Level p paramodular congruences of Harder type

Daniel Fretwell

School of Mathematics and Statistics,
University of Sheffield.

Submitted for the degree of Doctor of Philosophy (Mathematics), under the supervision of Dr Neil Dummigan.

March 2015

Abstract

In this thesis we will produce and investigate certain congruences, as predicted by Harder, between Hecke eigenvalues of Siegel and elliptic modular forms. Such congruences form a natural generalisation of the famous 691 congruence of Ramanujan. The moduli of our congruences will come from critical values of L-functions of elliptic modular forms.

In particular we will be interested in congruences between level p paramodular Siegel forms and $\Gamma_0(p)$ elliptic forms. Evidence for such congruences in these cases is rare (the only known examples being of level 2, due to Bergström et al).

In order to simplify matters on the Siegel side we move into spaces of algebraic modular forms for the group $\mathrm{GU}_2(D)$ for a quaternion algebra $D/\mathbb{Q}$ ramified at p, ∞. Here we can use a web of conjectures and results due to Ibukiyama along with trace formulae of Dummigan to produce Hecke eigenvalues of level p paramodular forms (allowing the congruences to be tested with ease). I provide new algorithms for finding explicit descriptions of these spaces of algebraic forms.

In order to provide justification for the paramodular nature of the congruence we will also consider the interplay between associated Galois representations and automorphic representations.

Acknowledgements

I would of course like to start by thanking my supervisor Neil Dummigan for simply being there in any way possible during the last 4 years. His faith in me has never diminished and I have learned so much from our discussions. I definitely have to admire his patience while this thesis was written at snail's pace!

Also I would like to thank Günter Harder for the continued interest in my work. It was both an honour and a pleasure to be invited to Bonn to meet such an established name in number theory. Many useful discussions provided me with plenty of avenues of future thought that I am grateful for.

A warm thanks goes to Andrew Jones, my closest colleague in the Number Theory group. His continued friendship and academic support during this time has been strong. What's more, his appetite for Yorkshire puddings at the University Arms is a close match for my own! It was my pleasure to attend Andrew's wedding recently and I wish both him and Jessica a wonderful life together.

I would like to also extend my thanks to the rest of the Number Theory group at Sheffield; Tobias Berger, Frazer Jarvis, Jayanta Manomarhayum, Haluk Sengun, David Spencer, Rudolph Chow, Tim Eardley, Konstantinos Tsaltas. I consider the group more a family and it has been great to see so much passion and insight for the subject.

Finally I wish to thank my family for constant support and encouragement throughout my life, in particular the last 4 years.

Contents

Introduction

Congruences between modular forms have been found and studied for many years. Perhaps the first interesting example is found in the work of Ramanujan. He studied in great detail the Fourier coefficients $\tau(n)$ of the discriminant function $\Delta(z)$, the first known example of a cusp form (appearing at weight 12).

Many of his observations about the τ function were originally thought to be mysterious, since at the time the theory of modular forms was still blossoming. Amongst the observations was a pretty congruence:

$$\tau(n) \equiv \sigma_{11}(n) \bmod 691.$$

Here $\sigma_{11}(n) = \sum_{d|n} d^{11}$ is a power divisor sum, a concrete number theoretic function. Ramanujan found many other congruences for the τ function but this one has become popular in the literature.

Viewed as an ad hoc result one can easily check this congruence computationally. In fact by the Sturm bound for modular forms one only needs to check this congruence holds for finitely many n in order prove it holds for all n. But much more is hidden within this congruence that is not revealed by this proof.

Natural questions arise; can we explain the occurrence of 691 in the modulus and why does $\sigma_{11}(n)$ appear? These questions can be answered by studying other proofs of the congruence. This is analogous to the folklore that an inductive proof rarely explains why a particular result exists, only other proofs will give satisfaction.

Indeed one can instead prove the congruence by not just studying the modular form Δ but the entire space of weight 12 modular forms. In doing so we link Δ with an Eisenstein series E_{12}. Hidden in the Fourier coefficients of E_{12} are the quantities $\sigma_{11}(n)$ and $B_{12} = -\frac{691}{2730}$ (the 12th Bernoulli number). Both questions are answered immediately!

Of course the true incarnation of the Bernoulli numbers here is via values of the Riemann zeta function. It is really $\zeta(12)$ that manifests itself, and that the prime 691 divides the "rational part" $\frac{\zeta(12)}{\pi^{12}} \in \mathbb{Q}$.

Since the work of Ramanujan there have been many generalizations of his congruences. Indeed by looking for primes dividing numerators of Bernoulli numbers one can provide similar congruences at level 1 between cusp forms and Eisenstein series for other weights.

In fact one can even give "local origin" congruences between higher level cusp forms and level 1 Eisenstein series by extending the divisibility criterion to include not just Bernoulli numerators but Euler factors of $\zeta(s)$ (see [20] for results and examples).

Given the above we would believe intuitively that congruences are determined by primes dividing L-values. But why should we care about congruences between modular forms? There are many reasons.

Firstly it is known that we can attach Galois representations to many types of modular form [69]. Congruences of the above type tell us a wealth of information about the associated Galois representation, such as the composition factors of certain of its residual representations. Since Galois representations have become an integral part of number theory (for example in studying elliptic curves) it is an advantage to know this information.

Another interest in congruences is in providing evidence for the Bloch-Kato conjecture [20]. This is a far-reaching generalization of many classical results and conjectures, such as the analytic class number formula for number fields and the Birch Swinnerton-Dyer conjecture for elliptic curves. The existence of congruences allows us to predict the existence of non-trivial elements in certain Shafarevich-Tate groups with prescribed orders. In the case of Ramanujan style congruences we recover the classical result that p-divisibility of Bernoulli numbers is linked with p-divisibility of class numbers of cyclotomic number fields (the existence of such a congruence allows us to construct an element of order p in the ideal class group). In generality these are interesting problems to us since Shafarevich-Tate groups are highly non-trivial to study (for the case of elliptic curves it is not even known if this group is finite).

Computationally we would like to have congruences in order to be able to efficiently calculate and study Fourier coefficients of forms. For example if one knows Ramanujan's congruence then one can conclude that $\tau(n) \neq 0$ for all n such that $691 \nmid \sigma_{11}(n)$. This gives an overwhelming amount of evidence for Lehmer's conjecture, that $\tau(n) \neq 0$ for all n.

There are also many types of congruences predicted between Hecke eigenvalues of genus 2 Siegel cusp forms and Eisenstein series. One particular type was conjectured to exist by Harder (made explicit in his 2002 paper, found in [31]). These congruences were originally predicted by studying the Hecke action on boundary cohomology of Siegel modular varieties. Evidence is known for level 1 forms (see Van der Geer's article in [9]) but is much rarer for higher levels (only level 2 evidence is known by Bergstrom et al and has been gained by methods

specific to this level [4]). One specific level 1 example of the congruence has been proved in a paper by Chenevier and Lannes (p.386 of [14]).

It should be noted that such congruences are more naturally described in terms of eigenvalues of Hecke operators acting on cuspidal automorphic representations of GSp_4 and on certain representations induced from its Borel subgroup (an Eisenstein like object). The modulus of the congruence comes as usual from an L-value, not from $\zeta(s)$ but from the L-function attached to the genus 1 form.

A big stumbling block in checking higher genus congruences is in trying to calculate Hecke eigenvalues for the Siegel forms. For elliptic forms there are certainly a wealth of efficient methods and lots of extensive tables exist. One can use the method of modular symbols, a computational way to utilize the cohomological view of modular forms due to Eichler-Shimura. Alternatively one can use correspondences due to Eichler and Jacquet-Langlands, allowing transfer of certain elliptic modular forms into modular forms for quaternion algebras. This method is well understood and studied. (We shall see this in detail in this thesis).

Given the need to find Hecke eigenvalues of Siegel modular forms one would hope that these methods would generalize to higher genus. Unfortunately the modular symbols method has not been developed enough to tackle higher genus forms. There is work in progress in this area, the theory of sharblies (see Gunnells' appendix in [62]) but these objects are not yet understood enough for computation.

However there are conjectural generalizations of the Eichler correspondence to higher genus due to Ibukiyama [37]. These are theoretical results which are not immediately susceptible to computation. A big chunk of the work done in this thesis has been to make these results computationally feasible, giving algorithms and explicit descriptions of all objects involved.

In this thesis I will provide new evidence for a level p version of Harder's conjecture for various small primes (including $p = 2$ but not exclusively). The Siegel forms will be of paramodular type and the elliptic forms will be of $\Gamma_0(p)$ type. Towards the end of the thesis I will justify my paramodular expectations by comparing Galois and automorphic representations.

Chapter 1 contains a brief overview of the theories of elliptic and Siegel modular forms. We see definitions of these objects as well as Hecke operators and classical results. A brief discussion of L-functions attached to elliptic modular forms is necessary too. Finally we end with a section giving precise statements of Harder's congruences.

Chapter 2 contains an overview of the theory of quaternion algebras. We give their definition as well as definitions of the associated norms, traces, maximal orders. Also given are well known theorems on classification of quaternion

algebras over $\mathbb{Q}$ via their ramification.

Chapter 3 contains a brief discussion of the theory of automorphic forms. Based on this we motivate spaces of algebraic modular forms and give some interesting results (in particular the trace formula). As an application we give the classical correspondence of Eichler between certain spaces of elliptic modular forms and algebraic forms for quaternion algebras. As a bonus we see a thorough computational example of this correspondence, motivating techniques used later. Finally we see Ibukiyama's correspondence as a generalization of the one given by Eichler. This result is important and so is discussed in great detail.

Chapter 4 contains the computational aspects of the work. Using the material in Chapter 3, I give algorithms for calculating the necessary spaces of algebraic forms, as well as Hecke representatives and dimensions. These are non-trivial calculations and in my case have never been seen in the literature. Finally I put everything together and give three different examples of level 3 congruences found via these calculations.

Chapter 5 contains a theoretical justification for why I expect a level p version of Harder's conjecture to mostly work for paramodular forms. Here I have to use Galois representations and automorphic representations and so we briefly review these as well as the Local Langlands Correspondence that unites the two. Finally I give similar justification for why I did not find congruences of "local origin" predicted by Harder.

The appendices contain tables of newform dimensions, congruences found as well as a discussion of how the work may be strengthened or continued in the future.

Chapter 1

Modular forms

1.1 Elliptic modular forms

The classical theory of elliptic modular forms began around 200 years ago but their secrets continue to be discovered. They have many uses:

- They contain mysterious links with elliptic curves and Galois representations. The famous modularity theorem implies that the Fourier series of particular modular forms contain arithmetic information on solution counts of elliptic curves modulo primes. It was mainly this link that allowed Fermat's Last Theorem to finally be solved.

- They have found uses in the theory of lattices. Given an integral lattice we may associate to it a modular form called a theta series. This modular form encodes data about the number of vectors of a given norm.

- Modular forms can be attached to quadratic forms to get what are also called theta series. The Fourier coefficients here measure representability of quadratic forms by integers. As an example of this one can study representations of numbers as sums of squares and get quantitative and asymptotic formulae. Since norm forms of lattices give quadratic forms these theta series are the same as the ones above.

- We can study (regular) sphere packings by studying lattices and hence modular forms. In fact given what little we can prove about questions such as optimum packings and the kissing problem, we do happen to be able to solve a lot of problems in 24 dimensions. This is due to the ability to create lattices with nice theta series (for example the Leech lattice).

- They can be used to form non-trivial relationships between arithmetic functions, such as power divisor sums $\sigma_k(n) = \sum_{d|n} d^k$. This is possible due to finite dimensionality results.
- They have found their uses in physics, notably in studying string theory.
- Modular forms are the stepping stone to higher objects such as automorphic forms and automorphic representations.

In this section we will see an overview of the theory of elliptic modular forms. We will define them, see examples of them along with results such as finite dimensionality and the existence of special bases. Many standard references will be used such as [19],[46],[62].

The classical theory starts with a particular group action, namely:

Lemma 1.1.1. *The group $SL_2(\mathbb{R}) = \{A \in M_2(\mathbb{R}) \mid det(A) = 1\}$ acts transitively on the upper half plane $\mathcal{H} = \{z \in \mathbb{C} \mid Im(z) > 0\}$ by Möbius transformations,*

i.e. if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{R})$ then

$$(\gamma, z) \longmapsto \gamma z = \frac{az + b}{cz + d}$$

defines a group action.

Transitivity follows since it is easy to show that $i \in \mathcal{H}$ has full orbit. What is the stabilizer of this element?

Theorem 1.1.2. *The stabilizer of i under the action of $SL_2(\mathbb{R})$ is:*

$$SO_2(\mathbb{R}) := \{A \in SL_2(\mathbb{R}) \mid AA^T = I\} = \left\{ \begin{pmatrix} cos(\theta) & sin(\theta) \\ -sin(\theta) & cos(\theta) \end{pmatrix} \middle| \, 0 \leq \theta < 2\pi \right\}.$$

Now that we know the stabilizer we can get an alternate way of describing the upper half plane by a simple use of the Orbit-Stabilizer theorem (noting also the continuity of the group action)

Corollary 1.1.3. *We have that $\mathcal{H} \cong SL_2(\mathbb{R})/SO_2(\mathbb{R})$ as an isomorphism of topological spaces.*

Given an action of a topological group G on a space X we might then be interested in well behaved functions on that space that are invariant under the action, i.e. $f : X \longmapsto \mathbb{C}$ such that $f(\gamma z) = f(z)$ for all $\gamma \in G$.

The above lemma really tells us that this is a trivial matter for the case of $G = \mathrm{SL}_2(\mathbb{R})$ and $X = \mathcal{H}$. By the transitivity of the action we would see that

any such function is constant, defined by its value at one particular point (say by $f(i)$).

However, if we instead look at the action of subgroups of $\mathrm{SL}_2(\mathbb{R})$ then it is possible that non-trivial examples arise. We tend to study the action of certain subgroups of arithmetical significance. One popular choice is $\mathrm{SL}_2(\mathbb{Z})$.

1.1.1 Modular forms for $\mathrm{SL}_2(\mathbb{Z})$

First we examine the case where we have invariance under the action of $\mathrm{SL}_2(\mathbb{Z})$.

Definition 1.1.4. Let $f : \mathcal{H} \longrightarrow \mathbb{C}$ be meromorphic. Then f is a weakly modular function if $f(\gamma z) = f(z)$ for each $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. □

We note since the matrix $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ any weakly modular function satisfies $f(Tz) = f(z+1) = f(z)$, i.e. f is periodic of period 1. Then f has a complex Fourier series of the form:

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

where:

$$a_n = \frac{1}{2\pi} \int_{-1}^{1} f(x) e^{-2\pi i n z} dz.$$

We often substitute $q = e^{2\pi i z}$, giving a more pleasant expression:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n.$$

Definition 1.1.5. This series expansion is called the "q-expansion" of f. □

The study of weakly modular functions first arose from the theory of elliptic curves. Recall that an elliptic curve over a field K is a non-singular projective curve E/K of genus 1 with a specified base point $\mathcal{O} \in E(K)$.

Whenever K is a subfield of $\mathbb{C}$ we can give the Lie group $E(\mathbb{C})$ the structure of a torus, i.e. there exists an isomorphism of Lie groups $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$ for some lattice Λ. The $\mathbb{C}$-isomorphism class of E is determined by the j-invariant of the curve. We define $j(z)$ to be the j-invariant of any elliptic curve having period lattice equivalent to $\mathbb{Z} \oplus \mathbb{Z}z = \langle 1, z \rangle$.

Omitting the details we find that the j-function is weakly modular and has the following q-expansion:

$$j(z) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + 20245856256q^4 + ...$$

Thus non-trivial weakly modular functions exist. Surprisingly there aren't any more interesting examples.

Theorem 1.1.6. *The $\mathbb{C}$-algebra of weakly modular functions is isomorphic to $\mathbb{C}(j)$, the field of rational functions in j.*

One can find a proof of this on p.73 of [19].

The j-function has many remarkable properties. One spectacular property is that the coefficients of its q-expansion give information on dimensions of the irreducible representations of the Monster group, the largest of the sporadic finite simple groups [12].

Let f be a weakly modular function. As we have seen we have a q-expansion:

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n.$$

We are interested in the behaviour of f "at infinity", i.e. $\lim_{y\to\infty} f(iy)$.

Note that the map $q : z \mapsto e^{2\pi iz}$ transforms the upper half plane $\mathcal{H}$ into the punctured unit disc $D' = D\backslash\{0\}$, where $D = \{q \in \mathbb{C} \,|\, |q| < 1\}$. We can thus think of q as being a local parameter of $\mathcal{H}$ "at infinity" and we observe that the above limit is interpreted as the "value" of the q-expansion at $q = 0$.

Definition 1.1.7. If $a_{-n} = 0$ for all $n \in \mathbb{N}$ then we say that f is holomorphic at infinity. If f is holomorphic on $\mathcal{H}$ and at infinity then f is called a modular function. □

Note that the j-function is not a modular function since the q-expansion reveals a simple pole at infinity.

Modular functions are much nicer functions than weakly modular functions due to being well behaved at infinity. In fact they are so nice that no interesting examples exist.

Corollary 1.1.8. *The $\mathbb{C}$-algebra of modular functions is isomorphic to $\mathbb{C}$, i.e. only the constant functions are modular functions.*

Since we have exhausted the possibilities for modular functions we weaken the invariance property in order to create modular forms.

Definition 1.1.9. A weakly modular form of weight $k \in \mathbb{Z}$ is a holomorphic function $f : \mathcal{H} \longrightarrow \mathbb{C}$ such that $f(\gamma z) = (cz+d)^k f(z)$ for each $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. □

The function $j(\gamma, z) = (cz + d)$ is often referred to as the automorphy factor. The reason why this should be included in the definition is not obvious here but soon we will see that it is a good choice for capturing interesting examples.

It is apparent that weakly modular forms of weight $k = 0$ are exactly the holomorphic weakly modular functions. Notice that any weakly modular form has a q-expansion too (by the same argument as before). Thus it still makes sense to be holomorphic at infinity.

Definition 1.1.10. A modular form of weight k is a weakly modular form of weight k that is holomorphic at infinity. □

One imagines that showing a function is a modular form is a tough thing to do since it must be shown that the function transforms correctly for every matrix in $\mathrm{SL}_2(\mathbb{Z})$. However this is not so bad since $\mathrm{SL}_2(\mathbb{Z})$ is finitely generated. A popular set of generators is given by $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. So in practice it suffices to show that $f(-\frac{1}{z}) = z^k f(z)$ and $f(z+1) = f(z)$ (along with holomorphicity of course).

Although the values taken by modular forms are not invariant under the action of $\mathrm{SL}_2(\mathbb{Z})$ on $\mathcal{H}$ we can rewrite the definition so as to introduce some notion of invariance. Note that $\mathrm{SL}_2(\mathbb{R})$ acts on functions $f : \mathcal{H} \to \mathbb{C}$ via the weight k slash operator (for $k \geq 0$):

$$(f|_k\gamma)(z) = j(\gamma, z)^{-k} f(\gamma z).$$

Proposition 1.1.11. *A holomorphic function $f : \mathcal{H} \to \mathbb{C}$ is weakly modular of weight k if and only if $f|_k\gamma = f$ for all $\gamma \in SL_2(\mathbb{Z})$.*

It is clear that the set of modular forms of a given weight k forms a $\mathbb{C}$-vector space. We will denote this space by $M_k(\mathrm{SL}_2(\mathbb{Z}))$. We need to reference $\mathrm{SL}_2(\mathbb{Z})$ because soon we will see a more general definition of modular form, requiring the transformation law to work for other interesting subgroups of $\mathrm{SL}_2(\mathbb{R})$.

For certain values of k we can see easily that there are no modular forms.

Lemma 1.1.12. *If $k < 0$ or k is odd then we have $M_k(SL_2(\mathbb{Z})) = \{0\}$.*

Proof. The first claim follows from the holomorphicity requirements of f and the second follows from the fact that $-I \in \mathrm{SL}_2(\mathbb{Z})$. □

We may also multiply two modular forms (of possibly different weights) and get another modular form. More precisely:

Lemma 1.1.13. *If $f \in M_k(SL_2(\mathbb{Z}))$ and $g \in M_l(SL_2(\mathbb{Z}))$ then the product satisfies $fg \in M_{k+l}(SL_2(\mathbb{Z}))$.*

Thus the space $M(SL_2(\mathbb{Z})) = \oplus_{k=0}^{\infty} M_k(SL_2(\mathbb{Z}))$ *has the structure of a graded* $\mathbb{C}$*-algebra.*

Proof. Holomorphicity is clear. Let $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. Then:

$$(fg)|_{k+l}\gamma = (f|_k\gamma)(g|_l\gamma) = fg.$$

□

Later we will see that this $\mathbb{C}$-algebra has a simple structure. However we have not yet seen any non-trivial examples of modular forms. Fortunately an infinite family of examples readily exists.

Definition 1.1.14. For $k \in \mathbb{Z}$ we consider the weight $2k$ Eisenstein series:

$$G_{2k}(z) = \sum_{(m,n)\in\mathbb{Z}\times\mathbb{Z}\setminus\{(0,0)\}} \frac{1}{(mz+n)^{2k}}.$$

□

Theorem 1.1.15. *Let* $k \geq 2$*. Then* G_{2k} *is absolutely convergent, holomorphic on* $\mathcal{H}$ *and at infinity. Further* $G_{2k} \in M_{2k}(SL_2(\mathbb{Z}))$*.*

Naturally we wish to know what the q-expansion of G_{2k} is. A simple calculation shows that $\lim_{t\to\infty} G_{2k}(it) = 2\zeta(2k)$ but the rest of the expansion is as follows (p.5 of [19]):

Theorem 1.1.16. *For* $k \geq 2$*:*

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

where $\zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$ *and* $\sigma_{2k-1}(n) = \sum_{d|n} d^{2k-1}$*.*

The coefficients of the above q-expansion contain a lot of arithmetic data. This is a common theme in the theory of modular forms; by definition they are tools of complex analysis but hidden in their q-expansion are many things of number theoretic interest.

Recall the following formula for $\zeta(2k)$:

$$\zeta(2k) = \frac{(-1)^{k+1}B_{2k}(2\pi)^{2k}}{2(2k)!},$$

where $B_{2k} \in \mathbb{Q}$ are the Bernoulli numbers, defined by the generating series $\frac{t}{e^t-1} = \sum_{m=0}^{\infty} B_m\frac{t^m}{m!}$.

Using the formula there is an alternate form of the q-expansion given by:

$$G_{2k}(z) = 2\zeta(2k)\left(1 - \frac{4k}{B_{2k}}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n\right).$$

Since $\zeta(\sigma) \neq 0$ for $\sigma > 1$ the constant terms of the G_k are all non-zero. So we can normalize to produce constant term 1.

Definition 1.1.17. For $k \geq 2$ the weight $2k$ normalized Eisenstein series is:

$$E_{2k}(z) = \frac{G_{2k}(z)}{2\zeta(2k)} \in M_{2k}(\mathrm{SL}_2(\mathbb{Z})).$$

□

It is clear that for $k \geq 2$ the normalized Eisenstein series have q-expansion:

$$E_{2k}(z) = 1 - \frac{4k}{B_{2k}}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n.$$

So for example:

$$E_4(z) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n$$

$$E_6(z) = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n$$

$$E_8(z) = 1 + 480\sum_{n=1}^{\infty}\sigma_7(n)q^n$$

$$E_{10}(z) = 1 - 264\sum_{n=1}^{\infty}\sigma_9(n)q^n$$

$$E_{12}(z) = 1 + \frac{65520}{691}\sum_{n=1}^{\infty}\sigma_{11}(n)q^n$$

Notice that all coefficients in these expansions are rational.

As a passing remark we note that there is a weight 2 Eisenstein series E_2 defined in a similar fashion to the q-expansion above for $k = 1$ (so contains the original divisor sum $\sigma_1(n) = \sigma(n)$). This function does not transform in the correct way to be a modular form but there are ways to modify this (p.18 of [19]).

We can use the functions E_{2k} to find new modular forms via use of Lemma 1.1.13. In fact the functions E_4 and E_6 are fundamental in this process.

Theorem 1.1.18. *There exists an isomorphism of $\mathbb{C}$-algebras:*

$$M(SL_2(\mathbb{Z})) \cong \mathbb{C}[E_4, E_6].$$

In particular:

$$M_k(SL_2(\mathbb{Z})) = \bigoplus_{4a+6b=k} \mathbb{C}E_4^a E_6^b.$$

This shows that in general it is easy to write down a basis for the space of modular forms of a given weight. However later we will seek a better basis for computation.

We give a name to modular forms that have a zero at infinity.

Definition 1.1.19. Let $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ be such that $a_0 = 0$ in the q-expansion. Then we call f a cusp form. The subspace of cusp forms in $M_k(\mathrm{SL}_2(\mathbb{Z}))$ will be denoted $S_k(\mathrm{SL}_2(\mathbb{Z}))$. □

Considering cusp forms of all weights together we find that:

$$S(\mathrm{SL}_2(\mathbb{Z})) = \oplus_{k=0}^{\infty} S_k(\mathrm{SL}_2(\mathbb{Z}))$$

is an ideal of the $\mathbb{C}$-algebra $M(\mathrm{SL}_2(\mathbb{Z}))$.

So far we have not seen any non-trivial examples of cusp forms. However it is not so difficult to construct one.

Consider the functions E_4^3 and E_6^2. Both must lie in $M_{12}(\mathrm{SL}_2(\mathbb{Z}))$ and have constant term 1 in their q-expansions. Thus $E_4^3 - E_6^2 \in M_{12}(\mathrm{SL}_2(\mathbb{Z}))$ must have a zero at infinity. Further this function is not identically zero since the q-coefficient in the q-expansion is $3(240\sigma_3(1)) + 2(504\sigma_5(1)) = 1728$.

Definition 1.1.20. The discriminant function is the function given by:

$$\Delta(z) = \frac{E_3^4 - E_6^2}{1728} \in S_{12}(\mathrm{SL}_2(\mathbb{Z})).$$

□

The discriminant is a special function since it was the first non-trivial cusp form to be constructed. In fact no non-trivial cusp forms exist for weights below 12.

The reason for the name is due to connections with the discriminant of elliptic curves over $\mathbb{C}$. Given the lattice $\langle 1, \tau \rangle$ for $\tau \in \mathcal{H}$ it turns out that the values $E_4(\tau), E_6(\tau)$ appear in the defining equation of the corresponding elliptic curve. The discriminant of this curve is then $\Delta(\tau)$.

Since Δ has a simple zero at infinity and E_4^3 is non-zero at infinity we see that the quotient $\frac{E_4^3}{\Delta}$ must have a simple pole at infinity. By cancellation of

weights we find that this must be a weakly modular function (it has weight 0). In fact it is the j-function defined earlier, giving further links to elliptic curves.

There are in fact alternative ways of writing the discriminant function. One such way is via an infinite product:

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

Alternatively we know that $\Delta(z)$ must have a q-expansion:

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

The numbers $\tau(n)$ were studied extensively by Ramanujan. A few of his observations and conjectures include:

- $\tau(mn) = \tau(m)\tau(n)$ for all coprime m, n, i.e. τ is multiplicative.
- $\tau(p^{m+2}) = \tau(p)\tau(p^{m+1}) - p^{11}\tau(p^m)$ for all primes p and $m \geq 0$.
- $|\tau(p)| \leq 2p^{\frac{11}{2}}$ for all primes p. This is an analogue of the Hasse bound for elliptic curves.
- $\tau(n) \equiv \sigma_{11}(n) \bmod 691$ for all n. This is an important congruence between Fourier coefficients of Δ and E_{12} modulo the prime 691 (the significance being that 691 divides the numerator of $\frac{\zeta(12)}{\pi^{12}}$). The aim of this thesis is to study Harder's conjecture, a generalisation of these congruences.

Most of these properties can be proved using the theory of Hecke operators (to be defined). Later we will see in detail how the congruence can be proved using finite dimensionality of the spaces of modular forms.

Many other conjectures and results relate to $\tau(n)$. For example it is currently an open problem, due to Lehmer, to show that $\tau(n) \neq 0$ for all n [47].

One important feature of the spaces of modular forms is that they are all finite dimensional. This is completely non-obvious. What is even more surprising is that we have a simple formula for this dimension.

Theorem 1.1.21. *For even k:*

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

Also $dim(S_k(SL_2(\mathbb{Z}))) = dim(M_k(SL_2(\mathbb{Z}))) - 1$.

Finite dimensionality allows modular forms to be efficiently computed. It also helps to provide mysterious links between objects of number theoretic significance.

Example 1.1.22. We know that $E_8, E_4^2 \in M_8(\mathrm{SL}_2(\mathbb{Z}))$. But this space of modular forms is 1-dimensional by the above formula. Thus E_8, E_4^2 are linearly dependent, meaning $E_8 = \alpha E_4^2$ for some $\alpha \in \mathbb{C}^\times$.

However, both have constant coefficient 1 in their q-expansions and so $E_8 = E_4^2$. On the level of q-expansions this gives the following surprising identity between power divisor sums for all $n \geq 1$:

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{k=1}^{n-1} \sigma_3(k)\sigma_3(n-k).$$

Such identities would be quite tough to formulate and prove using elementary methods.

By studying other spaces of modular forms for small weights one can extend the above argument to produce other non-trivial identities. □

Example 1.1.23. We can now prove Ramanujan's congruence:

$$\tau(n) \equiv \sigma_{11}(n) \bmod 691.$$

Consider the space $M_{12}(\mathrm{SL}_2(\mathbb{Z}))$. We know that this space is 2-dimensional. However E_{12}, E_4^3, Δ are all weight 12 modular forms and so must be linearly dependent. Thus:

$$E_{12} = \alpha E_4^3 + \beta \Delta,$$

for some $\alpha, \beta \in \mathbb{C}^\times$.

Comparing the constant coefficients and the q-coefficients in the q-expansion gives:

$$\alpha = 1$$
$$\frac{65520}{691} = 720\alpha + \beta,$$

thus $\alpha = 1, \beta = -\frac{432000}{691}$.

Clearing denominators gives:

$$691E_{12} = 691E_4^3 - 432000\Delta.$$

Comparing q-expansions we now see that for $n \geq 1$:

$$65520\sigma_{11}(n) = 691C_n - 432000\tau(n),$$

where $C_n \in \mathbb{Z}$ is the q^n-coefficient in the q-expansion of E_4^3.

Reducing mod 691 we see that:

$$566\sigma_{11}(n) \equiv 566\tau(n) \bmod 691,$$

for all n. Cancelling 566 from both sides gives the congruence. □

There are alternative ways to prove the Ramanujan congruence. An alternative way is to use the theory of Hecke operators (to be discussed later).

Another particularly interesting way to prove the congruence is by studying the theta series of the Leech lattice. This is a modular form of weight 12. The beauty of this particular proof comes from knowing in advance that the coefficients of the theta series must be integral (since they count numbers of vectors of a given norm). However these coefficients turn out to be $\frac{65520(\sigma_{11}(n)-\tau(n))}{691}$ and so 691 must divide $\sigma_{11}(n) - \tau(n)$.

Also it may be remarked that many generalizations of the Ramanujan congruence are known. Essentially the relevance of the 691 comes from the fact that this prime divides the rational part of the Riemann zeta value $\zeta(12)$ (alternatively it divides the numerator of a Bernoulli number), thus forcing the Eisenstein series E_{12} and the cusp form Δ to be equivalent mod 691. See [20] for other examples of Ramanujan style congruences.

1.1.2 Modular forms for congruence subgroups

We can define modular forms for other subgroups of $\mathrm{SL}_2(\mathbb{R})$. For the purposes of this thesis we will only see this for a nice enough family of subgroups of $\mathrm{SL}_2(\mathbb{Z})$ called congruence subgroups.

Definition 1.1.24. Let $N \in \mathbb{N}$. The principal congruence subgroup of level N is:

$$\Gamma(N) = \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A \equiv I \bmod N\},$$

(where congruence is entry wise).

Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$. We say that Γ is a congruence subgroup of level N if $\Gamma(N) \subseteq \Gamma$. □

In particular notice that $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$.

Note that $\Gamma(N)$ is the kernel of the reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Via this interpretation it is clear that $\Gamma(N)$ is a normal subgroup of $\mathrm{SL}_2(\mathbb{Z})$ and that it is of finite index (by the first isomorphism theorem $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = |\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})|$).

In fact we know this index exactly since it is known that $|\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})| = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$.

It follows that all congruence subgroups have finite index in $\mathrm{SL}_2(\mathbb{Z})$ (and that this index is a factor of $[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]$).

Some particularly interesting congruence subgroups are the following:

$$\Gamma_0(N) = \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A_{2,1} \equiv 0 \bmod N\}$$
$$\Gamma_1(N) = \{A \in \mathrm{SL}_2(\mathbb{Z}) \mid A_{2,1} \equiv 0 \bmod N, A_{1,1} \equiv A_{2,2} \equiv 1 \bmod N\}$$

Clearly there is a chain of inclusions:

$$\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq \mathrm{SL}_2(\mathbb{Z}).$$

It is also straightforward to see the following isomorphisms:

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

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

and so we may easily calculate:

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)] = \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)]}{N} = N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$$

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = \frac{[\mathrm{SL}_2(\mathbb{Z}) : \Gamma_1(N)]}{\phi(N)} = N \prod_{p|N} \left(1 + \frac{1}{p}\right)$$

We may define modular forms for congruence subgroups as follows:

Definition 1.1.25. A modular form of weight $k \in \mathbb{Z}$ for a congruence subgroup Γ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that:

- $f(\gamma z) = (cz + d)^k f(z)$ for each $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$.
- $f|_k\mu$ is homorphic at infinity for all $\mu \in \mathrm{SL}_2(\mathbb{Z})$.

□

The reason for the second condition is due to the fact that a fundamental domain for the action of Γ on $\mathcal{H}$ may have more than one "cusp" and so we need such functions to be nicely behaved at all of these points (rather than just at the "point at infinity"). This is all made formal and precise in Section 2.4 of [19].

As for $\mathrm{SL}_2(\mathbb{Z})$ we can consider the vector spaces $M_k(\Gamma)$ of modular forms with respect to congruence subgroup Γ. Also we have subspaces $S_k(\Gamma)$ of cusp forms

with respect to Γ, these being subspaces of forms which vanish at the "cusps". All of the above spaces are known to be finite dimensional and formulae are known in many cases (see p.92-93 of [46] for the case $\Gamma = \Gamma_0(N)$).

As with level 1 we still have Eisenstein series but their definition is more cumbersome. It is worth noting that that the spaces $M_k(\Gamma)$ still decompose into $S_k(\Gamma)$ and an Eisenstein subspace but now the dimension of the Eisenstein subspace is usually bigger than 1.

Another new occurrence for the spaces $S_k(\Gamma)$ is the existence of newforms. Since we only concern ourselves with $\Gamma_0(N)$ in this thesis we will only explain this notion in this case but note that generalizations to arbitrary congruence subgroups exist.

First note the fact that if $M|N$ then $\Gamma_0(N)$ is a subgroup of $\Gamma_0(M)$. Thus there is an obvious inclusion

$$\alpha_1 : S_k(\Gamma_0(M)) \hookrightarrow S_k(\Gamma_0(N))$$

given by

$$\alpha_1(f)(z) = f(z)$$

(since if $f|_k\gamma = f$ for all $\gamma \in \Gamma_0(M)$ then the same clearly holds for $\Gamma_0(N)$).

Naturally we would like to consider forms in the image of this map as being "old" since they came from an earlier level. But there are other ways that $S_k(\Gamma_0(M))$ may embed into $S_k(\Gamma_0(N))$.

To generalize the map α_1 we consider for each divisor $d \mid \frac{N}{M}$ the linear map

$$\alpha_d : S_k(\Gamma_0(M)) \hookrightarrow S_k(\Gamma_0(N))$$

given by

$$\alpha_d(f)(z) = f(dz).$$

We should consider each of the maps α_d as producing "old" modular forms from level M.

Of course we should play this game for each possible divisor M of N to get all "old" forms.

Definition 1.1.26. An oldform in $S_k(\Gamma_0(N))$ is any form that lies in:

$$\bigoplus_{M|N} \bigoplus_{d|\frac{N}{M}} \alpha_d(S_k(\Gamma_0(M))).$$

□

It is clear by definition that the oldforms make a subspace of $S_k(\Gamma_0(N))$. We will write this as $S_k^{\text{old}}(\Gamma_0(N))$.

The space $S_k(\Gamma_0(N))$ can be equipped with a natural inner product, the Petersson inner product (p.183 of [19]). Under this inner product the space $S_k^{\text{new}}(\Gamma_0(N))$ is the orthogonal complement of the space of oldforms. This space consists of forms that are not built from oldforms and so are "new" at level N.

We have a decomposition:

$$S_k(\Gamma_0(N)) = S_k^{\text{old}}(\Gamma_0(N)) \oplus S_k^{\text{new}}(\Gamma_0(N)),$$

so that $S_k^{\text{new}}(\Gamma_0(N))$ is really a complementary subspace of $S_k^{\text{old}}(\Gamma_0(N))$. Later we will see the importance of newforms.

Example 1.1.27. Let $N = p$ be prime. Then all oldforms must come from level 1, i.e. be modular forms for $\mathrm{SL}_2(\mathbb{Z})$. The two inclusions $S_k(\mathrm{SL}_2(\mathbb{Z})) \hookrightarrow S_k(\Gamma_0(p))$ are given by $f \mapsto f$ and $f \mapsto g$ where $g(z) = f(pz)$. □

1.1.3 Hecke operators

Following Ramanujan's observations about the numbers $\tau(n)$ similar patterns were discovered amongst other modular forms (in particular Eisenstein series). Naturally it was wondered how one could prove such properties of Fourier coefficients.

