Sorbonne Université

Université du Luxembourg

On the Asymptotic Behavior of the Coefficient Field of Newforms Modulo p

Author: Breki Pálsson

Advisor: Gabor Wiese

September 16, 2023

Acknowledgements

Thank you to my supervisor, Professor Gabor Wiese, for your time, patience, enhuisiasm, kindness, interest in me and everything you have taught me. I would also like to thank the University of Luxembourg for providing me with a workspace and resources so that I could work on this thesis.

During my two years as a master's student in Paris, I have been financially and academically supported by the *Foundation sciences mathématiques de Paris* as a PGSM scholar. For that I am very grateful.

This endeavor would not have been possible without the support of my family and friends. Especially from Hrafnhildur, Arna, Sverrir, Kristín, Stefanía, Páll, Laufey, Valgerður, Vladimir, Elias, Lachlan and Andishe.

Lastly, I'd like to thank all the friends that I met in Paris and Luxembourg. Thank you to Paris, you've taught me a lot of mathematics and a lot about myself. I'll never forget this experience.

Contents

Introduction

This Master's thesis is the result of five months of work under the supervision of Professor Gabor Wiese. Calculations were made using the programming language Sagemath [14].

A consequence of the Eichler-Shimura theorem is the following Corollary.

Corollary

Let $f = \sum_{n=1}^{\infty} a_n(f)q^n \in S_k(\Gamma_1(N); \mathbb{C})$ be a normalized Hecke eigenform.
Then $\mathbb{Q}_f := \mathbb{Q}(a_n(f)|n \in \mathbb{N})$ is a number field of degree less than or equal to $\dim_{\mathbb{C}}(S_k(\Gamma_1(N, \mathbb{C})))$.

Rings of integers of number fields are Dedekind domains; thus, all their ideals factor uniquely into prime ideals. One of the main characteristics that can be studied is the residue degree of prime ideals. Which will give us information of the factorization of ideals.

Studying the residue degree of prime ideals in the coefficient fields of modular forms can for example give us insights into the inverse Galois problem and the generalized Maedas conjecture.

Now let $f \in S_k(N; \mathbb{C})$ be a cusp form of level N and weight k. There are $\mathbb{C}$ linear maps for $n \in \mathbb{N}, T_n : S_k(N) \to S_k(N)$, which commute. These maps are called Hecke operators. If we work with the *newspace*, a subset of the space of cuspforms. Then T_n is diagonalizable, and as the Hecke operators commute, the T_n are also simultaneously diagonalizable.

We can find common eigenvectors in $S_k(N; \mathbb{C})$ called *Hecke eigenforms*, that allow us to connect modular forms to algebraic objects called *modular symbols*, making calculations much easier using various results from algebra.

For reasonable N and k and $f \in S_k^{new}(N; \mathbb{C})$ a normalized Hecke eigenform, one can compute $\mathbb{Q}_f$ as a number field. We want to study how $\mathbb{Q}_f$ behaves as we vary N and k.

If we fix $N = 1$ and vary k, we can use Maeda's conjecture and some elementary methods to understand $\mathbb{Q}_f$ and quicky calculate the residue degree of prime ideals $\mathfrak{p}$ above a prime $p \in \mathbb{N}$.

However, for more general N, we need stronger methods. We introduce algorithms to calculate the residue degree of the local components of the *Hecke algebra* of modular symbols. Then we connect the residue degrees of the local components of the Hecke algebra to the residue degrees of prime ideals $\mathfrak{p}$ in $\mathbb{Q}_f$.

We calculated the maximal residue degree of the Hecke algebras that correspond to normalized eigenforms $f \in S_k(N; \mathbb{C})$ for prime levels N in order to get insights to the question.

Question: Is the maximal residue degree a_p, of primes above p in $\mathbb{Q}_f$ related to b_n, the average maximum length of a cycle in a permutation of $\mathcal{S}_n$?

In particular, we ask if

$$\lim_{N\to\infty} a_p(N)/dim(S_k(N;\mathbb{C})) \sim \lambda/2$$

where λ is the *Golomb-Dickman* constant. Our calculations dont aggree with the heuristic. Interestingly it seems to suggest that on avereage $a_p(N)/dim(S_k(N;\mathbb{C}))$ depends only on the weight k and not on p. Furthermore, we seem to notice numerical evedence that

$$\lim_{n\to\infty} \sum_{N=1}^{n} \frac{a_p(N)/dim(S_k(N;\mathbb{C}))}{n} \approx 13/k.$$

We also found some evedence of regularity in the asymptotic behavior of $a_p(N)/N$ that seems to be in the spirit of the generalized Maedas Conjecture.

Chapter 1

Background

We will briefly review the theory of modular forms, Hecke operators, the q-expansion principle and newforms. This section will mostly follow Wiese's text [6] on the computational arithmetic of modular forms and Miyake [13] for the part about newforms.

1.1 Brief Introduction to Modular Forms

Congruence Subgroups

Recall that a congruence subgroup is a subgroup of $SL_2(\mathbb{Z})$ that contains

$$\Gamma(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right) (\text{mod } N) \right\} \tag{1.1}$$

for some $N \in \mathbb{N}$. Although one can consider modular forms even for non-congruence subgroups, see for example [17], we will only consider the standard congruence subgroups of $SL_2(\mathbb{Z})$ mainly for a given integer N,

$$\Gamma_0(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) (\text{mod } N) \right\}, \tag{1.2}$$

$$\Gamma_1(N) := \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) (\text{mod } N) \right\}. \tag{1.3}$$

In particular, we will consider modular forms for $\Gamma_0(N)$ or $\Gamma_1(N)$ depending on whether we are working with a character or not.

Modular Forms

We will here recall the definitions of modular forms with a character. For a more standard introduction, see [15, Serre] or [3, Diamond]. First, we will fix some notations. We will denote by

$$\mathbb{H} := \{z \in \mathbb{C} | Im(z) > 0\}$$

the *Poincaré upper half plane*. The set of cusps is defined by $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$. The group $PSL_2(\mathbb{Z})$ acts on $\mathbb{H}$ by Möbius transforms. That is, for an $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ and $z \in \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$ one sets

$$M.z = \frac{az+b}{cz+d}. \tag{1.4}$$

And we extend this to include ∞ by defining $M.(-d/c) = \infty$ and $M.(\infty) = a/c$.

For $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, an integer matrix with non-zero determinant, an integer k and a function $f : \mathbb{H} \to \mathbb{C}$, we put

$$(f|_k M)(z) = (f|M)(z) := f(M.z)\frac{\det(M)^{k-1}}{(cz+d)^k}.$$

Definition 1.1.1

For fixed integers $k \geq 1$ and $N \geq 1$. A function $f : \mathbb{H} \to \mathbb{C}$ given by a convergent power series

$$f(z) = \sum_{n=0}^{\infty} a_n(f)(e^{2\pi iz})^n = \sum_{n=0}^{\infty} a_n(f)q^n \text{ with } q(z) = e^{2\pi iz}$$

is called a *modular form of weight* k for $\Gamma_1(N)$ if the following statements hold:

(i) $(f|_k M)(z) = f(M.z)(cz+d)^{-k} = f(z)$ for all $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(N)$.

(ii) The function $(f|_k M)(z) = f(M.z)(cz+d)^{-k}$ admits a limit when z tends to $i\infty$ for all $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$.

We denote the set of all modular forms of weight k for $\Gamma_1(N)$ by $M_k(\Gamma_1(N); \mathbb{C})$. We call f a cusp form if we replace (ii) by

(ii)' The function $(f|_k M)(z) = f(M.z)(cz+d)^{-k}$ is a homomorphic function and the limit $f(M.z)(cz+d)^{-k}$ is 0 when z tends to $i\infty$.

We denote the set of all cusp forms of weight k for $\Gamma_1(N)$ as $S_k(\Gamma_1(N); \mathbb{C})$.
Let us now suppose we are given a Dirichlet character χ of modulus N as above. We call f a modular form of weight k for $\Gamma_0(N)$ and χ (respectively, cusp forms if they satisfy (ii)') if we replace (i) by:

(i)' $f(M.z)(cz+d)^{-k} = \chi(d)f(z)$ for all $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$.

In this case we will use the notation $M_k(N, \chi; \mathbb{C})$ and $S_k(N, \chi; \mathbb{C})$. When χ is the trivial character we write $M_k(N; \mathbb{C}) := M_k(N, \chi; \mathbb{C})$ and $S_k(N; \mathbb{C}) := S_k(N, \chi; \mathbb{C})$.

All these spaces are finite dimension $\mathbb{C}$-vector spaces, and if we consider all modular forms (or all cusp forms) of any weight, they form a structure of a $\mathbb{C}$ graded ring (or a graded ideal, respectively). The dimensions of the spaces are well known for $k \geq 2$ (see [3]); however, for the case $k = 1$, very little is known about the dimension when we vary the level. The above definition of modular forms might make

the reader think that modular forms are relatively obscure, complex analytical objects. This is not the case; modular forms are highly geometric, arithmetic, and topological in nature and are of interest in various fields of mathematics. We will end this section by introducing the coefficient field of modular forms, our study's object of most interest.

Definition 1.1.2

The *coefficient field* of a modular form f is the subfield of $\mathbb{C}$ generated by all the coefficients a_n of its q-expansion. That is $\mathbb{Q}_f := \mathbb{Q}(a_n(f)|n \in \mathbb{N})$.

We will see later by the Eichler-Shimura isomorphism—that coefficient fields of normalized eigenforms are number fields. The space of cusp forms $S_k(N, \chi; \mathbb{C})$ has a basis of modular forms that are simultaneous eigenforms for all Hecke operators and with algebraic Fourier coefficients. The coefficient field will be a number field for such eigenforms. Moreover, if m is the smallest positive integer such that the values of the character χ are contained in the cyclotomic field $\mathbb{Q}(\zeta_m)$, the coefficient field will contain $\mathbb{Q}(\zeta_m)$.

1.2 Hecke Operators

The Hecke operators are a large area within the theory of modular forms. One of the reasons it was first developed was to find a canonical basis for the vector space of cusp forms $S_k(\Gamma_1(N); \mathbb{C})$. Since cusp forms are more challenging to write explicitly than the Eisenstein series, specifying a basis requires more sophisticated methods than the direct calculations needed to find a basis for the Eisenstein Series.

Additionally, the *Peterson inner product* makes $S_k(\Gamma_1(N); \mathbb{C})$ an inner product space, and the Hecke operators $\langle n \rangle$ and T_n for n relatively prime to the level N are normal with respect to this inner product. Thus, by linear algebra, the space $S_k(\Gamma_1(N); \mathbb{C})$ has an orthonormal basis whose elements are simultaneously eigenfunctions for the Hecke operators relatively prime to N. Furthermore, we can decompose $S_k(\Gamma_1(N); \mathbb{C})$ into *old* and *new* subspaces. The new subspace has an orthonormal basis of eigenfunctions for all the Hecke operators, and if we normalize the basis, it becomes "canonical". Furthermore, the old subspace is composed of the image of new subspaces of lower levels.

Explicit Definitions and Formulas

Computing modular forms using the definition 1.1 is not always straightforward, so we use the Hecke operators to make some progress in working with them more explicitly. They and the diamond operator are at the base of everything we will do with modular forms. One can define the operators more conceptually using geometry. See for example [3]. For our purposes, we will define them with formulas.

If a is an integer coprime to N, then we may let σ_a be a matrix in $\Gamma_0(N)$ such that

$$\sigma_a \equiv \left(\begin{smallmatrix} a^{-1} & 0 \\ 0 & a \end{smallmatrix}\right) \bmod N. \tag{1.5}$$

We define the *diamond operator* $\langle a \rangle$ by the formula

$$\langle a \rangle f = f|_k \sigma_a.$$

If $f \in M_k(N, \chi, \mathbb{C})$ then by definition $\langle a \rangle f = \chi(a) f$. This means that the diamond operators give a group action of $(\mathbb{Z}/N\mathbb{Z})^\times$ on $M_k(\Gamma_1(N); \mathbb{C})$ and on $S_k(\Gamma_1(N), \mathbb{C})$, and $M_k(N, \chi; \mathbb{C})$ and $S_k(N, \chi, \mathbb{C})$ are the χ-eigenspaces for this action. Thus, we have the isomorphism

$$M_k(\Gamma_1(N), \mathbb{C}) \simeq \bigoplus_{\chi} M_k(N, \chi, \mathbb{C}) \tag{1.6}$$

for χ running through the characters of $(\mathbb{Z}/N\mathbb{Z})^\times$ and similarly for the cuspidal spaces. Let l be prime. We let

$$\mathcal{R}_l := \{\left(\begin{smallmatrix} 1 & r \\ 0 & l \end{smallmatrix}\right) | 0 \leq r \leq l-1\} \cup \{\sigma_l \left(\begin{smallmatrix} l & 0 \\ 0 & 1 \end{smallmatrix}\right)\}, \qquad \text{if } l \nmid N \tag{1.7}$$

$$\mathcal{R}_l := \{\left(\begin{smallmatrix} 1 & r \\ 0 & l \end{smallmatrix}\right) | 0 \leq r \leq l-1\}. \qquad \text{if } l | N \tag{1.8}$$

We use these sets to define the *Hecke Operator* $T_{l,k}$ acting on f as follows.

