Explicit Level Lowering for 2-Dimensional Modular Galois Representations

---

A Thesis
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
Mathematical Science

---

by
Rodney L Keaton
December 2010

Accepted by:
Dr. Kevin James, Committee Chair
Dr. Jim Brown, Committee Chair
Dr. Hui Xue

Abstract

Let f be a normalized eigenform of level $N\ell^\alpha$ for some positive integer α and some odd prime ℓ satisfying $\gcd(\ell, n) = 1$. A construction of Deligne, Shimura, et. al., attaches an ℓ-adic continuous two-dimensional Galois representation to f. The Refined Conjecture of Serre states that such a representation should in fact arise from a normalized eigenform of level prime to ℓ.

In this thesis we present a proof of Ribet which allows us to "strip" these powers of ℓ from the level while still retaining the original Galois representation, i.e., the residual of our new representation arising from level N will remain isomorphic to the residual of our original representation arising from level $N\ell^\alpha$.

Acknowledgments

I cannot overstate my appreciation for my advisors, Dr. Jim Brown and Dr. Kevin James. I would have been lost without their encouragement, insight, and patience at every step of the thesis writing process.

I thank my friends Alison Gaines, Caitlin McMahon, Charles Gamble, James Johnson, and Neil Mork for their support through which graduate school has been made much easier. In addition, I thank my colleague and friend Vincent Rusnell. It is from our conversations that I have drawn much inspiration for my work.

I also owe a debt of gratitude to my parents, brother, and sister for their love which provides the firm foundation that I have stood on all of my life.

Finally, I express my deepest thanks to my wife Anna for always believing in me. It is to her that I dedicate this thesis.

Table of Contents

Chapter 1

Elliptic Modular Forms

1.1 Modular forms over the full modular group

In order to define modular forms, we first need to introduce the full modular group, its congruence subgroups, and a group action which will be used throughout.

Let $\mathfrak{H} := \{x + yi \in \mathbb{C} | x, y \in \mathbb{R}, y > 0\}$ and $\mathrm{SL}_2(\mathbb{R}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{R}) | ad - bc = 1 \right\}$.

We will define a group action of $\mathrm{SL}_2(\mathbb{R})$ on $\mathfrak{H}$ by setting $\gamma \cdot z = \dfrac{az + b}{cz + d}$

where $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{R})$ and $z \in \mathfrak{H}$, i.e., $\mathrm{SL}_2(\mathbb{R})$ acts on $\mathfrak{H}$ by fractional linear transformations. We must verify that this satisfies the necessary properties to be a group action. Note that

$$\mathrm{Im}\,(\gamma \cdot z) = \mathrm{Im}\left(\frac{az + b}{cz + d}\right) = \mathrm{Im}\left(\frac{(az + b)(c\bar{z} + d)}{|cz + d|^2}\right) = |cz + d|^{-2}\mathrm{Im}\,(adz + bc\bar{z})$$

and

$$\mathrm{Im}(adz + bc\bar{z}) = (ad - bc)\mathrm{Im}(z) = \mathrm{Im}(z).$$

Thus, $\mathrm{Im}(\gamma \cdot z) = |cz+d|^{-2}\mathrm{Im}(z)$. Hence, $\mathfrak{H}$ is preserved.

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$ be elements of $\mathrm{SL}_2(\mathbb{R})$. Then

$$I_2 \cdot z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \cdot z = \frac{1z+0}{0z+1} = z$$

and

$$\gamma(\gamma' \cdot z) = \gamma \cdot \frac{az+b}{cz+d} = \frac{(aa'+bc')z + (ab'+bd')}{(ca'+dc')z + (cb'+dd')} = (\gamma\gamma') \cdot z.$$

Thus, this is a group action.

However, for our purposes we will restrict our attention to a certain subgroup of $\mathrm{SL}_2(\mathbb{R})$.

Definition 1. The *full modular group* is defined to be

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{Mat}_2(\mathbb{Z}) | ad - bc = 1 \right\}$$

and will be denoted by $\Gamma(1)$.

Note that since $\Gamma(1)$ is a subgroup of $\mathrm{SL}_2(\mathbb{R})$, $\Gamma(1)$ acts on $\mathfrak{H}$ as well. With this action in mind, we have the following definition.

Definition 2. Let $f : \mathfrak{H} \to \mathbb{C}$ be a meromorphic function. We say f is a *weakly modular function of weight k and level* $\Gamma(1)$ if it satisfies the following:

$$f(\gamma \cdot z) = (cz+d)^k f(z), \text{ for every } z \in \mathfrak{H} \text{ and } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1).$$

From this definition we can see that to study weakly modular functions, it will be helpful to know more about the structure of $\Gamma(1)$. In order to do this we will prove the following:

Proposition 1. *Let* $T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ *and* $S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. *Then,* $\Gamma(1) =< S, T >$.

Proof. First it is clear that since $S, T \in \Gamma(1)$, $< S, T > \subset \Gamma(1)$. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$. Note that if $c = 0$, i.e., γ is upper triangular, then $a = d = \pm 1$. Also, as $b \in \mathbb{Z}$, we see that $\gamma = \pm IT^b = \pm I \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$, where the sign on I matches the sign of a. Since $-I = S^2 \in \Gamma(1)$, we have that $\gamma \in < S, T >$. Now, suppose that $c \neq 0$. Then it is sufficient to show that we can transform γ into an upper triangular matrix using some element of $< S, T >$. First, note that

$$\gamma T^n = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & an + b \\ c & nc + d \end{pmatrix}.$$

Clearly, we can choose an $n \in \mathbb{Z}$ such that $|nc + d| \leq |c|/2 < |c|$. Therefore, given (c, d), the bottom row of γ, we can find a new matrix with bottom row (c, d'), with $|d'| \leq |c|/2$. Now, note that,

$$\gamma S = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$$

Using this we can use the bottom row (c, d') from above to find a matrix with bottom row $(d', -c)$. Hence, by repeating this process a finite number of times, we see that we can transform γ into an upper triangular matrix using an element of $< S, T >$. Thus, $\gamma \in < T, S >$, which completes the proof. □

Let f be weakly modular of weight k and level $\Gamma(1)$. Then we know that for every $z \in \mathfrak{H}$, f satisfies:

$$f(z + 1) = f(T \cdot z) = (1)^k f(z) = f(z)$$

$$f(z) = f(-I \cdot z) = (-1)^k f(z)$$

Thus, f has period 1, and either k is even or f is the zero function.

In order to define a modular form we must consider the action of $\Gamma(1)$ on $\overline{\mathfrak{H}}$, where $\overline{\mathfrak{H}} := \mathfrak{H} \cup \mathbb{Q} \cup \{i\infty\}$. Note, by $\mathbb{Q}$, we mean the set of complex numbers $x + yi$, where x is rational and y is zero. The action of $\Gamma(1)$ on $i\infty$ is given by, $\gamma \cdot i\infty = a/c$, for the same γ as before, and the action on $\mathbb{Q}$ is the same as was defined for $\mathfrak{H}$. We can now define an equivalence relation on the set $\mathbb{Q} \cup \{i\infty\}$, by $x \sim y$ if there exists some $\gamma \in \Gamma(1)$ such that $\gamma \cdot x = y$. It is not hard to see that $\Gamma(1)$ acts transitively on the set $\mathbb{Q} \cup \{i\infty\}$, i.e., the entire set becomes one equivalence class under the previously defined relation. While this relation is somewhat trivial in this case, it will become more important in later sections. We call this equivalence class the "cusp" at $i\infty$.

Let $f : \mathfrak{H} \to \mathbb{C}$ be a meromorphic period one function. Let $D := \{z \in \mathbb{C} \colon\ |z| < 1\}$ be the open unit disk in $\mathbb{C}$, and let $D' := D - \{0\}$. Consider the change of variables $z \mapsto q := e^{2\pi i z}$, where $z \in \mathfrak{H}$. Note, this map is periodic and sends $\mathfrak{H}$ to D' holomorphically. Also, this map gives us a function $g : D' \to \mathbb{C}$ corresponding to f by $g(q) = f(z)$. Since f is meromorphic, so is g. Let $g(q) = \sum_{n=-\infty}^{\infty} a_n q^n$ be the Laurent expansion of g. We see that as $\mathrm{Im}(z) \to \infty$, we have $q \to 0$. We say f is meromorphic at $i\infty$ if g extends meromorphically to the point at zero, i.e., if the coefficients a_n of the Laurent expansion of g are zero for all but finitely many negative n. Also, we say that f is holomorphic at $i\infty$ if $a_n = 0$ when n is negative, and finally we say that f vanishes at $i\infty$ if $a_n = 0$ when n is not positive. From now on we will just consider the Fourier expansion $f(z) = \sum_n a_n e^{2\pi i n z}$ directly without referring to the corresponding function g, although we will still denote $e^{2\pi i z}$ by q.

We saw earlier that our weakly modular functions were meromorphic and of period one, therefore by the preceding paragraph we can consider the behaviour of such functions at $i\infty$. This leads us to our next definition.

Definition 3. We say a weakly modular function f of weight k and $\Gamma(1)$ is a *modular form of weight k and level* $\Gamma(1)$ if f is holomorphic on $\mathfrak{H} \cup \{i\infty\}$. The set of all modular forms of

weight k and level $\Gamma(1)$ is denoted $M_k(\Gamma(1))$. Further, we say that a modular form of weight k and level $\Gamma(1)$ is a *cusp form of weight k and level* $\Gamma(1)$ if f vanishes at $i\infty$. The set of all cusp forms of weight k and level $\Gamma(1)$ is denoted $S_k(\Gamma(1))$.

Let $f(z),\ g(z) \in M_k(\Gamma(1))$. It is clear that $cf(z) \in M_k(\Gamma(1))$ for any $c \in \mathbb{C}$, and that $f(z) + g(z) \in M_k(\Gamma(1))$. Combining these two facts it is not hard to see that $M_k(\Gamma(1))$ forms a $\mathbb{C}$-vector space. Note, the same holds for $S_k(\Gamma(1))$. Further, if $f(z) \in M_{k_1}(\Gamma(1))$ and $g(z) \in M_{k_2}(\Gamma(1))$, then $f(z)g(z) \in M_{k_1+k_2}(\Gamma(1))$. Once again, the same thing is true for cusp forms. Therefore, $M(\Gamma(1)) := \bigcup_{k=0}^{\infty} M_k(\Gamma(1))$ and $S(\Gamma(1)) := \bigcup_{k=0}^{\infty} S_k(\Gamma(1))$ are graded $\mathbb{C}$-algebras.

To give an example of a modular form, let $k > 2$ with k even. Define an Eisenstein Series by

$$G_k(z) := \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(mz+n)^k}.$$

Proposition 2. *The Eisenstein series, $G_k(z)$, is a modular form of weight k and level $\Gamma(1)$.*

Proof. Let $z \in \mathfrak{H}$. Define the lattice $\Lambda := z\mathbb{Z} + \mathbb{Z}$. Then rewriting we have

$$G_k(z) = \sum_{\substack{\omega\in\Lambda \\ \omega\neq 0}} \frac{1}{\omega^k}.$$

Let P_1 be the parallelogram with boundary points $\{-1-z, -z, 1-z, 1, 1+z, z, -1+z, -1\}$. Let r and R denote the minimum and maximum distances from 0 to P_1, respectively. Then, if ω is any of these 8 non-zero lattice points in P_1, then $r \leq |\omega| \leq R$. If we now consider the parallelogram P_2 with boundary points

$$\{-2-2z, -1-2z, -2z, 1-2z, 2-2z, 2-z, 2, 2+z, 2+2z,$$

$$1+2z, 2z, -1+2z, -2+2z, -2+z, -2, -2-z\},$$

we see that if ω is now any of these 16 new lattice points in P_2, then $2r \leq |\omega| \leq 2R$. In general, in P_n we have $8n$ new lattice points such that $nr \leq |\omega| \leq nR$, for any new lattice point ω in P_n. Therefore,

$$\frac{1}{(nR)^k} \leq \frac{1}{|\omega|^k} \leq \frac{1}{(nr)^k},$$

for any new lattice point ω in P_n. Let S_n denote the sum of $\frac{1}{|\omega|^k}$ over the first n parallelograms P_i, i.e., we take the summation over the $8\sum_{l=1}^{n} l$ non-zero lattice points nearest to the origin. Then,

$$\sum_{l=1}^{n} \frac{8l}{(Rl)^k} = \frac{8}{R^k} \sum_{l=1}^{n} \frac{1}{l^{k-1}} \leq S_n \leq \frac{8}{r^k} \sum_{l=1}^{n} \frac{1}{l^{k-1}} = \sum_{l=1}^{n} \frac{8l}{(rl)^k}.$$

Thus, $S_n \leq \frac{8\zeta(k-1)}{r^k}$, where ζ is the Riemann zeta function. Note, our upper bound does not depend on n, hence

$$\lim_{n\to\infty} S_n \leq \frac{8\zeta(k-1)}{r^k} < \infty,$$

where the final inequality comes from the fact that $\zeta(s)$ converges when the real part of s is greater than 1. This gives us absolute convergence for $G_k(z)$. Note, that as $G_k(z)$ is absolutely convergent on all of $\mathfrak{H}$, then it is not hard to see that $G_k(z)$ is uniformly convergent on any compact subset of $\mathfrak{H}$. Thus, $G_k(z)$ is holomorphic on $\mathfrak{H}$.

Now, as S and T generate $\Gamma(1)$, it is sufficient to show that $G_k(z+1) = G_k(z)$, and $G_k(-1/z) = z^k G_k(z)$ in order to show that $G_k(z)$ is a weakly modular function over $\Gamma(1)$. Observe that,

$$\begin{aligned} G_k(z+1) &= \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(m(z+1)+n)^k} \\ &= \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(mz+(m+n))^k} \end{aligned}$$

$$
\begin{aligned}
&= \sum_{\substack{(m,d)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(mz+d)^k} \\
&= G_k(z)
\end{aligned}
$$

and

$$
\begin{aligned}
z^{-k}G_k(-1/z) &= \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{z^{-k}}{(m(-1/z)+n)^k} \\
&= \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \frac{1}{(m+nz)^k} \\
&= G_k(z).
\end{aligned}
$$

Thus, $G_k(z)$ is a weakly modular function of weight k and level $\Gamma(1)$. All that remains is to show that $G_k(z)$ is holomorphic at $i\infty$. In order to do this we will determine the Fourier expansion of $G_k(z)$.

Let $\sigma_k(n) := \sum_{d|n} d^{k-1}$ and let B_k denote the k^{th} Bernoulli number which is given as the k^{th} coefficient in the Taylor series expansion of $\frac{x}{e^x-1}$. We begin by taking the logarithmic derivative of the product formula for $\sin a$ for $a \in \mathfrak{H}$. We obtain

$$
\pi \cot \pi a = \frac{1}{a} + \sum_{n=1}^{\infty} \left(\frac{1}{a+n} + \frac{1}{a-n} \right). \tag{1.1}
$$

Note we have used Hadamard's formula in this step, which gives that $\sin \pi a = \prod_{n\in\mathbb{Z}} (a-n)$. We can rewrite the left hand side to get:

$$
\pi \cot \pi a = \pi i + \frac{2\pi i}{e^{2\pi i a} - 1}. \tag{1.2}
$$

Multiply both sides of (1.2) by a and replace $2\pi ia$ with x. The right hand side becomes

$$\begin{aligned} a\pi i + \frac{2\pi ia}{e^{2\pi ia}-1} &= \frac{x}{2} + \frac{x}{e^x-1} \\ &= \frac{x}{2} + \sum_{k=0}^{\infty} \frac{B_k x^k}{k!}. \end{aligned}$$

Multiplying the right hand side of (1.1) by a and rewriting yields:

$$\begin{aligned} 1 + \sum_{n=1}^{\infty} \left(\frac{a}{a+n} + \frac{a}{a-n} \right) &= 1 + \sum_{n=1}^{\infty} \frac{a}{n} \left(\frac{1}{a/n+1} + \frac{1}{a/n-1} \right) \\ &= 1 + \sum_{n=1}^{\infty} \frac{x}{2\pi in} \left(\frac{1}{1-\dfrac{-x}{2\pi in}} - \frac{1}{1-\dfrac{x}{2\pi in}} \right) \\ &= 1 + \sum_{n=1}^{\infty} \frac{x}{2\pi in} \left(\sum_{k=0}^{\infty} \left(\frac{-x}{2\pi in} \right)^k - \sum_{k=0}^{\infty} \left(\frac{x}{2\pi in} \right)^k \right) \\ &= 1 + \sum_{m=1}^{\infty} \left(\frac{(-1)^{m-1}}{(2\pi i)^m} \sum_{j=1}^{\infty} \frac{1}{j^m} - \frac{1}{(2\pi i)^m} \sum_{j=1}^{\infty} \frac{1}{j^m} \right) x^m \\ &= 1 - \sum_{m=1}^{\infty} \left(\frac{2}{(2\pi i)^{2m}} \zeta(2m) \right) x^{2m}. \end{aligned}$$

Our equation now looks like:

$$\frac{x}{2} + \sum_{k=0}^{\infty} \frac{B_k x^k}{k!} = 1 - \sum_{n=1}^{\infty} \left(\frac{2}{(2\pi i)^{2n}} \zeta(2n) \right) x^{2n}.$$