A clever idea was to try and exhibit a modular form as an eigenform of certain linear operators on $S_k(\Gamma)$, having eigenvalues equal to the Fourier coefficients. In this subsection we will define these operators.

Let $f : \mathcal{H} \to \mathbb{C}$ and $\gamma \in \mathrm{GL}_2^+(\mathbb{Q})$. We may extend the weight k slash operator to $\mathrm{GL}_2^+(\mathbb{Q})$via:

$$(f|_k\gamma)(z) = \det(\gamma)^{\frac{k}{2}} j(\gamma, z)^{-k} f(\gamma z).$$

This agrees with the previous definition if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

Now fix congruence subgroups $\Gamma_1, \Gamma_2 \subseteq \mathrm{SL}_2(\mathbb{Z})$. Then we may construct maps that transform modular forms for Γ_1 into modular forms for Γ_2.

For each $\alpha \in \mathrm{GL}_2^+(\mathbb{Q})$ consider the double coset decomposition:

$$\Gamma_1 \alpha \Gamma_2 = \coprod_i \Gamma_1 \mu_i.$$

It is known that there are finitely many coset representatives μ_i in such a decomposition.

Note that any choice of coset representatives is determined up to left multiplication by Γ_1. Thus the following is well defined (using the cocycle property $j(\gamma_1\gamma_2, z) = j(\gamma_1, \gamma_2, z)j(\gamma_2, z)$).

Definition 1.1.28. Let $f \in M_k(\Gamma)$. The weight k double coset operator $[\Gamma_1 \alpha \Gamma_2]_k$ acts via:

$$[\Gamma_1 \alpha \Gamma_2]_k(f) = \sum_i f|_k \mu_i.$$

□

Theorem 1.1.29. *For any α as above, the weight k double coset operator $[\Gamma_1 \alpha \Gamma_2]_k$ defines a linear map $M_k(\Gamma_1) \to M_k(\Gamma_2)$. These maps induce linear maps $S_k(\Gamma_1) \to S_k(\Gamma_2)$.*

If we now consider the case $\Gamma_1 = \Gamma_2 = \Gamma$ we get the following.

Corollary 1.1.30. *For any α as above the weight k double coset operator $[\Gamma \alpha \Gamma]_k$ defines an endomorphism of $M_k(\Gamma)$ (and of $S_k(\Gamma)$).*

Let p be prime and fix the weight k from now on. An important choice of α is $\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Q})$.

Definition 1.1.31. For this choice of α we call the corresponding double coset operator $T_p := \left[\Gamma \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma\right]_k$ the pth Hecke operator. The chosen representatives μ_i are called Hecke representatives for T_p. □

In general a family of Hecke operators is built, indexed by positive integers. For $m \in \mathbb{N}$ the Hecke operator T_m is defined to be the sum of double coset operators given by $\left[\Gamma \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \Gamma\right]_k$ for all pairs of positive integers $1 \leq a < d$ such that $ad = n$. However in practice only the T_p operators are needed due to the following properties:

$$\begin{aligned} T_1 &= \mathrm{id}, \\ T_{p^m} &= T_p T_{p^{m-1}} - p^{k-1} T_{p^{m-2}} \quad \text{if } m \geq 2, \\ T_{mn} &= T_m T_n \quad \text{if } m, n \text{ coprime}. \end{aligned}$$

Here we are working in the endomorphism ring $\mathrm{End}(M_k(\Gamma))$ with multiplication given by composition of maps.

As mentioned before we are interested in eigenvectors for these operators.

Definition 1.1.32. A modular form $f \in M_k(\Gamma)$ is a Hecke eigenform for T_n if $T_n(f) = \lambda_n f$ for some $\lambda_n \in \mathbb{C}$. The number λ_n is called a Hecke eigenvalue of f. □

From now on we concern ourselves only with the case $\Gamma = \Gamma_0(N)$ but note that most of what follows can be generalized. In this case the Hecke operators satisfy lots of really nice properties, in particular the following:

- The Hecke operators commute, i.e. $T_m T_n = T_n T_m$ for all m, n.
- If m is coprime to N then T_m is self adjoint with respect to the Petersson inner product on $S_k(\Gamma_0(N))$.

Tying these facts together with the spectral theorem of linear algebra gives the following:

Theorem 1.1.33. *The spaces $M_k(\Gamma_0(N))$ and $S_k(\Gamma_0(N))$ have bases consisting of simultaneous eigenforms for all T_m operators with m coprime to N. These bases are orthogonal with respect to the Petersson inner product.*

A special thing happens for newforms. Conveniently Hecke operators preserve the decomposition:

$$S_k(\Gamma_0(N)) = S_k^{\text{old}}(\Gamma_0(N)) \oplus S_k^{\text{new}}(\Gamma_0(N)).$$

In the new subspace we can actually construct a basis of eigenforms for all of the T_m operators (even those where m is not coprime to N). This can all be observed in Atkin and Lehner's paper [3].

Despite the abstract feel of everything discussed so far we can make it very computational.

Lemma 1.1.34. *Let p be prime. For $i = 0, 1, ..., p-1$ let $\mu_i = \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix}$ and let $\mu = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$. The following decomposition holds:*

$$\Gamma_0(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_0(N) = \begin{cases} \coprod_{i=0}^{p-1} \Gamma_0(N)\mu_i \coprod \Gamma_0(N)\mu & \text{if } p \nmid N \\ \coprod_{i=0}^{p-1} \Gamma_0(N)\mu_i & \text{if } p \mid N \end{cases}$$

Using these Hecke representatives we can get an explicit description of the action of T_p in terms of Fourier coefficients.

Lemma 1.1.35. *Let $f \in M_k(\Gamma_0(N))$ have q-expansion $f(z) = \sum_{n=0}^{\infty} a_n q^n$. Then the q-expansion of $T_p(f)$ is $T_p(f)(z) = \sum_{n=0}^{\infty} b_n q^n$ where:*

$$b_n = \begin{cases} a_{np} + p^{k-1} a_{\frac{n}{p}} & \text{if } p \nmid N \\ a_{np} & \text{if } p \mid N \end{cases}$$

(Here we take the convention that $a_{\frac{n}{p}} = 0$ if $p \nmid n$.)

Using the recursive relationships between Hecke operators it is possible to give similar formulae for the action of any T_m on modular forms for $\Gamma_0(N)$.

Corollary 1.1.36. *Let $f \in M_k(\Gamma_0(N))$ have q-expansion $f(z) = \sum_{n=0}^{\infty} a_n q^n$. Then the q-expansion of $T_m(f)$ is $T_m(f)(z) = \sum_{n=0}^{\infty} b_n q^n$ where:*

$$b_n = \begin{cases} \sum_{d|hcf(m,n)} d^{k-1} a_{\frac{mn}{d^2}} & \text{if } m \text{ is coprime to } N \\ a_{nm} & \text{otherwise} \end{cases}$$

Now suppose that $f \in M_k(\Gamma_0(N))$ is an eigenform for a single Hecke operator T_m. Then $T_m(f) = \lambda_m f$ for some $\lambda_m \in \mathbb{C}$. By direct comparison of q-expansions we would have that $b_1 = \lambda_m a_1$. However by the formulae we know that $b_1 = a_m$. Hence $a_m = \lambda_m a_1$. This gives us a nice link between Hecke eigenvalues and Fourier coefficients.

Next suppose that f is an eigenform for all Hecke operators T_m. Then we know that $a_m = \lambda_m a_1$ for all m. Now clearly if $a_1 = 0$ then $a_m = 0$ for all $m \geq 1$ and so $f = a_0$ would be constant. Thus we may assume that $a_1 \neq 0$.

Definition 1.1.37. An eigenform f is normalized if $a_1 = 1$. □

If $a_1 \neq 0$ then we may always scale f to give a normalized eigenform. The importance of this concept is that we would then have $\lambda_m = a_m$ for all m, so that the Hecke eigenvalues really are the Fourier coefficients.

It is then simple to see that due to the properties of Hecke operators we would have the following relationships between Fourier coefficients of normalized eigenforms:

$$a_{p^m} = a_p a_{p^{m-1}} + p^{k-1} a_{p^{m-2}} \quad \text{for all } m \geq 2 \text{ and primes } p$$
$$a_{mn} = a_m a_n \quad \text{for all } m, n \text{ coprime}$$

This justifies why we would want to have normalized eigenforms. Such forms have Fourier coefficients that satisfy nice properties, such as multiplicativity. This is a clear theme in the theory of modular forms. Normalized eigenforms tend to be ones with number theoretic Fourier coefficients.

Of course in general we do not have eigenforms for all Hecke operators but everything said above still holds true as long as one takes care to eliminate indices that are not coprime to the level N.

Example 1.1.38. The space $S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ is 1-dimensional and so any non-zero form in this space should be an eigenform for all Hecke operators. In particular the discriminant function $\Delta(z) = \sum_{n=1}^{\infty} \tau(n) q^n$ is a normalized eigenform for all Hecke operators.

This proves the following identities for the Ramanujan τ function:

$$\tau(p^m) = \tau(p)\tau(p^{m-1}) + p^{11}\tau(p^{m-2}) \quad \text{for all } m \geq 2 \text{ and primes } p$$
$$\tau(mn) = \tau(m)\tau(n) \quad \text{for all } m, n \text{ coprime}$$

These were famous observations of Ramanujan mentioned previously. □

Example 1.1.39. One can view the 691 congruence of Ramanujan as being between Hecke eigenvalues since the space $M_{12}(\mathrm{SL}_2(\mathbb{Z}))$ has a basis of eigenforms E_{12} and Δ with Hecke eigenvalues $\sigma_{11}(m)$ and $\tau(m)$ respectively. □

We finish this subsection by remarking that Hecke eigenvalues are algebraic numbers. By Proposition 4.24 in[46] one can in fact choose a basis of normalized eigenforms with Hecke eigenvalues that are real algebraic integers.

Definition 1.1.40. Given $f \in M_k(\Gamma_0(N))$ its field of definition is $\mathbb{Q}_f = \mathbb{Q}(\{a_n \mid n \in \mathbb{N}\})$. □

In general this field will be a transcendental extension of $\mathbb{Q}$ but for normalized eigenforms it is an algebraic extension of $\mathbb{Q}$ (by the above). More can be said.

Theorem 1.1.41. *If f is a normalized eigenform then $\mathbb{Q}_f$ is a number field, i.e. a finite extension of $\mathbb{Q}$.*

1.1.4 L-functions attached to modular forms

An important theme in both modern and classical number theory has been to study analytic functions associated to number theoretic objects. A famous example is the Riemann zeta function for $\mathrm{Re}(s) > 1$:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

and its functional equation given by Riemann in his famous 1859 paper:

$$\xi(s) = \xi(1-s)$$

where

$$\xi(s) = \frac{1}{2}\pi^{-\frac{s}{2}} s(s-1)\Gamma\left(\frac{s}{2}\right)\zeta(s).$$

This functional equation allows $\zeta(s)$ to be analytically continued to $\mathbb{C}\backslash\{1\}$ (once one continues $\zeta(s)$ to $0 < \mathrm{Re}(s) < 1$).

Hidden within $\zeta(s)$ are many interesting results on the distribution of prime numbers. A small justification for this lies in the Euler product expansion of $\zeta(s)$ for $\mathrm{Re}(s) > 1$:

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1},$$

this being an analytic way of expressing unique factorisation.

Riemann showed how the analytic continuation of $\zeta(s)$ allows us to find families of good approximations to the prime counting function $\pi(x)$, given

that the zeros of $\zeta(s)$ are well behaved. This is the subject of the Riemann Hypothesis, still an unsolved problem. Included in his approximations is the Prime Number Theorem:

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1.$$

There is also merit to studying the special values of $\zeta(s)$ at integers. Such values appear in the coefficients of Eisenstein series but it is also worth studying them for their own right to uncover mysterious identities. For example Euler was able to justify that:

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

and went on to find the general formula for $\zeta(2k)$ (given after Theorem 1.1.16). Note that $\zeta(2k) = \alpha_{2k}\pi^{2k}$ for some $\alpha_{2k} \in \mathbb{Q}$ so that these zeta values split neatly into rational and transcendental parts.

In general one can attach to any arithmetic function $g : \mathbb{N} \to \mathbb{C}$ a Dirichlet series:

$$L(g, s) = \sum_{n=1}^{\infty} \frac{g(n)}{n^s}.$$

Whenever g has nice enough properties such as multiplicativity there is a well known theory of Euler products.

It is hoped that analytic properties of $L(g, s)$ encode arithmetic properties of g amongst other things of number theoretic significance, e.g. distribution of primes.

Indeed the study of the functions $L(\chi, s)$ for lifts of characters χ of $(\mathbb{Z}/m\mathbb{Z})^\times$ allowed Dirichlet to prove his famous theorem on primes in arithmetic progressions, and to give information on densities of primes lying in given classes mod m.

Classically other notable Dirichlet series are ones attached to number fields, known as Dedekind zeta functions. Studying these gives precise information on class numbers, embeddings, fundamental units, discriminants etc. This is the basis of the Dirichlet class number formula.

In a modern setting we attach such "L-functions" and "zeta functions" to varieties, modular forms, Galois representations and many other interesting objects. We still appear to be finding deep number theoretic results encoded in such functions. For example the famous Birch Swinnerton-Dyer conjecture tells us how studying $L(E, s)$ for a rational elliptic curve gives lots of information of interest about E, such as the rank of the Mordell-Weil group $E(\mathbb{Q})$, the number of torsion points, the size of the Shafarevich-Tate group of E etc.

For the purposes of this thesis we will be interested in L-functions attached

to newforms for $\Gamma_0(N)$. Of course we already have an arithmetic function to hand given by the Fourier coefficients of the form.

Definition 1.1.42. Let $f \in M_k(\Gamma_0(N))$ have q-expansion $f(z) = \sum_{n=0}^{\infty} a_n q^n$. The L-function associated to f is:

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

□

It is known that this L-function converges absolutely for $\mathrm{Re}(s) > \frac{k+1}{2}$ if f is a cusp form and for $\mathrm{Re}(s) > k$ otherwise. This follows from known upper bounds for $|a_n|$.

First one asks whether such L-functions have Euler products. It turns out that in some cases they do but they have quadratic Euler factors in p^{-s} rather than linear ones.

Theorem 1.1.43. *The form f is a normalized eigenform for all Hecke operators if and only if $L(f,s)$ has an Euler product expansion of the form:*

$$L(f,s) = \prod_p (1 - a_p p^{-s} + p^{k-1-2s})^{-1}.$$

This again highlights the historical significance of eigenforms. In general $L(f,s)$ will not have such an expansion.

Of course we have seen that it is not always possible to construct normalized eigenforms for all Hecke operators, but that you may always find them for index coprime to the level. In such cases $L(f,s)$ will still have an Euler product but it will be of the form:

$$L(f,s) = \prod_{p|N} (1 - a_p p^{-s})^{-1} \prod_{p \nmid N} (1 - a_p p^{-s} + p^{k-1-2s})^{-1}.$$

Secondly we ask whether such L-functions have analytic continuation to the whole complex plane. Indeed they do but it is first convenient to define the completed L-function:

$$\Lambda(f,s) = N^{\frac{s}{2}} (2\pi)^{-s} \Gamma(s) L(f,s).$$

This function is the analogue of Riemann's ξ function mentioned above.

One can view $\Lambda(f,s)$ as a Mellin transform as follows:

$$\Lambda(f,s) = N^{\frac{s}{2}} \int_0^{\infty} f(iy) y^{s-1} dy.$$

Using this one proves a functional equation:

$$\Lambda(f,s) = i^k \Lambda(W_N(f), k-s).$$

Here $W_N(f) = N^{1-\frac{k}{2}} f|_k \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \in S_k(\Gamma_0(N))$ is the Atkin-Lehner involute of f. Whenever $W_N(f) = \pm f$ (i.e. f is an eigenvector for W_N) we have:

$$\Lambda(f,s) = \pm i^k \Lambda(f, k-s).$$

Finally we address the question of finding special values of such L-functions. It seems natural to want to evaluate $L(f,s)$ at integer values of s and get nice formulae. However this is very ambitious.

To put this in perspective consider the same question for the Riemann zeta function. We know next to nothing about closed formulae for $\zeta(2k+1)$ for positive integers k. We can only really compute these values numerically. It was only around 1979 that $\zeta(3)$ was proved to be irrational by Apéry [1].

However if we consider instead the values $\zeta(2k)$ then much is known. We happen to know that $\frac{\zeta(2k)}{\pi^{2k}} \in \mathbb{Q}$ and as seen earlier we even have a formula for the "rational part", involving Bernoulli numbers. Of course one can use the functional equation to deal with negative integer inputs.

It turns out that for L-functions of modular forms the integer inputs that we know the most about are $s = 1, 2, ..., k-1$. These are called the critical values of f. Note that by the symmetry in the functional equation it suffices to evaluate at the values $s = \frac{k}{2}, \frac{k}{2}+1, ..., k-1$.

As a brief remark the notion of critical value has been made precise in a paper of Deligne [17]. In this paper he defines critical values of L-functions $L(M,s)$ attached to motives (of which all previously stated L-functions are examples). For $\zeta(s)$ the critical values are, as expected, the even positive integers and the odd negative ones. For $L(f,s)$ they are exactly the critical values mentioned above.

Deligne even goes on to conjecture the existence of a "period" $c^+(M) \in \mathbb{C}$ such that $\frac{L(M,0)}{c^+(M)} \in \mathbb{Q}$. This is the natural generalisation of the statement $\frac{\zeta(2k)}{\pi^{2k}} \in \mathbb{Q}$. One might think of this period as being the "transcendental part" of the L-value, that once divided out leaves something algebraic.

For the case of modular forms Deligne's conjecture has been proved. However a surprise occurs in that the period we must divide by is only dependent on the parity of the critical value.

Theorem 1.1.44. *(Manin/Vishik) Let m be a critical value for f. There exist constants $\Omega^+, \Omega^- \in \mathbb{C}$ such that $\frac{\Lambda(f,m)}{\Omega^+} \in \mathbb{Q}_f$ if m is even and $\frac{\Lambda(f,m)}{\Omega^-} \in \mathbb{Q}_f$ if m is odd.*

The constants $\Omega^{\pm}$ are not unique but determined up to scalar multiples in $\mathbb{Q}_f^{\times}$. Often it is possible to pin it down to a scalar multiple in $\mathcal{O}_{\mathbb{Q}_f}^{\times}$ (so as to make it almost canonical). By making this normalization we can study divisibility of such values by primes without ambiguity.

The proof of the above result is beautiful and is found in Manin's paper [49]. The idea is to define for $m = 0, 1, 2, ..., k-2$ the periods of $f \in S_k(\Gamma_0(N))$:

$$r_m(f) = \int_0^{i\infty} f(z) z^m dz.$$

Note that $\Lambda(f, m+1) = N^{\frac{m+1}{2}} r_m(f)$ so that once one knows the periods of f it is possible to extract critical Λ-values.

Manin exhibits an infinite system of homogeneous linear equations for the periods of f by using certain actions of Hecke operators. The coefficients of these equations lie in $\mathbb{Q}_f$. He then manages to prove that these equations naturally break up into two sets of equations, one for the even index periods and one for the odd ones. Finally he is able to prove that the two sets of equations each give a 1-dimensional space of solutions, explaining the existence of $\Omega^{\pm}$. This gives an algebraic method for finding ratios of periods, at no point do we need to find the above integrals.

When a choice of $\Omega^{\pm}$ is fixed and m is critical we will write $\Lambda_{\text{alg}}(f, m) = \frac{\Lambda(f,m)}{\Omega^{\pm}}$ (where the choice of sign depends on the parity of m). We will be interested in special primes dividing these values since these will eventually be the moduli of our congruences (in direct analogue with the 691 in Ramanujan's congruence).

1.2 Siegel modular forms

Siegel modular forms are a higher dimensional generalization of the elliptic modular forms studied in the previous section. They can be considered as modular forms in one or more variables (with elliptic modular forms being functions of one variable).

Just as one can attach theta series to quadratic forms to measure representation numbers of an integer by a form, Siegel modular forms were designed as an attempt to measure representations of quadratic forms by other quadratic forms.

We begin with the symplectic group of genus g given by

$$\text{Sp}_{2g}(\mathbb{R}) = \{\gamma \in M_{2g}(\mathbb{R}) \,|\, \gamma J \gamma^T = J\},$$

where:

$$J = \begin{pmatrix} 0 & I_g \\ -I_g & 0 \end{pmatrix}.$$

One can view such a group as the group of matrices preserving a specific symplectic form on $\mathbb{R}^{2g}$. In particular $\mathrm{Sp}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})$.

In analogue to the relationship between the groups $\mathrm{SL}_2(\mathbb{R})$ and $\mathrm{GL}_2(\mathbb{R})$ we can construct the group of similitudes of $\mathrm{Sp}_{2g}(\mathbb{R})$:

$$\mathrm{GSp}_{2g}(\mathbb{R}) = \{\gamma \in M_{2g}(\mathbb{R}) \,|\, \gamma J \gamma^T = \mu(\gamma) J, \mu(\gamma) \in \mathbb{R}^\times\}.$$

One observes that the similitude map $\mu : \mathrm{GSp}_{2g}(\mathbb{R}) \longrightarrow \mathbb{R}^\times$ is a homomorphism that plays a role analogous to the determinant map for $\mathrm{GL}_n(\mathbb{R})$. Indeed just as $\mathrm{SL}_n(\mathbb{R})$ is the kernel of the determinant map $\det : \mathrm{GL}_n(\mathbb{R}) \longrightarrow \mathbb{R}^\times$ we see that $\mathrm{Sp}_{2g}(\mathbb{R})$ is the kernel of $\mu : \mathrm{GSp}_{2g}(\mathbb{R}) \to \mathbb{R}^\times$.

Analogous to the upper half plane we can also construct the Siegel upper half space of genus g:

$$\mathcal{H}_g = \{Z \in M_g(\mathbb{C}) \,|\, Z^T = Z, \mathrm{Im}(Z) \text{ is positive definite}\}.$$

Again for $g = 1$ this is the usual upper half plane $\mathcal{H}$.

Lemma 1.2.1. *The group $Sp_{2g}(\mathbb{R})$ acts transitively on $\mathcal{H}_g$ by fractional linear transformations, i.e. if $Z \in \mathcal{H}_g$ and $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sp_{2g}(\mathbb{R})$ is written in $g \times g$ blocks then:*

$$(\gamma, Z) \mapsto \gamma Z = (AZ + B)(CZ + D)^{-1}.$$

defines a transitive group action.

Of course the above is not as easy to prove as the classical case. There is now the non-trivial matter of the matrices $(CZ + D)$ being invertible. As previously we will still define the automorphy factor $j(\gamma, Z) = (CZ + D)$.

1.2.1 Siegel modular forms for $\mathbf{Sp}_{2g}(\mathbb{Z})$

One defines Siegel modular forms by considering nice enough arithmetic subgroups of $\mathrm{Sp}_{2g}(\mathbb{R})$. First let us deal with the simplest case, classical Siegel modular forms for the Siegel modular group $\mathrm{Sp}_{2g}(\mathbb{Z})$.

Definition 1.2.2. A holomorphic function $F : \mathcal{H}_g \longrightarrow \mathbb{C}$ is a classical Siegel modular form of genus g, weight k for $\mathrm{Sp}_{2g}(\mathbb{Z})$ if:

- $F(\gamma Z) = \det(j(\gamma, Z))^k F(Z)$ for all $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$.

- If $g = 1$ then F is holomorphic at infinity (as defined in the previous section).

□

We do not have to check holomorphy at infinity for $g \geq 2$. This is due to a phenomenon known as Koecher's principle (see Theorem 2 of Van der Geer's article in [9]).

For a given weight k the $\mathbb{C}$-vector space $M_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ of classical Siegel modular forms of weight k, genus g for $\mathrm{Sp}_{2g}(\mathbb{Z})$ is finite dimensional. It is still true that we require $k \geq 0$ for non-trivial examples to exist. Also kg should be even (which fits with the genus 1 case since we saw there that k had to be even).

Of course it is easy to see that the analogue of Lemma 1.1.13 still holds in this context and so the structure $M(\mathrm{Sp}_{2g}(\mathbb{Z})) = \oplus_{k=0}^{\infty} M_k(\mathrm{Sp}_{2g}(\mathbb{Z}))$ forms a graded $\mathbb{C}$-algebra. This $\mathbb{C}$-algebra is known to be finitely generated as in the $g = 1$ case although explicit generators are tough to find (although for $g = 2, 3$ generators are known, given to us by Igusa [42] and Tsuyumine [66] respectively).

A new feature that arises in studying Siegel modular forms is the notion of vector valued Siegel modular forms for $\mathrm{Sp}_{2g}(\mathbb{Z})$. Let:

$$\rho : \mathrm{GL}_g(\mathbb{C}) \longrightarrow \mathrm{GL}(V)$$

be a finite dimensional complex representation.

Definition 1.2.3. A holomorphic function $F : \mathcal{H}_g \longrightarrow V$ is a Siegel modular form of genus g, weight ρ for $\mathrm{Sp}_{2g}(\mathbb{Z})$ if:

- $F(\gamma Z) = \rho(j(\gamma, Z))F(Z)$ for all $\gamma \in \mathrm{Sp}_{2g}(\mathbb{Z})$.
- If $g = 1$ then F is holomorphic at infinity.

□

The case of classical Siegel modular forms arises when one takes the 1-dimensional representation $\rho = \det^k$ (so that the corresponding modular forms are "scalar-valued").

In a similar vein to before we may define the $\mathbb{C}$-vector space $M_\rho(\mathrm{Sp}_{2g}(\mathbb{Z}))$ of Siegel modular forms of weight ρ, genus g for $\mathrm{Sp}_{2g}(\mathbb{Z})$. Then one can construct a more general $M(\mathrm{Sp}_{2g}(\mathbb{Z}))$-module of Siegel modular forms $M_{\mathrm{vect}}(\mathrm{Sp}_{2g}(\mathbb{Z})) = \oplus_\rho M_\rho(\mathrm{Sp}_{2g}(\mathbb{Z}))$. In general this is not finitely generated.

However there is still an analogue of Lemma 1.1.13 in this more general setting. Note that if ρ decomposes as $\rho = \rho_1 \oplus \rho_2$ then $M_\rho(\mathrm{Sp}_{2g}(\mathbb{Z})) =$

$M_{\rho_1}(\mathrm{Sp}_{2g}(\mathbb{Z})) \oplus M_{\rho_2}(\mathrm{Sp}_{2g}(\mathbb{Z}))$. Thus in practice we need only concern ourselves with the case that ρ is irreducible.

Siegel modular forms possess Fourier expansions too. For a fixed genus g let S_g be the set of $g \times g$ half integral matrices with integral diagonal elements. Such matrices parametrize quadratic forms in g variables with integer coefficients.

If $F \in M_\rho(\mathrm{Sp}_{2g}(\mathbb{Z}))$ then the Fourier expansion of F is of the form:

$$F(Z) = \sum_{T \in S_g} a(T) e^{2\pi i \mathrm{Tr}(TZ)}.$$

Note how the Fourier coefficients are no longer indexed by integers but by integer quadratic forms in g variables. There are various results about these Fourier coefficients. For example similar T have related Fourier coefficients and $a(T) = 0$ for T that are not positive semi-definite. Compare this with $a_{-n} = 0$ for elliptic modular forms.

Recall that a genus 1 form is a cusp form if the constant term in the q-expansion is $a_0 = 0$. We have a similar condition for arbitrary genus.

Definition 1.2.4. A Siegel modular form $F \in M_\rho(\mathrm{Sp}_{2g}(\mathbb{Z}))$ is a cusp form if $a(T) = 0$ for each $T \in S_g$ that is positive semi-definite but not definite. □

There is another equivalent definition of cusp form that captures the notion of "zero at infinity". One can define the Siegel operator on $M_\rho(\mathrm{Sp}_{2g}(\mathbb{Z}))$ via:

$$\Phi(F)(Z') = \lim_{t \to \infty} F \begin{pmatrix} Z' & 0 \\ 0 & it \end{pmatrix},$$

where $Z' \in \mathcal{H}_{g-1}$ and $t \in \mathbb{R}$. This operator produces a Siegel modular form of genus $g-1$ (the weight can also be described). A cusp form is precisely a form that satisfies $\Phi(F) = 0$.

Let us now consider the notion of congruence subgroup of $\mathrm{Sp}_{2g}(\mathbb{Z})$.

Definition 1.2.5. The principal congruence subgroup of genus g, level N is given by:

$$\Gamma^{(2g)}(N) = \left\{ A \in \mathrm{Sp}_{2g}(\mathbb{Z}) \,|\, A \equiv I_{2g} \bmod N \right\}.$$

A subgroup $\Gamma \subseteq \mathrm{Sp}_{2g}(\mathbb{Z})$ is a congruence subgroup of level N if $\Gamma^{(2g)}(N) \subseteq \Gamma$. □

Congruence subgroups necessarily have finite index in $\mathrm{Sp}_{2g}(\mathbb{Z})$. A popular example is given by:

$$\Gamma_0^{(g)}(N) = \{\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_{2g}(\mathbb{Z}) \,|\, A, B, C, D \in M_g(\mathbb{Z}), C \equiv 0 \bmod N\}.$$

This is a straightforward generalization of the genus 1 congruence subgroup $\Gamma_0(N)$. When the genus is understood we will omit it from the notation.

We note that given a congruence subgroup Γ of genus g, level N we may define Siegel modular forms for Γ. It is clear how to do this. By Koecher's principle we do not need to consider behaviour "at the cusps" unless $g = 1$. We will denote such spaces and subspaces of cusp forms by $M_\rho(\Gamma), S_\rho(\Gamma)$.

1.2.2 Genus 2 Siegel modular forms

For the purposes of this thesis we will only need to deal with genus 2 Siegel modular forms and so we will restrict to this case from now on. Here we will discuss possible level p congruence subgroups and Hecke operators associated to spaces of Siegel modular forms.

First recall that an irreducible representation of $\mathrm{GL}_2(\mathbb{C})$ is parametrised by its highest weight, this being a pair of integers (λ_1, λ_2) such that $\lambda_1 \geq \lambda_2 \geq 0$. It is known that for $j, k \geq 0$ the irreducible representation of highest weight $(j + k, k)$ has an explicit desciption as the representation $\mathrm{Symm}^j(\mathbb{C}^2) \otimes \det^k$, where $\mathrm{GL}_2(\mathbb{C})$ is acting via matrix multiplication on $\mathbb{C}^2$.

Definition 1.2.6. If $g = 2$ and $\rho = \mathrm{Symm}^j(\mathbb{C}^2) \otimes \det^k$ then the spaces $M_\rho(\mathrm{Sp}_4(\mathbb{Z}))$ and $S_\rho(\mathrm{Sp}_4(\mathbb{Z}))$ will be written as $M_{j,k}(\mathrm{Sp}_4(\mathbb{Z}))$ and $S_{j,k}(\mathrm{Sp}_4(\mathbb{Z}))$ respectively. □

As mentioned earlier we know that these spaces are finite dimensional. For odd j we have $\dim(M_{j,k}(\mathrm{Sp}_4(\mathbb{Z}))) = 0$. Further there exist dimension formulae for even j [65].

In order to discuss possible congruence subgroups we note that two interesting examples exist at genus 2. Other than the subgroups $\Gamma_0(N)$ we have the paramodular groups:

$$K(N) = \begin{pmatrix} \mathbb{Z} & N\mathbb{Z} & \mathbb{Z} & \mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} & \mathbb{Z} & \frac{1}{N}\mathbb{Z} \\ \mathbb{Z} & N\mathbb{Z} & \mathbb{Z} & \mathbb{Z} \\ N\mathbb{Z} & N\mathbb{Z} & N\mathbb{Z} & \mathbb{Z} \end{pmatrix} \cap \mathrm{Sp}_4(\mathbb{Q}).$$

The paramodular groups may look strange but they appear in the Paramodular Conjecture, the genus 2 analogue of the modularity theorem for elliptic curves. This conjecture was originally made by Brumer and Kramer but evidence has recently been given in [53]. In this thesis we will mainly be interested in modular forms for $K(p)$, where p is prime.

It should be noted that Roberts and Schmidt have developed a theory of newforms for the paramodular group but this is not as straightforward as for

$\Gamma_0(N)$ since $K(M)$ is never a subgroup of $K(N)$ for any $M \neq N$ (so there are no obvious inclusions $S_{j,k}(K(M)) \hookrightarrow S_{j,k}(K(N))$). We will not state the details but refer the reader to [57].

Essentially Schmidt has constructed maps that multiply the level by p and p^2 for a prime p, giving non-trivial inclusions $S_{j,k}(K(N)) \hookrightarrow S_{j,k}(K(Np))$ and $S_{j,k}(K(N)) \hookrightarrow S_{j,k}(K(Np^2))$. He then defines the subspace of oldforms $S_{j,k}^{\mathrm{old}}(K(N))$ in the usual fashion; the subspace of $S_{j,k}(K(N))$ generated by the images of these maps from lower levels. The orthogonal complement of $S_{j,k}^{\mathrm{old}}(K(N))$ with respect to the Petersson inner product is the space of newforms $S_{j,k}^{\mathrm{new}}(K(N))$.

In our case we will be needing only paramodular forms of prime level p. Here the notion of "oldform" means what we expect, forms that come from level 1, i.e. $\mathrm{Sp}_4(\mathbb{Z})$ (although this is only intuition since the way we are lifting the level is non-trivial).

Finally we define Hecke operators on spaces of Siegel modular forms. The treatment is similar to the theory for elliptic modular forms but here we will not work in total generality.

We first generalize the weight k slash operator to genus 2. This can in fact be done easily for any genus.

If $F : \mathcal{H}_2 \to V$ and $\alpha \in \mathrm{GSp}_4^+(\mathbb{Q})$ (positive similitude) then the weight (j,k) slash operator is defined by:

$$(F|_{j,k}\alpha)(Z) = \mu(\alpha)^{j+k-3}\rho(j(\alpha,Z))^{-1}F(\alpha Z).$$

For each prime p we may define Hecke operators T_p and T_{p^2}. To do this we decompose the double cosets:

$$K(N)\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix}K(N) = \coprod_i K(N)\mu_i$$

$$K(N)\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ 0 & 0 & p^2 & 0 \\ 0 & 0 & 0 & p \end{pmatrix}K(N) = \coprod_i K(N)\eta_i.$$

As usual there are finitely many representatives in each decomposition.

If $F \in S_{j,k}(K(N))$ we set:

$$T_p(F) = \sum_i F|_{j,k}\mu_i$$

$$T_{p^2}(F) = \sum_i F|_{j,k}\eta_i.$$

The resulting functions indeed lie in $S_{j,k}(K(N))$ and the maps T_p, T_{p^2} are called the Hecke operators at prime p. There is a larger family of Hecke operators but we shall not concern ourselves with them here.

It should be noted that unlike elliptic modular forms the Hecke operator T_{p^2} cannot be written in terms of T_p.

As with elliptic modular forms it is possible to find a basis for the spaces $S_{j,k}(K(N))$ consisting of eigenforms for all Hecke operators with index p coprime to N.

The new subspace is preserved by the Hecke operators and it is possible to find a basis for $S^{\text{new}}_{j,k}(K(N))$ consisting of eigenforms for all Hecke operators. Such forms have Hecke eigenvalues that are algebraic integers and again the field of definition $\mathbb{Q}_F$ obtained by adjoining all Hecke eigenvalues is a number field.

One final remark is that Siegel modular forms are much more difficult to calculate with than elliptic modular forms. For example finding dimensions of new subspaces and Hecke eigenvalues for spaces of paramodular forms is a very tough thing to do. This will be a massive stumbling block when trying to generate level p evidence for Harder's conjecture (to be discussed).

One of the major aims of this thesis is to demonstrate a way of finding these objects by moving out of the spaces of Siegel modular forms and instead working with algebraic modular forms.

1.3 Harder's conjecture

Harder's conjecture predicts specific congruences between the Hecke eigenvalues of elliptic and Siegel modular forms. In some sense they generalise the famous 691 congruence of Ramanujan (see Example 1.1.23). Such congruences are known to be of use in describing the decomposition of certain Galois representations into smaller pieces (as we shall see in Chapter 5). Also they give evidence towards the Bloch-Kato conjecture and provide the existence of elements of certain orders in Shafarevich-Tate groups attached to certain motives [5].

Originally Harder's congruences were formulated by studying the decomposition of cohomology of Siegel modular varieties. The full details of this are mentioned in his original paper [31].

Conjecture 1.3.1. *(Harder's conjecture for level* 1*)*

Let j, k be integers with $j > 0$ and $k \geq 3$ and let $f \in S_{j+2k-2}(SL_2(\mathbb{Z}))$ be a normalized Hecke eigenform with eigenvalues a_n.

Suppose that $ord_\lambda(\Lambda_{alg}(f, j+k)) > 0$ for some prime λ of $\mathbb{Q}_f$ lying above a rational prime $l > j + 2k - 2$.

Then there exists a Hecke eigenform $F \in S_{j,k}(Sp_4(\mathbb{Z}))$ with eigenvalues $b_n \in \mathbb{Q}_F$ such that

$$b_p \equiv p^{k-2} + a_p + p^{j+k-1} \bmod \Lambda$$

for all primes p (where Λ is some prime lying above λ in the compositum $\mathbb{Q}_f\mathbb{Q}_F$).

Such a prime λ is often referred to as a "large prime" in the literature.