Definition 1.2.1

Let l be a prime. The l-th Hecke operator $T_{l,k}$ of weight k is the operator on the set of functions on $\mathbb{H}$ defined by

$$T_{l,k}(f) = \sum_{\gamma \in \mathcal{R}_l} f|_k \gamma.$$

We often drop k from the notation and write T_n when the weight is clear from context.

Lemma 1.2.1

Let $f \in M_K(N, \chi; \mathbb{C})$ and $g \in M_k(\Gamma_1(N), \mathbb{C})$. We can extend χ so that $\chi(l) = 0$ if l divides $\mathbb{N}$. We have the formulas

$$a_n(T_l f) = a_{nl}(f) + l^{k-1}\chi(l) a_{n/l}(f),$$

$$a_n(T_l g) = a_{nl}(g) + l^{k-1} a_{n/l}(g).$$

Where $a_{n/l}(f)$ is equal to 0 when l does not divide n.

If we are working with the spaces $M_k(\Gamma_1(N); \mathbb{C})$ or $S_k(\Gamma_1(N); \mathbb{C})$ we can furthermore define the Hecke

operators for composite n recursively by the following formulas

$$T_{mn} = T_m T_n \qquad \text{if } (m,n) = 1 \tag{1.9}$$

$$T_{l^n} = T_{l^{n-1}} T_l - l^{k-1} \langle l \rangle T_{l^{n-2}} \qquad \text{is } l \text{ is prime.} \tag{1.10}$$

And we can easily deduce the very important formula

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

The lemma and the formula above show that the Hecke operators commute among one another. Along with the fact that the Hecke operators preserve the spaces M_k and S_k (with character or not). It thus makes sense to consider modular forms, which are eigenvectors for every Hecke operator.

Definition 1.2.2

A Modular form that is an eigenvector for T_n where $n \in \mathbb{N}$ is called an *eigenform*. Additionally, an eigenform is said to be *normalized* if the q-coefficient in its Fourier series is one, i.e.

$$f = a_0 + q + \sum_{i=2}^{\infty} a_i q^i.$$

Now we can relate the diamond operators with the Hecke operators as a $\mathbb{Z}$ linear combination of the Hecke operators as follows

$$l^{k-1} \langle d \rangle = T_l^2 - T_{l^2}.$$

For all $l \equiv d \bmod N$. Now by Bézout's identity we can find $l_1 \neq l_2$ such that $1 = l_1^{k-1} r + l_2^{k-1} s$ for appropriate $r, s \in \mathbb{Z}$. Thus, we can write

$$\langle d \rangle = r T_{l_1}^2 - r T_{l_1^2} + s T_{l_2}^2 + s T_{l_2^2}.$$

1.3 Hecke Algebras and the q-Pairing

The Hecke algebra is an algebraic structure that encodes the arithmetic properties of modular forms. We will show that the Hecke algebra is the linear dual of the space of modular forms, and we can derive all knowledge about modular forms from it.

Definition 1.3.1

We define the *Hecke algebra* over a ring R of $M_k(\Gamma_1(N);\mathbb{C})$, $S_k(\Gamma_1(N);\mathbb{C}), M_k(N,\chi;\mathbb{C})$ and $S_k(N,\chi;\mathbb{C})$ to be the R-subalgebra inside the endomorphism ring of the respective $\mathbb{C}$-vector spaces generated by all the Hecke operators and all diamond operators, denoted

$$\mathbb{T}_R(M_k(\Gamma_1(N);\mathbb{C})), \mathbb{T}_R(S_k(\Gamma_1(N);\mathbb{C})), \mathbb{T}_R(M_k(N,\chi;\mathbb{C})), \mathbb{T}_R(S_k(N,\chi;\mathbb{C}))$$

respectively.

Not only that, but we now define a bilinear pairing, which we call the *(complex) q-pairing*, as

$$M_k(N,\chi;\mathbb{C}) \times \mathbb{T}_{\mathbb{C}}(M_k(N,\chi;\mathbb{C})) \to \mathbb{C}, \quad (f,T) \to a_1(Tf).$$

Lemma 1.3.1

Let $k \geq 1$. The complex q-pairing is perfect, as is the analogous pairing for $S_k(N,\chi;\mathbb{C})$. In particular,

$$M_k(N,\chi;\mathbb{C}) \simeq Hom_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}(M_k(N,\chi,\mathbb{C}),\mathbb{C})), \quad f \to (T \to a_1(Tf)).$$

And similarly for $S_k(N,\chi;\mathbb{C})$. For $S_k(N,\chi;\mathbb{C})$, the inverse is given by sending ϕ to $\sum_{n=1}^{\infty} \phi(T_n)q^n$.

Proof

Note that a pairing over a field is perfect if and only if it is nondegenerate. We already have the equation

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

If $0 = a_1(T_n f) = a_n(f)$, then $f = 0$. This is clear for cuspforms; for non-cuspforms, we can conclude that f is a constant. And since $k \geq 1$, the only constant modular form is the zero function. On the other hand if $a_1(T_n f) = 0$ for all f, then $a_1(T(T_n f)) = a_1(T_n T f) = a_n(Tf) = 0$ for all f. As the Hecke algebra is the subring in the endomorphism ring of $M_k(N,\chi;\mathbb{C})$ or $S_k(N,\chi;\mathbb{C})$, then T must be equal to zero, proving the non-degeneracy.

■

The perfectness of the q-pairing is also called the existence of a q-expansion principle. The importance of this principle is that modular forms are defined by their q-expansion.

We end this section by introducing a vital lemma

Lemma 1.3.2

Let $f \in M_k(\Gamma_1(N); \mathbb{C})$ or $M_k(\Gamma_0(N); \mathbb{C})$ be a normalized eigenform for $k \geq 1$. Then

$$T_n f = a_n(f) f, \text{ for all } n \in \mathbb{N}.$$

Moreover, the natural map from the above duality gives bijections

$$\{\text{Normalized eigenforms in } M_k(\Gamma_1(N); \mathbb{C})\} \leftrightarrow Hom_{\mathbb{C}-algebra}(\mathbb{T}_{\mathbb{C}}(M_k(\Gamma_1(N), \mathbb{C})), \mathbb{C})$$
$$\{\text{Normalized eigenforms in } M_k(N, \chi; \mathbb{C})\} \leftrightarrow Hom_{\mathbb{C}-algebra}(\mathbb{T}_{\mathbb{C}}(M_k(N, \chi, \mathbb{C})), \mathbb{C}).$$

Proof

Let f be a normalized eigenform, then by definition there exists $a_n(f)$ such that $T_n f = a_n(f) f$ for all $n \in \mathbb{N}$. We can easily construct a map from the normalized eigenforms, a homomorphism of the Hecke algebras with the map $f \to (T_n \to a_n(f))$. On the other hand, we want to construct an inverse map that takes $\rho \to f = a_0 + q + \sum_{n \geq 2} \phi(T_n) q^n$ to a normalized Hecke eigenform. First note that by 1.3.1 we can idendify the $\mathbb{C}$-linear homomorphisms ρ to a modular form $g \in M_k$ with the pairing $g \leftrightarrow (T \to a_1(Tf)) = \rho$. Also, ρ is a $\mathbb{C}$-algebra homomorphism so $a_1(g) = a_1(T_1 f) = \rho(T_1) = 1$ and in general for $n \geq 2$

$$\begin{aligned} a_n(T_m g) &= a_1(T_n T_m f) = \rho(T_n T_m) \\ &= \rho(T_n)\rho(T_m) = a_1(T_n g) a_1(T_m g) \\ &= a_n(f) a_m(f) = a_n(a_m(f) f). \end{aligned}$$

This caluation gives us the relation $a_n(T_m f - a_m(f) f) = 0$ for all $m, n \geq 2$. That is $T_m f - a_m(f) f \in M_k$ is a constant, but as the only constant modular form of positive weight is the zero function we have the equality

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

This shows that f is a normalized Hecke eigenform.

■

Thus, normalized Hecke eigenforms can be seen as ring homomorphisms, and we will be viewing them from this perspective in this text.

1.4 Newforms

The newforms are important objects of study and they play a fundamental role in the theory of modular forms and automorphic forms. They are special types of modular forms that are particularly interesting because they have certain desirable properties. They act like the "prime" modular forms because they

cannot be constructed from a modular form of lower level. In addition to their intrinsic mathematical interest, new forms also have important applications in other areas of mathematics, including the Langlands program, a vast web of conjectures and connections between number theory, algebraic geometry, and representation theory.

We are mostly interested in the way they can be used to decompose $S_k(\Gamma_1, \chi; \mathbb{C})$ into these "prime" spaces that have a "canonical" basis. The space of modular forms $M_k(\Gamma_1(N); \mathbb{C})$ can be viewed as the direct sum

$$M_k(\Gamma_1(N); \mathbb{C}) = M_k(\Gamma_1(N); \mathbb{C})^{eis} \oplus S_k(\Gamma_1(N); \mathbb{C})$$

with $M_k(\Gamma_1(N); \mathbb{C})^{eis}$ being the space of Eisenstein modular forms. Furthermore, the space of cusp forms can also be viewed as the direct sum

$$S_k(\Gamma_1(N); \mathbb{C}) := \bigoplus_{\chi} S_k(N, \chi; \mathbb{C}).$$

Now much is known about the space $M_k(\Gamma_1(N); \mathbb{C})^{eis}$, and its structure is simpler than that of $S_k(\Gamma_1(N); \mathbb{C})$. We should, therefore, want to study the spaces $S_k(\Gamma_0(N), \chi; \mathbb{C})$ closely. Lastly we can decompose the space $S_k(\Gamma_0(N), \chi; \mathbb{C})$ even further by

$$S_k(N, \chi; \mathbb{C}) = S_k(N, \chi; \mathbb{C})^{old} \oplus S_k(N, \chi; \mathbb{C})^{new}.$$

Moreover, the space $S_k(N, \chi; \mathbb{C})^{old}$ is formed by "new forms" of lower levels. The Peterson product defined below makes the spaces $S_k(\Gamma_0(N), \chi; \mathbb{C})^{old}, S_k(\Gamma_0(N), \chi; \mathbb{C})^{new}$ orthogonal. If we extend the definition, we can show in some sense that the space of cuspforms is even orthogonal to the space of the Eisenstein series.

Definition 1.4.1

Let S_k be the space of cusp forms (for either Γ_0 with a character χ or Γ_1). The mapping

$$\langle \cdot, \cdot \rangle : S_k \times S_k \to \mathbb{C}, \quad \langle f, g \rangle := \int_{\mathcal{F}} f(\tau)\overline{g(\tau)}(\operatorname{im} \tau)^k d\nu(\tau)$$

is called the *Petersson inner product*, where

$$\mathcal{F} := \{\tau \in \mathbb{H} : |\Re\tau| \leq 1/2, |\tau| \geq 1\}$$

is the fundamental region of the modular group and for $\tau = x + iy$ we let $d\nu(\tau) = y^{-2}dxdy$ be the hyperbolic volume form.

Atkin-Lehner-Li Theory

A construction shown by Atkin-Lehner gives a basis for the space of modular forms of a given level, which are eigenfunctions for the Hecke operators prime to that level. Taking forms from lower levels $M|N$ then we can see that $S_k(\Gamma_1(M);\mathbb{C}) \subseteq S_k(\Gamma_1(N);\mathbb{C})$. Another way to move between levels is to embed $S_k(\Gamma_1(M);\mathbb{C})$ into $S_k(\Gamma_1(N);\mathbb{C})$ by composing with a "multiply-by-d" map where d is any factor of N/M. Because for any such d, let

$$\alpha_d = \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right).$$

Then we have the relation $(f|_k(\alpha_d))(\tau) = d^{k-1}f(d\tau)$ for $f : \mathbb{H} \to \mathbb{C}$. Now α_d is an injective linear map that takes $S_k(\Gamma_1(M);\mathbb{C})$ to $S_k(\Gamma_1(N);\mathbb{C})$, increasing the level from M to N.

Definition 1.4.2

For each divisor d of N, let i_d be the map

$$i_d : (S_k(\Gamma_1(N/d);\mathbb{C}))^2 \to S_k(\Gamma_1(N);\mathbb{C}), \quad (f,g) \to f + g[\alpha_d]_k.$$

The subspace of *oldforms at level N* is defined as:

$$S_k(\Gamma_1(N);\mathbb{C})^{old} = \sum_{\substack{p|N \\ p \text{ is prime}}} i_p((S_k(\Gamma_1(N/p);\mathbb{C}))^2).$$

And then we define the subspace of *newforms at level N* as the orthogonal complement with respect to the Petersson inner product, that is

$$S_k(\Gamma_1(N);\mathbb{C})^{new} = (S_k(\Gamma_1(N);\mathbb{C})^{old})^{\perp}.$$

Miyake extended this idea to a more general case, including the modular forms in the sense of Langlands in the context of representation theory. To pass to this more general case of a cusp form with a character, we can define:

$$S_k(N,\chi;\mathbb{C})^{old} := \bigcup_M \bigcup_l \{f(lz) | f \in S_k(M,\chi;\mathbb{C})\}.$$

And the space of newforms as the orthogonal complement of oldforms with respect to the Petersson inner product. Here M runs through all positive integers such that $m_\chi|M, M|N$, and $M \neq N$; l runs through all positive divisors of N/M including 1 and N/M; m_χ is the conductor of χ. In other words, $S_k(N,\chi;\mathbb{C})^{old}$ is the subspace of $S_k(N,\chi;\mathbb{C})$ generated by cusp forms of lower levels.