Now, comparing the coefficients of x^{2n} gives us that $B_0 = 1$, $B_1 = -1/2$, and $B_{2k+1} = 0$ for every $k > 1$. Further, when $k > 0$ and even we have the following well known identity:

$$\frac{\zeta(k)}{\pi^k} = \frac{(2i)^k B_k}{2 \cdot k!}. \tag{1.3}$$

Combining (1.1) and (1.2) yields the following equality

$$\frac{1}{a}+\sum_{n=1}^{\infty}\left(\frac{1}{a+n}+\frac{1}{a-n}\right)=\pi i+\frac{2\pi i}{e^{2\pi i a}-1}. \tag{1.4}$$

Differentiating (1.4) with respect to a a total of $(k-1)$-times and replacing a with mz we get the following equation:

$$\sum_{n=-\infty}^{\infty}\frac{1}{(mz+n)^k}=\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}n^{k-1}e^{2\pi i n m z}.$$

Using the identity (1.3), replacing n by d, and $e^{2\pi i z}$ by q on the right hand side we get:

$$\frac{(2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty}n^{k-1}e^{2\pi i n m z}=\frac{-2k}{B_k}\zeta(k)\sum_{d=1}^{\infty}d^{k-1}q^{dm}.$$

Therefore,

$$\begin{aligned}
G_k(z) &= \sum_{m=-\infty}^{\infty}\sum_{n=-\infty}^{\infty}\frac{1}{(mz+n)^k} \quad \text{for } (m,n)\neq(0,0)\\
&= \sum_{n=-\infty}^{\infty}\left(\frac{1}{n^k}\right)+2\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty}\frac{1}{(mz+n)^k}\\
&= 2\zeta(k)+2\sum_{m=1}^{\infty}\sum_{n=-\infty}^{\infty}\frac{1}{(mz+n)^k}\\
&= 2\zeta(k)\left(1-\frac{2k}{B_k}\sum_{m,d=1}^{\infty}d^{k-1}q^{dm}\right).
\end{aligned}$$

Fix a power of q, say r. Then d must take the value of every divisor of n. Thus, our coefficient on q^n is $\sigma_{k-1}(n)$. Thus,

$$G_k(z)=2\zeta(k)\left(1-\frac{2k}{B_k}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n\right).$$

From here, we can see that the Fourier expansion of $G_k(z)$ has no negative terms, i.e., $G_k(z)$ is holomorphic at $i\infty$. This completes the proof that $G_k(z) \in M_k(\Gamma(1))$. $\square$

Not only have we proven that the Eisenstein series is a modular form, but in the process we have derived its Fourier expansion. In the future, we will need to make use of the normalized Eisenstein series, where normalized means that we multiply by a suitable constant so that the first Fourier coefficient is one. For this normalized series we get:

$$E_k(z) := \frac{1}{2\zeta(k)} G_k(z) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n.$$

Equivalently, we can define the normalized Eisenstein series as:

$$E_k(z) = \frac{1}{2} \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n)=1}} \frac{1}{(mz+n)^k}.$$

The equivalence of these is not hard to show and will be left as an exercise to the curious reader. Using these normalized Eisenstein series, we can construct a cusp form of $\Gamma(1)$ level. For example, consider the following function:

$$\Delta(z) := \frac{(2\pi)^{12}}{1728} (E_4(z)^3 - E_6(z)^2).$$

This is called the *discriminant modular form*, which comes from this function's application to elliptic curves. From previous results we see that $\Delta(z)$ is a modular form of $\Gamma(1)$ level and weight 12. Further, we have that the constant term in the Fourier expansion of $E_4(z)^3$ is cancelled by the constant term in the Fourier expansion of $E_6(z)^2$, hence $\Delta(z)$ is a cusp form. Using this same idea, we can prove the following:

Proposition 3. *For $k > 2$, $M_k(\Gamma(1)) = S_k(\Gamma(1)) \oplus \mathbb{C} \cdot E_k$.*

Proof. Let $f(z) = \sum_{n=0}^{\infty} a_n q^n \in M_k(\Gamma(1))$. Then $f(z) - a_0 E_k(z)$ has no constant term in its Fourier expansion. Hence, $f(z) - a_0 E_k(z) \in S_k(\Gamma(1))$. Noting that $E_k(z) \notin S_k(\Gamma(1))$, we have the desired result. □

1.2 Modular forms over congruence subgroups

In Section 1.1 we defined and gave examples of modular forms and cusp forms of full level. In this section we will be interested in defining modular forms and cusp forms of other levels. To begin, we must consider a special class of subgroups of $\Gamma(1)$.

Definition 4. For $N \in \mathbb{Z}_{>0}$, the subgroup

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

of $\Gamma(1)$ is called *the principal subgroup of level* N.

Note, if N' is a multiple of N, then $\Gamma(N') \leq \Gamma(N)$. We define a group homomorphism

$$\psi : \Gamma(1) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}), \text{ by } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \pmod{N}.$$

Then, $\ker(\psi) = \Gamma(N)$, so we get that $\Gamma(N) \lhd \Gamma(1)$.

Definition 5. We define a *congruence subgroup of level* N to be any subgroup H of $\Gamma(1)$ satisfying $\Gamma(N) \leq H \leq \Gamma(1)$.

Similarly, we have that if H is a congruence subgroup of level N and N' is a multiple of N, then H is a congruence subgroup of level N'. Some important congruence subgroups

that we will use throughout are:

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) | c \equiv 0 \pmod{N} \right\},$$

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) | a \equiv d \equiv 1 \pmod{N} \right\},$$

$$\Gamma_0(N, M) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) | b \equiv 0 \pmod{M} \right\}.$$

Since congruence subgroups are contained in $\Gamma(1)$, it is clear that we once again have a group action on $\overline{\mathfrak{H}}$. In order to define a modular function in this setting, we will need the weight k slash operator, which is defined in the following way:

$$f|_k[\gamma](z) := \det \gamma^{k/2}(cz + d)^{-k} f(\gamma z), \text{ for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q}),$$

where $\mathrm{GL}_2^+(\mathbb{Q})$ is the group of all two by two matrices with rational entries and positive determinant and $f : \mathfrak{H} \to \mathbb{C}$. Note, given the action of $\Gamma(1)$ on $\overline{\mathfrak{H}}$, the action of $\mathrm{GL}_2^+(\mathbb{Q})$ on $\overline{\mathfrak{H}}$ is obvious, although at the moment we are only concerned with elements of $\Gamma(1)$. Also, if k is clear from the context, we omit it. The following proposition gives us a useful property of the slash operator.

Proposition 4. *Let $f : \mathfrak{H} \to \mathbb{C}$, and let $k \in \mathbb{N}$. Also, let $\gamma, \gamma' \in \mathrm{GL}_2^+(\mathbb{Q})$. Then, $f|_k[\gamma\gamma'](z) = (f|_k[\gamma])\,|_k[\gamma'](z)$.*

Proof. Suppose that $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $\gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Expanding out $f|_k[\gamma\gamma'](z)$ yields:

$$\begin{aligned} f|_k[\gamma\gamma'](z) &= \det(\gamma\gamma')^{k/2}((dc' + ca')z + (cb' + dd'))^{-k} f((\gamma\gamma')z) \\ &= \det(\gamma)^{k/2} \det(\gamma')^{k/2} \left(\frac{ca'z + cb'}{c'z + d'} + d\right)^{-k} (c'z + d')^{-k} f(\gamma(\gamma' z)) \\ &= \det(\gamma')^{k/2}(c'z + d')^{-k} f|_k[\gamma](\gamma' z) \\ &= (f|_k[\gamma])\,|_k[\gamma'](z). \end{aligned}$$

□

Using this operator, we make the following definition.

Definition 6. Let $f : \mathfrak{H} \to \mathbb{C}$ be a meromorphic function. Let $\Gamma \leq \Gamma(1)$ be a congruence subgroup of level N. We say f is a *weakly modular function of weight k and level Γ* if it satisfies the following:

$$f|_k[\gamma](z) = f(z), \text{ for every } z \in \mathfrak{H}, \gamma \in \Gamma.$$

Note. if the subgroup is clear from context, we say that f has level N.

In order to define a modular form in this setting, we will need to examine the behaviour of such a function at all *cusps*. In order to make this more explicit, we must first define what is meant by a cusp. Note that while $\Gamma(1)$ acts transitively on the cusps, it is not true that congruence subgroups do the same. For example, it is not hard to see that there is no $\gamma \in \Gamma(3)$ such that $\gamma \cdot \{i\infty\} = 1/2$. Therefore, unlike the full level case, the equivalence relation defined in §1.1 divides $\{i\infty\} \cup \mathbb{Q}$ into multiple equivalence classes.

Definition 7. Let $\Gamma \leq \Gamma(1)$ be a congruence subgroup. A *cusp* is defined to be an equivalence class of $\{i\infty\} \cup \mathbb{Q}$ under the action of Γ on $\overline{\mathfrak{H}}$.

In order to make this behaviour of modular functions at the cusps more precise, we will first look at the cusp at $i\infty$ as we did in §1.1. The major difference in this setting is that for some congruence subgroups $\Gamma \leq \Gamma(1)$, we may not have that our translation matrix T from §1.1 is an element of Γ. However, we can see that for some $h \in \mathbb{Z}$,

$$T^h := \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma.$$

As an example, consider the group $\Gamma(N)$. The group has T^N as an element, but not T. With this difference in consideration, we see that a weakly modular function f may no longer have period 1, but will certainly have period h, for some integer h. Then, just as in the previous section, we see that there is some function $g : D' \to \mathbb{C}$ corresponding to our weakly modular function f, where D' is the punctured unit disc in the complex plane. However, we now have that $f(z) = g(q_h)$ where $q_h := e^{2\pi iz/h}$. Note, again we have that the map $z \mapsto q_h$ is a holomorphic map from $\mathbb{C}$ to D'. As in §1.1, we have the Fourier expansion $f(z) = \sum_n a_n e^{2\pi inz/h}$, and we say f is meromorphic at $i\infty$ if $a_n = 0$ for all but finitely many negative n. Also, f is holomorphic at $i\infty$ if $a_n = 0$ for all negative n, and f vanishes at $i\infty$ if $a_n = 0$ for all non-positive n.

In this setting, it is not enough to consider the behavior of a modular function at just one cusp since we will require holomorphicity at every cusp in order to define a modular form for a congruence subgroup. First note that since $\Gamma(1)$ acts transitively on the set $\{i\infty\} \cup \mathbb{Q}$, we have that for every rational number r, there exists some $\gamma \in \Gamma(1)$ such that $\gamma r = i\infty$. Using the same f as in the previous paragraph, we will consider the function $g(z) := f|_k[\gamma^{-1}](z)$. First, we will prove the following:

Proposition 5. *Let f be a weakly modular function of weight k and level Γ with $\Gamma(N) \leq \Gamma \leq \Gamma(1)$. Let $\gamma \in \Gamma(1)$. Then, $f|_k[\gamma]$ is a weakly modular function of weight k and level*

$\gamma^{-1}\Gamma\gamma$.

Proof. Note, for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $z \in \mathfrak{H}$, we have that $cz + d$ is never zero or infinity, hence $f|_k[\gamma]$ is still meromorphic with the same zeros and poles as f. Now, let $\gamma' \in \gamma^{-1}\Gamma\gamma$. We can write $\gamma' = \gamma^{-1}g\gamma$ for some $g \in \Gamma$. Then,

$$\begin{aligned} (f|_k[\gamma])|_k[\gamma'](z) &= (f|_k[\gamma])|_k[\gamma^{-1}g\gamma](z) \\ &= f|_k[\gamma\gamma^{-1}g\gamma](z) \\ &= f|_k[g\gamma](z) \\ &= f|_k[\gamma](z) \end{aligned}$$

Thus, completing the proof. □

An important fact to note in light of this proposition is that since $\Gamma(N) \lhd \Gamma(1)$, we have that $\Gamma(N) \leq \gamma^{-1}\Gamma\gamma$, i.e., $\gamma^{-1}\Gamma\gamma$ is again a congruence subgroup of the same level as Γ for every $\gamma \in \Gamma(1)$. From this we have that our translation matrix T^h is in $\gamma^{-1}\Gamma\gamma$ as well.

Returning to our previous function $g(z)$, we can see that g has period h for some positive integer h. From this, we get the Fourier expansion $g(z) := \sum_{n=-\infty}^{\infty} a_n q_h^n$, which we can then use to examine the behavior of g at $i\infty$. By construction the behavior of g near $i\infty$ is the same as the behavior of our original function $f(z)$ near our rational number r. Thus, we can use this method to examine the behavior of a weakly modular function at any rational number, hence at any cusp. This brings us to our main definition:

Definition 8. Let $\Gamma \leq \Gamma(1)$ be a congruence subgroup. Let k be a positive integer. Let f be a weakly modular function of weight k and level Γ which is also holomorphic on $\mathfrak{H}$. We say that f is a *modular form of weight k and level Γ* if $f|_k[\gamma]$ is holomorphic at $i\infty$ for all $\gamma \in \Gamma(1)$. Further, if $f|_k[\gamma]$ vanishes at $i\infty$ for all $\gamma \in \Gamma(1)$ then we say that f is a *cusp form*

of weight k and level Γ.

We denote the space of weight k, level Γ modular forms by $M_k(\Gamma)$. Similarly, we denote the space of weight k, level Γ cusp forms by $S_k(\Gamma)$.

As an example, we again consider an Eisenstein series, although this time of levels $\Gamma(N)$ and $\Gamma_1(N)$, for some $N \in \mathbb{N}$. Let $\overline{v} \in (\mathbb{Z}/N\mathbb{Z})^2$, and let $k > 2$ be an integer. Consider the following series

$$G_k^{\overline{v}}(z) := \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\equiv\overline{v} \pmod N}} \frac{1}{(mz+n)^k}.$$

Note, if $\overline{v} = (0,0)$ then remove the point $(m,n) = (0,0)$ from the summation. As in the previous section we can compute the Fourier expansion of such an Eisenstein series. In order to explicitly state the Fourier expansion of this Eisenstein series when $N > 1$ we will need the following definitions:

$$\begin{aligned}
\delta(v_1) &:= \left\{ \begin{array}{ll} 1 & \text{if } v_1 = 0 \\ 0 & \text{otherwise} \end{array} \right\}, \\
\zeta^{v_2}(k) &:= \sum_{\substack{d\equiv v_2 \pmod N \\ d\neq 0}} \frac{1}{d^k}, \\
C_k &:= \frac{(-2\pi i)^k}{(k-1)!}, \\
\xi_N &:= e^{2\pi i/N}, \\
\sigma_{k-1}^{\overline{v}} &:= \sum_{\substack{m|n \\ n/m\equiv v_1 \pmod N}} \operatorname{sgn}(m) m^{k-1} \xi_N^{v_2 m}.
\end{aligned}$$

Using these definitions we get the Fourier expansion,

$$G_k^{\overline{v}}(z) = \delta(v_1)\zeta^{v_2}(k) + \frac{C_k}{N^k} \sum_{n=1}^{\infty} \sigma_{k-1}^{\overline{v}}(n) q_N^n.$$

For more details regarding the derivation of this Fourier expansion, one can refer to Chapter

4, §2 of [5]. It should be mentioned that we can also consider the normalized Eisenstein series just as in §1. Let $\epsilon_N = 1/2$ if $N = 2$, otherwise let $\epsilon_N = 1$. Then, the normalized Eisenstein series associated to $G_k^{\overline{v}}(z)$ is given by:

$$E_k^{\overline{v}}(z) := \epsilon_N \sum_{\substack{(m,n)\equiv\overline{v} \pmod N \\ (m,n)=1}} \frac{1}{(mz+n)^k}.$$

The relation between $G_k^{\overline{v}}(z)$ and $E_k^{\overline{v}}(z)$ is the following:

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

Where $\zeta_+^n(k) := \sum_{\substack{m=1 \\ m\equiv n \pmod N}}^{\infty} \frac{1}{m^k}$ is a modified Riemann zeta function. The main thing to note from this relationship is that $G_k^{\overline{v}}$ can be represented as a linear combination of normalized Eisenstein series.

Proposition 6. *([12, Prop. 3.3.21]) $G_k^{\overline{v}}(z) \in M_k(\Gamma(N))$. Further, if $v_1 \equiv 0 \pmod N$, then $G_k^{\overline{v}}(z) \in M_k(\Gamma_1(N))$.*

Now, we wish to examine the structure of $M_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N))$ a little more closely. In order to do this we will need the following definition.

Definition 9. *A Dirichlet character modulo N* is a group homomorphism,

$$\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times.$$

Note. For conciseness in the future we will just refer to χ as a character modulo N.