Before moving on we recall that the algebraic integer $\Lambda_{\text{alg}}(f, j+k) = \frac{\Lambda(f,j+k)}{\Omega}$ depends on a choice of period Ω and that this is unique up to a multiple in $\mathbb{Q}_f^\times$. The exact period used by Harder determines the value $\Lambda_{alg}(f, j + k)$ up to a multiple in $\mathcal{O}_{\mathbb{Q}_f}^\times$ but for our purposes we will use the MAGMA command LRatio. This command computes the norm of $\Lambda_{\text{alg}}(f, j + k)$ but is only accurate up to sign and a power of 2. Neither of these features is a problem to us since we only care about divisibility by large primes.

It should be noted that Harder's conjecture has still not been proved for level 1 forms. However the specific example with $j = 4, k = 10$ and $l = 41$ mentioned in Harder's paper has recently been proved in a paper by Chenevier and Lannes [14]. The proof uses the Niemeier classification of 24-dimensional lattices and is specific to this particular case.

There are Harder-type congruences predicted for the other Hecke operators T_{p^2} but we shall not concern ourselves with those here. The methods developed in this thesis should be applicable to those too, with some minor modification.

1.3.1 Discussion of possible level p Harder's conjecture

There has been a substantial amount of evidence found for Harder's conjecture which will be discussed in the next subsection.

The main aim of this thesis is to provide and study a level p version of this conjecture. In order to do this there are a few details that need attention.

Firstly the level p structure to be used should be decided. On the elliptic side it is generally easiest to consider the congruence subgroup $\Gamma_0(N)$ so we would probably be most interested in studying the existence of congruences for these ones. Given this decision we must now predict the level p structure of our Siegel modular forms. The evidence provided in this thesis suggests that we can (almost) always find a paramodular form satisfying the congruence.

Secondly, we should only expect the congruence to hold away from p, i.e. for Hecke eigenvalues a_q, b_q with prime $q \neq p$.

Thirdly we should only expect the congruence to hold between newforms on both sides. This is not a problem for level 1 because there are no oldforms.

Finally we should not allow the prime λ to lie above the level p. This is a subtle issue that has not been necessary for level 1 computations (also for the level 2 calculations discussed in the next subsection).

Based on these details I give the following conjectural level p version of Harder's conjecture:

Conjecture 1.3.2. *(Level p paramodular Harder's conjecture)*

Let j, k be integers with $j > 0$ and $k \geq 3$ and let $f \in S^{new}_{j+2k-2}(\Gamma_0(p))$ be a normalized Hecke eigenform with eigenvalues a_n.

Suppose that $ord_\lambda(\Lambda_{alg}(f, j+k)) > 0$ for some prime λ of $\mathbb{Q}_f$ lying above a rational prime $l > j + 2k - 2$ (with $l \neq p$).

Then there exists a Hecke eigenform $F \in S^{new}_{j,k}(K(p))$ with eigenvalues $b_n \in \mathbb{Q}_F$ such that

$$b_q \equiv q^{k-2} + a_q + q^{j+k-1} \bmod \Lambda$$

for all primes $q \neq p$ (where Λ is some prime lying above λ in the compositum $\mathbb{Q}_f\mathbb{Q}_F$).

1.3.2 Review of evidence

Following the release of the level 1 conjecture around 2002 there has been a thorough search for evidence. Originally Faber and Van der Geer were able to do computations for cases when $S_{j,k}(\mathrm{Sp}_4(\mathbb{Z}))$ is 1-dimensional. They have now exhausted such spaces and have found the congruence to hold in all cases (for a substantial number of Hecke eigenvalues). Of course this doesn't prove that the congruence holds for all Hecke eigenvalues, due to the absence of a general Sturm bound for Siegel modular forms. Also at level 1 is evidence given for the special case of $j = 2$ by Ghitza, Ryan and Sulon [28].

Moving on to the level p analogue, a substantial amount of evidence has been provided by Bergström et al in the case where $p = 2$ [4]. Their methods are highly cohomological and they are able to collect many level 2 structures in one by associating to them representations of S_6. Again the calculations are mainly done in one dimensional spaces of forms for simplicity. Their methods are specific to level 2 and so finding evidence for other levels has proved difficult generally. However a small amount of evidence is known for levels other than 2. A congruence has been found for $(j, k, p, l) = (0, 3, 61, 43)$ by Anton Mellit (p.99 of [33]).

In this thesis we investigate general methods for finding evidence at any level by utilising the theory of algebraic modular forms and their recent advances. These methods are quite efficient computationally although still non-trivial.

Chapter 2

Quaternion algebras

2.1 Definitions and Examples

To be able to state certain correspondences between modular forms we will need to recall facts from the theory of quaternion algebras. In this chapter we see an overview of the theory.

Definition 2.1.1. Let K be a field with $\mathrm{char}(K) \neq 2$ and take $a, b \in K^\times$. The quaternion algebra $\left(\frac{a,b}{K}\right)$ is the 4-dimensional K-vector space with basis $\{1, i, j, k\}$ and multiplication defined by the relations:

$$\begin{aligned} i^2 &= a \in K^\times \\ j^2 &= b \in K^\times \\ ij &= -ji = k \end{aligned}$$

□

It is clear by definition that quaternion algebras are non-commutative algebras. In fact it is easy to show that the centre of such an algebra is K.

Note that the above conditions are enough to determine k^2 since

$$k^2 = (ij)^2 = -(ij)(ji) = -i(j^2)i = -bi^2 = -ab.$$

Similar arguments give all remaining products of the basis elements.

Example 2.1.2. The idea of the above definition is to generalize Hamilton's quaternions $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$. This quaternion algebra is a division algebra, i.e. every non-zero element has a multiplicative inverse. To see this one easily checks

that the multiplicative inverse of $\alpha + \beta i + \gamma j + \delta k \neq 0$ is:

$$\frac{\alpha - \beta i - \gamma j - \delta k}{\alpha^2 + \beta^2 + \gamma^2 + \delta^2}.$$

This is reminiscent of the multiplicative inverse of a complex number. There are striking similarites as we will see soon.

In fact $\mathbb{H}$ is the only quaternion division algebra over $\mathbb{R}$ (up to isomorphism). This will be clear soon. □

Example 2.1.3. For any field K we can view the matrix algebra $M_2(K)$ as the quaternion algebra $\left(\frac{1,b}{K}\right)$ for any $b \in K^\times$. We may do this by setting up an isomorphism:

$$1 \longmapsto I$$
$$i \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$
$$j \longmapsto \begin{pmatrix} 0 & b \\ 1 & 0 \end{pmatrix}$$

Since $M_2(K)$ contains non-invertible matrices we see that such quaternion algebras are not division algebras. It can be shown that any quaternion algebra over K is either a division algebra or is isomorphic to $M_2(K)$. □

The following lemma gives some nice relationships between quaternion algebras with different parameters a, b:

Lemma 2.1.4. *Given $a, b \in K^\times$ we have the following isomorphisms:*

1. $\left(\frac{a,b}{K}\right) \cong \left(\frac{b,a}{K}\right)$,
2. $\left(\frac{a\mu^2,b}{K}\right) \cong \left(\frac{a,b}{K}\right)$ *for any* $\mu \in K^\times$,

Proof. It is easily checked that the map:

$$i \longmapsto j \qquad j \longmapsto i$$

induces the first isomorphism whereas the map

$$i \longmapsto \mu^{-1} i \qquad j \longmapsto j$$

induces the second. □

Returning to quaternion algebras over $\mathbb{R}$, we now see the classification alluded to above.

Theorem 2.1.5. *Over $\mathbb{R}$ there are two isomorphism classes of quaternion algebras, represented by $\mathbb{H}$ and $M_2(\mathbb{R})$.*

Proof. Consider a fixed choice of $a, b \in \mathbb{R}^\times$. Recall that $M_2(\mathbb{R}) \cong \left(\frac{1,c}{\mathbb{R}}\right)$ for any $c \in \mathbb{R}^\times$.

Now if at least one of a, b is positive then by the first part of the above lemma we may assume that $a > 0$. Then by the second part we see that:

$$\left(\frac{a,b}{\mathbb{R}}\right) = \left(\frac{(\sqrt{a})^2,b}{\mathbb{R}}\right) \cong \left(\frac{1,b}{\mathbb{R}}\right) \cong M_2(\mathbb{R}).$$

Otherwise both $a, b < 0$ and thus:

$$\left(\frac{a,b}{\mathbb{R}}\right) = \left(\frac{-(\sqrt{-a})^2,-(\sqrt{-b})^2}{\mathbb{R}}\right) \cong \left(\frac{-1,-1}{\mathbb{R}}\right) = \mathbb{H}.$$

Thus there are at most two isomorphism classes. However $\mathbb{H} \ncong M_2(\mathbb{R})$ since $\mathbb{H}$ is a division algebra whereas $M_2(\mathbb{R})$ is not. Hence there are exactly two isomorphism classes. □

Analysing the above proof in more detail we notice that the only obstacle stopping $\mathbb{H}$ and $M_2(\mathbb{R})$ being isomorphic was really the absence of square roots of negative numbers. Thus we see that over $\mathbb{C}$ there should only be one isomorphism class of quaternion algebras, represented by $M_2(\mathbb{C})$. In particular $\mathbb{H} \otimes_{\mathbb{R}} \mathbb{C} \cong M_2(\mathbb{C})$.

More generally, it is clear that if L/K is a field extension then $\left(\frac{a,b}{K}\right) \otimes L \cong \left(\frac{a,b}{L}\right)$ by extension of scalars.

Definition 2.1.6. Let D be a quaternion algebra over a field K and let L/K be an extension. We say that L splits D if $D \otimes L \cong M_2(L)$. □

Thus we see that $\mathbb{C}$ splits $\mathbb{H}$. By the same argument

Proposition 2.1.7. *Let D be a quaternion algebra over a field K. Then any algebraic closure $\overline{K}$ splits D.*

Proof. As mentioned above $D \otimes \overline{K}$ is a quaternion algebra over $\overline{K}$. But all such quaternion algebras are isomorphic to $M_2(\overline{K})$. To see this take a quaternion algebra over $\overline{K}$, i.e. $D' \cong \left(\frac{a,b}{\overline{K}}\right)$ for some $a, b \in \overline{K}^\times$. Then since $\overline{K}$ is algebraically closed there exists $c \in \overline{K}^\times$ such that $c^2 = a$.

We then see that:

$$D' \cong \left(\frac{a,b}{\overline{K}}\right) \cong \left(\frac{c^2,b}{\overline{K}}\right) \cong \left(\frac{1,b}{\overline{K}}\right) \cong M_2(\overline{K}).$$

□

In fact we can do better than this. We only really need the introduction of a single square root to split a quaternion algebra.

Proposition 2.1.8. *Let D be a quaternion algebra over a field K. Then there exists a quadratic extension of K that splits D.*

Proof. Let $D \cong \left(\frac{a,b}{K}\right)$ for $a, b \in K^\times$. Then

$$D \otimes K(\sqrt{a}) \cong \left(\frac{a,b}{K(\sqrt{a})}\right) = \left(\frac{(\sqrt{a})^2,b}{K(\sqrt{a})}\right) \cong \left(\frac{1,b}{K(\sqrt{a})}\right) \cong M_2(K(\sqrt{a})).$$

□

It is now clear that for each $a, b \in K^\times$ there must exist an embedding:

$$\left(\frac{a,b}{K}\right) \hookrightarrow \left(\frac{a,b}{K(\sqrt{a})}\right) \cong M_2(K(\sqrt{a})),$$

so that any quaternion algebra over K can be embedded inside a matrix algebra (once K is extended to contain $\sqrt{a}$).

For later computations it is necessary to get an explicit description of the above embedding. We do this by realising that since

$$\alpha + \beta i + \gamma j + \delta k = (\alpha + \beta i) + (\gamma + \delta i)j$$

we have an isomorphism of K-algebras

$$\left(\frac{a,b}{K}\right) \cong K(\sqrt{a}) \oplus K(\sqrt{a})j,$$

$$\phi : (\alpha + \beta i) + (\gamma + \delta i)j \longmapsto (\alpha + \beta\sqrt{a}) + (\gamma + \delta\sqrt{a})j.$$

The following is then straight-forward to check.

Lemma 2.1.9. *Let σ be the nontrivial automorphism in $Gal(K(\sqrt{a})/K)$. Then there is an embedding of K-algebras:*

$$K(\sqrt{a}) \oplus K(\sqrt{a})j \hookrightarrow M_2(K(\sqrt{a}))$$

$$\psi : x + yj \longmapsto \begin{pmatrix} x & y \\ b\sigma(y) & \sigma(x) \end{pmatrix}.$$

Thus $\psi \circ \phi$ gives an embedding $\left(\frac{a,b}{K}\right) \hookrightarrow M_2(K(\sqrt{a}))$.

For example $\mathbb{H} = \left(\frac{-1,-1}{\mathbb{R}}\right)$ embeds in $M_2(\mathbb{C})$ via

$$\alpha + \beta i + \gamma j + \delta k \longmapsto \begin{pmatrix} \alpha + \beta i & \gamma + \delta i \\ -\gamma + \delta i & \alpha - \beta i \end{pmatrix}.$$

2.2 Norms and Traces

We have just seen that a quaternion algebra is essentially a non-commutative quadratic extension of a quadratic field. We would like to define norms and traces for quaternion algebras, much like we do for number fields. For this we need an analogue of complex conjugation.

Definition 2.2.1. Let D be a quaternion algebra over field K. An involution on a quaternion algebra D is a K-linear map $^- : D \to D$ such that for all $\alpha, \beta \in D$:

- $\overline{1} = 1$
- $\overline{\alpha\beta} = \overline{\beta}\overline{\alpha}$
- $\overline{\overline{\alpha}} = \alpha$

□

From this definition it is clear that $\overline{\alpha^{-1}} = (\overline{\alpha})^{-1}$ always holds.

Recall that if L/K is a quadratic extension of number fields and σ is the non-trivial automorphism in $\mathrm{Gal}(L/K)$ then we define the norm and trace maps via:

$$N(\alpha) = \alpha\sigma(\alpha),$$

$$tr(\alpha) = \alpha + \sigma(\alpha).$$

These quantities are fixed by the action of the Galois group and hence lie in K (since the extension is Galois).

If we are to do the same for quaternion algebras it seems natural to use an involution in place of σ. However, there are many involutions one may take on a quaternion algebra and due to the lack of "Galois theory" we cannot always have that $\alpha\overline{\alpha} \in K$ and $\alpha + \overline{\alpha} \in K$ for all $\alpha \in D$ (even though these elements are fixed by the involution). Thus we make an extra definition.

Definition 2.2.2. An involution on D is called standard if $\alpha\overline{\alpha} \in K$ for all $\alpha \in D$. □

Given a standard involution we may define the norm and trace:

$$N(\alpha) = \alpha\overline{\alpha} \in K$$

$$\mathrm{tr}(\alpha) = \alpha + \overline{\alpha} \in K.$$

(The fact that $\mathrm{tr}(\alpha) \in K$ given $N(\alpha) \in K$ is a simple consequence of the fact that $N(1+\alpha) = (1+\alpha)\overline{(1+\alpha)} \in K$.)

A nice result about standard involutions is the following.

Proposition 2.2.3. *Let D be a quaternion algebra. Then D has a unique standard involution.*

The proof of this can be found in Corollary 2.15 of [67]. For the rest of this Subsection most proofs will be omitted and can be found in Voight's book.

Example 2.2.4. For any field K, the quaternion algebra $M_2(K)$ has the adjoint transpose

$$\mathrm{adj}\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)^T = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}$$

as its standard involution since:

$$A(\mathrm{adj}(A)^T) = \det(A)I.$$

Thus the norm here is the determinant map and the trace is the usual trace since:

$$A + \mathrm{adj}(A)^T = (a+d)I.$$

□

Example 2.2.5. Take $D = \left(\frac{a,b}{K}\right)$ and let $x = \alpha+\beta i+\gamma j+\delta k$ for $\alpha, \beta, \gamma, \delta \in K$. Then the standard involution is given by:

$$\overline{x} = \alpha - \beta i - \gamma j - \delta k$$

since:

$$x\overline{x} = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2 \in K.$$

Thus:

$$N(x) = \alpha^2 - a\beta^2 - b\gamma^2 + ab\delta^2$$

$$\mathrm{tr}(x) = 2\alpha.$$

□

From now on, $\overline{\ }$ will always denote the standard involution applied to x.

It is easy to see that the properties of involutions force the norm to be multiplicative and the trace to be additive. This is again analogous to the number field case.

For Hamilton's quaternions the fact that the norm is multiplicative is really another way of giving Lagrange's four square identity (that if you multiply two sums of four squares you get another sum of four squares). This highlights the arithmetic significance of quaternion algebras.

For an alternative view of the norm and trace consider viewing $D = \left(\frac{a,b}{K}\right)$ as a 2-dimensional left $K(\sqrt{a})$-vector space with basis $\{1, j\}$ (as earlier). Then for $\alpha \in D$ we have the natural right multiplication by α map, $x \mapsto x\alpha$.

By identifying D with $K(\sqrt{a}) \oplus K(\sqrt{a})j$ (via ϕ as defined before Lemma 2.1.9) we see that this map is represented by a 2×2 matrix $A_\alpha \in M_2(K(\sqrt{a}))$, Thus we have a degree 2 characteristic polynomial

$$f_\alpha(x) = x^2 - \mathrm{tr}(A_\alpha)x + \det(A_\alpha) \in K(\sqrt{a})[x].$$

Proposition 2.2.6.

$$f_\alpha(x) = x^2 - tr(\alpha)x + N(\alpha) \in K[x].$$

Proof. Let σ be the non-trivial automorphism in $\mathrm{Gal}(K(\sqrt{a})/K)$. It is a simple calculation to see that if $\phi(\alpha) = \alpha_1 + \alpha_2 j$ for $\alpha_1, \alpha_2 \in K(\sqrt{a})$ then:

$$A_\alpha = \begin{pmatrix} \alpha_1 & b\sigma(\alpha_2) \\ \alpha_2 & \sigma(\alpha_1) \end{pmatrix}$$

It is now clear that $\mathrm{tr}(A_\alpha) = \mathrm{tr}(\alpha)$ and $\det(A_\alpha) = N(\alpha)$. Since these quantities lie in K we see that the characteristic polynomial is indeed defined over K as claimed. □

Recall the Cayley-Hamilton theorem. This says that $f_\alpha(\alpha) = 0$, a fact we will need to use later.

2.3 Ramification and classification results

We now seek to classify quaternion algebras. For local fields it turns out that quaternion algebras are easily described.

Theorem 2.3.1. *Let K be a local field not isomorphic to $\mathbb{C}$. Then there are exactly two isomorphism classes of quaternion algebras over K, consisting of the isomorphism class of $M_2(K)$ and the isomorphism class of some division algebra E_K.*

We have already seen this in action for the case $K = \mathbb{R}$. In this case we may take $E_{\mathbb{R}} = \mathbb{H}$.

Let K be a number field and D be a quaternion algebra over K. Then for each place v of K we can consider the quaternion algebra $D_v := D \otimes K_v$, where K_v is the completion at v. Now K_v is a local field, so D_v will be isomorphic either to $M_2(K_v)$ or to E_{K_v}.

Definition 2.3.2. Say D is split at v if $D_v \cong M_2(K_v)$, or ramified at v if $D_v \cong E_{K_v}$. □

It turns out that quaternion algebras over number fields can be classified by their ramification behaviour.

Theorem 2.3.3. *Let D/K be a quaternion algebra over a number field. Then D ramifies at a finite number of places and this number is even.*

Further, for each finite subset of places of even cardinality there exists exactly one isomorphism class of quaternion algebras that ramify at those places.

As with extensions of number fields there is an ideal called the discriminant that measures the ramification of a quaternion algebra. However this will not be important to us. Our main motivation will be to study quaternion algebras over $\mathbb{Q}$ that are ramified at p and ∞ for some prime p.

Definition 2.3.4. Let D be a quaternion algebra over $\mathbb{Q}$. Say D is definite if it is ramified at ∞, i.e. $D_\infty \cong \mathbb{H}$, and indefinite if it is split at ∞, i.e. $D_\infty \cong M_2(\mathbb{R})$. □

Definite and indefinite quaternion algebras behave in completely different ways. The main difference is due to the definite/indefinite nature of their norm forms. This is analogous to the difference between imaginary and real quadratic fields, where the nature of the norm form really determines the difference in arithmetic (units, class numbers etc).

Of course if we write $D = \left(\frac{a,b}{\mathbb{Q}}\right)$ then it is easy to see that D is definite if and only if both $a, b < 0$ (see the proof of Theorem 2.1.5). In this case it is obvious that the norm form is positive definite.

As mentioned above, we will ultimately concern ourselves with definite quaternion algebras ramified at a single prime. By the classification theorem above we know that for a fixed prime there is only one isomorphism class of such algebras. In fact it isn't too difficult to find a representative.

Proposition 2.3.5. *Let p be a prime and suppose D is a definite quaternion*

algebra over $\mathbb{Q}$ ramified at p. Then D is isomorphic to:

$$\begin{aligned}
&\left(\frac{-1,-1}{\mathbb{Q}}\right) && \text{if } p = 2\\
&\left(\frac{-1,-p}{\mathbb{Q}}\right) && \text{if } p \equiv 3 \bmod 4\\
&\left(\frac{-2,-p}{\mathbb{Q}}\right) && \text{if } p \equiv 5 \bmod 8\\
&\left(\frac{-l,-p}{\mathbb{Q}}\right) && \text{if } p \equiv 1 \bmod 8,
\end{aligned}$$

where $l \equiv 3 \bmod 4$ is a prime that is a square mod p.

The above proposition is linked heavily with Hilbert symbols and quadratic reciprocity. It is proved in [13]. The key idea is to study the norm form locally at each prime and try to force it to properly represent 0 in $\mathbb{Q}_q$ for $q \neq p$ and not to represent 0 in $\mathbb{Q}_p$. By Hensel's lemma, this reduces to a quadratic non-residue calculation in $\mathbb{F}_p$.

2.4 Integrality and maximal orders

Naturally we assign a notion of integrality to elements of quaternion algebras over number fields. It is clear how we should do this.

Definition 2.4.1. Let D be a quaternion algebra over a number field K, with ring of integers $\mathcal{O}_K$. An element $\alpha \in D$ is integral if $N(\alpha), \mathrm{tr}(\alpha) \in \mathcal{O}_K$ (so that the characteristic polynomial is defined over $\mathcal{O}_K$). □

It is now tempting to define the set of all integral elements and hope that this behaves exactly like the ring of integers of a number field. Unfortunately this set is not even a ring in general.

For example, in $M_2(K)$ consider the elements $A = \begin{pmatrix} 0 & \frac{1}{4} \\ 4 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 4 \\ \frac{1}{4} & 0 \end{pmatrix}$. Now A and B are integral since both have trace 0 and determinant 1, both of which lie in $\mathcal{O}_K$. However $A+B = \begin{pmatrix} 0 & \frac{17}{4} \\ \frac{17}{4} & 0 \end{pmatrix}$ and $AB = \begin{pmatrix} \frac{1}{16} & 0 \\ 0 & 16 \end{pmatrix}$ and neither of these are integral.

The correct way to proceed is to adopt instead the view that the ring of integers of a number field is the "maximal order". Thus for quaternion algebras we consider nice enough subrings of this set of integral elements.

Definition 2.4.2. Let K be a number field or a completion of a number field at a finite place and let $\mathcal{O}_K$ denote the ring of integers of K.

An order in a quaternion algebra D over K is a free $\mathcal{O}_K$-module of rank 4 that is also a subring of D.

A maximal order is an order that is not properly contained in any other order. □

Maximal orders definitely exist (Zorn's lemma) but there is usually more than one. This does not happen with number fields; the ring of integers is the unique maximal order.

Example 2.4.3. In $D = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ the sets $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$ and $\mathcal{O}' = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\frac{1+i+j+k}{2}$ are both orders in D. However $\mathcal{O} \subset \mathcal{O}'$ and so $\mathcal{O}$ cannot be maximal. It can be shown that $\mathcal{O}'$ is maximal but we omit the argument. The maximal order $\mathcal{O}'$ is known as the ring of Hurwitz quaternions. □

There are general algorithms for constructing maximal orders, involving the discriminant (again similar to number fields). We will not go into these in detail here, but note that there is a standard way to generate a maximal order for a definite quaternion algebra over $\mathbb{Q}$ ramified at a single prime p [38].

For the split quaternion algebra $M_2(\mathbb{Q}_p)$ we have a simple description of all maximal orders:

Proposition 2.4.4. *Every maximal order in $M_2(\mathbb{Q}_p)$ is conjugate by an element of $GL_2(\mathbb{Q}_p)$ to $M_2(\mathbb{Z}_p)$.*

This is a special case of Corollary 1.19 on p.30 of Voight's book [67] and will be useful in the next subsection.

Finally we note that the norm is still a useful tool for detecting units.

Proposition 2.4.5. *Let D be a definite quaternion algebra over $\mathbb{Q}$. Let $\mathcal{O}$ be a maximal order. Then $\mathcal{O}^\times = \{\alpha \in \mathcal{O} \mid N(\alpha) = 1\}$.*

Proof. Given an inverse for α lying in $\mathcal{O}$ we know that $\alpha\alpha^{-1} = 1$. Taking norms of both sides tells us that $N(\alpha) \in \mathcal{O}_\mathbb{Q}^\times = \mathbb{Z}^\times = \pm 1$. However the norm form is positive definite so that $N(\alpha) = 1$.

Conversely $N(\alpha) = 1$ implies that $\alpha\overline{\alpha} = 1$ so α is invertible in D. In fact it must be invertible in $\mathcal{O}$ since the involution preserves $\mathcal{O}$. □

Chapter 3

Algebraic modular forms

We begin by first transforming the classical notion of elliptic modular form into an object known as an automorphic form. Similar processes can be followed for Siegel modular forms and most other types of modular forms (Hilbert, Maass, Bianchi, etc), suggesting that the notion of automorphic form is the natural unification of all known theories for modular forms. More generally a space of automorphic forms will exist for arbitrary reductive groups.

It should be mentioned that traditionally one then goes from this theory into the theory of automorphic representations in order to truly study automorphic forms and their connections to the Langlands program. In this chapter we will not consider these topics since our main interest is in the forms themselves.

Algebraic modular forms are something similar to automorphic forms but for special groups. They have recently become extremely useful due to the fact that they are easier to compute with (see [18], [22], [48]).

In many cases one can find deep links between classical modular forms and certain algebraic counterparts. This allows transformation of complicated calculations on the classical side into much simpler calculations on the algebraic side.

We will see major examples of this philosophy by studying certain correspondences of Eichler and Ibukiyama for elliptic and Siegel modular forms respectively. It should be noted that such correspondences are naturally understood in terms of automorphic representations but we will not take this stance.

3.1 Classical automorphic forms

The study of automorphic forms is at the center of modern number theory. As mentioned previously they are a natural generalisation of the notion of modular form.

In order to motivate the ideas we will observe the rite of passage involved in promoting elliptic modular forms to automorphic forms. It is possible to carry out similar procedures for other common types of modular form but the details are not important to us here.

The approach here will be mainly taken from Chapter 7 of [7] although we will only see a brief overview of the theory.

To start the process we take an elliptic modular form $f \in S_k(\Gamma_0(N))$. Thus f is a holomorphic function $\mathcal{H} \to \mathbb{C}$ with specific transformation properties.

The action of $\mathrm{GL}_2^+(\mathbb{R}) = \{A \in \mathrm{GL}_2(\mathbb{R}) \,|\, \det(A) > 0\}$ on $\mathcal{H}$ is transitive as seen in Chapter 1. The element $i \in \mathcal{H}$ is special since the stabilizer of this element under the action is easily described, it is $K_\infty = Z_\infty K'$, where $Z_\infty := \{\mathrm{diag}(z,z) \,|\, z \in \mathbb{R}^\times\}$ is the center of $\mathrm{GL}_2^+(\mathbb{R})$ and $K' = \mathrm{SO}_2(\mathbb{R})$ is a maximal connected compact subgroup of $\mathrm{GL}_2^+(\mathbb{R})$.

We may now associate to f a smooth function Φ_f on $\mathrm{GL}_2^+(\mathbb{R})$ by "undoing" the action of the automorphy factor at i:

$$\Phi_f : \mathrm{GL}_2^+(\mathbb{R}) \longrightarrow \mathbb{C}$$

$$\Phi_f(g_\infty) = j(g_\infty, i)^{-k} f(g_\infty i).$$

Here the automorphy factor on $\mathrm{GL}_2^+(\mathbb{R})$ is extended from $\mathrm{SL}_2(\mathbb{R})$ by defining it as $j(\gamma, z) = \det(\gamma)^{-\frac{1}{2}}(cz + d)$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{R})$. This clearly agrees with the usual automorphy factor if we restrict to $\gamma \in \mathrm{SL}_2(\mathbb{R})$.

Note that from Φ_f we may recover f via $f(z) = j(g_\infty, i)^k \Phi(g_\infty)$ where $g_\infty \in \mathrm{GL}_2^+(\mathbb{R})$ is such that $z = g_\infty i$ (this exists by the transitivity of the action).

The following are simple consequences of the transformation properties of f.

Theorem 3.1.1. *The function Φ_f has the following properties:*

- $\Phi_f(\gamma g_\infty) = \Phi_f(g_\infty)$ *for each* $\gamma \in \Gamma_0(N)$.
- $\Phi_f(g z k_\theta) = \Phi_f(g_\infty) e^{ik\theta}$ *for each* $z k_\theta \in K_\infty$.

The first of these properties tells us that ϕ_f is well defined as a function on the coset space $\Gamma_0(N) \backslash \mathrm{GL}_2^+(\mathbb{R})$. This encodes the transformation property and

the level of the modular form f. The second property tells us how the weight of f is encoded in the action of the maximal connected compact subgroup K'.

It remains to see how we may capture the holomorphicity of f algebraically. First note that the Lie algebra $\mathfrak{gl}_2 = M_2(\mathbb{R})$ of $\mathrm{GL}_2^+(\mathbb{R})$ acts on smooth functions $\Phi : \mathrm{GL}_2^+(\mathbb{R}) \to \mathbb{C}$. For $X \in \mathrm{M}_2(\mathbb{R})$ this action is as follows:

$$X \cdot \Phi(g_\infty) = \frac{d}{dt}(\Phi(g_\infty \exp(tX)))_{t=0}.$$

By extending this action linearly we can allow the action of the complexification $\mathfrak{g} = \mathfrak{gl}_2 \otimes \mathbb{C}$. Two special elements of this Lie algebra are:

$$X_\pm = \frac{1}{2}\begin{pmatrix} 1 & \pm i \\ \pm i & -1 \end{pmatrix} \in \mathfrak{g}.$$

The action of these elements raise and lower the weight, i.e. for $k_\theta \in K'$ we have:

$$X_\pm \cdot \Phi(g_\infty k_\theta) = \Phi(g_\infty) e^{i\theta(k \pm 2)}.$$

The following intriguing result is the sought after analogue of holomorphicity, linking the action of X_- with the Cauchy-Riemann equations.

Lemma 3.1.2. *The modular form f is holomorphic if and only if $X_- \cdot \Phi_f = 0$.*

So now we have embedded $S_k(\Gamma_0(N))$ into a space of functions $\mathrm{GL}_2^+(\mathbb{R}) \to \mathbb{C}$ with the properties given in the above theorem and lemma.

Indeed one can study these spaces and produce nice results about modular forms but we are not quite finished yet. At the moment we are only focusing on a single completion of $\mathbb{Q}$ but experience tells us that we should be considering all completions, i.e. we would like to lift to a function on the adelic group $\mathrm{GL}_2(\mathbb{A})$.

In order to do so we must first think about what the analogue of $\Gamma_0(N)$ would be. What we require is a subgroup of $\mathrm{GL}_2(\mathbb{Q}_p)$ for each p that locally behaves like $\Gamma_0(N)$. For any prime p we may make the obvious choice:

$$K_p(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p) \middle| c \in p^{\mathrm{ord}_p(N)}\mathbb{Z}_p \right\} \subset \mathrm{GL}_2(\mathbb{Q}_p).$$

Note that if $p \nmid N$ then we have $K_p(N) = \mathrm{GL}_2(\mathbb{Z}_p)$ and so it makes sense to say that $K_f(N) = \prod_p K_p(N)$ is a subgroup of $\mathrm{GL}_2(\mathbb{A}_f)$. In fact it is an open compact subgroup. We also consider the open compact subgroup $K(N) = K_\infty K_f(N)$ of $\mathrm{GL}_2(\mathbb{A})$.

Recall the following decomposition of $\mathbb{A}^\times$:

$$\mathbb{A}^\times = \mathbb{Q}^\times \, \mathbb{R}^+ \hat{\mathbb{Z}}^\times,$$

where $\hat{\mathbb{Z}}^\times = \prod_p \mathbb{Z}_p^\times$. This is the adelic analogue of the Chinese remainder theorem and allows us to lift Dirichlet characters to continuous homomorphisms $\mathbb{Q}^\times\backslash\mathbb{A}^\times \to \mathbb{C}$.

One has a similar theorem for $\mathrm{GL}_2(\mathbb{A})$ and this result will allow us to achieve our goal of lifting Φ_f to a function on $\mathrm{GL}_2(\mathbb{A})$.

Theorem 3.1.3. *(Strong approximation) Suppose $K_f \subset GL_2(\mathbb{A}_f)$ is any open compact subgroup with $det(K_f) = \hat{\mathbb{Z}}^\times$. Then we have the decomposition:*

$$GL_2(\mathbb{A}) = GL_2(\mathbb{Q})GL_2^+(\mathbb{R})K_f.$$

Thus:

$$GL_2(\mathbb{Q})\backslash GL_2(\mathbb{A})/K_f \cong \Gamma\backslash GL_2^+(\mathbb{R}),$$

where $\Gamma = GL_2^+(\mathbb{Q}) \cap K_f$.

In the case where $K_f = K_f(N)$ we recover $\Gamma_0(N) = \mathrm{GL}_2^+(\mathbb{Q}) \cap K_f(N)$ (this is probably easiest to see for $N = 1$).

Note that the strong approximation theorem gives us an adelic version of the modular curve $\Gamma\backslash\mathcal{H}$ (the fundamental domain for the action of Γ on the upper half plane $\mathcal{H}$). Indeed quotienting further:

$$\mathrm{GL}_2(\mathbb{Q})\backslash\mathrm{GL}_2(\mathbb{A})/K_\infty K_f \cong \Gamma\backslash\left(\mathrm{GL}_2^+(\mathbb{R})/K_\infty\right) \cong \Gamma\backslash\left(\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})\right) \cong \Gamma\backslash\mathcal{H}.$$

If we consider this double coset instead over $\mathrm{GL}_2(\mathbb{A}_f)$ then we get a simple space.

Lemma 3.1.4. *$|GL_2(\mathbb{Q})\backslash GL_2(\mathbb{A}_f)/K_f|$ is finite (in fact if K_f is as in the strong approximation theorem then the size is 1).*

This result still holds for any connected reductive group G in place of GL_2 and any open compact subgroup $K_f \subseteq G(\mathbb{A}_f)$ (although strong approximation can fail due to the double quotient being non-trivial). However fixing representatives $g_i \in G(\mathbb{A}_f)$ for $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K_f$ the analogue of Theorem 3.1.3 is:

$$G(\mathbb{Q})\backslash G(\mathbb{A})/K_f \cong \coprod_i \Gamma_i\backslash G(\mathbb{R}),$$

where $\Gamma_i = G(\mathbb{Q}) \cap g_i^{-1}K_f g_i$.

Letting $K_\infty = Z(\mathbb{R})K'$ where Z is the center of G and K' is a maximal connected compact subgroup of $G(\mathbb{R})$ we then get a decomposition of $G(\mathbb{Q})\backslash G(\mathbb{A})/K_\infty K_f$ into a disjoint product of locally symmetric spaces. The role of the upper half plane $\mathcal{H} \cong \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})$ is now given by a connected component of the symmetric space $\mathcal{H}_G = G(\mathbb{R})/K_\infty$ (see Lemma 5.13 of [50]).

We tend to find arithmetic data in the double coset $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K_f$. Later we will see connections to the genus theory of lattices. For now we give its size an appropriate name.

Definition 3.1.5. When the choice of reductive G and open compact K_f is understood the number $h = |G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K_f|$ is referred to as the class number. □

Example 3.1.6. As mentioned earlier, for $G = \mathrm{GL}_2$ or $G = \mathrm{SL}_2$ and any suitable choice of K_f (for example ones corresponding to congruence subgroups) we have class number 1. □

The reason for the use of the term class number is not coincidental. Let F be any number field with ring of integers $\mathcal{O}_F$ and choose an ideal $\mathfrak{m} \subseteq \mathcal{O}_F$. Consider the reductive group $G = \mathbb{G}_m = \mathrm{GL}_1$ and open compact $K_f = \prod_{\mathfrak{p}} K_{\mathfrak{p}}$ with $K_{\mathfrak{p}} = 1 + \mathfrak{m}\mathcal{O}_{F,\mathfrak{p}}$ for each prime ideal $\mathfrak{p} \subset \mathcal{O}_F$. Then:

$$G(F)\backslash G(\mathbb{A}_{F,f})/K_f = I_{F,f}/F^{\times}K_f,$$

where $I_{F,f} = \mathbb{A}_{F,f}^{\times}$ are the finite ideles of F.