By definition, the following lemma is obvious:

Lemma 1.4.1

1 If χ is a primitive Dirichlet character of conductor N, then $S_k(N,\chi;\mathbb{C}) = S_k(N,\chi;\mathbb{C})^{new}$.

2 If $m_\chi | M, M|N$ and $M \neq N$, then $S_k(M,\chi;\mathbb{C}) \subseteq S_k(N,\chi;\mathbb{C})^{old}$.

3 $S_k(N,\chi;\mathbb{C})$ is generated by the set

$$\bigcup_M \bigcup_l \{f(lz) | f \in S_k(M,\chi;\mathbb{C})^{new}\}.$$

Here M runs through all positive integers such that $m_\chi|M, M|N$, and $M \neq N$; l runs through all positive divisors of N/M including 1 and N/M.

We can actually prove that $S_k(N,\chi;\mathbb{C})^{new}$ has a basis consisting of primitive forms [13] by using the following lemma

Lemma 1.4.2

The sets $\mathcal{S}_k(N,\chi)^{old}$ and $\mathcal{S}_k(N,\chi)^{new}$ are stable under Hecke operators $T(n)$ where $(n,N) = 1$.

We should emphasise that the newforms are the building blocks of the cuspidal space. If some new information comes by increasing the level, then it must come from the newspace. If we are looking at some statistics about the cuspidal space, we should only focus on the newspace since if we do not; we count the statistics for different levels many times. A simple way to do this that does not require complicated computations is by looking at the space $S_k(\Gamma_1(N);\mathbb{C})$ or the space $S_k(N,\chi;\mathbb{C})$ for prime N. The reason we do this is that their oldspace is composed only of the image of $S_k(\Gamma_1(1);\mathbb{C})$ and $S_k(1,\chi;\mathbb{C})$, which are well-known spaces that we can account for and thus easily calculate the newspace.

Chapter 2

Modular Symbols

We will first define the modular symbols formalism and define Hecke operators on them and show how the Eichler-Shimura theorem lets us establish a link between modular forms and modular symbols. Furthermore, we will define the Hecke Algebras.

This text is largely based on [6, Wiese's] text on the computational Arithmetic of Modular Forms, where all the proofs of the stated theroms can be found, with some inspiration from [16, Stein].

2.1 Modular Symbols Formalism

This section defines formal modular symbols, as implemented in [6]. But first, some motivation. Note the decomposition

$$M_k(\Gamma;\mathbb{C}) = S_k(\Gamma;\mathbb{C}) \oplus E_k(\Gamma;\mathbb{C})$$

where $E_k(\Gamma;\mathbb{C})$ is spanned by generalized Eisenstein series and $S_k(\Gamma;\mathbb{C})$ is the space of cusp forms. As we mentioned in the section about newforms, the structure of S_k is generally much more complicated than that of the Eisenstein series E_k.

An idea of Birch, called modular symbols, provides a method for computing $S_k(\Gamma)$, for a congruence subgroup Γ, and its various properties. For example, for understanding special values of L-functions and in our case making the calculations of modular forms much more explicit. Modular symbols are also an essential theoretical tool.

We can think of modular symbols $\{\alpha, \beta\}$ as the homology class relative to the cusps of a path or simply as a geodesic path between two cusps α and β in $\mathbb{P}^1(\mathbb{Q})$.

We will, however, give a combinatorial definition. For the rest of this section, we let R be a commutative ring with a unit and Γ be a subgroup of finite index in $PSL_2(\mathbb{Z}) := SL_2(\mathbb{Z})/\langle -1\rangle$. We choose to work with $PSL_2(\mathbb{Z})$ instead of $SL_2(\mathbb{Z})$ since it simplifies algebra and notation. We let V be a left $R[\Gamma]$-module.

Definition 2.1.1

We define the R-modules

$$\mathscr{M}_R := R[\{\alpha,\beta\}|\alpha,\beta\in\mathbb{P}^1(\mathbb{Q})]/\left\langle\{\alpha,\alpha\},\{\alpha,\beta\}+\{\beta,\gamma\}+\{\gamma,\alpha\}|\alpha,\beta,\gamma\in\mathbb{P}^1(\mathbb{Q})\right\rangle$$

and

$$\mathscr{B}_R := R[\mathbb{P}^1(\mathbb{Q})]$$

and equip both with the natural Γ-action. Furthermore, we let

$$\mathscr{M}_R(V) := \mathscr{M}_R \otimes_R V \quad \text{and } \mathscr{B}_R(V) := \mathscr{B}_R \otimes_R V$$

for the left diagonal Γ-action.

(a) We call the Γ-coinvariants

$$\mathscr{M}_R(\Gamma,V) := \mathscr{M}_R(V)_\Gamma = \mathscr{M}_R(V)/\left\langle(x-gx)|g\in\Gamma, x\in\mathscr{M}_R(V)\right\rangle$$

the space of (Γ,V)*-modular symbols.*

(b) We call the Γ-coinvariants

$$\mathscr{B}_R(\Gamma,V) := \mathscr{B}_R(V)_\Gamma = \mathscr{B}_R(V)/\left\langle(x-gx)|g\in\Gamma, x\in\mathscr{B}_R(V)\right\rangle$$

the space of (Γ,V)*-boundary symbols.*

(c) We define the *boundary map* as the map

$$\mathscr{M}_R(\Gamma,V)\to\mathscr{B}_R(\Gamma,V)$$

which is induced from the map $\mathscr{M}_R\to\mathscr{B}_R$ sending $\{\alpha,\beta\}$ to $\{\beta\}-\{\alpha\}$.

(d) The kernel of the boundary map is denoted by $\mathscr{CM}_R(\Gamma,V)$ and is called *the space of cuspidal* (Γ,V)*-modular symbols.*

Let $R[X,Y]_n$ be the homogeneous polynomials of degree n in two variables with coefficients in the ring R. We put $V_n(R)=R[X,Y]_n$ and

$$Mat_2(\mathbb{Z})_{det\neq 0} := GL_2(\mathbb{Q})\cap\mathbb{Z}^{2\times 2}.$$

Then $V_n(R)$ is a $Mat_2(\mathbb{Z})_{det\neq 0}$-module in several ways, for example:

$$(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).f)(X,Y) = f((X,Y)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) = f((aX+cY, bX+dY))$$
$$(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).f)(X,Y) = f(\left(\begin{smallmatrix} d & -b \\ -c & a \end{smallmatrix}\right)\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right)) = f(\left(\begin{smallmatrix} dX-bY \\ -cX+aY \end{smallmatrix}\right)).$$

Both these actions are isomorphic since the transpose of $(X,Y)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is isomorphic to $(X,Y)\sigma^{-1}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\sigma$, where $\sigma = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$. That is, we have an isomorphism

$$V_n(R) \xrightarrow[\sigma^{-1}.f]{} V_n(R)$$

carrying the action of the left-hand module to the action of the right-hand module. We also have the natural action by $Mat_2(\mathbb{Z})_{det\neq 0}$ given by:

$$(\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).f)\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right) = f((\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} X \\ Y \end{smallmatrix}\right)) = f(\left(\begin{smallmatrix} aX+bY \\ cX+dY \end{smallmatrix}\right)).$$

We will use the first mentioned action since Sagemath [14] implements it.

Now let $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$ be a Dirichlet character. By R^χ we denote the $R[\Gamma_0(N)]$-module which is defined to be R with the $\Gamma_0(N)$-action through χ, that is $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).r = \chi(a)r = \chi^{-1}(d)r$ for $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$ and $r \in R$. We let

$$V_n^\chi(R) := V_n(R) \otimes_R R^\chi$$

equipped with the natural diagonal left $\Gamma_0(N)$-actions. Note that if $\chi(-1) = (-1)^n$, then minus the identity it acts trivially on $V_n^\chi(R)$, thus we consider these modules also as $\Gamma_0(N)/\{\pm 1\}$ modules.

Definition 2.1.2

Let $N \geq 3, k \geq 2$ be integers. We define the modular symbols and the cuspidal modular symbols for the congruence subgroups $\Gamma_1(N)$ and $\Gamma_0(N)$ as

$$\begin{aligned} \mathscr{M}_k(\Gamma_1(N); R) &:= \mathscr{M}_R(\Gamma_1(N), V_{k-2}(R)), \\ \mathscr{CM}_k(\Gamma_1(N); R) &:= \mathscr{CM}_R(\Gamma_1(N), V_{k-2}(R)), \\ \mathscr{M}_k(N, \chi; R) &:= \mathscr{M}_R(\Gamma_0(N)/\{\pm 1\}, V_{k-2}(R)), \\ \mathscr{CM}_k(N, \chi; R) &:= \mathscr{CM}_R(\Gamma_0(N)/\{\pm 1\}, V_{k-2}(R)). \end{aligned}$$

Let $\eta := \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Now $\eta\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\eta = \left(\begin{smallmatrix} a & -b \\ -c & d \end{smallmatrix}\right)$ and

$$\eta\Gamma_1(N)\eta = \Gamma_1(N) \qquad \eta\Gamma_0(N)\eta = \Gamma_0(N).$$

We can use the matrix η to make an involution on the various modular symbols spaces. We use the diagonal action on $\mathscr{M}_R(V)$ provided η acts on V. On $V_{k-2}(R)$ we use the usual $Mat_2(\mathbb{Z})_{det\neq 0}$-action, and on $V_{k-1}^\chi = V_{k-2}^\chi \otimes R^\chi$ we let η only act on the first factor. We denote by superscript $^+$ the subspace

invariant under this involution, and by the superscript $^-$, we denote the anti-invariant one.

2.2 Hecke Operators on Modular Symbols

This section aims to extend the definition of Hecke operators and diamond operators on formal modular symbols, $\mathscr{M}_k(\Gamma_1(N);R), \mathscr{CM}_k(\Gamma_1(N);R), \mathscr{M}_k(N,\chi;R)$ and $\mathscr{CM}_k(N,\chi;R)$, for any ring R. We can see that they are conceptually very similar if we view them from a double coset formulation, as seen in [19] and [13].

We will now define the Hecke operators for modular symbols by only considering T_l for l prime, similarly to that of the Hecke operators for modular forms. Then we can use formulas 1.9 and 1.10 to define the T_n for composite n. Next, we define the diamond operators for any $n \in \mathbb{N}$.

Note the definition 1.7 and 1.8 of $\mathscr{R}_l$, let $x \in \mathscr{M}_k(\Gamma_1(N);R)$ or $x \in \mathscr{M}_k(N,\chi;R)$ and we define

$$T_l x := \sum_{\delta \in \mathscr{R}_l} \delta.x.$$

If a is an integer coprime to N, we define the diamond operator as

$$\langle a \rangle\, x := \sigma_a x$$

with σ_a defined as before in 1.5. Note that when $x = (m \otimes v \otimes 1)_{\Gamma_0(N)/\{\pm 1\}} \in \mathscr{M}_k(N,\chi;R)$, then $\langle a \rangle\, x = (\sigma_a m \otimes \sigma_a v \otimes \chi(a^{-1}))_{\Gamma_0(N)/\{\pm 1\}} = x$, thus $(\sigma_a m \otimes \sigma_a v \otimes 1)_{\Gamma_0(N)/\{\pm 1\}} = \chi(a)(m \otimes v \otimes 1)_{\Gamma_0(N)/\{\pm 1\}}$.

Hecke algebras

Just as in the section on modular forms, we define Hecke algebras on modular symbols similarly. We let $\mathbb{T}_R(\mathscr{M}_R(\Gamma_1(N));R))$ be the R-subalgebra of the R-endomorphism algebra of the R-module $\mathscr{M}_k(\Gamma_1(N);R)$ generated by the Hecke operators T_n. We define the Hecke algebra for cuspidal modular symbols similarly. Now, we state a very useful result without proof and a corollary that allows us to explicitly work with the Hecke algebras.

Proposition 2.2.1

The R-modules $\mathscr{M}_k(\Gamma_1(N),R), \mathscr{CM}_k(\Gamma_1(N),R), \mathscr{M}_k(N,\chi;R)$ and $\mathscr{CM}_k(N,\chi;R)$ are finitely presented.

Corollary 2.2.1

Let R be a Noetherian ring. The Hecke algebras $\mathbb{T}_R(\mathscr{M}_k(\Gamma_1(N),R))$,$\mathbb{T}_R(\mathscr{CM}_k(\Gamma_1(N),R))$, $\mathbb{T}_R(\mathscr{M}_k(N,\chi;R))$ and $\mathbb{T}_R(\mathscr{CM}_k(N,\chi;R))$ are finitely presented R-modules.

