\phi_1(s)$ in place of $\phi(s)$, we find that $\phi_1(s)$ is bounded on F. It follows that $|\phi(s)| = O(|\tau|^b)$ for $|\tau| \to \infty$. □

Definition 1.23. To a holomorphic function $f\colon \mathcal{H} \to \mathbb{C}$ satisfying Proposition 1.21 with Fourier series expansion $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$, we associate to it an ***L-function***, given by the Dirichlet series

$$L(s, f) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

Furthermore, for $N > 0$, define $\Lambda_N(s, f)$ by

$$\Lambda_N(s, f) = (2\pi/\sqrt{N})^{-s}\Gamma(s)L(s, f). \quad †$$

In the above definition, since $a_n = O(n^v)$, the Dirichlet series $L(s,f)$ converges absolutely and uniformly on compact subsets of $\{s \in \mathbb{C} : \mathrm{Re}(s) > 1+v\}$. We are interested in L-functions of modular forms $f \in \mathcal{M}_k(\Gamma_1(N))$, which do satisfy Proposition 1.21.

Definition 1.24. For a positive integer N, define $\omega_N \in \mathrm{GL}_2(\mathbb{R})$ by

$$\omega_n = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

Its action on functions on $\mathcal{H}$ appears in several results forthcoming, so we define it here. †

Theorem 1.25 (Hecke). *Fix positive integers k, N. Let f, g be holomorphic functions on $\mathcal{H}$ satisfing the hypotheses of Proposition 1.21, with Fourier expansions $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$ and $g(z) = \sum_{n=0}^{\infty} b_n e^{2\pi i n z}$. Then the following conditions are equivalent:*

(a) $g(z) = (f|_k[\omega_N])(z) = (\sqrt{N}z)^{-k} f(-1/Nz)$

(b) *Both $\Lambda_N(s,f)$ and $\Lambda(s,g)$ can be analytically continued to the whole s-plane, satisfy the functional equation*

$$\Lambda_N(s,f) = i^k \Lambda_N(k-s, g),$$

and the function

$$\Lambda_N(s,f) + \frac{a_0}{s} + \frac{i^k b_0}{k-s}$$

is holomorphic on the whole s-plane and is bounded on any vertical strip.

Proof. Suppose (a) holds. Since there exists $v > 0$ such that $a_n = O(n^v)$ and $b_n = O(n^v)$,

$$\sum_{n=1}^{\infty} |a_n| e^{-2\pi n t/\sqrt{N}} \quad (t > 0)$$

and

$$\sum_{n=1}^{\infty} \int_0^{\infty} |a_n| t^{\sigma} e^{-2\pi n t/\sqrt{N}} t^{-1} \mathrm{d}t \quad (\sigma > v+1)$$

are convergent. Hence for $\mathrm{Re}(s) > v+1$,

$$\begin{aligned}
\Lambda_N(s,f) &= \sum_{n=1}^{\infty} a_n (2\pi n/\sqrt{N})^{-s} \int_0^{\infty} t^{s-1} e^{-t} \mathrm{d}t \\
&= \sum_{n=1}^{\infty} \int_0^{\infty} a_n t^s e^{-2\pi n t/\sqrt{N}} \\
&= \int_0^{\infty} t^s \left(\sum_{n=1}^{\infty} a_n e^{-2\pi n t/\sqrt{N}} \right) t^{-1} \mathrm{d}t \\
&= \int_0^{\infty} t^s [f(it/\sqrt{N}) - a_0] t^{-1} \mathrm{d}t \\
&= -\frac{a_0}{s} + \int_1^{\infty} t^{-s} f(i/\sqrt{N}t) t^{-1} \mathrm{d}t + \int_1^{\infty} t^s [f(it/\sqrt{N}) - a_0] t^{-1} \mathrm{d}t.
\end{aligned}$$

Since $g(z) = (\sqrt{N}z)^{-k} f(-1/Nz)$, the above equality becomes

$$\Lambda_N(s,f) = -\frac{a_0}{s} - \frac{i^k b_0}{k-s} + i^k \int_1^{\infty} t^{k-s} [g(it/\sqrt{N}) - b_0] t^{-1} \mathrm{d}t + \int_1^{\infty} t^s [f(it/\sqrt{N}) - a_0] t^{-1} \mathrm{d}t, \tag{1.6}$$

which holds for $\mathrm{Re}(s) > \max\{k, v+1\}$. By Lemma 1.8, as t tends to ∞, $f(it) - a_0 = O(e^{-2\pi t})$ and $g(it) - a_0 = O(e^{-2\pi t})$ so that

$$\int_1^\infty t^s[f(it/\sqrt{N}) - a_0]t^{-1}\mathrm{d}t \quad \text{and} \quad \int_1^\infty t^{k-s}[g(it/\sqrt{N}) - b_0]t^{-1}\mathrm{d}t$$

are convergent absolutely and uniformly on any vertical strip. Therefore the functions these integrals define are holomorphic on the whole s-plane. It follows by (1.6) that $\Lambda_N(s,f)$ is a meromorphic function on the whole s-plane with $\Lambda_N(s,f) + a_0/s + i^k b_0/(k-s)$ an entire bounded function on any vertical strip. Similarly analytically continue $\Lambda_N(s,g)$ to the whole s-plane, satisfying

$$(1.7) \quad i^k\Lambda_N(k-s,g) = -\frac{a_0}{s} - \frac{i^k b_0}{k-s} + i^k\int_1^\infty t^{k-s}[g(it/\sqrt{N} - b_0)]t^{-1}\mathrm{d}t + \int_1^\infty t^s[f(it/\sqrt{N}) - a_0]t^{-1}\mathrm{d}t.$$

It follows from (1.6) and (1.7) that $\Lambda_N(s,f) = i^k\Lambda_N(k-s,g)$.

Conversely, suppose that (b) holds. Since $e^{-e^x}e^{\sigma x}$ is a Schwartz function for $\sigma > 0$, the inverse Mellin transform

$$e^{-t} = \frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\sigma}\Gamma(s)t^{-s}\mathrm{d}s$$

holds for $\sigma > 0$. It follows that

$$f(iy) = a_0 + \frac{1}{2\pi i}\sum_{n=1}^\infty a_n\int_{\mathrm{Re}(s)=\alpha}\Gamma(s)(2\pi ny)^{-s}\mathrm{d}s$$

for any $\alpha > 0$. Let $\alpha > v+1$, so that $L(s,f) = \sum_{n=1}^\infty a_n n^{-s}$ is uniformly convergent and bounded on $\mathrm{Re}(s) = \alpha$. In this case, Stirling's estimate $\Gamma(s) \sim \sqrt{2\pi}\tau^{\sigma-1/2}e^{-\pi|\tau|/2}$ (for $s = \sigma + i\tau$ and $|\tau| \to \infty$) shows that $\Lambda_N(s,f) = (2\pi/\sqrt{N})^{-s}\Gamma(s)L(s,f)$ is absolutely integrable, so that the order of integration and summation above may be interchanged to obtain

$$(1.8) \quad f(iy) = a_0 + \frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\alpha}(\sqrt{N}y)^{-s}\Lambda_N(s,f)\mathrm{d}s.$$

Since $L(s,f)$ is bounded on $\mathrm{Re}(s) = \alpha$, by Stirling's estimate we have for any $\mu > 0$ that

$$(1.9) \quad |\Lambda_N(s,f)| = O(|\mathrm{Im}(s)|^{-\mu}) \quad (|\mathrm{Im}(s)| \to \infty)$$

on $\mathrm{Re}(s) = \alpha$. Choose β so that $k - \beta > v+1$. Using a similar argument we deduce that for any $\mu > 0$,

$$|\Lambda_N(s,f)| = |\Lambda_N(k-s,g)| = O(|\mathrm{Im}(s)|^{-\mu}) \quad (|\mathrm{Im}(s)| \to \infty)$$

on $\mathrm{Re}(s) = \beta$. By assumption, $\Lambda_N(s,f) + a_0/s + i^k b_0/(k-s)$ is bounded on the vertical strip $\beta \le \mathrm{Re}(s) \le \alpha$. Thus for any $\mu > 0$, Lemma 1.22 implies that (1.9) holds uniformly on the strip $\beta \le \mathrm{Re}(s) \le \alpha$.

We may also assume that $\alpha > k$ and $\beta < 0$. Observe that $(\sqrt{N}y)^{-s}\Lambda_N(s,f)$ has simple poles at $s = 0, k$ with corresponding residues $-a_0, (\sqrt{N}y)^{-k}i^k b_0$. Combined with the fact that (1.9) holds uniformly on the strip $\beta \le \mathrm{Re}(s) \le \alpha$, we may change the path of integration from $\mathrm{Re}(s) = \alpha$ to $\mathrm{Re}(s) = \beta$ in (1.8) to obtain

$$f(iy) = (\sqrt{N}y)^{-k}i^k b_0 + \frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\beta}(\sqrt{N}y)^{-s}\Lambda_N(s,f)\mathrm{d}s.$$

From the functional equation in (b), we have

$$\begin{aligned} f(iy) &= (\sqrt{N}y)^{-k}i^k b_0 + \frac{1}{2\pi i}\int_{\mathrm{Re}(s)=\beta}(\sqrt{N}y)^{-s}i^k\Lambda_N(k-s,g)\mathrm{d}s \\ &= i^k\left[(\sqrt{N}y)^{-k}b_0 + \frac{1}{2\pi i}\int_{\mathrm{Re}(s)=k-\beta}(\sqrt{N}y)^{s-k}\Lambda_N(s,g)\mathrm{d}s\right] \\ &= i^k(\sqrt{N}y)^{-k}g(-1/iNy). \end{aligned}$$

Since f, g are holomorphic on $\mathcal{H}$, it follows that $f(z) = i^k(\sqrt{N}z/i)^{-k}g(-1/Nz)$, or equivalently $g(z) = (\sqrt{N}z)^{-k}f(-1/Nz)$. □

Corollary 1.26. *If $f(z) \in \mathcal{S}_k(N,\chi)$, then because any element of $\mathcal{S}_k(N,\chi)$ satisfies the conditions of Proposition 1.21 (see Corollary 1.11), it follows that $\Lambda_N(s,f)$ is holomorphic in s and satisfies the functional equation*

$$\Lambda_N(s,f) = i^k \Lambda_N(k-s, f|_k[\omega_N]).$$

2 Hecke operators

We outline how double cosets act on spaces of modular forms, and using them we define the Hecke operators $\langle n\rangle$ and T_n on the space $\mathcal{M}_k(\Gamma_1(N))$. The Hecke operators are akin to "averaging" operators which act on each of the eigenspaces from Proposition 1.19. We collect several properties of the Hecke operators for later use. For example, if a modular form is a common eigenfunction of all of the Hecke operators T_n, then its Fourier coefficients are proportional to its eigenvalues. Following the discussion of the Hecke operators, we restrict our view to the space of cusp forms $\mathcal{S}_k(\Gamma_1(N))$, on which we define the Petersson inner product and find adjoints to the Hecke operators $\langle p\rangle$ and T_p for primes p not dividing N. By doing so, we deduce that all of the Hecke operators $\langle n\rangle$ and T_n are normal operators on $\mathcal{S}_k(\Gamma_1(N))$ whenever n is coprime to N.

2.1 Double coset operators

Let Γ_1, Γ_2 be congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. For $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, the set

$$\Gamma_1\alpha\Gamma_2 = \{\gamma_1\alpha\gamma_2 : \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2\}$$

is a ***double coset*** in $\mathrm{GL}_2^+(\mathbb{Q})$. The group Γ_1 acts on the double coset $\Gamma_1\alpha\Gamma_2$ on the left by multiplication, partitioning it into orbits of the form $\Gamma_1\beta$, where $\beta = \gamma_1\alpha\gamma_2$ is some representative for this orbit. We show that the orbit space $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ is a finite disjoint union $\bigsqcup_j \Gamma_1\beta_j$ for some choice of representatives β_j.

Lemma 2.1. *Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ and Γ be a congruence subgroup. Then $\alpha^{-1}\Gamma\alpha \cap \mathrm{SL}_2(\mathbb{Z})$ is also a congruence subgroup.*

Proof. There exists N such that $\Gamma(N)$ is contained in Γ. Let M be the least common multiple of N and the entries of the matrices α and α^{-1} so that $\Gamma(M) \subset \Gamma$ and $M\alpha, M\alpha^{-1}$ are integer-valued matrices.

Observe that $\Gamma(M^3)$ is contained in $I + M^3\,\mathrm{M}_2(\mathbb{Z})$ so that

$$\alpha\Gamma(M^3)\alpha^{-1} \subset \alpha(I + M^3\,\mathrm{M}_2(\mathbb{Z}))\alpha^{-1} = I + M\cdot(M\alpha)\,\mathrm{M}_2(\mathbb{Z})(M\alpha^{-1}) \subset I + M\,\mathrm{M}_2(\mathbb{Z}).$$

Elements of $\alpha\Gamma(M^3)\alpha^{-1}$ have determinant 1, so $\alpha\Gamma(M^3)\alpha^{-1} \subset \mathrm{SL}_2(\mathbb{Z})$, from which it follows that $\alpha\Gamma(M^3)\alpha^{-1} \subset \Gamma(M)$. Hence $\Gamma(M^3) \subset \alpha^{-1}\Gamma(M)\alpha \subset \alpha^{-1}\Gamma\alpha$, and so $\Gamma(M^3) \subset \alpha^{-1}\Gamma\alpha \cap \mathrm{SL}_2(\mathbb{Z})$. □

Lemma 2.2. *Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ and Γ_1, Γ_2 be congruence subgroups. Let $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2 \subset \Gamma_2$. Then the map $\Gamma_2 \to \Gamma_1\alpha\Gamma_2$ given by left multiplication by α, $\gamma_2 \mapsto \alpha\gamma_2$, induces a natural bijection of the coset space $\Gamma_3\backslash\Gamma_2$ to the orbit space $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$.*

In other words, $\{\gamma_{2,j}\}$ is a set of coset representatives for $\Gamma_3\backslash\Gamma_2$ if and only if $\{\alpha\gamma_{2,j}\}$ is a set of orbit representatives for $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$.

Proof. It is evident that the map $\Gamma_2 \to \Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ given by $\gamma_2 \mapsto \Gamma_1\alpha\gamma_2$ is surjective, since elements of $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ are of the form $\Gamma_1\gamma_1\alpha\gamma_2$ for some $\gamma_1 \in \Gamma_1$ and $\gamma_2 \in \Gamma_2$. Two elements $\gamma_2, \gamma_2' \in \Gamma_2$ map to the same orbit if $\Gamma_1\alpha\gamma_2 = \Gamma_1\alpha\gamma_2'$, that is, if $\gamma_2'\gamma_2^{-1} \in \alpha^{-1}\Gamma_1\alpha$. It follows that by taking $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$ as above, that the induced map from the coset space $\Gamma_3\backslash\Gamma_2 \to \Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ is a bijection. □

Lemma 2.3. *Let Γ_1, Γ_2 be congruence subgroups. Then they are* ***commensurable****, that is, the indices $[\Gamma_1 : \Gamma_1 \cap \Gamma_2], [\Gamma_2 : \Gamma_1 \cap \Gamma_2]$ are finite.*

Proof. There exist positive integers N_1, N_2 such that $\Gamma(N_1) \subset \Gamma_1$ and $\Gamma(N_2) \subset \Gamma_2$. Then $\Gamma(\mathrm{lcm}(N_1, N_2)) \subset \Gamma(N_1) \cap \Gamma(N_2) \subset \Gamma_1 \cap \Gamma_2$ since N_1, N_2 divide their least common multiple. Then

$$[\Gamma_1 : \Gamma(\mathrm{lcm}(N_1, N_2))] = [\Gamma_1 : \Gamma_1 \cap \Gamma_2][\Gamma_1 \cap \Gamma_2 : \Gamma(\mathrm{lcm}(N_1, N_2))] \text{ and}$$
$$[\Gamma_2 : \Gamma(\mathrm{lcm}(N_1, N_2))] = [\Gamma_2 : \Gamma_1 \cap \Gamma_2][\Gamma_1 \cap \Gamma_2 : \Gamma(\mathrm{lcm}(N_1, N_2))].$$

The indices $[\Gamma_1 : \Gamma(\mathrm{lcm}(N_1, N_2))], [\Gamma_2 : \Gamma(\mathrm{lcm}(N_1, N_2))]$ are finite (see the discussion following Definition 0.5), so that the indices $[\Gamma_1 : \Gamma_1 \cap \Gamma_2], [\Gamma_2 : \Gamma_1 \cap \Gamma_2]$ are also finite. □

In Lemma 2.1, since $\alpha^{-1}\Gamma\alpha \cap \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup, the coset space $\Gamma_3\backslash\Gamma_2$ from Lemma 2.2 is finite, so that the orbit space $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ is also finite as desired. With this result, we can define an action of double cosets on modular forms.