This matches the definition of idele ray class groups for moduli with non-archimedean part $\mathfrak{m}$ (see Chapter 3 of [15]). In particular for $\mathfrak{m} = \mathcal{O}_F$ we recover the ideal class group of F and so the notion of class number here is really the size of $G(F)\backslash G(\mathbb{A}_f)/K_f$.

To summarize, so far we have taken $f \in S_k(\Gamma_0(N))$ and produced a function on $\Gamma\backslash \mathrm{GL}_2^+(\mathbb{R})$ with nice properties. Using strong approximation we may now produce a function $\Phi_f : \mathrm{GL}_2(\mathbb{A}) \to \mathbb{C}$ via:

$$\Phi_f(g) = \Phi_f(\gamma g_\infty k) = \Phi_f(g_\infty),$$

where $g \in \mathrm{GL}_2(\mathbb{A}), \gamma \in \mathrm{GL}_2(\mathbb{Q}), g_\infty \in \mathrm{GL}_2^+(\mathbb{R}), k \in K_f(N)$.

We now have the following result:

Theorem 3.1.7. *The map $f \mapsto \Phi_f$ is an isomorphism from $S_k(\Gamma_0(N))$ to the space of functions $GL_2(\mathbb{A}) \to \mathbb{C}$ satisfying:*

- *$\Phi_f(\gamma g k) = \Phi_f(g)$ for all $\gamma \in GL_2(\mathbb{Q})$ and $k \in K_f(N)$.*
- *The function $g_\infty \mapsto \Phi_f(g_\infty g_f)$ is smooth for any $g_f \in GL_2(\mathbb{A}_f)$ and satisfies the properties of Theorem 3.1.1 and Lemma 3.1.2.*
- *The function Φ_f is cuspidal, i.e:*

$$\int_{\mathbb{Q}\backslash\mathbb{A}} \Phi_f\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix} g\right) dx = 0$$

for all $g \in GL_2(\mathbb{A})$.

We will not explain how the third property translates cuspidality of f into this integral condition. A justification is found on p.137 – 138 of [7].

Definition 3.1.8. The function Φ_f is the automorphic form associated to f. □

We note that there are many generalisations of the automorphic forms constructed above.

- One can define automorphic forms for other open compact subgroups by using the exact same process as above.
- Given a character $\omega : \mathbb{Q}^\times \backslash \mathbb{A}^\times \to \mathbb{C}^\times$ we may modify the definition of automorphic form to demand that the center acts by this character, i.e. $\phi_f(gz) = \omega(z)f(g)$ for all $z \in Z_\infty$. Such automorphic forms are said to have central character ω.

  In this fashion modular forms with Dirichlet character χ lift to give automorphic forms with central character ω_χ (where ω_χ is the lift of χ by using strong approximation for $\mathbb{A}^\times$).
- One may define automorphic forms for other number fields, taking care of the possibility that more archimedean places may exist.
- We may define automorphic forms for other reductive groups in place of GL_2.

As a final remark we also note that not all automorphic forms are attached to modular forms. I refer the reader to p.138 – 139 of [7] for a general definition.

3.2 Algebraic modular forms

Algebraic modular forms have been around since the work of Gross [30]. It was generally observed by him that certain reductive groups have automorphic forms that can be described in a purely algebraic way. We will motivate this for certain types of group as well as outlining the underlying theory.

After this we will see the famous correspondence of Eichler between specific spaces of elliptic cusp forms and spaces of algebraic modular forms for multiplicative groups of definite quaternion algebras. This link is the main source of inspiration for the conjectural correspondence of Ibukiyama, which allows us to study certain spaces of Siegel modular forms algebraically too.

Most of the results in this section are well known although the proofs are often neglected. I have tried, where possible to fill in my own proofs.

We start with a connected reductive group $G/\mathbb{Q}$ with the added condition that the Lie group $G(\mathbb{R})$ is connected and compact modulo center.

Recall that a choice of level structure is given by a choice of open compact subgroup $K = K_\infty K_f \subset G(\mathbb{A})$ with $K_\infty = Z(\mathbb{R})K' \subseteq G(\mathbb{R})$ and K' maximal compact.

Let V be (the space of) a finite dimensional algebraic representation of G, defined over a number field F. Fixing a basis of V such a representation returns for each $g \in G$ a matrix $\rho(g) \in \mathrm{GL}_n(F)$ defined by polynomial equations in the entries of g. Since V is viewed as a "weight" for our forms we need this technical assumption to avoid having "fractional" weights.

Definition 3.2.1. The F-vector space of *algebraic modular forms* of level K, weight V for G is:

$$\mathcal{A}(G, K, V) = \{h : G(\mathbb{A}) \to V \mid h(\gamma g k) = k_\infty^{-1} h(g)\,, \forall (\gamma, g, k) \in G(\mathbb{Q}) \times G(\mathbb{A}) \times K\}.$$

□

One sees that the above definition mimics the automorphic form theory, yet it is not the best description to use computationally.

If we undo the action of the infinite component we find that

Lemma 3.2.2. *There is a natural isomorphism of vector spaces:*

$$\mathcal{A}(G, K, V) \cong \{f : G(\mathbb{A}) \to V \mid f(\gamma g k) = \gamma f(g), \forall (\gamma, g, k) \in G(\mathbb{Q}) \times G(\mathbb{A}) \times K\}.$$

Proof. Given $h \in \mathcal{A}(G, K, V)$ we define $f : G(\mathbb{A}) \to V$ via $f(g) = g_\infty h(g)$. The resulting function is easily checked to satisfy the conditions required. Thus the map $h \mapsto f$ is well defined.

It is also trivial to check that this map is an invertible linear map. Hence the two spaces are naturally isomorphic. □

The above lemma lets us trade invariance under $G(\mathbb{Q})$ on the left into invariance under K_∞ on the right. This allows us to minimise the involvement of the infinite place in calculations. From now on we will use this description of the space of algebraic modular forms.

Consider the adelic modular curve $G(\mathbb{Q})\backslash G(\mathbb{A})/K$. Recall that it has a decomposition

$$G(\mathbb{Q})\backslash G(\mathbb{A})/K \cong \coprod_m \Gamma_m \backslash \mathcal{H}_G,$$

where $\mathcal{H}_G = G(\mathbb{R})/K_\infty$ is the symmetric space attached to G. By the assumption on G the symmetric space is finite. Thus the automorphic forms for such a G can be described in purely algebraic terms, since the "modular curve" is finite.

Example 3.2.3. It is easiest to see the above when G is such that $G(\mathbb{R})$ is compact (e.g. special orthogonal and special unitary groups). In this case we are forced to take $K_\infty = G(\mathbb{R})$, so that the symmetric space is a single point. It follows that $G(\mathbb{Q})\backslash G(\mathbb{A})/K$ is in bijection with $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K_f$ (a set known to be finite). For such a group it suffices to define the space of algebraic modular forms as:

$$\mathcal{A}(G, K_f, V) = \{f : G(\mathbb{A}_f) \to V \mid f(\gamma g k_f) = \gamma f(g), \forall(\gamma, g, k_f) \in G(\mathbb{Q})\times G(\mathbb{A}_f)\times K_f\}.$$

□

The groups used in this thesis do not have the property that $G(\mathbb{R})$ is compact. However we may still use the same argument in more generality.

Let S be the maximal split torus in the center of G. Then we have a decomposition $G(\mathbb{R}) = S(\mathbb{R}) \times G(\mathbb{R})_1$, found in the proof of Proposition 1.4 of [30] (where $G(\mathbb{R})_1$ is a certain "norm one" subgroup constructed before the proof).

Example 3.2.4. Let G be such that $G(\mathbb{R})$ is compact modulo center and that the center $Z(\mathbb{R})$ is a split torus. Then $S(\mathbb{R}) = Z(\mathbb{R})$ and $G(\mathbb{R})_1 \cong G(\mathbb{R})/Z(\mathbb{R})$ is maximal compact. Hence the symmetric space $G(\mathbb{R})/Z(\mathbb{R})G(\mathbb{R})_1$ is a single point. Thus in this case we can still view algebraic modular forms as functions on $G(\mathbb{A}_f)$. We will take this stance from now on. □

A natural question to ask is whether these spaces of forms are finite dimensional, as is the case for elliptic and Siegel modular forms. Fortunately they are and this is much easier to prove than expected. In fact, to do this we will see an explicit description of these spaces, which lends itself to computation.

Suppose we have representatives $z_1, z_2, ..., z_h \in G(\mathbb{A}_f)$ for $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K_f$. Then it is easy to see that any $f \in \mathcal{A}(G, K_f, V)$ is determined completely by its values on the representatives z_m. Indeed each $g \in G(\mathbb{A}_f)$ generates a double coset equal to one generated by z_m for some (unique) m. Then $g = \gamma z_m k$ for some $\gamma \in G(\mathbb{Q})$ and $k \in K_f$, so that $f(g) = \gamma f(z_m)$.

It is now clear that the map:

$$\phi : \mathcal{A}(G, K_f, V) \longrightarrow V^h$$
$$f \longmapsto (f(z_1), ..., f(z_h))$$

is an embedding. However ϕ is not an isomorphism since the values $f(z_m)$ cannot be chosen arbitrarily to lie in V. There is a simple restriction that can be placed on these values that does provide an isomorphism, hence an explicit description of the spaces.

Theorem 3.2.5. *The map ϕ induces an isomorphism:*

$$\mathcal{A}(G, K_f, V) \cong \bigoplus_{m=1}^{h} V^{\Gamma_m},$$

where $\Gamma_m = G(\mathbb{Q}) \cap z_m K_f z_m^{-1}$ *for each* m.

Proof. First we see that this map is well defined. Indeed take $f \in \mathcal{A}(G, K_f, V)$. Then for a fixed $1 \leq m \leq h$ we can check that $f(z_m) \in V$ is fixed by the action of Γ_m as follows.

Let $\gamma \in \Gamma_m$ so that $\gamma = z_m k z_m^{-1}$ for some $k \in K_f$. Then since $\gamma \in G(\mathbb{Q})$

$$\gamma f(z_m) = f(\gamma z_m) = f(z_m k z_m^{-1} z_m) = f(z_m k) = f(z_m).$$

The map ϕ is clearly linear and injective and so it remains to prove surjectivity.

Take $(v_1, v_2, ..., v_h) \in \oplus_{m=1}^{h} V^{\Gamma_m}$. Then we may define

$$f : G(\mathbb{A}_f) \to V$$

$$g \longmapsto \gamma v_m$$

whenever $g \in G(\mathbb{Q}) z_m K_f$ with $g = \gamma z_m k$ for $\gamma \in G(\mathbb{Q})$ and $k \in K_f$.

We first show that f is well defined, i.e. independent of the choice of γ, z_m and k. It is clear that the choice of z_m is unique since $z_1, ..., z_h$ form a set of representatives for the double coset $G(\mathbb{Q}) \backslash G(\mathbb{A}_f) / K_f$.

Suppose $\gamma, \gamma' \in G(\mathbb{Q})$ and $k, k' \in K_f$ are such that $\gamma z_m k = \gamma' z_m k'$. Then $\gamma^{-1}\gamma' \in G(\mathbb{Q})$ but also $\gamma^{-1}\gamma' = z_m k k'^{-1} z_m^{-1} \in z_m K_f z_m^{-1}$. Hence $\gamma^{-1}\gamma' \in \Gamma_m$ and since $v_m \in V^{\Gamma_m}$ it is now clear that $\gamma^{-1}\gamma' v_m = v_m$. Thus $\gamma v_m = \gamma' v_m$ and so f is well defined.

It remains to prove that $f \in \mathcal{A}(G, K_f, V)$. Let $\gamma \in G(\mathbb{Q})$, $g \in G(\mathbb{A}_f)$ and $k \in K_f$.

We note that if $g = \gamma' z_m k'$ for some $\gamma' \in G(\mathbb{Q})$ and $k' \in K_f$ then $\gamma g = (\gamma\gamma') z_m k'$ and $gk = \gamma' z_m (k'k)$ and so

$$f(\gamma g) = (\gamma\gamma') v_m = \gamma(\gamma' v_m) = \gamma f(g)$$

$$f(gk) = \gamma' v_m = f(g)$$

as required. □

Corollary 3.2.6. *The spaces* $\mathcal{A}(G, K_f, V)$ *are finite dimensional with*

$$dim(\mathcal{A}(G, K_f, V)) = \sum_{m=1}^{h} dim(V^{\Gamma_m}) \leq h \, dim(V).$$

Proof. This follows from the theorem since V is finite dimensional, so each V^{Γ_m} must also be and $\mathcal{A}(G, K_f, V)$ is a finite direct sum of such spaces. □

Fortunately we know more about the groups Γ_m when G is sufficiently nice.

Proposition 3.2.7. *If $G(\mathbb{R})$ is compact then each Γ_m is a finite group.*

Proof. By the assumption on $G(\mathbb{R})$ each Γ_m is discrete and compact, hence finite (since a disjoint open cover is given by the open sets g for $g \in G$). □

For other groups the Γ_m groups may be infinite.

Example 3.2.8. For a number field F with ring of integers $\mathcal{O}_F$ let $G = \mathrm{Res}_{F/\mathbb{Q}}(\mathbb{G}_m)$. Note that at the infinite place we definitely have compactness modulo center (since this is an abelian group).

Then for $K_f = \prod_{v \nmid \infty} \mathcal{O}_v^\times$ we find that $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K_f$ is the ideal class group of F.

The groups Γ_m are all equal (since again we are in an abelian group). They are all copies of the unit group $\mathcal{O}_F^\times$. It is known that these groups can be infinite (for example if F is a real quadratic number field). □

To fix this issue Gross was able to give several equivalent conditions on a connected reductive group G that guarantee the Γ_m groups to be finite [30]. One such condition is that the group $G(\mathbb{R})_1$ mentioned before Example 3.2.4 is maximal compact. A simpler condition is the following:

Proposition 3.2.9. *The groups Γ_m are finite if and only if $G(\mathbb{Z})$ is finite.*

Note that for the example, $G(\mathbb{Z}) = \mathcal{O}_F^\times$ and in this case the condition captures what we want.

Later we will be interested in the computation of the groups Γ_m but for now it remains to construct Hecke operators for algebraic modular forms.

We do this by first choosing an adelic point $u \in G(\mathbb{A}_f)$ and decomposing the double coset $K_f u K_f = \coprod_{i=1}^r u_i K_f$. As usual a finite number of representatives occur. We then define a Hecke operator T_u on $\mathcal{A}(G, K_f, V)$ via

$$T_u(f)(g) := \sum_{i=1}^r f(gu_i), \qquad \forall g \in G(\mathbb{A}_f).$$

It is easy to see that this is independent of the choice of representatives u_i since they are determined up to right multiplication by K_f.

Proposition 3.2.10. $T_u(f) \in \mathcal{A}(G, K_f, V)$.

Proof. It is clear that if $\gamma \in G(\mathbb{Q})$ then for each $g \in G(\mathbb{A}_f)$:

$$T_u(f)(\gamma g) = \sum_{i=1}^r f((\gamma g)u_i) = \sum_{i=1}^r \gamma f(gu_i) = \gamma T_u(f)(g),$$

Next note that left multiplication by K_f is a faithful action on the left cosets u_iK_f. Indeed given $k \in K_f$ it is clear that $k(u_iK_f) = (ku_i)K_f$ is a left coset of K_f in K_fuK_f. The group action axioms are trivial to check and faithfulness is clear since $(ku_m)K_f = (ku_n)K_f$ implies $u_mK_f = u_nK_f$. Thus for each k there exists a permutation $\sigma \in S_r$ such that $(ku_i)K_f = u_{\sigma(i)}K_f$ for each i.

Thus for each i we may choose $k_{\sigma(i)} \in K_f$ such that $ku_i = u_{\sigma(i)}k_{\sigma(i)}$. Then:

$$T_u(f)(gk) = \sum_{i=1}^{r} f(gku_i) = \sum_{i=1}^{r} f(gu_{\sigma(i)}k_{\sigma(i)}) = \sum_{i=1}^{r} f(gu_{\sigma(i)}) = T_u(f)(g).$$

So $T_u(f) \in \mathcal{A}(G, K_f, V)$ as required. □

Definition 3.2.11. The u_i are often referred to as Hecke representatives and the number r is known as the degree of the Hecke operator T_u, denoted $\deg(T_u)$. □

In practice the choice of u will be of arithmetical significance (instances of this will be clear later).

We wish to find the Hecke representatives explicitly and efficiently. For this purpose a useful observation can be made when the class number is one.

Proposition 3.2.12. *If $h = 1$ then we may choose Hecke representatives that lie in $G(\mathbb{Q})$.*

Proof. Take any set of Hecke representatives $\{u_1, u_2, ..., u_r\}$ for T_u. If $h = 1$ then $G(\mathbb{A}_f) = G(\mathbb{Q})K_f$ (taking the identity as representative for the double quotient).

Thus in particular, for each i there exists $\gamma_i \in G(\mathbb{Q})$ and $k_i \in K_f$ such that $u_i = \gamma_i k_i$. But then $u_iK_f = \gamma_iK_f$ and so we have found a set of rational representatives:

$$K_fuK_f = \coprod u_iK_f = \coprod \gamma_iK_f.$$

□

From a computational perspective it is an advantage to know in advance that the Hecke representatives can be taken to be rational.

Finally we note that for G satisfying Proposition 3.2.9 there is a natural inner product on the space $\mathcal{A}(G, K, V)$. This is given in Gross' paper [30] but we shall give the rough details here.

Lemma 3.2.13. *Let G satisfy the property of Proposition 3.2.9 and V be a finite dimensional algebraic representation of G, defined over $\mathbb{Q}$. Then there exists a character $\mu : G \to \mathbb{G}_m$ and a positive definite symmetric bilinear form $\langle , \rangle : V \times V \to \mathbb{Q}$ such that:*

$$\langle \gamma u, \gamma v \rangle = \mu(\gamma)\langle u, v \rangle$$

for all $\gamma \in G(\mathbb{Q})$.

Proof. We sketch a proof of this result. A complete argument is found in Gross' paper.

For such a G Gross constructs a certain compact subgroup $G(\mathbb{R})_1$ of "norm one" elements (see Gross p.63). This subgroup will be clear in all of our applications.

By the usual averaging argument we can form a real valued $G(\mathbb{R})_1$-invariant inner product on $V \otimes \mathbb{R}$. Using this we can make a $G(\mathbb{Q})_1$-invariant rational valued form on V.

Fixing a maximal torus T lying in the center of G it is known that there exists a character $\chi : T \mapsto \mathbb{G}_m$ and a projection $\pi : G \to T$ such that for $\gamma \in G(\mathbb{R})$:

$$\langle \gamma u, \gamma v \rangle = \chi(\pi(\gamma))^2 \langle u, v \rangle$$

for all $u, v \in V \otimes \mathbb{R}$. This is the central character of V.

One then finds the unique character $\mu : G \to \mathbb{G}_m$ such that $\mu|_T = \chi^2$. Then μ satisfies $\langle \gamma u, \gamma v \rangle = \mu(\gamma)\langle u, v \rangle$ for all $u, v \in V$ and $\gamma \in G(\mathbb{Q})$. □

The character μ actually takes positive values on $G(\mathbb{R})$. On the adeles we get a character $\mu : G(\mathbb{A}) \to \mathbb{A}^\times$. But we may compose this with the natural projection map $\mathbb{A}^\times \to \mathbb{Q}^\times$ given by the decomposition $\mathbb{A}^\times = \mathbb{Q}^\times \mathbb{R}^+ \hat{\mathbb{Z}}^\times$ to give a homomorphism $\mu_{\mathbb{A}} : G(\mathbb{A}) \to \mathbb{Q}^\times$, giving positive values.

Proposition 3.2.14. *Let G satisfy Proposition 3.2.9. Choose representatives $z_1, z_2, ..., z_h \in G(\mathbb{A})$ for $G(\mathbb{Q})\backslash G(\mathbb{A})/K_f$ and fix positive definite symmetric bilinear form on V as in Lemma 3.2.13.*

The space $\mathcal{A}(G, K, V)$ has a natural inner product given by:

$$\langle f, g \rangle = \sum_{m=1}^{h} \frac{1}{|\Gamma_m| \mu_{\mathbb{A}}(z_m)} \langle f(z_m), g(z_m) \rangle,$$

where $\Gamma_m = G(\mathbb{Q}) \cap z_m K z_m^{-1}$.

Proof. The inner product axioms are clear. We show that the definition is independent of the choice of representatives z_m.

Suppose $y_1, ..., y_h$ is another set of representatives, ordered so that $G(\mathbb{Q}) y_m K = G(\mathbb{Q}) z_m K_f$. Then for each m we have $\gamma_m \in G(\mathbb{Q})$ and $k_m \in K$ such that $y_m = \gamma_m z_m k_m$.

Note that Γ_m depends on z_m but the group $\Gamma'_m = G(\mathbb{Q}) \cap y_m K y_m^{-1} = G(\mathbb{Q}) \cap (\gamma_m z_m K z_m^{-1} \gamma_m^{-1}) = \gamma_m \Gamma_m \gamma_m^{-1}$, so that $|\Gamma_m| = |\Gamma'_m|$ is invariant of the choice of representatives.

Then it is clear that:

$$\begin{aligned}
\frac{1}{|\Gamma'_m|\mu_{\mathbb{A}}(y_m)}\langle f(y_m), g(y_m)\rangle &= \frac{1}{|\Gamma_m|\mu_{\mathbb{A}}(\gamma_m z_m k_m)}\langle f(\gamma_m z_m k_m), g(\gamma_m z_m k_m)\rangle \\
&= \frac{1}{|\Gamma_m|\mu(\gamma)\mu_{\mathbb{A}}(z_m)}\langle \gamma_m f(z_m), \gamma_m g(z_m)\rangle \\
&= \frac{\mu(\gamma_m)}{|\Gamma_m|\mu(\gamma)\mu_{\mathbb{A}}(z_m)}\langle f(z_m), g(z_m)\rangle \\
&= \frac{1}{|\Gamma_m|\mu_{\mathbb{A}}(z_m)}\langle f(z_m), g(z_m)\rangle.
\end{aligned}$$

This shows the required independence. □

This inner product is the analogue of the Petersson inner product on usual spaces of modular forms. It can be shown that it behaves well with the Hecke operators, the adjoint of T_u with respect to this inner product is $\mu_{\mathbb{A}}(u)T_{u^{-1}}$.

3.3 Eichler's correspondence

The traditional Eichler correspondence (not to be confused with the Eichler-Shimura correspondence) links certain spaces of elliptic modular forms with spaces of algebraic modular forms for multiplicative groups of quaternion algebras. In modern language this translates into a specific transfer of automorphic representations for the reductive groups $\mathrm{GL}_2(\mathbb{Q})$ and $D^\times$ where D is a quaternion algebra with prescribed properties.

We will only concern ourselves here with the correspondence for level p elliptic modular forms since this is really all the motivation that we need to understand Ibukiyama's correspondence for Siegel modular forms.

Essentially the idea is to shift the notion of "level p" on the elliptic side into ramification at p on the quaternion algebra side.

3.3.1 The correspondence

For the remainder of the thesis D will denote a quaternion algebra over $\mathbb{Q}$ ramified at $\{p, \infty\}$ (for a fixed prime p) and $\mathcal{O}$ will be a fixed maximal order. Then $D_\infty^\times \cong \mathbb{H}^\times$ is connected with center $\mathbb{R}^\times$ (a split torus in $\mathbb{H}^\times$). Also Hamilton's quaternions is compact modulo its center.

Theorem 3.3.1. *There is an isomorphism of Lie groups:*

$$\mathbb{H}^\times/\mathbb{R}^\times \cong SU(2)/\{\pm I\}$$

Proof. Consider the subgroup of unit quaternions

$$\mathbb{H}_1^\times = \{\alpha \in \mathbb{H}^\times \mid N(\alpha) = 1\}$$

(often denoted Sp(1) in the literature). Then the matrix embedding mentioned in Lemma 2.1.9 induces an isomorphism:

$$\mathbb{H}_1^\times \longrightarrow \mathrm{SU}(2)$$

$$\alpha + \beta i + \gamma j + \delta k \longmapsto \begin{pmatrix} \alpha + \beta i & \gamma + \delta i \\ -\gamma + \delta i & \alpha - \beta i \end{pmatrix}$$

Further the isomorphism is clearly continuous under the usual topologies.

Thus we have a natural surjection $\mathrm{SU}(2) \to \mathbb{H}^\times/\mathbb{R}^\times$ that is continuous. The kernel is clearly $\mathrm{SU}(2) \cap \mathbb{R}^\times = \{\pm I\}$ and so the first isomorphism theorem gives the result. □

Due to this result we may consider algebraic modular forms for the group $D^\times$. Also note that all of the Γ_m groups of $D^\times$ will be finite. Indeed D is definite so $D^\times(\mathbb{Z}) = \mathcal{O}^\times$ is finite and the result follows from Proposition 3.2.9.

Let $D_q := D \otimes \mathbb{Q}_q$ be the local component at prime q (no restriction on q) and let $D_{\mathbb{A}_f}$ be the restricted direct product of the D_q's with respect to the local maximal orders $\mathcal{O}_q := \mathcal{O} \otimes \mathbb{Z}_q$.

Lemma 3.3.2. *For any prime $q \neq p$ there exists an isomorphism $\psi : D_q \cong M_2(\mathbb{Q}_q)$ such that:*

- *ψ transfers norm into determinant,*
- *ψ preserves trace maps,*
- *ψ preserves integrality (i.e. $\psi(\mathcal{O}_q) = M_2(\mathbb{Z}_q)$).*

Proof. Since D is split at q there must exist an isomorphism $\phi : D_q \cong M_2(\mathbb{Q}_q)$ by definition.

Recall from Proposition 2.2.3 that standard involutions are unique. It is then clear that $\phi(\overline{x}) = \overline{\phi(x)}$ for all $x \in D_q$. Hence we have $\phi(N(x)) = N(\phi(x)) = \det(\phi(x))$ and $\phi(\mathrm{tr}(x)) = \mathrm{tr}(\phi(x))$ for all $x \in D_q$.

Finally we consider the integrality condition. It is clear that $\phi(\mathcal{O}_q)$ must be a maximal order in $M_2(\mathbb{Q}_q)$. But by Proposition 2.4.4 this maximal order is conjugate to $M_2(\mathbb{Z}_q)$.

We are now done since conjugation preserves determinant and trace. Specifically the required isomorphism ψ is constructed by composing ϕ with the corresponding conjugation map. □

The reductive group $D^\times$ has an interesting connection with GL_2. Notice that once an isomorphism $D_q \to M_2(\mathbb{Q}_q)$ is established we find that:

$$D_q^\times \cong (M_2(\mathbb{Q}_q))^\times = \mathrm{GL}_2(\mathbb{Q}_q).$$

Thus locally away from the ramified prime, $D^\times$ behaves like GL_2.

In fact more is true. It is the case that the reductive groups $D^\times$ and GL_2 are inner forms of each other. Let us recall what this means.

Let G, H be two algebraic groups defined over a field K. It is not necessarily true that G, H are isomorphic over K (i.e. that there is a group isomorphism given by polynomials with coefficients in K). However G, H may become isomorphic if we extend K to a larger field L. If this is the case then we say that G and H are L/K-forms of each other.

It is known that the K-isomorphism classes of L/K-forms of G are in one to one correspondence with the classes of $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}_K(G))$ (note that $\mathrm{Gal}(L/K)$ acts on $\mathrm{Aut}_K(G)$ via $\sigma\alpha = \sigma \circ \alpha \circ \sigma^{-1}$).

The correspondence goes as follows. Let H be an L/K-form of G and let $\phi : G \to H$ be an isomorphism defined over L. For each $\sigma \in \mathrm{Gal}(L/K)$ one can define the map $a_\sigma \in \mathrm{Aut}_K(G)$ via $a_\sigma = \phi^{-1} \circ \sigma\phi$. It is then a lengthy process to show that a_σ is independent of the choice of ϕ and that the map $f_H : \sigma \mapsto a_\sigma$ is in fact a cocycle in $H^1(\mathrm{Gal}(L/K), \mathrm{Aut}_K(G))$. The class $[f_H] \in H^1(\mathrm{Gal}(L/K), \mathrm{Aut}_K(G))$ is then found to correspond to the K-isomorphism class of H.

We find that amongst the L/K-forms of G are certain special forms called L/K-inner forms. These are L/K-forms of G that correspond to classes in $H^1(\mathrm{Gal}(L/K), \mathrm{Inn}_K(G))$ (i.e. ones such that each a_σ is given by a conjugation of G defined over K). If G, H are L/K-inner forms for some L then we omit the extension and just refer to the groups as inner forms.

By the principle of Langlands functoriality (Chapter 11 of [7]) we expect a transfer of automorphic forms between groups that are inner forms of each other (since they have the same "L-group"). Thus we expect a transfer of automorphic forms between $D^\times$ and GL_2. Eichler was able to explicitly describe this transfer for classical modular forms, as we shall see later. Before stating his result we need a few details.

Note that we can produce representations of $D^\times$ from representations of $\mathrm{SU}_2/\{\pm I\}$ via:

$$D^\times \hookrightarrow \mathbb{H}^\times \longrightarrow \mathbb{H}^\times/\mathbb{R}^\times \cong \mathrm{SU}(2)/\{\pm I\}.$$

It is well known that each irreducible representation of $\mathrm{SU}(2)$ is isomorphic to $V_n = \mathrm{Symm}^n(\mathbb{C}^2)$ (for some $n \geq 0$). Here $\mathbb{C}^2$ is the standard representation of $\mathrm{SU}_2(\mathbb{C})$ given by matrix multiplication. For details of this construction see [24]. Clearly V_n gives a well defined representation of $\mathrm{SU}(2)/\{\pm I\}$ if and only if n is even.

Now that we have tackled the "weights" of the algebraic forms for $D^\times$ we need a "level".

Take $U = \prod_q \mathcal{O}_q^\times$. This is an open compact subgroup of $D_{\mathbb{A}_f}^\times$. One can view this as being a subgroup of "level 1".

Theorem 3.3.3. *(Eichler)*

Let $k > 2$. Then for each prime p there is a Hecke preserving isomorphism:

$$S_k^{new}(\Gamma_0(p)) \cong \mathcal{A}(D^\times, U, V_{k-2}).$$

For $k = 2$ the above holds if on the right we quotient out by the space of constant functions.

Eichler's work predated Langlands functoriality and the general theory of algebraic modular forms. Originally the spaces $\mathcal{A}(D^\times, U, V_{k-2})$ had to be defined in an ad-hoc way.

It remains to describe how the Hecke operators transfer over the isomorphism. We will only see this for a prime $q \neq p$.

The Hecke action at q for level p elliptic forms is defined using the double coset operator for the matrix $\begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Q}_q)$. Now since D splits at q we have that $D_q^\times \cong \mathrm{GL}_2(\mathbb{Q}_q)$. Fixing an isomorphism as in Lemma 3.3.2 we may choose $u_q \in D_q^\times$ such that $u_q \mapsto \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}$.

Let $u \in D_{\mathbb{A}_f}^\times$ have u_q as the component at q and have identity component elsewhere.

Definition 3.3.4. For the above choice of u, the corresponding Hecke operator on $\mathcal{A}(D^\times, U, V_{k-2})$ will be called $T_{u,q}$. □

Under Eichler's correspondence we have that:

$$T_q \longleftrightarrow T_{u,q}.$$

To end this subsection we will see a rough outline of how Eichler's transfer of modular forms works. This will be useful later for genus 2 forms. One can find this treatment on p.222-224 of [8] as well as generalizations.

Let $F \in \mathcal{A}(D^\times, U, V_{k-2})$. Using Theorem 3.2.5 we can view F as a h-tuple $(F_1, F_2, ..., F_h)$ where each $F_i \in V_{k-2}^{\Gamma_i} = \mathrm{Symm}^{k-2}(\mathbb{C}^2)^{\Gamma_i}$ (fixing representatives $z_1, z_2, ..., z_h$ for $D^\times \backslash D_{\mathbb{A}_f}^\times / U$).

For $v, n \in \mathbb{N}$ consider the space $\mathcal{P}_v^{(n)}$ of real harmonic homogeneous polynomials of degree v in n variables. Since $\mathbb{H} \cong \mathbb{R}^4$ as vector spaces we can view polynomials in $\mathcal{P}_v^{(4)}$ as polynomials in one quaternion variable.

It is well known that $V_{k-2} \cong \mathcal{P}^{(3)}_{\frac{k-2}{2}}$ and that $\mathcal{P}^{(3)}_{\frac{k-2}{2}} \otimes \mathcal{P}^{(3)}_{\frac{k-2}{2}} \cong \mathcal{P}^{(4)}_{k-2}$ (see the above referenced pages in [8]).

For each $1 \leq i, j \leq h$ it is possible to find a left $\mathcal{O}$-order $L_{i,j}$ of D such that $L_{i,j}$ is locally equivalent to $\overline{z_i}\mathcal{O}z_j$. One then constructs the partial theta series:

$$\theta_F^{(i,j)}(\tau) = \sum_{z \in L_{i,j}} F_{i,j}(z) e^{\frac{2\pi i N(z)}{N_{i,j}}}$$

where:

- $F_{i,j} \in \mathcal{P}_{k-2}^{(4)}$ corresponds to $F_i \otimes F_j$ under the isomorphisms mentioned above.
- $N_{i,j}$ is the unique positive generator of the ideal of $\mathbb{Z}$ generated by the norms of elements in $L_{i,j}$.

The theta series of F is defined to be:

$$\theta_F(\tau) = \sum_{i=1}^{h} \sum_{j=1}^{h} \frac{1}{|\Gamma_i||\Gamma_j|} \theta_F^{(i,j)}(\tau).$$

Eichler shows that θ_F is an elliptic modular form of weight k and is new at level $\Gamma_0(p)$. Further if $k \neq 2$ then this is a cusp form. It is also shown that θ_F is an eigenform for T_q if and only if F is an eigenform for $T_{u,q}$ and that the Hecke eigenvalues coincide.

More is known in generality about Eichler's correpondence. Eichler was able to tackle non-prime levels too, but for the purposes of this thesis we shall not need to concern ourselves with this. See Buzzard's notes [10] for more details.

On a deeper level the correspondence above was generalised to capture automorphic forms for $\mathrm{GL}_{2n}(\mathbb{Q})$. The underlying idea is the same; at a prime $q \neq p$ we have that $\mathrm{GL}_n(D_q) \cong \mathrm{GL}_{2n}(\mathbb{Q}_q)$ along with inner form behaviour and so a correspondence of Hecke modules is predicted.

Also there is nothing special about using a quaternion algebra. Other definite division algebras A of dimension d^2 can be used to relate algebraic forms for $\mathrm{GL}_n(A)$ with automorphic forms for GL_{dn} [6], [55].

3.3.2 Explicit results

Now that we have described Eichler's correspondence we seek the following:

- Information about the class number of $D^\times$ relative to U. In particular we are interested in the case where $h = 1$ since this is the easiest computationally.
- Explicit descriptions of the Γ_m groups. We will only consider the case where $h = 1$, then $\Gamma = D^\times \cap U = \mathcal{O}^\times$ (rational points that are integral locally everywhere are integral globally).
- Explicit descriptions of the Hecke representatives for $T_{u,q}$. Again we will only consider cases where $h = 1$ but general algorithms exist.

Let us begin by investigating the class number h. We define the mass of U in $D^\times_{\mathbb{A}_f}$:

$$M(U) := \sum_{m=1}^{h} \frac{1}{|\Gamma_m|}.$$

Eichler was able to prove a well-known formula for this mass, independent of knowing h or the elements of the groups Γ_m.

Theorem 3.3.5. *(Eichler's mass formula)*

If D is ramified at $\{p, \infty\}$ then:

$$M(U) = \frac{p-1}{24}.$$

Classically one proves this formula by linking the groups Γ_m with unit groups of certain right orders of D, which in turn are linked with automorphism groups of isomorphism classes of supersingular elliptic curves over $\overline{\mathbb{F}}_p$. A counting argument is then employed.

Lemma 3.3.6. *$h = 1$ if and only if $|\mathcal{O}^\times| = \frac{24}{p-1}$.*

Proof. Take $z = \mathrm{id}$ as one of the representatives of the double coset space $D^\times \backslash D^\times_{\mathbb{A}_f} / U$. Then the group $\Gamma = D^\times \cap U$ contributes $\frac{1}{|\Gamma|}$ to the finite sum $M(U)$.

We know in general that $\Gamma = D^\times \cap U = \mathcal{O}^\times$. It is then clear that $h = 1$ occurs if and only if

$$|\mathcal{O}^\times| = \frac{1}{M(U)}.$$

□

Fortunately due to the simple description of $\mathcal{O}^\times$ we know exactly which ramified primes give class number 1.

Corollary 3.3.7. *$h = 1$ if and only if $p = 2, 3, 5, 7, 13$.*

Proof. We know that $h = 1$ if and only if $|\mathcal{O}^\times| = \frac{24}{p-1}$. However $|\mathcal{O}^\times| \in \mathbb{N}$ so that $(p-1)|24$. But p is prime so $p = 2, 3, 5, 7, 13$ are the only possibilities.

It is then straight forward to generate D and $\mathcal{O}$ for each of these primes and check that $\mathcal{O}^\times$ has the correct size. □

It should be noted that there is a deep generalisation of the mass formula that applies to many classical groups (more specifically some of those which we use in the theory of algebraic modular forms). For such groups one can define the notion of mass in a similar fashion to above for any open compact subgroup of $G(\mathbb{A}_f)$. The paper by Gan, Hanke and Yu [25] then provides a useful formula for this quantity, involving tamagawa numbers and motivic L-values attached to G.