This means that we can find $q, p \in \mathbb{N}$ and surjective maps $R^q \to \mathbb{T}_R(\mathscr{M}_k(\Gamma_1(N), R))$ and $R^p \to \mathscr{M}(\Gamma_1(N), R)$. Then we can look at the space $\mathbb{T}_R(\mathscr{M}_k(\Gamma_1(N); R))$ and $\mathscr{M}_k(\Gamma_1(N); R)$ as elements in R^p and R^q respectively that have some relation between each other. If R is a ring, we can store all data about the modular symbols as a finite tuple, or better yet, if R is a field, then we can use linear algebra to calculate the modular symbols as a subspace of a finite-dimensional vector space. The same can be said of the cuspidal modular symbols and algebra.

Eichler–Shimura Isomorphism

Here, we state a theorem which is a fundamental result in the study of modular forms.

Theorem 2.2.1

(Eichler-Shimura) There are isomorphisms respecting the Hecke operators

(a) $M_k(N, \chi; \mathbb{C}) \oplus S_k(N, \chi, \mathbb{C})^\vee \simeq \mathscr{M}_k(N, \chi, \mathbb{C})$,

(b) $S_k(N, \chi, \mathbb{C}) \oplus S_k(N, \chi, \mathbb{C})^\vee \simeq \mathscr{C}\mathscr{M}_k(N, \chi, \mathbb{C})$,

(c) $S_k(N, \chi, \mathbb{C}) \simeq \mathscr{C}\mathscr{M}_k(N, \chi, \mathbb{C})^+$.

Similar isomorphism holds for modular forms and modular symbols on $\Gamma_1(N)$.

The theorem allows us to connect modular forms, a complex analytic function, with an algebraic object that is simpler to work with and can be easily represented in a computer. The isomorphism 2.2 above gives rise to the following three corollaries.

Corollary 2.2.2

Let R be a subring of $\mathbb{C}$ and. Then there is the natural isomorphism

$$\mathbb{T}_R(M_k(\Gamma_1(N); \mathbb{C})) \simeq \mathbb{T}_R(\mathscr{M}_k(\Gamma_1(N); \mathbb{C})).$$

A similar result holds for cusp forms.

Corollary 2.2.3

Let R be a subring of $\mathbb{C}$ and $\chi : (\mathbb{Z}/N\mathbb{Z})^\times \to R^\times$ a character. Then, the natural map

$$\mathbb{T}_R(M_k(N, \chi, \mathbb{C})) \otimes_R \mathbb{C} \simeq \mathbb{T}_\mathbb{C}(M_k(N, \chi; \mathbb{C}))$$

is an isomorphism. A similar result holds for cusp forms and $\Gamma_1(N)$.

Corollary 2.2.4

Let R be a subring of $\mathbb{C}$. Then we have the isomorphisms

$$\begin{aligned} M_k(\Gamma_1(N), \mathbb{C}) &\simeq Hom_R(\mathbb{T}_R(\mathscr{M}_k(\Gamma_1(N); R)), R) \otimes_R \mathbb{C} \\ &\simeq Hom_R(\mathscr{M}_k(\Gamma_1(N); R), \mathbb{C}) \\ S_k(\Gamma_1(N), \mathbb{C}) &\simeq Hom_R(\mathbb{T}_R(\mathscr{C}\mathscr{M}_k(\Gamma_1(N); R)), R) \otimes_R \mathbb{C} \\ &\simeq Hom_R(\mathscr{C}\mathscr{M}_k(\Gamma_1(N); R), \mathbb{C}). \end{aligned}$$

The above corollary lets us describe modular forms in linear algebra involving only modular symbols. Now, lastly and most importantly for our study is the following corollary.

Corollary 2.2.5

Let $f = \sum_{n=1}^{\infty} a_n(f) q^n \in S_k(\Gamma_1(N); \mathbb{C})$ be a normalized Hecke eigenform. Then $\mathbb{Q}_f := \mathbb{Q}(a_n(f) | n \in \mathbb{N})$ is a number field of degree less than or equal to $\dim_{\mathbb{C}} S_k(\Gamma_1(N); \mathbb{C})$. If f has Dirichlet character χ, then $\mathbb{Q}_f$ is a finite field extension of $\mathbb{Q}(\chi)$ of degree less than or equal to $\dim_{\mathbb{C}} S_k(N, \chi; \mathbb{C})$. Here $\mathbb{Q}(\chi)$ is the extension of $\mathbb{Q}$ generated by all the values of χ.

Proof

If we apply the previous corollaries with $R = \mathbb{Q}$ or $R = \mathbb{Q}(\chi)$ and note that Hecke eigenforms f correspond to algebra homomorphisms λ_f from the Hecke algebra into $\mathbb{C}$. Let's first note that by 2.2.3

$$\mathbb{T}_{\mathbb{Q}} \otimes_{\mathbb{Q}} \mathbb{C} = \mathbb{T}_{\mathbb{C}}.$$

That is, there exists a $\mathbb{Q}$-structure in $\mathbb{T}_{\mathbb{C}}$. In terms of matrices, this means that $\mathbb{T}_{\mathbb{C}}$ has a $\mathbb{C}$-basis consisting of matrices with coefficients in $\mathbb{Q}$. Additionally, we know that the Hecke algebra $\mathbb{T}_{\mathbb{C}}$ has a finite basis $\langle T^{(1)}, \ldots, T^{(d)} \rangle$. We also have the following equalities

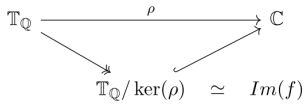
$$\begin{aligned} S_k &= Hom_{\mathbb{C}}(\mathbb{T}_{\mathbb{C}}, \mathbb{C}) \\ &= Hom_{\mathbb{C}}(\mathbb{C} \otimes_{\mathbb{Q}} \mathbb{T}_{\mathbb{Q}}, \mathbb{C}) \\ &= Hom_{\mathbb{Q}}(\mathbb{T}_{\mathbb{Q}}, \mathbb{C}). \end{aligned}$$

Any $\mathbb{C}$-linear map $f : \mathbb{T}_{\mathbb{C}} \to \mathbb{C}$ is uniquely determined by its values on a basis, and the same is true to determine $\mathbb{Q}$-linear maps $g : \mathbb{T}_{\mathbb{Q}} \to \mathbb{C}$. Now $\mathbb{T}_{\mathbb{Q}}$ is a finite-dimensional $\mathbb{Q}$-vector space and

$$Hom_{\mathbb{C}-alg}(\mathbb{T}_{\mathbb{C}}, \mathbb{C}) = Hom_{\mathbb{Q}-alg}(\mathbb{T}_{\mathbb{Q}}, \mathbb{C}).$$

Since the $\mathbb{C}$-algebra homomorphism and $\mathbb{Q}$-algebra homomorphism are determined by the identity

matrix going to one and the values on the basis elements.
This means that any normalized Hecke eigenform f can be seen as a $\mathbb{Q}$-algebra homomorphism ρ, and its image is the coefficient ring.



Now, the image of ρ is equal to the coefficient field of f and is a number field that is

$$Im(\lambda) = \mathbb{Q}(\rho(T_n)|n \in \mathbb{N}) = \mathbb{Q}(a_n(f)|n \in \mathbb{N}) = \mathbb{Q}_f.$$

■

Lastly, we mention a proposition and a corollary that tell us that when we are calculating the Hecke algebras for $\Gamma_0(N)$, we have an upper bound on the number of Hecke operators we need to make in order to calculate the Hecke algebra.

Proposition 2.2.2

Let $f \in M_k(N, \chi; \mathbb{C})$ such that $a_n(f) = 0$ for all $n \leq k\mu/12$, where $\mu = N \prod_{l|N \text{ prime}}(1 + 1/l)$. Then $f = 0$.

Corollary 2.2.6

Let K, N, μ and χ be as in the previous proposision. Then $\mathbb{T}_k(\mathscr{C}\mathscr{M}(N, \chi; K))$ can be generated as a K-vector space by the operators T_n for $1 \leq n \leq k\mu/12$.

2.3 Modular Forms Over General Rings

When studying the arithmetic properties of modular forms, it is often useful to work over rings. For example, when studying mod p Galois representations attached to modular forms, it is often easier to work with modular forms whose coefficients already lie in a finite field. If we define the modular forms over a ring R as the R-linear dual of the $\mathbb{Z}$-Hecke algebra of the holomorphic modular forms, that is, by taking q-expansions with coefficients in R, we can already get quite far.

If we are working with the congruence subgroup $\Gamma_1(N)$, then the modular forms with q-expansion in the integers form a lattice in the space of all modular forms.

We will here define modular forms over general rings as follows

Definition 2.3.1

Let $k \geq 1$ and $N \geq 1$. Let R be any ring. We use the q-pairing to define modular (cusp) forms over R. We let

$$\begin{aligned} M_k(\Gamma_1(N); R) &:= Hom_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C})), R) \\ &\simeq Hom_R(\mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C})) \otimes_{\mathbb{Z}} R, R) \\ S_k(\Gamma_1(N); R) &:= Hom_{\mathbb{Z}}(\mathbb{T}_{\mathbb{Z}}(S_k(\Gamma_1(N); \mathbb{C})), R) \\ &\simeq Hom_R(\mathbb{T}_{\mathbb{Z}}(S_k(\Gamma_1(N); \mathbb{C})) \otimes_{\mathbb{Z}} R, R). \end{aligned}$$

Likewise, we give a similar definition for $M_k(N, \chi; R)$ and $S_k(N, \chi; R)$

Every element f of $M_k(\Gamma_1(N); R)$ or $M_k(N, \chi; \mathbb{C})$ corresponds to a $\mathbb{Z}$-linear function $\Phi : \mathbb{T}_{\mathbb{Z}}(M_k(\Gamma_1(N); \mathbb{C})) \to R$ and is uniquely indentified by its formal q-expansion

$$f = \sum_{n \in \mathbb{N}} \Phi(T_n) q^n = \sum_n a_n(f) q^n \in \mathbb{R}[[q]].$$

Note that if we want to get the original q-expansion, a 0-th coefficient should also be there. However, for cusp forms, we do not have to worry about this. The definitions agree with that of 1.1 and as a special case $R = \mathbb{Z}$ then $M_k(\Gamma_1(N); \mathbb{Z})$ corresponds exactly to holomorphic modular forms $M_k(\Gamma_1(N); \mathbb{C})$ whose q-expansion take values in $\mathbb{Z}$.

Chapter 3

Methods

This chapter discusses the methods used to calculate statistics about the maximal residue degree of prime ideals in the coefficient fields of Hecke eigenforms in $S_k(N, \mathbb{C})^{new}$. There are a couple of reasons we chose to work with this space. Firstly, we have by corollary 2.2.5 that the coefficient field of Hecke eigenforms in the space $S_k(N, \mathbb{C})$ is a number field. Secondly, as discussed in the section about newforms, we would only like to count the new information on the space. Moreover, we choose to work with cusp forms for $\Gamma_0(N)$ since the space is much smaller than that of $\Gamma_1(N)$ as well as the fact that we can bound the number of calculations needed to make in order to generate the Hecke algebra, see 2.2.6.

We will first discuss an elementary method due to Kummer that we can use to calculate the residue degrees when working with the spaces $S_k(1, \mathbb{C})$, using Maeda's conjecture. Then discuss a more sophisticated method that calculates the residue degree of the local components of Hecke algebras over $\mathbb{F}_p$. Lastly we will show the connection between the residue degree of the Hecke algebra defined over $\mathbb{F}_p$ with the residue degree of the coefficient ring of Hecke eigenforms reduced modulo a prime above p.

This chapter is based on discussions between the author and Professor Wiese.

3.1 Maeda and Kummer

We begin by introducing Maeda's Conjecture, first proposed by the Japanese mathematician Yutaka Maeda [5], which is related to the structure of the Hecke algebra associated with modular forms. It states that the Hecke algebra of weight k modular forms on the full modular group is a simple algebra.

Conjecture 3.1.1

(Maeda) For any k and any normalized eigenform $f \in S_k(1)$, the coefficient field $\mathbb{Q}_f$ has degree equal to $d_k := \dim_{\mathbb{C}} S_k(1; \mathbb{C})$ and the Galois group of its normal closure over $\mathbb{Q}$ is the symmetric group S_{d_k}.

In simpler terms, Maeda's Conjecture suggests a remarkable and elegant algebraic structure for the Hecke algebra associated with modular forms of a certain weight. If true, this conjecture would provide

deep insights into the arithmetic and algebraic properties of modular forms and their underlying structures. A consequence of the conjecture is that the characteristic polynomial of T_2 on S_k is irreducible for any k. In the last thirty years, this statement has been verified numerically for $k \leq 12.000$, see 3.1, which we will use to calculate the number field. There are also some generalizations of Maeda's conjecture, see [11],

Source	weights
Lee-Hung	$k \leq 62, k \neq 60$
Buzzard	$k = 12l, l$ prime, $2 \leq l \leq 19$
Maeda	$k \leq 468$
Conrey-Farmer	$k \leq 500, k \equiv 0 \pmod 4$
Farmer-James	$k \leq 2.000$
Buzzard-Stein, Klansman	$k \leq 3.000$
Chu-Wee Lim	$k \leq 6.000$
Ghitza-McAndrew	$k \leq 12.000$

Table 3.1: Summary of known cases of Maeda's conjecture for T_2

that tell us about the structure of the Hecke algebra of modular forms of different levels. Another result related to Maeda's conjecture is the following proposision 3.1.1.

