Congruences Between Modular Forms

by

Ruhat Kabulantok

A Dissertation Submitted to the
Graduate School of Sciences and Engineering
in Partial Fulfillment of the Requirements for
the Degree of

Master of Science

in

Mathematics

KOÇ ÜNİVERSİTESİ

July, 2020

Congruences Between Modular Forms

Koç University

Graduate School of Sciences and Engineering

This is to certify that I have examined this copy of a master's thesis by

Ruhat Kabulantok

and have found that it is complete and satisfactory in all respects,
and that any and all revisions required by the final
examining committee have been made.

Committee Members:

_____

Asst. Prof. Dr. Nadim Rustom

_____

Assoc. Prof. Dr. Sinan Ünver

_____

Assoc. Prof. Dr. Alp Bassa

Date: _____

To my family

ABSTRACT

Congruences Between Modular Forms
Ruhat Kabulantok
Master of Science in Mathematics
July, 2020

Modular forms admit Fourier expansions whose coefficients encode a lot of interesting arithmetic information. One fruitful method of studying these coefficients is through studying their congruences modulo primes l or powers of l. This theory can be traced back to the work of Ramanujan, and was developed by Serre, Swinnerton-Dyer, and Katz, among others.

In this thesis, we will study Serre and Swinnerton-Dyer's theory of modular forms modulo l. We will examine some applications of this theory, including Jochnowitz's proof of finiteness of systems of Hecke eigenvalues modulo l. We will also give a brief exposition of Serre's theory of l-adic modular forms.

ÖZETÇE

Modüler Formlar Arasındaki Denklikler
Ruhat Kabulantok
Matematik, Yüksek Lisans
Temmuz, 2020

Modüler formların sahip oldukları Fourier serilerinin katsayıları birçok ilginç aritmetik bilgi içerir. Bu katsayıları incelemenin bir yolu, bu katsayıların modulo l ya da l'in kuvvetlerindeki denkliklerini incelemektir. Bu teori Ramanujan'ın çalışmalarına dayanır. Serre, Swinnerton-Dyer ve Katz bu teoriyi geliştiren isimler arasındadır.

Bu tezde, Serre ve Swinnerton-Dyer'in modulo l modüler formlar teorisinin üzerine çalışacağız. Jochnowitz'in modulo l Hecke özdeğerleri sisteminin sonlu oluşunun ispatı da dahil olmak üzere bu teorinin bazı sonuçlarını inceleyeceğiz. Ayrıca Serre'in l-adik modüler formlarından da kısaca bahsedeceğiz.

ACKNOWLEDGMENTS

First of all, I would like to express my deepest gratitude to my advisor Prof. Nadim Rustom for his support and encouragement. He helped me to deepen my understanding of mathematics and guided me in writing this thesis with his invaluable advice. I especially thank him for his patience and kindness during this study.

I also thank my professors at the Department of Mathematics of Koç University, especially Prof. Sinan Ünver, for sharing their knowledge. I am thankful to Prof. Muhammed Uludağ from Galatasaray University for his support during my undergraduate studies.

I am also thankful to my colleagues and friends from Koç University: Duygu, Begüm, Berkay, Rızacan, İhsan, Umut, Fırtına, İpek, Cem, Metehan, Serap, Seda, Mutlu and Yasin for their support, fruitful discussions and most importantly for all unforgettable memories.

I am thankful to my dearest friend Şeyma for her encouragement and support, also for the great time that we had in the last two years. I also thank my lifelong friends Aslı, Ayşenur, Betül, and Cavide. They always give me great support and encouragement.

I am grateful to my parents and my brother Süleyman for their endless love and support during my studies and in every single moment of my life.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

The modular forms are ubiquitous mathematical objects which are defined as complex holomorphic functions on the upper half-plane with some transformation properties under the action of the congruence subgroups of the modular group $SL_2(\mathbb{Z})$. Due to their symmetry properties, a modular form has q-expansion with complex coefficients, and these coefficients give plenty of arithmetic information. Therefore it is natural to study these coefficients and one way to do that is to examine their reductions modulo some prime l.

This thesis aims to study the space of modular forms modulo prime l investigated by Serre in [Serre, 1973b] and Swinnerton-Dyer in [Swinnerton-Dyer, 1973], to explain a generalization of their results given in [Jochnowitz, 1982] and then to introduce the l-adic modular forms constructed by Serre in [Serre, 1973b].

The first examples of non-trivial modular forms with respect to $SL_2(\mathbb{Z})$ are the Eisenstein series of weight k denoted by G_k and the normalized Eisenstein series, E_k, have the q-expansion:

$$E_k = 1 - \frac{2k}{B_k} \sum_{n \geqslant 1} \sigma_{k-1}(n) q^n$$

where $\sigma_k(n) = \sum_{d|n} d^k$ and B_k is the kth Bernoulli number.

The Hecke operator T_n is a linear operator on the space of modular forms, $\mathcal{M}_k(\Gamma)$. The pth Hecke operator T_p for some prime p, acts on the q-expansion of a modular form f by:

$$T_p(f) = \sum_{n=0}^{\infty} a_{np} q^n + p^{k-1} \sum_{n=0}^{\infty} a_n q^{np}.$$

For $n = p^r$, then we have $T_{p^r} := T_p T_{p^{r-1}} - p^{k-1} \langle p \rangle T_{p^{r-2}}$ and for $n = \prod_i p_i^{e_i}$, the nth

Hecke operator is defined by $T_n := \prod_i T_{p_i^{e_i}}$. A modular form which is simultaneously an eigenvector for all the Hecke operators is called an *eigenform* and an eigenform f is called *normalized* is $a_1(f) = 1$. For each normalized eigenform f, the eigenvalue corresponding to T_n is equal to the nth Fourier coefficient $a_n(f)$.

Modular forms can be approached in a classical way. Moreover, it is natural to analyze their properties modulo a prime l. From now on l and p are primes where $l \geqslant 5$, $p \neq l$ and $l \nmid N$. To study the reduction modulo l of modular forms, we choose the modular forms with rational numbers whose denominator is not divisible by l. Then the space of modular forms modulo l is a subspace of $\mathbb{F}_l[\![q]\!]$ such that:

$$\tilde{\mathcal{M}}_k(\Gamma) = \left\{ \tilde{f} = \sum_{n=0}^{\infty} \tilde{a}_n q^n \mid f = \sum_{n=0}^{\infty} a_n q^n \in \mathcal{M}_k(\Gamma_0(N), \mathbb{Q} \cap \mathbb{Z}_l) \text{ and } \tilde{a}_n \equiv a_n \pmod{l} \right\}.$$

The algebra $\tilde{\mathcal{M}}(\Gamma)$ is defined by the sum of $\tilde{\mathcal{M}}_k(\Gamma)$'s and this algebra is studied by Swinnerton-Dyer [Swinnerton-Dyer, 1973] and Serre [Serre, 1973b]. The operators U, V and θ on this algebra are defined by the following formulas:

- $U(f) = \sum_{n=0}^{\infty} a_{nl} q^n$
- $\theta(f) = \sum_{n=0}^{\infty} n a_n q^n$
- $V(f) = \sum_{n=0}^{\infty} a_n q^{nl}$

If we examine the Eisenstein series modulo prime l, we get the following two congruences:

Proposition. $E_k \equiv E_{k'} \pmod{l}$ when $k \equiv k' \neq 0 \pmod{(l-1)}$

Proposition. $E_k - 1 \in l\mathbb{Z}_l[\![q]\!]$ if and only if $(l-1) \mid k$

In the proof of these two congruences, we use two main congruences about the Bernoulli numbers, namely: *Kummer's Congruences* and *Clausen-von Staudt's theorem.* Since the reduction modulo l of E_{l-1} is one by the congruences above, there is an inclusion $\tilde{\mathcal{M}}_k(\Gamma) \subseteq \tilde{M}_{k+l-1}(\Gamma)$ obtained by multiplication by E_{l-1}. The smallest

weight of the space $\tilde{\mathcal{M}}_k(\Gamma)$ where the reduction of the modular form f contained in is called the *filtration* and it is denoted by $w(f) = \inf\{k : f \in \tilde{\mathcal{M}}_k(\Gamma)\}$.

The Hecke module where we take the quotient of the space of modular forms with coefficients in $\bar{\mathbb{F}}_l$ by the modular forms with the lower filtrations is denoted by:

$$W_k = (\tilde{\mathcal{M}}_k(\Gamma) \otimes \bar{\mathbb{F}}_l)/(\tilde{\mathcal{M}}_{k-l+1}(\Gamma) \otimes \bar{\mathbb{F}}_l)$$

A *twist of* W_k is the Hecke module $W_k[a]$ where $0 < a \leqslant l-1$ which $\bar{\mathbb{F}}_l$-vector space W_k with the action of the Hecke operator is p^a. These Hecke modules $W_k[a]$ and W_k are isomorphic as vector spaces. Moreover, if the system of eigenvalues $\{\lambda_p\}$ appears in W_k, then $\{p^a\lambda_p\}$ appears in the Hecke module $W_k[a]$. For each W_k there exist only finitely many twists. The set $\{\lambda_p : l \nmid p\}$ where $\lambda_p \in \bar{\mathbb{F}}_l$ is called the *system of eigenvalues mod* l, if there exists an integer $k \geqslant 0$ and $f \in \tilde{\mathcal{M}}_k(\Gamma) \otimes \bar{\mathbb{F}}_l$ such that $T_p f = \lambda_p f$ for all $p \nmid N$. In this thesis, the main theorem which is proved in [Jochnowitz, 1982] is the following.

Theorem 5.1.7. *There exist finitely many systems of eigenvalues mod l for fixed level N.*

This theorem has shown for level one in [Serre, 1975] and for an arbitrary level N by Jochnowitz, it immediately follows from:

Theorem 5.1.5. *Let j be a positive integer. Then there exists a positive integer k with $k \leqslant 2l$ such that the space W_j is isomorphic to a twist of the space W_k as a Hecke module.*

The idea of the proof relies on the fact that the operators U, V and θ induce the operators on W_k using the fact that the filtration $w(\theta f) = w(f) + l + 1$ when $l \nmid k$ and $w(Uf) = \frac{w(f)+l^2-1}{l}$ when $w(f) \equiv 1 \pmod{l}$. Moreover the operators U, V, θ and T_p commute as following:

- $T_p \circ \theta = p\theta \circ T_p$
- $T_p \circ V = V \circ T_p$
- $U \circ V = I$

- $V \circ U = I - \theta^{(l-1)}$

and these are the facts that are used in the proof.

As an application of the main theorem, we show that there exist only 9 systems of eigenvalues when $l = 7$ and the level is one. We also show there are 4 system of eigenvalues for $l = 5$ and the level one. Additionally, the main theorem has a nice corollary:

Corollary 5.1.10. *For fixed level N, there are finitely many congruence classes of normalized eigenforms.*

Besides, the modular forms can also be worked in the l-adic sense. The l-adic modular forms are defined as the limit of classical modular forms with rational coefficients. As a result of this construction, we will see that even though there is no Eisenstein series of weight 2, we can talk about l-adic Eisenstein series which are l-adic modular forms of weight 2. Finally, we have the following interesting result proved in [Serre, 1973b]:

Theorem 6.4.4. *If f is a classical modular form with respect to $\Gamma_0(l)$ with rational coefficients, it is also an l-adic modular form.*

Structure of the thesis

This thesis has three main parts. In the first part, we introduce the modular forms in the classical way and define the Hecke operators, closely following [Diamond and Shurman, 2005]. In the second part, the main reference is [Jochnowitz, 1982]. In this part, the space of modular forms mod l is described and this is the part where we try to understand our main theorem. Lastly, we give details on the l-adic modular forms which are constructed by Serre in 1973 [Serre, 1973b].

In Chapter 2, the fundamental notions of the classical theory of modular forms will be presented. In the first part of this chapter, we define the congruence subgroups Γ of the modular group $SL_2(\mathbb{Z})$, then the modular forms with respect to Γ. Next, the Eisenstein series will be introduced as non-trivial examples of the modular forms for level one.

In the second part of this chapter, our main goal is to give a dimension formula for the space of modular forms with respect to an arbitrary congruence subgroup, $\mathcal{M}_k(\Gamma)$. To do so, the compact modular curve $X(\Gamma) = \Gamma\backslash\mathcal{H}^*$ will be seen as a compact Riemann surface. Then we will give some necessary definitions including elliptic point, period of an elliptic point, and degree of a map between two compact Riemann surfaces. Finally, we will give the dimension formula using the *Riemann-Hurwitz theorem.*

In Chapter 3, The Hecke operator T_n which is a linear operator on the space of modular forms will be introduced by using the definition of the double coset operator. Particularly, the action of the Hecke operators on the q-expansion of a modular form will be stated. Finally, the eigenforms and the relation between their coefficients and the eigenvalues will be introduced.

In Chapter 4, we start by the congruences between the Eisenstein series. Then we introduce the space of modular forms modulo l and the operators U, V, and θ. We also define the filtration w and give the relations of the filtration with the operators above on the space of modular forms modulo l.

In Chapter 5, we define the system of eigenvalues and the Hecke module. This is the chapter where we give the detailed proof of the main theorem on the finiteness of the systems of eigenvalues in Theorem 5.1.7. Then we give the corollary on the finiteness of congruence classes of the modular forms modulo l. The chapter finishes with two concrete examples on the number of systems of eigenvalues modulo 5 and 7 in level one.

In Chapter 6, we give an introduction to l-adic modular forms constructed by Serre. We start by examining the Eisenstein series modulo l^m for some positive integer m. Then we define the l-adic modular forms and the space X of the weights of l-adic modular forms. Finally, the l-adic Eisenstein series will be introduced.

Chapter 2

MODULAR FORMS

This first chapter aims to introduce the basic concepts of the classical theory of modular forms. We will begin with presenting the congruence subgroups and modular forms with respect to these congruence subgroups. Then we will give some examples of modular forms. Lastly, we will give the dimension formula of the space of modular forms.

In the following two chapters, we're closely following [Diamond and Shurman, 2005].

2.1 Congruence Subgroups

The *modular group* $SL_2(\mathbb{Z})$ is the multiplicative group of 2×2 matrices with integer entries and with determinant 1. The modular group $SL_2(\mathbb{Z})$ acts on the upper-half-plane $\mathcal{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\}$ by the *fractional linear transformation*:

$$\gamma z = \frac{az + b}{cz + d}$$

where $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ and $z \in \mathcal{H}$.

We extend this to an action of $SL_2(\mathbb{Z})$ on extended upper-half-plane which is $\mathcal{H}^* = \mathcal{H} \cup \mathbb{Q} \cup \{\infty\}$. Here, we define the action of $SL_2(\mathbb{Z})$ on ∞ by $\gamma\infty = \frac{a}{c}$ and $\gamma z = \infty$ if $cz + d = 0$.

Proposition 2.1.1. *The modular group $SL_2(\mathbb{Z})$ is generated by the following two matrices:*

$$S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \qquad \textit{and} \qquad T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

Proof. First, observe that $S^2 = -I$ and $T^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.

Let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$. Suppose $c \neq 0$, then there exists $n, r \in \mathbb{Z}$ such that $d = cn + r$ with $0 \leqslant |r| < |c|$.

$$\gamma T^{-n} = \begin{bmatrix} a & -an + b \\ c & -cn + d \end{bmatrix} = \begin{bmatrix} a & b' \\ c & r \end{bmatrix} \text{ and } \gamma T^{-n} S = \begin{bmatrix} b' & -a \\ r & -c \end{bmatrix}.$$

As we keep multiplying with $T^{n_i} S$, we will eventually have a matrix in form $\tilde{\gamma} = \begin{bmatrix} \tilde{a} & \tilde{b} \\ 0 & \tilde{d} \end{bmatrix}$. Since this matrix is in $SL_2(\mathbb{Z})$, $\tilde{d} = \pm 1$. If $\tilde{d} = -1$, multiply by S^2 to get a matrix in forms $T^{\tilde{b}}$. Then $\begin{bmatrix} \tilde{a} & \tilde{b} \\ 0 & \tilde{d} \end{bmatrix} = \begin{bmatrix} 1 & \tilde{b} \\ 0 & 1 \end{bmatrix} = T^{\tilde{b}}$. So we have $\gamma = T^{\tilde{b}} T^{n_1} S^{-1} T^{n_2} S^{-1} \cdots T^n$. Thus any element of $SL_2(\mathbb{Z})$ can be written as a product of the matrices S and T.

□

Now, we will introduce some subgroups of the modular group, namely the congruence subgroups.

Definition 2.1.2. Let N be a positive integer. Then we define the following subsets of $SL_2(\mathbb{Z})$:

- $\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \middle| \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}$
  is called the *principal congruence subgroup of level* N of $SL_2(\mathbb{Z})$.
- $\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \middle| \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} * & * \\ 0 & * \end{bmatrix} \pmod{N} \right\}$
- $\Gamma_1(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z}) \middle| \begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \pmod{N} \right\}$

Note that $\Gamma(N) \subset \Gamma_1(N) \subset \Gamma_0(N) \subset SL_2(\mathbb{Z})$. They are also subgroups. In the chapter 3 and 4, we use especially $\Gamma_0(N)$.

Proposition 2.1.3. *The subgroup $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$.*

Proof. Let

$$\varphi : \Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^\times$$

which maps

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto d \pmod{N}.$$

This is a surjective group homomorphism. Since $ker\varphi = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| d \equiv 1 \pmod{N} \right\}$, $d \equiv 1 \pmod{N}$, then a is also congruent to 1 modulo N. So $ker\varphi = \Gamma_1(N)$. Thus $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$.