It remains to find an explicit description of the Hecke representatives for $T_{u,q}$. It is known how to do this for arbitrary class number. However when $h = 1$ they have an elegant description that will be useful later. Thus I will only concentrate on this case.

Proposition 3.3.8. *Let D be a quaternion algebra over $\mathbb{Q}$ ramified at $\{p, \infty\}$ with $p \in \{2, 3, 5, 7, 13\}$. Suppose $u \in D^\times_{\mathbb{A}_f}$ is chosen as in Definition 3.3.4. We have that*

$$UuU = \coprod_{[x_i] \in X_q/\mathcal{O}^\times} x_i U$$

where $X_q = \{v \in \mathcal{O} \mid N(u) = q\}$.

Proof. Consider an arbitrary decomposition:

$$UuU = \coprod x_i U$$

for $x_i \in D^\times_{\mathbb{A}_f}$. Note that by Proposition 3.2.12 we may take $x_i \in D^\times$ for all i (since the class number is 1). For the rest of the proof we embed $D^\times \hookrightarrow D^\times_{\mathbb{A}_f}$ diagonally.

We first show that we may take $x_i \in \mathcal{O}$ with $N(x_i) = q$.

Note that for any prime $l \neq q$ we have local double coset $U_l u_l U_l = U_l = \mathcal{O}_l^\times$. Thus $x_i \in \mathcal{O}_l^\times$ for all i. Also from this we have $N(x_i) \in \mathbb{Z}_l^\times$.

Consider the local double coset at q. Fix an isomorphism as in Lemma 3.3.2. Then $U_q u_q U_q = \mathcal{O}_q^\times u_q \mathcal{O}_q^\times$ is in bijection with $\mathrm{GL}_2(\mathbb{Z}_q) \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} \mathrm{GL}_2(\mathbb{Z}_q)$.

Since $u_q \mapsto \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} \in M_2(\mathbb{Z}_q)$ we see that $u_q \in \mathcal{O}_q$ and so $x_i \in \mathcal{O}_q$. Also since our isomorphism transfers norm into determinant we find that $N(u_q) = \det\left(\begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix}\right) = q$ and so $N(\mathcal{O}_q^\times u_q \mathcal{O}_q^\times) \subseteq q\mathbb{Z}_q^\times$. In particular $N(x_i) \in q\mathbb{Z}_q^\times$.

Globally we now see that $x_i \in D^\times \cap (\prod_l \mathcal{O}_l) = \mathcal{O}$ for each i. We also observe that $N(x_i) \in \mathbb{Z} \cap \left(q\mathbb{Z}_q^\times \prod_{l \neq q} \mathbb{Z}_l^\times\right) = \{\pm q\}$. However in our case the norm is positive definite so that $N(x_i) = q$.

Thus the x_i can be taken to lie in X_q. It is clear that each such element lies in the double coset.

It remains to see which elements of X_q generate the same left coset. We have $x_i U = x_j U$ if and only if $x_j^{-1} x_i \in U$. But also $x_i, x_j \in D^\times$, hence $x_j^{-1} x_i \in D^\times \cap U = \mathcal{O}^\times$. So equivalence of left cosets is up to right multiplication by units of $\mathcal{O}$. □

In practice we wish to know the degree of $T_{u,q}$ so that we can check we have the correct number of Hecke representatives to compute with.

Theorem 3.3.9. *Let D be ramified at $\{p, \infty\}$ (not necessarily of class number 1). Then for $q \neq p$:*

$$deg(T_{u,q}) = |X_q / \mathcal{O}^\times| = q + 1.$$

Proof. It has already been observed that decomposing the double coset UuU into left cosets of U is equivalent to decomposing $\mathrm{GL}_2(\mathbb{Z}_q) \begin{pmatrix} 1 & 0 \\ 0 & q \end{pmatrix} \mathrm{GL}_2(\mathbb{Z}_q)$ into left cosets of $\mathrm{GL}_2(\mathbb{Z}_q)$.

Fortunately this is a straight forward task and representatives can be taken to be $\begin{pmatrix} q & 0 \\ 0 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & x \\ 0 & q \end{pmatrix}$ for $x = 0, 1, 2..., (q-1)$ (see Lemma 6.4.1 of Roberts and Schmidt [56]). There are exactly $q + 1$ representatives here and so the degree of the Hecke operator is $q + 1$. □

3.3.3 An example

I have chosen to give a brief but illuminating example of the kind of calculations one expects when calculating Hecke eigenvalues of algebraic forms for $D^\times$.

Let $D = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and take Hurwitz quaternions $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\left(\frac{1+i+j+k}{2}\right)$ as a maximal order. Then D is ramified at $\{2, \infty\}$.

By Corollary 3.3.7 $h = 1$, giving $\Gamma = D^\times \cap U = \mathcal{O}^\times$.

Aside: In this case we may find an alternate proof that $\deg(T_{u,q}) = q + 1$ (when $q \neq 2$).

Proof. By definition $\deg(T_{u,q}) = |X_q/\mathcal{O}^\times|$, where $X_q = \{v \in \mathcal{O} \,|\, N(v) = q\}$. The elements of this set are in bijection with the integer solutions to:

$$(2\alpha + \delta)^2 + (2\beta + \delta)^2 + (2\gamma + \delta)^2 + \delta^2 = 4q.$$

By a well known theorem of Jacobi we know that there are $24(q + 1)$ ways to write $4q$ as a sum of 4 squares and each possibility gives integer values for $\alpha, \beta, \gamma, \delta$, since the squares are either all even or all odd.

In order to find $\mathcal{O}^\times$ we need to find elements of norm one in $\mathcal{O}$. Again these are in bijection with integer solutions to:

$$(2\alpha + \delta)^2 + (2\beta + \delta)^2 + (2\gamma + \delta)^2 + \delta^2 = 4.$$

Solving gives $\mathcal{O}^\times = \{\pm 1, \pm i, \pm j, \pm k, \frac{\pm 1 \pm i \pm j \pm k}{2}\}$ and we see that $|\mathcal{O}^\times| = 24$.

It is easily checked that each orbit under the action is full and so the number of orbits is

$$|X_q/\mathcal{O}^\times| = \frac{|X_q|}{|\mathcal{O}^\times|} = \frac{24(q+1)}{24} = q + 1.$$

□

Returning to our example we can generate Hecke representatives by using Proposition 3.3.8. A simple computation gives $X_3/\mathcal{O}^\times = \{[1 \pm i \pm j]\}$ and $X_5/\mathcal{O}^\times = \{[1 \pm 2i], [1 \pm 2j], [1 \pm 2k]\}$. Such lists can easily be generated for larger primes.

Now the Eichler correspondence in our case says that there should be an isomorphism of Hecke modules:

$$S_k^{\text{new}}(\Gamma_0(2)) \cong \mathcal{A}(D^\times, U, V_{k-2}) \cong V_{k-2}^{\mathcal{O}^\times}$$

for each $k \geq 2$ (where we remember to quotient out by constant functions for $k = 2$).

Take the standard basis $a = (1,0)^T, b = (0,1)^T$ for $\mathbb{C}^2$. Then $V_{k-2} = \mathrm{Symm}^{k-2}(\mathbb{C}^2)$ has basis consisting of $a^s b^{k-2-s}$ for $s = 0, 1, ..., k-2$.

Using the embedding:

$$D^\times \hookrightarrow \mathrm{GL}_2(\mathbb{C})$$
$$\alpha + \beta i + \gamma j + \delta k \longmapsto \begin{pmatrix} \alpha+\beta i & \gamma+\delta i \\ -\gamma+\delta i & \alpha-\beta i \end{pmatrix}$$

mentioned earlier we may explicitly compute the action of $D^\times$ on V_{k-2}. Thus it is now possible to find the spaces $V_{k-2}^{\mathcal{O}^\times}$.

Recall that $\dim(S_k(\Gamma_0(2))) = 0$ for odd $k \geq 0$. This has the following interpretation on the algebraic side:

Lemma 3.3.10. *If $k \geq 2$ is odd then $V_{k-2}^{\mathcal{O}^\times} = \{0\}$.*

Proof. We notice that $-1 \in \mathcal{O}^\times$ and this acts by the matrix $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ on $\mathbb{C}^2$ under the above embedding. Thus $(-1)\cdot a = -a$ and $(-1)\cdot b = -b$.

Take $x \in V_{k-2}^{\mathcal{O}^\times} \subseteq \mathrm{Symm}^{k-2}(\mathbb{C}^2)$. Then writing $x = \sum_{s=0}^{k-2} \alpha_s a^s b^{k-2-s}$ we see that:

$$x = (-1)\cdot x = \sum_{s=0}^{k-2} \alpha_s (-a)^s (-b)^{k-2-s} = (-1)^{k-2} \sum_{s=0}^{k-2} \alpha_s a^s b^{k-s-2} = -x$$

since $k-2$ is odd. Thus $x = 0$. Clearly the element $0 \in V_{k-2}$ is fixed by the action of $\mathcal{O}^\times$ and so the result follows. □

For even k we see by inspection that $V_0^{\mathcal{O}^\times} = \mathbb{C}$ and $V_2^{\mathcal{O}^\times} = V_4^{\mathcal{O}^\times} = \{0\}$. This fits with the fact that $S_k^{\mathrm{new}}(\Gamma_0(2))$ has dimension 0 for $k = 2, 4, 6$ (remembering to quotient out by constants in $V_0^{\mathcal{O}^\times}$).

Once we reach $k = 8$ we see that $V_6^{\mathcal{O}^\times} = \mathbb{C}(a^5 b - a b^5)$ is 1-dimensional. As expected it is also true that $\dim(S_8^{\mathrm{new}}(\Gamma_0(2))) = 1$. The unique normalized eigenform in this space has q-expansion:

$$f(z) = q - 8q^2 + 12q^3 + 64q^4 - 210q^5 - 96q^6 + 1016q^7 ...$$

so that $a_3 = 12$ and $a_5 = -210$.

As an example we will recover these values by explicitly computing the Hecke action on the algebraic modular forms for $D^\times$.

By definition the Hecke operator $T_{u,q}$ acts on this space of algebraic modular forms (viewed as $V_6^{\mathcal{O}^\times}$) via:

$$T_{u,q}\left(a^5 b - a b^5\right) = \sum_{[x_i] \in X_q/\mathcal{O}^\times} x_i \cdot (a^5 b - a b^5).$$

Since the space of forms is 1-dimensional, every non-zero element of $V_6^{\mathcal{O}^\times}$ is automatically an eigenform for all of the T_q operators ($q \neq 2$).

Recall that we may take as our Hecke representatives $X_3/\mathcal{O}^\times = \{[1 \pm i \pm j]\}$ and $X_5/\mathcal{O}^\times = \{[1 \pm 2i], [1 \pm 2j], [1 \pm 2k]\}$. By the matrix embedding we see that the representatives for $T_{u,3}$ act by the matrices:

$$\begin{pmatrix} 1 \pm i & 1 \\ -1 & 1 \mp i \end{pmatrix}, \begin{pmatrix} 1 \pm i & -1 \\ 1 & 1 \mp i \end{pmatrix}$$

and the representatives for $T_{u,5}$ act by:

$$\begin{pmatrix} 1 \pm 2i & 0 \\ 0 & 1 \mp 2i \end{pmatrix}, \begin{pmatrix} 1 & \pm 2 \\ \mp 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & \pm 2i \\ \pm 2i & 1 \end{pmatrix}.$$

Thus we find

$$\begin{aligned}(1 \pm i + j) \cdot a &= (1 \pm i)a - b \\ (1 \pm i - j) \cdot a &= (1 \pm i)a + b \\ (1 \pm i + j) \cdot b &= (1 \mp i)b + a \\ (1 \pm i - j) \cdot b &= (1 \pm i)b - a\end{aligned}$$

and

$$\begin{aligned}(1 \pm 2i) \cdot a &= (1 \pm 2i)a \\ (1 \pm 2j) \cdot a &= a \mp 2b \\ (1 \pm 2k) \cdot a &= a \pm 2ib \\ (1 \pm 2i) \cdot b &= (1 \mp 2i)b \\ (1 \pm 2j) \cdot b &= b \pm 2a \\ (1 \pm 2k) \cdot b &= b \pm 2ia\end{aligned}$$

From this we see that

$$(1 \pm i + j) \cdot (a^5 b - a b^5) = -5(1 \pm i)(a^6 - b^6) + 3(a^5 b - a b^5) - 15(1 \mp i)(a^4 b^2 - a^2 b^4) \pm 40 i a^3 b^3$$

and

$$(1 \pm i - j) \cdot (a^5 b - a b^5) = 5(1 \pm i)(a^6 - b^6) + 3(a^5 b - a b^5) + 15(1 \mp i)(a^4 b^2 - a^2 b^4) \pm 40 i b^3 a^3.$$

Summing gives

$$T_{u,3}(a^5 b - a b^5) = 12(a^5 b - a b^5).$$

Similarly

$$(1 \pm 2i) \cdot (a^5 b - a b^5) = -5((7 \pm 24i)a^5 b - (7 \mp 24i) a b^5),$$

$$(1 \pm 2j) \cdot (a^5 b - a b^5) = \mp 30 a^6 - 35 a^5 b \pm 150 a^4 b^2 \pm 150 a^2 b^4 + 35 a b^5 \mp 30 b^6,$$

$$(1 \pm 2k) \cdot (a^5 b - a b^5) = \mp 30 i a^6 - 35 a^5 b \mp 150 i a^4 b^2 \pm 150 i a^2 b^4 + 35 a b^5 \pm 30 i b^6.$$

Summing gives

$$T_{u,5}(a^5b - ab^5) = -210(a^5b - ab^5).$$

Thus the Hecke eigenvalues of $T_{u,3}$ and $T_{u,5}$ on the algebraic side are $a_3 = 12$ and $a_5 = -210$. This agrees with the q-expansion given earlier. One can perform similar calculations for other primes to find more occurences of the expected Hecke eigenvalues.

3.4 Dummigan's trace formula

Finding the eigenvalues of the Hecke action on algebraic modular forms is an easy task theoretically but usually involves a hefty calculation computationally. This trade off is due to the fact that the underlying representation V of G is typically big in dimension and so the matrices involved in computing the action of elements on V can be quite large.

Fortunately, in recent work, Dummigan reveals a way to bypass this issue and has provided a simple trace formula for Hecke operators on spaces of algebraic modular forms. This formula is most efficient when the dimension of the space $\mathcal{A}(G, K_f, V)$ is very small relative to the dimension of V.

The details of this formula can be found in [22] but for the purposes of completeness I will describe the main ideas.

Suppose we have the setup as described in previous subsections. In particular we have a set of representatives $Z = \{z_1, z_2, ..., z_h\}$ for $G(\mathbb{Q})\backslash G(\mathbb{A}_f)/K_f$ and have fixed a choice of $u \in G(\mathbb{A}_f)$ along with the decomposition $K_f u K_f = \coprod_{i=1}^{r} u_i K_f$. We wish to evaluate the trace of the action of the Hecke operator T_u on the space $\mathcal{A}(G, K_f, V)$.

First note that $G(\mathbb{A}_f)$ acts on the set Z on the left. This is due to the fact that $G(\mathbb{A}_f)$ acts on itself by left multiplication. More specifically, if we take $z_i \in Z$ and $w \in G(\mathbb{A}_f)$ then $wz_i \in G(\mathbb{A}_f)$ and so the double coset $G(\mathbb{Q})(wz_i)K_f$ must equal $G(\mathbb{Q})z_j K_f$ for some j (since Z is a full set of representatives for such double cosets). Thus we may define the action via $w \cdot z_i = z_j$.

Now for each $m = 1, 2, ..., h$ we consider the set $S_m = \{i \mid u_i \cdot z_m = z_m\}$, i.e. those u_i's that stabilize z_m under the action. The intuition here is that these elements should be the only ones to make a non-zero contribution to the trace of the Hecke operator.

Next for each $i \in S_m$ we may choose elements $k_{m,i} \in K_f$ and $\gamma_{m,i} \in G(\mathbb{Q})$ such that $\gamma_{m,i}^{-1} u_i z_m k_{m,i} = z_m$. This is possible since $z_m \in G(\mathbb{Q})(u_i z_m)K_f$, by equality of the double cosets.

Let χ_V denote the character of the representation of $G(\mathbb{Q})$ on V. Then the

trace of T_u acting on $\mathcal{A}(G, K_f, V)$ can be computed as follows:

Theorem 3.4.1. *(Dummigan)*

$$tr(T_u) = \sum_{m=1}^{h} \frac{1}{|\Gamma_m|} \sum_{\gamma \in \Gamma_m, i \in S_m} \chi_V(\gamma_{m,i}\gamma).$$

More generally:

$$tr(T_u^d) = \sum_{m=1}^{h} \frac{1}{|\Gamma_m|} \sum_{\gamma \in \Gamma_m, (i_n) \in S_m^d} \chi_V\left(\left(\prod_{n=1}^{d} \gamma_{m,i_n}\right)\gamma\right).$$

Letting $u = \mathrm{id}$ we recover the following.

Corollary 3.4.2. *We have that:*

$$dim(\mathcal{A}(G, K_f, V)) = \sum_{m=1}^{h} \frac{1}{|\Gamma_m|} \sum_{\gamma \in \Gamma_m} \chi_V(\gamma).$$

As a short remark we note that this formula was actually known to us earlier since by Corollary 3.2.6 we have $\dim(\mathcal{A}(G, K_f, V)) = \sum_{m=1}^{h} \dim(V^{\Gamma_m})$ and it is indeed known how to compute dimensions of isotropy subspaces of actions by finite groups (via use of the projection map $V \to V^G$ given by $\frac{1}{|G|}\sum_{\gamma \in G} \gamma$).

When we have class number 1 for K_f the situation becomes much simpler. In this case we may choose $z_1 = \mathrm{id}$ and $\gamma_{1,i} = u_i \in G(\mathbb{Q})$ for each i (this is possible by Corollary 3.2.12).

Corollary 3.4.3. *If the class number of K_f is 1 then we have*

$$tr(T_u) = \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma, 1 \leq i \leq r} \chi_V(u_i\gamma),$$

where $\Gamma = G(\mathbb{Q}) \cap K_f$.

The trace formula was introduced to test a $\mathrm{U}(2,2)$ analogue of Harder's conjecture. In this thesis we will use it to test the level p paramodular version of Harder's conjecture given by Conjecture 1.3.2.

3.4.1 An example: continued

Returning to our previous example of Eichler's correspondence we may instead use the trace formula to find the dimensions and Hecke eigenvalues on the algebraic side. Seeing this in action gives a brief glimpse of how much easier

computations can be when using the trace formula. Indeed it will be the chosen method in later computations.

As a brief reminder, we set $D = \left(\frac{-1,-1}{\mathbb{Q}}\right)$ and $\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\frac{1+i+j+k}{2}$ and $V_k = \mathrm{Symm}^k(\mathbb{C})$. Then Eichler's correspondence gives an isomorphism of Hecke modules:

$$S_k^{\mathrm{new}}(\Gamma_0(2)) \cong \mathcal{A}(D^\times, U, V_{k-2}) \cong V_{k-2}^{\mathcal{O}^\times}.$$

For $k \geq 0$ let χ_k denote the character of the representation V_k. Since $h = 1$ and $|\Gamma| = |\mathcal{O}^\times| = 24$ we know by Corollaries 3.4.2 and 3.4.3 that:

$$\dim(V_{k-2}^{\mathcal{O}^\times}) = \frac{1}{24} \sum_{\gamma \in \mathcal{O}^\times} \chi_{k-2}(\gamma),$$

$$\mathrm{tr}(T_{u,q}) = \frac{1}{24} \sum_{\gamma \in \mathcal{O}^\times, [x_i] \in X_q/\mathcal{O}^\times} \chi_{k-2}(x_i \gamma).$$

It remains to calculate the character values. Note that it is a trivial matter to find character values for symmetric power representations but for the purposes of later work we choose to use the Weyl character formula [24].

Given $\alpha \in D^\times$ we may produce a matrix $A \in \mathrm{GL}_2(\mathbb{C})$ via the embedding given previously. We know that the image of $\mathbb{H}_1^\times \cap D^\times$ under this embedding is a subgroup SU(2) so that the matrix $B = \frac{A}{\sqrt{\det(A)}} \in \mathrm{SU}(2)$. By writing $A = (\sqrt{\det(A)}I)B$ it now follows that:

$$\chi_{k-2}(\alpha) = \chi_{k-2}(A) = \det(A)^{\frac{k-2}{2}} \chi_{k-2}(B)$$

In the case of the Hecke operator $T_{u,q}$ we will always have $\det(A) = N(\alpha) = q$ and so the scaling factor here is simply $q^{\frac{k-2}{2}}$.

Finally it is not too difficult to find the value of $\chi_{k-2}(B)$. We find the eigenvalues of B (which is equivalent to conjugating into the maximal torus of diagonal matrices). Since $B \in \mathrm{SU}(2)$ these eigenvalues will take the form $z, \overline{z}$ for some z on the unit circle. The Weyl Character formula gives:

$$\chi_{k-2}(B) = \sum_{m=0}^{k-2} z^{(k-2-2m)}.$$

Letting $z = e^{i\theta}$ for $\theta \in [0, 2\pi)$, this simplifies to give:

$$\chi_{k-2}(B) = \begin{cases} \frac{\sin((k-1)\theta)}{\sin(\theta)} & \text{for } \theta \neq 0, \pi \\ k-1 & \text{for } \theta = 0 \\ (-1)^k(k-1) & \text{for } \theta = \pi \end{cases}$$

Now that we have the correct setup we may compute dimensions and Hecke eigenvalues using the formulae mentioned above. Doing this we find the following list of dimensions of $V_{k-2}^{\mathcal{O}^\times}$ for $k = 2, 3, 4, ..., 20$:

$$1, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 0, 2, 0, 1, 0, 1, 0, 2.$$

As expected, this list matches the corresponding list of dimensions for $S_k^{\text{new}}(\Gamma_0(2))$. In particular for odd k the trace formula has definitely produced dimension 0.

Also for the same range of k we find the following eigenvalues for $\text{tr}(T_{u,3})$ as acting on $V_{k-2}^{\mathcal{O}^\times}$:

$$4, 0, 0, 0, 0, 0, \mathbf{12}, 0, -156, 0, 0, 0, -600, 0, 6252, 0, 6084, 0, -66120$$

and similarly for $\text{tr}(T_{u,5})$:

$$6, 0, 0, 0, 0, 0, \mathbf{\text{-}210}, 0, 870, 0, 0, 0, -53460, 0, 90510, 0, 1255110, 0, 989820.$$

It is evident that each trace is an integer.

For $k = 8$ it is observed from these lists that the space $S_8^{\text{new}}(\Gamma_0(2))$ is 1-dimensional and thus the Hecke eigenvalues at 3 and 5 for the unique normalized eigenform are $a_3 = \text{tr}(T_{u,3}) = 12$ and $a_5 = \text{tr}(T_{u,5}) = -210$, as found earlier. This demonstrates the ease of using the trace formula over other ad-hoc methods.

Note that if one wishes to find the Hecke eigenvalues on a space that is not 1-dimensional it is not enough just to know $\text{tr}(T_{u,q})$. One must work out the sequence of values $\text{tr}(T_{u,q})$, $\text{tr}(T_{u,q}^2)$, ..., $\text{tr}(T_{u,q}^d)$, where d is the dimension of the space and then use symmetric polynomial algorithms to solve for the actual eigenvalues (since these traces are sums of powers of eigenvalues). This is still possible (see the statement of Theorem 3.4.1) but is a bigger computation as d increases.

3.5 Ibukiyama's correspondence

Following on from the Eichler-Jacquet-Langlands correspondence outlined in the previous section we now show how to capture certain spaces of Siegel modular forms algebraically. Such a correspondence was originally found empirically in the work of Ihara [43] but was made formal and rigorous by his student T. Ibukiyama in a series of papers dating back to the 1980's [37].

By analogy with GL_2 and $D^\times$ the strategy is to construct a reductive algebraic group G over $\mathbb{Q}$ such that:

- $G(\mathbb{R})$ is compact modulo its center, so that we may consider algebraic modular forms for such a group.

- $Z(\mathbb{R})$ is a split torus, so that the symmetric space associated to G is trivial (hence the algebraic forms attached to G can be viewed as functions on $G(\mathbb{A}_f)$).

- $G(\mathbb{Z})$ is finite, so that the Γ_m groups are finite.

- G is an inner form of GSp_4. Then by Langlands functoriality we expect a transfer of automorphic forms. Such a transfer should allow us to see certain spaces of Siegel modular forms as spaces of algebraic modular forms.

- $G(\mathbb{Q}_q) \cong \mathrm{GSp}_4(\mathbb{Q}_q)$ for all $q \neq p$.

As with the previous section, this will have a very concrete description and will be extremely helpful to us in finding Hecke eigenvalues for Siegel modular forms.

Given a definite quaternion algebra D ramified at prime p and a maximal order $\mathcal{O}$, Ihara and Ibukiyama constructed the unitary similitude group:

$$\mathrm{GU}_n(D) = \{g \in \mathrm{M}_n(D) \,|\, g\bar{g}^T = \mu(g)I,\, \mu(g) \in \mathbb{Q}^\times\}.$$

Here $\bar{g}$ means componentwise application of the standard involution of D.

We wish to prove that the above group behaves like GSp_4 locally at places where D is split. To this end let K be any field and define the matrix

$$M = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in M_4(K).$$

It is clear that $M = M^{-1} = M^T$. Further if $J = \begin{pmatrix} 0 & I \\ -I & 0 \end{pmatrix}$ then we observe that:

$$N := MJM = \begin{pmatrix} J' & 0 \\ 0 & J' \end{pmatrix}$$

where $J' = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. A nice property of J' is that for any $S \in M_2(K)$ we have $J'SJ'^{-1} = \mathrm{adj}(S)$ so that $J'S = \mathrm{adj}(S)J'$.

Now observe that for any $Z = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M_4(K)$

$$\begin{aligned} ZNZ^T &= \begin{pmatrix} AJ'A^T + BJ'B^T & AJ'C^T + BJ'D^T \\ CJ'A^T + DJ'B^T & CJ'C^T + DJ'D^T \end{pmatrix} \\ &= \begin{pmatrix} (A\,\mathrm{adj}(A^T) + B\,\mathrm{adj}(B^T))J' & (A\,\mathrm{adj}(C^T) + B\,\mathrm{adj}(D^T))J' \\ (C\,\mathrm{adj}(A^T) + D\,\mathrm{adj}(B^T))J' & (C\,\mathrm{adj}(C^T) + D\,\mathrm{adj}(D^T))J \end{pmatrix} \\ &= \begin{pmatrix} A\,\mathrm{adj}(A)^T + B\,\mathrm{adj}(B)^T & A\,\mathrm{adj}(C)^T + B\,\mathrm{adj}(D)^T \\ C\,\mathrm{adj}(A)^T + D\,\mathrm{adj}(B)^T & C\,\mathrm{adj}(C)^T + D\,\mathrm{adj}(D)^T \end{pmatrix} N \\ &= Z\overline{Z}^T N. \end{aligned}$$

This relation is very helpful in establishing the link mentioned above.

Theorem 3.5.1. *For any field K there exists a similitude-preserving isomorphism $GU_2(M_2(K)) \cong GSp_4(K)$.*

Proof. Consider the map:

$$\mathrm{GU}_2(M_2(K)) \longrightarrow \mathrm{GSp}_4(K)$$

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \longmapsto \begin{pmatrix} a_{1,1} & b_{1,1} & a_{1,2} & b_{1,2} \\ c_{1,1} & d_{1,1} & c_{1,2} & d_{1,2} \\ a_{2,1} & b_{2,1} & a_{2,2} & b_{2,2} \\ c_{2,1} & d_{2,1} & c_{2,2} & d_{2,2} \end{pmatrix}.$$

i.e. conjugation by the matrix M. The map will clearly be an isomorphism if we can show it is well defined.

Take $X \in \mathrm{GU}_2(M_2(K))$ of similitude $\mu \in K^\times$. Then

$$\begin{aligned} (MXM)J(MXM)^T = \mu J &\iff MX(MJM)X^TM = \mu J \\ &\iff MXNX^TM = \mu J \\ &\iff MX\overline{X}^T NM = \mu J \\ &\iff X\overline{X}^T = \mu I \end{aligned}$$

Thus $X \in \mathrm{GU}_2(M_2(K))$ if and only if $MXM \in \mathrm{GSp}_4(K)$. □

In fact essentially the same argument shows that $\mathrm{GU}_n(M_2(K)) \cong \mathrm{GSp}_{2n}(K)$ for any field K and $n \geq 1$ (Theorem 3.4 in [27]).

It is clear that $\mathrm{GU}_2(\mathbb{H})$ is connected. Let us now check that $\mathrm{GU}_2(\mathbb{H})$ is compact modulo its center.

Theorem 3.5.2. *There is an isomorphism of Lie groups:*

$$GU_2(\mathbb{H})/Z(GU_2(\mathbb{H})) \cong USp(4)/\{\pm I\}.$$

Here $USp(4) = U(4) \cap Sp_4(\mathbb{C})$.

Proof. We start by evaluating the center $Z(\mathrm{GU}_2(\mathbb{H}))$. To this end we note that for any $\overline{a} \in \mathbb{H}$ we have matrices $T_a := \begin{pmatrix} 1 & -a \\ \overline{a} & 1 \end{pmatrix} \in \mathrm{GU}_2(\mathbb{H})$.

Now suppose $X = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in Z(\mathrm{GU}_2(\mathbb{H}))$. Then $T_1X = XT_1$ implies $w = x$ and $z = -y$. Use of the relations $T_iX = XT_i, T_jX = XT_j$ and $T_kX = XT_k$ tells us that $x \in \mathbb{R}^\times$ and $y = 0$. Hence $X = \alpha I$ for some $\alpha \in \mathbb{R}^\times$. Clearly any matrix of the form αI for $\alpha \in \mathbb{R}^\times$ lies in the center and so we have $Z(\mathrm{GU}_2(\mathbb{H})) = \{\alpha I \,|\, \alpha \in \mathbb{R}^\times\}$.

Now consider the subgroup $\mathrm{GU}_2(\mathbb{H})_1 \subseteq \mathrm{GU}_2(\mathbb{H})$ consisting of matrices of similitude 1 (often denoted $\mathrm{Sp}(2)$ in the literature). Consider the following embedding:

$$\mathrm{GU}_2(\mathbb{H}) \hookrightarrow \mathrm{GU}_2(M_2(\mathbb{C})) \cong \mathrm{GSp}_4(\mathbb{C})$$

where the first inclusion comes from the matrix embedding $\mathbb{H} \hookrightarrow M_2(\mathbb{C})$ given by:

$$\alpha + \beta i + \gamma j + \delta k \longmapsto \begin{pmatrix} \alpha + \beta i & \gamma + \delta k \\ -\gamma + \delta i & \alpha - \beta i \end{pmatrix}$$

(see Lemma 2.1.9) and the second isomorphism comes from the previous theorem.

One easily checks that the image of $\mathrm{GU}_2(\mathbb{H})_1$ under this embedding is $\mathrm{USp}(4)$ and so we may identify the two groups.

Given the above we now have a surjection $\mathrm{USp}(4) \to \mathrm{GU}_2(\mathbb{H})/Z(\mathrm{GU}_2(\mathbb{H}))$ that is continuous. The kernel is $\mathrm{USp}(4) \cap Z(\mathrm{GU}_2(\mathbb{H})) = \{\pm I\}$. The result follows. □

The above shows that we may consider algebraic modular forms for $\mathrm{GU}_2(D)$. In fact we are even guaranteed that the Γ_m groups are finite. By Proposition 3.2.9 we only need check the following.

Lemma 3.5.3. *$GU_2(\mathcal{O}) = \{\gamma \in GU_2(D) \cap M_2(\mathcal{O}) \,|\, \mu(\gamma) \in \mathbb{Z}^\times\}$ is finite.*

Proof. Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GU}_2(\mathcal{O})$. Then the similitude $\mu(\gamma) \in \mathbb{Z}^\times = \{\pm 1\}$ but due to the definite nature of D we must have $\mu(\gamma) = 1$.

Then $\gamma\bar{\gamma}^T = I$ gives the following equations:

$$\begin{aligned} N(a) + N(b) &= 1 \\ N(c) + N(d) &= 1 \\ a\bar{c} + b\bar{d} &= 0 \end{aligned}$$

Since $a, b, c, d \in \mathcal{O}$ and so have non-negative integer norm it is easy to see that exactly one of a, b is a unit and the other is 0. Similarly for c, d.

Since $\mathcal{O}^\times$ is finite there must be only finitely many solutions to the equations, hence finitely many possibilities for γ. □

We may now observe that this group has the other properties that we desire:

Corollary 3.5.4. *For any $q \neq p$ there exists a similitude-preserving isomorphism $\psi : GU_2(D_q) \to GSp_4(\mathbb{Q}_q)$ that preserves integrality:*

$$\psi(GU_2(D_q) \cap M_2(\mathcal{O}_q)) = GSp_4(\mathbb{Q}_q) \cap M_4(\mathbb{Z}_q).$$

Proof. Since D splits at q we have that:

$$\mathrm{GU}_2(D_q) \cong \mathrm{GU}_2(M_2(\mathbb{Q}_q)) \cong \mathrm{GSp}_4(\mathbb{Q}_q),$$

where the second isomorphism uses the above theorem.

If we choose an isomorphism $D_q \to M_2(\mathbb{Q}_q)$ as in Lemma 3.3.2 so that $\mathcal{O}_q \to M_2(\mathbb{Z}_q)$ then the above clearly respects similitude and integrality. □

From now on we fix such an isomorphism at each $q \neq p$. As mentioned before we now have reason to expect a transfer of automorphic forms to exist. We will not see all forms on the algebraic side though (just as with Eichler's correspondence).

First let us see the conjectural correspondence, then we will explore it in detail. Recall that one may find this in Ibukiyama's paper [37].

Conjecture 3.5.5. *(Ibukiyama) Let $j \geq 0$ be an even integer and $k \geq 3$. Supppose $(j, k) \neq (0, 3)$. Then for each prime p there exists Hecke preserving isomorphisms:*

$$S_{j,k}^{new}(\Gamma_0(p)) \longrightarrow \mathcal{A}^{new}(GU_2(D), U_1, V_{j,k-3})$$

$$S_{j,k}^{new}(K(p)) \longrightarrow \mathcal{A}^{new}(GU_2(D), U_2, V_{j,k-3}),$$

where $U_1, U_2, V_{j,k-3}$ are to be defined.

If $(j, k) = (0, 3)$ then we also get an isomorphism after taking the quotient by the constant functions on the right.

We have yet to explain what U_1, U_2 and $V_{j,k-3}$ are, and to show how the actions of the Hecke operators agree on both sides. Descriptions of these are not as simple as for Eichler's correspondence. Also we do not yet have a notion of newform on the algebraic side. These questions will be answered throughout this section.

Since our eventual goal is to study Harder's conjecture for paramodular forms we will neglect the first of these isomorphisms. However, it will turn out that the open compact subgroup U_1 will prove useful in later calculations.

3.5.1 The weight space $V_{j,k-3}$.

In order to explain what the space $V_{j,k-3}$ is and how this is acted upon by $\mathrm{GU}_2(D)$ we follow a similar path to the one we saw for Eichler's correspondence.

Note that we can produce representations of $\mathrm{GU}_2(D)$ from representations of $\mathrm{USp}(4)/\{\pm I\}$ via:

$$\mathrm{GU}_2(D) \hookrightarrow \mathrm{GU}_2(\mathbb{H}) \longrightarrow \mathrm{GU}_2(\mathbb{H})/Z(\mathrm{GU}_2(\mathbb{H})) \cong \mathrm{USp}(4)/\{\pm I\}.$$

Irreducible representations of $\mathrm{USp}_4(\mathbb{C})$ are represented by their Young diagram parameters (m,n) for $m \geq n \geq 0$. With this in mind Ibukiyama predicts that the correct space $V_{j,k-3}$ should come from the irreducible representation of $\mathrm{GSp}_4(\mathbb{C})$ with Young diagram parameters $(j+k-3, k-3)$. There is no problem here since we are assuming $k \geq 3$ and $j \geq 0$. It is known that $V_{j,k-3}$ is a well defined representation of $\mathrm{USp}(4)/\{\pm I\}$ if and only if j is even.

Notice in particular that similar to Eichler's correspondence we have a shift in the weight, however this time it is by 3 rather than by 2. Also notice that the case $j = 0$ seems extremely close to Eichler's result (since there we had scalar valued elliptic modular forms and this is exactly what $j = 0$ means for our Siegel modular forms).

3.5.2 The level U_2 and the theory of $\mathcal{O}$-lattices

In order to construct the relevant open compact subgroup U_2 of $\mathrm{GU}_2(D_{\mathbb{A}_f})$ we must think about how to generalise the one used in Eichler's correspondence to higher dimensions. The "level 1" open compact subgroup $U = \prod_q \mathcal{O}_q^\times \subset D_{\mathbb{A}_f}^\times$ can be viewed as $\mathrm{Stab}_{D_{\mathbb{A}_f}^\times}(\mathcal{O})$ under an action defined by right multiplication.

Since $D_{\mathbb{A}_f}^\times = \mathrm{GU}_1(D_{\mathbb{A}_f})$ an obvious generalisation would be to consider the open compact subgroup

$$U_1 = \mathrm{Stab}_{\mathrm{GU}_2(D_{\mathbb{A}_f})}(\mathcal{O}^2) \subset \mathrm{GU}_2(D_{\mathbb{A}_f})$$

or indeed the $\mathrm{GU}_2(D_{\mathbb{A}_f})$-stabilizer of any free $\mathcal{O}$-module of rank 2 with action given by matrix multiplication. With this in mind we investigate the general theory of $\mathcal{O}$-lattices in D^2 and return to defining U_2 afterwards.