Proposition 3.1.1

If N is a prime, $k = 2$ and $f \in S_k(N, \mathbb{C})^{new}$ be a Hecke eigenform then there exists a prime p such that $\mathbb{Q}_f = \mathbb{Q}(a_p)$ [9].

Let $\mathbb{Q}_f = \mathbb{Q}(\alpha)$, then if we know α we can easily construct the coefficient field with the minimal polynomial of α. This makes the calculations of the residue degrees of the coefficient fields of normalized eigenforms over a prime $\mathfrak{p}$ straightforward, and we can use some elementary methods.

Let us now fix a p and study properties of the coefficient fields of a normalized eigenform $f \in S_k(1; \mathbb{C})$, denoted $\mathbb{Q}_f$ and then reduce it modulo some prime $\mathfrak{p}$ over the prime p in $\mathbb{Q}_f$. The idea is to reduce the minimal polynomial of α modulo p because this gives us all the information about the set

$$E_{f,p} := \left\{ [\mathcal{O}_{\mathbb{Q}_f}/\mathfrak{p}_1 : \mathbb{F}_p], [\mathcal{O}_{\mathbb{Q}_f}/\mathfrak{p}_2 : \mathbb{F}_p], \ldots \right\}.$$

We can do this because the eigenform coefficients are algebraic integers so we can reduce them over the finite field $\mathbb{F}_p$ first and then for a prime ideal over p. In particular, we would like to study the set $\cup_{k=12}^{B} E_{f,p}$ and make some observations.

Let F be a number field and $\alpha \in \mathcal{O}_F$ be such that $F = \mathbb{Q}(\alpha)$. The index of α is defined as $\text{ind}(\alpha) = |\mathcal{O}_F/\mathbb{Z}[\alpha]|$. This value characterizes when it is possible to factor $p\mathcal{O}_F$ by computing the factorization of a polynomial over $\mathbb{F}_p$.

Theorem 3.1.1

(Kummer) Let $f \in \mathbb{Z}[x]$ be the minimal polynomial of α over $\mathbb{Z}$ and suppose p does not divide $ind(\alpha)$. Let

$$\overline{f} = \prod_{j=1}^{k} \overline{f_j}^{e_j} \in \mathbb{F}_p[x]$$

be the factorization in monic irreducible polynomials, and define $P_j := (p, f_j(\alpha))$ where f_j is any lift of $\overline{f}_j$ to $\mathbb{Z}[x]$. Then

$$p\mathcal{O}_F = \prod_{j=1}^{k} P_j^{e_j}.$$

Note that this method does not always work. We might have to employ the Buchmann-Lenstra algorithm, which is quite technical and fully described in Cohen's book [2]. However, since we are interested in the asymptotic behaviour of the coefficient field, we do not have to worry about this particular case.

We can now compute $[\mathcal{O}_{\mathbb{Q}_f}/\mathfrak{p}_1 : \mathbb{F}_p]$ through the degree of the irreducible factor of the minimal polynomial of α for a prime p chosen with some caution.

3.2 Local Algebras

In order to make progress in calculating the residue degrees for $S_k(N;\mathbb{C})$, we need to use more sophisticated methods. We will show how to decompose the Hecke algebras into its local components. Then, we aim to connect the residue degree of the Hecke algebra with the residue degree of primes of the coefficient field of Hecke eigenforms.

The algebra $\mathbb{T} := \mathbb{T}_{\mathbb{F}_p}(\mathscr{C}\mathscr{M}_k(N;\mathbb{F}_p)) = Hom_{\mathbb{F}_p}(S_k(N;\mathbb{F}_p),\mathbb{F}_p)$ is a finite-dimensional commutative $\mathbb{F}_p$ algebra, and by results from commutative algebra we can also we write it as

$$\mathbb{T} \simeq \prod_{\mathfrak{p} \text{ prime ideals of } \mathbb{T}} \mathbb{T}_{\mathfrak{p}}$$

where the $\mathbb{T}_{\mathfrak{p}}$ are the local Hecke algebras associated to the prime ideal $\mathfrak{p}$.

We first propose Algorithm 1 to generate the mod p Hecke algebra $\mathbb{T} := \langle T_n | T_n \circlearrowleft S_k(N,\mathbb{F}_p)\rangle$. And then propose Algorithm 2 to decompose the Hecke algebra into its local components $\mathbb{T}_{\mathfrak{p}}$

Generating the Hecke algebra

First, we will calculate the dimension of the space of cusp forms, $d := \dim_{\mathbb{F}_p}(\mathbb{T}) = \dim_{\mathbb{F}_p}(S_k(N,\mathbb{F}_p))$, by known formulas, and use this as an indicator when we should stop our algorithm. Then, we can look at the algebra as a $\mathbb{F}_p$ vector space by 2.2 to simplify the calculations. Then, once we have enough Hecke operators to span our algebra, we can calculate the residue degree of the Hecke algebras after

Algorithm 1 Generate the Hecke Algebra

Require: $N \geq 1, k \geq 2$,
  calculate $d = \dim_{\mathbb{F}_p}(\mathbb{T}) = \dim_{\mathbb{F}_p}(S_k(N;\mathbb{C}))$
  $M \leftarrow 0 \subset \text{MatrixAlgebra}(\mathbb{F}_p, d)$
  while $\dim(M) \neq d$ **do**
    $M \leftarrow M + \langle T_n \rangle$
  end while
  Get a $\mathbb{F}_p$ basis of $M : T^{(1)}, \ldots, T^{(d)}$

localization. While calcuating decomposition of the algebra $\mathbb{T}_{\mathbb{F}_p}(\mathscr{CM}_k(N,\chi;\mathbb{F}_p))$ and $\mathbb{T}_{\mathbb{F}_p}(\mathscr{M}_k(N,\chi;\mathbb{F}_p))$ we can furthermore use the Sturm bound 2.2 to be sure we will end our calculations.

Decomposition of the Hecke algebra

Algorithm 2 Decomposition of Hecke algebra into it's local components

Require: A basis $\{T^{(1)}, \ldots, T^{(d)}\}$ of the commutative finite dimensional $\mathbb{F}_p$-algebra $\mathbb{T}$
  $S \leftarrow [\mathbb{F}_p^n]$
  for $T \in \{T^{(1)}, \ldots, T^{(d)}\}$ **do**
    $S_{new} = []$
    for $S_i \in S$ **do**
      Find minimal polynomial P of T on S_i
      Factor $P = \prod p_i^{e_i}$ into irreducible polynomials
      for irreducible factor p_i in the factorization of P **do**
        $S_{new} \leftarrow S_{new} + [Ker(p_i^{e_i}(T))]$
      end for
    end for
    $S \leftarrow S_{new}$
  end for
  return S

We can find the local algebras using a recursive algorithm and then easily calculate the residue degrees of each of them. If we assume we know a basis $B := \{T^{(1)}, \ldots, T^{(n)}\}$ of the commutative finite dimensional $\mathbb{F}_p$-algebra $\mathbb{T}$, we can use proposition 3.2.1 to achieve our goal.

Proposition 3.2.1

Let K be a field of characteristic 0 or a finite field. Let A be a finite-dimensional commutative algebra over K and let $a_1, \ldots, a_n$ be a $K-$basis of A with the property that the minimal polynomial of each a_i is a power of a prime polynomial $p_i \in K[X]$. Then A is local.

We have already established that $\mathbb{T}_{\mathbb{F}_p}(\mathscr{M}(\Gamma_1(N),\mathbb{F}_p))$ is a finitely presented $\mathbb{F}_p$-module 2.2. This means that there exists a surjection $\mathbb{F}_p^n \to \mathbb{T}_R(\mathscr{M}(\Gamma_1(N),\mathbb{F}_p))$. We can think of Hecke operators as homomorphisms of $\mathbb{F}_p^n$, or simply as matrices from $\mathbb{F}_p^n$ to $\mathbb{F}_p^n$. Let $T^{(1)}$ be a basis element, and $P = \prod p_i^{e_i}$

be the minimal polynomial of $T^{(1)}$ over $\mathbb{F}_p^n$, factored into irreducible polynomials. We can decompose our space $\mathbb{F}_p^n$ as follows

$$\mathbb{F}_p^n = \bigoplus Ker(p_i(T^{(1)^{e_i}}) \supseteq Ker(p_i(T^{(1)})).$$

If we let $S_i := Ker(p_i(T_1)^{e_i})$ we know that the minimal polynomial of $T^{(1)}$ on each of the S_i is a power of a prime polynomial.

Now let us suppose we have a second matrix M that commutes with $T^{(1)}$ then if $v \in S_i$, that is $p_i(T^{(1)})^{e_i} \cdot v = 0$, we have that $p_i(T^{(1)})^{e_i} M \cdot v = M p_i(T)^{e_i} \cdot v = M \cdot 0 = 0$ thus $M \cdot S_i \subseteq S_i$.

Recursively, we can now pick the next basis element $T^{(2)}$ and restrict it to S_i. Then we look at its minimal polynomial on the space S_i, let us call them $P_i = \prod p_{ij}^{e_{ij}}$. We can then furthermore decompose the space S_i as follows

$$S_i = \bigoplus Ker(p_{ij}(T^{(2)})^{e_{ij}}).$$

On S_{ij}, $T^{(2)}$ has minimal polynomial $p_{ij}^{e_{ij}}$, and $T^{(1)}$ has minimal polynomial $p_i^{e_i}$. After completing this procedure for each basis element, we have the decomposition

$$\mathbb{T} = \bigoplus \mathbb{T}_k \simeq \prod_{\mathfrak{p} \text{ prime}} \mathbb{T}_{\mathfrak{p}}.$$

We can write each $\mathbb{T}_{\mathfrak{p}}$ as the intersection of $Ker(q^e)$ with q being an irreducible polynomial. We are interested in the dimensions of the $\mathbb{T}'_k = \bigcap Ker(q)$, where the q are the same as before because $\mathbb{T}'_i$ are field extensions of $\mathbb{F}_p$.

3.3 Residue degree connection

In this section, we will discuss the connection between the residue degree of local Hecke algebras and the residue degree of primes in the coefficient field of Hecke eigenforms.

We will be looking at $\mathbb{T} \subseteq End(S_k(N, \mathbb{C}); \mathbb{C})$ (or any modular forms space of another kind); this is the ring generated by the Hecke operators T_n for all $n \in \mathbb{N}$. A normalized Hecke eigenform can be seen as a ring homomorphism.

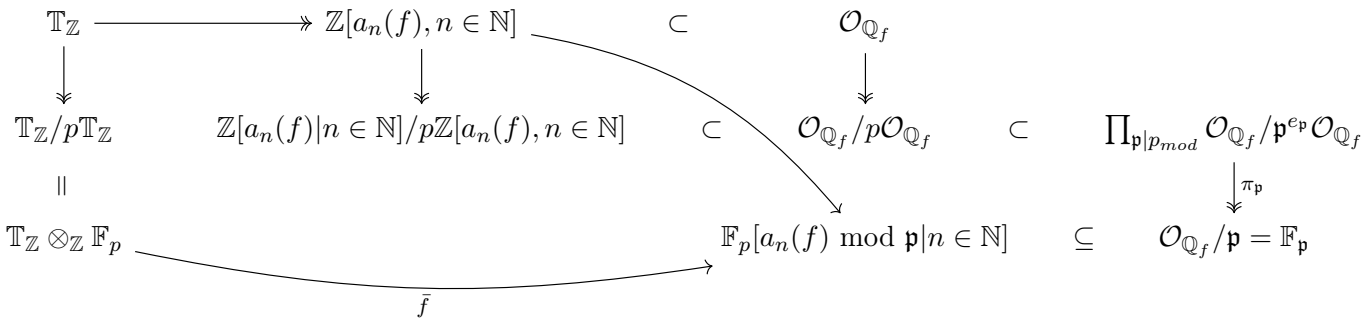
$$f : \mathbb{T}_{\mathbb{Z}} \to \mathbb{C}, \quad T_n \to a_n(f).$$

And we have the relation between its image, coefficient ring and its ring of integers.

$$\begin{array}{ccccc} \mathrm{Im}(f) & = & \mathbb{Z}[a_n(f) | n \in \mathbb{N}] & \subset & \mathbb{Q}(a_n(f) | n \in \mathbb{N}) \\ & & \cap| & & || \\ & & \mathcal{O}_{\mathbb{Q}_f} & \subset & \mathbb{Q}_f \end{array}$$

We can project the Hecke algbra $\mathbb{T}_{\mathbb{Z}}$ to the set $\mathbb{F}_p[a_n(f) \bmod \mathfrak{p} | n \in \mathbb{N}]$ by first projecting $\mathbb{T}_{\mathbb{Z}}$ to $\mathbb{T}_{\mathbb{Z}}/p\mathbb{T}_{\mathbb{Z}}$, which is equal to $\mathbb{T}_{\mathbb{Z}} \otimes_{\mathbb{Z}} \mathbb{F}_p$, and then look at its image by the map $\overline{f}$, which is defined as the reduction

of the coefficients of f modulo p. The diagram below then allows us to examine the connection between the residue degree $[\mathbb{F}_\mathfrak{p} : \mathbb{F}_p]$ of the prime $\mathfrak{p}$ above p and the Hecke algebra $\mathbb{T}_\mathbb{Z}$.