□

Proposition 2.1.4. *We have the index $[SL_2(\mathbb{Z}) : \Gamma_0(p)] = p + 1$ where p is prime.*

Proof. Let

$$\tilde{\varphi} : \Gamma_1(N) \to (\mathbb{Z}/N\mathbb{Z})$$

which maps

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \mapsto b \pmod{N}.$$

This is a surjective group homomorphism. Since $ker\tilde{\varphi} = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| b \equiv 0 \pmod{N} \right\}$, then $ker\tilde{\varphi} = \Gamma(N)$. Thus $\Gamma(N)$ is a normal subgroup of $\Gamma_1(N)$.

Therefore

$$\Gamma_1(N)/\Gamma(N) \cong \mathbb{Z}/N\mathbb{Z}$$

and by the previous proposition we know that

$$\Gamma_0(N)/\Gamma_1(N) \cong (\mathbb{Z}/N\mathbb{Z})^\times$$

Furthermore,

$$\phi : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/N\mathbb{Z})$$

has kernel $\Gamma(N)$. Then

$$SL_2(\mathbb{Z})/\Gamma(N) \cong SL_2(\mathbb{Z}/N\mathbb{Z})$$

Now, we need to show that:

$$[SL_2(\mathbb{Z}) : \Gamma(p)] = p^3 - p.$$

This means that we need to show $\mid SL_2(\mathbb{Z}/p\mathbb{Z}) \mid = p^3 - p$. First, let us find the order of $GL_2(\mathbb{Z}/p\mathbb{Z})$. Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{Z}/p\mathbb{Z})$. Since we don't want to have determinant zero, we're excluding the case $(a, b) = (0, 0)$. Then there is $p^2 - 1$ possibility for the tuple (a, b). Then the tuple (c, d) has $p^2 - p$ possible values because we're excluding the case where (c, d) is a multiple of (a, b). If this would be the case, we get determinant zero. Therefore $\mid GL_2(\mathbb{Z}/p\mathbb{Z}) \mid = (p^2 - p)(p^2 - 1)$. Since we have the surjection $\det : GL_2(\mathbb{Z}/p\mathbb{Z}) \to (\mathbb{Z}/p\mathbb{Z})^\times$ and it has kernel $SL_2(\mathbb{Z}/p\mathbb{Z})$, the order of $SL_2(\mathbb{Z}/p\mathbb{Z}) = \frac{(p^2-p)(p^2-1)}{p-1} = p^3 - p$. Therefore we have:

$$[SL_2(\mathbb{Z}) : \Gamma(p)] = [SL_2(\mathbb{Z}) : \Gamma_0(p)][\Gamma_0(p) : \Gamma_1(p)][\Gamma_1(p) : \Gamma(p)]$$

$$p^3 - p = [SL_2(\mathbb{Z}) : \Gamma_0(p)] \mid (\mathbb{Z}/p\mathbb{Z})^\times \mid . \mid \mathbb{Z}/p\mathbb{Z} \mid$$

$$p^3 - p = [SL_2(\mathbb{Z}) : \Gamma_0(p)](p - 1)p.$$

Hence

$$[SL_2(\mathbb{Z}) : \Gamma_0(p)] = p + 1$$

□

Definition 2.1.5. Let Γ be a subgroup of $SL_2(\mathbb{Z})$. The subgroup Γ is called a *congruence subgroup of level* N if N is the smallest positive integer which satisfies $\Gamma(N) \subset \Gamma$.

2.2 Modular Forms

In this section, we will introduce the modular forms of weight k with respect to the congruence subgroup Γ.

Definition 2.2.1. Let $f : \mathcal{H} \to \mathbb{C}$ be a function. The slash k operator $-|_k$ is defined by

$$(f \mid_k \gamma)(z) = (cz + d)^{-k} f(\gamma z)$$

where $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$ and $z \in \mathcal{H}$.

Definition 2.2.2. Let $f : \mathcal{H} \to \mathbb{C}$ be a holomorphic function. The function f is called *weakly modular of weight k with respect to* Γ if $f \mid_k \gamma = f$ for all $\gamma \in \Gamma$.

To define the modular forms, we should explain what it means to be *"holomorphic at the cusps"*. Let f be a weakly modular function of weight k with respect to Γ. Since $\Gamma(N) \subseteq \Gamma$, there exists $\gamma = \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} \in \Gamma$ for some $h \in \mathbb{Z}_{\geqslant 0}$. Then $f(z) = f(z+h)$ which means f is $h\mathbb{Z}$-periodic. Therefore f has a Fourier expansion $f = \sum_{n=-m}^{\infty} a_n q_h^n$ where $q_h^n = e^{2\pi i z/h}$, this is the q-expansion at ∞. If $a_n = 0$ for all $n < 0$, then f is called *holomorphic at* ∞.

If f is weakly modular for Γ, then for all $\alpha \in SL_2(\mathbb{Z})$, $f \mid_k \alpha$ is weakly modular for $\alpha^{-1}\Gamma\alpha$.

A *cusp* c is a Γ-equivalence class of the action of Γ on $\mathbb{Q} \cup \{\infty\}$. Let h be the minimal positive integer which satisfies $\begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} \in \alpha^{-1}\Gamma\alpha$ for all $\alpha \in SL_2(\mathbb{Z})$ with $c = \alpha \cdot \infty$, then h is called the *width of the cusp* c. The function $f \mid_k \alpha$ is $h\mathbb{Z}$-periodic where h is the width of the cusp c and the q-expansion of $f \mid_k \alpha$ at ∞ is the q-expansion of f at the cusp c.

We say f is *holomorphic at the cusp* c if $f \mid_k \alpha$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$ with $c = \alpha \cdot \infty$. Say f is holomorphic at the cusps if $f \mid_k \alpha$ is holomorphic at ∞ for all cusp c and for all $\alpha \in SL_2(\mathbb{Z})$ with $c = \alpha \cdot \infty$.

Proposition 2.2.3. *The action of $SL_2(\mathbb{Z})$ on the extended upper-half-plane $\mathcal{H}^*$ is transitive. Hence $\Gamma = SL_2(\mathbb{Z})$ has only one cusp.*

Proof. Let $\frac{a}{c} \in \mathbb{Q}$ where a and c are coprimes. Then there exist $b, d \in \mathbb{Z}$ such that $ad - bc = 1$ by Bézout's theorem. Let $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})$, then we have $\gamma \cdot \infty = \frac{a}{c}$. Therefore the action of $SL_2(\mathbb{Z})$ on $\mathbb{Q} \cup \{\infty\}$ is transitive. Thus there exists only one cusp.

□

Definition 2.2.4. Let Γ be a congruence subgroup and k be a non-negative integer. Let $f : \mathcal{H} \to \mathbb{C}$ be a holomorphic function. Then f is called a *modular form of weight k with respect to* Γ if it satisfies the following properties:

- f is weakly modular of weight k with respect to Γ,
- $f \mid_k \alpha$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$.

The set of all modular forms of weight k with respect to Γ is denoted by $\mathcal{M}_k(\Gamma)$ and this is a $\mathbb{C}$-vector space. The space of all modular forms of all weights is denoted by:

$$\mathcal{M}(\Gamma) := \bigoplus_{k \in \mathbb{Z}} \mathcal{M}_k(\Gamma)$$

and this is a graded ring.

The set of modular forms of weight k with coefficients in a ring $\mathbf{A} \subset \mathbb{C}$ is denoted by $\mathcal{M}_k(\Gamma, \mathbf{A})$. This set is an $\mathbf{A}$-module.

Remark. Let $f \in \mathcal{M}_k(SL_2(\mathbb{Z}))$. Since $\begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \in SL_2(\mathbb{Z})$, we have

$$f(z) = (-1)^k f(z)$$

and this implies that there is no non-zero modular form of odd weight with respect to $SL_2(\mathbb{Z})$.

Definition 2.2.5. A modular form f with respect to Γ of weight k is called a *cusp form* of weight k if $a_0(f \mid_k \alpha) = 0$ for all $\alpha \in SL_2(\mathbb{Z})$.

The set of all cusp forms of weight k is denoted by $\mathcal{S}_k(\Gamma)$ and it is a vector subspace of $\mathcal{M}_k(\Gamma)$.

2.3 Examples of Modular Forms of Level $N = 1$

The most trivial examples of modular forms are non-zero constant functions defined on the upper half-plane and they have weight zero, also the zero function which has weight k for all integers. Now, we will define the Eisenstein series of weight k which are the first examples of non-constant modular forms of level $N = 1$. Later, it will

be seen that they are important for the space of modular forms modulo l and the l-adic modular forms that we will study.

Let us define the following sum:

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

which is called the *Eisenstein series of weight k*.

Theorem 2.3.1. *The Eisenstein series G_k is a modular form of weight k where $k \geqslant 3$.*

Proof. Let $k \geqslant 3$ be odd. Then

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

Then G_k is a modular form for all odd weights k.

Let k be even. Then the Eisenstein series G_k converges absolutely and it is a holomorphic function for $k \geqslant 4$.[Serre, 2012]

To show that G_k is weakly modular, it is enough to show for the matrices S and T, since $SL_2(\mathbb{Z})$ is generated by these two matrices.

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

and

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

We could do these rearrangements in the series because G_k converges absolutely when $k \geqslant 4$. So G_k is weakly modular of weight k.

Now, we need to show that G_k is holomorphic at ∞. Since G_k converges uniformly,

$$\lim_{\Im(z)\to\infty} G_k(z) = \sum_{\substack{(m,n)\in\mathbb{Z}^2 \\ (m,n)\neq(0,0)}} \lim_{\Im(z)\to\infty} \frac{1}{(m+nz)^k} = \sum_{n\neq 0} \frac{1}{n^k} = 2\zeta(k)$$

Recall Riemann's removable singularity theorem from complex analysis. To show that it is holomorphic at ∞, it is enough to show that G_k is bounded. So G_k is holomorphic at ∞.

Thus the Eisenstein series G_k is a modular form of weight k.

□

Let $E_k := \frac{G_k}{2\zeta(k)}$ where $\zeta(k)$ is the Riemann zeta function, this series is called the *normalized Eisenstein series.*

Theorem 2.3.2. *The normalized Eisenstein series of weight $k \geqslant 3$ has a q-expansion*

$$E_k = 1 - \frac{2k}{B_k} \sum_{n\geqslant 1} \sigma_{k-1}(n) q^n$$

where $\sigma_k(n) = \sum_{d|n} d^k$ and B_k is the kth Bernoulli number which is defined by

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!}$$

Proof. See [Diamond and Shurman, 2005], Chapter 1.

□

Example 2.3.3.

- $E_4 = 1 + 240 \sum_{n\geqslant 1} \sigma_3(n) q^n$
- $E_6 = 1 - 504 \sum_{n\geqslant 1} \sigma_5(n) q^n$

Here we can see that all the coefficients of the q-expansions of E_4 and E_6 are integers. Furthermore, these two Eisenstein series generate the graded ring $\mathcal{M}(SL_2(\mathbb{Z})) = \bigoplus_{k\in\mathbb{Z}} \mathcal{M}_k(SL_2(\mathbb{Z}))$.

Another important example of a non-constant modular form is the modular discriminant.

Definition 2.3.4. The *modular discriminant* is defined as

$$\Delta := \frac{E_4^3 - E_6^2}{1728}$$

The modular discriminant Δ has q-expansion:

$$\Delta = \sum_{n=1}^{\infty} \tau(n) q^n$$

where $\tau(n)$ is called *Ramanujan tau function*. Since $a_0(\Delta) = 0$, it vanishes at ∞. So Δ is a cusp form of weight 12 and it generates the space of cusp forms $S_{12}(SL_2(\mathbb{Z}))$, since $dim(\mathcal{M}_{12}(SL_2(\mathbb{Z})) = 2$ and this means that $dim(\mathcal{S}_{12}(SL_2(\mathbb{Z}))) = 1$ by Example 2.4.11. One can also show that

$$\Delta = q \prod_{n=1}^{\infty} (1 - q^n)^{24}.$$

Remark. We can also define the Eisenstein series of weight 2 as follows:

$$E_2 = 1 - 24 \sum_{n \geqslant 1} \sigma_1(n) q^n$$

But this series fails to be absolutely convergent and hence it is not a modular form with respect to $SL_2(\mathbb{Z})$. Even though it is not a modular form in the classical sense, we will later see that we can talk about l-adic Eisenstein Series of weight 2 which is an l-adic modular form. This Eisenstein series E_2 is important because we will use this to define derivation ∂ on the space of modular forms.

2.4 Dimension Formula

The aim of this section is to give the dimension formula for the vector space of modular forms for an arbitrary weight k and level N, with respect to the congruence subgroup Γ.

First of all, we will define the necessary notions to state the formula such as the elliptic point and the period of an elliptic point. Then we will state the dimension formula. For the detailed proofs, see Chapter 3 of [Diamond and Shurman, 2005].

Definition 2.4.1. We define the *modular curve* as the quotient of the upper-half-plane by the left action of a congruence subgroup Γ and it is a Riemann surface.

We denote the modular curve by $Y(\Gamma) = \Gamma\backslash\mathcal{H}$. This can be compactified and the compact modular curve is denoted by $X(\Gamma) = \Gamma\backslash\mathcal{H}^*$

Definition 2.4.2. Let Γ be a congruence subgroup. An *elliptic point* is defined as the point $z \in \mathcal{H}$ such that $\{\pm I\}$ is a proper subgroup of $\{\pm I\}\Gamma_z$ where Γ_z is the stabilizer of z in Γ.

Definition 2.4.3. Let $z \in \mathcal{H}$ be an elliptic point. Then the *period* of this elliptic point is defined by

$$h_z = \begin{cases} \frac{|\Gamma_z|}{2} & \text{if } -I \in \Gamma_z \\ |\Gamma_z| & \text{otherwise.} \end{cases}$$

Proposition 2.4.4. *The elliptic points for $SL_2(\mathbb{Z})$ are the points i with period 2 and $\rho = e^{2\pi i/3} = \frac{-1+i\sqrt{3}}{2}$ with period 3.*

Proof. The points i and ρ are the only elliptic points, see [Miyake, 2006], Section 4.1. for the proof. We will only show the calculation of the periods of these points. First, we are looking for the stabilizer of i. Let $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbb{Z})_i$. We have

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} i = \frac{ai+b}{ci+d} = i$$

So $ai + b = di - c$. So $a = d$ and $b = -c$. Thus we have the stabilizer of i:

$$SL_2(\mathbb{Z})_i = \left\{ \pm I, \begin{bmatrix} 0 & \mp 1 \\ \pm 1 & 0 \end{bmatrix} \right\}$$

Then the period of i is $h_i = \frac{|SL_2(\mathbb{Z})_i|}{2} = 2$.

Now, we will find the period of ρ. To do so, we calculate the stabilizer of ρ which is:

$$SL_2(\mathbb{Z})_\rho = \left\{ \pm I, \begin{bmatrix} \mp 1 & \mp 1 \\ \pm 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & \mp 1 \\ \pm 1 & \pm 1 \end{bmatrix} \right\}$$

So the period of ρ is $h_\rho = \frac{|SL_2(\mathbb{Z})_\rho|}{2} = 3$.

□

Now, we will give a formula for the genus of a compact modular curve which follows from the *Riemann-Hurwitz formula*. First, let us recall the standard theorem from complex analysis [Busam and Freitag, 2009].

Theorem 2.4.5. *Let f be a non-constant analytic function at the point x such that $f(z) - \omega_0$ has order n at x. Then there exist a neighbourhood U of ω_0 and a neighbourhood V of x such that every $\omega \in U \backslash \{\omega_0\}$ has exactly n preimages in V.*

Let X and Y be two compact Riemann surfaces and $f : X \to Y$ be a non-constant holomorphic function. Let e_x be the non-negative integer which makes f an e_x-to-1 map near x by Theorem 2.4.5 and it is called the *ramification degree (multiplicity)* of f at x.

The *degree* d of f is the number of $x \in X$ such that $f(x) = y$ so it is $|f^{-1}(y)|$ and it is also equals to $\sum_{x \in f^{-1}(y)} e_x$ which is finite and independent from the choice of y.