Viewing D^n as a left D-module, we have a special Hermitian form given by

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i \overline{y_j}$$

(where $\overline{\ }$ is the standard involution on D). Under this interpretation we find that $GU_n(D)$ is the similitude group of this form.

Definition 3.5.6. Let L be a $\mathbb{Z}$-module in D^n. Then L is a left $\mathcal{O}$-lattice of D^n if it is a free left $\mathcal{O}$-module of D^n of rank n and also a $\mathbb{Z}$-lattice of D^n of rank n. □

A similar definition can be made for right $\mathcal{O}$-lattices, the distinction being made due to non-commutativity of multiplication in D.

Given a left $\mathcal{O}$-lattice $L \subseteq D^n$ we can consider its localizations $L_q := L \otimes \mathbb{Z}_q$, one for each prime q. By extension of scalars these are left $\mathcal{O}_q$-lattices in D_q^n (the definition being the same as above after tensoring everything with $\mathbb{Z}_q$).

We are mainly interested in equivalence classes of these lattices, both locally and globally.

Definition 3.5.7. Let M, M' be two left $\mathcal{O}_q$-lattices in D_q^n. We say that M and M' are equivalent if there exists $g_q \in \mathrm{GU}_2(D_q)$ such that $M = M' g_q$.

Let L, L' be two left $\mathcal{O}$-lattices in D^n. We say that L and L' are locally equivalent at q if L_q and L'_q are equivalent.

We also say that L and L' are globally equivalent if there exists $g \in \mathrm{GU}_2(D)$ such that $L' = Lg$. □

Clearly global equivalence implies local equivalence everywhere. Naturally we care about the converse since it tells us about local-global behaviour. Unfortunately the converse fails.

Definition 3.5.8. A genus of $\mathcal{O}$-lattices is a full set of $\mathcal{O}$-lattices that are locally equivalent everywhere. □

We can now speak of two lattices lying in the same genus, this being a weaker notion than global equivalence.

We will only concern ourselves with maximal lattices in this thesis. In order to learn something about the number of genera amongst maximal left $\mathcal{O}$-lattices we should first study equivalence classes of maximal left $\mathcal{O}_q$-lattices.

Shimura tells us the following (see [59]):

Theorem 3.5.9. *If D is split at q, i.e $D_q \cong M_2(\mathbb{Q}_q)$, then all maximal left $\mathcal{O}_q$-lattices of D_q^n are equivalent to $\mathcal{O}_q^n$.*

If D_q is a division algebra then there are exactly two equivalence classes of maximal left $\mathcal{O}_q$-lattices in D_q^n, one of which is represented by $\mathcal{O}_q^n$.

Corollary 3.5.10. *Let D be definite and ramified at m distinct finite primes. Then there are 2^m genera of maximal left $\mathcal{O}$-lattices in D^n.*

Proof. Let L be a maximal left $\mathcal{O}$-lattice in D^n. Then for any unramified place q of D we know that L_q is equivalent to $\mathcal{O}_q^n$.

At any ramified prime p we know that L_p is equivalent to one of two lattices, due to the Theorem. Since there are m ramified places of D and local equivalence is independent between choices of ramified primes we have at most 2^m genera.

It is shown in [59] that in fact all of these possibilities can occur. Thus we are done. □

In particular the above shows that in our case, where D has exactly one ramified finite prime, there should be exactly two genera. From now on assume we are in this case.

Definition 3.5.11. Let D be ramified at p, ∞ for some prime p:

- If a maximal left $\mathcal{O}$-lattice L is locally equivalent to $\mathcal{O}_q^n$ for all q then we say that L lies in the principal genus.
- If at the ramified prime p we have that L_p is locally inequivalent to $\mathcal{O}_p^n$ then we say that L lies in the non-principal genus.

□

For example the standard lattice $\mathcal{O}^n$ lies in the principal genus. The following explicit description of $\mathcal{O}$-lattices is due to Ibukiyama [40].

Theorem 3.5.12. *Let $n \geq 2$. Every maximal left $\mathcal{O}$-lattice in D^n can be written in the form $\mathcal{O}^n g$ for some $g \in GL_n(D)$.*

Further Ibukiyama was able to find a criterion on the matrix g that determines which genus the lattice belongs to.

Theorem 3.5.13. *Let $n \geq 2$ and suppose $L = \mathcal{O}^n g$ is a maximal left $\mathcal{O}$-lattice.*

- *L lies in the principal genus if and only if $g\overline{g}^T = mx$ for some positive $m \in \mathbb{Q}$ and some $x \in GL_n(\mathcal{O})$ such that $x = \overline{x}^T$ and such that x is positive definite, i.e. $yx\overline{y}^T > 0$ for all $y \in D^n$ with $y \neq 0$.*

- *L lies in the non-principal genus if and only if $g\overline{g}^T = m\begin{pmatrix} ps & r \\ \overline{r} & pt \end{pmatrix}$ where $m \in \mathbb{Q}$ is positive, $s, t \in \mathbb{N}, r \in \mathcal{O}$ lies in the two sided ideal of $\mathcal{O}$ above p and is such that $p^2st - N(r) = p$ (so that the matrix on the right has determinant p).*

Using the above it is easy to produce $\mathcal{O}$-lattices that are in either genus.

Example 3.5.14. The choice $g = I$ satisfies the properties in part 1 of the theorem and so $\mathcal{O}^n$ is a lattice in the principal genus, as expected. □

In practice one may almost always take $m = s = t = 1$ to produce lattices in the non-principal genus. We will make these choices from now on.

Given a maximal $\mathcal{O}$-lattice $L = \mathcal{O}^n g$ one can consider $\mathrm{Stab}_{\mathrm{GU}_n(D_{\mathbb{A}_f})}(L)$ (where we view L as the collection of its localizations). Such stabilizer subgroups are open compact subgroups of $\mathrm{GU}_n(D_{\mathbb{A}_f})$ and so serve well as level structures for algebraic modular forms on $GU_n(D)$.

Let $n = 2$ now. Earlier we defined $U_1 = \mathrm{Stab}_{\mathrm{GU}_2(D_{\mathbb{A}_f})}(\mathcal{O}^2)$. We now have an interpretation of this as the stabilizer of a lattice lying in the principal genus.

In a similar vein we fix a choice of $g \in \mathrm{GL}_2(D)$ as in part 2 of Theorem 3.5.13 (taking $m = s = t = 1$). Then the corresponding lattice lies in the non-principal genus and so we get a genuinely different open compact subgroup $U_2 = \mathrm{Stab}_{\mathrm{GU}_2(D_{\mathbb{A}_f})}(\mathcal{O}^2 g)$. This is the open compact subgroup used in Ibukiyama's correspondence.

As a final remark the adelic modular curves $\mathrm{GU}_2(D)\backslash\mathrm{GU}_2(D_{\mathbb{A}_f})/U_i$ for $i = 1, 2$ have interpretations in this setting as global equivalence classes of lattices within the genus determined by U_i. Thus the class number has an arithmetic significance here.

3.5.3 Hecke operators

Before discussing the new subspace of $\mathcal{A}(\mathrm{GU}_2(D), U_2, V_{j,k-3})$ it remains to explain the transfer of the Hecke operators. The story is similar to the Eichler correspondence but has subtle differences. Again, we will only see this for $q \neq p$.

The Hecke action of T_q at $q \neq p$ for level p Siegel forms is defined by the double coset operator for the matrix

$$M_q = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & q & 0 \\ 0 & 0 & 0 & q \end{pmatrix} \in \mathrm{GSp}_4(\mathbb{Q}_q).$$

Now since D splits at q we have that $\mathrm{GU}_2(D_q) \cong \mathrm{GSp}_4(\mathbb{Q}_q)$. Fixing such an isomorphism as in Corollary 3.5.4 we may choose $v_q \in \mathrm{GU}_2(D_q)$ such that $v_q \mapsto M_q$.

Let $g_q \in \mathrm{GL}_2(D_q)$ be the q component of the matrix g as chosen in Theorem 3.5.13 (as embedded diagonally into $\mathrm{GL}_2(D_{\mathbb{A}_f})$). We know by definition of the non-principal genus that $\mathcal{O}^2 g$ is locally equivalent to $\mathcal{O}^2$ at $q \neq p$. Thus there exists $h_q \in \mathrm{GU}_2(D_q)$ such that $\mathcal{O}_q^2 g_q = \mathcal{O}_q^2 h_q$. We then have a corresponding $u_q \in \mathrm{GU}_2(D_q)$ given by $u_q = h_q v_q h_q^{-1}$.

This may seem like a convoluted way to construct u_q in comparison to previous choices but the key point here is we cannot assume that g_q lies in $\mathrm{GU}_2(D_q)$. We will see why this is important later.

Let $u \in \mathrm{GU}_2(D_{\mathbb{A}_f})$ have u_q as the component at q and have identity component elsewhere.

Definition 3.5.15. For the above choice of u, the corresponding Hecke operator on $\mathcal{A}^{\mathrm{new}}(\mathrm{GU}_2(D), U_2, V_{j,k-3})$ will be called $T_{u,q}$. □

Under Ibukiyama's (conjectural) correspondence it is predicted that:

$$T_q \longleftrightarrow T_{u,q}.$$

Recall that we are really only interested in eigenvalues for the T_q operator in Harder's conjecture so we will only be interested in decomposing $U_2 u U_2$ into left cosets. This will be done later too in a similar fashion to the Eichler correspondence.

3.5.4 The new subspace

Our final task in defining Ibukiyama's correspondence is to explain what is meant by the new subspace $\mathcal{A}^{\mathrm{new}}(\mathrm{GU}_2(D), U_2, V_{j,k-3})$. We will not go into too much detail but will refer the reader to Ibukiyama's papers [39], [41]. The results below are written in much greater generality in this paper and the constructions will be similar to those found in the description of Eichler's correspondence (see subsection 3.3.1).

For convenience we will make the following definitions:

$$A_s(D) := \mathcal{A}(D^\times, U, V_s)$$
$$A_{s,t}(D) := \mathcal{A}(\mathrm{GU}_2(D), U_2, V_{s,t})$$

Suppose $x_1, x_2, ..., x_m$ are representatives for $D^\times \backslash D_{\mathbb{A}_f}^\times / U$ and $y_1, y_2, ..., y_n$ are representatives for $\mathrm{GU}_2(D) \backslash \mathrm{GU}_2(\mathbb{A}_f) / U_2$.

Let $G = D^\times \times \mathrm{GU}_2(D)$. Then we have an open compact subgroup $U' = U \times U_2$ and finite dimensional representations $W_{j,k-3} := V_j \otimes V_{j,k-3}$ of $G(\mathbb{A}_f)$.

We start with the decompositions:

$$\begin{aligned}\mathcal{A}(G, U', W_{j,k-3}) &\cong A_j(D) \otimes A_{j,k-3}(D) \\ &\cong \oplus_{a=1}^{m} \oplus_{b=1}^{n} W_{j,k-3}^{(a,b)}\end{aligned}$$

where $W_{j,k-3}^{(a,b)}$ is the subspace of $W_{j,k-3}$ fixed by both $E_a = D^\times \cap x_a U x_a^{-1}$ and $N_b = \mathrm{GU}_2(D) \cap y_b U_2 y_b^{-1}$.

Ibukiyama takes $F \in \mathcal{A}(G, U', W_{j,k-3})$. By the first decomposition $F = \sum_{i,j} F_{1,i} \otimes F_{2,j}$ where $F_{1,i} \in A_j(D)$ and $F_{2,j} \in A_{j,k-3}(D)$ are eigenforms. If F itself is an eigenform then $F = F_1 \otimes F_2$ for eigenforms F_1, F_2. He then associates a theta series θ_F to F. This is an elliptic modular form and one can measure the notion of old form in $A_{j,k-3}(D)$ using θ_F.

In order to describe θ_F we first need an explicit description of the representation spaces $W_{j,k-3}$.

For $v \in \mathbb{N}$ recall the spaces $\mathcal{P}_v^{(n)}$ of real harmonic homogeneous polynomials of degree v in n variables. Since $\mathbb{H}^2 \cong \mathbb{R}^8$ we can view polynomials in $\mathcal{P}_v^{(8)}$ as polynomials in 2 quaternion variables. It is known that $W_{j,k-3}$ can be viewed as a subspace $\mathcal{P}$ of $\mathcal{P}_{j+2k-6}^{(8)}$ (see p.309 of [39]).

Let $L = \mathcal{O}^2 g$ be a fixed lattice in the non-principal genus. Then for each pair (a, b) with $1 \leq a \leq m$ and $1 \leq b \leq n$ we can construct a left $\mathcal{O}$-lattice $L_{a,b}$ that is locally equivalent to $\overline{x_a} L y_b$ everywhere.

Now returning to our $F \in \mathcal{A}(G, U', W_{j,k-3})$ with components $F_{a,b} \in W_{j,k-3}^{(a,b)}$ we can construct the following partial theta series for each a, b (with $\tau \in \mathcal{H}$):

$$\theta_F^{(a,b)}(\tau) = \sum_{(x,y) \in L_{a,b}} F_{a,b}(x, y) e^{\frac{2\pi i \tau N(x,y)}{N_{a,b}}}$$

where:

- $F_{a,b}(x, y) \in \mathcal{P}_{j+2k-6}^{(8)}$ corresponds to $F_{a,b}$ under the isomorphism $W_{j,k-3} \cong \mathcal{P}$,
- $N(x, y) = N(x) + N(y)$ is the norm of a vector in $\mathbb{H}^2$ under the standard Hermitian form described before Definition 3.5.6,
- $N_{a,b}$ is the unique positive generator of the ideal of $\mathbb{Z}$ generated by the norms of elements in $L_{a,b}$.

One then constructs the theta series of F via a weighted sum:

$$\theta_F(\tau) = \sum_{a=1}^{m}\sum_{b=1}^{n} \frac{1}{|E_a||N_b|}\theta_F^{(a,b)}(\tau).$$

It is true that θ_F is an elliptic modular form for $SL_2(\mathbb{Z})$ of weight $j+2k-2$. In fact whenever $j+2k-6 \neq 0$ it is a cusp form.

Definition 3.5.16. The subspace of old forms $A^{\text{old}}_{j,k-3}(D) \subseteq A_{j,k-3}(D)$ is generated by those eigenforms $F_2 \in A_{j,k-3}(D)$ such that there exists an eigenform $F_1 \in A_j(D)$ satisfying $\theta_{F_1 \otimes F_2} \neq 0$.

The subspace of new forms $A^{\text{new}}_{j,k-3}(D)$ is the orthogonal complement of the old space with respect to the inner product in Proposition 3.2.14. □

It should be noted that by Eichler's correspondence $F_1 \in A_j(D)$ can be viewed as an elliptic modular form for $\Gamma_0(p)$ of weight $j+2$. Further it will be a new cusp form precisely when $j > 0$. Thus computationally it is not difficult to find the new and old subspaces.

Evidence for Ibukiyama's correspondence has been provided in [37] but a proof still eludes us. More specifically Ibukiyama has checked that the dimensions of both spaces of forms agree for almost all cases.

Theorem 3.5.17. *For $k > 4$ and even $j \geq 0$ we have:*

$$\begin{aligned} dim(S^{new}_{j,k}(K(p))) &= dim(A^{new}_{j,k}(D)) \\ &= dim(A_{j,k-3}(D)) - dim(S_{j+2k-2}(SL_2(\mathbb{Z})))dim(B^{new}_{j+2}(\Gamma_0(p))) \end{aligned}$$

where

$$B^{new}_{j+2}(\Gamma_0(p)) = \begin{cases} M_2(\Gamma_0(p)) & \text{for } j = 0 \\ S^{new}_{j+2}(\Gamma_0(p)) & \text{for } j > 0 \end{cases}$$

In some sense the evidence provided in this thesis can serve as either evidence towards this conjecture (assuming Harder's conjecture to be true) or as evidence for Harder's conjecture (assuming Ibukiyama's correspondence to be true).

Chapter 4

Finding evidence for Harder's conjecture

Now that we have linked spaces of Siegel modular forms $S^{\text{new}}_{j,k}(K(p))$ with spaces of algebraic modular forms $A^{\text{new}}_{j,k-3}(D) = \mathcal{A}^{\text{new}}(\mathrm{GU}_2(D), U_2, V_{j,k-3})$, we can begin to generate evidence for Harder's conjecture.

It should be noted that the results of this chapter are the author's unless otherwise stated.

4.1 Brief plan of the strategy

The main idea of our strategy is to work backwards from the algebraic side, since we have a few computational limitations there. In particular we require $\dim(A^{\text{new}}_{j,k-3}(D))$ to be small for the trace formula to be efficient. Also we would like the class number h to be small too. In this thesis we will deal with cases where $h = 1$ and $\dim(A^{\text{new}}_{j,k-3}(D)) = 1$. We will soon see that this is not as big a restriction as it seems, and that enough new congruences can be generated.

Here is the general strategy:

1. Find all primes p such that the class number $h = |G(\mathbb{Q})\backslash G(\mathbb{A}_f)/U_2| = 1$.
2. For each such p calculate the corresponding Γ-group, $\Gamma^{(2)} = \mathrm{GU}_2(D) \cap U_2$.
3. Calculate $\dim(A^{\text{new}}_{j,k-3}(D))$ for a wide range of j, k values and look for 1-dimensional spaces.

4. For each 1-dimensional space $A^{\text{new}}_{j,k-3}(D)$ look in the space of elliptic forms $S^{\text{new}}_{j+2k-2}(\Gamma_0(p))$ for normalized eigenforms f which have a "large prime" dividing $\Lambda_{\text{alg}}(f, j+k) \in \mathbb{Q}_f$ (recall that we have the MAGMA command LRatio to do this for us almost canonically).

   Note that j, k are fixed at this point, so we know exactly which L-value to look at.

5. Find the Hecke representatives for the $T_{u,q}$ operator at a chosen prime q.

6. Use the Dummigan trace formula to find $\text{tr}(T_{u,q})$ for T_q acting on $A_{j,k-3}(D)$.

7. Subtract off the trace contribution of $T_{u,q}$ acting on $A^{\text{old}}_{j,k-3}(D)$ in order to get the trace of the action on $A^{\text{new}}_{j,k-3}(D)$.

   Since the spaces of algebraic forms I am using are 1-dimensional, this trace should be exactly the Hecke eigenvalue of a new paramodular eigenform by Ibukiyama's conjecture.

8. Check that Harder's congruence holds.

The above strategy can be modified to work for bigger spaces of algebraic forms, but there is more to do computationally. In general there will be more Γ-groups, and we must calculate not just $\text{tr}(T_{u,q})$ but also $\text{tr}(T^2_{u,q})$, ..., $\text{tr}(T^d_{u,q})$, where $d = \dim(A^{\text{new}}_{j,k-2}(D))$ (and employ symmetric polynomial formulae, such as Newton's identities, to solve for the eigenvalues).

It should be noted that in this thesis I will only compute the action of $T_{u,3}$ when $p = 2$, and of $T_{u,2}$ otherwise. However, I will describe a general algorithm for finding the Hecke representatives at any q, which can easily be implemented for any class number one situation.

4.2 Explicit results for $A_{j,k-3}(D)$

Now that the strategy has been revealed, work can begin on finding all of the parameters needed to calculate with the algebraic forms. This will not be a straight forward task, as we shall see.

4.2.1 Finding the Γ-groups

Recall that the space of algebraic modular forms $A_{j,k-3}(D)$ can be expressed naturally as a direct sum of fixed subspaces of $V_{j,k-3}$:

$$A_{j,k-3}(D) \cong \oplus_{m=1}^{h} V_{j,k-3}^{\Gamma_m},$$

where $\{z_1, z_2, ..., z_h\} \subset \mathrm{GU}_2(\mathbb{A}_f)$ are representatives for $\mathrm{GU}_2(D)\backslash\mathrm{GU}_2(D_{\mathbb{A}_f})/U_2$, and for each $m = 1, 2, ..., h$ we have the group $\Gamma_m = \mathrm{GU}_2(D) \cap z_m U_2 z_m^{-1}$. Amongst these groups is the group $\Gamma^{(2)} = \mathrm{GU}_2(D) \cap U_2$.

If the class number h of U_2 is 1 then

$$A_{j,k-3}(D) \cong V_{j,k-3}^{\Gamma^{(2)}}.$$

How might one go about calculating $\Gamma^{(2)}$ explicitly? In this subsection an efficient algorithm will be proposed that works for D ramified at $\{p, \infty\}$. We will see that due to the geometric nature of U_2 as the stabilizer of an $\mathcal{O}$-lattice we can get an efficient algorithm to find $\Gamma^{(2)}$.

Previously we defined $U_2 = \mathrm{Stab}_{\mathrm{GU}_2(D_{\mathbb{A}_f})}(\mathcal{O}^2 g)$, where $g \in \mathrm{GL}_2(D)$ is such that

$$A := g\overline{g}^T = \begin{pmatrix} p & r \\ \overline{r} & p \end{pmatrix},$$

for some $r \in \mathcal{O}$ satisfying $N(r) = p(p-1)$ (in order for $\det(A) = p$ to hold). Such a choice of g guarantees that $\mathcal{O}^2 g$ is in the non-principal genus of $\mathcal{O}$-lattices of D^2. The matrix A is then the Gram matrix of such a lattice for the underlying Hermitian inner product.

For the results in this section we fix a choice of g (hence fixing A). Later we will make a specific choice to aid calculation.

We seek the group $\Gamma^{(2)}$ and by the above we find that

$$\Gamma^{(2)} = \mathrm{Stab}_{\mathrm{GU}_2(D)}(\mathcal{O}^2 g),$$

since the rational points of an algebraic group are embedded as a subgroup of the adelic points.

An explicit description can be found for this stabilizer. First we recall a basic fact from the theory of group actions.

Lemma 4.2.1. *Let G be a group and let X be a set equipped with a right action of G. Denote by S_y the stabilizer of $y \in X$ under this action. Then for each $(g, x) \in G \times X$ we have that:*

$$S_{xg} = g^{-1} S_x g,$$

so that stabilizer subgroups of elements in the same orbit are conjugate.

It will become necessary to refer to matrices in $\mathrm{GU}_2(D)$ of a specific similitude. For $\theta \in \mathbb{Q}^\times$ let:

$$\mathrm{GU}_n(D)_\theta = \{\gamma \in \mathrm{GU}_2(D) \,|\, \mu(\gamma) = \theta\},$$

In particular let $\mathrm{SU}_2(D) := \mathrm{GU}_2(D)_1$.

Lemma 4.2.2.

$$S := Stab_{GL_2(D)}(\mathcal{O}^2) = GL_2(\mathcal{O}).$$

Proof. Suppose $\gamma \in \mathrm{GL}_2(\mathcal{O})$. Then both γ and γ^{-1} have integral entries so that

$$\mathcal{O}^2\gamma \subseteq \mathcal{O}^2$$

and

$$\mathcal{O}^2\gamma^{-1} \subseteq \mathcal{O}^2.$$

Then $\mathcal{O}^2 \subseteq \mathcal{O}^2\gamma$. Equality follows and thus $\gamma \in S$.

Conversely suppose that $\gamma \in S$ so that $\gamma \in \mathrm{GL}_2(D)$ and

$$\mathcal{O}^2\gamma = \mathcal{O}^2\gamma^{-1} = \mathcal{O}^2.$$

In particular the four vectors $(1,0)\gamma, (1,0)\gamma^{-1}, (0,1)\gamma$ and $(0,1)\gamma^{-1}$ lie in $\mathcal{O}^2$. Thus both γ and γ^{-1} have entries in $\mathcal{O}$, hence $\gamma \in \mathrm{GL}_2(\mathcal{O})$. □

Tying together the lemmas gives us the following explicit description of $\Gamma^{(2)}$.

Theorem 4.2.3. *Given a choice of g as above the group $\Gamma^{(2)}$ consists of the following set of matrices:*

$$\Gamma^{(2)} = SU_2(D) \cap g^{-1}GL_2(\mathcal{O})g$$

Proof. We know that:

$$\Gamma^{(2)} = \mathrm{Stab}_{\mathrm{GU}_2(D)}(\mathcal{O}^2 g) = \mathrm{GU}_2(D) \cap \mathrm{Stab}_{\mathrm{GL}_2(D)}(\mathcal{O}^2 g)$$

$$= \mathrm{GU}_2(D) \cap g^{-1}Sg = \mathrm{GU}_2(D) \cap g^{-1}\mathrm{GL}_2(\mathcal{O})g.$$

It remains to show that any such matrix has similitude 1.

Take $\gamma \in \mathrm{GU}_2(D) \cap g^{-1}\mathrm{GL}_2(\mathcal{O})g$. Then $\gamma\overline{\gamma}^T = \mu(\gamma)I$ for some $\mu(\gamma) \in \mathbb{Q}^\times$. But also $\gamma = g^{-1}\psi g$ for some $\psi \in \mathrm{GL}_2(\mathcal{O})$ so we must have $\mu(\gamma) = \mu(\psi) \in \mathbb{Z}^\times = \{\pm 1\}$.

Since D is a definite quaternion algebra over $\mathbb{Q}$ it must be that $\mu(\gamma) > 0$ (since the norm form is positive definite). Hence $\mu(\gamma) = 1$. □

Recall also that we have defined another compact open subgroup $U_1 = \mathrm{Stab}_{\mathrm{GU}_2(\mathbb{A}_f)}(\mathcal{O}^2) \subset \mathrm{GU}_2(D_{\mathbb{A}_f})$. This is the stabilizer of a left $\mathcal{O}$-lattice lying in the principal genus.

In this case the analogue of the group $\Gamma^{(2)}$ is the group $\Gamma^{(1)} = \mathrm{GU}_2(D) \cap U_1$. We can employ identical arguments to the above to show the following:

Lemma 4.2.4.

$$\Gamma^{(1)} = SU_2(D) \cap GL_2(\mathcal{O})$$

Notice the striking similarity between this result and the description $\Gamma = D^\times \cap U = \mathcal{O}^\times$ in subsection 3.3.2. Indeed $\Gamma^{(1)}$ consists of integral matrices of similitude 1 whereas $\mathcal{O}^\times$ consists of integral quaternions with norm 1. Later more similarities will be observed for the Hecke representatives.

Now that we have simple descriptions of $\Gamma^{(1)}$ and $\Gamma^{(2)}$, one might be tempted to try and set up a brute force search for the elements of these groups. For $\Gamma^{(1)}$ this is simple.

Theorem 4.2.5.

$$\Gamma^{(1)} = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \beta \end{pmatrix}, \begin{pmatrix} 0 & \alpha \\ \beta & 0 \end{pmatrix} \middle| \alpha, \beta \in \mathcal{O}^\times \right\}.$$

Proof. Take $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma^{(1)}$. Then $a, b, c, d \in \mathcal{O}$.

The fact that $\gamma \in \mathrm{SU}_2(D)$ tells us that:

$$N(a) + N(b) = 1$$

$$N(c) + N(d) = 1$$

$$a\bar{c} + b\bar{d} = 0$$

Since $N(a), N(b), N(c), N(d) \in \mathbb{Z}$ the first two equations tell us that that exactly one of a, b lies in $\mathcal{O}^\times$, exactly one of c, d lies in $\mathcal{O}^\times$ and the other two elements are 0. However, the third equation tells us that $N(a)N(c) = N(b)N(d)$ and so it must either be that $a, d \in \mathcal{O}^\times$ and $b = c = 0$ or $b, c \in \mathcal{O}^\times$ and $a = d = 0$.

Clearly each such matrix is in $\Gamma^{(1)}$ and so we are done. □

Computationally it is not straight forward to find the elements of $\Gamma^{(2)}$ due to the non-integrality of the entries of such matrices. We would like to find a better description of this group such that the norm equations involved are easier to solve.

We note that the non-integrality of the matrices in $\Gamma^{(2)}$ is due to the fact that such matrices lie in $g^{-1}\mathrm{GL}_2(\mathcal{O})g$. Thus $g\Gamma^{(2)}g^{-1} \subseteq \mathrm{GL}_2(\mathcal{O})$.

For $\theta \in \mathbb{Q}^\times$ consider the sets

$$Y_\theta = \mathrm{GU}_2(D)_\theta \cap g^{-1}M_2(\mathcal{O})^\times g$$

and

$$W_\theta = \{\nu \in M_2(\mathcal{O})^\times \mid \nu A\overline{\nu}^T = \theta A\},$$

where $M_2(\mathcal{O})^\times = \mathrm{GL}_2(D) \cap M_2(\mathcal{O})$ and $A = g\bar{g}^T$.

Then in particular $Y_1 = \Gamma^{(2)}$. Later we will need to consider the sets Y_q for prime $q \neq p$ when finding Hecke representatives.

Proposition 4.2.6. *For each $\theta \in \mathbb{Q}^\times$ there exists a bijection:*

$$\Phi_\theta : Y_\theta \longrightarrow W_\theta$$

given by:

$$\gamma \longmapsto g\gamma g^{-1}.$$

In particular:

$$\Gamma^{(2)} = g^{-1} W_1 g.$$

Proof. Since Φ_θ is given by conjugation the map is invertible as long as we can show it is well defined.

Take $\gamma \in Y_\theta$. Note that:

$$\begin{aligned}(g\gamma g^{-1})A\overline{(g\gamma g^{-1})}^T = \theta A &\iff g\gamma\overline{\gamma}^T\overline{g}^T = \theta A \\ &\iff \gamma\overline{\gamma}^T = \theta I.\end{aligned}$$

Thus $\gamma \in Y_\theta$ if and only if $\Phi_\theta(\gamma) \in W_\theta$ and so we are done. The claim about $\Gamma^{(2)}$ is the case $\theta = 1$. □

Unfortunately it is still not an easy task to find the elements of W_θ since A has non-diagonal entries.

To fix this we diagonalize A. By the spectral theory of quaternionic Hermitian matrices we can find an invertible matrix $P \in \mathrm{GL}_2(D)$ such that $PA\overline{P}^T = B$ where $B \in M_2(D)$ is a diagonal matrix. Then another explicit description of W_θ arises.

Proposition 4.2.7. *For each $\theta \in \mathbb{Q}^\times$ the map*

$$W_\theta \longrightarrow Z_\theta := \{\eta \in P\, M_2(\mathcal{O})^\times\, P^{-1} \,|\, \eta B\overline{\eta}^T = \theta B\}$$

$$\nu \longmapsto P\nu P^{-1},$$

is a bijection.

In particular:

$$W_1 = P^{-1} Z_1 P.$$

Proof. Again the map is given by conjugation so is invertible if we can show it is well defined.

Take $\nu \in W_\theta$. Then $(P\nu P^{-1})B\overline{(P\nu P^{-1})}^T = \theta B$ if and only if $P(\nu A\overline{\nu}^T)\overline{P}^T = \theta B$ (using the fact that $B = PA\overline{P}^T$). This is clearly equivalent to $\nu A\overline{\nu}^T = \theta A$.

Thus $\nu \in W_\theta$ if and only if $P\nu P^{-1} \in Z_\theta$ and so we are done. The claim about W_1 is the case $\theta = 1$. □

Notice that we were able to diagonalize A but at the expense of creating non-integral entries in the matrices $P\nu P^{-1}$. However we will now observe that if we make an appropriate choice of g then we can diagonalize A in such a way as to preserve one integral entry in $P\nu P^{-1}$, making a search for the elements of Z_θ more efficient.

Lemma 4.2.8. *Suppose we can choose $\lambda, \mu \in \mathcal{O}$ such that $N(\lambda) = p - 1$ and $N(\mu) = p$. Then*

$$g_{\lambda,\mu} := \begin{pmatrix} 1 & \lambda \\ 0 & \mu \end{pmatrix}$$

is a valid choice.

Proof. We must check that the Gram matrix $A_{\lambda,\mu} = g_{\lambda,\mu}\overline{g_{\lambda,\mu}}^T$ has the correct form. This is a simple calculation:

$$A_{\lambda,\mu} = \begin{pmatrix} 1 & \lambda \\ 0 & \mu \end{pmatrix}\begin{pmatrix} 1 & 0 \\ \overline{\lambda} & \overline{\mu} \end{pmatrix} = \begin{pmatrix} 1+N(\lambda) & \lambda\overline{\mu} \\ \mu\overline{\lambda} & N(\mu) \end{pmatrix} = \begin{pmatrix} p & r \\ \overline{r} & p \end{pmatrix},$$

where $r = \lambda\overline{\mu}$. It is now observed that $\det(A_{\lambda,\mu}) = p^2 - N(r) = p^2 - p(p-1) = p$ as required. □

Such an upper triangular g is the simplest choice, since no diagonal matrix can have Gram matrix of the correct form.

In addition to the conditions above I would also like to assume that $r = \lambda\overline{\mu}$ has trace zero. The reasons for this will become clear soon.

A natural question to ask at this stage is whether, given a fixed maximal order, it is always possible to choose $\lambda, \mu \in \mathcal{O}$ that satisfy $N(\lambda) = p - 1$, $N(\mu) = p$ and $\mathrm{tr}(r) = 0$. Unfortunately the answer is no. However, it is in fact always possible to find **some** maximal order $\mathcal{O}$ where these choices are possible. For proof of this I refer to an online discussion with Voight [70], of which the author is grateful.

For now, assume we have a fixed $\mathcal{O}$ with the property that such elements may be found. We now seek a suitable invertible matrix that diagonalises $A_{\lambda,\mu}$.

Lemma 4.2.9. *The matrix*

$$P_{\lambda,\mu} = \begin{pmatrix} 1 & \frac{\overline{r}}{p} \\ 0 & 1 \end{pmatrix}$$

diagonalises A. Further $P_{\lambda,\mu}^{-1} = \overline{P_{\lambda,\mu}}$.

Proof. We check

$$P_{\lambda,\mu} A \overline{P_{\lambda,\mu}}^T = \begin{pmatrix} 1 & \frac{\overline{r}}{p} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & r \\ \overline{r} & p \end{pmatrix} \begin{pmatrix} 1 & 0 \\ \frac{r}{p} & 1 \end{pmatrix} = \begin{pmatrix} p + \frac{r^2}{p} + \frac{\overline{r}}{p}(\mathrm{tr}(r)) & \mathrm{tr}(r) \\ \mathrm{tr}(r) & p \end{pmatrix}$$

$$= \begin{pmatrix} p + \frac{r^2}{p} & 0 \\ 0 & p \end{pmatrix}$$

since $\mathrm{tr}(r) = 0$.

Recall that the characteristic polynomial of $\alpha \in D$ is

$$f_\alpha(x) = x^2 - \mathrm{tr}(\alpha)x + N(\alpha)$$

and that α must satisfy $f_\alpha(\alpha) = 0$ (Cayley-Hamilton). Then r satisfies

$$r^2 + p(p-1) = 0,$$

i.e. $r^2 = -p(p-1)$. Thus

$$P_{\lambda,\mu} A \overline{P_{\lambda,\mu}}^T = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}.$$

The final claim follows from

$$P_{\lambda,\mu} \overline{P_{\lambda,\mu}} = \begin{pmatrix} 1 & \frac{\overline{r}}{p} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \frac{r}{p} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{\mathrm{tr}(r)}{p} \\ 0 & 1 \end{pmatrix} = I$$

and similarly for $\overline{P_{\lambda,\mu}} P_{\lambda,\mu}$. □

We now show that the elements of the set Z_θ each have an integral entry if we choose to use $g_{\lambda,\mu}$ and $P_{\lambda,\mu}$.

Corollary 4.2.10. *Let $\nu \in M_2(\mathcal{O})$. Then the bottom left entries of ν and $P_{\lambda,\mu}\nu\overline{P_{\lambda,\mu}}$ are equal (in particular this entry remains in $\mathcal{O}$).*

Proof. Let $\nu = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ with $\alpha, \beta, \gamma, \delta \in \mathcal{O}$. Then a simple calculation shows that

$$P_{\lambda,\mu}\nu\overline{P_{\lambda,\mu}} = \begin{pmatrix} \alpha + \frac{\overline{r}\gamma}{p} & (\frac{\alpha r}{p} + \beta) + \frac{\overline{r}}{p}(\frac{\gamma r}{p} + \delta) \\ \gamma & \frac{\gamma r}{p} + \delta \end{pmatrix}.$$

The bottom left entry is $\gamma \in \mathcal{O}$, as required. □

Now consider the equations that must be satisfied for a matrix to be in Z_θ. Let $\eta = \begin{pmatrix} x & y \\ z & w \end{pmatrix} \in M_2(D)$. In order to satisfy

$$\eta \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \overline{\eta}^T = \theta \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$$

the entries of η must solve three equations:

$$N(x) + pN(y) = \theta$$

$$N(z) + pN(w) = \theta p$$

$$x\overline{z} + py\overline{w} = 0.$$

Clearly these equations can have no solutions for $\theta < 0$ and so we only consider $\theta \geq 0$.

Notice that these three equations imply that $N(x) = N(w)$ and $N(z) = p^2 N(y)$. This is obvious if $\theta = 0$ since the norm form is positive definite so all four norms would have to be 0 (in fact $x = y = z = w = 0$ is the only possibility for the elements).

If $\theta > 0$ then it is still straight forward to check. Indeed $x\overline{z} + py\overline{w} = 0$ implies $N(x)N(z) = p^2 N(y)N(w)$ and by using the first two equations to eliminate $N(z)$ and $N(y)$ we find that:

$$N(x)(\theta p - pN(w)) = p^2 \left(\frac{\theta - N(x)}{p} \right) N(w)$$

which simplifies to

$$N(x)(\theta - N(w)) = (\theta - N(x))N(w)$$

giving $N(x) = N(w)$ (since $\theta \neq 0$).