An important note is that the ring of integers is not the same as the integers in addition to the coefficients of the eigenform. It is of finite index. If p divides $[\mathcal{O}_{\mathbb{Q}_f}/\mathfrak{p} : \mathbb{F}_p]$ we will not get the desired residue degrees by the reduction mod p, however we do not expect this to happen for many N. Thus, we will assume p does not divide the index we will a and see where that leads us. Or at least, as in our case, it gives us some idea about understanding the behaviour asymptotically.

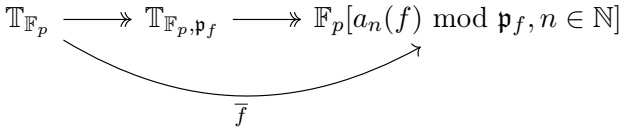
To further explain the residue connection we will look at $\mathbb{T}_{\mathbb{F}_p}$. Since $\mathbb{T}_{\mathbb{F}_p}$ is an Artin ring prime ideals are maximal. Thus, we can write $\mathbb{T}_{\mathbb{F}_p}$ as a product of local algebras $\mathbb{T}_{\mathbb{F}_p,\mathfrak{p}}$ where $\mathfrak{p}$ is a prime ideal, that is:

$$\mathbb{T}_\mathbb{Z}/p\mathbb{T}_\mathbb{Z} =: \mathbb{T}_{\mathbb{F}_p} = \prod_{\mathfrak{p}|p} \mathbb{T}_{\mathbb{F}_p,\mathfrak{p}}.$$

We can generate the prime ideals using the image of the reduced mod p Hecke eigenform $\bar{f}$, by the ring homomorphism map, that is:

$$\mathfrak{p}_f = \ker(\bar{f})$$

And have the natural surjection, that is also a ring homomorphism with kernel $\mathfrak{p}_f$ that goes to a residue field connecting the two residue degrees by commutative algebra, described below



$$\mathbb{T}_{\mathbb{F}_p,\mathfrak{p}}/\mathfrak{p} = \mathbb{T}_{\mathbb{F}_p}/\mathfrak{p}_\mathfrak{f} = \mathbb{T}_{\mathbb{F}_p}/ker(\overline{f}) \simeq Im(\overline{f}) = \mathbb{F}_p[a_n(f) \bmod \mathfrak{p}_f, n \in \mathbb{N}] \subseteq \mathcal{O}_{\mathbb{Q}_f}/\mathfrak{p}.$$

Taking into account that the last subset is an equaliy if the index of p divides $[\mathcal{O}_{\mathbb{Q}_f}/\mathfrak{p} : \mathbb{F}_p]$.

We can similarly read the argument backwards as follows. Let $\mathbb{T}_{\mathbb{F}_p} = \prod_\mathfrak{p} \mathbb{T}_{\mathbb{F}_p}, \mathfrak{p}$, we want to give meanings to the residue degrees. Fix a maximal ideal $\mathfrak{p}$ we have an associated map $\bar{f}$ to the ideal,

$$\begin{array}{ccccccc} \bar{f} : \mathbb{T}_{\mathbb{F}_p} & \xrightarrow{T_n \to \bar{f}(T_n)} & \mathbb{T}_{\mathbb{F}_p,\mathfrak{p}} & & & & \\ \uparrow\!\uparrow & & \downarrow & & & & \\ \mathbb{T}_{\mathbb{Z}} & & \mathbb{T}_{\mathbb{F}_p,\mathfrak{p}}/\mathfrak{p} & = & \mathbb{T}_{\mathbb{F}_p}/\mathfrak{p} & \subseteq & \bar{\mathbb{F}_p}. \end{array}$$

Proposition 3.3.1

Given a ring homomorphism $\bar{f} : \mathbb{T}_{\mathbb{Z}} \to \bar{\mathbb{F}_p}$ (or a smaller extension), we fix a $\pi : \overline{\mathbb{Z}} \twoheadrightarrow \overline{\mathbb{F}_p}$ then there exists a ring homomorphism $f : \mathbb{T}_{\mathbb{Z}} \to \overline{\mathbb{Z}} \subseteq \mathbb{C}$ such that $\mathbb{T}_{\mathbb{Z}} \underset{f}{\to} \overline{\mathbb{Z}} \underset{\pi}{\to} \overline{\mathbb{F}_p}$ equals f.

If f is a Hecke eigenform and $\bar{f}(T_n) = \pi(a_n(f))$ then we can write f as $\sum_n^\infty a_n(f)q^n = \sum_n^\infty f(T_n)q^n$ and we can think of $\pi(a_n(f)) = a_n(f) \bmod \mathfrak{p}$, for suitable $\mathfrak{p}$. We have the equalities

$$\mathbb{F}_p[\pi(a_n(f))|n \in \mathbb{N})] = \mathrm{Im}(\bar{f}) = \pi(\mathrm{Im}(f)).$$

And we also have the relations

$$\begin{array}{ccccccccc} \mathbb{Z} \subseteq \mathrm{Im}(f) = \mathbb{Z}[a_n(f)|n \in \mathbb{N}] & \subset & \mathcal{O}_{\mathbb{Q}_f} & \subset & \overline{\mathbb{Z}} & \subset & \mathbb{C} \\ & & \downarrow & \overset{\alpha}{\searrow} & \downarrow \pi & & \\ & & \mathcal{O}_{\mathbb{Q}_f}/\mathfrak{p} & \hookrightarrow & \overline{\mathbb{F}_p} & & \end{array}$$

that show that $Ker(\alpha) = \mathfrak{p}$.

Let's now assume that $\mathbb{T}$ is a commutative finite dimensional $\mathbb{F}_p$ algebra, with an $\mathbb{F}_p$ basis $T_1, ..., T_n$. If we let H be a subalgebra of $\mathbb{T}$, then H is local only if the minimal polynomial of each T_i is a power of an irreducible polynomial. Note that

Suppose now that it is local. Then, the residue field is the extension of $\mathbb{F}_p$ generated by the images of the basis elements, and the residue field is the splitting field of all the minimal polynomials f_i seen in the diagram below.

$$\begin{array}{ccccc} \mathbb{T} & \twoheadrightarrow & \mathbb{T}/\mathfrak{p} & = & \mathbb{F}_{p^d} \\ \cup & & & & \cup \\ T_i & \longmapsto & \mathbb{T}_i \bmod \mathfrak{p} & := & a_i \end{array}$$

We have that $0 = f_i^{e_i}(T_i) \implies f_i(a_i)^{e_i} = 0 \implies f_i(a_i) = 0$. A consequence is that over $\mathbb{F}_p$, there is a unique extension of a given degree, which is normal. The splitting field of the composition of the $\mathbb{F}_p[X]/(f_i(X)) = \mathbb{F}_{p^{d_i}}$,so it is equal to $\mathbb{F}_{p^d}$ where $d = lcm(d_1, \ldots, d_n)$ and d_i is the degree of the irreducible polynomial f_i.

Chapter 4

Experiments

In this chapter, we will be looking at calculations and observations made by studying the asymptotic behaviour of the maximal residue degree of primes $\mathfrak{p}$ in the coefficient field $\mathbb{Q}_f$ of Hecke eigenforms lying in $S_k^{new}(N, \mathbb{C})$.

We should note that we only made calculations for prime levels, and $N = 1$, as this allows us to calculate the newspace $S_k^{new}(N; \mathbb{C})$ quickly and at the same time we do not lose any information asymptotically.

The author made all the calculations using [14, Sagemath].

Golomb Dickman Constant

The motivation for our calculations came from the question: Is the maximal residue degree a_p of the Hecke algebra over $\mathbb{F}_p$ related to the expected average maximum length b_d of a cycle in a permutation in the permutation group $\mathcal{S}_d$? Here d is equal to $dim_{\mathbb{C}}(S_k(N; \mathbb{C}))/2$. The idea comes from the fact that if we pick a random polynomial with integer coefficient, it is irreducible and has Galois group equal to the full symmetric group $\mathcal{S}_d$ where d is the degree of the polynomial. The Hecke algebra for a normalized eigenform $f \in S_k^{new}(N : \mathbb{C})$ has a so called *Atkin-Lehner involution* that splits the algebra into two equally dimensional subalgebras. Other than that, we should not expect the space to break down any further unless there is a special reason for it to do so.

If p is unramified in $\mathbb{Q}_f$, then $Frob_p$ is well-defined up to conjugacy and can be viewed as an element of the permutation group. Then, by proposision 4.0.1 we can connect this $Frob_p$ to the residue degrees of prime ideals $\mathfrak{p}$ over p.

Proposition 4.0.1

Let M/K be a separable field extension of degree d, where K is a number field. Let $\mathfrak{p}$ be a prime of K and $\mathfrak{P}$ be a prime of L dividing $\mathfrak{p}$. We suppose that $\mathfrak{P}/\mathfrak{p}$ is unramified. Then the cycle lengths in the cycle decomposition of $Frob_{\mathfrak{P}/p} \in \mathcal{S}_d$ are precisely the residue degrees of the primes of M lying above $\mathfrak{p}$ [18].

Together with Chebotarev Density Theorem, as we vary p, we expect the maximal residue degree of primes $\mathfrak{p}$ over p in $\mathbb{Q}_f$ to be related to b_d where d is the degree of the number field $\mathbb{Q}_f$. We want to see what happens if we fix p and vary the weight or the level to see whether we can develop a similar statistical statement.

Golomb and Gaal [4] already studied the behaviour of the average maximal length of a cycle permutation. They noticed that if b_n is the average, taken over all the permutations of a set of n elements, of the longest cycle in each permutation. Then

$$\lambda := \lim_{n\to\infty} \frac{b_n}{n} \approx 0.6243\ldots.$$

This constant is called the *Golomb-Dickman constant* because of its relation to the Dickman function; it also appears in connection with the average size of the largest prime factor of an integer, that is

$$\lambda = \lim_{n\to\infty} \frac{\log(P_1(k))}{\log(k)},$$

where $P_1(k)$ is the largest prime factor of k.

We want to know if there is a similar relationship with the degree d of the cuspidal space $S_k(N;\mathbb{C})$ and the maximal residue degree a_p, of primes $\mathfrak{p}$ over some prime $p \in \mathbb{N}$. That is if there is a linear relationship. We should account for a factor of two since, for prime levels, an Atkin-Lehner involution splits the Hecke algebra into two equal-dimensional subspaces. We want to see if we have the relation

$$\lim_{N\to\infty} a_p(N)/dim_{\mathbb{C}}(S_k(N:\mathbb{C})) \sim \lambda/2.$$

4.1 Fixed Level

We first fixed the level $N = 1$ to use Maeda's conjecture. Plot 4.1 shows that for primes above 101, the maximal residue degree does not seem to go higher than 7, and the maximal residue degree of primes above 53 behaves similarly. The residue degrees do not exceed 4. Furthermore, the behaviour of the residue degree seems to become periodic after a certain point as we increase the weight. This can be explained by a Theorem by Jochnowitz [7] stating that if we know all eigenforms of level 1 and weight $\leq p+1$, then we essentially get all the eigenforms over $\mathbb{F}_p$ in all weights by multiplying those of low weights by A_p, where $A_p = 1$ is a modular form of weight $p-1$ and level 1 over $\mathbb{F}_p$.

Additionally, we performed experiments by fixing the level $N > 1$, see 4.2, and we noticed the same behaviour. After a certain point, the maximal residue degree does not increase. The plots lead us to believe that experiments with fixed weights might be more fruitful.

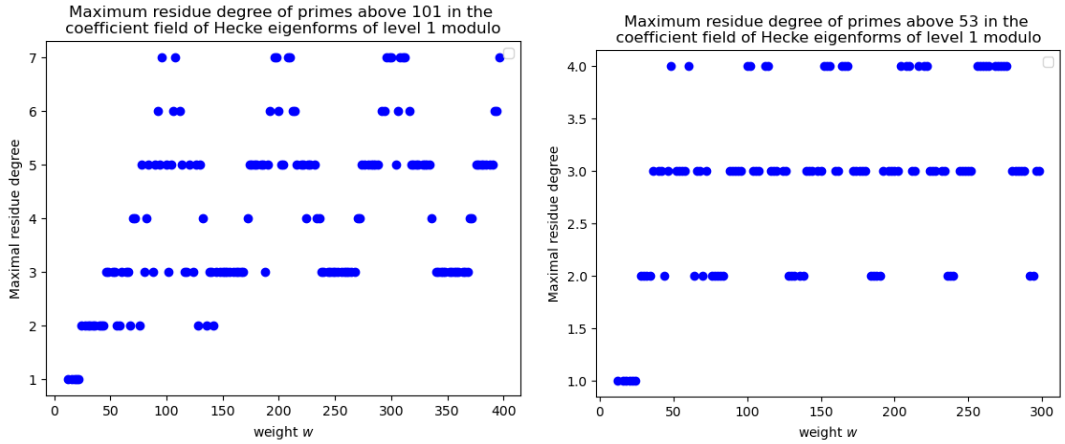


Figure 4.1: The asymptotic behaviour of the maximal residue degree of prime ideals in $\mathbb{Q}_f$ for level $N = 1$.