Theorem 2.4.6 (Riemann-Hurwitz Formula)**.** *Let X and Y be compact Riemann surfaces. Let $f : X \to Y$ be a non-constant holomorphic function with degree d and X has genus g_1, Y has genus g_2. Then we have the following formula:*

$$2g_1 - 2 = d(2g_2 - 2) + \sum_{x \in X} (e_x - 1)$$

Proposition 2.4.7. *Let Γ_1 and Γ_2 be congruence subgroups such that $\Gamma_1 \subset \Gamma_2$. Then the degree d of natural projection $f : X(\Gamma_1) \to X(\Gamma_2)$ such that $f(\Gamma_1 z) = \Gamma_2 z$ is*

$$d = [\{\pm I\}\Gamma_2 : \{\pm I\}\Gamma_1]$$

Proof. Since $\Gamma_1 \subset \Gamma_2$, we have $\{\pm I\}\Gamma_2 = \bigcup_j \{\pm I\}\Gamma_1\gamma_j$ where $\gamma_j \in \Gamma_2$. Let $y = \Gamma_2 z \in X(\Gamma_2)$. Then the degree $d = |f^{-1}(y)| = |f^{-1}(\Gamma_2 z)| = |\{\Gamma_1\gamma_j z\}|$. Assume $\Gamma_1\gamma_1 z = \Gamma_1\gamma_2 z$ where $\gamma_1 \neq \gamma_2$, then $\Gamma_1\gamma_1\gamma_2^{-1} \in (\Gamma_2)_z$. Then z is an elliptic point for Γ_2. So if z is not an elliptic point for Γ_2, the elements of the set $\{\Gamma_1\gamma_j z\}$ are distinct. Therefore $|\{\Gamma_1\gamma_j z\}|$ is the number of elliptic points which is $d = [\{\pm I\}\Gamma_2 : \{\pm I\}\Gamma_1]$. □

Theorem 2.4.8. *Let $f : X(\Gamma) \to X(SL_2(\mathbb{Z}))$ be the natural projection such that $f(\Gamma z) = SL_2(\mathbb{Z})z$. Let d be the degree of this projection. Then the genus g of $X(\Gamma)$ can be found as*

$$g = 1 + \frac{d}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2}$$

where ε_2 : the number of elliptic points of period 2

ε_3 : the number of elliptic points of period 3

ε_∞ : the number of cusps.

Proof. See [Miyake, 2006], Chapter 4. □

Before defining the dimension formula, we should define the regular and irregular cusps:

Let h be the width of the cusp c. The cusp c is is called an *irregular cusp* if the stabilizer of c, $(\alpha^{-1}\Gamma\alpha)_c$, is generated by the matrix $\begin{bmatrix} -1 & -h \\ 0 & -1 \end{bmatrix}$. Otherwise, it is called a *regular cusp.*

Theorem 2.4.9. *The dimension formula for the modular forms of weight k with respect to the congruence subgroup Γ, $\mathcal{M}_k(\Gamma)$, is*

$$dim(\mathcal{M}_k(\Gamma)) = \begin{cases} (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \frac{k}{2}\varepsilon_\infty & \text{if } k \geqslant 2, \text{ even} \\ (k-1)(g-1) + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \frac{k}{2}\varepsilon_\infty^{reg} + \frac{k-1}{2}\varepsilon_\infty^{irr} & \text{if } k \geqslant 3, \text{ odd} \\ 1 & \text{if } k = 0 \\ 0 & \text{if } k < 0. \end{cases}$$

The dimension formula for the cusp forms of weight k with respect to the congruence subgroup Γ, $\mathcal{S}_k(\Gamma)$, is

$$dim(\mathcal{S}_k(\Gamma)) = \begin{cases} (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \left(\frac{k}{2} - 1\right) \varepsilon_\infty & \text{if } k \geqslant 4, \text{ even} \\ (k-1)(g-1) + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \frac{k-2}{2}\varepsilon_\infty^{reg} + \frac{k-1}{2}\varepsilon_\infty^{irr} & \text{if } k \geqslant 3, \text{ odd} \\ g & \text{if } k = 2 \\ 0 & \text{if } k \leqslant 0 \end{cases}$$

where g : the genus

ε_2 : the number of elliptic points of period 2

ε_3 : *the number of elliptic points of period* 3

ε_∞ : *the number of cusps*

ε_∞^{reg} : *the number of regular cusps*

ε_∞^{irr} : *the number of irregular cusps*

Proof. See [Diamond and Shurman, 2005], Chapter 3.

□

Since we especially will be interested in the space of modular forms with respect to $\Gamma_0(N)$, let us see the following example.

Example 2.4.10. For $\Gamma = \Gamma_0(N)$ where $N > 2$, the necessary ingredients for the dimension formula of $\mathcal{M}_k(\Gamma_0(N))$ are as follows:

- $d = [SL_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$
- $\varepsilon_2 = \begin{cases} \prod_{p|N} \left(1 + \left(\frac{-1}{p}\right)\right) & \text{if } 4 \nmid N \\ 0 & \text{if } 4 \mid N \end{cases}$
- $\varepsilon_3 = \begin{cases} \prod_{p|N} \left(1 + \left(\frac{-3}{p}\right)\right) & \text{if } 9 \nmid N \\ 0 & \text{if } 9 \mid N \end{cases}$
- $\varepsilon_\infty = \sum_{d|N} \phi(gcd(d, N/d))$

See [Diamond and Shurman, 2005], Section 3.9.

Now, let us see the dimension formula for level one.

Example 2.4.11. Let k be even and positive. We know that $\varepsilon_\infty = 1$ by Proposition 2.2.3 and $\varepsilon_2 = \varepsilon_3 = 1$ for $SL_2(\mathbb{Z})$ by Proposition 2.4.4. The degree of the natural projection $f : X(SL_2(\mathbb{Z})) \to X(SL_2(\mathbb{Z}))$ is $d = 1$. Then we have genus:

$$g = 1 + 1 - \frac{1}{4} - \frac{1}{3} - \frac{1}{2} = 0.$$

Then we have the following dimension formula when k is an even, positive integer:

$$dim(\mathcal{M}_k(SL_2(\mathbb{Z}))) = (1-k) + \left\lfloor \frac{k}{4} \right\rfloor + \left\lfloor \frac{k}{3} \right\rfloor + \frac{k}{2}$$

and

$$dim(\mathcal{S}_k(SL_2(\mathbb{Z}))) = (1-k) + \left\lfloor \frac{k}{4} \right\rfloor + \left\lfloor \frac{k}{3} \right\rfloor + \frac{k}{2} - 1$$

Therefore, we have $dim(\mathcal{M}_k(SL_2(\mathbb{Z}))) = dim(\mathcal{S}_k(SL_2(\mathbb{Z})))+1$ and $E_k \notin \mathcal{S}_k(SL_2(\mathbb{Z}))$, since it does not vanishes at the cusp ∞. Hence, we have the following decomposition:

$$\mathcal{M}_k(SL_2(\mathbb{Z})) = \mathbb{C}E_k \oplus \mathcal{S}_k(SL_2(\mathbb{Z}))$$

Besides, we have

$$dim(\mathcal{M}_k(SL_2(\mathbb{Z}))) = \begin{cases} \lfloor \frac{k}{12} \rfloor & \text{if } k \equiv 2 \pmod{12} \\ \lfloor \frac{k}{12} \rfloor + 1 & \text{otherwise} \end{cases}$$

Moreover, we have some equalities between the Eisenstein series.

Example 2.4.12. The space $\mathcal{M}_{10}(SL_2(\mathbb{Z}))$ has dimension one by the previous example. Then it is generated by E_{10} and we have $E_{10} = 1 - 264\sum_{n\geqslant 1}\sigma_9(n)q^n$. Since $E_4E_6 \in \mathcal{M}_{10}(SL_2(\mathbb{Z}))$, there exist $\lambda \in \mathbb{C}$ such that $E_4E_6 = \lambda E_{10}$. Since $a_0(E_4E_6) = 1 = a_0(E_{10})$, we have $\lambda = 1$, and hence $E_{10} = E_4E_6$.

$$\begin{aligned} E_4E_6 &= \left(1 + 240\sum_{n\geqslant 1}\sigma_3(n)q^n\right)\left(1 - 504\sum_{n\geqslant 1}\sigma_5(n)q^n\right) \\ &= 1 + \sum_{n\geqslant 1}(240\sigma_3(n) - 504\sigma_5(n))q^n + \left(240\sum_{n\geqslant 1}\sigma_3(n)q^n\right)\left(-504\sum_{n\geqslant 1}\sigma_5(n)q^n\right) \\ &= 1 + \sum_{n\geqslant 1}(240\sigma_3(n) - 504\sigma_5(n))q^n - 120960\sum_{n\geqslant 2}\sum_{i=1}^{n-1}\sigma_5(n-i)\sigma_3(n)q^n \end{aligned}$$

Then we have

$$240\sigma_3(n) - 504\sigma_5(n) - 120960\sum_{i=1}^{n-1}\sigma_5(n-i)\sigma_3(n) = -264\sigma_9(n).$$

So we have the following identity relation between the functions $\sigma_3(n)$, $\sigma_5(n)$ and $\sigma_9(n)$ for $n \geqslant 2$:

$$11\sigma_9(n) = -10\sigma_3(n) + 21\sigma_5(n) + 5040\sum_{i=1}^{n-1}\sigma_5(n-i)\sigma_3(n).$$

Chapter 3

HECKE OPERATORS

In this chapter, we will introduce some operators on the space of modular forms such as the diamond and the Hecke operators.

In the first chapter we defined the slash operator for $SL_2(\mathbb{Z})$. We can extend this definition to $GL_2^+(\mathbb{Q})$ as

$$(f\ |_k\ \gamma)(z) = det(\gamma)^{\frac{k}{2}}(cz+d)^{-k}f(\gamma z)$$

where $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2^+(\mathbb{Q})$ and $z \in \mathcal{H}$.

Definition 3.0.1. Let Γ_1, Γ_2 be congruence subgroups of $SL_2(\mathbb{Z})$. The set of

$$\Gamma_1\alpha\Gamma_2 = \{\gamma_1\alpha\gamma_2 \mid \gamma_1 \in \Gamma_1, \gamma_2 \in \Gamma_2, \alpha \in GL_2^+(\mathbb{Q})\}$$

is called the *double coset*.

Lemma 3.0.2. *If Γ is a congruence subgroup of $SL_2(\mathbb{Z})$, then $\alpha^{-1}\Gamma\alpha \cap SL_2(\mathbb{Z})$ where $\alpha \in GL_2^+(\mathbb{Q})$, is also a congruence subgroup of $SL_2(\mathbb{Z})$.*

Proof. See [Diamond and Shurman, 2005], Lemma 5.1.1.

□

There exists an action of Γ_1 on $\Gamma_1\alpha\Gamma_2$ by multiplication on the left. So we have $\Gamma_1\alpha\Gamma_2 = \bigcup_j \Gamma_1\beta_j$ where β_j's are the orbit representatives of the action.

Now, we can define double coset operators.

Definition 3.0.3. Let Γ_1, Γ_2 be two congruence subgroups and $f \in \mathcal{M}_k(\Gamma_1)$. Then the weight k double coset operator, $-|_k\Gamma_1\alpha\Gamma_2$ is defined as follows:

$$f|_k\Gamma_1\alpha\Gamma_2 = \sum_j f|_k\beta_j$$

and $f|_k\Gamma_1\alpha\Gamma_2 \in \mathcal{M}_k(\Gamma_2)$.

First, we need to show that $(f \mid_k \Gamma_1\alpha\Gamma_2) \mid_k \tilde{\alpha} = f \mid_k \Gamma_1\alpha\Gamma_2$ for all $\tilde{\alpha} \in \Gamma_2$.

$$\begin{aligned}(f \mid_k \Gamma_1\alpha\Gamma_2) \mid_k \tilde{\alpha} &= \left(\sum_j f|_k\beta_j\right) \mid_k \tilde{\alpha} \\ &= \sum_j f|_k\beta_j\tilde{\alpha} \\ &= f \mid_k \Gamma_1\alpha\Gamma_2\end{aligned}$$

since $\beta_j\tilde{\alpha}$'s are also orbit representatives of $\Gamma_1\alpha\Gamma_2$. Moreover, $f \mid_k \Gamma_1\alpha\Gamma_2$ is holomorphic at the cusps, and hence $f|_k\Gamma_1\alpha\Gamma_2 \in \mathcal{M}_k(\Gamma_2)$.

Now, we will check this is well-defined. Let $\beta_1 = \gamma_1\alpha\gamma_2$ and $\beta_2 = \tilde{\gamma}_1\alpha\tilde{\gamma}_2$ be in the same orbit where $\gamma_1, \tilde{\gamma}_1 \in \Gamma_1$ and $\gamma_2, \tilde{\gamma}_2 \in \Gamma_2$. This means that there exists $\gamma \in \Gamma_1$ such that $\beta_1 = \gamma\beta_2$ Then

$$\begin{aligned}f \mid_k \beta_1(z) &= f \mid_k \gamma_1\alpha\gamma_2(z) = f \mid_k \gamma\tilde{\gamma}_1\alpha\tilde{\gamma}_2(z) \\ &= f \mid_k \tilde{\gamma}_1\alpha\tilde{\gamma}_2(z) = f \mid_k \beta_2 \text{ since } f \in \mathcal{M}_k(\Gamma_1)\end{aligned}$$

So $f \mid_k \beta_1 = f \mid_k \beta_2$. Thus the operator -$\mid_k \Gamma_1\alpha\Gamma_2$ is well defined.

Let $\alpha \in \Gamma_0(N)$ and $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$. The subgroup $\Gamma_1(N)$ is normal in $\Gamma_0(N)$ as we showed in the previous chapter. So $\alpha^{-1}\Gamma_1(N)\alpha = \Gamma_1(N)$. Then we have

$$f \mid_k \Gamma_1(N)\alpha\Gamma_1(N) = f \mid_k \Gamma_1(N)\alpha = f \mid_k \alpha.$$

Now, we can define the diamond operator which is a Hecke operator.

Definition 3.0.4. Let $d \in (\mathbb{Z}/N\mathbb{Z})^\times$. Then the *diamond operator*

$$\langle d\rangle : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N)) \text{ defined as } \langle d\rangle f = f \mid_k \gamma$$

where $\gamma = \begin{bmatrix} a & b \\ c & \delta \end{bmatrix} \in \Gamma_0(N)$ with $d \equiv \delta \pmod N$.

Definition 3.0.5. A *Dirichlet character modulo N* is a group homomorphism

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

Any such homomorphism takes elements of $(\mathbb{Z}/N\mathbb{Z})^\times$ to roots of unity in $\mathbb{C}^\times$. The group $(\mathbb{Z}/N\mathbb{Z})^\times$ is denoted by G_N. The set of Dirichlet characters *modulo N* forms a group $\hat{G}_N$ such that $(\chi\varphi)(x) = \chi(x)\varphi(x)$ for all $x \in G_N$. This multiplicative group is called dual group of G_N.

Definition 3.0.6. Let $\chi : G_N \to \mathbb{C}^\times$ be a Dirichlet character modulo N. We define the χ-eigenspace of

$$\mathcal{M}_k(\Gamma_0(N), \chi) = \{f \in \mathcal{M}_k(\Gamma_1(N)) \mid \langle d \rangle f = \chi(d) f, \forall d \in G_N\}.$$

3.1 The Hecke Operators

First, we will define the Hecke operator T_p where p is prime. Then we will generalize the definition to T_n for $n \in \mathbb{Z}^+$.

Definition 3.1.1. Let p be a prime. Then we define the Hecke operator

$$T_p : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))$$

such that

$$T_p(f) = f \mid_k \Gamma_1(N) \alpha \Gamma_1(N)$$

where $\alpha = \begin{bmatrix} 1 & 0 \\ 0 & p \end{bmatrix}$.

Proposition 3.1.2. *Let $f \in \mathcal{M}_k(\Gamma_1(N))$. Then we have the following formula:*

$$T_p(f) = \begin{cases} \displaystyle\sum_{j=0}^{p-1} f \mid_k \begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix} & \text{if } p \mid N \\ \displaystyle\sum_{j=0}^{p-1} f \mid_k \begin{bmatrix} 1 & j \\ 0 & p \end{bmatrix} + f \mid_k \begin{bmatrix} mp & n \\ Np & p \end{bmatrix} & \text{if } p \nmid N \text{ and } mp - nN = 1 \end{cases}$$

In this thesis, what is important for us is how the Hecke operators act on the q-expansion of modular forms.

Proposition 3.1.3. *Let $f \in \mathcal{M}_k(\Gamma_1(N))$ with q-expansion $\displaystyle\sum_{n=0}^{\infty} a_n q^n$. If p does not divide N,*

$$T_p(f) = \sum_{n=0}^{\infty} a_{np} q^n + p^{k-1} \sum_{n=0}^{\infty} a_n q^{np}.$$

If p divides N, then we have

$$T_p(f) = \sum_{n=0}^{\infty} a_{np} q^n.$$

Proposition 3.1.4. *Let $\langle d_1 \rangle$, $\langle d_2 \rangle$, T_{p_1} and T_{p_2} be the Hecke operators where p_1, p_2 are primes and $d_1, d_2 \in (\mathbb{Z}/N\mathbb{Z})^\times$. These operators are commute.*

Now, we will generalize the Hecke operator for an arbitrary positive integer n.

Definition 3.1.5. Let $T_1 = I$. If $n = p^r$, then we have the following formula:

$$T_{p^r} := T_p T_{p^{r-1}} - p^{k-1}\langle p \rangle T_{p^{r-2}}.$$

This is well defined by Proposition 3.1.4.

If $n = \prod_i p_i^{e_i}$, then the nth Hecke operator is defined by $T_n := \prod_i T_{p_i^{e_i}}$.

Definition 3.1.6. Let $f \in \mathcal{M}_k(\Gamma_1(N))$ with q-expansion $f = \sum_{n=0}^{\infty} a_n q^n$. This modular form f is called an *eigenform* if it is simultaneously an eigenvector for all the Hecke operators T_n and $\langle n \rangle$. Moreover, an eigenform is called a *normalized eigenform* if $a_1(f) = 1$.

Proposition 3.1.7. *Let $f \in \mathcal{M}_k(\Gamma_1(N))$ be a normalized eigenform with q-expansion $f = \sum_{n=0}^{\infty} a_n q^n$. Then we have:*

$$T_n(f) = a_n(f) f$$

In general, for any eigenform f:

$$T_n(f) = \frac{a_n(f)}{a_1(f)} f$$

Proof. Suppose that $a_1(f) = 1$ and $T_n(f) = \lambda_n f$ for all $n \geqslant 1$. By Proposition 3.1.3 and from Definition 3.1.5,

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

which implies that

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

Then we have $T_n(f) = a_n(f) f$.