Definition 2.4. Let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ and Γ_1, Γ_2 be congruence subgroups. The ***weight-k $\Gamma_1\alpha\Gamma_2$ operator*** ("double coset operator") $|_k[\Gamma_1\alpha\Gamma_2]$ is given by

$$f|_k[\Gamma_1\alpha\Gamma_2] = (\det\alpha)^{k/2-1}\sum_j f|_k[\beta_j],$$

where $\{\beta_j\}$ is a set of orbit representatives of $\Gamma_1\alpha\Gamma_2$ (that is, $\Gamma_1\alpha\Gamma_2 = \bigsqcup_j \Gamma_1\beta_j$). It takes modular forms in $\mathcal{M}_k(\Gamma_1)$ to modular forms in $\mathcal{M}_k(\Gamma_2)$, and takes cusp forms in $\mathcal{S}_k(\Gamma_1)$ to cusp forms in $\mathcal{S}_k(\Gamma_2)$. †

We check that this definition is well defined, that is, independent of the choice of orbit representatives for $\Gamma_1\alpha\Gamma_2$. Let $\beta = \gamma_1\alpha\gamma_2$ and $\beta' = \gamma_1'\alpha\gamma_2'$ represent the same orbit in $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$, so that $\Gamma_1\beta = \Gamma_1\beta'$. It follows that $\alpha\gamma_2 \in \Gamma_1\alpha\gamma_2'$. Since f is weight-k invariant under Γ_1, we have $f|_k[\beta] = f|_k[\alpha\gamma_2] = f|_k[\eta_1\alpha\gamma_2'] = f|_k[\alpha\gamma_2'] = f|_k[\beta']$. Thus the action of the double coset $\Gamma_1\alpha\Gamma_2$ is well defined.

We also check that the double coset operator takes modular forms to modular forms and cusp forms to cusp forms. For $f \in \mathcal{M}_k(\Gamma_1)$, we verify that $f|_k[\Gamma_1\alpha\Gamma_2]$ is Γ_2-invariant and holomorphic at the cusps of Γ_2.

Note that any $\gamma_2 \in \Gamma_2$ permutes the orbit space $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$ by right multiplication. So given a set of orbit representatives $\{\beta_j\}$ for $\Gamma_1\backslash\Gamma_1\alpha\Gamma_2$, then $\{\beta_j\gamma_2\}$ is also a set of orbit representatives. Therefore

$$(f|_k[\Gamma_1\alpha\Gamma_2])|_k[\gamma_2] = (\det\alpha)^{k/2-1}\sum_j f|_k[\beta_j\gamma_2] = f|_k[\Gamma_1\alpha\Gamma_2].$$

It follows that $f|_k[\Gamma_1\alpha\Gamma_2]$ is weight-k invariant under Γ_2 as needed.

Observe that for any $f \in \mathcal{M}_k(\Gamma_1)$ and any $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$, the function $f|_k[\gamma]$ is holomorphic at infinity; that is, it has a Fourier expansion

$$(f|_k[\gamma])(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z/h}$$

for some positive integer h by Lemma 1.5. Then for any $\delta \in \mathrm{SL}_2(\mathbb{Z})$,

$$(f|_k[\Gamma_1\alpha\Gamma_2])|_k[\delta] = (\det\alpha)^{k/2-1}\sum_j f|_k[\beta_j\delta]$$

for some set of orbit representatives $\{\beta_j\}$ of $\Gamma_1\alpha\Gamma_2$, from which holomorphicity of $f|_k[\Gamma_1\alpha\Gamma_2]$ at all cusps of Γ_2 follows, since each summand above is holomorphic at infinity. In the case that f is a cusp form, $f|_k[\gamma]$ vanishes at infinity for any $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$ as we saw in Lemma 1.5. Therefore the double coset operator takes modular forms to modular forms and cusp forms to cusp forms.

Particular choices of Γ_1, Γ_2 yield notable double coset operators:

(1) If $\Gamma_2 \subset \Gamma_1$ and $\alpha = I$, then $f|_k[\Gamma_1\alpha\Gamma_2] = f$ and the double coset operator $|_k[\Gamma_1\alpha\Gamma_2]$ is the natural inclusion of $\mathcal{M}_k(\Gamma_1)$ into $\mathcal{M}_k(\Gamma_2)$.

(2) If $\Gamma_2 = \alpha^{-1}\Gamma_1\alpha$, then $f|_k[\Gamma_1\alpha\Gamma_2] = (\det\alpha)^{k/2-1}f|_k[\alpha]$, and the double coset operator $|_k[\Gamma_1\alpha\Gamma_2]$ is an isomorphism of $\mathcal{M}_k(\Gamma_1)$ with $\mathcal{M}_k(\Gamma_2)$.

(3) Finally, if $\Gamma_1 \subset \Gamma_2$ and $\alpha = I$, take $\{\gamma_{2,j}\}$ to be a set of coset representatives for $\Gamma_1\backslash\Gamma_2$. Then $f|_k[\Gamma_1\alpha\Gamma_2] = \sum_j f|_k[\gamma_{2,j}]$, and the double coset operator $|_k[\Gamma_1\alpha\Gamma_2]$ is the natural trace map projecting $\mathcal{M}_k(\Gamma_1)$ onto its subspace $\mathcal{M}_k(\Gamma_2)$ by symmetrizing over the quotient, a surjection. (The action of Γ_1 on Γ_2 is to permute the coset representatives of $\Gamma_1\backslash\Gamma_2$, so the action of Γ_1 on elements in the image of the natural trace map is the identity.)

Any double coset operator is a composition of these three operators. Indeed, given Γ_1, Γ_2, and α, set $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$ and $\Gamma_3' = \alpha\Gamma_3\alpha^{-1} = \Gamma_1 \cap \alpha\Gamma_2\alpha^{-1}$. Then $\Gamma_3' \subset \Gamma_1$, $\alpha^{-1}\Gamma_3'\alpha = \Gamma_3$, and $\Gamma_3 \subset \Gamma_2$. Composing their corresponding double coset operators, we have for $f \in \mathcal{M}_k(\Gamma_1)$ that $f \mapsto f \mapsto (\det\alpha)^{k/2-1} f|_k[\alpha] \mapsto (\det\alpha)^{k/2-1}\sum_j f|_k[\alpha\gamma_{2,j}]$. By Lemma 2.2 the composition above agrees with the double coset operator $|_k[\Gamma_1\alpha\Gamma_2]$.

2.2 Hecke operators $\langle n\rangle$ and T_n

Recall the congruence subgroups

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod N \right\} \text{ and}$$
$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod N \right\}.$$

Since $\Gamma_1(N) \subset \Gamma_0(N)$, we have the containment $\mathcal{M}_k(\Gamma_0(N)) \subset \mathcal{M}_k(\Gamma_1(N))$ of modular forms. We define the two operators $\langle n\rangle$ and T_n on the larger space $\mathcal{M}_k(\Gamma_1(N))$.

Let $\alpha \in \Gamma_0(N)$ and consider the weight-k double coset operator $|_k[\Gamma_1(N)\alpha\Gamma_1(N)]$. From Lemma 0.8 we have that $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ and that $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$, so the double coset operator $|_k[\Gamma_1(N)\alpha\Gamma_1(N)]$ is of the form (2) in the list of notable double coset operators following Definition 2.4. Hence this double coset operator translates a function $f \in \mathcal{M}_k(\Gamma_1(N))$ to $f|_k[\Gamma_1(N)\alpha\Gamma_1(N)] = f|_k[\alpha] \in \mathcal{M}_k(\Gamma_1(N))$. In this way the group $\Gamma_0(N)$ acts on $\mathcal{M}_k(\Gamma_1(N))$, and its subgroup $\Gamma_1(N)$ acts trivially. Thus $\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$ acts on $\mathcal{M}_k(\Gamma_1(N))$. In particular, if $d \in (\mathbb{Z}/N\mathbb{Z})^\times$, there exists $\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right) \in \Gamma_0(N)/\Gamma_1(N)$ with $d' \equiv d \pmod N$. From this fact, we obtain the diamond operator $\langle d\rangle$ on $\mathcal{M}_k(\Gamma_1(N))$:

Proposition 2.5. *The action of d on $\mathcal{M}_k(\Gamma_1(N))$, called the diamond operator $\langle d\rangle\colon \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$, is given by*

$$\langle d\rangle f = f|_k[\alpha] \quad \textit{for any } \alpha = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma_0(N) \textit{ with } d' \equiv d \pmod N.$$

For any character χ, we have that the space $\mathcal{M}_k(N,\chi)$ from Proposition 1.19 is really the "χ-eigenspace of the diamond operators"; that is,

$$\mathcal{M}_k(N,\chi) = \{ f \in \mathcal{M}_k(\Gamma_1(N)) : \langle d\rangle f = \chi(d) f \text{ for all } d \in (\mathbb{Z}/N\mathbb{Z})^\times \},$$

with a similar definition for $\mathcal{S}_k(N,\chi)$. In other words, the diamond operator $\langle d\rangle$ acts on $\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_\chi \mathcal{M}_k(N,\chi)$ by acting on each χ-eigenspace by multiplication by $\chi(d)$. We can now give an elementary proof of Proposition 1.19:

Proposition 2.6. *The following decompositions hold:*

$$\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_\chi \mathcal{M}_k(N,\chi), \quad \mathcal{S}_k(\Gamma_1(N)) = \bigoplus_\chi \mathcal{S}_k(N,\chi).$$

Proof. For any character $\chi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, define the operator $\pi_\chi\colon \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$ by

$$\pi_\chi = \frac{1}{\phi(N)} \sum_{d \in (\mathbb{Z}/N\mathbb{Z})^\times} \chi(d)^{-1}\langle d\rangle.$$

Observe that for any $d, e \in (\mathbb{Z}/N\mathbb{Z})^\times$, we have $\langle d\rangle\langle e\rangle = \langle e\rangle\langle d\rangle = \langle de\rangle$: For any $f \in \mathcal{M}_k(N,\chi)$, we have

$\langle d\rangle\langle e\rangle f = \langle d\rangle\chi(e)f = \chi(de)f$ as needed. It follows that

$$\begin{aligned}\pi_\chi^2 &= \frac{1}{\phi(N)}\sum_{d\in(\mathbb{Z}/N\mathbb{Z})^\times}\chi(d)^{-1}\langle d\rangle\left(\frac{1}{\phi(N)}\sum_{e\in(\mathbb{Z}/N\mathbb{Z})^\times}\chi(e)^{-1}\langle e\rangle\right)\\ &= \frac{1}{\phi(N)^2}\sum_{d\in(\mathbb{Z}/N\mathbb{Z})^\times}\sum_{e\in(\mathbb{Z}/N\mathbb{Z})^\times}\chi(de)^{-1}\langle de\rangle\\ &= \frac{1}{\phi(N)}\sum_{d\in(\mathbb{Z}/N\mathbb{Z})^\times}\chi(d)^{-1}\langle d\rangle\\ &= \pi_\chi.\end{aligned}$$

Since π_χ is idempotent, it follows from linear algebra that it is a projection operator of $\mathcal{M}_k(\Gamma_1(N))$ onto some subspace. Let $f \in \mathcal{M}_k(\Gamma_1(N))$. Then

$$\langle e\rangle\pi_\chi(f) = \langle e\rangle\frac{1}{\phi(N)}\sum_{d\in(\mathbb{Z}/N\mathbb{Z})^\times}\chi(d)^{-1}\langle d\rangle f = \chi(e)\frac{1}{\phi(N)}\sum_{d\in(\mathbb{Z}/N\mathbb{Z})^\times}\chi(de)^{-1}\langle de\rangle f = \chi(e)\pi_\chi(f)$$

for any $e \in (\mathbb{Z}/N\mathbb{Z})^\times$. Furthermore, for any $f \in \mathcal{M}_k(N,\chi)$, we have that $\pi_\chi(f) = f$. Hence π_χ is the projection of $\mathcal{M}_k(\Gamma_1(N))$ onto $\mathcal{M}_k(N,\chi)$.

Choose the characters so that they satisfy the orthogonality conditions in Proposition 1.16. Then

$$\begin{aligned}\sum_\chi \pi_\chi &= \frac{1}{\phi(N)}\sum_\chi\sum_d \chi(d)^{-1}\langle d\rangle\\ &= \frac{1}{\phi(N)}\sum_d\left(\sum_\chi \chi(d)\right)\langle d\rangle\\ &= \langle 1\rangle\\ &= \mathrm{id}_{\mathcal{M}_k(\Gamma_1(N))},\end{aligned}$$

and for two nonequal characters χ, χ', we have

$$\pi_\chi\circ\pi_{\chi'} = \frac{1}{\phi(N)}\sum_d \chi(d)^{-1}\langle d\rangle\pi_{\chi'} = \frac{1}{\phi(N)}\sum_d\chi(d)^{-1}\chi'(d)\pi_{\chi'} = \frac{1}{\phi(N)}\left(\sum_d(\chi^{-1}\chi')(d)\right)\pi_{\chi'} = 0.$$

It follows that the χ-eigenspaces span $\mathcal{M}_k(\Gamma_1(N))$ and are pairwise disjoint, which proves the result. The same argument follows for cusp forms. □

We extend the definition of the diamond operator $\langle d\rangle$ for $d \in (\mathbb{Z}/N\mathbb{Z})^\times$ to $\langle n\rangle$ for $n \in \mathbb{Z}^+$.

Definition 2.7. The ***Hecke operator*** $\langle n\rangle\colon \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$ for $n \in \mathbb{Z}^+$ is given by the zero operator when $\gcd(n,N) > 1$ and is given by $\langle\overline{n}\rangle$ when $\gcd(n,N) = 1$ (where $\overline{\cdot}$ denotes reduction modulo N). †

Let p be a prime number, and consider the weight-k double coset operator $T_p\colon \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$ given by $T_p f = f|_k[\Gamma_1(N)\alpha\Gamma_1(N)]$, where $\alpha = \left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)$.

Lemma 2.8. *For a prime p, the double coset $\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)$ is given by*

$$\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N) = \left\{\gamma\in\mathrm{M}_2(\mathbb{Z}) : \gamma\equiv\begin{pmatrix}1&*\\0&p\end{pmatrix} \pmod N, \det\gamma = p\right\}.$$

Proof. We sketch the proof since it is rather computational. The containment

$$\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N) \subseteq \left\{\gamma\in\mathrm{M}_2(\mathbb{Z}) : \gamma\equiv\begin{pmatrix}1&*\\0&p\end{pmatrix} \pmod N, \det\gamma = p\right\}$$

is clear. We show that the other containment holds.

Let $L=\mathbb{Z}^2$, and let $L_0=\left\{\left(\begin{smallmatrix}x\\y\end{smallmatrix}\right)\in L: y\equiv 0 \pmod N\right\}$. Let $\mathrm{M}_2(\mathbb{Z})$ acts on L by left multiplication. Choose $\gamma\in \mathrm{M}_2(\mathbb{Z})$ such that $\gamma\equiv\left(\begin{smallmatrix}1&*\\0&p\end{smallmatrix}\right) \pmod N$ and $\det\gamma=p$. Because the determinant of γ is positive, $[L:\gamma L_0]=[L:L_0][L_0:\gamma L_0]=Np$.

By the theory of finitely generated Abelian groups there exists a basis $\{u,v\}$ of L such that $\det(u\ v)=1$ and $\gamma L_0=mu\mathbb{Z}\oplus nv\mathbb{Z}$, where $0<m,n,\ m\mid n$, and $mn=Np$. Write the first column of γ as $\left(\begin{smallmatrix}a_\gamma\\c\end{smallmatrix}\right)$ with $a_\gamma\equiv 1 \pmod N$ and $c\equiv 0 \pmod N$. We can also write the first column of γ as $\gamma e_1\in\gamma L_0$ (e_i is the i-th standard basis vector), and hence is the zero vector modulo m. Since $\gcd(a_\gamma,N)=1$, we have $\gcd(m,N)=1$, from which we deduce that $m=1$ and $n=Np$. Hence $\gamma L_0=u\mathbb{Z}\oplus Npv\mathbb{Z}$.

There are unique subgroups $L_0=u\mathbb{Z}\oplus Nv\mathbb{Z}$ and $\gamma L=u\mathbb{Z}\oplus pv\mathbb{Z}$, of index p and N respectively inside $L=u\mathbb{Z}\oplus v\mathbb{Z}$, that contain γL_0. Let $\gamma_1=(u\ v)$. Because $u\in L_0$, it follows that $\gamma_1\in\Gamma_0(N)$. Let $\gamma_2=\left(\gamma_1\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\right)^{-1}\gamma=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ be an element of $\mathrm{GL}_2^+(\mathbb{Q})$ with determinant 1. The condition for $\gamma e_1\in\gamma L_0$ to hold is given by $au+cpv\in u\mathbb{Z}\oplus Npv\mathbb{Z}$, so that we must have $a\in\mathbb{Z}$ and $c\in N\mathbb{Z}$. Similarly, for γe_2 to be an element of γL we must have $b,d\in\mathbb{Z}$. It follows that $\gamma_2\in\Gamma_0(N)$. Since $a_\gamma\equiv 1 \pmod N$, $\gamma e_1\equiv e_1 \pmod N$ and so the equation $\gamma=\gamma_1\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\gamma_2$ shows that $au_1\equiv 1 \pmod N$ (where u_1 is the first component of u), using only that $\gamma_1,\gamma_2\in\Gamma_0(N)$. Thus if $\gamma=\gamma_1\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\gamma_2$ for $\gamma_1,\gamma_2\in\Gamma_0(N)$ such that either γ_1 or γ_2 lies in $\Gamma_1(N)$, then both do.