4.2 Fixed Weights

Calculating the residue degrees of primes in $\mathbb{Q}_f$ for modular forms f of levels ≥ 2 is more complex, so we will use the before-mentioned algorithms to calculate the residue degrees of the Hecke algebras instead.

When we calculated the residue degrees for Hecke algebras, with $f \in S_k(N, \mathbb{C})$ with a fixed weight k and prime p and varying level, we noticed a clear trend 4.3. The data points form a cone. We calculated the slopes of the lines that best fit our data. At a quick glance, the slopes do not follow any noticeable pattern. The slopes do not agree if we change the weight k or the prime p. However, if we fix p and plot the slope of the best-fit line for different weights, we notice a pattern, see 4.4. We get the same slope for different levels when the weight becomes big enough. This means that some chaotic behaviour occurs for low levels, but after a certain point, the behaviour becomes regular. This result is in the spirit of the generalized Maeda's conjecture. In addition, we plotted the value that the line seems to converge to against the prime p, see 4.4, and we got another interesting result. If we consider the weight k big enough, we get a relation that looks to depend linearly on p. We could conjecture that

$$\lim_{k\to\infty} \lim_{N\to\infty} \frac{a_p(N)}{N} \sim 0.0273p.$$

Given the time constraint, we could only calculate six data points. We would have to calculate deeper with respect to N and p to assert the relation confidently.

Next, we plotted the maximal residue degree divided by the dimension of $S_k(N, \mathbb{C})$, see 4.5. The distribution of points looks rather chaotic, but as we calculated the best-fit line, we got a clear, almost horizontal line. Supporting the idea that on average $\frac{a_p(N)}{S_k(N,\mathbb{C})}$ is a constant.

However, contrary to our predictions, the constant is not obviously related to the Golomb-Dickman constant. It is not even the same for different weights k, but if we plot the constant against the weight for a fixed p, see 4.6, we notice the graphs are similar for different p. Furthermore, the simple function $13/k$ is close to the plots we observe. Supporting the conjecture that the limit below is independent of p

and that

$$\lim_{n\to\infty} \sum_{N=1}^{n} \frac{a_p(N)/dim(S_k(N;\mathbb{C})}{n} \sim 13/k.$$

4.3 Future questions

Even though our heuristics were incorrect, we now understand that the structure of the coefficient field of normalized Hecke eigenforms is more complex than our first guess. We want to be able to understand this behaviour. The next step would be to gather more data points to see if the limiting behaviour of the slopes $a_p(N)/N$ continues even if we calculate large weights. It would also be interesting to see if the relation

$$\lim_{k\to\infty} \lim_{N\to\infty} \frac{a_p(N)}{N} \sim 0.0273p.$$

holds for bigger primes. We would also like to understand why we seem to get the relation

$$\lim_{n\to\infty} \sum_{N=1}^{n} \frac{a_p(N)/dim(S_k(N;\mathbb{C})}{n} \sim 13/k.$$

To better understand the Hecke algebra, we could calculate the Galois group of the minimal polynomial of Hecke operators and find some patterns to explain our observed behaviour.

We could also study the average residue degree instead of the maximal residue degree. We could also look at modular forms with respect to $\Gamma_0(N)$ with a character. Furthermore, we could look at modular forms with respect to $\Gamma_1(N)$. However, this will become computationally much more expensive since the dimension of the space grows by a squared factor contrary to a linear factor when working with $\Gamma_0(N)$. Before making generalizations, we should aim to understand the behaviour for the simplest case.