If $a_1(f) \neq 1$,

$$T_n\left(\frac{f}{a_1(f)}\right) = a_n\left(\frac{f}{a_n(f)}\right)\frac{f}{a_1(f)} = \frac{a_n(f)}{a_1(f)}\frac{f}{a_1(f)}$$

This implies that $T_n(f) = \frac{a_n(f)}{a_1(f)} f$

□

Example 3.1.8. Take $E_4 \in \mathcal{M}_4(SL_2(\mathbb{Z}))$. By dimension formula the space $\mathcal{M}_4(SL_2(\mathbb{Z}))$ has dimension 1. Then we have $T_n(E_4) = \lambda_n E_4$. We know that $E_4 = 1 + 240\sum_{n\geqslant 1}\sigma_3(n)q^n$. Since $\sigma_3(3) = 28$, $a_3 = 28 \times 240$ and $a_1 = 240$. We also have the following:

$$\sigma_3(3n) = \begin{cases} \sigma_3(3)\sigma_3(n) & \text{if } 3 \nmid n \\ \\ \sigma_3(3^{e+1})\sigma_3(m) & \text{if } n = 3^e m \text{ where } 3 \nmid m \end{cases}$$

Then

$$\begin{aligned} T_3(E_4) &= 1 + 240\sum_{n\geqslant 1}\sigma_3(3n)q^n + 27\left(1 + 240\sum_{n\geqslant 1}\sigma_3(n)q^n\right) \\ &= 28\left(1 + 240\sum_{n\geqslant 1}\sigma_3(n)q^n\right) \\ &= \frac{a_3(E_4)}{a_1(E_4)}E_4 \end{aligned}$$

Remark. In this chapter, we defined the Hecke operators for $f \in \mathcal{M}_k(\Gamma_1(N))$, in fact we can define this operator for the congruence subgroup $\Gamma_0(N)$.

Chapter 4

CONGRUENCES OF MODULAR FORMS MOD l

In the following chapter, we introduce the modular forms modulo l. To do so, we will start by introducing the two congruences between the Eisenstein series. Then we will present the space of modular forms modulo l and we will define some operators on this space. For this chapter, we follow [Jochnowitz, 1982] and [Serre, 1973b].

Throughout this chapter, l is a prime, and $l \geqslant 5$ unless stated otherwise. Let p be a prime and assume $l \neq p$. From now on, $\Gamma_0(N)$ will be denoted by Γ and $\mathbb{Q} \cap \mathbb{Z}_l$ will be denoted by $\mathcal{R}$.

Let $x \in \mathbb{Q}_l$, this x is called an l-integral, or an l-integer if $x \in \mathbb{Z}_l$, this means the l-adic valuation $v_l(x) \geqslant 0$.

4.1 Congruences of Eisenstein Series

We willl state some of the congruences between the Eisenstein series. To do so, we need the following two theorems:

Theorem 4.1.1 (Kummer's Congruence)**.** *Let l be a prime, k be an even, positive integer such that $(l-1) \nmid k$. Then $\frac{B_k}{k}$ is an l-integer and if $k_1 \equiv k_2 \pmod{(l-1)}$,*

$$\frac{B_{k_1}}{k_1} \equiv \frac{B_{k_2}}{k_2} \pmod{l}.$$

Proof. See [Borevich and Shafarevich, 1986].

□

Theorem 4.1.2 (Clausen-von Staudt's Theorem)**.** *Let l be a prime and k be an even, positive integer such that $(l-1) \nmid k$. Then l does not divide the denominator of B_k. Moreover, we have $lB_k \equiv 1 \pmod{l}$, if $(l-1) \mid k$.*

Proof. See [Borevich and Shafarevich, 1986].

□

Theorem 4.1.3. *If* $k \equiv k' \pmod{(l-1)}$ *and* $k \not\equiv 0 \pmod{(l-1)}$, *then* $E_k \equiv E_{k'} \pmod{l}$.

Proof. Suppose that $k \equiv k' \pmod{(l-1)}$. Without loss of generality, we may assume $k = k^{'} + l - 1$. Then

$$\sigma_k(n) = \sigma_{k^{'}+l-1}(n) = \sum_{d|n} d^{k^{'}+l-1} = \sum_{d|n} d^{k^{'}} d^{l-1} \equiv \sum_{d|n} d^{k^{'}} = \sigma_{k'}(n) \pmod{l}$$

by Fermat's Little Theorem.

$$E_k = 1 - \frac{2k}{B_k} \sum_{n \geqslant 1} \sigma_{k-1}(n) q^n \equiv 1 - \frac{2k'}{B_{k'}} \sum_{n \geqslant 1} \sigma_{k'-1}(n) q^n = E_{k'+l-1} \pmod{l}$$

by Theorem 4.1.1 and the congruence $\sigma_k(n) \equiv \sigma_{k'}(n) \pmod{l}$.

□

Theorem 4.1.4. *We have* $E_k - 1 \in l\mathbb{Z}_l[\![q]\!]$ *if and only if* $(l-1) \mid k$.

Proof. Suppose that $(l-1) \mid k$, then $v_l(B_k) = -1$ by Theorem 4.1.2. This implies that $v_l\left(\frac{k}{B_k}\right) \geqslant 1$. We conclude that $E_k \equiv 1 \pmod{l}$. So we have $E_k - 1 \in l\mathbb{Z}_l[\![q]\!]$.

For the other direction of the proof, suppose that $E_k - 1 \in l\mathbb{Z}_l[\![q]\!]$ and assume that $(l-1) \nmid k$. By Theorem 4.1.1, $\frac{B_k}{k}$ is an l-integer. This means that $v_l\left(\frac{B_k}{k}\right) \geqslant 0$ and this implies that $v_l\left(\frac{k}{B_k}\right) \leqslant 0$. We also assumed that $E_k - 1 \in l\mathbb{Z}_l[\![q]\!]$, this means $E_k \equiv 1 \pmod{l}$. So we have $\frac{2k}{B_k} \equiv 0 \pmod{l}$, then $v_l\left(\frac{2k}{B_k}\right) \geqslant 1$. Since we assumed that $l \geqslant 5$ in the beginning of the chapter, we have $v_l\left(\frac{k}{B_k}\right) \geqslant 1$. This is a contradiction. Hence we have $(l-1) \mid k$.

□

4.2 The Space of Modular Forms mod l

In this part, we will introduce the space of modular forms mod l.

Definition 4.2.1. Let $\tilde{\mathcal{M}}_k(\Gamma)$ be the subset of $\mathbb{F}_l[\![q]\!]$ such that

$$\tilde{\mathcal{M}}_k(\Gamma) = \left\{ \tilde{f} = \sum_{n=0}^{\infty} \tilde{a}_n q^n \mid f = \sum_{n=0}^{\infty} a_n q^n \in \mathcal{M}_k(\Gamma, \mathcal{R}) \text{ and } \tilde{a}_n \equiv a_n \pmod{l} \right\}.$$

The set $\tilde{\mathcal{M}}_k(\Gamma)$ is called the *space of modular forms mod l of weight k, level N.*

Proposition 4.2.2. $\tilde{\mathcal{M}}_k(\Gamma) \cong \mathcal{M}_k(\Gamma, \mathcal{R})/l\mathcal{M}_k(\Gamma, \mathcal{R}) \cong \mathcal{M}_k(\Gamma, \mathcal{R}) \otimes \mathbb{F}_l$.

When $l = 2$ or 3, the reduction modulo l of the Eisenstein series of weight 4 and 6 are $\tilde{E}_4 = \tilde{E}_6 = 1$.

Proposition 4.2.3. $\dim_{\mathbb{F}_l} \tilde{\mathcal{M}}_k(\Gamma) = \dim_{\mathbb{C}} \mathcal{M}_k(\Gamma, \mathbb{C})$.

Proof. We know that the ring $\mathcal{R}$ is a discrete valuation ring. So it is a principal ideal domain. We also know that the space of modular forms $\mathcal{M}_k(\Gamma, \mathcal{R})$ is a finitely generated torsion free $\mathcal{R}$-module. Since $\mathcal{R}$ is a principal ideal domain, this implies that $\mathcal{M}_k(\Gamma, \mathcal{R})$ is a free $\mathcal{R}$-module.

Since $\mathcal{M}_k(\Gamma, \mathcal{R})$ is a free $\mathcal{R}$-module, $\mathcal{M}_k(\Gamma, \mathcal{R}) \cong \mathcal{R}^n$ for some $n \in \mathbb{N}$. Then we have

$$\mathcal{M}_k(\Gamma, \mathcal{R}) \otimes \mathbb{C} = \mathcal{M}_k(\Gamma, \mathbb{C}) \Rightarrow \mathcal{R}^n \otimes \mathbb{C} = \mathbb{C}^{\dim_{\mathbb{C}} \mathcal{M}_k(\Gamma, \mathbb{C})} \Rightarrow \mathbb{C}^n = \mathbb{C}^{\dim_{\mathbb{C}} \mathcal{M}_k(\Gamma, \mathbb{C})}$$

So $n = \dim_{\mathbb{C}} \mathcal{M}_k(\Gamma, \mathbb{C})$. Then

$$\mathcal{M}_k(\Gamma, \mathcal{R}) \otimes \mathbb{F}_l = \mathcal{R}^{\dim_{\mathbb{C}} \mathcal{M}_k(\Gamma, \mathbb{C})} \otimes \mathbb{F}_l = \mathbb{F}_l^{\dim_{\mathbb{C}} \mathcal{M}_k(\Gamma, \mathbb{C})}.$$

Thus $\dim_{\mathbb{F}_l} \tilde{\mathcal{M}}_k(\Gamma) = \dim_{\mathbb{C}} \mathcal{M}_k(\Gamma, \mathbb{C})$.

□

Definition 4.2.4. Let $\tilde{\mathcal{M}}(\Gamma) := \sum_{k=0}^{\infty} \tilde{\mathcal{M}}_k(\Gamma)$. There is an injection

$$\tilde{\mathcal{M}}_k(\Gamma) \hookrightarrow \tilde{\mathcal{M}}_{k+l-1}(\Gamma)$$

defined by multiplication with E_{l-1}, because $E_{l-1} \equiv 1 \pmod{l}$ from Theorem 4.1.4. From this map, it can be seen that $\tilde{\mathcal{M}}_k(\Gamma) \subseteq \tilde{\mathcal{M}}_{k+l-1}(\Gamma)$. Thus this sum is not a direct sum.

But this space has the following direct sum decomposition:

$$\tilde{\mathcal{M}}(\Gamma) = \bigoplus_{\alpha \in \mathbb{Z}/(l-1)\mathbb{Z}} \tilde{\mathcal{M}}_k{}^{\alpha}(\Gamma)$$

where $\tilde{\mathcal{M}}_k{}^{\alpha}(\Gamma)$ is $\sum_{k=0}^{\infty} \tilde{\mathcal{M}}_k(\Gamma)$ where $k \equiv \alpha \pmod{(l-1)}$ for all k. This also implies that the space $\tilde{\mathcal{M}}(\Gamma)$ is a graded algebra. For the level $N = 1$, see [Serre, 1973a] and see [Katz, 1973] for an arbitrary level N.

Theorem 4.2.5. *The intersection of $\tilde{\mathcal{M}}_k(\Gamma)$ and $\tilde{\mathcal{M}}_{k'}(\Gamma)$ is non-empty if and only if the weights satisfy $k \equiv k' \pmod{(l-1)}$.*

Proof. Suppose that $k \equiv k' \pmod{(l-1)}$. The fact that $\tilde{\mathcal{M}}_k(\Gamma) \cap \tilde{\mathcal{M}}_{k'}(\Gamma) \neq \varnothing$ directly follows from Definition 4.2.4.

For the other direction, suppose that $\tilde{f} \in \tilde{\mathcal{M}}_k(\Gamma) \cap \tilde{\mathcal{M}}_{k'}(\Gamma)$. Then there exists $f \in \mathcal{M}_k(\Gamma)$ and $f' \in \mathcal{M}_{k'}(\Gamma)$ such that $\tilde{f} \equiv f \equiv f' \pmod{l}$. Then we have the result for level one that will be shown in Theorem 6.1.2. For arbitrary level N, see [Katz, 1977].

□

Definition 4.2.6. The filtration w is defined on $\tilde{\mathcal{M}}(\Gamma)$ by

$$w(f) = \inf\{k : f \in \tilde{\mathcal{M}}_k(\Gamma)\}$$

and by convention $w(f) = -\infty$, if $f = 0$.

Example 4.2.7.

- $w(E_{l-1}) = 0$, because $E_{l-1} \equiv 1 \pmod{l}$ and 1 has weight 0.
- When we have the level $N = 1$, the filtration $w(E_{l+1}) = l + 1$, since in modulo l, the Eisenstein series E_{l+1} is congruent to E_2 but this is not a modular form. The only modular from of weight 2 in level 1 is $f = 0$.

4.3 Operators on Modular Forms

Definition 4.3.1. Let f has the q-expansion $\sum_{n=0}^{\infty} a_n q^n$. Define the operators U, V and θ on $\mathbb{F}_l[\![q]\!]$ by

- $U(f) = \sum_{n=0}^{\infty} a_{nl} q^n$
- $\theta(f) = \sum_{n=0}^{\infty} n a_n q^n$
- $V(f) = \sum_{n=0}^{\infty} a_n q^{nl}$

If $l = p$, we have $T_p(\tilde{f}) = U(\tilde{f})$ when $\tilde{f} \in \tilde{\mathcal{M}}(\Gamma)$.

Theorem 4.3.2. *The operators U, V and θ induce operators on $\tilde{\mathcal{M}}(\Gamma)$.*

Proof. Let $\tilde{f} \in \tilde{\mathcal{M}}(\Gamma)$, we will show that $U(\tilde{f})$ is also in $\tilde{\mathcal{M}}(\Gamma)$. It can be seen that $U(\tilde{f}) \in \mathbb{F}_l[\![q]\!]$. If $f \in \mathcal{M}_k(\Gamma, \mathcal{R})$ we know that $T_l(f)$ is also in $\mathcal{M}_k(\Gamma, \mathcal{R})$ and we have seen that $T_l(f) = U(f) + l^{k-1}V(f) \equiv U(f) \pmod{l}$. So $U(\tilde{f}) \in \tilde{\mathcal{M}}_k(\Gamma)$.

For the operator V, we have $V(f) \equiv f^l \pmod{l}$ by the Fermat's little theorem as in the Theorem 4.3.6 and hence $V(\tilde{f}) \in \tilde{\mathcal{M}}(\Gamma)$.

The fact that $\theta(\tilde{f}) \in \tilde{\mathcal{M}}(\Gamma)$ follows from the following Theorem 4.3.3 and the fact that $E_2 \equiv E_{l+1} \pmod{l}$.

□

If $f \in \mathcal{M}_k(\Gamma)$, usually $\frac{d}{dz}f(z)$ is not a modular form and $\theta(f)$ is also usually not a modular form.

Theorem 4.3.3. *There exist a map $\partial : \mathcal{M}_k(\Gamma, \mathcal{R}) \to \mathcal{M}_{k+2}(\Gamma, \mathcal{R})$ defined by*

$$\partial(f) = \theta(f) - \frac{k}{12}E_2 f.$$

Furthermore, ∂ is a derivation on $\tilde{\mathcal{M}}(\Gamma, \mathcal{R})$.

Proof. First, let us show that $\partial : \mathcal{M}_k(\Gamma, \mathcal{R}) \to \mathcal{M}_{k+2}(\Gamma, \mathcal{R})$. Let $f \in \mathcal{M}_k(\Gamma, \mathcal{R})$. Let $\partial(f) = \theta(f) - \frac{k}{12}E_2 f = g$. We have to show that $g \in \mathcal{M}_{k+2}(\Gamma, \mathcal{R})$. It can be seen that g is holomorphic on $\mathcal{H}$ since f, E_2 and $\theta(f)$ are holomorphic on $\mathcal{H}$.

To begin with, we need to show that ∂f is weakly modular. Let $\alpha = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \Gamma_0(N)$.

$$\begin{aligned}
\partial f \mid_{k+2} \alpha &= \theta(f) \mid_{k+2} \alpha - \frac{k}{12}(E_2 \mid_2 \alpha)(f \mid_k \alpha) \\
&= \frac{1}{2\pi i}f' + \frac{1}{2\pi i}\frac{ck}{(cz+d)}f - \frac{k}{12}\left(E_2 + \frac{1}{2\pi i}\frac{12c}{(cz+d)}\right)f \\
&= \frac{1}{2\pi i}f' - \frac{k}{12}E_2 f \\
&= \theta(f) - \frac{k}{12}E_2 f = \partial(f)
\end{aligned}$$

Therefore $\partial(f)$ is weakly modular of weight $k+2$.

Now, we need to show that ∂ is a derivation. This map is clearly linear. We need to show that ∂ satisfies the Leibniz formula. Let $f \in \mathcal{M}_k$ and $g \in \mathcal{M}_{k'}$.

$$\begin{aligned}\partial(fg) &= \theta(fg) - \frac{(k+k')}{12}E_2fg \\ &= \theta(f)g + f\theta(g) - \frac{k}{12}E_2fg - \frac{k'}{12}E_2fg \\ &= (\theta(f) - \frac{k}{12}E_2f)g + (\theta(g) - \frac{k'}{12}E_2g)f \\ &= \partial(f)g + f\partial(g)\end{aligned}$$

So ∂ is a derivation on $\mathcal{M}(\Gamma, \mathcal{R})$.