It now suffices to show that $\Gamma_0(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_0(N)=\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_0(N)$. The containment $\Gamma_0(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_0(N)\supseteq\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_0(N)$ is clear. For the other containment, note that $\Gamma_1(N)\backslash\Gamma_0(N)$ is represented by matrices of the form $\left(\begin{smallmatrix}a&b\\N&d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z})$. Thus it suffices to show that for each such matrix there exists a matrix $\delta\in\Gamma_1(N)$ such that $\left(\begin{smallmatrix}a&b\\N&d\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_0(N)=\delta\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_0(N)$; equivalently a matrix $\delta'\in\Gamma_1(N)$ such that

$$\begin{pmatrix}1&0\\0&p\end{pmatrix}^{-1}\delta'\begin{pmatrix}a&b\\N&d\end{pmatrix}\begin{pmatrix}1&0\\0&p\end{pmatrix}\in\Gamma_0(N).$$

If $p\mid N$, then $\delta'=\left(\begin{smallmatrix}dN+1&-1\\-dN&1\end{smallmatrix}\right)$ is a valid choice. Otherwise, if $p\nmid N$, then any $\delta'=\left(\begin{smallmatrix}*&*\\N&d'\end{smallmatrix}\right)$ with $d'\equiv 1 \pmod N$ and $d'\equiv -a \pmod p$ is a valid choice in this case. □

So in the definition of T_p, we may replace α with any matrix in the double coset $\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)$.

We record the explicit action of T_p on elements of $\mathcal{M}_k(\Gamma_1(N))$.

Proposition 2.9. *The operator $T_p\colon\mathcal{M}_k(\Gamma_1(N))\to\mathcal{M}_k(\Gamma_1(N))$ is given explicitly by*

$$T_pf=\begin{cases}p^{k/2-1}\sum_{j=0}^{p-1}f|_k[\left(\begin{smallmatrix}1&j\\0&p\end{smallmatrix}\right)] & \text{if } p\mid N,\\ p^{k/2-1}\sum_{j=0}^{p-1}f|_k[\left(\begin{smallmatrix}1&j\\0&p\end{smallmatrix}\right)]+p^{k/2-1}f|_k[\left(\begin{smallmatrix}m&n\\N&p\end{smallmatrix}\right)\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)] & \text{if } p\nmid N,\ \text{where } mp-nN=1.\end{cases}$$

Proof. We find orbit representatives for $\Gamma_1(N)\backslash\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)$ by finding coset representatives for $\Gamma_3\backslash\Gamma_1(N)$, where $\Gamma_3=\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)^{-1}\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\cap\Gamma_1(N)$.

Define the subgroups

$$\Gamma^0(p)=\left\{\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbb{Z}):\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\equiv\left(\begin{smallmatrix}*&0\\ *&*\end{smallmatrix}\right) \pmod p\right\}$$

and $\Gamma_1^0(N,p)=\Gamma_1(N)\cap\Gamma^0(p)$. A short computation reveals that Γ_3 is equal to $\Gamma_1^0(N,p)$. We show that the coset representatives of $\Gamma_3\backslash\Gamma_1(N)$ are $\gamma_{2,j}=\left(\begin{smallmatrix}1&j\\0&1\end{smallmatrix}\right)$ for $0\le j<p$.

Given $\gamma_2=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\Gamma_1(N)$, we have $\gamma_2\in\Gamma_3\gamma_{2,j}$ if $\gamma_2\gamma_{2,j}^{-1}\in\Gamma_3$. Observe that $\gamma_2,\gamma_{2,j}\in\Gamma_1(N)$, so it suffices to find j so that the upper right entry $b-ja$ of $\gamma_2\gamma_{2,j}^{-1}$ is some multiple of p.

If $p\nmid a$, then $j=ba^{-1} \pmod p$ is a valid choice. So in this case we find that $\gamma_{2,j}=\left(\begin{smallmatrix}1&j\\0&1\end{smallmatrix}\right)$ for $0\le j<p$ form a complete set of coset representatives as needed (for each representative, one may also take $j+lp$ for any integer l in place of j).

If $p\mid a$, then $b-ja$ cannot be zero $\pmod p$ for any j; if there was a choice of j that made $b-ja$ zero, then p would divide b and hence also $\det\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)=1$, which is impossible. The cases where $\gamma_2\in\Gamma_1(N)$ with $p\mid a$

occur if and only if $p \nmid N$, in which case $\gamma_{2,j} = \left(\begin{smallmatrix}1 & j\\ 0 & 1\end{smallmatrix}\right)$ for $0 \le j < p$ fail to represent $\Gamma_3\backslash\Gamma_1(N)$. To complete the set of coset representatives, set

$$\gamma_{2,\infty} = \begin{pmatrix} mp & n \\ N & 1\end{pmatrix} \quad \text{where } mp - nN = 1.$$

So given $\gamma_2 = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \Gamma_1(N)$ with $p \mid a$, we have $\gamma_2\gamma_{2,\infty}^{-1} \equiv \left(\begin{smallmatrix}* & 0\\ * & *\end{smallmatrix}\right) \pmod p$ as needed. It is also routine to check that the $\gamma_{2,j}$ represent distinct cosets.

The corresponding orbit representatives of $\Gamma_1(N)\backslash\Gamma_1(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\Gamma_1(N)$ are given by $\alpha\gamma_{2,j}$ for each j:

$$\alpha\gamma_{2,j} = \begin{pmatrix}1 & j\\ 0 & p\end{pmatrix} \text{ for } 0 \le j < p, \quad \alpha\gamma_{2,\infty} = \begin{pmatrix} m & n\\ N & p\end{pmatrix}\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix} \text{ if } p \nmid N. \qquad \square$$

A related result, which we do not prove but will be used later, is the following:

Lemma 2.10. *Let N be a positive integer and p a prime. Then*

$$\Gamma_1(pN)\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma_1(N) = \begin{cases} \coprod_{v=0}^{p-1} \Gamma_1(pN)\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\gamma_v & \text{if } p \mid N,\\ \coprod_{v=0}^{p} \Gamma_1(pN)\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\gamma_v & \text{if } p \nmid N;\end{cases}$$

here γ_v for $0 \le v < p$ is an element of $\Gamma_0(N)$ such that $\gamma_v \equiv \left(\begin{smallmatrix}1 & v\\ 0 & 1\end{smallmatrix}\right) \pmod p$, and γ_p for $p \nmid N$ is an element of $\Gamma_0(N)$ such that

$$\gamma_p \equiv \begin{cases} \left(\begin{smallmatrix}0 & -a\\ a^{-1} & 0\end{smallmatrix}\right) \pmod p & \text{for } a \text{ coprime to } p,\\ \left(\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right) \pmod N.\end{cases}$$

See [Miy05, Lemma 4.5.11] for details.

Lemma 2.11. *Let $f \in \mathcal{M}_k(\Gamma_1(N))$ have Fourier expansion*

$$f(z) = \sum_{n=0}^{\infty} a_n(f)q^n, \quad q = e^{2\pi i z}.$$

Then $T_p f$ has Fourier expansion

$$\begin{aligned}(T_p f)(z) &= \sum_{n=0}^{\infty} a_{np}(f)q^n + \mathbf{1}_N(p)p^{k-1}\sum_{n=0}^{\infty} a_n(\langle p\rangle f)q^{np}\\ &= \sum_{n=0}^{\infty}(a_{np}(f) + \mathbf{1}_N(p)p^{k-1}a_{n/p}(\langle p\rangle f))q^n,\end{aligned}$$

where $a_{n/p} = 0$ whenever n/p is not an integer.

Proof. Let $p \mid N$. For $0 \le j < p$, we have

$$\begin{aligned}p^{k/2-1}(f|_k[\left(\begin{smallmatrix}1 & j\\ 0 & p\end{smallmatrix}\right)])(z) &= p^{k-1}p^k f\left(\frac{z+j}{p}\right)\\ &= \frac{1}{p}\sum_{n=0}^{\infty} a_n(f)e^{2\pi i n(z+j)/p}\\ &= \frac{1}{p}\sum_{n=0}^{\infty} a_n(f)q_p^n\mu_p^{nj},\end{aligned}$$

where $q_p = e^{2\pi i z/p}$ and $\mu_p = e^{2\pi i/p}$. We use Proposition 2.9 and the observation that the geometric sum $\sum_{j=0}^{p-1}\mu_p^{nj}$ is equal to p when $p \mid n$ and is zero otherwise to obtain

$$(T_p f)(z) = p^{k/2-1}\sum_{j=0}^{p-1}(f|_k[\left(\begin{smallmatrix}1 & j\\ 0 & p\end{smallmatrix}\right)])(z) = \sum_{n\equiv 0 \pmod p} a_n(f)q_p^n = \sum_{n=0}^{\infty} a_{np}(f)q^n.$$

When $p \nmid N$, the series expansion for $T_p f$ is the one given above plus the term

$$\begin{aligned} p^{k/2-1}(f|_k[\left(\begin{smallmatrix} m & n \\ N & p \end{smallmatrix}\right)\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)])(z) &= p^{k/2-1}((\langle p\rangle f)|_k[\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)])(z) \\ &= p^{k-1} z^{-k}(\langle p\rangle f)(pz) \\ &= p^{k-1}\sum_{n=0}^{\infty} a_n(\langle p\rangle f) q^{np}. \end{aligned}$$

□

Corollary 2.12. *If $f \in \mathcal{M}_k(N,\chi)$ has Fourier expansion $f(z) = \sum_{n=0}^{\infty} a_n(f)q^n$, with $q = e^{2\pi i z}$, then $T_p f$ has Fourier expansion*

$$(T_p f)(z) = \sum_{n=0}^{\infty}(a_{np}(f) + \mathbf{1}_N(p)\chi(p)p^{k-1}a_{n/p}(f))q^n,$$

where $a_{n/p} = 0$ whenever n/p is not an integer. This follows directly from the definition of the diamond operator.

Lemma 2.13. *Let $d, e \in (\mathbb{Z}/N\mathbb{Z})^\times$ and p, q be prime. Then*

(1) $\langle d\rangle T_p = T_p\langle d\rangle$,

(2) $\langle d\rangle\langle e\rangle = \langle e\rangle\langle d\rangle = \langle de\rangle$, *and*

(3) $T_pT_q = T_qT_p$.

Proof. To show (1), let $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$ and observe that $\gamma\alpha\gamma^{-1} \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & p \end{smallmatrix}\right) \pmod N$ for any $\gamma \in \Gamma_0(N)$. If $\Gamma_1(N)\alpha\Gamma_1(N) = \bigcup_j \Gamma_1(N)\beta_j$, then by Lemma 2.8 and the fact that $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ we have that

$$\Gamma_1(N)\alpha\Gamma_1(N) = \Gamma_1(N)\gamma\alpha\gamma^{-1}\Gamma_1(N) = \gamma\Gamma_1(N)\alpha\Gamma_1(N)\gamma^{-1} = \gamma\bigcup_j \Gamma_1(N)\beta_j\gamma^{-1} = \bigcup_j \Gamma_1(N)\gamma\beta_j\gamma^{-1}.$$

Comparing the decompositions $\Gamma_1(N)\alpha\Gamma_1(N) = \bigcup_j \Gamma_1(N)\beta_j = \bigcup_j \Gamma_1(N)\gamma\beta_j\gamma^{-1}$, we find that $\bigcup_j \Gamma_1(N)\beta_j\gamma = \bigcup_j \Gamma_1(N)\gamma\beta_j$. Thus for any $f \in \mathcal{M}_k(\Gamma_1(N))$ and any $\gamma \in \Gamma_0(N)$ with lower right entry $\delta \equiv d \pmod N$,

$$\langle d\rangle T_p f = \sum_j f|_k[\beta_j\gamma] = \sum_j f|_k[\gamma\beta_j] = T_p\langle d\rangle.$$

Because $\langle d\rangle$ and T_p commute, it follows that the action of T_p on $\mathcal{M}_k(\Gamma_1(N))$ respects the decomposition $\mathcal{M}_k(\Gamma_1(N)) = \bigoplus_\chi \mathcal{M}_k(N,\chi)$, and similarly for $\mathcal{S}_k(\Gamma_1(N)) = \bigoplus_\chi \mathcal{S}_k(N,\chi)$ and $\mathcal{E}_k(\Gamma_1(N)) = \bigoplus_\chi \mathcal{E}_k(N,\chi)$. That is, T_p maps a χ-eigenspace to itself.

To see (2) and (3), it suffices to show that these equalities of operators hold on elements of $\mathcal{M}_k(N,\chi)$, for each χ.

Indeed, let $f \in \mathcal{M}_k(N,\chi)$. Then

$$\langle d\rangle\langle e\rangle f = \langle d\rangle\chi(e)f = \chi(d)\chi(e)f = \chi(de)f = \langle de\rangle f,$$

and similarly obtain that $\langle d\rangle\langle e\rangle = \langle e\rangle\langle d\rangle$.

To see that T_p and T_q commute, we investigate the Fourier coefficients of $T_p(T_q(f))$ for $f \in \mathcal{M}_k(N,\chi)$. From Corollary 2.12, we have that the n-th Fourier coefficient of $T_p(f)$ is $a_n(T_pf) = a_{np}(f) + \chi(p)p^{k-1}a_{n/p}(f)$, where $a_{n/p}(f) = 0$ whenever n/p is not an integer. Applying this formula twice yields the n-th Fourier coefficient of $T_p(T_q(f))$:

$$\begin{aligned} a_n(T_p(T_qf)) &= a_{np}(T_qf) + \chi(p)p^{k-1}a_{n/p}(T_qf) \\ &= a_{npq}(f) + \chi(q)q^{k-1}a_{np/q}(f) \\ &\quad + \chi(p)p^{k-1}(a_{nq/p}(f) + \chi(q)q^{k-1}a_{n/pq}(f)) \\ &= a_{npq}(f) + \chi(q)q^{k-1}a_{np/q}(f) + \chi(p)p^{k-1}a_{nq/p}(f) + \chi(pq)(pq)^{k-1}a_{n/pq}(f). \end{aligned}$$

Since the above expression is symmetric in p and q, we obtain the result. □

Definition 2.14. The ***Hecke operator*** $T_n \colon \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$ for $n \in \mathbb{Z}^+$ is defined inductively. Let $T_1 = \mathrm{id}_{\mathcal{M}_k(\Gamma_1(N))}$ (the identity operator), and above we had defined $T_p f = f|_k[\Gamma_1(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\Gamma_1(N)]$ for primes p. For prime powers, let

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1}\langle p \rangle T_{p^{r-2}} \quad \text{for } r \geq 2.$$

Then for $n = \prod_i p_i^{r_i}$, define

$$T_n = \prod_i T_{p_i^{r_i}},$$

where the previous lemma justifies the multiplicative notation above. †

By Lemma 2.13, the mapping $n \mapsto \langle n \rangle$ is totally multiplicative; that is, $\langle nm \rangle = \langle n \rangle \langle m \rangle$ for all positive integers n, m. The same lemma implies that the mapping $n \mapsto T_n$ is multiplicative; that is, for n, m coprime, $T_{nm} = T_n T_m$.

Definition 2.15. The ***Hecke algebra*** $\mathcal{R}(N)$ is the polynomial ring

$$\mathcal{R}(N) = \mathbb{Z}[T_p, \langle q \rangle : p, q \in \mathbb{P}, q \nmid N].$$

From previous results it follows that $\mathcal{R}(N)$ is a commutative unital ring. †

Often (and especially so in the next section), we will restrict the action of the Hecke operators to an arbitrary χ-eigenspace. We use the same symbols to denote the restrictions of these operators, since it will be clear from context when we are taking the restriction.

In [Miy05], the Hecke algebra is generated by Hecke operators $T(p), T(p,p)$ that are defined differently. The Hecke operators $T(p), T(p,p)$ are related to the Hecke operators $T_p, \langle p \rangle$ by the equations $T(p) = T_p$ and $T(p,p) = p^{k-2}\langle p \rangle$.

Lemma 2.16. *Let K be a commutative unital ring, and assume that two sequences $\{t_n\}_{n=1}^{\infty}, \{d_n\}_{n=1}^{\infty}$ of elements of K satisfy the following conditions:*

(i) $t_1 = d_1 = 1$, *and*

(ii) $d_{mn} = d_m d_n$ *for any positive integers m, n.*

Then the following are equivalent:

(1) *If* $\gcd(m,n) = 1$, *then* $t_{mn} = t_m t_n$ *and*

$$t_p t_{p^e} = t_{p^{e+1}} + p d_p t_{p^{e-1}}$$

for all prime numbers p and all positive integers e.

(2) *The formal Dirichlet series $\sum_{n=1}^{\infty} t_n n^{-s}$ has formal Euler product*

$$\sum_{n=1}^{\infty} t_n n^{-s} = \prod_{p \in \mathbb{P}} (1 - t_p p^{-s} + p d_p p^{-2s})^{-1}.$$

(3) *For any positive integers m, n,*

$$t_m t_n = \sum_{\substack{l>0 \\ l \mid \gcd(m,n)}} l d_l t_{mn/l^2}.$$

Proof. We show that (1) implies (2). From the first condition of (1), we have formally that

$$\sum_{n=1}^{\infty} t_n n^{-s} = \prod_{p\in\mathbb{P}} \Big(\sum_{e=0}^{\infty} t_{p^e} p^{-es}\Big).$$

From the second condition of (1), we have

$$(1 - t_p p^{-s} + p d_p p^{-2s})\Big(\sum_{e=0}^{\infty} t_{p^e} p^{-es}\Big) = 1,$$

from which (2) follows.

We show that (2) implies (3). Formal Dirichlet series and formal Euler products are elements of the ring of formal power series $K[[p^{-s} : p \in \mathbb{P}]]$. Finding inverses in $K[[p^{-s}]]$ of the elements $1 - t_p p^{-s} + p d_p p^{-2s}$ recursively (cf. [DF04, Exercise 7.2.3(c)]), and comparing coefficients of

$$\sum_{n=1}^{\infty} t_n n^{-s} = \prod_{p\in\mathbb{P}} (1 - t_p p^{-s} + p d_p p^{-2s})^{-1}$$

reveals that the sequence $\{t_n\}_{n=1}^{\infty}$ is multiplicative. That is, if $\gcd(m, n) = 1$, then $t_{mn} = t_m t_n$.