Let χ be a character modulo N. If we define $\chi(n) = 0$ for all non-units $n \in \mathbb{Z}/N\mathbb{Z}$, then we can think of χ as map from $\mathbb{Z}/N\mathbb{Z}$ to $\mathbb{C}$. Further, for all $n \in \mathbb{Z}$ if we define

$\chi(n) := \chi(n \pmod N)$, then we can think of χ as a map from $\mathbb{Z}$ to $\mathbb{C}$. For a character χ modulo N define the following set

$$M_k(N, \chi) := \{f \in M_k(\Gamma_1(N)) \mid f|_k[\gamma] = \chi(\gamma)f \text{ for } \gamma \in \Gamma_0(N)\}$$

where $\chi(\gamma) := \chi(d)$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. If $\chi'(n) = 1$ for all n satisfying $(n, N) = 1$, we call χ' the trivial character modulo N, and $M_k(N, \chi') = M_k(\Gamma_0(N))$. Note, if $f \in M_k(N, \chi)$, we say f is a modular form with character χ. It is not hard to see that the set $M_k(N, \chi) = \{0\}$ if $\chi(-1) \neq (-1)^k$. To see this let $\gamma = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Suppose $N > 2$. Note, $\gamma \in \Gamma_0(N)$. Let $f \in M_k(N, \chi)$. Then we have the following:

$$f|[\gamma] = (-1)^k f = \chi(-1)f.$$

Therefore, if $(-1)^k \neq \chi(-1)$ then $f = 0$. In the future, unless otherwise stated, we will assume that this parity condition is satisfied by our associated characters.

As an example of such a form we can construct an Eisenstein series which is a certain linear combination of our previous Eisenstein series $G_k^{\overline{v}}$. Let χ and ψ be characters modulo s and t respectively, where $st = N$. Also, we require that $(\chi\psi)(-1) = (-1)^k$. Let ψ be primitive. Now define the following Eisenstein series for $k > 2$:

$$G_k^{\chi,\psi}(z) := \sum_{c=0}^{s-1} \sum_{d=0}^{t-1} \sum_{e=0}^{s-1} \chi(d)\overline{\psi}(d) G_k^{\overline{(cv, d+ev)}}(z).$$

Where $\overline{\psi}$ denotes the complex conjugate of ψ.

Proposition 7. *([5, Pg. 127]) $G_k^{\chi,\psi}(z) \in M_k(N, \chi\psi)$. Note, we are considering χ and ψ lifted to characters modulo N, so it makes sense to take their product.*

To see the Fourier expansion of this Eisenstein series we will give the Fourier expansion of the corresponding normalized Eisenstein series and the constant multiple which yields $G_k^{\chi,\psi}(z)$. First, define the following normalized Eisenstein series by its Fourier expansion:

$$E_k^{\chi,\psi}(z) := \delta(\chi)L(1-k,\psi) + 2\sum_{n=1}^{\infty}\sigma_{k-1}^{\chi,\psi}(n)q^n,$$

where $\delta(\chi) = 1$ if χ is the trivial character, otherwise $\delta(\chi) = 0$. Also, set

$$\sigma_{k-1}^{\chi,\psi}(n) := \sum_{\substack{m|n \\ m>0}} \chi(n/m)\psi(m)m^{k-1}.$$

Theorem 8. *([5, Thm. 4.5.1]) We have*

$$G_k^{\chi,\psi}(z) = \frac{C_k g(\overline{\psi})}{t^k} E_k^{\chi,\psi}(z).$$

This property of being able to explicitly compute the Fourier coefficients of Eisenstein series will be very useful in later sections.

Concerning the structure of the sets $M_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N))$ we have the following proposition.

Proposition 9. *([12, Prop. 3.3.28]) The spaces $M_k(\Gamma_1(N))$ and $S_k(\Gamma_1(N))$ have the following decompositions*

$$M_k(\Gamma_1(N)) \cong \bigoplus_{\chi} M_k(N,\chi),$$

$$S_k(\Gamma_1(N)) \cong \bigoplus_{\chi} S_k(N,\chi),$$

where the definition of $S_k(N,\chi)$ should be clear from above and the summation is taken over all characters modulo N.

1.3 Hecke Operators

In this section we will define and examine a certain set of operators on our space $M_k(\Gamma)$. Throughout let $f \in M_k(N, \chi)$ unless otherwise stated. To begin, we will need some preliminary operators, namely, the U_n and V_n operators, defined as follows:

$$\begin{aligned} f|U_n &:= n^{k/2-1} \sum_{u=0}^{n-1} f| \begin{pmatrix} 1 & u \\ 0 & n \end{pmatrix} \\ f|V_n &:= n^{-k/2} f| \begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix}. \end{aligned}$$

Of particular interest with these operators is their affect on the Fourier expansion of a given modular form.

Proposition 10. *Let $f(z) = \sum_{n=0}^{\infty} a_n q^n \in M_k(\Gamma)$ for some congruence subgroup Γ. Then we have the following:*

1. $$(f|U_m)(z) = \sum_{n=0}^{\infty} a_{mn} q^n.$$

2. $$(f|V_m)(z) = \sum_{n=0}^{\infty} a_n q^{mn}.$$

Proof. Expanding out the definition of the U_m operator gives the following:

$$\begin{aligned}
(f|U_m)(z) &= m^{k/2-1}\sum_{u=0}^{m-1} f|\begin{pmatrix}1 & u\\ 0 & m\end{pmatrix}(z)\\
&= m^{k/2-1}\sum_{u=0}^{m-1} m^{k/2}m^{-k}f\left(\frac{z+u}{m}\right)\\
&= m^{-1}\sum_{u=0}^{m-1}\sum_{n=0}^{\infty} a_n e^{2\pi i n(z+u)/m}\\
&= m^{-1}\sum_{u=0}^{m-1}\sum_{n=0}^{\infty} a_n e^{2\pi i nz/m}e^{2\pi i nu/m}.
\end{aligned}$$

Note if $m|n$ then $\sum_{u=0}^{m-1} e^{2\pi i nu/m} = m$ and if $(m,n) = d < m$ then $\sum_{u=0}^{m-1} e^{2\pi i nu/m} = \sum_{u=0}^{m-1} e^{2\pi i \frac{n}{d}u/\frac{m}{d}} = 0$ as this would be $(\frac{n}{d})$ summations of all $(\frac{m}{d})^{th}$ roots of unity. Using this fact we get the following:

$$\begin{aligned}
(f|U_m)(z) &= m^{-1}\sum_{n=0}^{\infty} m a_n e^{2\pi i nz/m}\\
&= \sum_{n=0}^{\infty} a_n e^{2\pi i nz/m}.
\end{aligned}$$

This gives us the following Fourier expansion,

$$(f|U_m)(z) = \sum_{n=0}^{\infty} b_n q^n,$$

where $b_n := a_{nm}$, which is the desired result.

Note, part (2) follows from a similar argument. □

Notice, from the Fourier expansions of $f|U_m$ and $f|V_m$ it is clear that the U and V operators preserve the property of "vanishing at cusps". Let p be a prime. Using the U and

V operators define the following operator:

$$T_p f := \begin{cases} f|U_p & \text{if} \quad (p,N) \neq 1 \\ f|U_p + \chi(p)p^{k-1}f|V_p & \text{if} \quad (p,N) = 1. \end{cases}$$

The operator T_p is known as the p^{th} Hecke operator. We have the following lemma, which we will not prove.

Lemma 11. *([5, Prop. 5.2.2]) If $f \in M_k(N,\chi)$ then so is $T_p f$. Further, if $f \in S_k(N,\chi)$ then so is $T_p f$.*

We will prove the following basic fact about the commutativity of Hecke operators.

Lemma 12. *Let p and q be distinct primes. Then $T_p T_q = T_q T_p$.*

Proof. To begin, we denote the n^{th} Fourier coefficient of a modular form f by $a_n(f)$. In order to prove this fact we will simply prove that the n^{th} Fourier coefficient of $T_p(T_q f)$ is the same as the n^{th} Fourier coefficient of $T_q(T_p f)$. Suppose that $(p,N) \neq 1$ and $(q,N) \neq 1$ where N is the level of f. Note, we will only prove this case since the other two cases follow similarly and are in fact easier. We have the following,

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

This completes the proof. □

We extend our definition to T_n where n is not necessarily prime. In order to do this let $n = \prod_{i=1}^{r} p_i^{e_i}$ be the prime factorization of n. Define T_1 to be the identity operator. For an

integer $s \geq 2$, define the following:

$$T_{p^s} := T_p T_{p^{s-1}} - p^{k-1}\chi(p) T_{p^{s-2}}.$$

This gives a way to inductively deal with powers of primes. Further, for any positive integers i, j and q a prime different from p we define

$$T_{p^i q^j} := T_{p^i} T_{q^j}.$$

Combining these two gives us the following:

$$T_n = \prod_{i=1}^{r} T_{p_i^{e_i}}.$$

Note, from above we also easily get that $T_m T_n = T_n T_m$ for m, n integers such that $(m, n) = 1$. Just as with the U and V operators we will be interested in looking at the Fourier expansion of $T_n f$. With regards to this we have the following proposition.

Proposition 13. *([5, Prop. 5.3.1]) Let $f \in M_k(N, \chi)$. Then,*

$$a_m(T_n f) = \sum_{d \mid \gcd(m,n)} \chi(d) d^{k-1} a_{mn/d^2}(f).$$

Proof. This proof is similar to the proof of the Fourier expansion of $f|U_n$, albeit slightly more involved. □

1.4 Eigenforms

In this section we will delve deeper into the structure of the spaces $M_k(\Gamma)$ and $S_k(\Gamma)$, where Γ is a congruence subgroup. To begin, we will define an inner product on the space

$S_k(\Gamma)$. We will need the following definition.

Definition 10. Let $\mathcal{F}$ be a closed region in $\mathfrak{h}$. Let Γ be congruence subgroup. We say $\mathcal{F}$ is a *fundamental domain for* Γ if for every $z \in \mathfrak{h}$ there exists some $\gamma \in \Gamma$ and $z' \in \mathcal{F}$ such that $\gamma \cdot z = z'$, and if for any two interior points $z_1, z_2 \in \mathcal{F}$ there is no $\gamma \in \Gamma$ such that $\gamma \cdot z_1 = z_2$. We will denote a fundamental domain for Γ by $\Gamma\backslash\mathfrak{h}$.

As an example we have the following fundamental domain for $\Gamma(1)$:

$$\Gamma(1)\backslash\mathfrak{h} = \{z \in \mathfrak{h} | -1/2 \leq \mathrm{Re}(z) \leq 1/2 \text{ and } |z| \geq 1\}.$$

We define an inner product on $S_k(\Gamma)$ for Γ a congruence subgroup as follows.

Definition 11. Let Γ be a congruence subgroup. Define $\overline{\Gamma}(1) := \Gamma(1)/\pm I$, and let $\overline{\Gamma}$ be defined to be the image of Γ in $\overline{\Gamma}(1)$. We define the *Petersson inner product*

$$<,>_\Gamma \colon M_k(\Gamma) \times S_k(\Gamma) \to \mathbb{C},$$

given by

$$< f, g >_\Gamma = \frac{1}{[\overline{\Gamma}(1) : \overline{\Gamma}]} \int_{\Gamma\backslash\mathfrak{h}} f(z)\overline{g(z)}y^k \frac{dxdy}{y^2}.$$

We will drop the subscript on $<,>$ when it is clear from context.

It is clear that $<,>_\Gamma$ is linear in the first term and anti-linear in the second term, and that $< f, g >_\Gamma = \overline{< g, f >_\Gamma}$. These are the properties necessary for $<,>_\Gamma$ to be a Hermitian inner product. Therefore, with $<,>_\Gamma$ we have that $S_k(\Gamma)$ is an inner product space. We should also note that if both f and g are not cusp forms then the integral will not converge. Recall that if we have an operator T on an inner product space then we define the adjoint of T to be the operator T^* satisfying

$$< Tf, g > = < f, T^* g > .$$

We have the following result describing the adjoints of the Hecke operators with respect to the Petersson inner product

Proposition 14. *([12, Prop. 48]) Let $f, g \in M_k(N, \chi)$ with at least one a cusp form. Then for n prime to N we have $< T_n f, g >= \chi(n) < f, T_n g >$.*

From the previous proposition we see that for n prime to N, then $T_n^* = \chi(n) T_n$. Therefore, $T_n T_n^* = T_n^* T_n$, i.e., T_n is a normal operator on $M_k(N, \chi)$. The spectral theorem from linear algebra tells us that we can find an orthogonal basis of $M_k(N, \chi)$ where each basis element is a simultaneous eigenfunction of all Hecke operators T_n for $(n, N) = 1$. Since these eigenfunctions are also modular forms, we will refer to them as eigenforms.

We can further refine our view of this basis by considering the subspaces $S_k(N, \chi)$ and $\mathcal{E}_k(N, \chi) := S_k(N, \chi)^\perp$, where the orthogonal complement is taken with respect to the Petersson inner product in the space $M_k(N, \chi)$. By construction we have that

$$M_k(N, \chi) \cong S_k(N, \chi) \oplus \mathcal{E}_k(N, \chi),$$

which should be reminiscent of Proposition 3 from §1.1. Naturally, we call $\mathcal{E}_k(N, \chi)$ the space of weight k, level N, Eisenstein series with associated character χ.

To conclude this section we will show that the Eisenstein series $E_k^{\chi,\psi} \in M_k(N, \chi\psi)$ from §1.2 is in fact an eigenform for all Hecke operators. We will need the following properties of the generalized divisor sum

$$\begin{aligned}
&\sigma_{k-1}^{\chi,\psi}(mn) = \sigma_{k-1}^{\chi,\psi}(m)\sigma_{k-1}^{\chi,\psi}(n) && \text{for } (m,n) = 1,\\
&\sigma_{k-1}^{\chi,\psi}(np) = \chi(p)\sigma_{k-1}^{\chi,\psi}(n) + \psi(p^{e+1})(p^{e+1})^{k-1}\sigma_{k-1}^{\chi,\psi}(m) && \text{for } n = mp^e \text{ and } (m,p) = 1,\\
&\chi\psi(p)p^{k-1}\sigma_{k-1}^{\chi,\psi}(n/p) = \psi(p)p^{k-1}\sigma_{k-1}^{\chi,\psi}(n) - \psi(p^{e+1})(p^{e+1})^{k-1}\sigma_{k-1}^{\chi,\psi}(m) && \text{for } n = mp^e \text{ and } (m,p) = 1,
\end{aligned}$$

where the proof of these properties is left as an exercise to the interested reader. Using these

three properties we have the following for $p \nmid N$

$$\sigma_{k-1}^{\chi,\psi}(np) + \chi\psi(p)p^{k-1}\sigma_{k-1}^{\chi,\psi}(n/p) = (\chi(p) + \psi(p)p^{k-1})\sigma_{k-1}^{\chi,\psi}(n),$$

where $n = p^e m$. Using this for p prime and $n > 0$ yields

$$\begin{aligned} a_n(T_p E_k^{\chi,\psi}) &= a_{np}(E_k^{\chi,\psi}) + \chi\psi(p)p^{k-1}a_{n/p}(E_k^{\chi,\psi}) \\ &= 2\sigma_{k-1}^{\chi,\psi}(np) + 2\chi\psi(p)p^{k-1}\sigma_{k-1}^{\chi,\psi}(n/p) \\ &= 2(\chi(p) + \psi(p)p^{k-1})\sigma_{k-1}^{\chi,\psi}(n) \\ &= (\chi(p) + \psi(p)p^{k-1})a_n(E_k^{\chi,\psi}). \end{aligned}$$

It remains to check that the same result holds for $n = 0$, which will be left as an exercise. Hence, we have that $E_k^{\chi,\psi}$ is an eigenform for all Hecke operators. Notice, we do not require the condition that the Hecke operator be away from the level. This is a phenomenon we will explore for cuspidal eigenforms in the next section.

1.5 Newforms

Up until this point we have been concerned only with modular forms at a fixed level N. In this section we will discuss what it means for a cusp form at level N to come from a lower level $M|N$. Our goal will be to make explicit what is meant by a cusp form which is "new" at a given level.

Note, we can trivially move between levels by noting that for $M|N$ we have that $S_k(\Gamma_1(M)) \subset S_k(\Gamma_1(N))$. However, there is a more interesting embedding of $S_k(\Gamma_1(M))$ into $S_k(\Gamma_1(N))$ using the V operator from §1.3. In fact we have the following propositions from [14], the first of which will be useful in Chapter 2, and the second we will use in this section.

Proposition 15. $V_r : M_k(\Gamma_1(N)) \to M_k(\Gamma_0(r) \cap \Gamma_1(N))$.

Proof. Let $f \in M_k(\Gamma_1(N))$. From Prop 5 we know that

$$f|V_r \in M_k\left(\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma_1(N) \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}\right) = M_k\left(\begin{pmatrix} 1/r & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(N) \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}\right).$$

Now, let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$.

Then,

$$\begin{pmatrix} 1/r & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b/r \\ cr & d \end{pmatrix}.$$

As the set of all matrices of the form $\begin{pmatrix} a & b/r \\ cr & d \end{pmatrix}$ contains $\begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}^{-1} \Gamma_1(N) \begin{pmatrix} r & 0 \\ 0 & 1 \end{pmatrix}$ we can see

$$\begin{pmatrix} a & b/r \\ cr & d \end{pmatrix} \in (\Gamma_0(r) \cap \Gamma_1(N)).$$

This completes the proof. □

Proposition 16. *Let $M|N$ and let $r = N/M$. For $f \in S_k(M, \chi)$ we have that $f|V_r \in S_k(N, \chi)$.*

Proof. Let $\gamma = \begin{pmatrix} a & b \\ crM & d \end{pmatrix} \in \Gamma_0(N)$. Note, $V_r \gamma V_r^{-1} = \begin{pmatrix} a & br \\ cM & d \end{pmatrix} \in \Gamma_0(M)$. Therefore,

$$\begin{aligned} (f|V_r)|\gamma &= (f|V_r \gamma V_r^{-1})|V_r \\ &= \chi(d) f|V_r. \end{aligned}$$

Thus, $f|V_r \in S_k(N, \chi)$. □

The following definition will use the previous proposition to make explicit what is meant by a cusp form which comes from a lower level.