□

Remark. The operator θ can be written as $\theta(f) = \partial(f) + \frac{k}{12}E_2f$. Since $E_{l-1} \equiv 1 \pmod{l}$ and $E_2 \equiv E_{l+1} \pmod{l}$, we get $\theta(f) \equiv \partial(f)E_{l-1} + \frac{k}{12}E_{l+1}f \pmod{l}$. So $\theta(f) \in \tilde{\mathcal{M}}_{k+l+1}(\Gamma)$.

Theorem 4.3.4. *The filtration satisfies $w(\theta f) \leqslant w(f) + l + 1$ and if $l \nmid w(f)$, then this is an equality.*

Proof. Let $w(f) = k$. If $l \mid k$, then $\theta(f) \equiv \partial(f) \pmod{l}$. Since ∂ maps a weight k modular form to a weight $k+2$ modular form, $\theta(f) \in \tilde{\mathcal{M}}_{k+2}(\Gamma)$. Therefore $w(\theta f) \leqslant k + 2 = w(f) + 2$.

For the case $l \nmid k$, see the [Katz, 1977].

□

Proposition 4.3.5. $T_p \circ \theta = p\theta \circ T_p$

Proof. Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a modular form of weight k. Then

$$\begin{aligned}
(T_p \circ \theta)(f) = T_p\left(\sum_{n=0}^{\infty} n a_n q^n\right) &= \sum_{n=0}^{\infty} npa_{np}q^n + p^{(k+l+1)-1}\left(\sum_{n=0}^{\infty} a_n q^{np}\right) \\
&= \sum_{n=0}^{\infty} npa_{np}q^n + p^{k+1}\left(\sum_{n=0}^{\infty} a_n q^{np}\right) \\
&= p\left(\sum_{n=0}^{\infty} na_{np}q^n + p^{k-1}\sum_{n=0}^{\infty} npa_n q^{np}\right) \\
&= p\theta\left(\sum_{n=0}^{\infty} a_{np}q^n + p^{k-1}\sum_{n=0}^{\infty} a_n q^{np}\right) \\
&= p\theta\left(T_p\left(\sum_{n=0}^{\infty} a_n q^n\right)\right) \\
&= (p\theta \circ T_p)(f)
\end{aligned}$$

because θ operator changes the weight k to $k + l + 1$ and $p^{l-1} \equiv 1 \pmod{l}$ by Fermat's Little Theorem.

□

Theorem 4.3.6. *Let $f \in \tilde{\mathcal{M}}_k(\Gamma)$, then $Vf \in \tilde{\mathcal{M}}_{kl}(\Gamma)$.*

Proof. Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a modular form of weight k. Then $Vf = \sum_{n=0}^{\infty} a_n q^{nl}$. Since l is a prime, we have $Vf = f^l$ by Fermat's Little Theorem. Therefore $Vf \in \tilde{\mathcal{M}}_{kl}(\Gamma)$.

□

Theorem 4.3.7. *The filtration $w(Vf) = lw(f)$.*

Proof. For the proof see [Katz, 1977].

□

Proposition 4.3.8. *Let I be the identity map. We have the following relations between the operators U, V, T_p and θ on $\tilde{\mathcal{M}}(\Gamma)$:*

1. $T_p \circ V = V \circ T_p$

2. $U \circ V = I$

3. $V \circ U = I - \theta^{(l-1)}$

Proof. Let $f = \sum_{n=0}^{\infty} a_n q^n$ be a modular form of weight k.

1. Then:

$$\begin{aligned}(T_p \circ V)(f) = T_p\left(\sum_{n=0}^{\infty} a_n q^{nl}\right) &= \sum_{n=0}^{\infty} a_{np} q^{nl} + p^{k-1} \sum_{n=0}^{\infty} a_n q^{npl} \\ &= V\left(\sum_{n=0}^{\infty} a_{np} q^n + p^{k-1} \sum_{n=0}^{\infty} a_n q^{np}\right) \\ &= V\left(T_p\left(\sum_{n=0}^{\infty} a_n q^n\right)\right) \\ &= (V \circ T_p)(f)\end{aligned}$$

2. We have:

$$(U \circ V)(f) = U\left(\sum_{n=0}^{\infty} a_n q^{nl}\right) = U\left(\sum_{n=0}^{\infty} b_n q^n\right)$$

where $b_n = 0$ if $l \nmid n$ and $b_n = a_{\frac{n}{l}}$ if $l \mid n$. Then we have

$$U\left(\sum_{n=0}^{\infty} b_n q^n\right) = \sum_{n=0}^{\infty} b_{nl} q^n = \sum_{n=0}^{\infty} a_n q^n$$

Hence $U \circ V = I$.

3. We have the following equality:

$$\begin{aligned}(V \circ U)(f) &= V\left(\sum_{n=0}^{\infty} a_{nl} q^n\right) \\ &= \sum_{n=0}^{\infty} a_{nl} q^{nl}\end{aligned}$$

We can see $\sum_{n=0}^{\infty} a_{nl} q^{nl}$ as $\sum_{n=0}^{\infty} b_n q^n$ where $b_n = 0$ if $l \nmid n$ and $b_n = a_n$ if $l \mid n$. Then:

$$\begin{aligned}(I-\theta^{l-1})(f) &= f - \sum_{n=0}^{\infty} n^{(l-1)} a_n q^n \\ &\equiv f - \sum_{\substack{n=0 \\ l\nmid n}}^{\infty} n^{(l-1)} a_n q^n \pmod{l} \\ &= f - \sum_{\substack{n=0 \\ l\nmid n}}^{\infty} a_n q^n \text{ by Fermat's Little Theorem} \\ &= \sum_{n=0}^{\infty} b_n q^n\end{aligned}$$

where $b_n = 0$ if $l \nmid n$ and $b_n = a_n$ if $l \mid n$. Therefore $V \circ U = I - \theta^{l-1}$.

□

Proposition 4.3.9. *We have the following exact sequence:*

$$0 \longrightarrow \tilde{\mathcal{M}}(\Gamma) \xrightarrow{V} \tilde{\mathcal{M}}(\Gamma) \xrightarrow{\theta} \tilde{\mathcal{M}}(\Gamma) \xrightarrow{U} \tilde{\mathcal{M}}(\Gamma) \longrightarrow 0$$

Proof. First, we will show that the operator V is injective. Let $f, g \in \tilde{\mathcal{M}}(\Gamma)$. Suppose that $Vf = Vg$. Then we have $U(Vf) = U(Vg)$. Since $U \circ V$ is the identity map by Proposition 4.3.8(2), we have $f = g$. Thus V is injective.

The fact that the operator U is surjective directly follows from $U(Vf) = f$ for all $f \in \tilde{\mathcal{M}}(\Gamma)$.

Now, we will show that $\operatorname{Im} V = \ker \theta$.

$$\begin{aligned}\theta(Vf) = \theta\left(V\left(\sum_{n=0}^{\infty} a_n q^n\right)\right) &= \theta\left(\sum_{n=0}^{\infty} a_n q^{nl}\right) \\ &= \sum_{n=0}^{\infty} nl a_n q^{nl} \equiv 0 \pmod{l}\end{aligned}$$

Hence, we have $\operatorname{Im} V \subseteq \ker \theta$.

For the other direction of the inclusion, let $f = \sum_{n=0}^{\infty} a_n q^n$ such that $\theta f = 0$. We want to show that there exists g such that $Vg = f$. Let $g = Uf$. Then

$$\begin{aligned}Vg = V(Uf) &= f - \theta^{(l-1)} f \text{ by Proposition 4.3.8(3)} \\ &\equiv f \pmod{l}.\end{aligned}$$

So we have $\ker\theta \subseteq \operatorname{Im} V$, and hence $\ker\theta = \operatorname{Im} V$.

Lastly, we need to show $\operatorname{Im}\theta = \ker U$. Let $Uf = 0$. This implies $\sum_{n=0}^{\infty} a_{nl}q^n = 0$. So $a_{nl} = 0$ for all $n \in \mathbb{N}$. Then $f = \sum_{\substack{n=0 \\ l\nmid n}}^{\infty} a_n q^n$. If we apply the operator θ, we get:

$$\theta^{l-1}f = \sum_{\substack{n=0 \\ l\nmid n}}^{\infty} n^{l-1}a_n q^n = \sum_{\substack{n=0 \\ l\nmid n}}^{\infty} a_n q^n = f.$$

Thus $\ker U \subseteq \operatorname{Im}\theta$. For the other direction of the inclusion:

$$\begin{aligned} U(\theta f) = U\left(\theta\left(\sum_{n=0}^{\infty} a_n q^n\right)\right) &= U\left(\sum_{n=0}^{\infty} n a_n q^n\right) \\ &= \sum_{n=0}^{\infty} n l a_{nl} q^n \equiv 0 \pmod{l}. \end{aligned}$$

Hence $\operatorname{Im}\theta = \ker U$. Therefore we have the exact sequence.

□

Proposition 4.3.10. *We have the following inequality:*

$$w(Uf) \leqslant \frac{w(f) + l^2 - 1}{l}.$$

When $w(f) \equiv 1 \pmod{l}$, this is an equality.

Proof. We already know that

$$\begin{aligned} w(V(Uf)) &= w(f - \theta^{l-1}f) \text{ by Proposition 4.3.8(3)} \\ &= w(\theta^{l-1}f) \\ &\leqslant w(f) + l^2 - 1 \text{ by Theorem 4.3.4.} \end{aligned}$$

We also know that $w(V(Uf)) = lw(Uf)$ by Theorem 4.3.7. Therefore we have

$$w(Uf) \leqslant \frac{w(f) + l^2 - 1}{l}.$$

Let $w(f) \equiv 1 \pmod{l}$. Then by Theorem 4.3.4, we have $w(\theta^{l-1}f) = w(f) + l^2 - 1$. Hence we have $w(Uf) = \frac{w(f)+l^2-1}{l}$.

□

Corollary 4.3.11. *When the filtration $w(f) \equiv 1 \pmod{l}$, Uf is nonzero.*

Proof. Since we have $\Gamma_0(N)$ as the congruence subgroup, the filtration should be even. So $w(f) \neq 1$. Therefore $w(Uf)$ is non-zero. Hence Uf is also non-zero by the Proposition 4.3.10.

□

Chapter 5

SYSTEMS OF EIGENVALUES OF MODULAR FORMS

In this chapter, our main goal is to give the proof of the theorem which says there exist finitely many systems of eigenvalues modulo l for a fixed level N. To do so, we will be following [Jochnowitz, 1982] as in the previous chapter. First, we will define the system of eigenvalues, and the Hecke module. Then we will prove our main theorem.

We fix a level N and a prime l such that $l \geqslant 5$ and $l \nmid N$, as in the previous chapter.

5.1 Number of Systems of Eigenvalues

Definition 5.1.1. The set $\{\lambda_p : l \nmid p\}$ where $\lambda_p \in \bar{\mathbb{F}}_l$ is called the *system of eigenvalues mod* l, if there exists an integer $k \geqslant 0$ and $f \in \tilde{\mathcal{M}}_k(\Gamma) \otimes \bar{\mathbb{F}}_l$ such that $T_p f = \lambda_p f$ for all $p \nmid N$.

Let us denote the following quotient space:

$$W_k = (\tilde{\mathcal{M}}_k(\Gamma) \otimes \bar{\mathbb{F}}_l)/(\tilde{\mathcal{M}}_{k-l+1}(\Gamma) \otimes \bar{\mathbb{F}}_l).$$

Definition 5.1.2. Let p be a prime not dividing the level N. The endomorphisms of the space $\tilde{\mathcal{M}}(\Gamma)$ of modular forms mod l is an $\mathbb{F}_l$-algebra. Let $\mathcal{A}$ be the subalgebra generated by the Hecke operators T_p. The modules over this ring $\mathcal{A}$ are called Hecke modules.

Since the Hecke operators also act on the space W_k, it is a Hecke module.

Definition 5.1.3. We define the Hecke module $W_k[a]$ where a is a positive integer and $a \leqslant l-1$ as the $\bar{\mathbb{F}}_l$-vector space W_k with the action of the Hecke operators modified to give the following commutative diagram of $\bar{\mathbb{F}}_l$-vector spaces:

$$\begin{array}{ccc} W_k & \xrightarrow{T_p} & W_k \\ {\scriptstyle id}\downarrow & & \downarrow{\scriptstyle \times p^a} \\ W_k[a] & \xrightarrow{T_p} & W_k[a] \end{array}$$

Here $l \neq p$, so p is invertible modulo l. This implies that the map $\times p^a$ is an isomorphism. Hence, the Hecke modules $W_k[a]$ and W_k are isomorphic as vector spaces.

If the system of eigenvalues $\{\lambda_p\}$ appears in W_k, then $\{p^a\lambda_p\}$ appears in the Hecke module $W_k[a]$. The module $W_k[a]$ is called a *twist of* W_k, also the system $\{p^a\lambda_p\}$ is called a *twist of the system* $\{\lambda_p\}$. Since we assumed $a \leqslant (l-1)$, for each W_k there exist finitely many twists.

Lemma 5.1.4. *Let $l \nmid k$. We have the operator $\bar{\theta} : W_k \to W_{k+l+1}$ which is induced by the operator θ. This map is an injection. In addition to that, it is an isomorphism of $\bar{\mathbb{F}}_l$-vector spaces when $k \geqslant l+1$.*

Proof. Let $l \nmid k$. Then $w(\theta f) = w(f) + l + 1$ by Theorem 4.3.4. Therefore θ induces a map $\bar{\theta} : W_k \to W_{k+l+1}$.

Let $f \in \ker \bar{\theta}$. Then $\bar{\theta} f \in \tilde{\mathcal{M}}_{k+2}(\Gamma)$. Since we know that θ maps a weight k modular form to a weight $k+l+1$, we have $f \in \tilde{\mathcal{M}}_{k-l+1}(\Gamma)$. So $\bar{\theta}$ is an injection.

Let $k \geqslant l+1$. We want to show that θ is an isomorphism. To do so, it is enough to show that W_k and W_{k+l+1} have the same dimension as vector spaces. Since $W_k = (\tilde{\mathcal{M}}_k(\Gamma) \otimes \bar{\mathbb{F}}_l)/(\tilde{\mathcal{M}}_{k-l+1}(\Gamma) \otimes \bar{\mathbb{F}}_l)$, we have:

$$\dim_{\bar{\mathbb{F}}_l} W_k = \dim_{\mathbb{F}_l} \tilde{\mathcal{M}}_k(\Gamma) - \dim_{\mathbb{F}_l} \tilde{\mathcal{M}}_{k-l+1}(\Gamma)$$

We showed that $\dim_{\mathbb{F}_l} \tilde{\mathcal{M}}_k(\Gamma) = \dim_{\mathbb{C}} \mathcal{M}_k(\Gamma, \mathbb{C})$ in Proposition 4.2.3. So

$$\dim_{\bar{\mathbb{F}}_l} W_k = \dim_{\mathbb{C}} \mathcal{M}_k(\Gamma, \mathbb{C}) - \dim_{\mathbb{C}} \mathcal{M}_{k-l+1}(\Gamma, \mathbb{C})$$

By the dimension formula that we stated in Theorem 2.4.9:

$$\begin{aligned}\dim_{\bar{\mathbb{F}}_l} W_k &= (k-1)(g-1) + \left\lfloor \frac{k}{4} \right\rfloor \varepsilon_2 + \left\lfloor \frac{k}{3} \right\rfloor \varepsilon_3 + \frac{k}{4}\varepsilon_\infty - (k-l+1-1)(g-1) \\ &\quad - \left\lfloor \frac{k-l+1}{4} \right\rfloor \varepsilon_2 - \left\lfloor \frac{k-l+1}{3} \right\rfloor \varepsilon_3 - \frac{k-l+1}{4}\varepsilon_\infty \\ &= (l-1)(g-1) + \left(\left\lfloor \frac{k}{4} \right\rfloor - \left\lfloor \frac{k-l+1}{4} \right\rfloor \right) \varepsilon_2 \\ &\quad + \left(\left\lfloor \frac{k}{3} \right\rfloor - \left\lfloor \frac{k-l+1}{3} \right\rfloor \right) \varepsilon_3 + \frac{l-1}{4}\varepsilon_\infty\end{aligned}$$

Let $k = 4a + b$ and $l = 4a' + b'$ where $b = 0, 2$ and $b' = 1, 3$. Then we have:

$$\begin{aligned}\left\lfloor \frac{k}{4} \right\rfloor - \left\lfloor \frac{k-l+1}{4} \right\rfloor &= \left\lfloor \frac{4a+b}{4} \right\rfloor - \left\lfloor \frac{4(a-a')+(b-b')+1}{4} \right\rfloor \\ &= a - (a-a') - \left\lfloor \frac{(b-b')+1}{4} \right\rfloor \\ &= \begin{cases} a' & \text{if } b' = 1 \text{ or } b = 2 \\ \\ a'+1 & \text{otherwise} \end{cases}\end{aligned}$$

and

$$\begin{aligned}\left\lfloor \frac{k+l+1}{4} \right\rfloor - \left\lfloor \frac{k+2}{4} \right\rfloor &= \left\lfloor \frac{4(a+a')+(b+b')+1}{4} \right\rfloor - \left\lfloor \frac{4a+b+2}{4} \right\rfloor \\ &= a + a' + \left\lfloor \frac{(b+b')+1}{4} \right\rfloor - a - \left\lfloor \frac{b+2}{4} \right\rfloor \\ &= \begin{cases} a' & \text{if } b' = 1 \text{ or } b = 2 \\ \\ a'+1 & \text{otherwise} \end{cases}\end{aligned}$$

Hence we have:

$$\left\lfloor \frac{k}{4} \right\rfloor - \left\lfloor \frac{k-l+1}{4} \right\rfloor = \left\lfloor \frac{k+l+1}{4} \right\rfloor - \left\lfloor \frac{k+2}{4} \right\rfloor$$

and with a similar calculation we have:

$$\left\lfloor \frac{k}{3} \right\rfloor - \left\lfloor \frac{k-l+1}{3} \right\rfloor = \left\lfloor \frac{k+l+1}{3} \right\rfloor - \left\lfloor \frac{k+2}{3} \right\rfloor$$

Therefore $\dim_{\bar{\mathbb{F}}_l} W_k = \dim_{\bar{\mathbb{F}}_l} W_{k+l+1}$ and this means that $\bar{\theta}$ is an isomorphism of $\bar{\mathbb{F}}_l$-vector spaces.