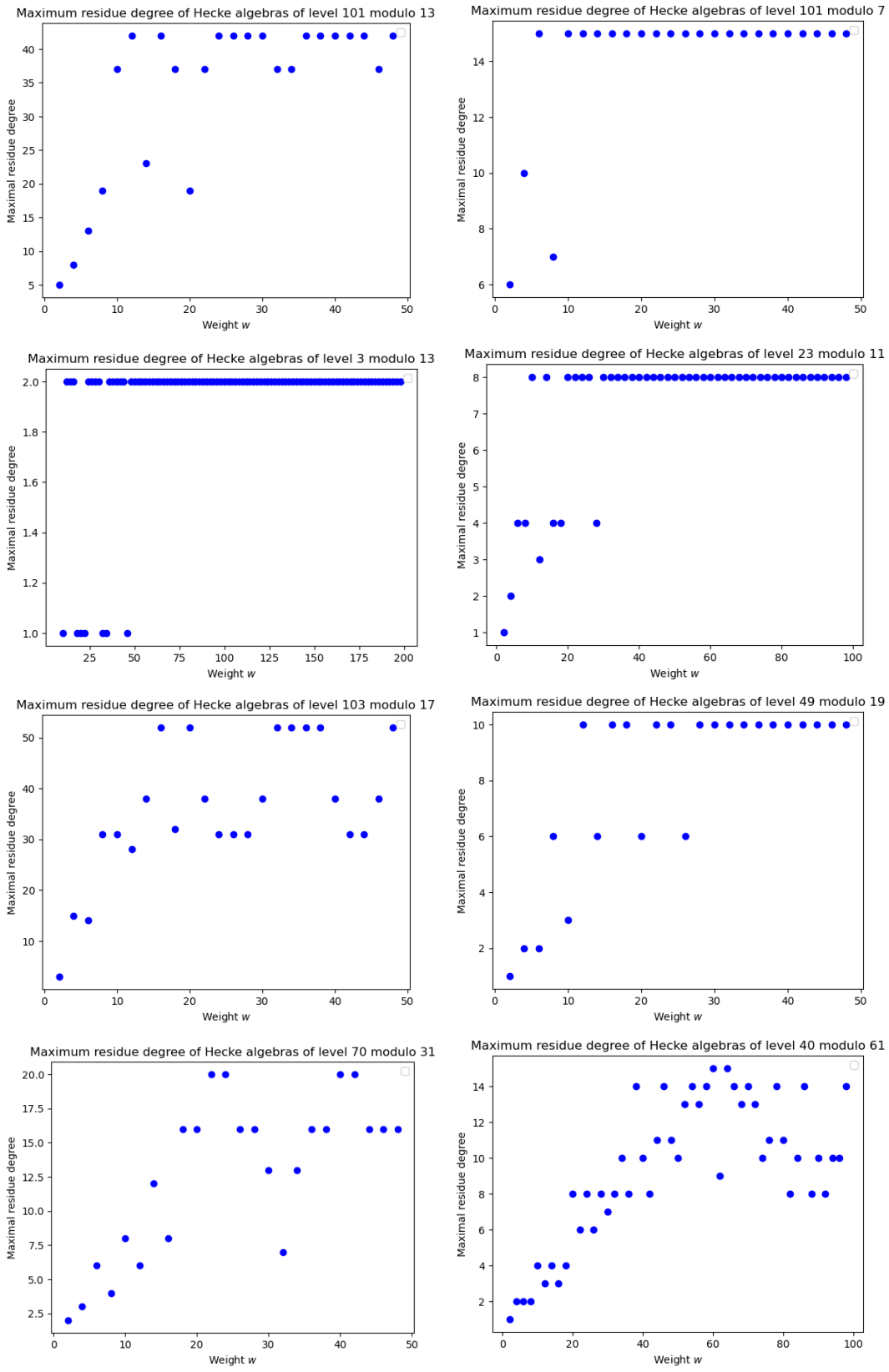


Figure 4.2: Plots of fixed level and varying weights

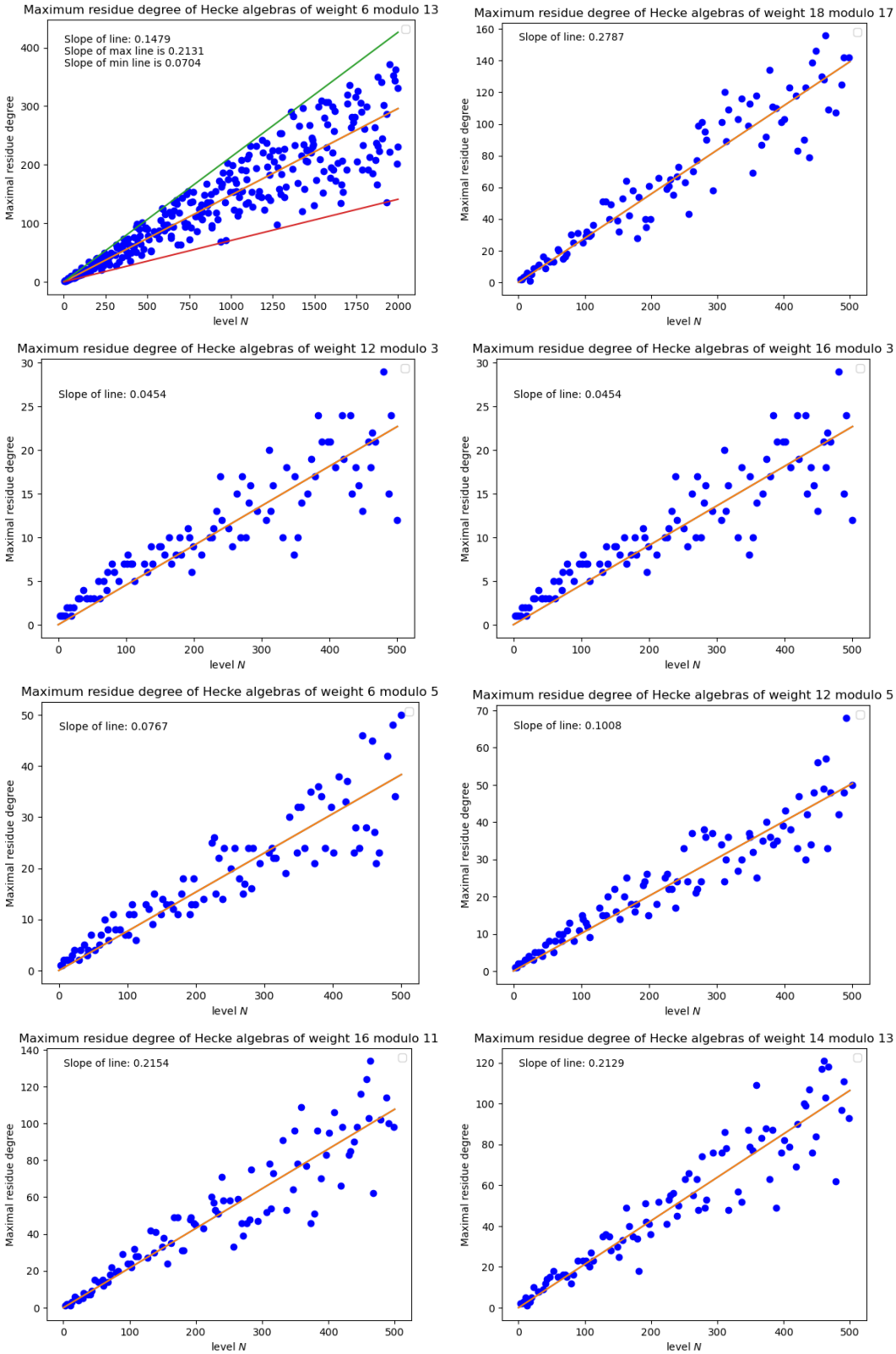


Figure 4.3: Fixed weight and varying levels

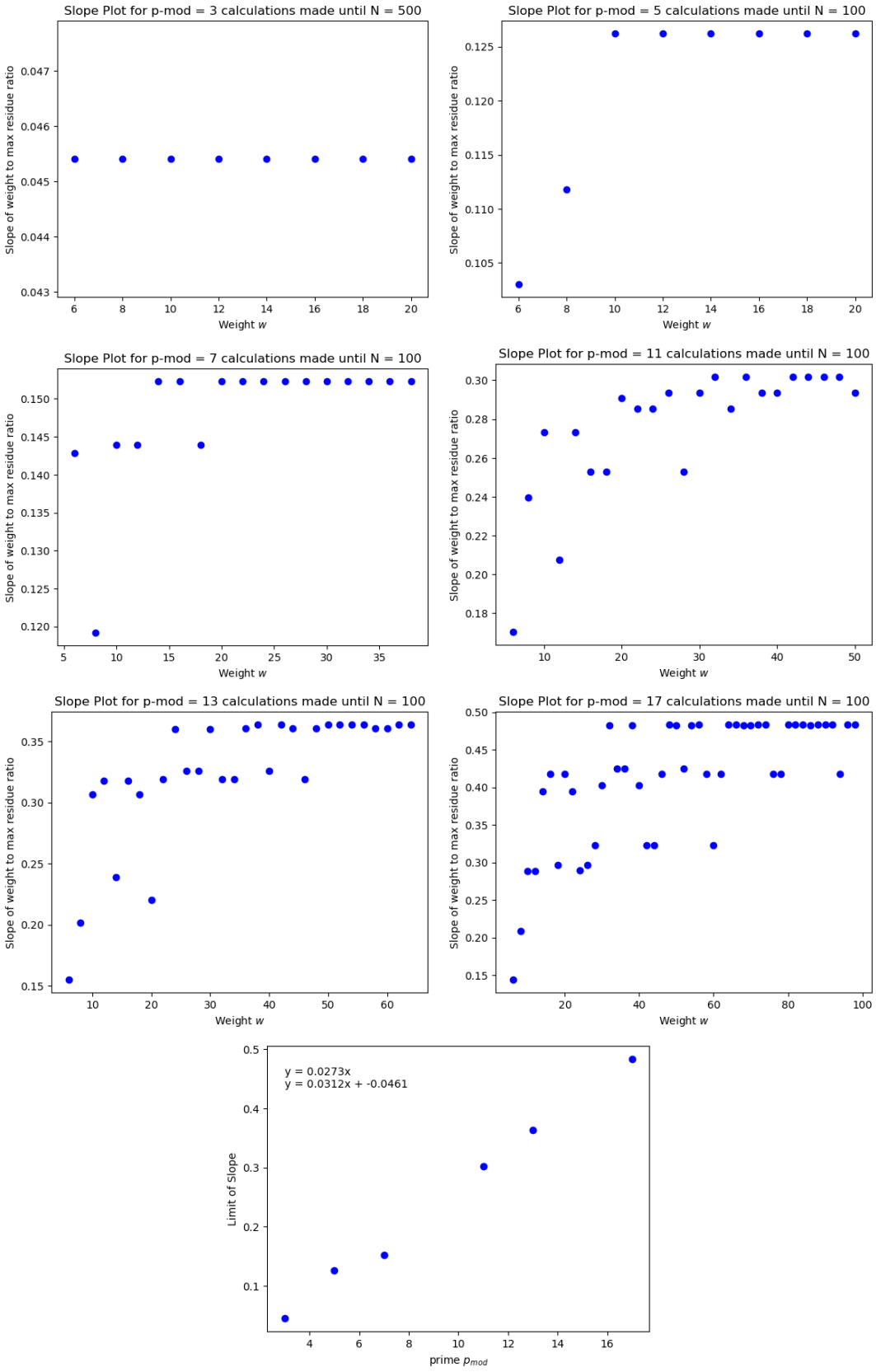


Figure 4.4: Slopes, fixed prime varying weights

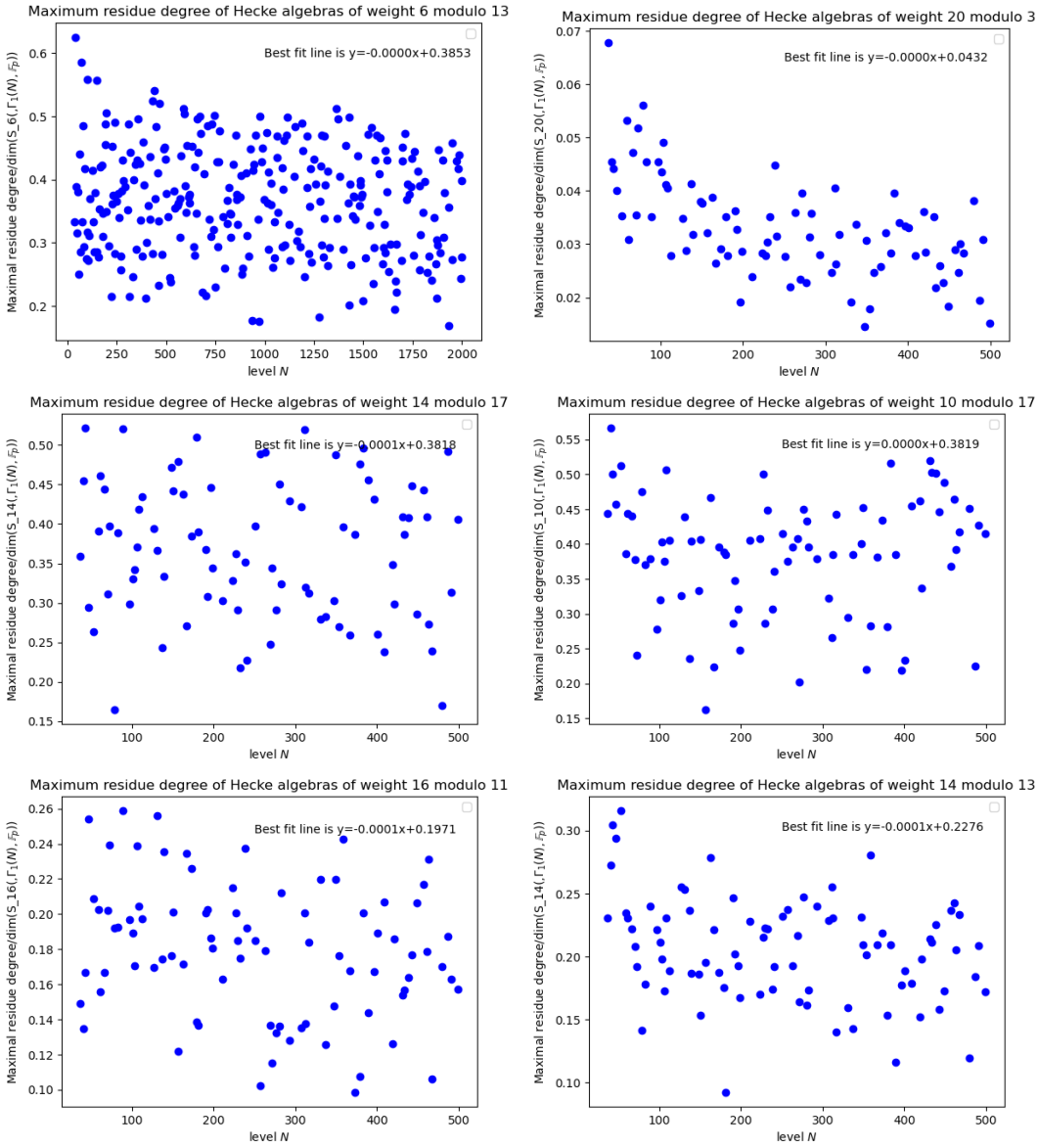


Figure 4.5: Normalized plots of fixed level and varying weights

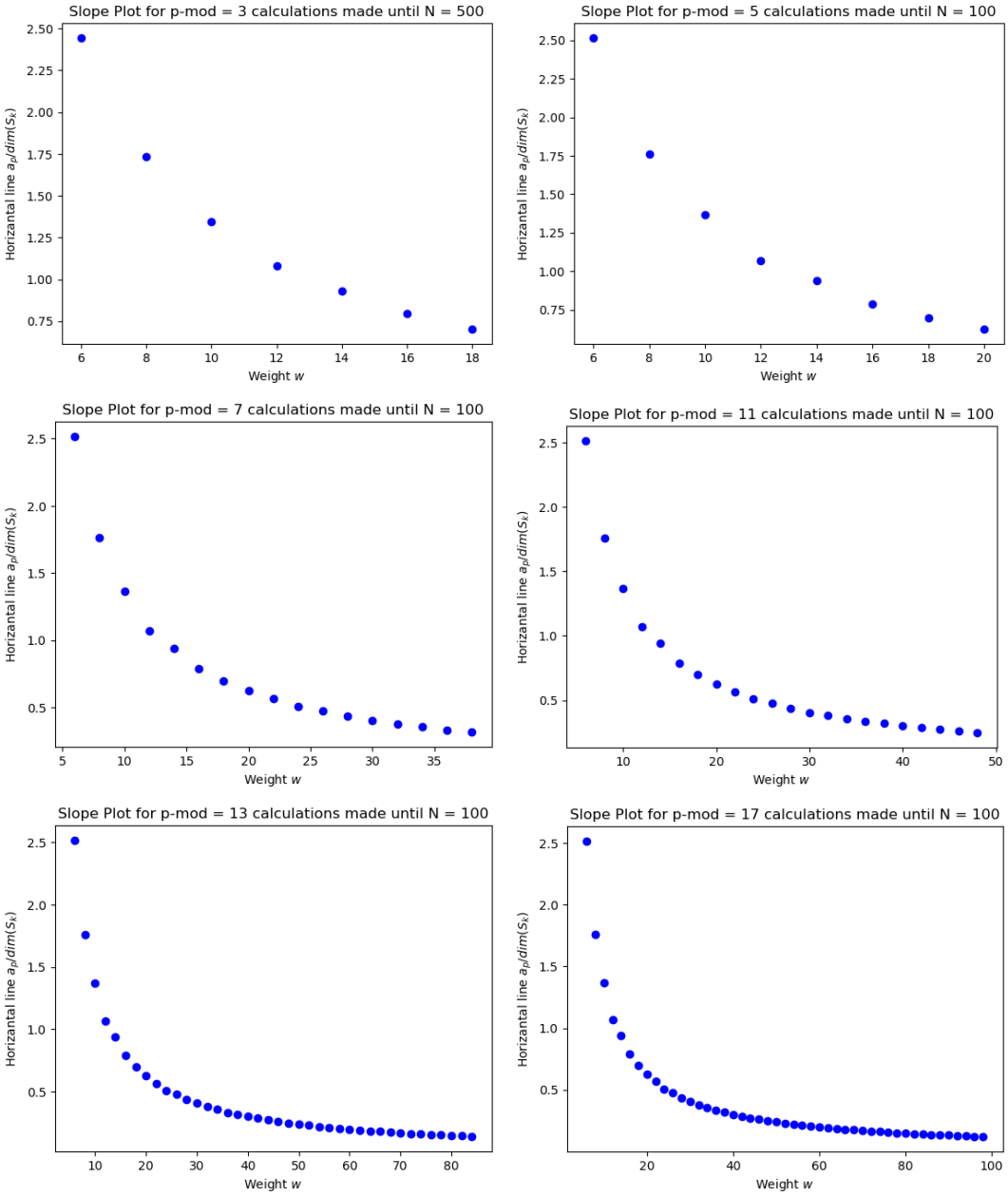


Figure 4.6: The average of $a_p/dim(S_k)$, fixed prime varying weights

Bibliography

[1] Ghitza A. and A. McAndrew. *Experimental evidence for Maeda's conjecture on modular forms*. 2012. arXiv: 1207.3480 [math.NT].

[2] H. Cohen. *A Course in Computational Algebraic Number Theory*. Graduate Texts in Mathematics. Springer Berlin Heidelberg, 2013.

[3] F. Diamond and J. Shurman. *A First Course in Modular Forms*. Graduate Texts in Mathematics. Springer New York, 2006.

[4] S.W. Golomb and P. Gaal. *Probabilistic methods in discrete mathematics: Proceedings of the Fourth international petrozavodsk conference, Petrozavodsk, Russia, June 3-7, 1996*. VSP, 1996, pp. 211–218.

[5] H. Hida and Y. Maeda. "Non-abelian base change for totally real fields." In: *Pacific Journal of Mathematics, (Special Issue)* (1997), pp. 189–217.

[6] I. Inam and E. Büyükaşık. *Notes from the International Autumn School on Computational Number Theory*. Tutorials, schools, and workshops in the mathematical sciences. Springer International Publishing, 2019.

[7] N. Jochnowitz. "Congruences Between Systems of Eigenvalues of Modular Forms". In: *Transactions of the American Mathematical Society* 270.1 (1982), pp. 269–285. URL: http://www.jstor.org/stable/1999772.

[8] L.J.P. Kilford. *Modular Forms: A Classical and Computational Introduction*. Imperial College Press, 2008.

[9] T.K. Koopa, W.A Stein, and G. Wiese. "On the generation of the coefficient field of a newform by a single Hecke eigenvalue". en. In: *Journal de théorie des nombres de Bordeaux* 20.2 (2008), pp. 373–384. DOI: 10.5802/jtnb.633.

[10] S. Lang. *Introduction to Modular Forms*. 2001.

[11] K. Martin. "An on-average Maeda-type conjecture in the level aspect". In: *Proceedings of the American Mathematical Society* 149.4 (Feb. 2021), pp. 1373–1386.

[12] A. McAndrew. "Maeda's Conjecture on Elliptic and Siegel Modular Forms". Available at http://math.bu.edu/people/angusmca/Research/Thesis_1.pdf. PhD thesis. The University of Melbourne, Nov. 2013.

[13] T. Miyake and Y. Maeda. *Modular Forms*. Springer Monographs in Mathematics. Springer Berlin Heidelberg, 2006.

[14] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version x.y.z)*. 2023. URL: https://www.sagemath.org.

[15] J.P. Serre. *A course in arithmetic*. Springer, 1993.

[16] W.A. Stein. *Modular Forms, a Computational Approach*. Graduate studies in mathematics. American Mathematical Society, 2007. ISBN: 9780821839607.

[17] J.G. Thompson. "Hecke operators and non congruence subgroups". In: *Proceedings of the Singapore Group Theory Conference held at the National University of Singapore, June 8–19, 1987*. Ed. by Kai N. Cheng and Yu K. Leong. Berlin, Boston: De Gruyter, 1989, pp. 215–224. DOI: doi:10.1515/9783110848397-016.

[18] G. Wiese. *An Application of Maeda's Conjecture to the Inverse Galois Problem*. 2013. arXiv: 1210.7157 [math.NT].

[19] G. Wiese. "Modular Forms of Weight One Over Finite Fields". Available at https://math.uni.lu/wiese/thesis/Thesis.pdf. PhD thesis. Universiteit Leiden, Oct. 2005.