Let $m = \prod_{p\in\mathbb{P}} p^e$ and $n = \prod_{p\in\mathbb{P}} p^f$ be the prime factorizations of m and n. Then

$$\sum_{\substack{l>0\\ l\mid\gcd(m,n)}} l d_l t_{mn/l^2} = \prod_{p\in\mathbb{P}} \Big(\sum_{0\le g\le\min\{e,f\}} p^g d_{p^g} t_{p^{e+f-2g}}\Big).$$

Therefore it suffices to prove that (2) implies (3) in the case that m and n are powers of the same prime p. By assumption, we have

$$(1 - t_p p^{-s} + p d_p p^{-2s})^{-1} = \sum_{e=0}^{\infty} t_{p^e} p^{-es}.$$

Let τ_p and δ_p be two indeterminates over $\mathbb{Q}$, and define a (unital) ring homomorphism $\psi\colon \mathbb{Z}[\tau_p, \delta_p] \to K$ by $\psi(\tau_p) = t_p$ and $\psi(\delta_p) = d_p$. Define the elements τ_{p^e} and δ_{p^e} of $\mathbb{Z}[\tau_p, \delta_p]$ by $\delta_{p^e} = (\delta_p)^e$ and by the formal power series equality

$$\sum_{e=0}^{\infty} \tau_{p^e} p^{-es} = (1 - \tau_p p^{-s} + p\delta_p p^{-2s})^{-s}. \tag{2.1}$$

It follows that $\psi(\tau_{p^e}) = t_{p^e}$ and $\psi(\delta_{p^e}) = d_{p^e}$.

Let u, v be indeterminates over $\mathbb{Q}$, and define a ring homomorphism $\phi\colon \mathbb{Z}[\tau_p, \delta_p] \to \mathbb{Q}[u, v]$ by $\phi(\tau_p) = u + v$ and $\phi(\delta_p) = uv/p$. Since $u + v$ and uv/p are algebraically independent over $\mathbb{Q}$, ϕ is injective. Viewing $\mathbb{Z}[\tau_p, \delta_p]$ as a subring of $\mathbb{Q}[u, v]$, we may factor $1 - \tau_p p^{-s} + p\delta_p p^{-2s}$ into $(1 - up^{-s})(1 - vp^{-s})$. Inverting this element and comparing coefficients in (2.1), we find that

$$\tau_{p^e} = \sum_{i+j=e} u^i v^j = (u^{e+1} - v^{e+1})/(u - v).$$

Assume that $0 \le e \le f$. Then

$$\begin{aligned}
\tau_{p^e}\tau_{p^f} &= \left(\sum_{i+j=e} u^i v^j\right) \cdot (u^{f+1} - v^{f+1})/(u-v) \\
&= \left(u^{f+1}\sum_{j=0}^{e} u^{e-j}v^j - v^{f+1}\sum_{j=0}^{e} u^j v^{e-j}\right)\Big/(u-v) \\
&= \sum_{g=0}^{e} u^g v^g (u^{e+f-2g+1} - v^{e+f-2g+1})/(u-v) \\
&= \sum_{g=0}^{e} p^g \delta_{p^g}\tau_{p^{e+f-2g}}.
\end{aligned}$$

By taking ψ on both sides of the above equation, obtain

$$t_{p^e}t_{p^f} = \sum_{g=0}^{e} p^g d_{p^g} t_{p^{e+f-2g}}$$

as desired. So in all cases, (2) implies (3).

To see that (3) implies (1), observe that (1) is a special case of (3), with $m = p$ and $n = p^e$. □

Theorem 2.17. *We have*

(1) $T_m T_n = \sum_{\substack{l>0 \\ l\mid\gcd(m,n) \\ \gcd(l,N)=1}} l^{k-1}\langle l\rangle T_{mn/l^2}$, *and*

(2) *the formal Dirichlet series* $\sum_{n=1}^{\infty} T_n n^{-s}$ *has the formal Euler product*

$$\sum_{n=1}^{\infty} T_n n^{-s} = \prod_{p\nmid N}(1 - T_n p^{-s} + (p^{k-2}\langle p\rangle)p^{1-2s})^{-1} \cdot \prod_{p\mid N}(1 - T_p p^{-s})^{-1}$$

Proof. Apply the previous lemma with

$$K = \mathcal{R}(N), \quad t_n = T_n, \quad \text{and} \quad d_n = \begin{cases} n^{k-2}\langle n\rangle & \text{if } \gcd(n,N) = 1, \\ 0 & \text{if } \gcd(n,N) \ne 1 \end{cases}$$

to obtain the result. □

We record one result (without proof) which will be useful in the next result. For $f \in \mathcal{M}_k(N,\chi)$, we have

$$(T_n f)(z) = n^{k-1} \sum_{\substack{d>0 \\ d\mid n \\ ad=n}} \sum_{b=0}^{d-1} \chi(a) d^{-k} f((az+b)/d).$$

The following result is similar to Lemma 2.11, but for T_n acting on $\mathcal{M}_k(N,\chi)$.

Lemma 2.18. *Let f be an element of $\mathcal{M}_k(N,\chi)$, and let*

$$f(z) = \sum_{n=0}^{\infty} c_n e^{2\pi i n z}, \quad (T_m f)(z) = \sum_{n=0}^{\infty} b_n e^{2\pi i n z}$$

be Fourier series expansions. Then

$$b_n = \sum_{\substack{d>0 \\ d\mid\gcd(m,n)}} \chi(d) d^{k-1} c_{mn/d^2}.$$

Proof. Observe that $f((az+b)/d) = \sum_{n=0}^{\infty} c_n e^{2\pi in(az+b)/d}$. Then by the explicit action of T_n on elements of $\mathcal{M}_k(N,\chi)$ (which appears just before this lemma), we have

$$(T_m f)(z) = m^{k-1} \sum_{\substack{d>0 \\ d|n}} \sum_{b=0}^{d-1} \chi(m/d) d^{-k} \sum_{n=0}^{\infty} c_n e^{2\pi in((m/d)z+b)/d}.$$

Then use the fact that $\sum_{b=0}^{d-1} e^{2\pi inb/d}$ is equal to d if $d \mid n$ and is 0 otherwise to simplify the above expression into

$$\sum_{n=0}^{\infty} \sum_{\substack{d>0 \\ d|\gcd(m,n)}} \chi(m/d)(m/d)^{k-1} c_n e^{2\pi i(nm/d^2)z}.$$

Change summation variables to obtain

$$\sum_{n=0}^{\infty} \sum_{a>0 a|\gcd(m,n)} \chi(a) a^{k-1} c_{dn/a} e^{2\pi inz},$$

and with $ad = m$, it follows that $c_{dn/a} = c_{mn/a^2}$, and the result follows. □

Lemma 2.19. *Let $f(z) = \sum_{n=0}^{\infty} c_n e^{2\pi inz}$ be an element of $\mathcal{M}_k(N,\chi)$, and P a set of prime numbers where $T_p f = t_p f$ for $p \in P$, $t_p \in \mathbb{C}$. Then*

(1) *If all prime factors of a positive integer m lie in P, then f is an eigenfunction of T_m. In this case, let $T_m f = t_m f$ for some $t_m \in \mathbb{C}$, from which it follows that $c_m = t_m c_1$.*

(2) *We have $L(s,f) = \prod_{p\in P}(1 - t_p p^{-s} + \chi(p)p^{k-1-2s})^{-1} \cdot \sum_n' c_n n^{-s}$, where the summation $\sum_n'$ is taken over the positive integers coprime to every element of P.*

Proof. The first claim in (1) is clear. Let n be a positive integer coprime to m. Comparing the n-th Fourier coefficients of $T_m f$ and $t_m f$, we obtain $t_m c_n = c(mn)$ by Lemma 2.18. By taking $n = 1$, the second claim in (1) follows.

By the equality $t_m c_n = c(mn)$, we have the formal equality

$$L(s,f) = \Bigl(\sum_m{}'' t_m m^{-s}\Bigr) \cdot \Bigl(\sum_n{}' c_n n^{-s}\Bigr),$$

where the summation $\sum_m''$ is taken over 1 and the positive integers whose prime factors are all contained in P, and the summation $\sum_n'$ is taken over the positive integers copimre to all primes in P. Then by Theorem 2.17(1),

$$t_n t_m = \sum_{\substack{l>0 \\ l|\gcd(m,n) \\ \gcd(l,N)=1}} \chi(l) l^{k-1} t_{mn/l^2}$$

for m, n in the indexing sets for the summations $\sum_m''$ and $\sum_n'$, respectively. So formally obtain

$$\sum_m{}'' t_m m^{-s} = \prod_{p\in P}(1 - t_p p^{-s} + \chi(p)p^{k-1-2s})^{-1}$$

by a similar argument as in Lemma 2.16. Furthermore, if $c_n = O(n^\alpha)$ for some α, then the equality above holds on $\mathrm{Re}(s) > \alpha + 1$. If f is a cusp form, then we have this growth condition on c_n due to Corollary 1.11. We do not prove the result when f is not a cusp form. □

The next lemma gives a necessary and sufficient condition for a modular form $f \in \mathcal{M}_k(N,\chi)$ to be a simultaneous eigenfunction of all of the Hecke operators T_n, in terms of being able to write down an Euler product for the L-function for f. More importantly, the lemma shows that the eigenvalues of such an eigenfunction are proportional to the Fourier coefficients of the modular form.

Theorem 2.20. *Let $f(z) = \sum_{n=0}^{\infty} c_n e^{2\pi i n z}$ be a nonzero element of $\mathcal{M}_k(N,\chi)$. Then the following are equivalent:*

(1) *$f(z)$ is a common eigenfunction of every Hecke operator T_n;*

(2) *$c_1 \neq 0$ and*

$$L(s,f) = c_1 \prod_{p\in\mathbb{P}} (1 - t_p p^{-s} + \chi(p) p^{k-1-2s})^{-1}, \quad t_n = \frac{c_n}{c_1}.$$

Moreover, if $f(z)$ satisfies the above conditions, then $T_n f = t_n f$ for all $n \geq 1$.

Proof. Assume that (1) holds, and let $T_n f = t_n f$. By Lemma 2.19, we have $c_n = t_n c_1$ for $n \geq 1$. Then if $c_1 = 0$, $f(z) = c_0$. Since $k \geq 1$, we have in this case that $f(z) = 0$, which cannot happen by assumption. Therefore $c_1 \neq 0$. Obtain (2) from Lemma 2.19(2), taking P to be the set of all prime numbers $\mathbb{P}$.

Now assume that (2) holds, and let $t_n = c_n/c_1$ for $n \geq 1$. Then

$$\sum_{n=1}^{\infty} t_n n^{-s} = \prod_{p\in\mathbb{P}} (1 - t_p p^{-s} + \chi(p) p^{k-1-2s})^{-1}.$$

By Lemma 2.16,

$$t_m t_n = \sum_{\substack{d>0 \\ d|\gcd(m,n)}} d^{k-1}\chi(d) t_{mn/d^2},$$

and multiplying both sides of this equality by c_1 we obtain

$$t_m c_1 = \sum_{\substack{d>0 \\ d|\gcd(m,n)}} d^{k-1}\chi(d) c_{mn/d^2}.$$

But the expression on the right hand side of this equality is equal to the n-th Fourier coefficient of $T_m f$ by Lemma 2.18. Let b_0 denote the constant term of the Fourier expansion of $T_m f$. Then $(T_m f)(z) - t_m f = b_0 - c_0$, and since $T_m f - t_m f$ is an element of $\mathcal{M}_k(N,\chi)$ with $k \geq 1$, we have that $b_0 = c_0$. Hence $T_m f = t_m f$ as desired. □

2.3 The Petersson inner product, adjoints of Hecke operators

We study the space $\mathcal{S}_k(\Gamma_1(N))$ by endowing it with an inner product. Define the ***hyperbolic measure*** μ on $\mathcal{H}$ by $\mathrm{d}\mu(z) = \mathrm{d}x\mathrm{d}y/y^2$ for $z = x+iy \in \mathcal{H}$ (we will sometimes suppress the (z)). This measure is invariant under the action of $\mathrm{GL}_2^+(\mathbb{R})$ on $\mathcal{H}$: For $\alpha \in \mathrm{GL}_2^+(\mathbb{R})$ and $z = x+iy \in \mathcal{H}$, let $\alpha(z) = \sigma(x,y) + i\tau(x,y)$. A few computations using Wirtinger derivatives reveal that $\left|\frac{\partial(\sigma,\tau)}{\partial(x,y)}\right| = \left|\frac{\mathrm{d}\alpha}{\mathrm{d}z}\right|^2 = \left(\det\alpha/|j(\alpha,z)|^2\right)^2$ and $\tau(z) = y\det\alpha/|j(\alpha,z)|^2$. Then for a measurable set A in $\mathcal{H}$,

$$\mu(\alpha(A)) = \int_{\alpha(A)} \frac{\mathrm{d}\sigma\mathrm{d}\tau}{\tau^2} = \int_A \left|\frac{\partial(\sigma,\tau)}{\partial(x,y)}\right| \frac{\mathrm{d}x\mathrm{d}y}{(\tau(x,y))^2} = \int_A \frac{(\det\alpha)^2}{|j(\alpha,z)|^4} \frac{|j(\alpha,z)|^4\mathrm{d}x\mathrm{d}y}{(\det\alpha)^2 y^2} = \int_A \frac{\mathrm{d}x\mathrm{d}y}{y^2} = \mu(A)$$

as desired. In particular $\mathrm{d}\mu$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant. Since $\mathbb{Q}\cup\{\infty\}$ is countable, its measure is zero, so we may integrate over the extended upper half plane $\mathcal{H}^*$ with respect to μ.

Recall that a fundamental domain for $\mathcal{H}^*$ under the action of $\mathrm{SL}_2(\mathbb{Z})$ is given by

$$\mathcal{D}^* = \{z \in \mathcal{H} : |\mathrm{Re}(z)| \leq 1/2, |z| \geq 1\} \cup \{\infty\};$$

that is, any point of $\mathcal{H}$ is sent to a point in $\mathcal{D}$ by a suitable element of $\mathrm{SL}_2(\mathbb{Z})$, which is unique for most points of $\mathcal{H}$ (there are a few cases involving points on the boundary of $\mathcal{D}$). Every point $s \in \mathbb{Q}\cup\{\infty\}$ may be sent to ∞ by suitable elements of $\mathrm{SL}_2(\mathbb{Z})$. We show that the integral $\int_{\mathcal{D}^*} \varphi(\alpha(z))\mathrm{d}\mu$ converges for any continuous, bounded function $\varphi\colon \mathcal{H} \to \mathbb{C}$ and any $\alpha \in \mathrm{SL}_2(\mathbb{Z})$: Choose $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ such that $\gamma^{-1}\mathcal{D}^*$ is a compact set. By the invariance of the measure under the action of $\mathrm{SL}_2(\mathbb{Z})$, we have

$$\int_{\mathcal{D}^*} \varphi(\alpha(z))\mathrm{d}\mu = \int_{\gamma^{-1}D^*} \varphi(\alpha(\gamma(z)))\mathrm{d}\mu,$$

from which it follows that the integral converges.

Let Γ be a congruence subgroup, and let $\{\alpha_j\}$ be a set of representatives for the coset space $\{\pm I\}\,\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$; that is, we have the disjoint union $\mathrm{SL}_2(\mathbb{Z}) = \bigsqcup_j \{\pm I\}\,\Gamma\alpha_j$. If φ is Γ-invariant, then the sum $\sum_j \int_{\mathcal{D}^*} \varphi(\alpha_j(z))\mathrm{d}\mu$ is independent of the choice of coset representatives α_j. Since $\mathrm{d}\mu$ is $\mathrm{SL}_2(\mathbb{Z})$-invariant, the sum is equal to $\int_{\bigcup_j \alpha_j(\mathcal{D}^*)} \varphi(z)\mathrm{d}\mu$. Since $\bigcup_j \alpha_j(\mathcal{D}^*)$ represents the modular curve $X(\Gamma)$ up to identification of boundaries, we define

$$\int_{X(\Gamma)} \varphi(z)\mathrm{d}\mu = \int_{\bigcup_j \alpha_j(\mathcal{D}^*)} \varphi(z)\mathrm{d}\mu = \sum_j \int_{\mathcal{D}^*} \varphi(\alpha_j(z))\mathrm{d}\mu.$$

In particular the volume of $X(\Gamma)$ is given by $V_\Gamma = \int_{X(\Gamma)} \mathrm{d}\mu = [\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\,\Gamma]V_{\mathrm{SL}_2(\mathbb{Z})}$.