□

The following theorem will imply our main theorem.

Theorem 5.1.5. *Let j be a positive integer. Then there exists a positive integer k with $k \leqslant 2l$ such that the space W_j is isomorphic to a twist of the space W_k as a Hecke module.*

Proof. If $j \leqslant 2l$, the Hecke modules W_j and $W_j[0]$ are isomorphic as Hecke modules. So let $j > 2l$. We will show that there exists $k < j$ and there exists $a \leqslant (l-1)$ such that $W_j \cong W_k[a]$. We will divide the proof into the two cases: $j \not\equiv 1 \pmod{l}$ and $j \equiv 1 \pmod{l}$.

Suppose that $j \not\equiv 1 \pmod{l}$. Let $k = j - l - 1$. Since $T_p \circ \theta = p\theta \circ T_p$ by Proposition 4.3.5 and we have induced operator $\bar{\theta}$, we have the following diagram commutes:

$$\begin{array}{ccc} W_k & \xrightarrow{\bar{\theta}} & W_{k+l+1} \\ {\scriptstyle T_p}\downarrow & & \downarrow{\scriptstyle T_p} \\ W_k & \xrightarrow{p\bar{\theta}} & W_{k+l+1} \end{array}$$

Moreover, $\bar{\theta}$ and $p\bar{\theta}$ are isomorphisms of vector spaces. Therefore $W_{k+l+1} \cong W_k[1]$ as Hecke modules. Thus when $j \not\equiv 1 \pmod{l}$ and $j > 2l$, we have the result.

Suppose that $j \equiv 1 \pmod{l}$. We know that $w(Uf) = \frac{w(f)+l^2-1}{l}$ by Proposition 4.3.10. Then the operator U induces an operator $\bar{U} : W_j \to W_{\frac{j+l^2-1}{l}}$ which is an injection. We also know that $w(Vf) = lw(f)$ by Theorem 4.3.7. So the operator V also induces an injection $\bar{V} : W_{\frac{j+l^2-1}{l}} \to W_{j+l^2-1}$. Then we have:

$$\bar{V} \circ \bar{U} : W_j \to W_{j+l^2-1}$$

By Proposition 4.3.8(3), we know that $V \circ U = I - \theta^{l-1}$. As $w(f) \leqslant j + l^2 - 1$, the operator $\bar{V} \circ \bar{U} = -\bar{\theta}^{l-1}$.

We showed that θ is an isomorphism. Since $j \equiv 1 \pmod{l}$, the operator $\bar{\theta}^{l-1}$ is also an isomorphism of $\bar{\mathbb{F}}_l$-vector spaces, and hence $\bar{V} \circ \bar{U}$ is also an isomorphism. Then $\bar{V}$ is surjective. We know that the operators $\bar{U}$ and $\bar{V}$ are injections. Then $\bar{V}$ is an isomorphism, and hence $\bar{U}$ is also an isomorphism of $\bar{\mathbb{F}}_l$-vector spaces. Moreover,

we have the following commuting diagram:

$$\begin{array}{ccc} W_j & \xrightarrow{\bar{U}} & W_{\frac{j+l^2-1}{l}} \\ {\scriptstyle T_p}\downarrow & & \downarrow{\scriptstyle T_p} \\ W_j & \xrightarrow{\bar{U}} & W_{\frac{j+l^2-1}{l}} \end{array}$$

Hence W_j and $W_{\frac{j+l^2-1}{l}}$ are isomorphic as Hecke modules. Therefore, we also have the result when $j \equiv 1 \pmod{l}$ and $j > 2l$.

□

Example 5.1.6. Let $l = 5$ and $k > 24$. Then

$$W_k \cong W_{k-6}[1] \cong W_{k-12}[2] \cong W_{k-18}[3] \cong W_{k-24}[4] = W_{k-24}$$

Theorem 5.1.7. *There exist finitely many systems of eigenvalues mod l for fixed level N.*

Proof. By the *Theorem* 5.1.5, every system of eigenvalues modulo l appears in the twists of W_k where $0 \leqslant k \leqslant 2l$ and we also know that each W_k has finitely many twists. Hence there exist finitely many systems of eigenvalues modulo l.

□

This theorem has a nice corollary on the finiteness of the congruence classes of the normalized eigenforms mod l. For the corollary, we need the following two lemmas.

Lemma 5.1.8. *For a given sequence $\{\lambda_p \in \bar{\mathbb{F}}_l : p \text{ is a prime}\}$ where p is not necessarily different from l, there are only finitely many normalized eigenforms $f = \sum_{n \geqslant 0} a_n q^n$ such that $a_p \equiv \lambda_p \pmod{l}$, for all primes p.*

Proof. Recall from Definition 3.1.5 that the Hecke operator T_{p^r} is defined by the following formula:

$$T_{p^r} := T_p T_{p^{r-1}} - p^{k-1} T_{p^{r-2}}$$

and the n-th Hecke operator is defined by the product of $T_{p_i^{e_i}}$'s. So we have:

$$a_{p^r} = a_p a_{p^{r-1}} - p^{k-1} a_{p^{r-2}}$$

Each $a_{p^r} \pmod{l}$ is determined by a_1 which is 1 in this case because f is normalized, a_p which is λ_p modulo l, r and congruence class of $p^{k-1} \pmod{l}$, and hence by the congruence class of $k \pmod{(l-1)}$. Then for fixed r, the set $\{a_{p^r} : r \geqslant 0\}$ is completely determined by the eigensystem and by $k \pmod{l-1}$. For a fixed integer $n = p_1^{e_1} p_2^{e_2} ... p_m^{e_m}$, the coefficient a_n is completely determined by the eigensystem and by $k \pmod{l-1}$. Consequently, there are only finitely many normalized eigenforms $f = \sum_{n \geqslant 0} a_n q^n$ such that $a_p \equiv \lambda_p \pmod{l}$, for all primes p.

□

Lemma 5.1.9. *Let $k > l+1$, then $U(W_k) = 0$.*

Proof. Let $k > l+1$ and let $f \in W_k$. By Proposition 4.3.10, we have

$$w(Uf) \leqslant \frac{w(f) + l^2 - 1}{l} < l + 1 < k.$$

Hence, we have $Uf = 0$.

□

Corollary 5.1.10. *There are only finitely many congruence classes of normalized eigenforms mod l for fixed level N.*

Proof. Let $\underline{\lambda} = \{\lambda_p : l \nmid p\}$ be a system of eigenvalues mod l. Let $f \in \tilde{\mathcal{M}}(\Gamma) \otimes \bar{\mathbb{F}}_l$ be a normalized eigenform with q-expansion $\sum_{n \geqslant 0} a_n q^n$ that gives the system $\underline{\lambda}$. Since $a_p \equiv \lambda_p \pmod{l}$ when $p \neq l$, the set of sequences $\{a_p(f) \pmod{l} : p \neq l\}$ is finite because there exist finitely many systems of eigenvalues by Theorem 5.1.7.

The operators U and T_l are equal modulo l and if $w(f) > l+1$, then $U(f) = 0$ by Lemma 5.1.9, and hence $a_l(f) \equiv 0 \pmod{l}$. If $w(f) \leqslant l+1$, then f appears in a space of modular form of weight at most $l+1$. Since each space of modular forms has finite dimension, there are finitely many possibilities for $a_l(f)$ since it is the eigenvalue of the operator U.

Hence, there exist only finitely many congruence classes of eigenforms modulo l by Lemma 5.1.8.

□

Example 5.1.11. Let $l = 5$ and the level $N = 1$. We will try to find all systems of eigenvalues. Every system of eigenvalues appears up to twist in weight at most $2l = 10$. In $\mathcal{M}_0$, there are only constant modular forms and in $\mathcal{M}_2$ there are no non-zero modular forms. The space $\mathcal{M}_4$ is generated by E_4 and $\mathcal{M}_8$ is generated by E_4^2. We know that $E_4 \equiv 1 \pmod 5$ by Theorem 4.1.4. Therefore $\tilde{\mathcal{M}}_4$ and $\tilde{\mathcal{M}}_8$ contain only constant modular forms. The space $\tilde{\mathcal{M}}_6$ is generated by $\tilde{E}_6$. Moreover, the space $\mathcal{M}_{10}$ is generated by the Eisenstein series E_{10} and it is equal to E_4E_6 by Example 2.4.12. Then $\tilde{\mathcal{M}}_{10}$ is also generated by $\tilde{E}_6$. Hence there are up to twist only the systems of eigenvalues coming from the weight 6. Every system of eigenvalues coming from the twists $\theta^a(G_6)$ where $0 \leqslant a \leqslant 3$.

$$a_p(G_6) = 1 + p^5 \equiv 1 + p \pmod 5$$
$$a_p(\theta G_6) \equiv p + p^2 \pmod 5$$
$$a_p(\theta^2 G_6) \equiv p^2 + p^3 \pmod 5$$
$$a_p(\theta^3 G_6) \equiv p^3 + p^4 \equiv p^3 + 1 \pmod 5$$

So these are only 4 systems of eigenvalues that appear in modulo 5.

Example 5.1.12. Let $l = 7$ and the level $N = 1$. We use the same idea as in the previous example. We're only checking up to the weight 14. Again, the space $\mathcal{M}_0$ contains only constant modular forms and in the space $\mathcal{M}_2$ there is only zero. Since $E_6 \equiv 1 \pmod 7$, the space $\tilde{\mathcal{M}}_6$ also consist of constant modular forms. We know that $\tilde{\mathcal{M}}_4$ is generated by $\tilde{E}_4$ and the space $\tilde{\mathcal{M}}_{10}$ is also generated by $\tilde{E}_4$ because $E_{10} = E_4E_6 \equiv E_4 \pmod 7$. There are the systems of eigenvalues coming from G_4.

$$a_p(G_4) = 1 + p^3$$
$$a_p(\theta G_4) \equiv p + p^4 \pmod 7$$
$$a_p(\theta^2 G_4) \equiv p^2 + p^5 \pmod 7$$
$$a_p(\theta^3 G_4) \equiv p^3 + p^6 \equiv 1 + p^3 \equiv a_p(G_4) \pmod 7$$

We also know that $\tilde{\mathcal{M}}_8$ is generated by $\tilde{E}_8$. Additionally, the space $\tilde{\mathcal{M}}_{14}$ is generated by $\tilde{E}_8$ because $E_{14} = E_8E_6 \equiv E_8 \pmod 7$. So we have the systems of eigenvalues

coming from G_8.

$$a_p(G_8) = 1 + p^7 \equiv 1 + p \pmod 7$$
$$a_p(\theta G_8) \equiv p + p^2 \pmod 7$$
$$a_p(\theta^2 G_8) \equiv p^2 + p^3 \pmod 7$$
$$a_p(\theta^3 G_8) \equiv p^3 + p^4 \pmod 7$$
$$a_p(\theta^4 G_8) \equiv p^4 + p^5 \pmod 7$$
$$a_p(\theta^5 G_8) \equiv p^5 + p^6 \equiv 1 + p^5 \pmod 7$$

The space of modular forms $\mathcal{M}_{12}$ is generated by E_{12} and Δ. We calculated on *SAGE*:

$$E_{12} = E_6^2 + \frac{762048}{691}\Delta \equiv 1 \pmod 7$$

and hence the only new eigensystem coming from $\mathcal{M}_{12}$ is the system of eigenvalues coming from $\Delta = \sum_{n \geqslant 1} \tau(n) q^n$ where τ is the Ramanujan tau function.

Since $E_{10} = E_4 E_6$, we have $w(E_{10}) = 4$. Then $w(\theta E_{10}) = 4 + 7 + 1 = 12$ by Theorem 4.3.4. So $\theta(E_{10})$ can be written as a linear combination of E_{12} and Δ.

$$\theta(E_{10}) = \lambda E_{12} + \beta\Delta \equiv \lambda + \beta\Delta \pmod 7$$

since $\theta(E_{10})$ and Δ have no constant coefficient $\lambda = 0$. The Eisenstein series E_{10} has the q-expansion $1+2q+4q^2+...$ modulo 7. Then we have $\theta(E_{10}) \equiv 2q+8q^2+... \equiv 2\Delta \pmod 7$. This means that $\theta(G_{10}) \equiv \Delta \pmod 7$. Therefore

$$\tau(n) \equiv n\sigma_9(n) \pmod 7$$

Here we showed that $\tilde{\Delta}$ is a twist of the Eisenstein series $\tilde{G}_{10}$. We already found that the eigenvalues with respect to E_{10} come from the system of eigenvalues of the Eisenstein series G_4. So there are exactly 9 systems of eigenvalues appear in modulo 7.

Chapter 6

SERRE'S l-ADIC MODULAR FORMS

In the previous chapters, we talked about the reductions of modular forms modulo prime l. Now we will introduce the l-adic modular forms with level $N = 1$ and we are following [Serre, 1973b]. Throughout this chapter l is a prime.

6.1 Congruences modulo l^m

In the Chapter 4, we talked about the congruences modulo l satisfied by the Eisenstein series. Now, it is natural to examine the congruences of Eisenstein series modulo l^m where m is a positive integer.

Proposition 6.1.1. *Let m be a positive integer. Then we have $E_k - 1 \in l^m\mathbb{Z}_l[\![q]\!]$ if and only if $(l-1)l^{m-1}$ divides the weight k when $l > 2$ and l^{m-2} divides k when $l = 2$.*

Proof. Let $(l-1)l^{m-1}$ divides the weight k and $l > 2$. Since $(l-1) \mid k$, we have $v_l\left(\frac{B_k}{k}\right) < 0$ by Theorem 4.1.2. So $v_l\left(\frac{2k}{B_k}\right) > 0$ and we also know that $l^{m-1} \mid k$. Therefore $v_l\left(\frac{2k}{B_k}\right) \geqslant m$. If $l = 2$ and $l^{m-2} \mid k$, then $v_l\left(\frac{k}{B_k}\right) \geqslant m-1$. So we have $v_l\left(\frac{2k}{B_k}\right) \geqslant m$. Hence $E_k - 1 \in l^m\mathbb{Z}_l[\![q]\!]$.

For the other direction of the proof, suppose that $E_k - 1 \in l^m\mathbb{Z}_l[\![q]\!]$. This implies that $E_k - 1 \in l\mathbb{Z}_l[\![q]\!]$ and $(l-1) \mid k$ by Theorem 4.1.4. Since $E_k - 1 \in l^m\mathbb{Z}_l[\![q]\!]$, the valuation $v_l\left(\frac{k}{B_k}\right) \geqslant m$ when $l > 2$ and $v_l\left(\frac{k}{B_k}\right) \geqslant m-1$ when $l = 2$. Since $(l-1)$ divides k, we know that $v_l(B_k) = -1$. If we combine these two results, we get $v_l(k) \geqslant m-1$ when $l > 2$ and we have $v_l(k) \geqslant m-2$ when $l = 2$. Therefore we have the result.

□

Theorem 6.1.2. *Let $m \geqslant 1$. Let $f \in \mathcal{M}_k(SL_2(\mathbb{Z}), \mathbb{Q})$ which is non-zero and $f' \in \mathcal{M}_{k'}(SL_2(\mathbb{Z}), \mathbb{Q})$. Suppose that*

$$v_l(f - f') \geqslant v_l(f) + m.$$

Then we have the following congruences between the weights k and k':

$$k \equiv k' \pmod{(l-1)l^{m-1}} \qquad \text{if} \quad l > 2$$

$$k \equiv k' \pmod{l^{m-2}} \qquad \text{if} \quad l = 2$$

Proof. The existence of the integral basis implies that the coefficients of f have valuations bounded from below (for the existence, see [Kilford, 2008]). Therefore, without loss of generality, we can assume that $v_l(f) = 0$. Then we have

$$v_l(f - f') \geqslant m.$$

This means that $f - f' \equiv 0 \pmod{l^m}$. Then reducing modulo l we have $\tilde{f} = \tilde{f'}$. This means that there exists $\alpha \in \mathbb{Z}/(l-1)\mathbb{Z}$ such that $f, f' \in \tilde{\mathcal{M}}^\alpha$. Therefore we have $k \equiv k' \pmod{(l-1)}$. This means we have the result when $m = 1$.