Definition 12. For each divisor r of N, let i_r be the map

$$i_r : \left(S_k(\Gamma_1(Nr^{-1}))\right)^2 \to S_k(\Gamma_1(N))$$

given by

$$(f, g) \mapsto f + g|V_r.$$

The subspace of *oldforms at level N* is

$$S_k(\Gamma_1(N))^{\text{old}} := \sum_{\substack{p|N \\ p \text{ prime}}} i_p((S_k(\Gamma_1(Np^{-1})))^2)$$

and the subspace of *newforms at level N*, denoted $S_k(\Gamma_1(N))^{\text{new}}$, is the orthogonal complement of $S_k(\Gamma_1(N))^{\text{old}}$ with respect to the Petersson inner product.

The following proposition gives an important property with regards to the Hecke operators.

Proposition 17. *([5, Prop. 5.6.2]) The subspaces $S_k(\Gamma_1(N))^{\text{old}}$ and $S_k(\Gamma_1(N))^{\text{new}}$ are stable under the Hecke operators T_n for all n.*

The following corollary of this proposition follows from the same argument as in the previous section.

Corollary 18. *([5, Cor. 5.6.3]) The subspaces $S_k(\Gamma_1(N))^{\text{old}}$ and $S_k(\Gamma_1(N))^{\text{new}}$ each have an orthogonal basis of eigenforms for all Hecke operators away from the level.*

We are concerned primarily with the space of newforms, since we can relax the condition that our basis elements are only eigenforms away from the level. In order to make this more explicit we will need to following theorem.

Theorem 19. *([5, §5.7]) If $f \in S_k(\Gamma_1(N))$ has Fourier expansion $f(z) = \sum_{n=1}^{\infty} a_n q^n$ with $a_n = 0$ whenever $(n, N) = 1$, then f takes the form $f = \sum_{p|N} V_p f_p$ with each $f_p \in S_k(\Gamma_1(N/p))$.*

This theorem gives us a way to test if a cusp form is an oldform, which we will need in the following discussion.

We are now ready to define explicitly our basis elements of $S_k(\Gamma_1(N))^{\text{new}}$.

Definition 13. A *newform*, is an eigenform for the Hecke operators T_n, for all n, which is normalized so that the first Fourier coefficient is equal to 1.

Suppose that $f \in S_k(\Gamma_1(N))$ is an eigenform for Hecke operators away from the level. Further, suppose that $a_1(f) = 0$, i.e., we can not normalize f in the sense of the previous definition. We want to show that this forces $f \in S_k(\Gamma_1(N))^{\text{old}}$. Recall Proposition 13 in §1.3, this gives us that for all $n \in \mathbb{Z}^+$,

$$a_1(T_n f) = a_n(f).$$

Since f is an eigenform away from the level, we also have that

$$a_1(T_n f) = \lambda_n a_1(f),$$

where $(n, N) = 1$ and λ_n is the eigenvalue of f associated to T_n. These combine to yield

$$a_n(f) = \lambda_n a_1(f)$$

where $(n, N) = 1$. Since $a_1(f) = 0$ we have $a_n(f) = 0$ when $(n, N) = 1$, and by Thm. 19, $f \in S_k(\Gamma_1(N))^{\text{old}}$. We are now ready to prove the following theorem which will give the desired result for eigenforms in the subspace of newforms.

Theorem 20. *Let $f \in S_k(\Gamma_1(N))^{\text{new}}$ be a nonzero eigenform for all Hecke operators away from the level. Then,*

1. *f is an eigenform for all Hecke operators and some suitable multiple of f is a newform.*

2. *If $\tilde{f}$ satisfies the same condition as f and has the same eigenvalues, then $\tilde{f} = cf$ for some constant c.*

The set of newforms in the space $f \in S_k(\Gamma_1(N))^{\text{new}}$ form an orthogonal basis of this space. Each such newform lies in $S_k(N, \chi)$, for some character χ, and satisfies $T_n f = a_n(f)$ for all $n \in \mathbb{Z}^+$.

Proof. From the argument given before this theorem we may assume that we can normalize f so that $a_1(f) = 1$. Without loss of generality assume that f is normalized in this way. Let $m \in \mathbb{Z}^+$. Define the following function,

$$g_m = T_m f - a_m(f) f.$$

Then, by Proposition 17 we know that $g_m \in S_k(\Gamma_1(N))^{\text{new}}$. Computing the first Fourier coefficient of g_m yields

$$a_1(g_m) = a_1(T_m f) - a_1(a_m(f) f) = a_m(f) - a_m(f) = 0.$$

Hence, $g_m \in S_k(\Gamma_1(N))^{\text{old}}$. We have that $g_m \in S_k(\Gamma_1(N))^{\text{new}} \cap S_k(\Gamma_1(N))^{\text{old}} = \{0\}$. Thus, $T_m f = a_m(f) f$ for all $m \in \mathbb{Z}^+$. This completes the proof of part 1. It should be clear that part 2 follows immediately from part 1. Note, this property is known as the *Multiplicity One* property of newforms. We will conclude by showing that the set of newforms in $S_k(\Gamma_1(N))^{\text{new}}$ is linearly independent and the rest will be left as an exercise. Suppose there is a nontrivial linear relation

$$\sum_{i=1}^{n} c_i f_i = 0,$$

where $c_i \in \mathbb{C}$ are nonzero and n is taken to be as small as possible. For any prime p, we will

apply $T_p - a_p(f_1)$ to the relation, this yields

$$\sum_{i=2}^{n} c_i(a_p(f_1) - a_p(f_i))f_i = 0.$$

Since this summation contains fewer terms we know this is a trivial relation, i.e., $a_p(f_1) = a_p(f_i)$ for all primes p. Hence, $f_i = f_1$ for all i, which is a contradiction. This completes the proof. $\square$

Chapter 2

Galois Representations and Modular Forms

In this chapter we will give a brief introduction to Galois representations and their connection with modular forms by way of a construction of Deligne, Shimura, et. al. [3], and a conjecture of Serre [20]. We will conclude with a theorem of Ribet from [17] on lowering the level of modular Galois representations.

2.1 Galois Representations

Throughout we will use $G_{\mathbb{Q}}$ to denote $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, the absolute Galois group of $\mathbb{Q}$. Our goal is to better understand this group. A standard technique in number theory for understanding rather unwieldy objects is to examine them "locally", i.e., look at their behaviour with respect to a single prime. Our technique for understanding $G_{\mathbb{Q}}$ will follow along this line. In order to do this we will first fix an embedding of $\overline{\mathbb{Q}}_\ell \hookrightarrow \mathbb{C}$. We will now need the following definitions.

Definition 14. Let $G = \varprojlim_i G_i$, where each G_i is a finite group with the discrete topology.

Note, $G \subseteq \prod_i G_i$. Endow $\prod_i G_i$ with the product topology and let G have the subspace topology. Then we say G has the *profinite*.

A special case of this topology is given by placing the profinite topology on the ℓ-adic integers $\mathbb{Z}_\ell = \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}$. Recall that $G_\mathbb{Q}$ can also be expressed as an inverse limit of finite groups, hence the following definition is another special case of the profinite topology. The proof that these two topologies are equivalent is left as an exercise.

Definition 15. *The Krull topology* on $G_\mathbb{Q}$ is given by the following. Let $U \subset G_\mathbb{Q}$. Then U is open in $G_\mathbb{Q}$ if for every $\sigma \in U$ there exists an intermediate field $K \subset \overline{\mathbb{Q}}$ satisfying the following:

1. $[K : \mathbb{Q}] < \infty$,
2. if $\sigma' \in G_\mathbb{Q}$, and $\sigma|_K = \sigma'|_K$ then $\sigma' \in U$.

To make this definition more clear, consider the following subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{2})) \leq G_\mathbb{Q}$. Note, $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ is a finite field extension and for any two elements $\sigma, \sigma' \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{2}))$ we have that $\sigma|_{\mathbb{Q}(\sqrt{2})} = \sigma'|_{\mathbb{Q}(\sqrt{2})} = id$. Thus, $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{2}))$ is an open set of $G_\mathbb{Q}$. Further, as $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{2}))$ is a subgroup we have that it is a closed set of $G_\mathbb{Q}$ as well.

Now, we come to our objects of primary interest in this section.

Definition 16. Let d be a positive integer, and let ℓ be prime. Suppose that $\mathbb{Q}_\ell \subseteq K$ is a field extension. Let $G_\mathbb{Q}$ be endowed with the Krull topology and $\mathrm{GL}_d(K)$ be endowed with the profinite topology. A *d-dimensional ℓ-adic Galois representation* is a continuous homomorphism

$$\rho : G_\mathbb{Q} \to \mathrm{GL}_d(K)$$

where $\mathbb{Q}_\ell \subseteq K$.

If ρ and ρ' are both d-dimensional ℓ-adic Galois representations such that for some $M \in \mathrm{GL}_d(L)$ we have $\rho'(\sigma) = M^{-1}\rho(\sigma)M$ for every $\sigma \in G_{\mathbb{Q}}$, then we say ρ is isomorphic to ρ'. The following proposition gives a nice property which we will need later.

Proposition 21. *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_d(K)$ be an ℓ-adic Galois representation. Then ρ is isomorphic to a Galois representation $\rho' : G_{\mathbb{Q}} \to \mathrm{GL}_d(\mathcal{O}_K)$, where $\mathcal{O}_K$ is the ring of integers of K.*

Proof. Let $\Lambda := \mathcal{O}_K^d$. Then Λ is a lattice of K^d, hence Λ is a finitely generated $\mathbb{Z}_\ell$-module. Therefore, Λ is compact in K^d. Note, we can use ρ to construct a continuous map

$$K^d \times G_{\mathbb{Q}} \to K^d, \text{ given by } (v, \sigma) \mapsto \rho(\sigma) \cdot v.$$

Since our map is continuous and $G_{\mathbb{Q}}$ is compact, we have that the image Λ' of $\Lambda \times G_{\mathbb{Q}}$ is compact under the above map. Let λ be a uniformizer of $\mathcal{O}_K$ lying over ℓ. Then, Λ' lies in $\lambda^{-r}\Lambda$ for some $r \in \mathbb{Z}^+$. This gives us that Λ' is finitely generated. Since Λ' contains Λ, its rank is at least d. As $\mathcal{O}_K$ is an integral domain, we have that Λ' is free, and it follows that its rank is exactly d. Note, by construction Λ' contains all elements of Λ and all of their Galois conjugates. Thus, for every $x \in \Lambda'$ and every $\sigma \in G_{\mathbb{Q}}$, we have that $\rho(\sigma) \cdot x \in \Lambda'$. Therefore, we have that by choosing an $\mathcal{O}_K$ basis of Λ' we obtain the desired representation,

$$\rho' : G_{\mathbb{Q}} \to \mathrm{GL}_d(\mathcal{O}_K).$$

□

The following three definitions will also be needed later.

Definition 17. Let ρ be an ℓ-adic Galois representation. Note that complex conjugation is an automorphism of $\overline{\mathbb{Q}}$ which fixes $\mathbb{Q}$, i.e., complex conjugation is an element of $G_{\mathbb{Q}}$. Denote this element by $\mathfrak{conj}$. We say that ρ is *odd* if $\det \rho(\mathfrak{conj}) = -1$.

Definition 18. Let G be a group and V a vector space. We say that a representation $\rho : G \to \mathrm{Aut}(V)$ is *irreducible* if ρ has no nontrivial invariant subspaces, i.e, if there does not exist a nontrivial subspace $W \subset V$ such that $\rho(g) \cdot W = W$ for every $g \in G$.

To make this more clear we will give an explicit example of a reducible representation. We will consider the representation of $(\mathbb{R}, +)$ on $\mathbb{R}^2$ given by

$$\rho(a) = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

Then,

$$\rho(a) \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x + ay \\ y \end{pmatrix}$$

and we see that the subspace $y = 0$ of $\mathbb{R}^2$ is fixed, i.e., ρ is reducible.

Let the ring of integers of $\overline{\mathbb{Q}}$ be denoted by $\overline{\mathbb{Z}}$. Suppose that $\mathfrak{p} \subset \overline{\mathbb{Z}}$ is a maximal ideal with $\mathfrak{p} \cap \mathbb{Z} = p$. We can use $\mathfrak{p}$ as the kernel to define the reduction map $\overline{\mathbb{Z}} \to \overline{\mathbb{F}}_p$. Recall that the *decomposition group of* $\mathfrak{p}$ is defined to be:

$$D_{\mathfrak{p}} := \{\sigma \in G_{\mathbb{Q}} | \mathfrak{p}^{\sigma} = \mathfrak{p}\}.$$

We have that $D_{\mathfrak{p}}$ acts on $\overline{\mathbb{Z}}/\mathfrak{p}$, which can in turn be viewed as an action of $D_{\mathfrak{p}}$ on $\overline{\mathbb{F}}_p$. This action gives us a surjective map

$$\phi : D_{\mathfrak{p}} \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p).$$

From this map we define an *absolute Frobenius element over* p to be any element of the preimage of the Frobenius automorphism $\sigma_p \in \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$, and we denote such an element as $\mathrm{Frob}_{\mathfrak{p}}$. Hence, $\mathrm{Frob}_{\mathfrak{p}}$ is defined only up to the kernel of ϕ. This kernel is called the *inertia*

group of $\mathfrak{p}$, and by definition is the following set

$$I_{\mathfrak{p}} := \left\{\sigma \in D_{\mathfrak{p}} | x^{\sigma} \equiv x \pmod{\mathfrak{p}} \text{ for all } x \in \overline{\mathbb{Z}}\right\}.$$

Definition 19. Let ρ be an ℓ-adic Galois representation and let $p \neq \ell$ be a prime. We say that ρ is *unramified at* p if $I_{\mathfrak{p}} \subset \ker \rho$ for any maximal ideal $\mathfrak{p} \subset \overline{\mathbb{Z}}$ lying over p.

With regards to the importance of these absolute Frobenius elements when dealing with continuous representations we have the following theorem, which follows from the Tchebotarov Density Theorem ([5, Thm. 9.1.2]).

Theorem 22. *([5, Thm. 9.3.1]) For each maximal ideal* $\mathfrak{p} \subset \overline{\mathbb{Z}}$ *lying over any but a finite set of rational primes, choose an absolute Frobenius element* $\mathrm{Frob}_{\mathfrak{p}}$. *The set of such elements forms a dense subset of* $G_{\mathbb{Q}}$.

As an example consider the following maps

$$G_{\mathbb{Q}} \xrightarrow{\pi} \mathrm{Gal}\left(\mathbb{Q}(\mu_\ell)/\mathbb{Q}\right) \xrightarrow{\sim} (\mathbb{Z}/\ell\mathbb{Z})^{\times} \xrightarrow{\omega_\ell} \mathbb{Z}_\ell^{\times},$$

where π is the projection to $G_{\mathbb{Q}}/\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_\ell)\right) \cong \mathrm{Gal}\left(\mathbb{Q}(\mu_\ell)/\mathbb{Q}\right)$, and ω_ℓ is the Teichmüller character, i.e., the unique character of order $\ell - 1$, conductor ℓ, which maps each element of $(\mathbb{Z}/\ell\mathbb{Z})^{\times}$ to a distinct $(\ell-1)^{st}$ root of unity in $\mathbb{Z}_\ell$. Note, the subscript may be omitted when it is clear from context. If we take the composition of these maps we get the ℓ^{th} cyclotomic character

$$\chi_\ell : G_{\mathbb{Q}} \to \mathbb{Z}_\ell^{\times}.$$

This is a continuous, odd, one-dimensional, ℓ-adic representation. Note that for $p \neq \ell$ we have that p is unramified in $\mathrm{Gal}\left(\mathbb{Q}(\mu_\ell)/\mathbb{Q}\right)$, i.e., for any $\mathfrak{p}$ lying over p in $\mathbb{Q}(\mu_\ell)$ we have that the inertia group $I_{\mathfrak{p}}$ is trivial. Therefore, $I_{\mathfrak{p}} \subseteq \ker \chi_\ell$, hence χ_ℓ is unramified at each rational

prime $p \neq \ell$. In fact, for any maximal ideal $\mathfrak{p} \subset \overline{\mathbb{Z}}$ lying over a rational prime $p \neq \ell$ we have the following

$$\chi_\ell(\mathrm{Frob}_\mathfrak{p}) = p,$$

which from our previous theorem determines χ_ℓ completely on $G_\mathbb{Q}$.