Observe that for any $f, g \in \mathcal{S}_k(\Gamma)$ for a congruence subgroup Γ, the function $\varphi(z) = f(z)\overline{g(z)}(\mathrm{Im}(z))^k$ for $z \in \mathcal{H}$ is continuous, and more importantly, Γ-invariant. Indeed, for any $\gamma \in \Gamma$, we have

$$\begin{aligned}
\varphi(\gamma(z)) &= f(\gamma(z))\overline{g(\gamma(z))}(\mathrm{Im}(\gamma(z)))^k \\
&= (f|_k[\gamma])(z)j(\gamma,z)^k\overline{(g|_k[\gamma])(z)j(\gamma,z)}^k(\mathrm{Im}(z))^k|j(\gamma,z)|^{-2k} \\
&= (f|_k[\gamma])(z)\overline{(g|_k[\gamma])(z)}(\mathrm{Im}(z))^k \\
&= \varphi(z).
\end{aligned}$$

To show that φ is bounded on $\mathcal{H}$, we show that φ is bounded on $\bigcup_j \alpha_j(\mathcal{D})$, which is a finite union. Therefore it suffices to show that for any $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, the function $\varphi \circ \alpha$ is bounded on $\mathcal{D}$. On any compact subset of $\mathcal{D}$, continuity of $\varphi \circ \alpha$ implies boundedness. For the neighborhoods $\{\mathrm{Im}(z) > M\}$ of $i\infty$, note that the Fourier expansions

$$(f|_k[\alpha])(z) = \sum_{n=1} a_n(f|_k[\alpha])q_h^n, \quad (g|_k[\alpha])(z) = \sum_{n=1} a_n(g|_k[\alpha])q_h^n \quad \text{for } q_h = e^{2\pi i z/h} \text{ for some } h \in \mathbb{Z}^+$$

are of order $O(q_h)$ as $\mathrm{Im}(z) \to \infty$. It follows that $\varphi(\alpha(z)) = (f|_k[\gamma])(z)\overline{(g|_k[\gamma])(z)}(\mathrm{Im}(z))^k = O(q_h)^2(\mathrm{Im}(z))^k$. Moreover, since $|q_h| = e^{-2\pi\,\mathrm{Im}(z)/h}$, $\varphi(\alpha(z)) \to 0$ as $\mathrm{Im}(z) \to \infty$, from which it follows $\varphi \circ \alpha$ is bounded on the neighborhoods $\{\mathrm{Im}(z) > M\}$ of $i\infty$ of $\mathcal{D}$, hence on all of $\mathcal{D}$.

Definition 2.21. The ***Petersson inner product*** $\langle\cdot,\cdot\rangle_\Gamma\colon \mathcal{S}_k(\Gamma) \times \mathcal{S}_k(\Gamma) \to \mathbb{C}$ for a congruence subgroup Γ is given by

$$\langle f, g\rangle_\Gamma = \frac{1}{V_\Gamma}\int_{X(\Gamma)} f(z)\overline{g(z)}(\mathrm{Im}(z))^k\mathrm{d}\mu.$$

We omit the subscript $_\Gamma$ in $\langle\cdot,\cdot\rangle_\Gamma$ when it is clear from context. †

One can check that the Petersson inner product is a Hermitian inner product. If we have the containment $\Gamma' \subset \Gamma$ of congruence subgroups, then $\langle\cdot,\cdot\rangle_{\Gamma'} = \langle\cdot,\cdot\rangle_\Gamma$ on $\mathcal{S}_k(\Gamma)$: If $\{\beta_m\}$ is a set of coset representatives for $\{\pm I\}\,\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$ and $\{\gamma_j\}$ is a set of coset representatives for $\{\pm I\}\,\Gamma'\backslash \{\pm I\}\,\Gamma$, then $\{\gamma_j\beta_m\}$ form a set of coset representatives for $\{\pm I\}\,\Gamma'\backslash \mathrm{SL}_2(\mathbb{Z})$, from which we obtain

$$\begin{aligned}
\frac{1}{V_\Gamma}\int_{X(\Gamma)} f(z)\overline{g(z)}(\mathrm{Im}(z))^k\mathrm{d}\mu &= \frac{[\{\pm I\}\,\Gamma : \{\pm I\}\,\Gamma']}{V_{\Gamma'}}\sum_m \int_{\mathcal{D}^*} f(\beta(z))\overline{g(\beta(z))}(\mathrm{Im}(\beta(z)))^k\mathrm{d}\mu \\
&= \frac{1}{V_{\Gamma'}}\sum_{j,m}\int_{\mathcal{D}^*} f((\gamma\beta)(z))\overline{g((\gamma\beta)(z))}(\mathrm{Im}((\gamma\beta)(z)))^k\mathrm{d}\mu = \frac{1}{V_{\Gamma'}}\int_{X(\Gamma')} f(z)\overline{g(z)}(\mathrm{Im}(z))^k\mathrm{d}\mu
\end{aligned}$$

as expected.

Recall that if T is a linear operator on the inner product space V, then there exists a unique operator T^* on V called the adjoint of T, that satisfies $\langle Tv, w\rangle = \langle v, T^*w\rangle$ for all $v, w \in V$. If T commutes with T^*, we say that T is a normal operator. Give $\mathcal{S}_k(\Gamma_1(N))$ the Petersson inner product. We show that the Hecke operators $\langle n\rangle$ and T_n for n coprime to N are normal operators.

Let Γ be a congruence subgroup, and write $\mathrm{SL}_2(\mathbb{Z}) = \bigcup_j \{\pm I\}\,\Gamma\alpha_j$ for some representatives α_j of the coset space $\{\pm I\}\,\Gamma\backslash \mathrm{SL}_2(\mathbb{Z})$. If $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$, then the map $\mathcal{H} \to \mathcal{H}$ given by $z \mapsto \alpha(z)$ induces a bijection $\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}^* \to X(\Gamma)$. It follows that the union $\bigcup_j \alpha^{-1}\alpha_j(\mathcal{D}^*)$ up to some boundary identifications is in bijection with $\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}^*$. For continuous, bounded, $\alpha^{-1}\Gamma\alpha$-invariant functions $\varphi\colon \mathcal{H} \to \mathbb{C}$ define

$$\int_{\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}^*} \varphi(z)\mathrm{d}\mu = \sum_j \int_{\mathcal{D}^*} \varphi(\alpha^{-1}\alpha_j(z))\mathrm{d}\mu.$$

Lemma 2.22. *Let Γ be a congruence subgroup and let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$.*

(1) *If $\varphi\colon \mathcal{H} \to \mathbb{C}$ is continuous, bounded, and Γ-invariant, then*

$$\int_{\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}^*} \varphi(\alpha(z))\mathrm{d}\mu = \int_{X(\Gamma)} \varphi(z)\mathrm{d}\mu.$$

(2) *If $\alpha^{-1}\Gamma\alpha \subset \mathrm{SL}_2(\mathbb{Z})$, then $V_{\alpha^{-1}\Gamma\alpha} = V_\Gamma$ and $[\mathrm{SL}_2(\mathbb{Z}) : \alpha^{-1}\Gamma\alpha] = [\mathrm{SL}_2(\mathbb{Z}) : \Gamma]$.*

(3) *There exist $\beta_1, \dots, \beta_n \in \mathrm{GL}_2^+(\mathbb{Q})$ with $n = [\Gamma : \alpha^{-1}\Gamma\alpha \cap \Gamma] = [\Gamma : \alpha\Gamma\alpha^{-1} \cap \Gamma]$, such that*

$$\Gamma\alpha\Gamma = \bigsqcup_j \Gamma\beta_j = \bigsqcup_j \beta_j\Gamma.$$

Proof. From the discussion above, (1) follows immediately. The first equality in (2) follows from (1), and the second equality is a consequence of the equation $V_\Gamma = [\mathrm{SL}_2(\mathbb{Z}) : \{\pm I\}\,\Gamma]V_{\mathrm{SL}_2(\mathbb{Z})}$ and the observation that $-I \in \alpha^{-1}\Gamma\alpha$ if and only if $-I \in \Gamma$.

To obtain (3), we apply (2) with $\alpha\Gamma\alpha^{-1} \cap \Gamma$ in place of Γ to obtain

$$[\mathrm{SL}_2(\mathbb{Z}) : \alpha^{-1}\Gamma\alpha \cap \Gamma] = [\mathrm{SL}_2(\mathbb{Z}) : \alpha\Gamma\alpha^{-1} \cap \Gamma],$$

from which we deduce that $[\Gamma : \alpha^{-1}\Gamma\alpha \cap \Gamma] = [\Gamma : \alpha\Gamma\alpha^{-1} \cap \Gamma]$. Thus there exist coset representatives $\gamma_1, \dots, \gamma_n$ and $\eta_1^{-1}, \dots, \eta_n^{-1}$ in Γ for the coset spaces $(\alpha^{-1}\Gamma\alpha \cap \Gamma)\backslash\Gamma$ and $(\alpha\Gamma\alpha^{-1} \cap \Gamma)\backslash\Gamma$ respectively. That is,

$$\Gamma = \bigsqcup_j (\alpha^{-1}\Gamma\alpha \cap \Gamma)\gamma_j = \bigsqcup_j (\alpha\Gamma\alpha^{-1} \cap \Gamma)\eta_j^{-1}.$$

In Lemma 2.2, set $\Gamma_1 = \Gamma_2 = \Gamma$ to obtain

$$\Gamma\alpha\Gamma = \bigsqcup_j \Gamma\alpha\gamma_j \quad \text{and} \quad \Gamma\alpha^{-1}\Gamma = \bigsqcup_j \Gamma\alpha^{-1}\eta_j^{-1}.$$

The second equation implies that $\Gamma\alpha\Gamma = \bigsqcup_j \eta_j\alpha\Gamma$. For each j, the intersection $\Gamma\alpha\gamma_j \cap \eta_j\alpha\Gamma$ is nonempty, since otherwise we would have $\Gamma\alpha\gamma_j \subset \bigsqcup_{i\neq j} \eta_i\alpha\Gamma$. Multiplying this equality from the right by Γ gives $\Gamma\alpha\Gamma \subset \bigsqcup_{i\neq j} \eta_i\alpha\Gamma$, a contradiction. So for each j, choose some $\beta_j \in \Gamma\alpha\gamma_j \cap \eta_j\alpha\Gamma$, from which we obtain $\Gamma\alpha\Gamma = \bigsqcup_j \Gamma\beta_j = \bigsqcup_j \beta_j\Gamma$. ☐

The following proposition will be used to compute adjoints of the Hecke operators.

Proposition 2.23. *Let Γ be a congruence subgroup and let $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$.*

(1) *If* $\alpha^{-1}\Gamma\alpha \subset \mathrm{SL}_2(\mathbb{Z})$*, then for all* $f \in \mathcal{S}_k(\Gamma)$ *and* $g \in \mathcal{S}_k(\alpha^{-1}\Gamma\alpha)$

$$\langle f|_k[\alpha], g\rangle_{\alpha^{-1}\Gamma\alpha} = \langle f, g|_k[\det(\alpha)\alpha^{-1}]\rangle_\Gamma.$$

(2) *For all* $f, g \in \mathcal{S}_k(\Gamma)$*,*

$$\langle f|_k[\Gamma\alpha\Gamma], g\rangle = \langle f, g|_k[\Gamma\det(\alpha)\alpha^{-1}\Gamma]\rangle.$$

We have $|_k[\Gamma\alpha\Gamma]^* = |_k[\Gamma\det(\alpha)\alpha^{-1}\Gamma]$*. If* $\alpha^{-1}\Gamma\alpha = \Gamma$*, then* $|_k[\alpha]^* = |_k[\det(\alpha)\alpha^{-1}]$*.*

Proof. To prove (1), note that α' acts on elements of $\mathcal{H}^*$ in the same way as α^{-1}, and apply Lemma 2.22(1) to obtain

$$\begin{aligned}\int_{\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}^*}(f|_k[\alpha])(z)\overline{g(z)}(\mathrm{Im}(z))^k\mathrm{d}\mu &= \int_{\alpha^{-1}\Gamma\alpha\backslash\mathcal{H}^*}(\det\alpha)^{k/2}j(\alpha,z)^{-k}f(\alpha(z))\overline{g(z)}(\mathrm{Im}(z))^k\mathrm{d}\mu\\ &= \int_{X(\Gamma)} f(z)(\det\alpha)^{k/2}j(\alpha,\alpha'(z))^{-k}\overline{g(\alpha'(z))}(\mathrm{Im}(\alpha'(z)))^k\mathrm{d}\mu\end{aligned}$$

Recall the identities $j(\alpha\alpha', z) = j(\alpha, \alpha'(z))j(\alpha', z)$ and $\mathrm{Im}(\alpha'(z)) = (\det\alpha')\,\mathrm{Im}(z)/|j(\alpha', t)|^2$, and observe that $\det\alpha' = \det\alpha$. Continuing with the computation gives

$$\begin{aligned}&= \int_{X(\Gamma)} f(z)\overline{(\det\alpha)^{k/2}j(\alpha',z)^{-k}g(\alpha'(z))}(\mathrm{Im}(z))^k\mathrm{d}\mu\\ &= \int_{X(\Gamma)} f(z)\overline{(g|_k[\alpha'])(z)}(\mathrm{Im}(z))^k\mathrm{d}\mu.\end{aligned}$$

Since $V_{\alpha^{-1}\Gamma\alpha} = V_\Gamma$ by Lemma 2.22(2), the result follows.

To show part (2), from Lemma 2.22(3), there exist $\{\beta_j\}$ for which $\Gamma\alpha\Gamma = \bigsqcup_j \beta_j\Gamma$, from which we deduce that $\Gamma\alpha'\Gamma = \bigsqcup_j \Gamma(\det\beta_j)\beta_j^{-1}$. Then apply part (1) of this lemma with each $\beta_j\Gamma\beta_j^{-1}\cap\Gamma$ in place of Γ in the following:

$$\begin{aligned}\langle f|_k[\Gamma\alpha\Gamma], g\rangle_\Gamma &= (\det\alpha)^{k/2-1}\sum_j\langle f|_k[\beta_j], g\rangle_{\Gamma\cap\beta_j^{-1}\Gamma\beta_j}\\ &= (\det\alpha')^{k/2-1}\sum_j\langle f, g|_k[(\det\beta_j)\beta_j^{-1}]\rangle_{\beta_j\Gamma\beta_j^{-1}\cap\Gamma}\\ &= \langle f, g|_k[\Gamma\alpha'\Gamma]\rangle_\Gamma.\end{aligned}$$

□

We obtain the adjoints of the Hecke operators without much trouble using the above proposition.

Theorem 2.24. *For* $p \nmid N$*, the Hecke operators* $\langle p\rangle, T_p\colon \mathcal{S}_k(\Gamma_1(N)) \to \mathcal{S}_k(\Gamma_1(N))$ *have adjoints*

$$\langle p\rangle^* = \langle p\rangle^{-1} \quad \text{and} \quad T_p^* = \langle p\rangle^{-1}T_p.$$

Furthermore, one can show that $T_n^* = \langle n\rangle^{-1}T_n$ *for* n *coprime to* N*. It follows that the Hecke operators* $\langle n\rangle, T_n$ *for* n *coprime to* N *are normal operators.*

Proof. Let $f, g \in \mathcal{S}_k(\Gamma_1(N))$. Since $\Gamma_1(N)$ is normal in $\Gamma_0(N)$, we have by Proposition 2.23(1) that $\langle p\rangle^*$ is given by $|_k[\alpha]^* = |_k[\alpha^{-1}]$, where α is any element of $\Gamma_0(N)$ such that $\alpha \equiv \left(\begin{smallmatrix} * & * \\ 0 & p\end{smallmatrix}\right) \pmod N$. But the action of $\langle p\rangle^{-1}$ is exactly $|_k[\alpha^{-1}]$.

From Proposition 2.23(2), we have T_p^* given by

$$|_k[\Gamma_1(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p\end{smallmatrix}\right)\Gamma_1(N)]^* = |_k[\Gamma_1(N)\left(\begin{smallmatrix} p & 0 \\ 0 & 1\end{smallmatrix}\right)\Gamma_1(N)].$$

Choose m, n with $mp - nN = 1$, and observe that $\left(\begin{smallmatrix} p & 0 \\ 0 & 1\end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & n \\ N & mp\end{smallmatrix}\right)^{-1}\left(\begin{smallmatrix} 1 & 0 \\ 0 & p\end{smallmatrix}\right)\left(\begin{smallmatrix} p & n \\ N & m\end{smallmatrix}\right)$, with $\left(\begin{smallmatrix} 1 & n \\ N & mp\end{smallmatrix}\right)^{-1} \in \Gamma_1(N)$ and $\left(\begin{smallmatrix} p & n \\ N & m\end{smallmatrix}\right) \in \Gamma_0(N)$. Thus with $\Gamma_1(N)$ normal in $\Gamma_0(N)$, we have

$$\Gamma_1(N)\left(\begin{smallmatrix} p & 0 \\ 0 & 1\end{smallmatrix}\right)\Gamma_1(N) = \Gamma_1(N)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p\end{smallmatrix}\right)\Gamma_1(N)\left(\begin{smallmatrix} p & n \\ N & m\end{smallmatrix}\right).$$

If $\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)=\bigsqcup_j \Gamma_1(N)\beta_j$, then $\Gamma_1(N)\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)\Gamma_1(N)=\bigsqcup_j \Gamma_1(N)\beta_j\left(\begin{smallmatrix}p&n\\N&m\end{smallmatrix}\right)$. Since $m\equiv p^{-1} \pmod N$, we have $T_p^*=\langle p\rangle^{-1}T_p$ as desired. □

Corollary 2.25. *By the spectral theorem, the space $\mathcal{S}_k(\Gamma_1(N))$ has an orthogonal basis of simultaneous eigenvectors, called eigenfunctions (or eigenforms), of the Hecke operators $\{\langle n\rangle, T_n : \gcd(n,N)=1\}$.*

Recall that $\omega_N=\left(\begin{smallmatrix}0&-1\\N&0\end{smallmatrix}\right)$. The next result will have several consequences in Section 3.2, where we discuss simultaneous eigenfunctions of the Hecke operators.