To see the second claim we note that again by the first two equations

$$N(z) = p(\theta - N(w)) = p(\theta - N(x)) = p^2 N(y).$$

We can now give explicit norm equations defining the elements of W_θ.

Corollary 4.2.11. *Let $\theta \geq 0$. Then W_θ consists of all matrices $\nu = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathcal{O})^\times$ such that:*

$$pN(p\alpha + \overline{r}\gamma) + N(p(\alpha r + p\beta) + \overline{r}(\gamma r + p\delta)) = \theta p^3$$

$$pN(\gamma) + N(\gamma r + p\delta) = \theta p^2$$

$$p\alpha\overline{\gamma} + (\alpha r + p\beta)(\overline{\gamma r + p\delta}) = -\theta p\overline{r}.$$

Proof. We have already seen that W_θ is in bijection with Z_θ via $\nu \mapsto P_{\lambda,\mu}\nu\overline{P_{\lambda,\mu}}$. Let $\nu = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathcal{O})^\times$.

We have just seen (in the proof of Corollary 4.2.10) that

$$P_{\lambda,\mu}\nu\overline{P_{\lambda,\mu}} = \begin{pmatrix} \alpha + \frac{\overline{r}\gamma}{p} & (\frac{\alpha r}{p} + \beta) + \frac{\overline{r}}{p}(\frac{\gamma r}{p} + \delta) \\ \gamma & \frac{\gamma r}{p} + \delta \end{pmatrix}.$$

Also we know the equations that must be satisfied by these entries in order for the corresponding matrix to lie in Z_θ. Substituting these in and clearing denominators gives the required equations (after simplification of the third equation). □

It now becomes clear why we wanted to preserve one of the entries of ν. From the second equation it is easily seen that $N(\gamma) \leq \theta p$, and since $\gamma \in \mathcal{O}$ there are only finitely many such elements (each norm must be a positive integer and there are only finitely many elements for each possibility).

It is possible now to develop an algorithm to calculate W_θ. For simplicity we assume $\theta \in \mathbb{N}$ but it will be clear how this algorithm can be modified for rational $\theta \geq 0$.

Recall that we denote by X_i the subset of $\mathcal{O}$ consisting of norm i elements.

Algorithm 1

Step 0: Set $j := 0$. For each integer $0 \leq i \leq \theta p$, generate the norm lists $X_i, X_{p(\theta p - i)}, X_{p^2 i}$.

Step 1: For each pair of elements $(\gamma, \gamma') \in X_j \times X_{p(\theta p - j)}$ check whether the element $\delta := \frac{\gamma' - \gamma r}{p} \in \mathcal{O}$.

Thus we have generated the possible pairs (γ, δ) that can satisfy the second norm equation of Corollary 4.2.11 when $N(\gamma) = j$.

Step 2: For each putative $\gamma \in X_j$ from Step 1 find all elements $\gamma'' \in X_{p(\theta p - j)}$ such that the element $\alpha := \frac{\gamma'' - \overline{r}\gamma}{p} \in \mathcal{O}$.

Thus we have generated the possible triples (α, γ, δ) that can satisfy the norm equations of Corollary 4.2.11 when $N(\gamma) = j$.

Step 3: For each putative triple (α, γ, δ) from Step 2 and each $\gamma''' \in X_{p^2 j}$ test whether the element $\beta := \frac{\gamma''' - (\overline{r}(\gamma r + p\delta) + p\alpha r)}{p^2} \in \mathcal{O}$.

This gives us all possible tuples $(\alpha, \beta, \gamma, \delta)$ satisfying the norm equations of Corollary 4.2.11 with $N(\gamma) = j$.

Step 4: Check that the entries of each putative tuple from Step 4 satisfies the third equation of Corollary 4.2.11.

This produces all matrices $\nu = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in W_\theta$ with $N(\gamma) = j$.

Step 5: Set $j := j + 1$ and repeat steps 1-4 until $j > \theta p$.

Of course once the elements of W_θ have been found it is straight forward to generate the elements of Y_θ by inverting the bijection Φ_θ in Proposition 4.2.6.

It should be noted that if we run this algorithm for $p = 2$ with the following choices

$$D = \left(\frac{-1,-1}{\mathbb{Q}}\right)$$

$$\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\frac{1+i+j+k}{2}$$

$$\lambda = -1$$

$$\mu = i - k$$

$$\theta = 1$$

then we get exactly the same elements for $Y_1 = \Gamma^{(2)}$ as Ibukiyama does on p.592 of [37].

4.2.2 Finding h

In a similar vein to Eichler's correspondence we can use mass arguments to get information on class numbers h_1 and h_2 for U_1 and U_2.

We define the mass of open compact $U \subset \mathrm{GU}_2(D_{\mathbb{A}_f})$ as follows:

$$M(U) := \sum_{m=1}^{h} \frac{1}{|\Gamma_m|},$$

where $\Gamma_m = \mathrm{GU}_2(D) \cap z_m U z_m^{-1}$ for representatives $z_1, z_2, ..., z_m \in \mathrm{GU}_2(D_{\mathbb{A}_f})$ of $\mathrm{GU}_2(D) \backslash \mathrm{GU}_2(D_{\mathbb{A}_f}) / U$.

Ibukiyama provides the following formulae for $M(U_1)$ and $M(U_2)$ in [37].

Theorem 4.2.12. *If D is ramified at p and ∞ then:*

$$M(U_1) = \frac{(p-1)(p^2+1)}{5760},$$

$$M(U_2) = \frac{p^2-1}{5760}.$$

This formula is analogous to the Eichler mass formula and is also a special case of the mass formula of Gan, Hanke and Yu [25].

Proposition 4.2.13. *$h_1 = 1$ if and only if $|\Gamma^{(1)}| = \frac{5760}{(p-1)(p^2+1)}$. Similarly $h_2 = 1$ if and only if $|\Gamma^{(2)}| = \frac{5760}{p^2-1}$.*

Proof. For $i = 1, 2$ take $z = \mathrm{id}$ as one of the representatives for the double coset space $\mathrm{GU}_2(D)\backslash\mathrm{GU}_2(D_{\mathbb{A}_f})/U_i$. Then the group $\Gamma^{(i)} = \mathrm{GU}_2(D) \cap U_i$ contributes $\frac{1}{|\Gamma^{(i)}|}$ to the finite sum $M(U_i)$.

It is then clear that $h_i = 1$ occurs for U_i if and only if

$$|\Gamma^{(i)}| = \frac{1}{M(U_i)}.$$

□

In the case of the Eichler mass formula the group $\Gamma = \mathcal{O}^\times$ is straight forward to compute and so it is a simple matter to see when $h = 1$. For the GU_2 case we can still do this for $\Gamma^{(1)}$ and $\Gamma^{(2)}$, but it needs more computation.

Corollary 4.2.14. *$h_1 = 1$ if and only if $p = 2, 3$. Similarly $h_2 = 1$ if and only if $p = 2, 3, 5, 7, 11$.*

Proof. By the proposition, $h_1 = 1$ if and only if $|\Gamma^{(1)}| = \frac{5760}{(p-1)(p^2+1)}$. However $|\Gamma^{(1)}| \in \mathbb{N}$ so $(p-1)(p^2+1)|5760$. Since $(n-1)(n^2+1) > 5760$ for $n \geq 19$ we must have $p \leq 17$. A quick calculation shows that the only such primes to satisfy the divisibility criterion are $p = 2, 3$.

It remains to check that for these two primes we have $|\Gamma^{(1)}| = \frac{5760}{(p-1)(p^2+1)}$. Using the explicit description of $\Gamma^{(1)}$ found in the previous subsection:

$$|\Gamma^{(1)}| = 2|\mathcal{O}^\times|^2.$$

It is then a simple calculation to show that for $p = 2, 3$ we have $|\mathcal{O}^\times| = 24, 12$ respectively. Since $\frac{5760}{(2-1)(2^2+1)} = 1152 = 2(24^2)$ and $\frac{5760}{(3-1)(3^2+1)} = 288 = 2(12^2)$ we are done.

A similar argument proves the other claim. However now we do not have a nice formula for $|\Gamma^{(2)}|$. Instead we can use Algorithm 1 to list the elements of these groups and hence get their cardinalities that way.

The primes satisfying $\frac{5760}{p^2-1} \in \mathbb{N}$ are $p = 2, 3, 5, 7, 11, 17, 19, 31$. A lengthy check (using a computer program) reveals that the only primes to satisfy $|\Gamma^{(2)}| = \frac{5760}{p^2-1}$ are $p = 2, 3, 5, 7, 11$. □

It was surprising to see for $\Gamma^{(2)}$ that although there were primes satisfying the divisibility criterion, some of them did not satisfy the equality $|\Gamma^{(2)}| = \frac{5760}{p^2-1}$. This behaviour did not happen for $\Gamma^{(1)}$ and neither did it happen when finding class numbers of quaternion algebras.

It should be noted that Ibukiyama and Hashimoto have produced formulae in [34] and [35] that give the values of h_1 and h_2 for any ramified prime. Their formulae agree with this result, especially for h_2; giving $h_2 = 1$ for $p = 2, 3, 5, 7, 11$, $h_2 = 2$ for $p = 17, 19$ and $h_2 = 3$ for $p = 31$. This supports the validity of Algorithm 1.

4.2.3 Finding the Hecke representatives

Now that we have found an algorithm to generate the elements of $\Gamma^{(2)}$ we consider the same question for the Hecke representatives for the $T_{u,q}$ operator on $A_{j,k-3}(D)$ (where $q \neq p$). In this subsection we consider $q \neq p$ to be a fixed prime.

It turns out that we have an arithmetic description of these representatives similar to the one found in Proposition 3.3.8.

Proposition 4.2.15. *Let D be a quaternion algebra over $\mathbb{Q}$ ramified at p, ∞ for some $p \in \{2, 3, 5, 7, 11\}$. Suppose $u \in GU_2(D_{\mathbb{A}_f})$ is chosen as in Definition 3.5.15. Then*

$$U_2 u U_2 = \coprod_{[x_i] \in Y_q/\Gamma^{(2)}} x_i U_2,$$

where $Y_\theta = GU_2(D)_\theta \cap g^{-1} M_2(\mathcal{O})^\times g$, as defined before Proposition 4.2.6.

Proof. Consider an arbitrary decomposition:

$$U_2 u U_2 = \coprod x_i U_2$$

for $x_i \in \mathrm{GU}_2(D_{\mathbb{A}_f})$. Note that by Proposition 3.2.12 we may take $x_i \in \mathrm{GU}_2(D)$ for all i (since the class number is 1). For the rest of the proof we embed $\mathrm{GU}_2(D) \hookrightarrow \mathrm{GU}_2(D_{\mathbb{A}_f})$ diagonally.

We show that we may take $x_i \in \mathrm{GU}_2(D) \cap g^{-1} M_2(\mathcal{O})^\times g$ with similitude $\mu(x_i) = q$.

Note that for any prime $l \neq q$ we have local double coset

$$U_{2,l} u_l U_{2,l} = U_{2,l} = \mathrm{Stab}_{\mathrm{GU}_2(D_l)}(\mathcal{O}_l^2 g_l) = \mathrm{GU}_2(D_l) \cap g_l^{-1} \mathrm{GL}_2(\mathcal{O}_l) g_l$$

Thus $x_i \in \mathrm{GU}_2(D_l) \cap g_l^{-1} M_2(\mathcal{O}_l)^\times g_l$ and $\mu(x_i) \in \mathbb{Z}_l^\times$ for all i.

Consider the local double coset at q and let $G = \mathrm{GU}_2(D_q) \cap \mathrm{GL}_2(\mathcal{O}_q)$. Fix a choice of $h_q \in \mathrm{GU}_2(D_q)$ such that $\mathcal{O}_q^2 g_q = \mathcal{O}_q^2 h_q$ (which is possible since $\mathcal{O}_q^2 g_q$ is locally equivalent to $\mathcal{O}_q^2$). Note that $h_q g_q^{-1} \in \mathrm{GL}_2(\mathcal{O}_q)$ so that $h_q = k_q g_q$ for some $k_q \in \mathrm{GL}_2(\mathcal{O}_q) \subseteq M_2(\mathcal{O}_q)^\times$.

The conjugation by h_q homomorphism gives a bijection between $U_{2,q} u_q U_{2,q}$ and $G(h_q u_q h_q^{-1})G$. If we fix an isomorphism as in Proposition 3.5.4 then the double coset $G(h_q u_q h_q^{-1})G$ is in bijection with $\mathrm{GSp}_4(\mathbb{Z}_q) M_q \mathrm{GSp}_4(\mathbb{Z}_q)$ (where $M_q = \mathrm{diag}(1,1,q,q)$).

Since by definition $h_q u_q h_q^{-1} \mapsto M_q \in \mathrm{GSp}_4(\mathbb{Q}_q) \cap M_4(\mathbb{Z}_q)$ we see that $h_q u_q h_q^{-1} \in M_2(\mathcal{O}_q)^\times$ and so $u_q \in \mathrm{GU}_2(D_q) \cap h_q^{-1} M_2(\mathcal{O}_q)^\times h_q$.

However:

$$h_q^{-1} M_2(\mathcal{O}_q)^\times h_q = g_q^{-1}(k_q^{-1} M_2(\mathcal{O}_q)^\times k_q) g_q = g_q^{-1} M_2(\mathcal{O}_q)^\times g_q,$$

thus $u_q \in \mathrm{GU}_2(D_q) \cap g_q^{-1} M_2(\mathcal{O}_q)^\times g_q$ and the same can be said about the x_i.

Also since both the conjugation and our chosen isomorphism respect similitude we find that $\mu(u_q) = \mu(M_q) = q$ and so $\mu(U_{2,q} u_q U_{2,q}) \subseteq q\mathbb{Z}_q^\times$. In particular $\mu(x_i) \in q\mathbb{Z}_q^\times$.

Globally we now see that

$$x_i \in \mathrm{GU}_2(D) \cap \prod_l \left(\mathrm{GU}_2(D_l) \cap g_l^{-1} M_2(\mathcal{O}_l)^\times g_l\right) = \mathrm{GU}_2(D) \cap g^{-1} M_2(\mathcal{O})^\times g$$

for each i. We also observe that $\mu(x_i) \in \mathbb{Z} \cap \left(q\mathbb{Z}_q^\times \prod_{l \neq q} \mathbb{Z}_l^\times\right) = \{\pm q\}$. However in our case the similitude is positive definite so that $\mu(x_i) = q$.

Thus the x_i can be taken to lie in Y_q. It is clear that each such element lies in the double coset.

It remains to see which elements of Y_q generate the same left coset. We have $x_i U_2 = x_j U_2$ if and only if $x_j^{-1} x_i \in U_2$. But also $x_i, x_j \in \mathrm{GU}_2(D)$, hence $x_j^{-1} x_i \in \mathrm{GU}_2(D) \cap U_2 = \Gamma^{(2)}$. So equivalence of left cosets is upto right multiplication by $\Gamma^{(2)}$. □

It may be remarked that the above proof is much more technical than the one provided for Eichler's correspondence. The reason we have to invoke conjugation by h_q as opposed to g_q is due to the fact that $g_q \notin \mathrm{GU}_2(D_q)$ in general. Thus when performing the conjugation by g_q we do not necessarily preserve the $\mathrm{GU}_2(D_q)$ part of $\mathrm{GU}_2(D_q) \cap g_q^{-1} M_2(\mathcal{O}_q)^\times g_q$.

In direct analogue with algebraic modular forms for $D^\times$ we have a nice formula for the degree of $T_{u,q}$, found in the work of Ihara [43].

Proposition 4.2.16. *For $q \neq p$ we have that $\deg(T_{u,q}) = (q+1)(q^2+1)$.*

Proof. As mentioned in the previous proof the number of x_i is the same as the number of representatives in the decomposition of the double coset

$$\mathrm{GSp}_4(\mathbb{Z}_q)\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&q&0\\0&0&0&q\end{pmatrix}\mathrm{GSp}_4(\mathbb{Z}_q)$$

into single cosets.

Roberts and Schmidt have computed this decomposition on p.189 of [56] and found that a set of representatives can be taken to be (for x, y, z running through a set of representatives mod q):

$$\begin{pmatrix}1&0&y&z\\0&1&x&y\\0&0&q&0\\0&0&0&q\end{pmatrix},\begin{pmatrix}1&x&0&z\\0&q&0&0\\0&0&1&-x\\0&0&0&q\end{pmatrix},\begin{pmatrix}q&0&0&0\\0&1&x&0\\0&0&q&0\\0&0&0&1\end{pmatrix},\begin{pmatrix}q&0&0&0\\0&q&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}.$$

Clearly there are $q^3+q^2+q+1=(q+1)(q^2+1)$ of these as expected. □

From this we see that whenever the prime 2 is unramified for D there will be $(2+1)(2^2+1)=15$ Hecke representatives for $T_{u,2}$ and similarly whenever the prime 3 is unramified for D there will be $(3+1)(3^2+1)=40$ Hecke representatives for $T_{u,3}$. These numbers are extremely small but clearly as q increases we are expecting a significant increase in the number of representatives.

Since we already have an algorithm to calculate the group $\Gamma^{(2)}$ and the sets Y_q for any q we are now done and can calculate Hecke representatives for U_2. However as q increases the amount of effort needed to calculate these increases dramatically (due to having to search through norm lists up to qp^2).

Let us consider now the case of finding Hecke representatives for U_1 when $p=2,3$ (so that the class number of U_1 is 1). We will see that due to the explicit nature of $\Gamma^{(1)}$ there is also an explicit description of Hecke representatives.

Employing similar arguments to Proposition 4.2.15 we get the following:

Proposition 4.2.17. *Let D be a quaternion algebra over $\mathbb{Q}$ ramified at p,∞ for some $p\in\{2,3\}$. Suppose $u\in GU_2(D_{\mathbb{A}_f})$ is chosen as in Definition 3.5.15. Then*

$$U_1uU_1=\coprod_{[x_i]\in(GU_2(D)_q\cap M_2(\mathcal{O})^\times)/\Gamma^{(1)}}x_iU_1.$$

Corollary 4.2.18. *Let $n\in\mathbb{N}$. For each $k\in\mathbb{N}$ let $X_k=\{\alpha\in\mathcal{O}\,|\,N(\alpha)=k\}$, $t_k=|X_k/\mathcal{O}^\times|$ and $x_{1,k},x_{2,k},...,x_{t_k,k}$ be a set of representatives for $X_k/\mathcal{O}^\times$. For such a choice of k define:*

$$R_k:=\left\{\begin{pmatrix}x_{i,k}&v\\w&x_{j,k}\end{pmatrix}\;\middle|\;\begin{array}{c}1\le i,j\le t_k,\quad v,w\in X_{n-k}\\x_{i,k}\overline{w}+v\overline{x_{j,k}}=0\end{array}\right\}.$$

The following matrices are representatives for $(GU_2(D)_n \cap M_2(\mathcal{O})^\times)/\Gamma^{(1)}$:

$$\bigcup_{k=m+1}^{n} R_k, \qquad \text{if } n = 2m+1 \text{ is odd}$$

$$\left(\bigcup_{k=m+1}^{n} R_k \right) \cup R'_m, \qquad \text{if } n = 2m \text{ is even.}$$

The finite subset $R'_m \subset R_m$ is to be constructed in the proof.

Proof. Let $\nu = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in M_2(\mathcal{O})^\times$. In order for $\nu \in \mathrm{GU}_2(D)_n$ to hold we must satisfy the equations:

$$N(\alpha) + N(\beta) = n$$

$$N(\gamma) + N(\delta) = n$$

$$\alpha\overline{\gamma} + \beta\overline{\delta} = 0.$$

In a similar vein to previous discussion these equations imply that $N(\alpha) = N(\delta)$ and $N(\beta) = N(\gamma)$. Note that the first equation implies that $0 \leq N(\alpha) \leq n$.

We wish to study equivalence of these matrices under right multiplication by:

$$\Gamma^{(1)} = \left\{ \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}, \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} \,\middle|\, x, y \in \mathcal{O}^\times \right\}.$$

Case 1: $N(\alpha) < N(\beta)$ or $N(\alpha) > N(\beta)$.

By equation one this is the same as $N(\alpha) < \frac{n}{2}$ or $N(\alpha) > \frac{n}{2}$.

Every ν with $N(\alpha) < \frac{n}{2}$ is equivalent to one with $N(\alpha) > \frac{n}{2}$ since for any choice of $x, y \in \mathcal{O}^\times$:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} = \begin{pmatrix} \beta y & \alpha x \\ \delta y & \gamma x \end{pmatrix}$$

and $N(\beta y) = N(\beta) = n - N(\alpha) > n - \frac{n}{2} = \frac{n}{2}$.

Thus from now on we may assume that $N(\alpha) > \frac{n}{2}$. None of these matrices can be equivalent under multiplication by the anti-diagonal matrices in $\Gamma^{(1)}$ so it remains to see which are equivalent under multiplication by diagonal matrices.

Now:

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} \alpha x & \beta y \\ \gamma x & \delta y \end{pmatrix}.$$

For a fixed value of $k := N(\alpha)$ satisfying $\frac{n}{2} < k \leq n$ we notice that we may choose $x, y \in \mathcal{O}^\times$ so that $\alpha x = x_{i,k}$ and $\delta y = x_{j,k}$ for some $1 \leq i, j \leq t_k$ (since $x_{1,k}, x_{2,k}, ..., x_{t_k,k}$ are representatives for $X_k/\mathcal{O}^\times$).

So far we have observed that each ν must be equivalent to a matrix of the form $\begin{pmatrix} x_{i,k} & v \\ w & x_{j,k} \end{pmatrix}$ for some k satisfying $\frac{n}{2} < k \leq n$.

In fact none of these matrices can be properly equivalent since if

$$\begin{pmatrix} x_{a,k} & v \\ w & x_{b,k} \end{pmatrix} \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} x_{c,m} & v' \\ w' & x_{d,m} \end{pmatrix}$$

for some $x, y \in \mathcal{O}^\times$ then immediately we observe that $x_{a,k}x = x_{c,m}$ and $x_{b,k}y = x_{d,m}$. Taking norms shows that $k = m$ and then $x_{a,k} = x_{c,m}, x_{b,k} = x_{d,m}$ (again by the fact that these are representatives for $X_k/\mathcal{O}^\times$) and $x = y = 1$ (since the unit multiplication action is faithful). Then $v = v'$ and $w = w'$ are forced.

It now remains to impose the extra conditions on such matrices so that they belong to $\mathrm{GU}_2(D)_n \cap M_2(\mathcal{O})^\times$. By the norm equations it is clear that we need $v, w \in X_{n-k}$ and by the third equation it is clear that $x_{i,k}\overline{w} + v\overline{x_{j,k}} = 0$ must be satisfied too. Thus we are done since ν is equivalent to some element of R_k for a unique choice of k satisfying $\frac{n}{2} < k \leq n$ and all such matrices are inequivalent.

Case 2: $N(\alpha) = N(\beta) = \frac{n}{2}$ (only occurs when $n = 2m$ is even).

In this case we may still use diagonal unit matrices to reduce the problem to equivalence between matrices of the form $\begin{pmatrix} x_{i,m} & v \\ w & x_{j,m} \end{pmatrix}$ where $v, w \in X_m$.

However, we may now have equivalence under the anti-diagonal matrices (since all of the entries have the same norm).

Suppose

$$\begin{pmatrix} x_{i,m} & v \\ w & x_{j,m} \end{pmatrix} \begin{pmatrix} 0 & x \\ y & 0 \end{pmatrix} = \begin{pmatrix} x_{s,m} & v' \\ w' & x_{t,m} \end{pmatrix}.$$

Then two equations we observe are

$$vy = x_{s,m}$$

$$wx = x_{t,m}.$$

Note that these equations determine $x_{s,m}$ and $x_{t,m}$ uniquely since $v, w \in X_m$, $x, y \in \mathcal{O}^\times$ and the elements $x_{1,m}, x_{2,m}, ..., x_{t_m,m}$ are a set of representatives for $X_m/\mathcal{O}^\times$.

But now x, y are uniquely determined as:

$$x = \frac{\overline{w}x_{t,m}}{m}$$

$$y = \frac{\overline{v}x_{s,m}}{m}.$$

Thus each such matrix $\begin{pmatrix} x_{i,m} & v \\ w & x_{j,m} \end{pmatrix}$ with $v, w \in X_m$ can only be equivalent to at most one other matrix:

$$\begin{pmatrix} x_{s,m} & \frac{x_{i,m}\overline{w}x_{t,m}}{m} \\ \frac{x_{j,m}\overline{v}x_{s,m}}{m} & x_{t,m} \end{pmatrix},$$

where $x_{s,m}$ and $x_{t,m}$ are uniquely determined by $v \sim x_{s,m}$ and $w \sim x_{t,m}$ under the action of right unit multiplication.

Let R'_m be a set consisting of a choice of matrix from each of these equivalence pairs (as $x_{i,m}$ and $x_{j,m}$ run through representatives for $X_m/\mathcal{O}^\times$ and v, w run through elements of X_m satisfying $x_{i,m}\overline{w} + v\overline{x}_{j,m} = 0$). Then it is now clear that R'_m is a set of representatives for this case. □

The above set of representatives may not look appealing but they can be written down explicitly (at least for n odd). Since we only really want this result for n prime this is not too much of a restriction. The $n = 2$ case turns out to be extremely explicit and will be considered in a moment.

First consider the subcase of Case 1 where the top left entries have norm $k = n - 1$. There is a simpler way to generate representatives here. Note that the top right entry will have norm $n - k = 1$ and so will be a unit. Each such matrix will be equivalent by an anti-diagonal matrix to some matrix with top left entry a unit. Then we need only search for matrices of the form:

$$\begin{pmatrix} x_{i,1} & v \\ w & x_{j,1} \end{pmatrix}$$

with $v, w \in X_{n-1}$.

However $X_1 = \mathcal{O}^\times$ and clearly we may take 1 as a representative for $\mathcal{O}^\times/\mathcal{O}^\times$. The condition $x_{i,1}\overline{w} + v\overline{x_{j,1}} = 0$ then translates into $w = -\overline{v}$.

Hence (at least when $n > 2$) we may identify:

$$R_{n-1} \longleftrightarrow \left\{ \begin{pmatrix} 1 & z \\ -\overline{z} & 1 \end{pmatrix} \middle| \, z \in X_{n-1} \right\}.$$

When $n = 2$ exactly half of these will form a set of representatives for this particular subcase. In fact it is simple to see that the equivalent pairs would be:

$$\begin{pmatrix} 1 & z \\ -\overline{z} & 1 \end{pmatrix} \sim \begin{pmatrix} 1 & -z \\ \overline{z} & 1 \end{pmatrix}$$

(since the uniquely determined values x and y are $x = -z$ and $y = \overline{z}$ here). Thus we may take (for $n = 2$):

$$R_1' = \left\{ \left(\begin{array}{cc} 1 & z_i \\ -\overline{z_i} & 1 \end{array} \right) \middle| \, [z_i] \in \mathcal{O}^\times / \{\pm 1\} \right\}.$$

Example 4.2.19. If we apply Corollary 4.2.18 to the choices:

$$D = \left(\frac{-1, -1}{\mathbb{Q}} \right)$$

$$\mathcal{O} = \mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\frac{1+i+j+k}{2}$$

$$n = 3$$

$$X_3/\mathcal{O}^\times = \{[1 \pm i \pm j]\}$$

we find that Hecke representatives for U_1 with ramified prime $p = 2$ and $q = 3$ are given by:

$$\left(\begin{array}{cc} x & 0 \\ 0 & y \end{array} \right), \qquad x, y \in \{1 \pm i \pm j\}$$

$$\left(\begin{array}{cc} 1 & z \\ -\overline{z} & 1 \end{array} \right), \qquad z \in \mathcal{O}, N(z) = 2.$$

There are 40 representatives here as expected and they agree with the explicit representatives given by Ibukiyama on p.594 of [37]. □

So far we have not actually needed the open compact subgroup U_1 but it is actually of use to us in studying U_2. Under certain local conditions it is possible to decompose Hecke operators simultaneously, so that the same Hecke representatives may be used for either.

The following is shown on p.6 of [29].

Theorem 4.2.20. *Let $G/\mathbb{Q}$ be a reductive group such that $G(\mathbb{R})$ is compact modulo center. Suppose $u \in G(\mathbb{A}_f)$ and $K, K' \subseteq G(\mathbb{A}_f)$ are open compact with the property that $K_q = K_q'$ whenever a local component satisfies $u_q \notin K_q$. Then the Hecke representatives for T_u with respect to K and K' can be taken to be the same, i.e. if*

$$KuK = \coprod_{i=1}^{r} u_i K$$

for some $u_1, u_2, ..., u_r \in G(\mathbb{A}_f)$ then

$$K'uK' = \coprod_{i=1}^{r} u_i K'$$

We observe that in our specific case the pair U_1 and U_2 have this property.

Lemma 4.2.21. *Let $u \in GU_2(D_{\mathbb{A}_f})$ be chosen to form the $T_{u,q}$ operator with respect to both U_1 and U_2 (for prime $q \neq p$). Then the Hecke representatives for $T_{u,q}$ with respect to U_1 and U_2 can be taken to be the same.*

Proof. Recall that u has identity component away from q and $u_q \notin U_{2,q}$ so the there is only one local condition to check, that $U_{2,q} = U_{1,q}$.

Now $U_2 = \mathrm{Stab}_{\mathrm{GU}_2(D_{\mathbb{A}_f})}(\mathcal{O}^2 g)$ where $g \in \mathrm{GL}_2(D)$ is chosen so that $\mathcal{O}^2 g$ is in the non-principal genus.

We know that $U_{2,q} = \mathrm{Stab}_{\mathrm{GU}_2(D_q)}(\mathcal{O}_q^2 g_q)$. However by construction we know that $\mathcal{O}_q^2 g_q$ is equivalent to $\mathcal{O}_q^2$ (since $q \neq p$). Thus there exists $h_q \in \mathrm{GU}_2(D_q)$ such that $\mathcal{O}_q^2 g_q = \mathcal{O}_q^2 h_q$.

It is then clear that:

$$\mathrm{Stab}_{\mathrm{GU}_2(D_q)}(\mathcal{O}_q^2 g_q) = \mathrm{Stab}_{\mathrm{GU}_2(D_q)}(\mathcal{O}_q^2 h_q) = \mathrm{Stab}_{\mathrm{GU}_2(D_q)}(\mathcal{O}_q^2).$$

Thus $U_{2,q} = U_{1,q}$ and so we are done. □

This result is a huge help since we have seen that it is generally easier to generate Hecke representatives for $T_{u,q}$ with respect to U_1. Of course we always have the simultaneous coset decomposition (whatever the ramified prime p is). However to guarantee rational representatives exist for both it is perhaps plausible to restrict to the case where both U_1 and U_2 have class number 1.

Corollary 4.2.22. *Let the ramified prime of D be $p \in \{2, 3\}$. Then we may use the representatives from Corollary 4.2.18 as Hecke representatives for $T_{u,q}$ with respect to U_2 (for $q \neq p$).*

Proof. Since $p \in \{2, 3\}$ we know that both the class numbers of U_1, U_2 are 1. Hence both admit rational Hecke representatives.

We also know that given Hecke representatives for $T_{u,q}$ with respect to U_1 we may use them for U_2. Thus the rational representatives from Corollary 4.2.18 can be used for U_2. □

4.2.4 Implementing the trace formula

Now that we have algorithms that generate the data needed to use the trace formula we discuss some of the finer details in its implementation, namely how I find character values. We follow a similar path to Subsection 3.4.1.

For this subsection we denote by $\chi_{j,k-3}$ the character of the representation $V_{j,k-3}$.

Given $g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GU}_2(D)$ we may produce a matrix $A \in \mathrm{GSp}_4(\mathbb{C})$ via the embedding:

$$g \longmapsto \begin{pmatrix} \alpha_1 + \alpha_2\sqrt{a} & \beta_1 + \beta_2\sqrt{a} & \alpha_3 + \alpha_4\sqrt{a} & \beta_3 + \beta_4\sqrt{a} \\ \gamma_1 + \gamma_2\sqrt{a} & \delta_1 + \delta_2\sqrt{a} & \gamma_3 + \gamma_4\sqrt{a} & \delta_3 + \delta_4\sqrt{a} \\ b(\alpha_3 - \alpha_4\sqrt{a}) & b(\beta_3 - \beta_4\sqrt{a}) & \alpha_1 - \alpha_2\sqrt{a} & \beta_1 - \beta_2\sqrt{a} \\ b(\gamma_3 - \gamma_4\sqrt{a}) & b(\delta_3 - \delta_4\sqrt{a}) & \gamma_1 - \gamma_2\sqrt{a} & \delta_1 - \delta_2\sqrt{a} \end{pmatrix}.$$

This is the composition of the standard embedding $D^\times \hookrightarrow M_2(K(\sqrt{a}))$ given in Lemma 2.1.9 and the isomorphism $\mathrm{GU}_2(M_2(K(\sqrt{a}))) \cong \mathrm{GSp}_4(K(\sqrt{a})) \subseteq \mathrm{GSp}_4(\mathbb{C})$ given in Theorem 3.5.1.

We know that the image of $\mathrm{GU}_2(\mathbb{H})_1 \cap \mathrm{GU}_2(D)$ under this embedding is a subgroup of $\mathrm{USp}(4)$, so that the matrix $B = \frac{A}{\sqrt{\mu(A)}} \in \mathrm{USp}(4)$. By writing $A = (\sqrt{\mu(A)}I)B$ it follows that:

$$\chi_{j,k-3}(g) = \chi_{j,k-3}(A) = \mu(A)^{\frac{j+2k-6}{2}}\chi_{j,k-3}(B).$$

In order to find $\chi_{j,k-3}(B)$ we first find the eigenvalues of B. This is equivalent to conjugating into the maximal torus of diagonal matrices. Since $B \in \mathrm{USp}(4)$ these eigenvalues will come in two conjugate pairs $z, \overline{z}, w, \overline{w}$ for z, w on the unit circle.

The Weyl character formula gives:

$$\chi_{j,k-3}(B) = \frac{w^{j+1}(w^{2(k-2)} - 1)(z^{2(j+k-1)} - 1) - z^{j+1}(z^{2(k-2)} - 1)(w^{2(j+k-1)} - 1)}{(z^2 - 1)(w^2 - 1)(zw - 1)(z - w)(zw)^{j+k-3}}.$$

For any of the cases $z^2 = 1, w^2 = 1, zw = 1, z = w$ one must formally expand this concise formula into a polynomial expression (not an infinite sum since each factor on the denominator except zw divides the numerator). It is easy for a computer package to compute this expansion for a given j, k.

4.2.5 Finding the trace contribution for the new subspace

In this subsection I give brief details of how one obtains the trace of the action of $T_{u,q}$ on $A^{\mathrm{new}}_{j,k-3}(D)$ from the trace of its action on $A_{j,k-3}(D)$. This is the final link in the chain, once this has been achieved it is possible to begin generating congruences.

Let $\mathrm{tr}(T_{u,q})^{\mathrm{new}}$ and $\mathrm{tr}(T_{u,q})^{\mathrm{old}}$ be the traces of the action of $T_{u,q}$ on $A^{\mathrm{new}}_{j,k-3}(D)$ and $A^{\mathrm{old}}_{j,k-3}(D)$ respectively.

It is clear that since $A_{j,k-3}(D) = A^{\mathrm{new}}_{j,k-3}(D) \oplus A^{\mathrm{old}}_{j,k-3}(D)$ we have that $\mathrm{tr}(T_{u,q})^{\mathrm{new}} = \mathrm{tr}(T_{u,q}) - \mathrm{tr}(T_{u,q})^{\mathrm{old}}$. Thus we focus on calculating $\mathrm{tr}(T_{u,q})^{\mathrm{old}}$. To

do this we return to the lifting procedure encountered in Subsection 3.5.4 and study it in more depth. Again the results here are due to Ibukiyama [41] and are provided in greater generality there.

Consider a Hecke eigenform $F = F_1 \otimes F_2$ for the group $G = D^\times \times \mathrm{GU}_2(D)$ with respect to the $T_{u,q}$ operators for $q \neq p$, as acting on both components. This is equivalent to F_1 and F_2 being Hecke eigenforms away from p in their respective spaces of algebraic modular forms.

Suppose that α_n, β_n are the Hecke eigenvalues of F_1, F_2 respectively for $p \nmid n$. Also suppose that $\theta_F \neq 0$ and that this theta series is a Hecke eigenform for all of the T_n (we will return to this assumption soon). Let γ_n be the eigenvalues of θ_F.

Ibukiyama finds a link between these three families of eigenvalues by studying the L-functions attached to F_1, F_2, θ_F.

Theorem 4.2.23. *For $q \neq p$ we have the following identity in $\mathbb{C}(t)$:*

$$\sum_{k=0}^{\infty} \beta_{q^k} t^k = \frac{1 - q^{j+2k-4}t^2}{(1 - \alpha_q q^{k-2}t + q^{j+2k-3}t^2)(1 - \gamma_q t + q^{j+2k-3}t^2)}.$$

Corollary 4.2.24. *For $q \neq p$ we have $\beta_q = \gamma_q + q^{k-2}\alpha_q$.*

Proof. This is simply a case of rearranging and then equating the t coefficients of both sides of the identity above. □

So we now return to calculating $\mathrm{tr}(T_{u,q})^{\mathrm{old}}$. The idea is as follows. First choose a basis of eigenforms in $A^{\mathrm{old}}_{j,k-3}(D)$ for the $T_{u,q}$ operators at $q \neq p$. Then $\mathrm{tr}(T_{u,q})^{\mathrm{old}}$ will be equal to the sum of the corresponding eigenvalues. However we can use the above corollary to find these eigenvalues by instead looking at the eigenvalues of the corresponding elliptic modular forms (since each old form provides some theta series that is non-zero by definition).