Now, we will give another example which is a little more involved and will be more interesting for our purposes. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. For m a positive integer, define the multiplication by m map to be

$$[m] : P \to \overbrace{P + ... + P}^{m\text{-times}}$$

where $P \in E\left(\overline{\mathbb{Q}}\right)$ and $P + P$ is the usual addition law on $E(\overline{\mathbb{Q}})$. Define the m-torsion subgroup to be

$$E[m] := \left\{ P \in E\left(\overline{\mathbb{Q}}\right) | [m](P) = \boldsymbol{0} \right\},$$

where $\boldsymbol{0}$ is the identity element of the abelian group of $\overline{\mathbb{Q}}$-points on E. It is well known that $E[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$, for instance see chapter 3 of [23]. Note, we can define an action of $G_\mathbb{Q}$ on the points of an elliptic curve as follows. For $P = (x, y)$ we have that $x, y \in \overline{\mathbb{Q}}$ and we can define the action by $P^\sigma = (x^\sigma, y^\sigma)$, and it is clear that $P^\sigma \in E\left(\overline{\mathbb{Q}}\right)$ since σ is a homomorphism. Using this it is not hard to see that $G_\mathbb{Q}$ acts on $E[m]$, i.e., let $P \in E[m]$, then we have

$$[m](P^\sigma) = \overbrace{P^\sigma + ... + P^\sigma}^{m\text{-times}} = \left(\overbrace{P + ... + P}^{m\text{-times}} \right)^\sigma = \boldsymbol{0}^\sigma = \boldsymbol{0}.$$

From this we have a mod m representation

$$\overline{\rho}_{m,E} : G_\mathbb{Q} \to \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}),$$

where the isomorphism involves a choice of basis. The following proposition will be needed in the future.

Proposition 23. *$\overline{\rho}_{m,E}$ is continuous, where $G_{\mathbb{Q}}$ has the Krull topology and $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ has the discrete topology.*

Proof. Note, as $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ has the discrete topology and the operations of multiplication and of inversion are continuous we know that the identity of $\mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z})$ is a topological basis. Therefore, it is sufficient to show that $(\overline{\rho}_{m,E})^{-1}(e)$ is open in $G_{\mathbb{Q}}$, where e is the identity automorphism. By definition $(\overline{\rho}_{m,E})^{-1}(e) = \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(E[m])\right)$, where by $\mathbb{Q}(E[m])$ we mean that we have adjoined the x and y coordinates of each point in $E[m]$. It is not hard to see that $[\mathbb{Q}(E[m]) : \mathbb{Q}] < \infty$ since we have adjoined a finite set of algebraic numbers. Also, by definition we have that any $\sigma \in G_{\mathbb{Q}}$ which fixes $\mathbb{Q}(E[m])$ will be in $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(E[m])\right)$. Thus, $\mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}(E[m])\right)$ is open in $G_{\mathbb{Q}}$, which completes the proof. □

While this is a representation of $G_{\mathbb{Q}}$, it is not yet an ℓ-adic representation. However, we can use this representation to construct an ℓ-adic representation.

Definition 20. The *ℓ-adic Tate module* of an elliptic curve E is the group

$$T_\ell(E) := \varprojlim_n E[\ell^n],$$

where the inverse limit is taken with respect to the maps

$$E[\ell^{n+1}] \xrightarrow{[\ell]} E[\ell^n].$$

Note, it should be clear that $T_\ell(E) \cong \mathbb{Z}_\ell^2$. Further, we have that for $P \in E[\ell^n]$ and $\sigma \in G_{\mathbb{Q}}$

$$[\ell]P^\sigma = \overbrace{P^\sigma + ... + P^\sigma}^{\ell\text{-times}} = \overbrace{(P + ... + P)^\sigma}^{\ell\text{-times}} = ([\ell]P)^\sigma .$$

Therefore, from our action of $G_{\mathbb{Q}}$ on the ℓ^n-torsion subgroup, we acquire a natural action of $G_{\mathbb{Q}}$ on $T_\ell(E)$. Note, this action identifies each element of $G_{\mathbb{Q}}$ with an element of the automorphisms of $T_\ell(E)$, i.e., we have the following representation,

$$\rho_{\ell,E} : G_{\mathbb{Q}} \longrightarrow \mathrm{Aut}(T_\ell(E)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell),$$

where once again the latter isomorphism requires a choice of basis for $T_\ell(E)$. The first property to note about $\rho_{\ell,E}$ is that it is continuous. To see this, note that we have the following commutative diagram for every n

$$\begin{array}{ccc} & G_{\mathbb{Q}} & \\ {\scriptstyle\overline{\rho}}\swarrow & & \searrow{\scriptstyle\overline{\rho}} \\ \mathrm{Aut}\,(E[\ell^{n-1}]) & \xleftarrow[[\ell]]{} & \mathrm{Aut}\,(E[\ell^n]) \end{array}$$

where the subscripts on $\overline{\rho}$ are omitted as it should be clear which map is meant. We have that the following diagram commutes for every n

$$\begin{array}{ccc} G_{\mathbb{Q}} & \xrightarrow{\quad\rho\quad} & \mathrm{Aut}\,(T_\ell(E)) \\ & {\scriptstyle\overline{\rho}}\searrow \quad \swarrow{\scriptstyle\pi} & \\ & \mathrm{Aut}\,(E[\ell^n]) & \end{array}$$

where π is the projection mapping and ρ is the map $\rho_{\ell,E}$. Now, we state a universal property satisfied by the inverse limit.

Proposition 24. *([16, Prop. IV.2.5.]) Let $G = \varprojlim_i G_i$ with homomorphisms $g_{ij} : G_j \to G_i$. If H is a topological group and $h_i : H \to G_i$ is a family of continuous homomorphisms such that $h_i = g_{ij} \circ h_j$ for $i \leq j$, then there exists a unique continuous homomorphism $h : H \to G$ satisfying $h_i = g_i \circ h$ for all i.*

We know that the projection map π and the representations $\overline{\rho}$ are continuous, hence

by the previous proposition we have $\rho_{\ell,E}$ is continuous. Thus, $\rho_{\ell,E}$ is an ℓ-adic representation. Regarding the other properties of interest which these representations exhibit, we have the following theorem.

Theorem 25. *([5, Thm. 9.4.1]) Let ℓ be prime and E be as above. The Galois representation $\rho_{\ell,E}$ is irreducible and unramified at every prime $p \nmid \ell N$. Further, for any such p, let $\mathfrak{p} \subset \overline{\mathbb{Z}}$ be any maximal ideal lying over p. Then the characteristic polynomial of $\rho_{\ell,E}(\mathrm{Frob}_{\mathfrak{p}})$ is*

$$x^2 - a_p(E)x + p$$

where $a_p(E) := p + 1 - |\tilde{E}(\mathbb{F}_p)|$ is the so called "trace of Frobenius".

From this theorem and the fact that our representation $\rho_{\ell,E}$ is continuous and two-dimensional, we see that $\rho_{\ell,E}$ is now completely determined on $G_{\mathbb{Q}}$.

To conclude this section, we will give a definition and some related results which will be needed in the next section.

Definition 21. A representation $\rho : G \to \mathrm{GL}_d(K)$ is *semi-simple* if K^d can be written as a direct sum of simple G-modules K_i, ie.,

$$K^d \cong K_1 \oplus ... \oplus K_n.$$

For our purposes consider the Galois representation

$$\rho : G_{\mathbb{Q}} \to \mathrm{GL}_d(K).$$

Then, as K^d is a $G_{\mathbb{Q}}$-module, by [21, I-10] we know that K^d has a composition series of ρ-invariant subspaces given by

$$K^d = K_0 \supset K_1 \supset ... \supset K_{n-1} = 0$$

such that each K_i/K_{i+1} is simple. Let $K' := \bigoplus_{i=0}^{n-2} K_i/K_{i+1}$ and define a new d-dimensional representation

$$\rho^{ss} : G_{\mathbb{Q}} \to \mathrm{GL}(K').$$

The new Galois representation ρ^{ss} is called the *semi-simplification* of ρ. As an example, let k, k' be integers and consider the four dimensional Galois representation given by,

$$\rho(\sigma) = \begin{pmatrix} \chi_\ell^k(\sigma) & * & * \\ 0 & \rho_{\ell,E}(\sigma) & * \\ 0 & 0 & \chi_\ell^{k'}(\sigma) \end{pmatrix},$$

where χ_ℓ is the ℓ-adic cyclotomic character and $\rho_{\ell,E}$ is the irreducible ℓ-adic representation associated to an elliptic curve E of conductor prime to ℓ. After choosing a basis we may take $K_0 = \mathbb{Z}_\ell^4$, $K_1 = \mathbb{Z}_\ell^3$, $K_2 = \mathbb{Z}_\ell$, and $K_3 = 0$. Then, the semi-simplification $\rho^{ss} : G_{\mathbb{Q}} \to \mathbb{Z}_\ell \oplus \mathbb{Z}_\ell^2 \oplus \mathbb{Z}_\ell$ of ρ is given by,

$$\rho^{ss}(\sigma) = \begin{pmatrix} \chi_\ell^k(\sigma) & 0 & 0 \\ 0 & \rho_{\ell,E}(\sigma) & 0 \\ 0 & 0 & \chi_\ell^{k'}(\sigma) \end{pmatrix}.$$

Note, if our representation ρ is irreducible then $\rho^{ss} = \rho$.

2.2 Motivation

Let $f \in S_k(\Gamma_1(N))$ be an eigenform for all of the Hecke operators with associated character χ. It is a well-known result that the Fourier coefficients of f are algebraic integers and along with the values of χ generate a finite extension of $\mathbb{Q}$, denote this extension by $\mathbb{Q}(f)$. To prevent cumbersome notation, we will denote $\mathbb{Q}(f)$ by K in this section. We have

a construction of Deligne, Shimura, et. al., in [3] which attaches to f a family of continuous, irreducible representations

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

where λ runs over the set of maximal ideals of K, and K_λ denotes the completion of K at λ. Note, these are precisely the ℓ-adic representations defined in the previous section, where ℓ is the rational prime which λ lies over. Also, these representations are characterized up to isomorphism by

$$\mathrm{trace}(\rho_{f,\lambda}(\mathrm{Frob}_p)) = a_p,$$

$$\det\left(\rho_{f,\lambda}(\mathrm{Frob}_p)\right) = \chi(p)p^{k-1},$$

for primes p which are relatively prime to N and to the norm of λ.

Using Proposition 21 from the previous section we may consider $\rho_{f,\lambda}$ as a representation on $(\mathcal{O}_\lambda)^2$, where $\mathcal{O}_\lambda$ is the ring of integers of K_λ. Note, we also have the reduction map

$$\mathrm{GL}_2(\mathcal{O}_\lambda) \to \mathrm{GL}_2(\mathbb{F}_\lambda),$$

where $\mathbb{F}_\lambda := \mathcal{O}_\lambda/\lambda\mathcal{O}_\lambda$ is the residue field of λ. Composing these two maps gives a representation

$$\overline{\rho}_{f,\lambda} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{F}_\lambda).$$

However, there is some ambiguity attached to our representation $\overline{\rho}_{f,\lambda}$ since it depended on a choice of basis in Proposition 21. This ambiguity is removed by taking the semisimplification of this representation to obtain $\overline{\rho}^{ss}_{f,\lambda}$, which we shall also refer to as the residual of $\rho_{f,\lambda}$. Note, regardless of our choice of basis, the semisimplifications of $\overline{\rho}_{f,\lambda}$ are all isomorphic. This $\overline{\rho}^{ss}_{f,\lambda}$ is the desired representation for our purposes.

Fixing a rational prime ℓ we have a canonical inclusion

$$\mathbb{F}_\lambda \hookrightarrow \overline{\mathbb{F}}_\ell,$$

where λ is a maximal ideal lying over ℓ in K. Using this inclusion we can view our previous representation $\overline{\rho}^{ss}_{f,\lambda}$ as taking values in $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$. Note, with $\overline{\mathbb{F}}_\ell$ having the discrete topology our representation is still continuous. This brings us to the main question of this section, namely, if we are given a continuous semisimple representation $\rho : G_\mathbb{Q} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$, then when can we expect ρ to be isomorphic to one of our $\overline{\rho}^{ss}_{f,\lambda}$ from above? In order to answer this question we will need the following argument.

Identify our character χ with a character defined on $G_\mathbb{Q}$ using a similar argument as in the previous section for the cyclotomic character, i.e., by composing the following maps

$$G_\mathbb{Q} \xrightarrow{\pi} \mathrm{Gal}\left(\mathbb{Q}(\mu_N)/\mathbb{Q}\right) \xrightarrow{\sim} (\mathbb{Z}/N\mathbb{Z})^\times \xrightarrow{\chi} \mathbb{C}^\times.$$

As it should not cause any confusion, we will just call this character χ as well. Using work from the previous section and the fact that $\det\left(\rho_{f,\lambda}(\mathrm{Frob}_p)\right) = \chi(p)p^{k-1}$ for primes p prime to the level of f and the norm of λ, we have the following identity

$$\det \rho_{f,\lambda} = \chi\chi_\ell^{k-1},$$

where χ_ℓ is the cyclotomic character defined in the previous section. If we reduce this identity mod λ, we have $\det \overline{\rho_{f,\lambda}} = \overline{\chi} \cdot \overline{\chi_\ell}^{k-1}$. Note, $\overline{\chi_\ell}$ is the mod ℓ-cyclotomic character, i.e., the character which maps $G_\mathbb{Q}$ to $(\mathbb{Z}/\ell\mathbb{Z})^\times$. Let $\mathfrak{conj} \in G_\mathbb{Q}$ denote complex conjugation as before. From §2.1 we know that χ_ℓ is odd, i.e., $\chi_\ell(\mathfrak{conj}) = -1$. Further, with regards to our character χ, we have that when we restrict $G_\mathbb{Q}$ to $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$, our element $\mathfrak{conj}$ is sent to the automorphism $\mu_N \to \mu_N^{-1}$. Therefore, $\chi(\mathfrak{conj}) = \chi(-1)$. From our parity condition on

characters associated to modular forms we have that $\chi(-1) = -1^k$. Combining these yields

$$\det \overline{\rho}_{f,\lambda}(\mathfrak{conj}) = -1.$$

In other words, our representation $\overline{\rho}^{ss}_{f,\lambda}$ is odd. In [20], J.P. Serre conjectured that this parity condition was sufficient to answer the question above. This resulted in the following theorem

Theorem 26. ***(Serre's Conjecture)*** *Let $\rho : G_{\mathbb{Q}} \to \mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$ be an irreducible, odd representation. Then ρ is isomorphic to the representation $\overline{\rho}^{ss}_{f,\lambda}$ associated to some eigenform $f \in S_k(\Gamma_1(N))$.*

Further, in [20], Serre states a stronger result, in which he computes explicitly the level $\Gamma_1(N(\rho))$ and weight $k(\rho)$ of such an eigenform. This so called Refined Conjecture was proven in 2006 by C. Khare and J.P. Wintenberger in [10] and [11].

Our goal is to provide a connection between the Serre conjecture and the Refined conjecture in a particular case by way of a theorem of K. Ribet presented in [17]. To this end we will be primarily concerned with the level of such an eigenform. In particular, suppose that ρ is an ℓ-adic representation which arises from an eigenform of level $\Gamma_1(M)$, where $M = N\ell^\alpha$ and $(N, \ell) = 1$. While we have not stated the Refined conjecture, we will need to note that $(N(\rho), \ell) = 1$. The theorem of Ribet, which is stated explicitly and proven in the next section, will allow us to show that our original representation ρ is isomorphic to the residual of a representation which arises from a form of level $\Gamma_1(N)$. This will be done by showing that we can find an eigenform of the lower level which has Fourier coefficients congruent to the Fourier coefficients of the original eigenform modulo ℓ.

2.3 The Deligne-Serre Lifting Lemma

In this section our goal is to prove the Deligne-Serre lifting lemma ([4, Lemme 6.11]) which will be used in the proof of our main result. Note, the proof of this lemma is from ([4],[18]). To begin we will recall some definitions and results from commutative algebra. Throughout, let R be a commutative ring with unity and M an R-module.

Definition 22. A *discrete valuation ring* is a principal ideal domain with a unique maximal ideal.

Definition 23. We R is *Artinian* if R satisfies the descending chain condition for ideals, i.e., if

$$I_0 \supseteq I_1 \supseteq ...$$

is an infinite chain of ideals in R, then for some $n \in \mathbb{N}$, $I_n = I_{n'}$ for every $n' > n$.

We have the following lemma which we will need in the proof of the Deligne Serre lifting lemma.

Lemma 27. *Let R be an Artinian ring. Then any prime ideal of R is also a maximal ideal.*

In order to prove this we will need the following lemma.

Lemma 28. *If R is an Artinian integral domain then R is a field.*

Proof. Let $x \in R$ be non-zero and consider the chain $(x) \supseteq (x^2) \supseteq ....$ Since R is Artinian we know that this chain must eventually stabilize. Therefore, $(x^{n+1}) = (x^n)$ for some $n \in \mathbb{Z}$. Hence, $x^n = ax^{n+1}$ for some $a \in R$. As R is an integral domain we can conclude that $1 = ax$, i.e., x is a unit. Thus, R is a field as desired. □

We are now ready to prove lemma 27.