Theorem 2.26. *The following diagram is commutative:*

$$\begin{array}{ccc}
\mathcal{M}_k(N,\chi) & \xrightarrow{\;T_n\;} & \mathcal{M}_k(N,\chi) \\
\big\downarrow{\scriptstyle |_k[\omega_N]} & & \big\downarrow{\scriptstyle |_k[\omega_N]} \\
\mathcal{M}_k(N,\overline{\chi}) & \xrightarrow{\;T_n^*\;} & \mathcal{M}_k(N,\overline{\chi}).
\end{array}$$

Proof. It suffices to show the result for $\langle p\rangle$ and T_p in place of T_n.

Let $f\in\mathcal{M}_k(N,\overline{\chi})$. Then $\langle p\rangle^* f=\langle p\rangle^{-1}f=\chi(p)f$, and for any $\gamma\in\Gamma_0(N)$ with $\gamma\equiv\left(\begin{smallmatrix}*&*\\0&p\end{smallmatrix}\right) \pmod N$, we have $\omega_N^{-1}\gamma\omega_N\equiv\left(\begin{smallmatrix}*&*\\0&p^{-1}\end{smallmatrix}\right) \pmod N$, where p^{-1} is the inverse of p modulo N. Therefore $f|_k[\omega_N^{-1}\gamma\omega_N]=\chi(p)f$ as desired.

Let $\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)=\bigsqcup_v \Gamma_1(N)\alpha_v$. A computation reveals that $\omega_N^{-1}\Gamma_1(N)\omega_N=\Gamma_1(N)$, from which we obtain

$$\Gamma_1(N)\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)\Gamma_1(N)=\omega_N^{-1}\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)\omega_N=\bigsqcup_v \Gamma_1(N)(\omega_N^{-1}\alpha_v\omega_N).$$

Thus

$$\begin{aligned}
((f|_k[\omega_N^{-1}])|_k[\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)])|_k[\omega_N] &= p^{k/2-1}\sum_v f|_k[\omega_N^{-1}\alpha_v\omega_N] \\
&= f|_k[\Gamma_1(N)\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)\Gamma_1(N)].
\end{aligned}$$

The result follows from the fact that T_p^* is given by $|_k[\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)]^*=|_k[\Gamma_1(N)\left(\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right)\Gamma_1(N)]$. □

We include the following result without proof.

Theorem 2.27. *Let M be a multiple of N, and n a positive integer coprime to M. Then the following diagram is commutative:*

$$\begin{array}{ccc}
\mathcal{M}_k(N,\chi) & \xrightarrow{\;T_n\ (\textit{resp. } T_n^*)\;} & \mathcal{M}_k(N,\chi) \\
\big\downarrow & & \big\downarrow \\
\mathcal{M}_k(M,\chi) & \xrightarrow{\;T_n\ (\textit{resp. } T_n^*)\;} & \mathcal{M}_k(M,\chi)
\end{array}$$

Here the vertical arrows indicate the natural embeddings. The Hecke operators are taken at the appropriate levels.

See [Miy05, Theorem 4.5.10] for details.

Similarly to $\mathcal{R}(N)$, we collect the adjoints of the Hecke operators and form the following algebra:

Definition 2.28. Denote by $\mathcal{R}^*(N)$ the polynomial ring

$$\mathcal{R}^*(N)=\mathbb{Z}[T_p^*, \langle q\rangle^* : p,q\in\mathbb{P}, q\nmid N].$$

The ring $\mathcal{R}^*(N)$ is the ring of all adjoints of Hecke operators in the Hecke algebra $\mathcal{R}(N)$. †

We would like to eliminate the requirement that $\gcd(n, N) = 1$ and find a space of cusp forms for which all of the Hecke operators are simultaneously diagonalizable.

3 Oldforms, newforms, and strong multiplicity one

We consider an elementary way of moving between spaces of modular forms at different levels, specifically to take forms of lower levels M dividing N to forms of level N. Restricting our view to cusp forms, we define the so-called spaces of oldforms and newforms, which distinguish between the cusp forms that may be obtained by lifting cusp forms of lower levels up to level N, and those which are not obtained in this way. We show that the space of newforms has a basis consisting of normalized simultaneous eigenfunctions of all of the Hecke operators, and conclude with the strong multiplicity one property. The strong multiplicity one property shows that a normalized cusp form that is a common eigenfunction of all of the Hecke operators is completely determined by almost all of its eigenvalues.

3.1 Oldforms and newforms for χ-eigenspaces

For the remainder of this work, we restrict our view to various χ-eigenspaces of $\mathcal{M}_k(\Gamma_1(N))$ and $\mathcal{S}_k(\Gamma_1(N))$. Specifically, we fix N and consider χ-eigenspaces at different levels M, where M divides N.

Definition 3.1. In what follows, denote by α_ℓ the matrix

$$\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$$

for a positive integer ℓ. The action of matrices of this form on modular forms, which is essentially to scale the argument by ℓ, appears many times in what follows. †

Lemma 3.2. *For $f \in \mathcal{M}_k(N, \chi)$, the function $f \circ \alpha_\ell$ is an element of $\mathcal{M}_k(\ell N, \chi)$ with*

$$(f \circ \alpha_\ell)(z) = f(\ell z) = \ell^{-k/2}(f|_k[\alpha_\ell])(z).$$

If f is a cusp form, then so is $f \circ \alpha_\ell$.

Proof. Indeed, for any $\gamma = \left(\begin{smallmatrix} a & b \\ c\ell N & d \end{smallmatrix}\right) \in \Gamma_0(\ell N)$,

$$(f|_k[\alpha_\ell])|_k[\gamma] = (f|_k[\alpha_\ell \gamma \alpha_\ell^{-1}])|_k[\alpha_\ell] = (f|_k[\left(\begin{smallmatrix} a & b\ell \\ cN & d \end{smallmatrix}\right)])|_k[\alpha_\ell] = \chi(d) f|_k[\alpha_\ell] = \chi(\gamma) f|_k[\alpha_\ell],$$

which implies that $f|_k[\alpha_\ell] \in \mathcal{M}_k(\ell N, \chi)$. The last statement is clear. □

In this setting, the map α_ℓ provides a way to move between χ-eigenspaces at different levels.

We saw at the end of the previous section that the Hecke operators T_n, for n coprime to N, are simultaneously diagonalizable on $\mathcal{S}_k(\Gamma_1(N))$ and hence also on $\mathcal{S}_k(N, \chi)$. Unfortunately, $\mathcal{S}_k(N, \chi)$ does not necessarily have a basis of eigenfunctions of *all* Hecke operators T_n. However, $\mathcal{S}_k(N, \chi)$ does have such a basis when χ is a primitive character of conductor N. We might expect that if we exclude cusp forms of lower levels in $\mathcal{S}_k(N, \chi)$ (that is, the cusp forms appearing as the image of some suitable α_ℓ in the manner described above), we may be able to simultaneously diagonalize all of the Hecke operators T_n. This is indeed the case, as we will see.

Lemma 3.3. *The Hecke operators $T_n, \langle n \rangle$ commute with the action of α_ℓ whenever n is coprime to ℓN; that is, the diagram*

$$\begin{array}{ccc} \mathcal{M}_k(N, \chi) & \xrightarrow{T_n \ (resp.\ \langle n \rangle)} & \mathcal{M}_k(N, \chi) \\ \big\downarrow{\scriptstyle |_k[\alpha_\ell]} & & \big\downarrow{\scriptstyle |_k[\alpha_\ell]} \\ \mathcal{M}_k(\ell N, \chi) & \xrightarrow[T_n \ (resp.\ \langle n \rangle)]{} & \mathcal{M}_k(\ell N, \chi) \end{array}$$

commutes.

Proof. Let f be an element of $\mathcal{M}_k(N,\chi)$. Since $\gcd(n,\ell N)=1$, we have $(\langle n\rangle f)|_k[\alpha_\ell]=\chi(n)f|_k[\alpha_\ell]=\langle n\rangle(f|_k[\alpha_\ell])$.

Therefore it suffices to show that T_p commutes with the action of α_ℓ for primes p not dividing ℓN. From Proposition 2.9,

$$\begin{aligned}T_p(f|_k[\alpha_\ell]) &= p^{k/2-1}\sum_{j=0}^{p-1} f|_k[\alpha_\ell\left(\begin{smallmatrix}1 & j\\ 0 & p\end{smallmatrix}\right)] + p^{k/2-1}\chi(p)f|_k[\alpha_\ell\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right)]\\ &= p^{k/2-1}\sum_{j=0}^{p-1} f|_k[\left(\begin{smallmatrix}1 & \ell j\\ 0 & p\end{smallmatrix}\right)\alpha_\ell] + p^{k/2-1}\chi(p)f|_k[\left(\begin{smallmatrix}p & 0\\ 0 & 1\end{smallmatrix}\right)\alpha_\ell]\\ &= (T_pf)|_k[\alpha_\ell],\end{aligned}$$

where in the last equality we used the fact that ℓ and p are coprime to see that

$$\left\{\begin{pmatrix}1 & \ell j\\ 0 & p\end{pmatrix}, \begin{pmatrix}m & n\\ N & p\end{pmatrix}\begin{pmatrix}p & 0\\ 0 & 1\end{pmatrix} : 0\le j<p, mp-nN=1\right\}$$

form a set of coset representatives for $\Gamma_1(N)\backslash\Gamma_1(N)\left(\begin{smallmatrix}1 & 0\\ 0 & p\end{smallmatrix}\right)\Gamma_1(N)$. The result follows. □

We state the next lemma without proof.

Lemma 3.4. *Let f be an element of $\mathcal{M}_k(N,\chi)$. If there exists an element $\alpha=\left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right)\in \mathrm{M}_2(\mathbb{Z})$ such that $c\equiv 0 \pmod N$, $\gcd(a,N)=1$, and $\det\alpha>0$ that satisfies the following conditions, then $f=0$.*

(1) $\det\alpha>1$, $\gcd(\det\alpha,N)=1$, *and* $\gcd(a,b,c,d)=1$, *and*

(2) $f|_k[\alpha]\in\mathcal{M}_k(N,\chi)$.

This is a technical result that will be used in a few results to come. See [Miy05, Lemma 4.6.3] for details.

The next result provides a way to determine if a cusp form may be obtained as a cusp form at a lower level.

Theorem 3.5. *Let ℓ be a positive integer, and let f be a holomorphic function on $\mathcal{H}$ such that $f(z+1)=f(z)$ and $f\circ\alpha_\ell\in\mathcal{M}_k(N,\chi)$. Denote by m_χ the conductor of χ. Then*

(1) *if $\ell m_\chi \mid N$, then $f\in\mathcal{M}_k(N/\ell,\chi)$, and*

(2) *if $\ell m_\chi \nmid N$, then $f=0$.*

Here m_χ is the conductor of χ. If $f\circ\alpha_\ell$ is a cusp form, then so is f.

Proof. We may assume that ℓ is a prime number. We first show that $f\in\mathcal{M}_k(N,\chi)$. Let

$$\Gamma' = \left\{\begin{pmatrix}a & b\\ cN & d\end{pmatrix}\in\Gamma_0(N) : b\equiv 0 \pmod{\ell}\right\},$$

and let $\gamma=\left(\begin{smallmatrix}a & b\ell\\ cN & d\end{smallmatrix}\right)$ be an element of Γ'. Since $\alpha_\ell^{-1}\gamma\alpha_\ell=\left(\begin{smallmatrix}a & b\\ c\ell N & d\end{smallmatrix}\right)\in\Gamma_0(N)$, we have

$$f|_k[\gamma\alpha_\ell]=f|_k[\alpha_\ell\alpha_\ell^{-1}\gamma\alpha_\ell]=(f|_k[\alpha_\ell])|_k[\alpha_\ell^{-1}\gamma\alpha_\ell]=\chi(d)f|_k[\alpha_\ell],$$

from which it follows that $f|_k[\gamma]=\chi(d)f$. Let Γ'' be the group generated by Γ' and the matrix $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. Since $[\Gamma'':\Gamma']\ge\ell$ and

$$[\Gamma_0(N):\Gamma'] = \begin{cases}\ell & \ell\mid N,\\ \ell+1 & \ell\nmid N,\end{cases}$$

we have that $\Gamma'' = \Gamma_0(N)$ or $\Gamma_0(N)$ is generated by $\left(\begin{smallmatrix}1&1\\0&1\end{smallmatrix}\right)$ and Γ'. Since $f(z+1) = f(z)$, we have that $f \in \mathcal{M}_k(N,\chi)$.

Suppose that ℓ is coprime to N. By taking $\alpha = \alpha_\ell$ in Lemma 3.4, it follows that $f = 0$. So assume that $\ell \mid N$. For any element $\gamma_1 = \left(\begin{smallmatrix}a&b\\cN&d\end{smallmatrix}\right) \in \Gamma_0(N)$, we have

$$f|_k[\left(\begin{smallmatrix}a&b\ell\\cN/\ell&d\end{smallmatrix}\right)] = f|_k[\alpha_\ell\gamma_1\alpha_\ell^{-1}] = \chi(d)f,$$

and in particular we have $f|_k[\left(\begin{smallmatrix}1&0\\N/\ell&1\end{smallmatrix}\right)] = f$. Therefore, with $\gamma = \left(\begin{smallmatrix}1&m\\0&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&0\\N/\ell&1\end{smallmatrix}\right)\left(\begin{smallmatrix}1&n\\0&1\end{smallmatrix}\right)$ for any integers n, m, we have $f|_k[\gamma] = f$. Now choose n to be any integer such that $nN/\ell + 1 \not\equiv 0 \pmod{\ell}$, from which we may choose m to be an integer such that $n(1+mN/\ell)+m = n+m(nN/\ell+1) \equiv 0 \pmod{\ell}$. Then

$$\alpha_\ell^{-1}\gamma\alpha_\ell = \begin{pmatrix}1+mN/\ell & [n(1+mN/\ell)+1]/\ell\\ N & nN/\ell+1\end{pmatrix} \in \Gamma_0(N),$$

and so $f|_k[\gamma] = \chi(1+nN/\ell)f$.

Therefore, if $f \neq 0$, then $\chi(1+nN/\ell) = 1$ for any integer n satisfying $\gcd(nN/\ell+1, \ell) = 1$. This implies that χ is defined modulo N/ℓ, and that N is divisible by ℓm_χ. This proves (2) in the statement. Now assume that $\ell m_\chi \mid N$. Since $\Gamma_0(N/\ell)$ is generated by $\left(\begin{smallmatrix}1&0\\N/\ell&1\end{smallmatrix}\right)$ and $\Gamma_0(N)$, we have that $f \in \mathcal{M}_k(N/\ell,\chi)$ as needed. Lastly, it is clear that if $f \circ \alpha_\ell$ is a cusp form, then so is f. □

Lemma 3.6. *Let $f \in \mathcal{M}_k(N,\chi)$ have Fourier series expansion $f(z) = \sum_{n=0}^\infty a_n e^{2\pi i n z}$. For a positive integer L, let g be given by*

$$g(z) = \sum_{\substack{n\geq 0\\ \gcd(n,L)=1}} a_n e^{2\pi i n z}.$$

Then $g \in \mathcal{M}_k(M,\chi)$, with

$$M = N\prod_{\substack{p\mid L\\ p\mid N}} p \prod_{\substack{p\mid L\\ p\nmid N}} p^2,$$

where the products are to be taken over primes p. If f is a cusp form, then so is g.

Proof. It suffices to show the result when L is a prime number p. Let $N' = N$ if $p \mid N$ and $N' = pN$ otherwise. Since $p \mid N'$, we have by Proposition 2.9 that

$$(T_pf)(z) = \frac{1}{p}\sum_{n=0}^\infty a_n \sum_{m=0}^{p-1} e^{2\pi i n(z+m)/p} = \sum_{n=0}^\infty a_{np}e^{2\pi i n z},$$

where T_p is acting at level N'. Hence $(T_pf)(pz) = \sum_{n=0}^\infty a_{np}e^{2\pi i n p z}$, which belongs to $\mathcal{M}_k(N'p,\chi)$ by Lemma 3.2. Then the function g, given by

$$g(z) = f(z) - (T_pf)(pz),$$

is an element of $\mathcal{M}_k(N'p,\chi)$. The last assertion is clear. □

Lemma 3.7. *Let χ be a Dirichlet character modulo N, ℓ a positive integer, and p a prime number that does not divide ℓ. Let $M = \ell N$. Then the following diagrams commute.*

$$\begin{array}{ccc}
\mathcal{M}_k(pN,\chi) & \xrightarrow{\Gamma_1(pN)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)} & \mathcal{M}_k(N,\chi)\\
\downarrow & & \downarrow\\
\mathcal{M}_k(pM,\chi) & \xrightarrow{\Gamma_1(pM)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(M)} & \mathcal{M}_k(M,\chi)
\end{array} \tag{3.1}$$

(In the above diagram, the vertical arrows indicate the natural embeddings.)

$$\begin{array}{ccc} \mathcal{M}_k(pN,\chi) & \xrightarrow{\Gamma_1(pN)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)} & \mathcal{M}_k(N,\chi) \\ \downarrow{\scriptstyle\alpha_\ell} & & \downarrow{\scriptstyle\alpha_\ell} \\ \mathcal{M}_k(pM,\chi) & \xrightarrow{\Gamma_1(pM)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(M)} & \mathcal{M}_k(M,\chi) \end{array} \tag{3.2}$$

Similar results hold for cusp forms.