Now, we will show the result for $m > 1$ and $l \geqslant 5$. Let $h := k' - k$. To finish the proof we need to show that $l^{m-1} \mid h$. The modular forms f' and $f'E_{l^n(l-1)}$ have the same q-expansion by reduction modulo l. Hence we can replace f' by $f'E_{l^n(l-1)}$ for some n positive integer to get $h > 2$. In this way, we have the Eisenstein series of weight h, E_h. Since $h \equiv 0 \pmod{(l-1)}$, we have $E_h - 1 \equiv 0 \pmod{l}$ by Proposition 6.1.1. Let us define $r := v_l(h) + 1$. If we show that $r \geqslant m$, we would have $v_l(h) \geqslant m - 1$ and this means that $l^{m-1} \mid h$ so we would be done.

Assume that $m > r$. By hypothesis, we know that $f - f' \equiv 0 \pmod{l^m}$. Therefore $f - f' \equiv 0 \pmod{l^r}$. We also know that $h \equiv 0 \pmod{(l-1)l^{r-1}}$ and hence $E_h - 1 \equiv 0 \pmod{l^r}$ by Proposition 6.1.1. Therefore we have the following equality:

$$fE_h - f' = f - f' + f(E_h - 1) \equiv 0 \pmod{l^r}.$$

Then we have

$$l^{-r}(fE_h - f') \equiv l^{-r} f(E_h - 1) \pmod{l}.$$

Then by Theorem 4.1.2, we have $v_l(B_h) = -1$. So we have:

$$v_l\left(l^{-r}\frac{2h}{B_h}\right) = v_l(l^{-r}) + v_l(2h) - v_l(B_h) = 0.$$

Therefore, we have the following:

$$l^{-r}(E_h - 1) = t\varphi$$

where $gcd(t, l) = 1$ and $\varphi = \sum_{n\geqslant 1} \sigma_{h-1}(n)q^n$. Then we have

$$f\varphi = (tl^r)^{-1} f(E_h - 1) \equiv (tl^r)^{-1}(fE_h - f') \pmod{l}.$$

We have

$$\begin{aligned}
\varphi - \varphi^l &\equiv \sum_{l\nmid n} \sigma_{h-1}(n)q^n \pmod{l} \\
&\equiv \theta^{h-1}\left(\sum_{n\geqslant 1}\sigma_1(n)q^n\right) \pmod{l} \\
&\equiv \theta^{h-1}\left(-\frac{\tilde{E}_2}{24}\right) \\
&\equiv -\frac{\theta^{p-2}(\tilde{E}_2)}{24}.
\end{aligned}$$

Then if we look at their filtration we have

$$w(\tilde{\varphi} - \tilde{\varphi}^l) = w\left(-\frac{\theta^{l-2}(\tilde{E}_2)}{24}\right).$$

This means that $w(\tilde{\varphi}^l) = w(\theta^{l-2}(\tilde{E}_{l+1}))$ since $E_2 \equiv E_{l+1} \pmod{l}$ by Theorem 4.1.3. We know that $w(\tilde{\varphi}^l) = lw(\tilde{\varphi})$ by [Katz, 1977]. We also know that $w(E_{l+1}) = l + 1$ by example 4.2.7. Then $w(\theta^{l-2}(\tilde{E}_{l+1})) = (l-1)(l+1)$ by Theorem 4.3.4. Therefore $lw(\tilde{\varphi}) = l^2 - 1$ but this is a contradiction since $l^2 - 1$ is not divisible by l. Hence $r \geqslant m$ and this means $l^{m-1} \mid h = k' - k$. Therefore $k' - k$ is divisible by $(l-1)l^{m-1}$.

For the case $l < 5$, see [Serre, 1973b].

□

6.2 l-adic Modular Forms

In this part, we will introduce l-adic modular forms which is constructed by Serre and we will describe some of its properties. Then we will give an example of Serre's l-adic modular forms which is l-adic Eisenstein series.

Definition 6.2.1. Let $f \in \mathbb{Q}_l[\![q]\!]$ with $f = \sum_{n=0}^{\infty} a_n q^n$. We define the l-adic valuation on the formal power series by

$$v_l(f) = \inf v_l(a_n).$$

In order to define the l-adic modular forms, we introduce the following group which will be the group of weights of l-adic modular forms.

Definition 6.2.2. The group X is defined by the inverse limit $X = \varprojlim X_m$ where $X_m = \mathbb{Z}/l^{m-1}\mathbb{Z} \times \mathbb{Z}/(l-1)\mathbb{Z}$ when $l > 2$ and $X_m = \mathbb{Z}/2^{m-2}\mathbb{Z}$ when $l = 2$. Therefore

$$X \cong \mathbb{Z}_l \times \mathbb{Z}/(l-1)\mathbb{Z} \text{ when } l > 2$$

where $\mathbb{Z}_l$ is the set of l-adic integers and

$$X \cong \mathbb{Z}_2 \text{ when } l = 2.$$

Let $k \in X$. This k is called *even* if it lies in $2X$.

Definition 6.2.3. Let $f \in \mathbb{Q}_l[\![q]\!]$. This power series f is called an l-adic modular form if there exists a sequence of modular forms $f_i \in \mathcal{M}_{k_i}(SL_2(\mathbb{Z}, \mathbb{Q}))$ which converges to f in the sense that $\lim_{i\to\infty} v_l(f - f_i) = +\infty$.

Proposition 6.2.4. *Let f_i be a sequence of modular forms with rational coefficients, of weight k_i which converges to an l-adic modular form f. Then the sequence of weights k_i converges to some $k \in X$.*

Proof. If the sequence $\{f_i\}$ converges, this means that $v_l(f - f_i)$ goes to $+\infty$ when $i \to +\infty$. So there exist N such that $v_l(f_i - f_j) \geqslant m$ for all $i, j \geqslant N$. Therefore $k_i \equiv k_j \pmod{(l-1)l^{m-1}}$ by Theorem 6.1.2. Then the image of k_i is eventually constant in X_m for every m. So the limit k of the sequence $\{k_i\}$ exists in X.

□

This $k \in X$ is called the weight of the l-adic modular form f. Furthermore, this weight k always lies in $2X$. Therefore the weight of an l-adic modular form is also even.

Recall that we showed in Theorem 6.1.2 that: if $f \in \mathcal{M}_k(SL_2(\mathbb{Z}), \mathbb{Q})$ is non-zero and $f' \in \mathcal{M}_{k'}(SL_2(\mathbb{Z}), \mathbb{Q})$ with $v_l(f - f') \geqslant v_l(f) + m$ for $m \geqslant 1$, then $k \equiv k' \pmod{(l-1)l^{m-1}}$. Actually the same is true also for l-adic modular forms.

Lemma 6.2.5. *Let $\{f_i\}$ be a Cauchy sequence in $\mathbb{Q}_l[\![q]\!]$. If $\lim_{i \to +\infty} |f_i|_l \neq 0$, then $v_l(f_i) = v_l(f)$ for $i \gg 0$.*

Proof. Since $\lim_{i \to +\infty} |f_i|_l \neq 0$, there exists $\varepsilon = l^{-r} > 0$ and $N \in \mathbb{N}$ such that $|f_i|_l \geqslant \varepsilon$ if $i \geqslant N$. This means that $v_l(f_i) = \inf\{v_l(a_{n,i})\} \leqslant r$. Since $\{f_i\}$ is a Cauchy sequence there exists N' such that $|f_m - f_{m'}|_l < \varepsilon$ if $m, m' \geqslant N'$ and it means that $v_l(f_m - f_{m'}) = \inf\{v_l(a_{n,m} - a_{n,m'})\} > r$. Then we choose $\tilde{N} = \max\{N, N'\}$, for $m, m' \geqslant \tilde{N}$

$$\begin{aligned} v_l(f_m) &= v_l(f_m - f_{m'} + f_{m'}) \\ &\geqslant \min\{v_l(f_m - f_{m'}), v_l(f_{m'})\} \\ &= v_l(f_{m'}) \end{aligned}$$

By symmetry, we have $v_l(f_m) \leqslant v_l(f_{m'})$ and hence $v_l(f_m) = v_l(f_{m'})$. Thus $v_l(f_i) = v_l(f)$ for $i \geqslant \tilde{N}$.

□

Proposition 6.2.6. *Let $m \geqslant 1$ and let f and f' be nonzero l-adic modular forms with weights k and k'. Suppose that $v_l(f - f') \geqslant v_l(f) + m$. Then*

$$k \equiv k' \pmod{(l-1)l^{m-1}} \qquad \text{if} \quad l > 2$$

$$k \equiv k' \pmod{l^{m-2}} \qquad \text{if} \quad l = 2$$

and this means that $k - k'$ is zero in X_m.

Proof. The statement is clear if $f = f'$. Suppose that f, f' are distinct. By definition of l-adic modular forms, there exist a sequence of modular forms f_i of weights k_i which converges to f and a sequence of modular forms f_i' of weights k_i' which converges to f'. Since f and f' are nonzero, by the previous lemma we have $v_l(f) = v_l(f_i)$ and $v_l(f - f') = v_l(f_i - f_i')$ for i big enough.

Thus

$$v_l(f - f') = v_l(f_i - f_i') \geqslant v_l(f_i) + m = v_l(f) + m$$

as $i \to \infty$. Then $k_i \equiv k_i' \pmod{(l-1)l^{m-1}}$ when $l > 2$ and $k_i \equiv k_i' \pmod{l^{m-2}}$ when $l = 2$ by Theorem 6.1.2. Therefore

$$k \equiv k' \pmod{(l-1)l^{m-1}} \qquad \text{if} \quad l > 2$$

$$k \equiv k' \pmod{l^{m-2}} \qquad \text{if} \quad l = 2$$

and hence $k - k' = 0 \in X_m$.

□

Corollary 6.2.7. *Let f be an l-adic modular form of weight k with q-expansion $\sum_{n\geqslant 0} a_n q^n$. Suppose that $m \geqslant 0$ and $k \pmod{(l-1)l^m}$ is nonzero. Then*

$$v_l(a_0) + m \geqslant v_l\left(\sum_{n\geqslant 1} a_n q^n\right).$$

Proof. Let $f' = a_0$. If $a_0 = 0$, we have $v_l(a_0) = +\infty$ and we have the result. Suppose that a_0 is nonzero. Then f' has weight zero. We assumed that $k \not\equiv 0 \pmod{(l-1)l^m}$. Then $v_l(f - f') < v_l(f) + m + 1$ by Proposition 6.2.6. This means $v_l\left(\sum_{n\geqslant 1} a_n q^n\right) < v_l(f) + m + 1$. Therefore we have

$$v_l\left(\sum_{n\geqslant 1} a_n q^n\right) \leqslant v_l(f) + m.$$

Since we defined $v_l(f) = \inf v_l(a_n)$, we have the result:

$$v_l\left(\sum_{n\geqslant 1} a_n q^n\right) \leqslant v_l(a_0) + m.$$

□

Corollary 6.2.8. *Let f_i's be l-adic modular forms of weight k_i which have q-expansions $f_i = \sum_{n\geqslant 0} a_{n,i} q^n$. Suppose that the following hold:*

- *For each $n \geqslant 1$, there are $a_n \in \mathbb{Q}_l$ such that $a_{n,i}$ converges uniformly to a_n as $i \to +\infty$.*

- *The sequence of weights $\{k_i\}$ converges to nonzero k in the group X.*

Then the sequence of the constant terms $a_{0,i}$ converges to a_0. Furthermore, the sequence f_i converges to an l-adic modular form f whose q-expansion is $\sum_{n\geqslant 0} a_n q^n$ and which has weight k.

Proof. Since we assumed k is nonzero, then we can choose an $m \geqslant 1$ such that k is nonzero in X_m. The sequence $a_{n,i}$ converges as $i \to +\infty$ uniformly to a_n for each $n \geqslant 1$, then $|a_{n,i}|_l$ uniformly converges to $|a_n|_l$. This implies that $|a_{n,i}|_l$ is uniformly bounded. Then we can choose $r \in \mathbb{Z}$ such that there exists $N_r \in \mathbb{N}$

$$v_l(a_{n,i}) \geqslant r$$

for all $n \geqslant 1$ and $i \geqslant N_r$.

By the previous corollary, we

$$v_l(a_{0,i}) + m \geqslant v_l\left(\sum_{n\geqslant 1} a_{n,i} q^n\right) = \inf v_l(a_{n,i}) \geqslant r$$

for all $n \geqslant 1$ and $i \geqslant N_r$.

So

$$v_l(a_{0,i}) \geqslant r - m$$

This means that $l^{r-m} \mid a_{0,i}$. Therefore $a_{0,i} \in l^{r-m}\mathbb{Z}_l$. The space $\mathbb{Z}_l$ is compact and since it is a metric space it is also sequentially compact. Let $\{a_{0,i_j}\}$ be a subsequence of $\{a_{0,i}\}$ which converges to a_0 and $\{a_{0,i_h}\}$ be a subsequence of $\{a_{0,i}\}$ which converges to $\tilde{a}_0$. Then these two limits give the following two l-adic modular forms of weight k:

$$f = a_0 + \sum_{n\geqslant 1} a_n q^n \qquad \text{and} \qquad \tilde{f} = \tilde{a}_0 + \sum_{n\geqslant 1} a_n q^n$$

Since these two have weight k, their difference $f - \tilde{f}$ also has weight k nonzero. But $f - \tilde{f} = a_0 - \tilde{a}_0$ has also zero weight. Therefore $a_0 - \tilde{a}_0 = 0$. So different subsequences have the same limit, and hence the sequence $a_{0,i}$ has the limit a_0. Therefore, we conclude $f_{n,i}$ converges to l-adic modular form $f = \sum_{n\geqslant 0} a_n q^n$.

□

6.3 l-adic Eisenstein Series

We know that the Eisenstein series of weight 2 is not a modular form in the classical theory of modular forms. But after defining l-adic Eisenstein series we will see that there exists l-adic Eisenstein series of weight 2.

Let k be an integer. We know that $\sigma_k(n) = \sum_{d|n} d^k$. Let $k \in X$ and n be a non-negative integer. If l does not divide d, then d is contained in $\mathbb{Z}_l^\times$. Then we can define $\sigma_k^*(n)$ as follows:

$$\sigma_k^*(n) = \sum_{\substack{d|n \\ (l,d)=1}} d^k.$$

In order to make sense of this definition, we need to define the term d^k:

Since d is in $\mathbb{Z}_l^\times$, we can write it as $d = d_1 d_2$ where d_1 is a $(l-1)$st root of unity and $d_2 \equiv 1 \pmod{l}$. Let $k \in X$ such that $k = (m_1, m_2) \in \mathbb{Z}_l \times \mathbb{Z}/(l-1)\mathbb{Z}$. Then

$$d^k := d_1^{m_2} d_2^{m_1}$$

Now, we will show that the term $d_2^{m_1}$ is well-defined. Let $z = 1 + la \in 1 + l\mathbb{Z}_l$ and $\tau \in \mathbb{Z}_l$ such that $\tau = \sum_{i \geqslant 0} a_i l^i$ where $0 \leqslant a_i \leqslant (l-1)$. Let $\tau_j = \sum_{i=0}^{j} a_i l^i$. Then

$$\begin{aligned} v_l(z^{\tau_h} - z^{\tau_j}) &\geqslant v_l(la) + v_l(\tau_h - \tau_j) \\ &= 1 + v_l(a) + v_l(a_{j+1} l^{j+1} + a_{j+2} l^{j+2} + ... + a_h l^h) \end{aligned}$$

This means that z^{τ_j} converges to z^τ. Therefore raising to an l-adic power can be defined by this limit:

$$z^\tau := \lim_{j \to +\infty} z^{a_o + a_1 l + ... + a_j l^j}$$

Let $k_i \geqslant 4$ be a sequence which converges to k in X in the sense of l-adic topology and $|k_i|$ goes to $+\infty$ in the usual sense. Since k_i converges to k in X:

$$d^{k_i - 1} \to d^{k-1} \text{ as } i \to +\infty, \text{ if } l \nmid d$$

Since $|k_i| \to +\infty$:

$$d^{k_i - 1} \to 0 \text{ as } i \to +\infty, \text{ if } l \mid d$$

Therefore we have:

$$\sigma_{k_i-1}(n) \to \sigma^*_{k-1}(n)$$

as $i \to +\infty$. Now, we will show that this convergence is also uniform in n.

$$\begin{aligned}\left|\sigma_{k_i-1}(n) - \sigma^*_{k-1}(n)\right|_l &= \left|\sum_{l|d} d^{k_i-1} + \sum_{l\nmid d} d^{k_i-1} - \sum_{l\nmid d} d^{k-1}\right|_l \\ &\leqslant \max\left\{\left|\sum_{l|d} d^{k_i-1}\right|_l, \left|\sum_{l\nmid d}(d^{k_i-1} - d^{k-1})\right|_l\right\}\end{aligned}$$

We have

$$\left|\sum_{l|d} d^{k_i-1}\right|_l \leqslant \max\left\{\left|d^{k_i-1}\right|_l : d \mid n, l \mid d\right\} \leqslant l^{1-k_i}$$

We also have

$$\begin{aligned}\left|\sum_{l\nmid d}(d^{k_i-1} - d^{k-1})\right|_l &\leqslant \max\left\{\left|d^{k_i-1} - d^{k-1}\right|_l : d \mid n, l \nmid d\right\} \\ &\leqslant \max\left\{\left|d_1^{k_i-1}d_2^{k_i-1} - d_1^{m_2-1}d_2^{m_1-1}\right|_l : d \mid n, l \nmid d\right\} \\ \text{since } k \equiv k_i \pmod{(l-1)l^{m-1}} &\text{ then } m_2 \equiv k_i \pmod{(l-1)} \\ &\leqslant l^{-v_l(d_2^{k_i-1} - d_2^{m_1-1})} \\ &\leqslant l^{-v_l(m_1-k_i)}\end{aligned}$$

Thus

$$\left|\sigma_{k_i-1}(n) - \sigma^*_{k-1}(n)\right|_l \leqslant \max\{l^{1-k_i}, l^{-v_l(m_1-k_i)}\}$$

Hence we have an upper bound which does not depend on n. Therefore it converges uniformly.