Proof. Let $\wp \subseteq R$ be a prime ideal. Then $R/\wp$ is an Artinian integral domain, hence a field. Thus, $\wp$ is a maximal ideal. □

Definition 24. Let $x \in M$. Then the *annihilator of x over R*, denoted $\mathrm{Ann}_R(x)$, is defined to be the set of all $r \in R$ such that $r \cdot x = 0$.

Definition 25. A prime ideal $\wp \subset R$ is said to be *associated* to M if $\wp$ is the annihilator of an element of M.

Definition 26. Let $U \subseteq R$ be a multiplicatively closed subset. We define *the localization of M at U*, denoted $U^{-1}M$, to be the set of equivalence classes of pairs (m, u) with $m \in M$ and $u \in U$ where the equivalence relation is given to be $(m, u) \sim (m', u')$ if there exists an element $v \in U$ such that $v(mu' - um') = 0$. Note, there is a natural map $\pi : M \to U^{-1}M$ given by $r \mapsto (r, 1)$.

Proposition 29. *([6, Prop. 2.1]) An element $m \in M$ maps to zero under π iff m is annihilated by an element $u \in U$. In particular, if M is finitely generated, then $U^{-1}M = 0$ iff M is annihilated by an element of U.*

Definition 27. Let $\wp \subset R$ be a prime ideal and let $U := R - \wp$. Note, U is multiplicatively closed since $\wp$ is a prime ideal. We say $\wp$ is in the *support* of M, denoted $\mathrm{Supp}(M)$, if $M_\wp := U^{-1}M \neq 0$.

Lemma 30. *Let M be an R-module. Then the set of prime ideals of R which are associated primes of M is contained in the set of prime ideals of R which are in the support of M.*

Proof. Let $\mathcal{P}$ be an associated prime of M. Then $\mathcal{P}$ is the annihilator of some $m \in M$. If $M_\mathcal{P} = 0$ then there exists $s \in R - \mathcal{P}$ such that $sm = 0$. But, that would mean s is in $\mathcal{P}$ which is a contradiction. Thus, $M_\mathcal{P} \neq 0$, i.e., $\mathcal{P}$ is a support prime of M. □

Lemma 31. *Let A be a Noetherian ring, M be a non-zero A-module,and $\wp \in Supp(M)$. Then, $\wp$ contains an associated prime of M.*

Proof. Since $\wp$ is a support prime, $M_\wp \neq 0$. Then, there exists some $x \in M$ such that $(Ax)_\wp \neq 0$. Since A is Noetherian, by Theorem 3.1 of [6] we have that the set of associated primes of $(Ax)_\wp$ is non-empty. From the previous lemma we have that the set of associated primes of $(Ax)_\wp$ is contained in the set of support primes of $(Ax)_\wp$. Let λ be an associated prime of $(Ax)_\wp$. Hence, there is a non-zero element $\frac{y}{s}$ of $(Ax)_\wp$ with $y \in Ax$ and $s \in R - \wp$ such that λ is the annihilator of $\frac{y}{s}$. Note, if there exists $b \in \lambda - \wp$, then $b\frac{y}{s} = 0$ implies that $\frac{y}{s} = 0$ since b is a unit in $(Ax)_\wp$. This is a contradiction, so no such b exists.
As A is Noetherian we have that any λ is finitely generated. Say $\{b_1, ..., b_n\}$ is a set of generators of λ. Then, for each b_i, there exists $t_i \in A - \wp$ such that $b_i t_i y = 0$. Let $t = t_1 ... t_n$. Then λ is the annihilator of $ty \in M$, hence is an associated prime of M. □

Now, we are prepared to present the main result of this section.

Theorem 32. ***(Deligne-Serre Lifting Lemma):*** *Let $\mathfrak{D}$ be a discrete valuation ring with field of fractions K, maximal ideal $\mathfrak{m}$, and residue field $\mathbf{k} = \mathfrak{D}/\mathfrak{m}$. Let M be a free $\mathfrak{D}$-module of finite rank and $\mathcal{T}$ a set of commuting $\mathfrak{D}$-endomorphisms of M. Let $f \in M/\mathfrak{m}M \cong \mathbf{k} \otimes M$ be a non-zero eigenvector for all $T \in \mathcal{T}$ with eigenvalues $a_T \in \mathbf{k}$. Then, there exists a discrete valuation ring $\mathfrak{D}'$ containing and finite over $\mathfrak{D}$, with maximal ideal $\mathfrak{m}'$ such that $\mathfrak{D} \cap \mathfrak{m}' = \mathfrak{m}$ and a nonzero element $f' \in M' = \mathfrak{D}' \otimes_{\mathfrak{D}} M$ which is an eigenvector for all $T \in \mathcal{T}$ with eigenvalue a'_T such that $a'_T \equiv a_T \pmod{\mathfrak{m}'}$.*

Proof. Let $\mathcal{H}$ be the $\mathfrak{D}$-subalgebra of $\mathrm{End}_{\mathfrak{D}}(M)$ generated by $\mathcal{T}$ over $\mathfrak{D}$. Since M is a free $\mathfrak{D}$-module of finite rank, say r, we have that $\mathrm{End}_{\mathfrak{D}}(M)$ is a free $\mathfrak{D}$-module of rank r^2. Since $\mathcal{H}$ is a subalgebra of $\mathrm{End}_{\mathfrak{D}}(M)$, $\mathcal{H}$ is a free $\mathfrak{D}$-module of finite rank. Choosing a basis for $\mathcal{H}$, we may assume that our generating set $\mathcal{T}$ is finite, say $\mathcal{T} = \{T_1, T_2, ..., T_n\}$. Note, in order to prove our desired result for all of $\mathcal{H}$, it will be sufficient to show it is true for the basis elements. Let m_{T_i} be the minimal polynomial of T_i. By adjoining all the roots of each m_{T_i} to K, we have a finite field extension K' of K such that each m_{T_i} splits over K'. Taking the

integral closure of $\mathfrak{D}$ in K' gives us a discrete valuation ring $\mathfrak{D}'$. The ring $\mathfrak{D}'$ has maximal ideal $\mathfrak{m}'$ lying over $\mathfrak{m}$, i.e., $\mathfrak{D} \cap \mathfrak{m}' = \mathfrak{m}$. Further, $\mathfrak{D}'$ has residue field k' containing k. Also, the analogous module to M in this setting is $\mathfrak{D}' \otimes_{\mathfrak{D}} M$, which we shall continue to denote as M. The analogous subalgebra of the endomorphisms of M is $\mathfrak{D}' \otimes_{\mathfrak{D}} \mathcal{H}$, which we shall also continue to denote as just $\mathcal{H}$. Now, consider the homomorphism of $\mathfrak{D}'$-algebras,

$$\pi_f : \mathcal{H} \to k', \text{ given by } \pi_f : T \mapsto a_T \pmod{\mathfrak{m}'}.$$

Note, $\mathfrak{D}' \hookrightarrow \mathcal{H}$ by $\alpha \mapsto \alpha \otimes I_{\mathcal{H}}$, where $I_{\mathcal{H}}$ is the multiplicative identity of $\mathcal{H}$ and $\alpha \in \mathfrak{D}'$. Hence, π_f is surjective. Further, using Zorn's lemma we can choose a minimal non-zero prime ideal (with respect to inclusion) $\mathfrak{p} \subset \mathcal{H}$ contained in the maximal ideal $\ker \pi_f$.

Claim 33. *The prime ideal $\mathfrak{p}$ is a subset of the set of zero divisors of $\mathcal{H}$.*

Proof. Let Z denote the set of zero divisors of $\mathcal{H}$. Let $D := \mathcal{H} - Z$. Note, if $x, y \in D$ then, $xy \in D$, i.e., D is closed under multiplication. Consider the set $S := \mathcal{H} - \mathfrak{p}$. Since $\mathfrak{p}$ is a prime ideal, we have that S is a multiplicatively closed set. Suppose that $S \subset S'$, where S' is a multiplicatively closed set. Then, either $S' = \mathcal{H}$ or $S' = \mathcal{H} - \mathfrak{p}'$, for some prime ideal $\mathfrak{p}'$. To see this note that if $S' \neq \mathcal{H}$ and $\mathfrak{p}'$ is not prime then there are two elements $x, y \in S' = \mathcal{H} - \mathfrak{p}'$ such that $xy \in \mathfrak{p}'$, i.e., S' is not multiplicatively closed. If $S' = \mathcal{H} - \mathfrak{p}'$, then $\mathfrak{p}' \subset \mathfrak{p}$, which contradicts the minimality of $\mathfrak{p}$. Hence, $S' = \mathcal{H}$ and S is a maximal multiplicatively closed set. Note, if $D \not\subset S$, then SD is a multiplicatively closed set that is strictly larger than S. Thus, $D \subset S$, which gives us that $\mathfrak{p} \subset Z$, as desired. □

Using the claim and the fact that $\mathcal{H}$ is free over $\mathfrak{D}'$ and that $\mathfrak{D}'$ is an integral domain, we have that $\mathfrak{p} \cap \mathfrak{D}' = 0$. Note, once again we are considering $\mathfrak{D}' \hookrightarrow \mathcal{H}$. Note, as $\mathcal{H}$ is finitely generated over $\mathfrak{D}'$, so is $\mathcal{H}/\mathfrak{p}\mathcal{H}$, hence $\mathfrak{D}'[h]$ is finitely generated for every $h \in \mathcal{H}$. Therefore, $\mathcal{H}/\mathfrak{p}\mathcal{H}$ is a finite integral extension of $\mathfrak{D}'$. Let L be the field of fractions of $\mathcal{H}/\mathfrak{p}\mathcal{H}$, and let

$\mathfrak{D}_L$ denote the integral closure of $\mathfrak{D}'$ in L. Let $\mathfrak{m}_L$ be the maximal ideal of $\mathfrak{D}_L$, and l the residue field. Note, $\mathfrak{m}' = \mathfrak{D}' \cap \mathfrak{m}_L$. Consider the projection map

$$\pi'_f : \mathcal{H} \to \mathcal{H}/\mathfrak{p}\mathcal{H} \, (\hookrightarrow \mathfrak{D}_L) \, ,$$

where the final injection just follows from $\mathfrak{D}_L$ being the integral closure of $\mathcal{D}'$ in the field of fractions of $\mathcal{H}/\mathfrak{p}\mathcal{H}$, and $\mathcal{H}/\mathfrak{p}\mathcal{H}$ being an integral extension of $\mathfrak{D}'$. Let $\pi'_f(T) = a'_T \in \mathcal{H}/\mathfrak{p}\mathcal{H} \subset \mathfrak{D}_L$, for all $T \in \mathcal{H}$. Define the map,

$$\pi'_f : \mathcal{H} \to \mathfrak{D}' \, (\hookrightarrow \mathcal{H}/\mathfrak{p}\mathcal{H})$$

given by reduction mod $\mathfrak{p}$. Since $\ker \pi_f$ is a maximal ideal in $\mathcal{H}$, by Proposition 4.15 of [6], we have that there exists a prime ideal in $\mathcal{I} \subset \mathfrak{D}_L$ such that $\mathcal{I} \cap \mathcal{H}/\mathfrak{p}\mathcal{H} = \ker \pi_f$. By Corollary 4.17 of [6], we have that $\mathcal{I}$ is maximal, hence $\mathcal{I} = \mathfrak{m}_L$. Thus, $\pi'_f(\ker \pi_f) \subseteq \mathfrak{m}_L$. Notice,

$$\pi_f(T - a_T I) = \pi_f(T) - a_T \pi_f(I) = a_T - a_T = 0, \text{ i.e., } T - a_T \in \ker \pi_f$$

Therefore,

$$\mathfrak{m}_L \ni \pi'_f(T - a_T I) = \pi'_f(T) - a_T \pi'_f(I) = a'_T - a_T I.$$

Thus, $a'_T \equiv a_T \pmod{\mathfrak{m}_L}$.

Let $\mathfrak{P}$ be the prime ideal in $K' \otimes_{\mathfrak{D}'} \mathcal{H}$ generated by $\mathfrak{p}$. Note, since $\mathfrak{p}$ is a minimal prime, so is $\mathfrak{P}$. We want to show that $\mathfrak{P}$ is an associated prime of $K' \otimes_{\mathfrak{D}'} M$, i.e., that $\mathfrak{P}$ is the annihilator of some nonzero element of $K' \otimes_{\mathfrak{D}'} M$. We begin by showing that that $\mathrm{Ann}_{K' \otimes \mathcal{H}}(K' \otimes M) \subset \mathfrak{P}$. First, we will need that $K' \otimes \mathcal{H}$ is Artinian and has all maximal ideals isomorphic. To see this note that $\mathcal{H}$ is free and of finite rank over $\mathfrak{D}'$, so we can think

of $\mathcal{H}$ as a finite direct sum of copies of $\mathfrak{D}'$. Hence, we have

$$K' \otimes_{\mathfrak{D}'} \mathcal{H} \cong K' \otimes_{\mathfrak{D}'} \bigoplus \mathfrak{D}' \cong \bigoplus (K' \otimes_{\mathfrak{D}'} \mathfrak{D}') \cong \bigoplus K'.$$

Note, the second isomorphism is obtained by noting that the tensor product distributes over direct sums, and the third isomorphism is obtained by noting that $K \otimes_R R \cong K$ where R is an arbitrary ring and K is the field of fractions of R. Now, $\bigoplus K'$ clearly has all maximal ideals isomorphic and is an Artinian ring since K' is Artinian.

Note that $\mathrm{Ann}_{K' \otimes \mathcal{H}}(K' \otimes M)$ is an ideal of $K' \otimes \mathcal{H}$, hence it is contained in some maximal ideal of $K' \otimes \mathcal{H}$. Using Lemma 27 and the fact that $\mathfrak{P}$ is prime, we have that $\mathfrak{P}$ is a maximal ideal of $K' \otimes \mathcal{H}$. Since all maximal ideals of $K' \otimes \mathcal{H}$ are isomorphic, we may assume that $\mathrm{Ann}_{K' \otimes \mathcal{H}}(K' \otimes M) \subset \mathfrak{P}$. By Corollary 2.7 from [6] we have that $\mathfrak{P}$ is in the support of $K \otimes M$. Using Lemma 31 we see that $\mathfrak{P}$ contains an associated prime. As $\mathfrak{P}$ is a minimal prime, we have that $\mathfrak{P}$ is an associated prime of $K' \otimes_{\mathfrak{D}'} M$. Therefore, there exists a nonzero $f'' \in K \otimes_{\mathfrak{D}'} M$ which is annihilated by $\mathfrak{P}$. Hence we can find a nonzero multiple of f'', say f', which is an element of M and is annihilated by $\mathfrak{P}$. Note, $T - a'_T \in \mathfrak{P}$. Thus, $(T - a'_T)f' = 0$, i.e., $Tf' = a'_T f'$. We have already shown that $a'_T \equiv a_T \pmod{\mathfrak{m}_L}$, hence this is our desired eigenform. □

Corollary 34. *Let $M := S_k(\Gamma_0(\ell^r) \cap \Gamma_1(N))$. Note, by fixing an embedding of $\overline{\mathbb{Q}}_\ell \hookrightarrow \overline{\mathbb{Q}}$, we can think of M as a $\mathbb{Z}_\ell$-module. Let $f \in M/\ell M = \mathbb{F}_\ell \otimes M$ be a simultaneous eigenform for all Hecke operators, i.e., $T_p f = a_p(f) f \pmod{\ell}$. Then, there exists a discrete valuation ring $\mathfrak{O}_\lambda$ that contains $\mathbb{Z}_\ell$ and has maximal ideal λ satisfying $\mathbb{Z}_\ell \cap \lambda = \ell$ so that there exists a nonzero $f' \in M' := \mathfrak{D}_\lambda \otimes_{\mathbb{Z}_\ell} M$ which is a simultaneous eigenform for all Hecke operators, with eigenvalues $a'_p(f')$ satisfying $a'_p(f') \equiv a_p(f) \pmod{\lambda}$.*

Corollary 35. *Let $M := S_k(\Gamma_1(N))$. Let $f \in M/\ell M = \mathbb{F}_\ell \otimes M$ be a simultaneous eigenform for all Hecke operators, i.e., $T_p f = a_p(f) f \pmod{\ell}$. Then, there exists a discrete valuation*

ring $\mathfrak{O}_\lambda$ that contains $\mathbb{Z}_\ell$ and has maximal ideal λ satisfying $\mathbb{Z}_\ell \cap \lambda = \ell$ so that there exists a nonzero $f' \in M' := \mathfrak{O}_\lambda \otimes_{\mathbb{Z}_\ell} M$ which is a simultaneous eigenform for all Hecke operators, with eigenvalues $a'_p(f')$ satisfying $a'_p(f') \equiv a_p(f) \pmod{\lambda}$.

2.4 Level-lowering for elliptic modular forms

In this section we present our main result.

Theorem 36. *([17, Thm. 2.1]) Let $k \geq 2$ and let $\ell \geq 3$ be prime. Let $f(z) = \sum_{n=1}^{\infty} a_n q^n \in S_k(\Gamma_1(N\ell^\alpha))$ be a normalized eigenform where $\alpha > 0$, and $N \in \mathbb{N}$ with $(N, \ell) = 1$. Let λ be a prime lying above ℓ in $\mathbb{Q}(f)$. Then, there exists a normalized eigenform $g \in S_k(\Gamma_1(N))$ with $g \equiv_{ev} f \pmod{\lambda}$, i.e., $a_n(g) \equiv a_n(f) \pmod{\lambda}$ when $(n, N\ell) = 1$.*

Proof. We will prove this theorem in four steps.