Proof. By assumption, $p \mid N$ if and only if $p \mid M$. Therefore, by Lemma 2.10, the commutativity of diagram 3.1 is clear.

Now let f be an element of $\mathcal{M}_k(pN,\chi)$, and let $g = f|_k[\alpha_\ell]$. Let

$$d = \begin{cases} p-1 & \text{if } p \mid M \\ p & \text{otherwise,} \end{cases}$$

and $\gamma_v = \left(\begin{smallmatrix}1&v\\0&1\end{smallmatrix}\right)$ for $0 \le v < p$. If $d = p$, choose γ_p as in Lemma 2.10. Then we have

$$\Gamma_1(pM)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(M) = \bigsqcup_{v=0}^{d} \Gamma_1(pM)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\gamma_v$$

and

$$\begin{aligned} p^{1-k/2} g|_k[\Gamma_1(pM)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(M)] &= \sum_{v=0}^{d} g|_k[\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\gamma_v] \\ &= \sum_{v=0}^{d} f|_k[\alpha_\ell\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\gamma_v] \\ &= \sum_{v=0}^{d} f|_k[\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)(\alpha_\ell\gamma_v\alpha_\ell^{-1})\alpha_\ell]. \end{aligned}$$

Observe that $\alpha_\ell\gamma_v\alpha_\ell^{-1} = \left(\begin{smallmatrix}1&\ell v\\0&1\end{smallmatrix}\right)$ for $0 \le v < p$, and that for $p \nmid N$, we have

$$\alpha_\ell\gamma_p\alpha_\ell^{-1} \equiv \begin{cases} \left(\begin{smallmatrix}0&-a\ell\\(a\ell)^{-1}&0\end{smallmatrix}\right) \pmod{p}, \\ \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right) \pmod{N}. \end{cases}$$

It follows from Lemma 2.10 that

$$\Gamma_1(pN)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N) = \bigsqcup_{v=0}^{d} \Gamma_1(pN)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)(\alpha_\ell\gamma_v\alpha_\ell^{-1}).$$

Thus

$$g|_k[\Gamma_1(pM)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)] = (f|_k[\Gamma_1(pN)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N)])|_k[\alpha_\ell].$$

□

Lemma 3.8. *Let ℓ be a positive square-free integer, and let $f \in \mathcal{M}_k(N,\chi)$ have Fourier series expansion $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$. If $a_n = 0$ for all n coprime to ℓ, then*

$$f(z) = \sum_{p \mid \ell} g_p(pz) \quad \text{where } g_p \in \mathcal{M}_k(N\ell^2,\chi),$$

and p runs over all prime factors of ℓ. Furthermore, if $\ell \mid N$, then we may choose g_p from $\mathcal{M}_k(N\ell,\chi)$. If f is a cusp form, then each g_p can be chosen to be cusp forms as well.

Proof. The proof is by induction on the number of prime factors of ℓ. Suppose first that ℓ is prime. Then g given by $g(z) = f(z/\ell)$ satisfies the conditions of Theorem 3.5, so that $g \in \mathcal{M}_k(N/\ell, \chi)$ or $f = g = 0$, depending on whether ℓm_χ divides N or not. Thus $g \in \mathcal{M}_k(N\ell, \chi)$ with $f(z) = g(\ell z)$. Now let ℓ be a composite number, and assume the result holds for any proper divisor of ℓ. Let p be a prime factor of ℓ and let $\ell' = \ell/p$. Let h be given by

$$h(z) = \sum_{\substack{n \geq 0 \\ \gcd(n,p)=1}} a_n e^{2\pi i n z}.$$

Then $h \in \mathcal{M}_k(Np^2, \chi)$ by Lemma 3.6. Let b_n for $n \geq 0$ be the Fourier coefficients of $f - h$; that is, $f(z) - h(z) = \sum_{n=0}^{\infty} b_n e^{2\pi i n z}$. Then if $\gcd(n,p) = 1$, $b_n = 0$. Define g_p by

$$g_p(z) = f(z/p) - h(z/p),$$

and observe that $g_p \in \mathcal{M}_k(Np, \chi)$ by the inductive hypothesis. Furthermore, note that h satisfies the assumption of the lemma with Np^2 and ℓ' in place of N and ℓ, respectively. Therefore we may find $g_q \in \mathcal{M}_k(Np^2(\ell')^2, \chi) = \mathcal{M}_k(N\ell^2, \chi)$ for each prime factor q of ℓ' satisfying $h(z) = \sum_{q|\ell'} g_q(qz)$. Combining this with the observation that $f(z) = g_p(pz) + h(z)$ yields the first half of the lemma. From Lemma 3.6 it is clear that we may take g_p from $\mathcal{M}_k(N\ell, \chi)$ if $\ell \mid N$. Lastly, it is clear that the g_p may be chosen to be cusp forms if f is a cusp form. □

The following theorem generalizes Theorem 3.5.

Theorem 3.9. *Let ℓ be a positive integer, and let $f \in \mathcal{M}_k(N, \chi)$ have Fourier series expansion $f(z) = \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$. Let m_χ be the conductor of χ, and assume that $a_n = 0$ for all n coprime to ℓ.*

(1) *If $\gcd(\ell, N/m_\chi) = 1$, then $f = 0$.*

(2) *If $\gcd(\ell, N/m_\chi) \neq 1$, then there exist $f_p \in \mathcal{M}_k(N/p, \chi)$ for all prime factors p of $\gcd(\ell, N/m_\chi)$ such that*

$$f(z) = \sum_{p|\gcd(\ell, N/m_\chi)} f_p(pz).$$

If f is a cusp form, then we may choose the f_p to be cusp forms as well.

Proof. We may assume that ℓ is square-free, and we prove the result by induction on the number of factors of ℓ. When ℓ is a prime number, the result is obtained from Theorem 3.5 for $f(z/\ell)$. Now assume that ℓ is composite and that the lemma holds for any proper divisor of ℓ. Let p be a prime factor of ℓ, and let $\ell' = \ell/p$.

Let h and g be given by

$$h(z) = \sum_{\substack{n \geq 0 \\ \gcd(n,\ell') \neq 1}} a_n e^{2\pi i n z} \quad \text{and} \quad g(z) = f(z) - h(z) = \sum_{\substack{n \geq 0 \\ \gcd(n,\ell')=1}} a_n e^{2\pi i n z}.$$

Observe that h and g are elements of $\mathcal{M}_k(N(\ell')^2, \chi)$ by Theorem 3.5. Let $d = p - 1$ if $p^2 \mid N$, or let $d = p$ if $p^2 \nmid N$. Then choose elements $\gamma_v \in \Gamma_1(N(\ell')^2/p)$ for $0 \leq v < d$ (via Lemma 2.10) so that

$$\Gamma_1(N(\ell')^2)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_0(N(\ell')^2/p) = \bigsqcup_{v=0}^{d} \Gamma_1(N(\ell')^2)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\gamma_v.$$

Then

$$\begin{aligned} g|_k[\Gamma_1(N(\ell')^2)\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\Gamma_1(N(\ell')^2/p)] &= p^{k/2-1} \sum_{v=0}^{d} \overline{\chi(\gamma_v)} g|_k[\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)\gamma_v] \\ &= p^{-1} \sum_{v=0}^{d} \overline{\chi(\gamma_v)} g_p|_k[\gamma_v] \\ &= (d+1)p^{-1} g_p. \end{aligned}$$

Hence

$$g(z) = g_p(pz) = p(d+1)^{-1}\big(g|_k[\Gamma_1(N(\ell')^2)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N(\ell')^2/p)]\big)(pz).$$

Let

$$f_p(z) = p(d+1)^{-1}\big(f|_k[\Gamma_1(N)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N/p)]\big)(z).$$

Then $f_p \in \mathcal{M}_k(N/p,\chi)$, and by Lemma 3.7(1),

$$f_p(z) = p(d+1)^{-1}\big(f|_k[\Gamma_1(N(\ell')^2)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N(\ell')^2/p)]\big)(z). \tag{3.3}$$

We show that $f(z) - f_p(pz)$ satisfies the assumption of the theorem for ℓ'. It is clear that $f(z) - f_p(pz)$ defines an element of $\mathcal{M}_k(N,\chi)$. We have

$$\begin{aligned} f(z) - f_p(pz) &= f(z) - f_p(pz) - g(z) + g_p(pz) \\ &= (f(z) - g(z)) - p(d+1)^{-1}\big((f-g)|_k[\Gamma_1(N(\ell')^2)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N(\ell')^2/p)]\big)(pz) \\ &= h(z) - p(d+1)^{-1}\big(h|_k[\Gamma_1(N(\ell')^2)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N(\ell')^2/p)]\big)(pz). \end{aligned} \tag{3.4}$$

Since the n-th Fourier coefficient of h vanishes if n is coprime to ℓ', we may write

$$h(z) = \sum_{q|\ell'} h_q(qz) \quad \text{with } h_q \in \mathcal{M}_k(N(\ell')^3 m,\chi)$$

by Lemma 3.8. Moreover, for any prime factor q of ℓ',

$$h|_k[\Gamma_1(N(\ell')^2)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N(\ell')^2/p)] = h|_k[\Gamma_1(N(\ell')^3 q)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N(\ell')^3 q/p)]$$

by Lemma 3.7(1). Combined with Lemma 3.7(2), we have that

$$\begin{aligned} \big(h|_k[\Gamma_1(N(\ell')^2)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N(\ell')^2/p)]\big)(z) &= \Bigg(\Bigg(\sum_{q|\ell'} q^{-k/2} h_q|_k[\alpha_q]\Bigg)\Bigg|_k[\Gamma_1(N(\ell')^3)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N(\ell')^3 q/p)]\Bigg)(z) \\ &= \sum_{q|\ell'} \big(h_q|_k[\Gamma_1(N(\ell')^3)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N(\ell')^3/p)]\big)(qz). \end{aligned}$$

In particular, the n-th Fourier coefficient of $\big(h|_k[\Gamma_1(N(\ell')^2)\left(\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right)\Gamma_1(N(\ell')^2/p)]\big)(z)$ vanishes whenever $\gcd(n,\ell') = 1$. As a result, the n-th Fourier coefficient of $f(z) - f_p(pz)$ vanishes by (3.4). Therefore, by the inductive hypothesis, we have

$$f(z) - f_p(pz) = \sum_q f_q(qz), \quad \text{for } f_q \in \mathcal{M}_k(N/q,\chi),$$

where q runs over all prime factors of ℓ'. This proves part (2) of the theorem. If f is a cusp form, then it is clear that each of the modular forms appearing in the proof may be chosen to be cusp forms also. □

In what follows, we only consider cusp forms.

Definition 3.10. Denote by $\mathcal{S}_k^1(N,\chi)$ the subspace of ***oldforms at level*** N of $\mathcal{S}_k(N,\chi)$, which is generated by the set

$$\bigcup_M \bigcup_\ell \{f \circ \alpha_\ell : f \in \mathcal{S}_k(M,\chi)\}.$$

Here M runs over all positive integers such that $m_\chi \mid M$, $M \mid N$, and $M \neq N$; here ℓ runs over all positive divisors of N/M, including 1 and N/M. (As usual, m_χ denotes the conductor of χ.)

In other words, $\mathcal{S}_k^1(N,\chi)$ is the subspace of $\mathcal{S}_k(N,\chi)$ generated by cusp forms coming from lower levels.

Denote by $\mathcal{S}_k^0(N,\chi)$ the subspace of ***newforms at level*** N, given by the orthogonal complement of $\mathcal{S}_k^1(N,\chi)$ in $\mathcal{S}_k(N,\chi)$ with respect to the Petersson inner product. †

In other sources, the ^{1} and ^{0} denoting the spaces of oldforms and newforms is replaced by $^{\text{old}}$ and $^{\text{new}}$, respectively.

By the above definition, we immediately obtain the following lemma:

Lemma 3.11. (1) *If χ is a primitive Dirichlet character of conductor N, then $\mathcal{S}_k(N,\chi) = \mathcal{S}_k^0(N,\chi)$.*

(2) *Let χ be a character of conductor m_χ. If $m_\chi \mid M$, $M \mid N$, and $M \neq N$, then $\mathcal{S}_k(M,\chi) \subset \mathcal{S}_k^1(N,\chi)$.*

(3) *The space $\mathcal{S}_k(N,\chi)$ is generated by the set*

$$\bigcup_M \bigcup_\ell \left\{ f \circ \alpha_\ell : f \in \mathcal{S}_k^0(N,\chi) \right\}.$$

Here M runs over all positive integers such that $m_\chi \mid M$ and $M \mid N$; here ℓ runs over all positive divisors of N/M, including 1 and N/M.

Lemma 3.12. *The subspaces $\mathcal{S}_k^1(N,\chi)$ and $\mathcal{S}_k^0(N,\chi)$ are stable under the action of the Hecke operators T_n for n coprime to N.*

Proof. Let $f \in \mathcal{S}_k^1(N,\chi)$. By definition, we may write f as

$$f(z) = \sum_v f_v(\ell_v z) \quad \text{for } f_v \in \mathcal{S}_k(M_v,\chi), \quad \text{with } \ell_v M_v \mid N,\ M_v \neq N.$$

Let g_v be given by $g_v(z) = f_v(\ell_v z)$. Since $\gcd(n, \ell_v N) = 1$, we have

$$(T_n f)(z) = \sum_v (T_n g_v)(z) = \sum_v (T_n f_v)(\ell_v z)$$

by Theorem 2.27 and Lemma 3.3. Hence $T_n f \in \mathcal{S}_k^1(N,\chi)$; that is, $\mathcal{S}_k^1(N,\chi)$ is stable under T_n. Since the adjoint of T_n on $\mathcal{S}_k(N,\chi)$ is $\langle n \rangle T_n$ (see Theorem 2.24), it follows that $\mathcal{S}_k^0(N,\chi)$ is also stable under T_n. □

It follows from the above lemma that the subspaces $\mathcal{S}_k^0(N,\chi)$ and $\mathcal{S}_k^1(N,\chi)$ of $\mathcal{S}_k(N,\chi)$ have a basis of simultaneous eigenfunctions of all of the Hecke operators T_n, for n coprime to N.

3.2 Primitive forms

In this section we briefly focus on simultaneous eigenfunctions of the Hecke operators in the space of newforms.

Lemma 3.13. *Let $f \in \mathcal{S}_k^0(N,\chi)$ have series expansion $\sum_{n=1}^\infty a_n e^{2\pi i n z}$. If f is a common eigenfunction of the Hecke operators T_n for all n coprime to some integer L, then $a_1 \neq 0$.*

Proof. Assume by way of contradiction that $a_1 = 0$. By Lemma 2.19(1), we have that $a_n = 0$ for all n coprime to L. Hence $f \in \mathcal{S}_k^1(N,\chi)$ by Theorem 3.9, which is a contradiction. □

Theorem 3.14. *Let $f(z) \in \mathcal{S}_k^0(N,\chi)$ and $g(z) \in \mathcal{S}_k(N,\chi)$. If $f(z)$ and $g(z)$ are common eigenfunctions of T_n with the same eigenvalue for each n coprime to some integer L, then $g(z)$ is a constant multiple of $f(z)$.*

Proof. Let f have Fourier expansion $\sum_{n=1}^\infty a_n e^{2\pi i n z}$. Since $a_1 \neq 0$ by Lemma 3.13, normalize f so that $a_1 = 1$. Furthermore assume that $N \mid L$. Decompose g into $g^0 + g^1$, the sum of its newform and oldform components. By Lemma 3.12, both g^0 and g^1 are common eigenfunctions of the operators T_n with the same eigenvalue a_n for each n coprime to L.

Assume that $g^0 \neq 0$, and write $g^0(z) = \sum_{n=1}^\infty b_n e^{2\pi i n z}$. By Lemma 3.13, $b_1 \neq 0$. We show that $g^0 = b_1 f$. Let $\sum_{n=1}^\infty c_n e^{2\pi i n z}$ be the Fourier series expansion for $g^0 - b_1 f$. Since $b_1 a_n = b_n$ for all n coprime to L by

Lemma 2.19(1), we have that $c_n = 0$ for all n coprime to L. Then Theorem 3.9 implies that $g^0 - b_1 f \in \mathcal{S}_k^1(N,\chi)$, and that $g^0 = b_1 f$.

Next we show that $g^1(z) = 0$. First suppose that $N = m_\chi$, the conductor of χ. Then $\mathcal{S}_k^1(N,\chi) = 0$, so that $g^1 = 0$. If $N \neq m_\chi$.

If $g^1 \neq 0$, then there exists a proper divisor M of N satisfying $m_\chi \mid M$, and a nonzero element h of $\mathcal{S}_k^0(M,\chi)$ such that $T_n h = a_n h$ for all n coprime to L. Then by definition we may write

$$g^1(z) = \sum_v h_v(\ell_v z), \quad h_v \in \mathcal{S}_k^0(M_v,\chi), \ell_v M_v \mid N, M_v \neq N.$$

Since M_v divides N, Lemma 3.12 implies that $\mathcal{S}_k^0(M_v,\chi)$ has a basis consisting of eigenfunctions of the operators T_n for all n coprime to L. Therefore we may assume that all h_v are common eigenfunctions of T_n for all n coprime to L. Since eigenfunctions with distinct eigenvalues are linearly independent, the summation of all $h_v(\ell_v z)$ whose eigenvalues for T_n are different from a_n must vanish. So by removing those functions from the sum, we may assume that the h_v appearing in the sum $g^1(z) = \sum_v h_v(\ell_v z)$ satisfy $T_n h_v = a_n h_v$ for all n coprime to L. Therefore we may take any h_v as h and any M_v as M.