Recall that

$$G_k := -\frac{B_k}{2k} + \sum_{n\geqslant 1}\sigma_{k-1}(n)q^n$$

Let G_{k_i} be the Eisenstein series of weight k_i. We know $a_{n,i} = \sigma_{k_i-1}(n)$ converges uniformly to $a_n = \sigma^*_{k-1}(n)$ for each $n \geqslant 1$ and the weights k_i converges to k in X. Therefore, by Corollary 6.2.8, the sequence of Eisenstein series G_{k_i} has a limit G^*_k which is an l-adic modular form whose q-expansion is

$$G^*_k = \lim_{i\to+\infty} -\frac{B_{k_i}}{2k_i} + \sum_{n\geqslant 1}\sigma^*_{k-1}(n)q^n$$

We need to show that there exists a sequence of $k_i \geqslant 4$ which converges to $2 \in X$. Then we can conclude that there exists l-adic Eisenstein series of weight 2. Let

$$k_i = 2 + (l-1)l^i$$

Then for m big enough we have:

$$k_i \equiv 2 \pmod{(l-1)l^{m-1}}$$

So k_i converges to 2 in X as $i \to +\infty$ and $|k_i| \to +\infty$ in the usual sense. Therefore we have the l-adic Eisenstein series of weight 2:

$$G_2^* = \lim_{i \to +\infty} -\frac{B_{k_i}}{2k_i} + \sum_{n \geqslant 1} \sigma_1^*(n) q^n$$

6.4 Modular forms with respect to $\Gamma_0(l)$

In this part of the chapter, we will show that if f is a classical modular form with rational coefficients with respect to $\Gamma_0(l)$, then it is also an l-adic modular form.

First we define the trace of a modular form.

Definition 6.4.1. Let f be a modular form with respect to $\Gamma_0(l)$. Let γ_i where $i \in \{1, ..., l+1\}$ be coset representatives of $\Gamma_0(l)$ in $SL_2(\mathbb{Z})$. Then the *trace of* f is defined by:

$$Tr : \mathcal{M}_k(\Gamma_0(l)) \to \mathcal{M}_k(SL_2(\mathbb{Z}))$$
$$Tr(f) = \sum_{i=1}^{l+1} f|_k \gamma_i$$

Notice that this definition comes from the double coset definition in Definition 3.0.3. Let $\Gamma_1 = \Gamma_0(l)$, $\Gamma_2 = SL_2(\mathbb{Z})$ and α be the identity matrix I, then we get this trace map.

Let $W = \begin{bmatrix} 0 & 1 \\ -l & 0 \end{bmatrix}$. Then $W^2 = \begin{bmatrix} -l & 0 \\ 0 & -l \end{bmatrix}$. Recall that we defined the slash k operator by:

$$f \mid_k \gamma(z) = (\det \gamma)^{\frac{k}{2}} (cz + d)^{-k} f(\gamma z).$$

Therefore we have:

$$\begin{aligned} f \mid_k W^2(z) &= (\det W^2)^{\frac{k}{2}}(0z - l)^{-k} f(W^2 z) \\ &= (-1)^{-k} f(z) = f(z). \end{aligned}$$

Let f be a modular form with respect to $\Gamma_0(l)$ and $\gamma = \begin{bmatrix} a & b \\ ln & d \end{bmatrix} \in \Gamma_0(l)$. Then

$$W\gamma W^{-1} = \begin{bmatrix} 0 & 1 \\ -l & 0 \end{bmatrix} \begin{bmatrix} a & b \\ ln & d \end{bmatrix} \begin{bmatrix} 0 & \frac{1}{l} \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} d & -n \\ -lb & a \end{bmatrix} \in \Gamma_0(l).$$

Since we said $f \in \mathcal{M}_k(\Gamma_0(l))$,

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

Then we have

$$(f \mid_k W) \mid_k \gamma = f \mid_k W$$

and hence $f \mid_k W$ is also a modular form with respect to $\Gamma_0(l)$.

Lemma 6.4.2. *Suppose that f is a modular form with respect to $\Gamma_0(l)$. Then we have the following formula:*

$$Tr(f) = f + l^{1-\frac{k}{2}} U(f \mid_k W)$$

where U is the operator defined in Definition 4.3.1.

Proof. We know that $[SL_2(\mathbb{Z}) : \Gamma_0(l)] = l + 1$ by Proposition 2.1.4. Let the coset representatives of $\Gamma_0(l)$ in $SL_2(\mathbb{Z})$ be:

$$\gamma_{l+1} = I$$

and if $j \in \{1, ..., l\}$

$$\gamma_j = \begin{bmatrix} 0 & -1 \\ 1 & j \end{bmatrix}.$$

Let $\beta_j = \begin{bmatrix} \frac{1}{l} & \frac{j}{l} \\ 0 & 1 \end{bmatrix}$. Then we have

$$\begin{bmatrix} 0 & -1 \\ l & 0 \end{bmatrix} \begin{bmatrix} \frac{1}{l} & \frac{j}{l} \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & -1 \\ 1 & j \end{bmatrix}.$$

This means that we can write each $\gamma_j = W\beta_j$. Then

$$\begin{aligned} Tr(f) = \sum_{j=1}^{l+1} f|_k\gamma_j &= f + \sum_{j=1}^{l} f|_k\gamma_i \\ &= f + \sum_{j=1}^{l} f|_k W\beta_j \\ &= f + \sum_{j=1}^{l} (f|_k W)|_k\beta_j \\ &= f + \sum_{j=1}^{l} \left(\frac{1}{l}\right)^{\frac{k}{2}} l^{-k} f|_k W\left(\frac{z+j}{l}\right) \\ &= f + l^{-\frac{k}{2}} \sum_{j=1}^{l} f|_k W\left(\frac{z+j}{l}\right). \end{aligned}$$

Since $f|_k W$ is a modular form, it has a q-expansion, say $f|_k W(z) = \sum_{n\geqslant 0} a_n q^n$ where $q = e^{2\pi i z}$. Then

$$\begin{aligned} \sum_{j=1}^{l} f\ |_k\ W\left(\frac{z+j}{l}\right) &= \sum_{j=1}^{l}\sum_{n\geqslant 0} a_n e^{2\pi n i\frac{z+j}{l}} \\ &= \sum_{n\geqslant 0} a_n \sum_{j=1}^{l} e^{\frac{2\pi n i(z+j)}{l}} \\ &= \sum_{n\geqslant 0} a_n e^{\frac{2\pi n i z}{l}} \sum_{j=1}^{l} e^{\frac{2\pi n i j}{l}} \end{aligned}$$

and

$$\begin{aligned} \sum_{j=1}^{l} e^{\frac{2\pi n i j}{l}} &= \sum_{j=1}^{l} \left(e^{\frac{2\pi n i}{l}}\right)^j \\ &= \frac{1-(e^{\frac{2\pi n i}{l}})^l}{1-e^{\frac{2\pi n i}{l}}} \\ &= \begin{cases} 0, & \text{if } l \nmid n \\ l, & \text{if } l \mid n. \end{cases} \end{aligned}$$

Then we have

$$\sum_{j=1}^{l} f\ |_k\ W\left(\frac{z+j}{l}\right) = l\sum_{n\geqslant 0} a_n e^{\frac{2\pi n i z}{l}} \text{ where } \ l \mid n.$$

This means

$$\sum_{j=1}^{l} f \mid_k W \left(\frac{z+j}{l} \right) = lU(f|_k W).$$

Hence, we have the result:

$$Tr(f) = f + l^{1-\frac{k}{2}} U(f \mid_k W).$$

□

In order to show that every modular form with rational coefficients with respect to $\Gamma_0(l)$ is also an l-adic modular form, we need the following the lemma.

Lemma 6.4.3. *Let $h \geqslant 4$ be an integer such that $(l-1) \mid h$ and let $g = E_h - l^{\frac{h}{2}} E_h|_h W$. Then $g \equiv 1 \pmod{l}$. Moreover, $g|_h W \equiv 0 \pmod{l^{1+\frac{h}{2}}}$.*

Proof. Since $(l-1) \mid h$, we have $E_h \equiv 1 \pmod{l}$ by Theorem 4.1.4. This implies that $g \equiv 1 \pmod{l}$.

The matrix W can be written as

$$W = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} l & 0 \\ 0 & 1 \end{bmatrix}.$$

Since $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \in SL_2(\mathbb{Z})$, we have

$$\begin{aligned} E_h \mid_h W &= E_h \mid_h \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} l & 0 \\ 0 & 1 \end{bmatrix} \\ &= \left(E_h \mid_h \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \right) \mid_h \begin{bmatrix} l & 0 \\ 0 & 1 \end{bmatrix} \\ &= E_h \mid_h \begin{bmatrix} l & 0 \\ 0 & 1 \end{bmatrix} \\ &= l^{\frac{h}{2}} E_h(lz) \\ &= l^{\frac{h}{2}} V(E_h) \end{aligned}$$

where V is the operator we defined in Definition 4.3.1. Therefore, we have:

$$\begin{aligned} g|_h W &= E_h|_h W - l^{\frac{h}{2}} E_h|_h W^2 \\ &= E_h|_h W - l^{\frac{h}{2}} E_h \\ &= l^{\frac{h}{2}} V(E_h) - l^{\frac{h}{2}} E_h \\ &= l^{\frac{h}{2}} (V(E_h) - E_h) \\ &\equiv 0 \pmod{l^{1+\frac{h}{2}}} \end{aligned}$$

because we showed $E_h \equiv 1 \pmod{l}$ and we also have $V(E_h) \equiv 1 \pmod{l}$, so $l|(V(E_h) - E_h)$. Hence we have $g|_h W \equiv 0 \pmod{l^{1+\frac{h}{2}}}$.

□

Theorem 6.4.4. *Let $f \in \mathcal{M}_k(\Gamma_0(l), \mathbb{Q})$. Then f is an l-adic modular form.*

Proof. In order to show that f is an l-adic modular form, we need to find a sequence of modular forms with rational coefficients $\{f_i\}$ which converges to f. So we need to show that $v_l(f_i - f) \to +\infty$ with $v_l(k_i - k) \to +\infty$ as $i \to +\infty$.

Let $f_i := Tr(fg^{l^i})$ where $g = E_h - l^{\frac{h}{2}} E_h|_h W$ as in the previous lemma. We know that $Tr(fg^{l^i}) \in \mathcal{M}_{k_i}(SL_2(\mathbb{Z}), \mathbb{Q})$ where $k_i := k + l^i h$, since f has weight k and g has weight h, the weight of f_i is $k_i = k + l^i h$. Then we have

$$\begin{aligned} v_l(f_i - f) &= v_l(Tr(fg^{l^i}) - f) \\ &= v_l(fg^{l^i} + l^{1-\frac{k_i}{2}} U(fg^{l^i}\ |_{k_i} W) - f) \\ &= v_l(f(g^{l^i} - 1) + l^{1-\frac{k_i}{2}} U(fg^{l^i}\ |_{k_i} W)) \\ &\geqslant \min\{v_l(f(g^{l^i} - 1)), v_l(l^{1-\frac{k_i}{2}} U(fg^{l^i}\ |_{k_i} W))\} \end{aligned}$$

Let us calculate $v_l(f(g^{l^i} - 1))$ and $v_l(l^{1-\frac{k_i}{2}} U(fg^{l^i}\ |_{k_i} W))$.

$$\begin{aligned} v_l(f(g^{l^i} - 1)) &= v_l(f) + v_l(g^{l^i} - 1) \\ &= v_l(f) + i + 1 \end{aligned}$$

because we showed in the previous lemma, $g \equiv 1 \pmod{l}$.

$$\begin{aligned} v_l(l^{1-\frac{k_i}{2}}U(fg^{l^i}\mid_{k_i} W)) &= 1 - \frac{k_i}{2} + v_l(U(fg^{l^i}\mid_{k_i} W)) \\ &\geqslant 1 - \frac{k_i}{2} + v_l(fg^{l^i}\mid_{k_i} W) \\ &= 1 - \frac{k_i}{2} + v_l((f\mid_k W)(g\mid_h W)^{l^i}) \\ &= 1 - \frac{k_i}{2} + v_l(f\mid_k W) + l^i v_l(g\mid_h W) \\ \text{Since } g|_h W \equiv 0 \pmod{l^{1+\frac{h}{2}}} \text{ we have} &= 1 - \frac{k}{2} - \frac{hl^i}{2} + v_l(f\mid_k W) + l^i\left(1+\frac{h}{2}\right) \\ &= 1 - \frac{k}{2} + v_l(f\mid_k W) + l^i \end{aligned}$$

Then

$$v_l(f_i - f) \geqslant \min\{v_l(f) + i + 1, 1 - \frac{k}{2} + v_l(f\mid_k W) + l^i\}$$

Therefore $v_l(f_i - f) \to +\infty$ as $i \to +\infty$. So this sequence $\{f_i\}$ converge to f. Since $k_i = k + hl^i$, the sequence $\{k_i\}$ converge to $k \in X$. Hence f is an l-adic modular form of weight k. □

Corollary 6.4.5. *Let $f \in \mathcal{M}_k(\Gamma_0(l), \mathbb{Z})$. Then there exists $f' \in \mathcal{M}_{k+i(l-1)}(SL_2(\mathbb{Z}), \mathbb{Z})$ such that $f \equiv f' \pmod{l}$ for i is big enough.*

Proof. Let $h = l - 1$. Then we have $g = E_{l-1} - l^{\frac{l-1}{2}}E_{l-1}|_{l-1}W$ as in Lemma 6.4.3. Let us choose $f' := f_i = Tr(fg^{l^i}) \in \mathcal{M}_{k+i(l-1)}(SL_2(\mathbb{Z}), \mathbb{Z})$ where i is big enough such that $v_l(f\mid_k W) + l^i \geqslant \frac{k}{2}$. Then as in the previous theorem we have,

$$v_l(f' - f) \geqslant \min\{v_l(f) + i + 1, 1 - \frac{k}{2} + v_l(f\mid_k W) + l^i\}$$

Since f has integer coefficients, $v_l(f) \geqslant 0$ and since we chose i so that $v_l(f\mid_k W) + l^i \geqslant \frac{k}{2}$, we have $1 - \frac{k}{2} + v_l(f\mid_k W) + l^i \geqslant 1$. Hence, we have $v_l(f' - f) \geqslant 1$. Therefore $f \equiv f' \pmod{l}$.

□

BIBLIOGRAPHY

[Borevich and Shafarevich, 1986] Borevich, Z. I. and Shafarevich, I. R. (1986). *Number theory*. Academic press.

[Busam and Freitag, 2009] Busam, R. and Freitag, E. (2009). *Complex analysis*. Springer.

[Diamond and Shurman, 2005] Diamond, F. and Shurman, J. M. (2005). *A first course in modular forms*, volume 228. Springer.

[Gouvêa, 1997] Gouvêa, F. Q. (1997). p-adic numbers. In *p-adic Numbers*, pages 43–85. Springer.

[Jochnowitz, 1982] Jochnowitz, N. (1982). Congruences between systems of eigenvalues of modular forms. *Transactions of the American Mathematical Society*, 270(1):269–285.

[Katz, 1973] Katz, N. M. (1973). P-adic properties of modular schemes and modular forms. In *Modular functions of one variable III*, pages 69–190. Springer.

[Katz, 1977] Katz, N. M. (1977). A result on modular forms in characteristic p. In *Modular functions of one variable V*, pages 53–61. Springer.

[Kilford, 2008] Kilford, L. J. P. (2008). *Modular Forms: A classical and computational introduction*. World Scientific.

[Lang, 2012] Lang, S. (2012). *Introduction to modular forms*, volume 222. Springer Science & Business Media.

[Miyake, 2006] Miyake, T. (2006). *Modular forms*. Springer Science & Business Media.

[Serre, 1973a] Serre, J.-P. (1973a). Congruences et formes modulaires. In *Séminaire Bourbaki vol. 1971/72 Exposés 400–417*, pages 319–338. Springer.

[Serre, 1973b] Serre, J.-P. (1973b). Formes modulaires et fonctions zêta p-adiques. In *Modular functions of one variable III*, pages 191–268. Springer.

[Serre, 1975] Serre, J.-P. (1975). Valeurs propres des opérateurs de hecke modulo . *Astérisque*, 24:109–117.

[Serre, 2012] Serre, J.-P. (2012). *A course in arithmetic*, volume 7. Springer Science & Business Media.

[Swinnerton-Dyer, 1973] Swinnerton-Dyer, H. P. F. (1973). On -adic representations and congruences for coefficients of modular forms. In *Modular functions of one variable III*, pages 1–55. Springer.