Step 1: *There exists an eigenform $g \in S_k(\Gamma_0(\ell^r) \cap \Gamma_1(N\ell))$ such that $g \equiv_{ev} f \pmod{\lambda}$, for some $r > 0$.*

Let $f \in S_k(\Gamma_1(N\ell^\alpha))$ with associated Dirichlet character χ. Then $\chi : (\mathbb{Z}/N\ell^\alpha\mathbb{Z})^\times \to \mathbb{C}^\times$. Note, since N and ℓ are relatively prime, we have $(\mathbb{Z}/N\ell^\alpha\mathbb{Z})^\times \cong (\mathbb{Z}/N\mathbb{Z})^\times \times (\mathbb{Z}/\ell^\alpha\mathbb{Z})^\times$. Hence, we can write $\chi = \kappa\chi'$, where $\kappa : (\mathbb{Z}/N\mathbb{Z})^\times \to \mathbb{C}^\times$, and $\chi' : (\mathbb{Z}/\ell^\alpha\mathbb{Z})^\times \to \mathbb{C}^\times$. As, $|(\mathbb{Z}/\ell^\alpha\mathbb{Z})^\times| = \phi(\ell^\alpha) = \ell^{\alpha-1}(\ell - 1)$, Sylow's Theorem gives that there exists a subgroup $H \subset (\mathbb{Z}/\ell^\alpha\mathbb{Z})^\times$ with $|H| = \ell^{\alpha-1}$. Clearly, H is a normal subgroup, and $\left|(\mathbb{Z}/\ell^\alpha\mathbb{Z})^\times/H\right| = \ell - 1$. Now, we can write $\chi' = \eta\omega^i$, where $\eta : H \to \mathbb{C}^\times$, and $\omega : (\mathbb{Z}/\ell\mathbb{Z})^\times \to \mathbb{Z}_\ell^\times$ is the Teichmüller character as defined in §2.1. We see now that $\chi = \kappa\eta\omega^i$. Since η has ℓ-power order, and ℓ is odd, we can write $\eta^{2m+1}(h) = 1$, for every $h \in H$ and some $m \in \mathbb{N}$. Let $\xi := \eta^{-(m+1)}$. We have $\eta = \xi^{-2}$ where ξ has ℓ-power order and ℓ-power conductor. Let $f_\xi(z) := \sum_{n=1}^{\infty} \xi(n) a_n q^n$. By [12, Prop. III.17] we know that $f_\xi \in S_k(\Gamma_1(N\ell^r))$ and has associated character $\kappa\omega^i$ for any $r \geq \alpha$ such that ℓ^r is greater than the square of the conductor of ξ. Note, for $\gamma \in \Gamma_0(N\ell^r)$, we have $f_\xi|_k[\gamma] = \kappa\omega^i(\gamma) f_\xi(z)$. Therefore, if $\gamma \in \Gamma_0(\ell^r) \cap \Gamma_1(N\ell)$, $f_\xi|_k[\gamma] = \kappa\omega^i(\gamma) f_\xi(z) = f_\xi(z)$.

Hence, $f_\xi(z) \in S_k\left(\Gamma_0(\ell^r) \cap \Gamma_1(N\ell)\right)$. All that remains is to show that $f_\xi \equiv_{ev} f \pmod{\lambda}$. In order to show that $a_n(f) \equiv a_n(f_\xi) \pmod{\lambda}$, it is sufficient to show $\xi(n) \equiv 1 \pmod{\lambda}$ when $(n, \ell) = 1$, since $a_n(f_\xi) = \xi(n)a_n(f)$. First, we will show $\xi(n) \equiv 1 \pmod{\lambda'}$, where λ' is a prime lying above ℓ in $\mathbb{Q}(\zeta)$, ζ a primitive $(\ell^r)^{th}$ root of unity. In this extension, ℓ is totally ramified, and $\lambda' = (1 - \zeta')$, for any primitive $(\ell^r)^{th}$ root of unity ζ'. Take $\zeta' = \xi(n)$ with $(n, \ell) = 1$ to see that $\xi(n) \in (1 - \lambda')$. Now, consider $\lambda' = \lambda_1^{\mathrm{ord}_{\lambda_1}(\lambda')} ... \lambda_m^{\mathrm{ord}_{\lambda_m}(\lambda')}$, the prime factorization of λ' in $\mathbb{Q}(\zeta, f)$. Since $\xi(n) \equiv 1 \pmod{\lambda'}$ we see that $\xi(n) \equiv 1 \pmod{\lambda_i^{\mathrm{ord}_{\lambda_i}}}$ for $1 \leq i \leq m$. Hence, $\xi(n) \equiv 1 \pmod{\lambda_i}$, for $1 \leq i \leq m$. Thus, $f(z) \equiv f_\xi(z) \pmod{\lambda}$. This concludes Step 1.

Step 2: *There exists an eigenform $g \in S_k\left(\Gamma_0(\ell^r) \cap \Gamma_1(N)\right)$ such that $g \equiv_{ev} f_\xi \pmod{\lambda}$, for some $r > 0$.*

Note, from step one we have that $f_\xi \in S_k\left(\Gamma_0(\ell^r) \cap \Gamma_1(N\ell)\right)$ is an eigenform with associated character $\kappa\omega^i$. If $i = 0, 1, 2$, then choose a new $i > 3$ such that $i \equiv 0, 1, 2 \pmod{\ell - 1}$, respectively. From [15, Lemma. 7.1.2] and [15, Thm. 7.1.3], we have that the Eisenstein series

$$G(z) := L(1 - i, \omega^i)/2 + \sum_{n=1}^{\infty} \left(\sum_{d|n} \omega^i(d) d^{i-1} \right) q^n$$

is in $M_i(\Gamma_0(\ell^r), \omega^{-i})$. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\ell^r) \cap \Gamma_1(N)$.

Then,

$$f(\gamma z)G(\gamma z) = (cz + d)^{k+i} \kappa\omega^i(\gamma)\omega^{-i}(\gamma) f(z)G(z) = (cz + d)^{k+i} \kappa(\gamma) f(z)G(z).$$

This gives us that $fG \in S_{i+k}(\Gamma_0(\ell^r) \cap \Gamma_1(N))$, with associated character κ. Now, we want

to show that the order at λ of $L(1-i,\omega^i)$ is negative. From [9, Thm. 3.4.2], we have that

$$L(1-i,\omega^i) = \frac{-B_{i,\omega^{-i}}}{i}.$$

Since, $1 \leq i \leq \ell - 1$, it is sufficient to show that the order at λ of $B_{i,\omega^{-i}}$ is negative. Expanding out the generalized Bernoulli number using [25, page 31] gives us

$$\begin{aligned} B_{i,\omega^{-i}} &= \ell^{i-1} \sum_{a=1}^{\ell} \omega^{-i}(a) B_i(a/\ell) \\ &= \ell^{i-1} \sum_{a=1}^{\ell} \omega^{-i}(a) \sum_{j=0}^{i} \binom{i}{j} B_j a^{i-j} \ell^{j-i} \\ &= \sum_{a=1}^{\ell-1} \omega^{-i}(a) \left(a^i \ell^{-1} + \frac{i}{2} a^{i-1} + \sum_{j=2}^{i} \binom{i}{j} B_j a^{i-j} \ell^{j-1} \right) \end{aligned}$$

Note, we need not consider when $a = \ell$ since ℓ is the conductor of ω. Also, we need not consider when $j \geq 3$ and odd, since in this case $B_j = 0$. Let
$F := (a^i \ell^{-1} + \frac{i}{2} a^{i-1} + \sum_{j=2}^{i} \binom{i}{j} B_j a^{i-j} \ell^{j-1})$. Note, by a corollary [8, page 233] to the theorem of Clausen and von-Staudt,

$$\begin{aligned} |\ell B_j|_\ell &= 1, \text{when } (\ell-1)|j \\ |\ell B_j|_\ell &< 1, \text{when } (\ell-1) \nmid j \end{aligned}$$

This gives us that $\ell F \equiv a^i \bmod \ell$ and since $a \not\equiv 0 \pmod{\ell}$ we have that the order at ℓ of F, hence λ, is negative. Thus, the order of $L(1-i,\omega^i)/2$ at λ is negative. Let $c := L(1-i,\omega^i)/2$. Then, $E := c^{-1}G$ is a modular form with λ-integral coefficients. Note, $E \equiv 1 \pmod{\lambda}$. Hence, $fE \equiv_{ev} f \pmod{\lambda}$, i.e., fE is an eigenform when viewed mod λ. Further, $fE \in S_{i+k}(\Gamma_0(\ell^r) \cap \Gamma_1(N), \kappa)$. Using the Deligne-Serre lifting lemma (see Corollary 34) we can find an eigenform in $\Gamma_0(\ell^r) \cap \Gamma_1(N)$ with eigenvalues congruent modulo λ to fE, hence

f. This concludes step 2.

Step 3: *There exists an eigenform $g \in S_k(\Gamma_0(\ell) \cap \Gamma_1(N))$ such that $g \equiv_{ev} f \pmod{\lambda}$, where $f \in S_{i+k}(\Gamma_0(\ell^r) \cap \Gamma_1(N))$ is the desired eigenform from step 2.*

Let $f(z) = \sum_{n=1}^{\infty} a_n q^n \in S(\Gamma_0(\ell^r) \cap \Gamma_1(N))$ be an eigenform, with $r > 1$. Let K be the Galois closure of $\mathbb{Q}(f)$, and let $\sigma \in G_{K/\mathbb{Q}}$ be a Frobenius element for λ. Thus, $\sigma a \equiv a^\ell \pmod{\lambda}$ for all $a \in \mathcal{O}_K$, the ring of integers of K. By Corollary 2 of [7] the series $\sum_{n=1}^{\infty} \sigma^{-1}(a_n) q^n$ is the Fourier expansion of a normalized eigenform $\sigma^{-1} f(z)$ of the same weight as $f(z)$. We want to show that $f(z)$ is congruent mod λ to an eigenform on $\Gamma_0(\ell^{r-1}) \cap \Gamma_1(N)$. Consider $g(z) := (\sigma^{-1} f(z))^\ell | U_\ell$, where U_ℓ is the ℓ^{th} Hecke operator. By Lemma 37, $g(z)$ is an eigenform on $\Gamma_0(\ell^{r-1}) \cap \Gamma_1(N)$. Further, we have that,

$g(z) = \left(\sum_{n=1}^{\infty} \sigma^{-1}(a_n) q^n \right)^\ell | U_\ell \equiv \left(\sum_{n=1}^{\infty} (\sigma^{-1}(a_n) q^n)^\ell \right) | U_\ell \pmod{\lambda}$.

Note that,

$$\begin{aligned} \left(\sum_{n=1}^{\infty} (\sigma^{-1}(a_n) q^n)^\ell \right) | U_\ell &= \left(\sum_{n=1}^{\infty} (\sigma^{-1}(a_n))^\ell q^{\ell n} \right) | U_\ell \\ &= \left(\sum_{n=1}^{\infty} (\sigma^{-1}(a_{\ell n}))^\ell q^{\ell n} \right) \\ &\equiv \left(\sum_{n=1}^{\infty} a_n q^n \right) \pmod{\lambda} \end{aligned}$$

By repeating this process $r-1$ times we get an eigenform on $\Gamma_0(\ell) \cap \Gamma_1(N)$, which is congruent to our original eigenform $f(z)$.

Step 4: *There exists an eigenform $g \in S_k(\Gamma_1(N))$ such that $g \equiv_{ev} f \pmod{\lambda}$, where f is the desired eigenform from step 3.*

In order to prove this final step we will use an argument given by Serre in [19]. Let V_ℓ be the operator $\sum a_n q^n \mapsto \sum a_n q^{\ell n}$, which by Proposition 15 takes forms on $\Gamma_1(N)$ to forms on

$\Gamma_0(\ell) \cap \Gamma_1(N)$. Further, let W be the operator given by the matrix $\begin{pmatrix} \ell x & y \\ N\ell z & \ell \end{pmatrix}$, where x, y, and z are integers such that $\ell x - Nyz = 1$. Note, that W is the operator denoted by $V_\ell^{N\ell}$ in [14]. Let $F(z)$ be an eigenform on $\Gamma_0(\ell) \cap \Gamma_1(N)$ of weight k with associated character χ of conductor N. First, note that by Lemma 38, we have that $F|W \in S_k(\Gamma_0(\ell) \cap \Gamma_1(N))$. Further, by Lemma 2 of [14], $F|W^2 = \chi(\ell)F(z)$.

Define the trace of F to be the function:

$$\mathrm{Tr}(F) = F + \kappa^{-1}(\ell)\ell^{1-k/2}F|W|U_\ell.$$

We want to show that $\mathrm{Tr}(F) \in S_k(\Gamma_1(N))$. By applying Lemma 39 to $F|W \in S_k(\Gamma_0(\ell) \cap \Gamma_1(N))$ we have that $(F|W|U_\ell + \ell^{k/2-1}F|W|W) \in S_k(\Gamma_1(N))$. Hence,

$$\begin{aligned} \kappa^{-1}(\ell)\ell^{1-k/2}(F|W|U_\ell + \ell^{k/2-1}F|W|W) &= \kappa^{-1}(\ell)\ell^{1-k/2}(F|W|U_\ell + \kappa(\ell)\ell^{k/2-1}F) \\ &= F + \kappa^{-1}\ell^{1-k/2}F|W|U_\ell \\ &= \mathrm{Tr}(F) \in S_k(\Gamma_1(N)) \end{aligned}$$

Further, if $G \in M_k(\Gamma_1(N))$ with character χ, Prop 1.5 of [1] gives us that $G|W = \ell^{k/2}\chi(\ell)G|V_\ell$.

If $\ell > 3$, let $E(z) = E_{\ell-1}(z)$, the normalized Eisenstein series of weight $\ell - 1$ on $\Gamma(1)$. Note, $E(z)$ has Fourier expansion $1 - \dfrac{2(\ell-1)}{B_{\ell-1}}\displaystyle\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n$, where $\sigma_{k-1}(n) = \displaystyle\sum_{d|n} d^{k-1}$. By the corollary to the theorem of Clausen and Von-Staudt used in step 2, we have that the order at ℓ of $B_{\ell-1}$ is negative. Hence, $E \equiv 1 \pmod{\ell}$. Similarly, if $\ell = 3$, let $E(z) = E_4(z)$, the normalized Eisenstein series of weight 4 on $\mathrm{SL}_2(\mathbb{Z})$, and we once again have that $E \equiv 1 \pmod{\ell}$. Let a denote the weight of $E(z)$. As in [19] we introduce:

$$g(z) := E - \ell^{a/2}E|W = E - \ell^a E|V_\ell.$$

It is clear that $g(z) \equiv 1 \pmod{\ell}$. Further, from [19] we have that

$$g|W = E|W - \ell^{a/2}E = \ell^{a/2}(E|V_\ell - E).$$

Since, $E|V_\ell \equiv E \equiv 1 \pmod{\ell}$, we see that $g|W \equiv 0 \pmod{\ell^{1+a/2}}$.

Let $f(z)$ be the eigenform on $\Gamma_0(\ell) \cap \Gamma_1(N)$ obtained from step 3, let the weight of f be denoted as k. Consider $\mathrm{Tr}(fg^{\ell^m})$ where m is a positive integer. We have that $\mathrm{Tr}(fg^{\ell^m}) \in S_{k_m}(\Gamma_1(N))$, where $k_m := k + \ell^m a$ is the weight of fg^{ℓ^m}. All that remains is to show that $\mathrm{Tr}(fg^{\ell^m}) \equiv f \pmod{\ell}$. First, for any modular form $F = \sum a_n q^n$, we define $\mathrm{ord}_\ell(F) := \inf_n \mathrm{ord}_\ell(a_n)$. In order to show the desired congruence, we will follow §3.2 of [19] to show that $\lim_{m\to\infty} \mathrm{ord}_\ell(\mathrm{Tr}(fg^{\ell^m}) - f) = \infty$. Note this shows that for sufficiently large m, we have that $\mathrm{Tr}(fg^{\ell^m})$ and f are congruent modulo any power of ℓ. To prove that the limit goes to infinity, we will show that $\mathrm{ord}_\ell(\mathrm{Tr}(fg^{\ell^m}) - f) \geq \inf(m + 1 + \mathrm{ord}_\ell(f), \ell^m + 1 + \mathrm{ord}_\ell(f|W) - k/2)$, which clearly increases as m increases.

Before we can begin, we must have that $\mathrm{ord}_\ell(f) > -\infty$. In other words, the order of ℓ in the denominators of the Fourier coefficients of f must be bounded above. This result follows from Theorem 3.52 of [22], which says that we can find a basis for $S_k(\Gamma_1(N))$ that consists of cusp forms for which the Fourier coefficients are rational integers. Note, since the denominators of the Fourier coefficients of f are restricted in this sense, we also have that the denominators of the Fourier coefficients of $f|W$ are restricted.