Let $h(z) = \sum_{n=1}^\infty c'_n e^{2\pi i n z}$ be the Fourier series of the element h from before. Since $T_n h = a_n h$ for all n coprime to L, we have that $c'_1 \neq 0$ by Lemma 3.13. Let $\sum_{n=1}^\infty d_n e^{2\pi i n z}$ be the Fourier series expansion for $h - c'_1 f$. By Lemma 2.19(1), $d_n = 0$ if n is coprime to L, and so by Theorem 3.9, $h - c'_1 f \in \mathcal{S}_k^1(N,\chi)$.

Hence $f(z) = -c'_1(h(z) - c'_1 f(z)) + c'_1 h(z)$, so that f is an element of $\mathcal{S}_k^1(N,\chi)$, which contradicts the assumption that f was an element of $\mathcal{S}_k^0(N,\chi)$. Therefore g^1 must be zero, so that $g = g^0 = b_1 f$. □

Definition 3.15. An element $f \in \mathcal{S}_k^0(N,\chi)$ is a ***primitive form*** of conductor N if the following conditions are satisfied:

(1) f is a common eigenfunction of all of the Hecke operators T_n for n coprime to N, and

(2) f is normalized; that is, f has Fourier series expansion $f(z) = \sum_{n=1}^\infty a_n e^{2\pi i n z}$ with $a_1 = 1$.

We also call $\mathcal{S}_k^0(N,\chi)$ the space of primitive forms of level N with character χ. †

In other sources, primitive forms are called newforms, which may be confusing.

Theorem 3.16. *Primitive forms are common eigenfunctions of all operators in $\mathcal{R}(N) \cup \mathcal{R}^*(N)$, and $\mathcal{S}_k^0(N,\chi)$ has a basis consisting of primitive forms.*

Proof. Let f be a primitive form in $\mathcal{S}_k^0(N,\chi)$, and let $T_n f = a_n f$ for all n coprime to N. Let T and T^* be elements of $\mathcal{R}(N)$ and $\mathcal{R}^*(N)$, respectively. Since T commutes with T_n, T^* commutes with T_n^*, and $T_n f = \chi(n) T_n^* f$, we have that T^* commutes with T_n. Therefore Tf and $T^* f$ are also common eigenfunctions of the operators T_n, with the same eigenvalue a_n.

Then Theorem 3.14 implies that both Tf and $T^* f$ are constant multiples of f, as desired.

Since $\mathcal{S}_k^0(N,\chi)$ and $\mathcal{S}_k(N,\chi)$ have bases consisting of common eigenfunctions of the operators T_n for n coprime to N, what we just proved along with Lemma 3.13 imply that $\mathcal{S}_k^0(N,\chi)$ has a basis of primitive forms. □

Let f be a primitive form of $\mathcal{S}_k^0(N,\chi)$ with Fourier series expansion $f(z) = \sum_{n=1}^\infty a_n e^{2\pi i n z}$. Then

$$T_n(f|_k[\omega_N]) = \overline{a_n} f|_k[\omega_N] \quad \text{and} \quad T_n^*(f|_k[\omega_N]) = a_n f|_k[\omega_N] \tag{3.5}$$

for all positive integers n.

We omit the proofs of the following three results.

Theorem 3.17. (1) *By the action of ω_N, we obtain the isomorphisms $\mathcal{S}_k^0(N,\chi) \cong \mathcal{S}_k^0(N,\overline{\chi})$ and $\mathcal{S}_k^1(N,\chi) \cong \mathcal{S}_k^1(N,\overline{\chi})$, and*

(2) *if $f(z)$ is a primitive form of $\mathcal{S}_k^0(N,\chi)$, then $f_p(z)$ is a primitive form of $\mathcal{S}_k^0(N,\overline{\chi})$ and*

$$f|_k[\omega_N] = cf_p(z)$$

for some $c \in \mathbb{C}$.

See [Miy05, Theorem 4.6.15] for details.

Let γ_q and γ_q' be two elements of $\mathrm{SL}_2(\mathbb{Z})$ such that

$$\gamma_q \equiv \begin{cases} \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \pmod{N_q^2} \\ \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{(N/N_q)^2} \end{cases} \qquad \text{and} \quad \gamma_q' \equiv \begin{cases} \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) \pmod{N_q^2} \\ \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \pmod{(N/N_q)^2}. \end{cases}$$

Then let $\eta_q = \gamma_q \left(\begin{smallmatrix} N_q & 0 \\ 0 & 1 \end{smallmatrix}\right)$ and $\eta_q' = \gamma_q' \left(\begin{smallmatrix} N/N_q & 0 \\ 0 & 1 \end{smallmatrix}\right)$.

Theorem 3.18. *We have*

(1) *By the action of η_q, we have the isomorphisms*

$$\mathcal{S}_k^0(N,\chi) \cong \mathcal{S}_k^0(N,\chi_q'\overline{\chi_q}), \quad \mathcal{S}_k^1(N,\chi) \cong \mathcal{S}_k^1(N,\chi_q'\overline{\chi_q}).$$

(2) *By the action of η_q', we have the isomorphisms*

$$\mathcal{S}_k^0(N,\chi) \cong \mathcal{S}_k^0(N,\overline{\chi_q'}\chi_q), \quad \mathcal{S}_k^1(N,\chi) \cong \mathcal{S}_k^1(N,\overline{\chi_q'}\chi_q).$$

(3) *For $f \in \mathcal{S}_k(N,\chi)$, we have $f|_k[\eta_q^2] = \chi_q(-1)\overline{\chi_q'}(N_q)f$, $f|_k[\eta_q'^2] = \chi_q'(-1)\overline{\chi_q}(N/N_q)f$, and $f|_k[\eta_q\eta_q'] = \overline{\chi_q'}(N_q)f|_k[\omega_N]$.*

(4) *Let $f \in \mathcal{S}_k^0(N,\chi)$ be a primitive form with $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$, and write*

$$(f|_k[\eta_q])(z) = c\sum_{n=1}^{\infty} b_n e^{2\pi i n z} \quad (\textit{with } b_1 = 1).$$

Let $g_q(z) = \sum_{n=1}^{\infty} b_n e^{2\pi i n z}$.
Then g_q is a primitive form of $\mathcal{S}_k^0(N,\chi_q'\overline{\chi_q})$, with

$$b_p = \begin{cases} \overline{\chi_q}(p)a_p & \textit{if } p \neq q, \\ \chi_q'(p)\overline{a_p} & \textit{if } p = q \end{cases}$$

for any prime p.

See [Miy05, Theorem 4.6.16] for details.

Theorem 3.19. *Let $f(z) = \sum_{n=1}^{\infty} a_n e^{2\pi i n z}$ be a primitive form of $\mathcal{S}_k^0(N,\chi)$, and m the conductor of χ. For a prime factor q of N, denote by N_q and m_q the q-components of N and m, respectively; that is, N_q and m_q are the largest powers of p dividing N and m, respectively.*

(1) *If $N_q = m_q$, then $|a_q| = q^{(k-1)/2}$.*

(2) *If $N_q = q$ and $m_q = 1$, then $a_q^2 = \chi_q'(q)q^{k-2}$.*

(3) *Otherwise, that is, if $q^2 \mid N_q$ and $N_q \neq m_q$, then $a_q = 0$.*

See [Miy05, Theorem 4.6.17] for details.

3.3 Strong multiplicity one

We finally prove the strong multiplicity one property for classical modular forms. Let $g \in \mathcal{S}_k(M,\lambda)$ be a cusp form at level M that is normalized; that is, g has first Fourier coefficient equal to 1, and is a common eigenfunction of all of the Hecke operators. If there exists a primitive form $f \in \mathcal{S}_k^0(N,\chi)$ at level N (which need not be the same as M) whose Fourier coefficients, that is to say its eigenvalues, agree with the Fourier coefficients of g at all indices n coprime to some integer L, we show that g is equal to the primitive form f at level N.

Theorem 3.20 (Strong multiplicity one). *Let f be a primitive form in $\mathcal{S}_k^0(N,\chi)$ and let g be an element of $\mathcal{S}_k(M,\lambda)$, with Fourier series expansions $f(z)=\sum_{n=1}^\infty a_n e^{2\pi i n z}$ and $g(z)=\sum_{n=1}^\infty b_n e^{2\pi i n z}$. If $b_1 = 1$, g is a common eigenfunction of $\mathcal{R}(M)\cup\mathcal{R}^*(M)$, and $a_n = b_n$ for all n coprime to some integer L, then $N = M$ and $f = g$.*

Proof. Without loss of generality we may take L to be a common multiple of N and M. If p is a prime number coprime to L, we have from $T_{p^2} = T_pT_p - p^{k-1}\langle p\rangle$ that

$$\begin{aligned}\chi(p)p^{k-1} &= a_p^2 - a_{p^2}\\ &= b_p^2 - b_{p^2}\\ &= \lambda(p)p^{k-1},\end{aligned}$$

so that $\chi(p)=\lambda(p)$. It follows that $\chi(n)=\lambda(n)$ for all n coprime to L.

We show that $M \mid N$. By Theorem 2.20, $L(s,f)$ and $L(s,g)$ have Euler product expansions, so that

$$\frac{\Lambda_N(s,f)}{\Lambda_M(s,g)} = \left(\frac{\sqrt{N}}{\sqrt{M}}\right)^s \prod_{p\mid L} \frac{1-b_pp^{-s}+\lambda(p)p^{k-1-2s}}{1-a_pp^{-s}+\chi(p)p^{k-1-2s}} \tag{3.6}$$

for $\mathrm{Re}(s) > k/2+1$. Since the ratio in the right-hand side is a meromorphic function on the whole s-plane, (3.6) holds for all s on the s-plane except at the poles.

On the other hand, we have

$$\frac{\Lambda_N(s,f)}{\Lambda_M(s,g)} = \frac{\Lambda_N(k-s,f|_k[\omega_N])}{\Lambda_M(k-s,g|_k[\omega_M])}$$

by Corollary 1.26. Furthermore, $T_n g = b_n g$, and since g is a common eigenfunction of T_n^* by assumption, we have that $T_n^* g = \overline{b_n} g$ and

$$T_n^*(g|_k[\omega_M]) = \overline{b_n}(g|_k[\omega_M])$$

by Theorem 2.26. Then by Theorem 2.20 it follows that $L(s,g|_k[\omega_M])$ also has an Euler product expansion. Combined with Theorem 3.17(2), we have

$$\frac{\Lambda_N(s,f)}{\Lambda_M(s,g)} = \frac{\Lambda_N(k-s,f|_k[\omega_N])}{\Lambda_M(k-s,g|_k[\omega_M])} = c\left(\frac{\sqrt{N}}{\sqrt{M}}\right)^{k-s} \prod_{p\mid L} \frac{1-\overline{b_p}p^{s-k}+\overline{\lambda}(p)p^{2s-k-1}}{1-\overline{a_p}p^{s-k}+\overline{\chi}(p)p^{2s-k-1}} \tag{3.7}$$

for some constant c. By combining (3.6) and (3.7) together, we obtain

$$\left(\frac{N}{M}\right)^s \prod_{p\mid L} \frac{1-b_pp^{-s}+\lambda(p)p^{k-1-2s}}{1-a_pp^{-s}+\chi(p)p^{k-1-2s}} = c\left(\frac{\sqrt{N}}{\sqrt{M}}\right)^{k} \prod_{p\mid L} \frac{1-\overline{b_p}p^{s-k}+\overline{\lambda}(p)p^{2s-k-1}}{1-\overline{a_p}p^{s-k}+\overline{\chi}(p)p^{2s-k-1}}.$$

Denote by M_p and N_p the p-components of M and N respectively; that is, M_p and N_p are the largest powers of p dividing M and N, respectively. Then for any prime factor p of L,

$$\left(\frac{N_p}{M_p}\right)^s \frac{1-b_pp^{-s}+\lambda(p)p^{k-1-2s}}{1-a_pp^{-s}+\chi(p)p^{k-1-2s}} = c_p \frac{1-\overline{b_p}p^{s-k}+\overline{\lambda}(p)p^{2s-k-1}}{1-\overline{a_p}p^{s-k}+\overline{\chi}(p)p^{2s-k-1}} \tag{3.8}$$

holds for some constant c_p by Lemma 1.20. Let $x = p^{-s}$, and let u and v be the degrees of

$$1 - a_p p^{-s} + \chi(p)p^{k-1-2s} = 1 - a_p x + \chi(p)p^{k-1}x^2 \text{ and}$$
$$1 - b_p p^{-s} + \lambda(p)p^{k-1-2s} = 1 - b_p x + \lambda(p)p^{k-1}x^2$$

as polynomials of x, respectively. Thus $0 \le u, v \le 2$. Furthermore, write $M_p/N_p = p^e$, so that (3.8) becomes

$$x^e \frac{1 - b_p x + \lambda(p)p^{k-1}x^2}{1 - a_p x + \chi(p)p^{k-1}x^2} = c_p \frac{1 - \overline{b_p} p^{-k} x^{-1} + \overline{\lambda}(p)p^{-k-1}x^{-2}}{1 - \overline{a_p} p^{-k} x^{-1} + \overline{\chi}(p)p^{-k-1}x^{-2}}. \tag{3.9}$$

We investigate each combination of values that u, v may take, and show that if a particular combination of u, v implies that $e > 0$, that case could not occur. Thus in the remaining cases, $e \le 0$ so that $M_p \mid N_p$.

(1) If $u = v$, take $x \to \infty$ in (3.10) (by taking $\mathrm{Re}(s) \to \infty$) to deduce that $e = 0$.

(2) If $u = 1$ and $v = 0$, then $a_p \neq 0$ so that (3.9) may be rewritten as

$$x^e(1 - \overline{a_p} p^{-k} x^{-1}) = c_p(1 - a_p x).$$

Then $e = 1$, and multiplying the above equality by a^p we may rearrange to obtain

$$-a_p c_p = \frac{a_p x - |a_p|^2 p^{-k}}{a_p x - 1},$$

from which it follows that $|a_p|^2 = p^k$. This is in contradiction with Theorem 3.19, so this case could not occur.

(3) If $u = 0$ and $v = 1$, then (3.9) becomes $x^e(1 - b_p x) = c_p(1 - \overline{b_p} p^{-k} x^{-1})$, from which it follows that $e = -1$.

(4) If $u = 2$ and $v = 0$, rewrite (3.9) as

$$x^e(1 - \overline{a_p} p^{-k} x^{-1} + \overline{\chi}(p)p^{-k-1}x^{-2}) = c_p(1 - a_p x + \chi(p)p^{k-1}x^2). \tag{3.10}$$

Then $e = 2$, so that we have

$$\chi(p)p^{k-1}c_p = \frac{\chi(p)p^{k-1}x^2 - \chi(p)\overline{a_p} p^{-1} x + |\chi(p)|^2 p^{-2}}{\chi(p)p^{k-1}x^2 - a_p x + 1}.$$

It follows that $\chi(p)p^{k-1}c_p = 1$ and $|\chi(p)|^2 = p^2$; the latter is impossible.

(5) If $u = 0$ and $v = 2$, deduce that $e = -2$.

(6) If $u = 2$ and $v = 1$, rewrite (3.9) as

$$x^e \frac{1 - \overline{a_p} p^{-k} x^{-1} + \overline{\chi}(p)p^{-k-1}x^{-2}}{1 - \overline{b_p} p^{-k} x^{-1}} = c_p \frac{1 - a_p x + \chi(p)p^{k-1}x^2}{1 - b_p x},$$

so that $e = 1$, and rewrite this equation as

$$\frac{x^2 - \overline{a_p} p^{-k} x + \overline{\chi}(p)p^{-k-1}}{x - \overline{b_p} p^{-k}} = c_p \frac{x^2 - \overline{\chi}(p) a_p p^{-k+1} x + \overline{\chi}(p)p^{-k+1}}{\overline{\chi}(p)p^{-k+1}(1 - b_p x)}.$$

The roots of the polynomials

$$x^2 - \overline{a_p} p^{-k} x + \overline{\chi}(p)p^{-k-1} \quad \text{and} \quad x^2 - \overline{\chi}(p) a_p p^{-k+1} x + \overline{\chi}(p)p^{-k+1}$$

agree. However, since the product of the roots of these polynomials are equal to the constant terms of each polynomial, we must have $\overline{\chi}(p)p^{-k-1} = \overline{\chi}(p)p^{-k+1}$, a contradiction.

(7) If $u = 1$ and $v = 2$, deduce that $e = -1$ by taking limits.

In any case, it follows for any p that $M_p \mid N_p$ so that $M \mid N$, and that χ is induced by λ. Then Theorem 3.14 implies $f(z) = g(z)$, so that $N = M$. ☐

Symbols and definitions

References

[DF04] David S. Dummit and Richard M. Foote, *Abstract Algebra*, John Wiley & Sons, Inc., 2004.

[DS05] Fred Diamond and Jerry Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics, Springer New York, NY, 2005.

[DI95] Fred Diamond and John Im, *Modular forms and modular curves*, CMS Conf. Proc. **17** (1995), 39-133. MR1357209

[Miy05] Toshitsune Miyake, *Modular Forms*, Springer Monographs in Mathematics, Springer Berlin, Heidelberg, 2005.

[Ser78] Jean-Pierre Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics, Springer New York, NY, 1978.