In order to get the desired result begin by writing $\mathrm{Tr}(fg^{\ell^m}) - f = (\mathrm{Tr}(fg^{\ell^m}) - fg^{\ell^m}) + f(g^{\ell^m} - 1)$. As stated previously, we have that $g \equiv 1 \pmod{\ell}$, therefore $g^{\ell^m} \equiv 1 \pmod{\ell^{m+1}}$. Hence, $\mathrm{ord}_\ell(f(g^{\ell^m} - 1)) \geq m + 1 + \mathrm{ord}_\ell(f)$.

We know that $\mathrm{Tr}(fg^{\ell^m}) - fg^{\ell^m} = \kappa^{-1}(\ell)\ell^{1-k_m/2}(fg^{\ell^m}|W|U_\ell)$. This gives us the following:

$$\begin{aligned}
\mathrm{ord}_\ell(\mathrm{Tr}(fg^{\ell^m})) - fg^{\ell^m} &\geq 1 - k_m/2 + \mathrm{ord}_\ell(fg^{\ell^m}|W|U_\ell) \\
&\geq 1 - k_m/2 + \mathrm{ord}_\ell(fg^{\ell^m}|W) \\
&= 1 - k_m/2 + \mathrm{ord}_\ell(f|W) + \ell^m \mathrm{ord}_\ell(g|W) \\
&\geq 1 - k_m/2 + \mathrm{ord}_\ell(f|W) + \ell^m(1 + a/2) \\
&= 1 + \ell^m + \mathrm{ord}_\ell(f|W) - k/2
\end{aligned}$$

Therefore, $\lim_{m\to\infty} \mathrm{ord}_\ell(\mathrm{Tr}(fg^{\ell^m}) - f) = \infty$, and we have that for sufficiently large m, $\mathrm{Tr}(fg^{\ell^m}) \equiv_{ev} f \pmod{\ell}$. Finally, we have the desired eigenform by using Corollary 35.

□

2.5 Required Lemmas

Lemma 37. *([14, Lemma 1.]) Let $f(z) \in S_k(\Gamma_0(\ell^r) \cap \Gamma_1(N))$ with associated character κ of conductor N, and $r > 1$. Then, $f|U_\ell \in S_k((\Gamma_0(\ell^{r-1}) \cap \Gamma_1(N))$.*

Proof. Note that $f|U_\ell = \ell^{k/2-1} f| \sum_{u \pmod{\ell}} \begin{pmatrix} 1 & u \\ 0 & \ell \end{pmatrix} = \ell^{k/2-1} f| \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} | \sum_{u \pmod{\ell}} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}$.

First, we will prove that $\ell^{k/2} f| \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \in S_k\left(\Gamma_0(\ell^{r-1}, \ell) \cap \Gamma_1(N)\right)$.

Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\ell^r) \cap \Gamma_1(N)$. From Proposition 5 we know that

$$\ell^{k/2} f| \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \in S_k\left(\left(\begin{pmatrix} 1 & 0 \\ 0 & 1/\ell \end{pmatrix} (\Gamma_0(\ell^r) \cap \Gamma_1(N)) \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}\right)\right).$$

Note,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1/\ell \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} = \begin{pmatrix} a & b\ell \\ c/\ell & d \end{pmatrix} \in \Gamma_0(\ell^{r-1}, \ell) \cap \Gamma_1(N).$$

Thus,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1/\ell \end{pmatrix} (\Gamma_0(\ell^r) \cap \Gamma_1(N)) \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} = \Gamma_0(\ell^{r-1}, \ell) \cap \Gamma_1(N),$$

which proves the claim.

Note, a set of right coset representatives of $(\Gamma(\ell^{r-1}, \ell) \cap \Gamma_1(N)) \setminus (\Gamma_0(\ell^{r-1}) \cap \Gamma_1(N))$ is given by $\left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} | 0 \leq u < \ell \right\}$. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\ell^{r-1}) \cap \Gamma_1(N)$.
It is clear that

$$\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a_u & b_u \\ c_u & d_u \end{pmatrix} \begin{pmatrix} 1 & u' \\ 0 & 1 \end{pmatrix},$$

for some

$$\begin{pmatrix} a_u & b_u \\ c_u & d_u \end{pmatrix} \in \Gamma_0(\ell^{r-1}, \ell) \cap \Gamma_1(N).$$

Hence, we have:

$$\begin{aligned}
f|U_\ell|\begin{pmatrix} a & b \\ c & d \end{pmatrix} &= \ell^{k/2-1} f|\left(\left(\begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}_u \sum_{(\mathrm{mod}\ \ell)} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}\right)\right|\begin{pmatrix} a & b \\ c & d \end{pmatrix} \\
&= \ell^{k/2-1} f|\begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}_{u'} \sum_{(\mathrm{mod}\ \ell)} \begin{pmatrix} a_u & b_u \\ c_u & d_u \end{pmatrix}\begin{pmatrix} 1 & u' \\ 0 & 1 \end{pmatrix} \\
&= \ell^{k/2-1} f|\begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}\begin{pmatrix} a_u & b_u \\ c_u & d_u \end{pmatrix}_{u'} \sum_{(\mathrm{mod}\ \ell)} \begin{pmatrix} 1 & u' \\ 0 & 1 \end{pmatrix} \\
&= \ell^{k/2-1} f|\begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix}_{u'} \sum_{(\mathrm{mod}\ \ell)} \begin{pmatrix} 1 & u' \\ 0 & 1 \end{pmatrix} \\
&= f|U_\ell.
\end{aligned}$$

□

Lemma 38. *([14, Lemma 2.]) Let $f(z) \in S_k\left(\Gamma_0(\ell) \cap \Gamma_1(N)\right)$. Then, $(f|W)(z) \in S_k\left(\Gamma_0(\ell) \cap \Gamma_1(N)\right)$.*

Proof. From Proposition 5 we have that,

$$(f|W)(z) \in S_k\left(W^{-1}\left(\Gamma_0(\ell) \cap \Gamma_1(N)\right) W\right).$$

What remains is to show that

$$W^{-1}\left(\Gamma_0(\ell) \cap \Gamma_1(N)\right) W = \Gamma_0(\ell) \cap \Gamma_1(N).$$

Let,

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\ell) \cap \Gamma_1(N)$$

First, note that

$$\begin{aligned} W^{-1}\gamma W &= \begin{pmatrix} 1 & -y/\ell \\ -Nz & x \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \ell x & y \\ N\ell z & \ell \end{pmatrix} \\ &= \begin{pmatrix} a - cy/\ell & b - dy/\ell \\ cx - aNz & dx - bNz \end{pmatrix} \begin{pmatrix} \ell x & y \\ N\ell z & \ell \end{pmatrix} \\ &= \begin{pmatrix} a\ell x - cxy + bN\ell z - dNy & a\ell x - cxy + b\ell - dy \\ c\ell x^2 - aN\ell xz + dN\ell xz - bN^2\ell z^2 & cxy - aNyz + d\ell x - bN\ell z \end{pmatrix}. \end{aligned}$$

Hence, $W^{-1}\gamma W \in \Gamma_0(\ell) \cap \Gamma_1(N)$, i.e., $W^{-1}\left(\Gamma_0(\ell) \cap \Gamma_1(N)\right) W \subseteq \Gamma_0(\ell) \cap \Gamma_1(N)$. Finally, notice that

$$\gamma = W^{-1}W\gamma W^{-1}W.$$

It is clear that $W\gamma W^{-1} \in \Gamma_0(\ell) \cap \Gamma_1(N)$, thus $\gamma \in W^{-1}\left(\Gamma_0(\ell) \cap \Gamma_1(N)\right) W$. From this we see that $\Gamma_0(\ell) \cap \Gamma_1(N) = W^{-1}\left(\Gamma_0(\ell) \cap \Gamma_1(N)\right) W$, Which completes the proof. □

Lemma 39. *([14, Lemma 3.]) Suppose that $f(z) \in S_k\left(\Gamma_0(\ell) \cap \Gamma_1(N)\right)$ with associated character κ of conductor N. Then, $f|(U_\ell + \ell^{k/2-1}W) \in S_k(\Gamma_1(N)$.*

Proof. First, note that

$$W = \begin{pmatrix} x\ell & y \\ N\ell z & \ell \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \begin{pmatrix} x\ell & y \\ Nz & 1 \end{pmatrix}.$$

From Lemma 37 we know that $f|\begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} \in S_k\left(\Gamma_0(1,\ell) \cap \Gamma_1(N)\right)$. It is clear that for a set

$\{\gamma_j\}$ of right coset representatives of $(\Gamma_0(1,\ell)\cap\Gamma_1(N))\backslash\Gamma_1(N)$ we have that

$$\sum_j \left(f| \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} |\gamma_j \right) \in S_k(\Gamma_1(N)).$$

For our coset representatives we will use the matrices $\gamma_j := \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix}$ for $0 \leq j < \ell$ and $\gamma_\ell = \begin{pmatrix} \ell x & y \\ Nz & 1 \end{pmatrix}$. Using these representatives we have:

$$\begin{aligned} \ell^{k/2-1}\sum_{j=0}^{\ell} \left(f| \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} |\gamma_j \right) &= f| \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} |\sum_{j=0}^{\ell-1} \begin{pmatrix} 1 & j \\ 0 & 1 \end{pmatrix} + f| \begin{pmatrix} 1 & 0 \\ 0 & \ell \end{pmatrix} | \begin{pmatrix} x\ell & y \\ Nz & 1 \end{pmatrix} \\ &= \ell^{k/2-1}(\ell^{1-k/1} f|U_\ell + f|W) \\ &= f|(U_\ell + \ell^{k/2-1}W). \end{aligned}$$

□

2.6 Example

To conclude this chapter we compute an example of these pairs of congruent eigenforms which we now know exist by Ribet's theorem. The main tool we will use to make this comparison is the following.

Corollary 40. *([2, Cor. 2.]) Let f_1 and f_2 be normalized cusp forms of level $\Gamma_1(N)$, weights k_1 and k_2, respectively. Further, suppose that both f_1 and f_2 have trivial associated characters. Let λ lie over an odd prime ℓ in the number field $\mathbb{Q}(f_1, f_2)$. Then, $a_p(f_1) \equiv a_p(f_2) \pmod{\lambda}$ for all primes $p \nmid \ell N$ if and only if this congruence holds for all primes*

$$p \leq \frac{\max\{k_1, k_2\}[\Gamma(1) : \Gamma_1(N)]}{12} \text{ with } p \nmid \ell N \text{ and } k_1 \equiv k_2 \pmod{\ell - 1}.$$

Before we compute our example, we must verify that the two weights satisfy the congruence condition. Let $\ell > 3$ be a prime. Let $f \in S_k(\Gamma_1(\ell^\alpha N))$ with trivial associated character. Let g be the desired form from Theorem 36. Then, we have that $g \in S_{k'}(N)$ with trivial associated character, and weight $k' = \ell^j(\ell - 1) + \ell k$. Therefore,

$$\begin{aligned} k' &= \ell^j(\ell - 1) + \ell k \\ &\equiv \ell k \pmod{\ell - 1} \\ &\equiv k \pmod{\ell - 1}. \end{aligned}$$

Note, if we let $\ell = 3$ then the weight of g is $k' = 3^j(4) + 3k$ which is clearly congruent to $k \pmod 2$. For our example we begin with a normalized eigenform $f \in S_k(\Gamma_1(\ell^\alpha N))$. Then, we use SAGE to search at the lower level N and our higher weight k' to find some candidate forms. Finally, using SAGE again, we make the comparison of Fourier coefficients up to the bound given in Corollary 40 to determine if our candidate form is our desired form from Theorem 36. Note, in order to use Corollary 40 we are considering our candidate forms as elements of $S_k(\Gamma_1(\ell^\alpha N))$.

Example 1. Let f be the normalized eigenform in the one dimensional space $S_6(\Gamma_1(3))$. Note, in this example we are letting $\ell = 3$ and $N = 1$. We see from above that our desired form $g \in S_{k'}(\Gamma(1))$, must have weight $k' = 4 \cdot 3^j + 18$ for some non-negative j. Choosing $j = 0$ gives the space $S_{22}(\Gamma(1))$, which is dimension one. Using Corollary 40, we see that in order to show that $f \equiv g \pmod 3$ we need only verify that $a_p(f) \equiv a_p(g) \pmod 3$ for all primes $p \leq \frac{k'[\Gamma(1) : \Gamma_1(3)]}{12} = 14\frac{2}{3}$, such that $p \neq 3$. Below are listed the Fourier coefficients of f which we will need to make our comparison,

p	$a_p(f)$	$a_p(f) \pmod 3$
2	-6	0
5	6	0
7	-40	2
11	-564	0
13	638	2

Let g be the single normalized eigenform of this space. The Fourier coefficients of g are listed below:

p	$a_p(g)$	$a_p(g) \pmod 3$
2	-288	0
5	21640950	0
7	-768078808	2
11	-94724929188	0
13	-80621789794	2

Comparing these two tables we see that $a_p(f) \equiv a_p(g) \pmod 3$ for all primes $p \leq 14\frac{2}{3}$ with $p \neq 3$. Thus, by our corollary we have that in fact $a_p(f) \equiv a_p(g) \pmod 3$ for all primes $p \nmid 3$. Therefore, using the multiplicativity of the Fourier coefficients we have that $f \equiv_{ev} g \pmod 3$ in the sense of Theorem 36.

Chapter 3

Future Work

Analogous to the work of Deligne, Shimura, et. al., we know that there exist four dimensional Galois representations associated to Siegel modular forms of degree 2 from the work of Laumon [13] and Weissauer [26]. Given this, it is natural to ask if there is an analog to Serre's conjecture and the associated Refined conjecture in this four dimensional setting. In order to understand what such an analog would look like, I plan to generalize the level lowering argument given in §2.3 to the four dimensional setting. The first case I plan to consider is lowering the level of a Siegel modular form in the Maass space, i.e., a Siegel modular form which arises from the Saito-Kurokawa correspondence.

Bibliography

[1] A. Atkin and W. Li. Twists of newforms and pseudo-eigenvalues of w-operators. *Invent. Math.*, 48:221–243, 1978.

[2] I. Chen, I. Kiming, and J. Rasmussen. On the congruences mod $\mathfrak{p}^m$ between eigenforms and their attached galois representations. *J. Number Theory*, 130:608–619, 2010.

[3] P. Deligne. Formes modulaires et représentations ℓ-adiques. *Ann. scient. Ec. Norm. Sup.*, 7:507–530, 1974.

[4] P. Deligne and J-P. Serre. Formes modulaires de poids 1. *Ann. scient. Ec. Norm. Sup.*, 7:507–530, 1974.

[5] F. Diamond and J. Shurman. *A First Course in Modular Forms*, volume 228 of *Graduate Texts in Mathematics*. Springer, 2005.

[6] D. Eisenbud. *Commutative Algebra With a View Toward Algebraic Geometry*, volume 150 of *Graduate Texts in Mathematics*. Springer-Verlag, 1995.

[7] H. Hida. *Elementary Theory of L-functions and Eisenstein series*, volume 26 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1993.

[8] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 1990.

[9] K. Iwasawa. *Lectures on p-adic L-functions*. Princeton University Press, 1972.

[10] C. Khare and J-P. Wintenberger. Serres modularity conjecture (i). *Invent. Math.*, 178:485–504, 2009.

[11] C. Khare and J-P. Wintenberger. Serres modularity conjecture (ii). *Invent. Math.*, 178:505–586, 2009.

[12] N. Koblitz. *Introduction to Elliptic Curves and Modular Forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag New York, 1984.

[13] G. Laumon. Fonctions zéta des variétés de Siegel de dimension trois. *Astérisque*, 302:1–66, 2005.

[14] W. Li. Newforms and functional equations. *Math. Ann.*, 212:285–315, 1975.

[15] T. Miyake. *Modular Forms*. Springer-Verlag Berlin Heidelberg, 1989.

[16] J. Neukirch. *Algebraic Number Theory*. Springer-Verlag Berlin Heidelberg, 1999.

[17] K. Ribet. Report on mod ℓ representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$. In *Motives*, volume 55 of *Proc. Sympos. Pure. Math*, pages 639–676. Amer. Math. Soc.

[18] A. Saikia. Ribet's construction of a suitable cusp eigenform. *arXiv:0910.1408*.

[19] J-P. Serre. Formes modulaires et fonctions zêta p-adiques. *Lecture Notes in Mathematics*, 350:191–268, 1973.

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

[21] J-P. Serre. Abelian ℓ-adic representations and elliptic curves. *Research Notes in Mathematics*, 7, 1998.

[22] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Forms*. Princeton University Press, 1971.

[23] J. Silverman. *The Arithmetic of Elliptic Curves*, volume 106 of *Graduate Texts in Mathematics*. Springer Dordrecht Heidelberg, 1986.

[24] J. Sturm. On the congruence of modular forms. *Lecture Notes in Mathematics*, 1240:275–280, 1980.

[25] L. Washington. *Introduction to Cyclotomic Fields*. Springer-Verlag New York, 1982.

[26] R. Weissauer. Four dimensional Galois representations. *Astérisque*, 302:67–150, 2005.