We will assume that the lifting procedure is bijective, i.e. that each pair (F_1, θ_F) must give rise to a unique F_2 and that all such eigenforms occur. This is conjectured to occur. Of course we are still making some assumptions about θ_F too but these assumptions are harmless by the following result of Ibukiyama.

Theorem 4.2.25.
- *$\theta_F \neq 0$ is equivalent to $\left(\frac{\partial \theta_F}{\partial q}\right)_{q=0} = 0$, i.e. the q coefficient in the q-expansion is non-zero.*
- *If either condition is satisfied then θ_F is an eigenform for all Hecke operators.*

With this in mind it is now possible to calculate the oldform trace contribution. Under the above assumptions we have the following.

Corollary 4.2.26. *Let $g_1, g_2, ..., g_m \in S_{j+2k-2}(SL_2(\mathbb{Z}))$ and $h_1, h_2, ..., h_n \in S^{new}_{j+2}(\Gamma_0(p))$ be bases of normalized eigenforms with Hecke eigenvalues a_{q,g_i} and a_{q,h_j} respectively.*

Then for $q \neq p$ and $j > 0$:

$$tr(T_{u,q})^{old} = n\left(\sum_{i=1}^{m} a_{q,g_i}\right) + mq^{k-2}\left(\sum_{j=1}^{n} a_{q,h_j}\right).$$

Proof. We know that $\mathrm{tr}(T_{u,q})^{\mathrm{old}}$ is the sum of the eigenvalues occuring in each lift of a pair (g_i, h_j). By Corollary 4.2.24 we know that each pair gives a lift with eigenvalue $a_{q,g_i} + q^{k-2}a_{q,h_j}$. Summing gives:

$$\begin{aligned}\mathrm{tr}(T_{u,q})^{\mathrm{old}} = \sum_{i=1}^{m}\sum_{j=1}^{n}(a_{q,g_i} + q^{k-2}a_{q,h_j}) &= \sum_{i=1}^{m}\left(na_{q,g_i} + q^{k-2}\left(\sum_{j=1}^{n} a_{q,h_j}\right)\right) \\ &= n\left(\sum_{i=1}^{m} a_{q,g_i}\right) + mq^{k-2}\left(\sum_{j=1}^{n} a_{q,h_j}\right)\end{aligned}$$

□

4.3 Examples and Summary

Now that the tools are set in place, calculations can be done. In this section I provide a brief discussion of the evidence that I have generated.

The following table highlights the valid choices of $D, \mathcal{O}, \lambda, \mu$ that I used for each ramified prime $p \in \{2, 3, 5, 7, 11\}$.

p	D	$\mathcal{O}$	λ	μ
2	$\left(\frac{-1,-1}{\mathbb{Q}}\right)$	$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}\left(\frac{1+i+j+k}{2}\right)$	1	$i-k$
3	$\left(\frac{-1,-3}{\mathbb{Q}}\right)$	$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\left(\frac{1+j}{2}\right) \oplus \mathbb{Z}\left(\frac{i+k}{2}\right)$	$1+i$	j
5	$\left(\frac{-2,-5}{\mathbb{Q}}\right)$	$\mathbb{Z} \oplus \mathbb{Z}\left(\frac{2-i+k}{4}\right) \oplus \mathbb{Z}\left(\frac{2+3i+k}{4}\right) \oplus \mathbb{Z}\left(\frac{-1+i+j}{2}\right)$	2	j
7	$\left(\frac{-1,-7}{\mathbb{Q}}\right)$	$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\left(\frac{1+j}{2}\right) \oplus \mathbb{Z}\left(\frac{i+k}{2}\right)$	$2 + \frac{1}{2}i - \frac{1}{2}k$	j
11	$\left(\frac{-1,-11}{\mathbb{Q}}\right)$	$\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}\left(\frac{1+j}{2}\right) \oplus \mathbb{Z}\left(\frac{i+k}{2}\right)$	$1+3i$	j

Using these choices along with the algorithms and results mentioned previously I was able to calculate the groups $\Gamma^{(1)}, \Gamma^{(2)}$ for each such p, hence generating tables of dimensions of the spaces $A^{\mathrm{new}}_{j,k-3}(D)$ (using Corollary 3.4.2 and Theorem 3.5.17). These tables are given in Appendix A.1.

From these tables I was able to isolate 1-dimensional spaces (these being the most suitable for calculation). For each possibility I then used the MAGMA command LRatio to test for large primes dividing Λ_{alg} on the elliptic side. The remaining cases were ones where I expected to find examples of Harder's congruence and so I then computed the trace of either $T_{u,2}$ or $T_{u,3}$ (depending on p).

These computations (once modified by subtracting the old subspace contribution to the trace) gave me Hecke eigenvalues of the relevant Siegel modular forms and it was then a simple matter to check that Harder's congruence did indeed work.

I should mention that the methods outlined in this thesis will work for $T_{u,q}$ for any $q \neq p$. The only reason for restriction to $T_{u,2}$ or $T_{u,3}$ was for simplicity.

Tables of the congruences observed can be found in Appendix A.2. In particular for $p = 2$ one observes congruences provided in Bergström [4].

The following table is a summary of the number of congruences found at each level:

p	New dimension 1 cases	With large prime	Congruences found
2	20	11	11
3	12	7	7
5	5	1	1
7	6	3	3
11	2	1	0

The only problem seemed to be at level $p = 11$. Here I expected to find one congruence yet the large prime dividing the normalized L-value was found to lie above 11 itself. This has never been an issue in the literature since almost all evidence has been provided at levels 1 or 2 and in this case primes lying above 2 could never be considered to be large primes.

It is for this reason that I include the condition that the large prime λ should not lie over the level p in my statement of Harder's conjecture.

We finish this chapter with some examples for $p = 3$.

Example 4.3.1. By Appendix A.1 we see that

$$\dim(A_{2,5}(D)) = \dim(A_{2,5}^{\text{new}}(D)) = \dim(S_{2,8}^{\text{new}}(K(3))) = 1.$$

Then $j = 2$ and $k = 8$ so that $j + 2k - 2 = 16$. Let $F \in S_{2,8}^{\text{new}}(K(3))$ be the unique normalized eigenform.

One easily checks that $\dim(S_{16}^{\text{new}}(\Gamma_0(3))) = 2$. This space is spanned by the

two normalized eigenforms with q-expansions:

$$f_1(\tau) = q - 234q^2 - 2187q^3 + 21988q^4 + 280710q^5 + ...$$
$$f_2(\tau) = q - 72q^2 + 2187q^3 - 27584q^4 - 221490q^5 + ...$$

Indeed MAGMA informs us that $\mathrm{ord}_{109}(\Lambda_{\mathrm{alg}}(f_1, 10)) = 1$ and so we expect a congruence of the form:

$$b_q \equiv a_q + q^9 + q^6 \bmod 109$$

for all $q \neq 3$, where b_q are the Hecke eigenvalues of F and a_q the Hecke eigenvalues of f_1. As discussed earlier we will only work with the case $q = 2$ for simplicity.

The algorithms mentioned earlier then calculate the necessary $\frac{5760}{3^2-1} = 720$ matrices belonging to $\Gamma^{(2)}$ and the $(2+1)(2^2+1) = 15$ Hecke representatives for the operator $T_{u,2}$. Applying the trace formula we find that $\mathrm{tr}(T_{u,2}) = -312$.

Now since $A_{2,5}(D) = A^{\mathrm{new}}_{2,5}(D)$ we have that $\mathrm{tr}(T_{u,2}) = \mathrm{tr}(T_{u,2})^{\mathrm{new}}$. Also the spaces are 1-dimensional and so in fact $b_2 = \mathrm{tr}(T_{u,2})^{\mathrm{new}} = -312$.

The congruence is then simple to check:

$$-312 \equiv -234 + 2^9 + 2^6 \bmod 109.$$

□

Example 4.3.2. We see an example where we must subtract off the oldform contribution from the trace. By Appendix A.1 we see that

$$\dim(A_{8,2}(D)) = 3$$

whereas

$$\dim(A^{\mathrm{new}}_{8,2}(D)) = \dim(S^{\mathrm{new}}_{8,5}(K(3))) = 1.$$

Then $j = 8$ and $k = 5$ so that $j + 2k - 2 = 16$ again. Let $F \in S^{\mathrm{new}}_{8,5}(K(3))$ be the unique normalized eigenform.

MAGMA informs us that $\mathrm{ord}_{67}(\Lambda_{\mathrm{alg}}(f_2, 13)) = 1$ and so we expect a congruence of the form:

$$b_q \equiv a_q + q^{12} + q^3 \bmod 67$$

for all $q \neq 3$.

Applying the trace formula this time gives $\mathrm{tr}(T_{u,2}) = 300$. However since $\dim(A_{8,2}(D)) > \dim(A^{\mathrm{new}}_{8,2}(D))$ there is an oldform contribution to this trace. In order to find it we need Hecke eigenvalues of normalized eigenforms for the spaces $S_{16}(SL_2(\mathbb{Z}))$ and $S^{\mathrm{new}}_{10}(\Gamma_0(3))$.

It is known that $\dim(S_{16}(SL_2(\mathbb{Z}))) = 1$ and that the unique normalized eigenform has q-expansion:

$$g(\tau) = q + 216q^2 - 3348q^3 + 13888q^4 + 52110 + ...$$

Also $\dim(S_{10}^{\text{new}}(\Gamma_0(3))) = 2$ and the normalized eigenforms have the following q-expansions:

$$h_1(\tau) = q - 36q^2 - 81q^3 + 784q^4 - 1314q^5 + ...$$
$$h_2(\tau) = q + 18q^2 + 81q^3 - 188q^4 - 1540q^5 + ...$$

Thus using Corollary 4.2.26 the oldform contribution is:

$$\begin{aligned}\text{tr}(T_{u,2})^{\text{old}} = 2a_{2,g} + 2^3(a_{2,h_1} + a_{2,h_2}) &= 512 + 8(-36 + 18) \\ &= 288\end{aligned}$$

Hence $\text{tr}(T_{u,2})^{\text{new}} = \text{tr}(T_{u,2}) - \text{tr}(T_{u,2})^{\text{old}} = 300 - 288 = 12$. Since our space of algebraic forms is 1-dimensional we must have $b_2 = \text{tr}(T_{u,2})^{\text{new}} = 12$.

The congruence is then simple to check:

$$12 \equiv -72 + 2^{12} + 2^3 \bmod 67.$$

□

Example 4.3.3. Our final example is a case where the Hecke eigenvalues of the elliptic modular form lie in a quadratic extension of $\mathbb{Q}$.

By Appendix A.1 we see that

$$\dim(A_{6,2}(D)) = \dim(A_{6,2}^{\text{new}}(D)) = \dim(S_{6,5}^{\text{new}}(K(3))) = 1.$$

Then $j = 6$ and $k = 5$ so that $j + 2k - 2 = 14$. Let $F \in S_{6,5}^{\text{new}}(K(3))$ be the unique normalized eigenform.

One easily checks that $\dim(S_{14}^{\text{new}}(\Gamma_0(3))) = 3$. This space is spanned by the three normalized newforms with q-expansions:

$$f_1(\tau) = q - 12q^2 - 729q^3 + ...$$
$$f_2(\tau) = q - (27 + 3\sqrt{1969})q^2 + 729q^3 + ...$$
$$f_3(\tau) = q - (27 - 3\sqrt{1969})q^2 + 729q^3 + ...$$

MAGMA informs us that $\text{ord}_{47}(N_{\mathbb{Q}(\sqrt{1969})/\mathbb{Q}}(\Lambda_{\text{alg}}(f_2, 11))) = 1$ and so we expect a congruence of the form:

$$b_q \equiv a_q + q^{10} + q^3 \bmod \lambda$$

for some prime ideal λ of $\mathbb{Z}\left[\frac{1+\sqrt{1969}}{2}\right]$ satisfying $\lambda \mid 47$ (note that 47 splits in this extension).

The trace formula gives $\mathrm{tr}(T_{u,2}) = 72$ and the usual arguments show that $b_2 = 72$. It is then observed that

$$N_{\mathbb{Q}(\sqrt{1969})/\mathbb{Q}}(b_2 - a_2 - 2^{10} - 2^3) = N_{\mathbb{Q}(\sqrt{1969})/\mathbb{Q}}(-933 + 3\sqrt{1969}) = 852768$$

This is divisible by 47 and so the congruence holds for $q = 2$. □

Chapter 5

Justification of the level p conjecture.

Naturally one may ask why the proposed level p analogue of Harder's conjecture (Conjecture 1.3.2) features the paramodular group $K(p)$ and not some other level p congruence subgroup, such as $\Gamma_0(p)$. In this section I will justify this choice by considering the behaviour of the Galois/automorphic representations associated to the forms f and F, given that the congruence holds.

5.1 Galois and Automorphic representations

In this section we give a survey of the main results that we require about Galois and automorphic representations. This will be brief although the reader can find more in depth discussions in [7] and [69].

5.1.1 Galois Representations

Recall that, given a field K we may constuct an algebraic closure $\overline{K}$ of K. This is an infinite Galois extension and its Galois group $\mathrm{Gal}(\overline{K}/K)$ is considered to be a topological group under the Krull topology. This topology is created by declaring the collection of subgroups $\mathrm{Gal}(\overline{K}/L)$ for finite extensions L/K to be a basis of neighbourhoods of the identity.

In fact one can show that:

$$\mathrm{Gal}(\overline{K}/K) = \varprojlim_{L/K \text{ finite}} \mathrm{Gal}(L/K),$$

making the group $\mathrm{Gal}(\overline{K}/K)$ a profinite group. The profinite topology matches the Krull topology above.

These absolute Galois groups are an object of interest in modern number theory, for reasons we shall see soon. However due to the complicated nature of these groups we instead try and study representations of Galois groups. By this we mean continuous homomorphisms:

$$\rho : \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}(V),$$

where V is a (finite dimensional) L-vector space for some field L (not necessarily K). The usual representation theoretic tools/definitions still make sense, such as reducibility, equivalence, characters etc.

Three common situations are as follows:

- $L \subseteq \mathbb{C}$. In this case ρ is an Artin representation.
- $L \subseteq \overline{\mathbb{Q}}_l$ for some prime l. In this case ρ is an l-adic representation.
- $L \subseteq \overline{\mathbb{F}}_l$ for some prime l. In this case ρ is a mod l representation.

In the first and third cases ρ necessarily has finite image (due to the topologies one takes). However, l-adic representations can have infinite image.

Suppose $L \subseteq \overline{\mathbb{Q}}_l$. Choosing a basis for V we note that the image of ρ lies in $\mathrm{GL}_n(\overline{\mathbb{Q}}_l)$. It is known that one may find an equivalent representation with image in $\mathrm{GL}_n(\overline{\mathbb{Z}}_l)$. Given such a choice it is then clear that we may compose with the reduction mod l map to produce a mod l representation $\overline{\rho}$.

There are many mod l representations attached to ρ due to the choice of integral representation. These reductions may not even be isomorphic. However, the composition factors are well defined and often, $\overline{\rho}^{ss}$ will denote the semi-simplification of any choice of mod l reduction (the representation formed by just taking the direct sum of the composition factors).

Quite often in number theory we encounter Galois representations with K a number field. Such (global) Galois groups are highly complicated but one can use local methods to study them. Given a prime $\mathfrak{q}$ of K we may choose an embedding of K into $K_{\mathfrak{q}}$. Then it is clear that $\mathrm{Gal}(\overline{K}_{\mathfrak{q}}/K_{\mathfrak{q}})$ embeds into $\mathrm{Gal}(\overline{K}/K)$ by restriction. This is not a natural embedding, it depends on the choice of embedding $K \hookrightarrow K_{\mathfrak{q}}$.

Thus it is possible to restrict global Galois representations to give a family of local ones, one for each prime of the number field. This is fruitful since the structure of the local Galois groups is much simpler than that of the global one. We investigate this in more detail for the case $K = \mathbb{Q}$, remarking that the concepts are mainly those encountered in class field theory but extended to infinite Galois groups.

Let p be a prime. Then there is a natural surjective homomorphism:

$$\Phi : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \longrightarrow \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p).$$

The kernel of this map is the inertia subgroup I_p, so that

$$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)/I_p \cong \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p).$$

Now $\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ is (topologically) generated by the Frobenius automorphism Frob_p, given by $\mathrm{Frob}_p(x) = x^p$. Thus there exists a unique coset of I_p inside $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ consisting of elements that map onto Frob_p under Φ. We call these Frobenius elements too. We will usually denote by ϕ_p such an element.

An interesting dense subgroup of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is the Weil subgroup $W_{\mathbb{Q}_p}$, consisting of all $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ such that $\Phi(\sigma) = \mathrm{Frob}_p^n$ for some $n \in \mathbb{Z}$. Explicitly, $W_{\mathbb{Q}_p} = \{\phi_p^n u \,|\, n \in \mathbb{Z}, u \in I_p\}$ (for any choice of lift ϕ_p).

We say that a local Galois representation $\rho : \mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{GL}(V)$ is unramified if $\rho(I_p) = \{\mathrm{id}\}$, i.e. I_p acts trivially on V. In this case ρ is completely determined by $\rho(\phi_p)$ and this is independent of the choice of lift ϕ_p of Frobenius. For ramified representations this is not true but the trace and determinant of this matrix is independent of lift.

Returning to global Galois representations of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ one may ask a similar question. Are such representations completely determined by their image of all (lifts of) Frobenius elements? One can view this as a "local-global" principle for Galois representations. Indeed the answer is yes by a famous theorem of Cebotarev (stated in modern language):

Theorem 5.1.1. *(Cebotarev density theorem) The (lifts of) Frobenius elements are dense in the absolute Galois group Gal*$(\overline{\mathbb{Q}}/\mathbb{Q})$.

In fact the result is still true if one discards finitely many Frobenius elements. So a Galois representation is completely determined by the image of a lift of Frobenius at all but finitely many primes.

Another interesting theorem lets us determine equivalence of certain Galois representations by their character values.

Theorem 5.1.2. *(Brauer-Nesbitt) Let ρ_1, ρ_2 be semisimple n-dimensional Galois representations over a field L of characteristic 0 or $l > n$. Then $\rho_1 \sim \rho_2$ if and only if $tr(\rho_1) = tr(\rho_2)$.*

The case $l \leq n$ is also tackled in the Brauer-Nesbitt theorem but will not be important to us.

We will see a few brief examples of Galois representations. These will all be over $\mathbb{Q}$ for simplicity but can be extended to other settings. More details can be found in Wiese's notes [69].

Cyclotomic characters

Let l be prime and $n \geq 1$. Consider the group μ_{l^n} of l^n roots of unity in $\overline{\mathbb{Q}}$. Note that $\mu_{l^n} \cong \mathbb{Z}/l^n\mathbb{Z}$. For a fixed l these groups form a projective system with respect to the lth power map. We can thus take the inverse limit:

$$\mu_{l^\infty} = \varprojlim_n \mu_{l^n} \cong \mathbb{Z}_l.$$

The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts by homomorphisms on each group μ_{l^n} and the actions are compatible with the lth power map. Hence $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on μ_{l^∞}, giving an l-adic representation:

$$\chi_l : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_1(\mathbb{Z}_l) = \mathbb{Z}_l^\times.$$

This 1-dimensional Galois representation is called the l-adic cyclotomic character. It is unramified at all primes $p \neq l$ and satisfies $\chi_l(\phi_p) = p$ for all such primes.

The mod l reduction $\overline{\chi}_l$ is a 1-dimensional mod l Galois representation and matches the action above restricted to μ_l.

Galois representations of elliptic curves

Take an elliptic curve E defined over $\mathbb{Q}$ (for simplicity). Then the set $E(\overline{\mathbb{Q}})$ of $\overline{\mathbb{Q}}$-valued points on the curve forms an abelian group . For each prime l and each $n \geq 1$ one can consider the torsion subgroups $E(\overline{\mathbb{Q}})[l^n]$. It is known that $E(\overline{\mathbb{Q}})[l^n] \cong \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$.

Note that for a fixed l the finite groups $E(\overline{\mathbb{Q}})[l^n]$ form a projective system with respect to the multiplication by l map. Thus it is possible to take the inverse limit:

$$T_l(E) = \varprojlim_n E(\overline{\mathbb{Q}})[l^n] \cong \mathbb{Z}_l \times \mathbb{Z}_l.$$

This is the Tate module of E (to be compared with the 1-dimensional μ_{l^∞} constructed above).

The Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts linearly on each of the groups $E(\overline{\mathbb{Q}})[l^n]$ and this action is compatible with the multiplication by l map. Hence $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on $T_l(E)$, giving an l-adic representation:

$$\rho_{E,l} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{Z}_l).$$

Much is known about these representations, in particular they are unramified at primes of good reduction not dividing l. At such primes $\mathrm{tr}(\rho_{E,l}(\phi_p)) = a_p = p + 1 - |E(\mathbb{F}_p)|$, numbers of significance in the theory of elliptic curves. Also $\det(\rho_{E,l}(\phi_p)) = p$ (in fact $\det(\rho_{E,l}) = \chi_l$).

One can also construct mod l Galois representations attached to E by considering just the Galois action on $E(\overline{\mathbb{Q}})[l]$. These representations are compatible with the ones above by reduction.

Galois representations attached to modular forms

One can attach Galois representations to modular forms. However this process is not as easy as the above examples. Essentially (for weight 2) one follows in the same vein but by considering the action of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the l-adic "Tate module" associated to the Jacobian of the corresponding modular curve. We will not need the details but one can see Wiese's notes [69].

Let $f \in S_k(\Gamma_0(N))$ be a normalized eigenform with Hecke eigenvalues a_q $(q \nmid N)$. Then it is known that there exists a 2-dimensional l-adic Galois representation attached to f:

$$\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{Q}}_l)$$

such that:

- ρ_f is irreducible,
- ρ_f takes values in $\mathbb{Q}_f \hookrightarrow \overline{\mathbb{Q}_l}$,
- ρ_f is odd (i.e. $\det(\rho_f(c)) = -1$ for any complex conjugation $c \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$),
- ρ_f is unramified at all primes $p \nmid Nl$. For such primes we have $\det(\rho_f(\phi_p)) = p^{k-1}$ and $\mathrm{tr}(\rho_f(\phi_p)) = a_p$.

The construction of these Galois representations is due to Shimura for weight 2 and Deligne for all other weights.

Note how the Hecke eigenvalues are encoded in the trace of Frobenius in analogue with elliptic curves. The famous modularity theorem can be viewed as giving certain equivalences of Galois representations attached to rational elliptic curves and weight 2 modular forms. One can observe many similarities in the theorems stated above (for example by comparing the primes at which the representations are unramified the level of the modular form matches the conductor of the elliptic curve).

One can conjugate and reduce ρ_f to get a semisimple mod l representation

$$\overline{\rho}_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_l)$$

such that:

- $\overline{\rho}_f$ is odd,

- $\overline{\rho}_f$ is unramified at all primes $p \nmid Nl$. For such primes $\det(\overline{\rho}(\phi_p)) \equiv p^{k-1} \bmod \Lambda$ and $\mathrm{tr}(\overline{\rho}_f(\phi_p)) \equiv a_p \bmod \Lambda$, where Λ is a prime of $\mathbb{Q}_f$ lying above l.

For each prime q let $\overline{\rho}_{f,q}$ be the restriction of $\overline{\rho}_f$ to $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$. The above tells us lots about $\overline{\rho}_{f,q}$ for $q \nmid Nl$ but also much is known about $\overline{\rho}_{f,l}$. The following theorems are found in [23]:

Theorem 5.1.3. *(Deligne) Let $f \in S_k(\Gamma_0(N))$ be an eigenform for all Hecke operators $q \nmid N$ with eigenvalues a_q. Let l be a prime satisfying $2 \leq k \leq l+1$ and $a_l \not\equiv 0 \bmod l$. Then $\overline{\rho}_{f,l}$ is reducible and*

$$\overline{\rho}_{f,l} \sim \begin{pmatrix} \overline{\chi}_l^{k-1}\overline{\lambda}_{a_l^{-1}} & \star \\ 0 & \overline{\lambda}_{a_l} \end{pmatrix},$$

where λ_a is the unramified character $Gal(\overline{\mathbb{Q}}_l/\mathbb{Q}_l) \longrightarrow \overline{\mathbb{Z}}_l^{\times}$ such that $\lambda_a(\phi_l) = a$.

Theorem 5.1.4. *(Fontaine) Suppose that f and l are as above but that $a_l \equiv 0 \bmod l$. Then $\overline{\rho}_{f,l}$ is irreducible.*

In fact more is said in Fontaine's theorem. It is known that the restriction to I_p is completely reducible and splits into two special "fundamental characters" of level 2.

Naturally one asks about the structure of $\overline{\rho}_{f,p}$ for $p|N$. The following theorem can be found on p.309 of [36].

Theorem 5.1.5. *(Langlands-Carayol) Let $f \in S_k(\Gamma_0(N))$ be a Hecke eigenform for all Hecke operators $q \nmid N$ with eigenvalues a_q. Suppose p is a prime such that $ord_p(N) = 1$. Then:*

$$\overline{\rho}_{f,p} \sim \begin{pmatrix} \overline{\chi}_l\overline{\lambda}_a & \star \\ 0 & \overline{\lambda}_a \end{pmatrix}$$

for some fixed a (where λ_a is the unramified character $Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \longrightarrow \overline{\mathbb{Z}}_l^{\times}$ such that $\lambda_a(\phi_p) = a$).

Again more is known. The value of a is predicted to be the Hecke eigenvalue of the U_p operator on f.

Without going into any detail we note that there is a similar construction for Siegel modular forms due to Taylor, Laumon and Weissauer [68] (if $j \geq 0$ and $k \geq 2$). Each eigenform $F \in S_{j,k}(K(p))$ has an attached 4-dimensional Galois representation

$$\rho_F : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_4(\overline{\mathbb{Q}}_l)$$

with desirable properties (i.e. irreducible, unramified away from the level and l, the trace of Frobenius is the Hecke eigenvalue, $\overline{\rho}_F$ semisimple etc). Also there is a residual representation $\overline{\rho}_F$ with the usual properties.

5.1.2 Automorphic representations

We observed at the beginning of Chapter 3 a method for converting modular forms into a more general type of function called an automorphic form. These exist for any reductive group G and are functions $G(\mathbb{A}) \longrightarrow \mathbb{C}$ with certain nice transformation laws and analytic properties. In particular elliptic modular forms gave automorphic forms for $G = \mathrm{GL}_2$ and Siegel modular forms of genus g gave automorphic forms for $G = \mathrm{GSp}_{2g}$.

In order to fully study automorphic forms we use representation theoretic tools. Note that $G(\mathbb{A})$ acts on functions $f : G(\mathbb{A}) \longrightarrow \mathbb{C}$ by the right regular representation $(g \cdot f)(x) = f(xg)$. In this manner we may consider spaces of automorphic forms as representations of $G(\mathbb{A})$ and refer to irreducible subspaces of this as automorphic representations of G.

The center $Z(\mathbb{A}) \subseteq G(\mathbb{A})$ will act on these spaces by a character $\omega : \mathbb{Q}^\times \backslash \mathbb{A}^\times \to \mathbb{C}^\times$. This is called the central character ω. For automorphic representations attached to classical modular forms (without character) the central character is trivial.

It is known that each automorphic representation π has a "factorisation" $\pi = \otimes'_{p \leq \infty} \pi_p$ where π_∞ is a certain representation of the Lie group $G(\mathbb{R})$ and for finite p the local representation π_p is of $G(\mathbb{Q}_p)$. This is a restricted tensor product of local representations, meaning that all but finitely of the representations π_p are unramified (i.e. contains a vector fixed by the subgroup $G(\mathbb{Z}_p)$).

For $G = \mathrm{GL}_2$ and GSp_4 it is even known that the subspace of each unramified π_p fixed by $G(\mathbb{Z}_p)$ is 1-dimensional (which fits with the fact that fixed vectors should correspond to automorphic forms).

Let us turn to more general notions in the representation theory of G over local fields. We know that $G(\mathbb{R})$ is a Lie group and its representations are well understood (also are not important to us in this thesis). Consider the group $G(\mathbb{Q}_p)$. A representation (space) V of $G(\mathbb{Q}_p)$ is said to be smooth if for each $v \in V$ there exists an open compact subgroup K such that $v \in V^K$ (i.e. v is a fixed vector under the action of K). We say that V is admissible if further V^K is finite dimensional for every open compact subgroup K of G.

One popular way to create admissible representations for a reductive group G is via the process of parabolic induction. The idea is to take a parabolic subgroup P and use the Levi decomposition $P = MN$ where M is a Levi subgroup and N is a unipotent subgroup. Then one takes a representation of M, extends it to P by letting N act trivially and induces the result to G. We will see concrete examples of this in the cases GL_2 and GSp_4.

GL_2

For GL_2 the only parabolic subgroup (up to conjugation) is the Borel sub-

group

$$B = \left\{ \begin{pmatrix} a & c \\ 0 & b \end{pmatrix} \middle| a, b \in F^\times, c \in F \right\},$$

consisting of upper triangular matrices. In this case the Levi subgroup turns out to be the maximal torus

$$M = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \middle| a, b \in F^\times \right\}$$

and the unipotent subgroup is

$$N = \left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \middle| c \in F \right\}.$$

We work over $\mathbb{Q}_p$ for some prime p. Then taking two characters χ_1, χ_2 of $\mathbb{Q}_p^\times$ we may define a character χ of M via

$$\chi \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} = \chi_1(a)\chi_2(b).$$

Then we may induce this character to B to make an admissible representation $V(\chi_1, \chi_2)$. This space may be realised as a space of smooth functions $f : \mathrm{GL}_2(\mathbb{Q}_p) \to \mathbb{C}$ such that $f\left(\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} g \right) = \chi_1(a)\chi_2(b) \left|\frac{a}{b}\right|_p^{\frac{1}{2}} f(g)$ with action of $\mathrm{GL}_2(\mathbb{Q}_p)$ given by right translation, i.e. $(g \cdot f)(x) = f(xg)$ (the right regular representation). The extra $\left|\frac{a}{b}\right|_p^{\frac{1}{2}}$ is just a normalization factor and is not important.

Much is known about these induced representations:

- If $\chi_1\chi_2^{-1} \neq |\cdot|_p^{\pm 1}$ then $V(\chi_1, \chi_2)$ is irreducible and has $\mathrm{GL}_2(\mathbb{Z}_p)$-fixed vectors. These are called principal series representations.
- If $\chi_1\chi_2^{-1} = |\cdot|_p^{\pm 1}$ then $V(\chi_1, \chi_2)$ is reducible but breaks up into a 1-dimensional piece and an infinite dimensional irreducible piece (which is a twist of the Steinberg representation). The Steinberg representation and its twists do not contain $\mathrm{GL}_2(\mathbb{Z}_p)$-fixed vectors but do contain vectors fixed by the subgroup of matrices of the form $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}_p)$ with $\gamma \in p\mathbb{Z}_p$ (i.e. the local analogue of $\Gamma_0(p)$).

There are clear equivalences $V(\chi_1, \chi_2) \cong V(\chi_2, \chi_1)$. In fact these are the only equivalences between induced representations. Also the central character of $V(\chi_1, \chi_2)$ is given by $\chi_1\chi_2$.

These induced representations form a large part of the classification of all irreducible admissible representations of $\mathrm{GL}_2(\mathbb{Q}_p)$. The only other such representations are characters $\chi \circ \det$ and supercuspidal representations (these are not induced from characters).

Let $f \in S_k^{\mathrm{new}}(\Gamma_0(p))$. Then we have an automorphic representation $\pi_f = \otimes_{q \leq \infty} \pi_{f,q}$ attached to f. Naturally one asks what the local representations are at each place. It is known that:

- $\pi_{f,\infty}$ is an infinite dimensional discrete series representation of weight k (p.146 − 147 of [7]).
- For $q \neq p$ we have $\pi_{f,q} \cong V(\chi, \chi^{-1})$ for some unramified character χ of $\mathbb{Q}_q^\times$ such that $\chi^2 \neq |\cdot|_p^{\pm 1}$. We are forced to have $\chi_1 = \chi_2^{-1} = \chi$ since the central character has to be trivial. For modular forms with character this condition will change.
- $\pi_{f,p}$ is either the Steinberg representation or its twist by the unique unramified quadratic character of $\mathbb{Q}_p^\times$ (again since the central character is trivial).

$\mathbf{GSp}_4$

For GSp_4 there are three parabolic subgroups (up to conjugation):

- The Borel subgroup B, consisting of upper triangular matrices

$$B = \left\{ \begin{pmatrix} \star & \star & \star & \star \\ 0 & \star & \star & \star \\ 0 & 0 & \star & \star \\ 0 & 0 & 0 & \star \end{pmatrix} \right\} \cap \mathrm{GSp}_4(F).$$

  The Levi subgroup is

$$M_B = \left\{ \left. \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & \frac{c}{a} & 0 \\ 0 & 0 & 0 & \frac{c}{b} \end{pmatrix} \right| a, b, c \in F^\times \right\}.$$

  Again this is just the maximal torus, with c standing for the similitude.

- The Klingen parabolic

$$Q = \left\{ \begin{pmatrix} \star & 0 & \star & \star \\ \star & \star & \star & \star \\ \star & 0 & \star & \star \\ 0 & 0 & 0 & \star \end{pmatrix} \right\} \cap \mathrm{GSp}_4(F).$$

The Levi subgroup is

$$M_Q = \left\{ \left(\begin{array}{cccc} a & 0 & b & 0 \\ 0 & t & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & \frac{\Delta}{t} \end{array} \right) \middle| a,b,c,d \in K, t \in F^\times, \Delta = ad - bc \in F^\times \right\}.$$

The similitude here is given by the determinant Δ.

- The Siegel parabolic

$$P = \left\{ \left(\begin{array}{cccc} \star & \star & \star & \star \\ \star & \star & \star & \star \\ 0 & 0 & \star & \star \\ 0 & 0 & \star & \star \end{array} \right) \right\} \cap \mathrm{GSp}_4(F).$$

The Levi subgroup is

$$M_P = \left\{ \left(\begin{array}{cccc} a & b & 0 & 0 \\ c & d & 0 & 0 \\ 0 & 0 & \frac{\lambda d}{\Delta} & -\frac{\lambda c}{\Delta} \\ 0 & 0 & -\frac{\lambda b}{\Delta} & \frac{\lambda a}{\Delta} \end{array} \right) \middle| a,b,c,d \in F, \lambda \in F^\times, \Delta = ad - bc \in F^\times \right\}.$$

This can be written in block form as

$$M_P = \left\{ \left(\begin{array}{cc} A & 0 \\ 0 & \lambda A' \end{array} \right) \middle| A \in \mathrm{GL}_2(F), \lambda \in F^\times \right\},$$

where λ stands for the similitude and $A' = (A^T)^{-1}$.

Let χ_1, χ_2, σ be unramified characters of $F^\times$ and let π be an admissible representation of $\mathrm{GL}_2(F)$. Parabolic induction for each is described by defining characters on the Levi subgroups as follows:

$$\chi_B \left(\left(\begin{array}{cccc} a & 0 & 0 & 0 \\ 0 & b & 0 & 0 \\ 0 & 0 & \frac{c}{a} & 0 \\ 0 & 0 & 0 & \frac{c}{b} \end{array} \right) \right) = \chi_1(a)\chi_2(b)\sigma(c)$$

$$\chi_Q \left(\begin{array}{cccc} a & 0 & b & 0 \\ 0 & t & 0 & 0 \\ c & 0 & d & 0 \\ 0 & 0 & 0 & \frac{\Delta}{t} \end{array} \right) = \sigma(t)\pi \left(\left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \right)$$

$$\chi_P \left(\left(\begin{array}{cc} A & 0 \\ 0 & \lambda A' \end{array} \right) \right) = \sigma(\lambda)\pi(A)$$

The corresponding inductions are denoted as $\chi_1 \times \chi_2 \rtimes \sigma, \pi \rtimes \sigma$ and $\sigma \rtimes \pi$ respectively. It will not be important to have explicit realisations of the spaces

of functions formed by these inductions. However one can find these descriptions in [56].

In a similar nature to GL_2 there is a well known classification of all non-supercuspidal irreducible admissible representations of $\mathrm{GSp}_4(\mathbb{Q}_p)$, due to Sally and Tadic. There are many more possibilities for GSp_4 than GL_2 (see the table in Appendix A.1).

5.2 Why paramodular?

As mentioned at the start of this chapter we wish to justify the use of paramodular forms in the statement of Conjecture 1.3.2. We are now in a position to do this. It should be noted that, unless otherwise stated, all results and arguments in this section and the next are the author's.

Throughout this section we will fix the following notation:

- F will be a genus 2 Siegel modular form of weight (j,k) for some congruence subgroup. This will be a Hecke eigenform. Attached to F is an automorphic representation $\pi_F = \otimes_{q\leq\infty}\pi_{F,q}$ of GSp_4 (see [2]). We will assume that π_F is unramified away from a single prime p.
- $f \in S^{\mathrm{new}}_{j+2k-2}(\Gamma_0(p))$. Attached to f is an automorphic representation $\pi_f = \otimes_{q\leq\infty}\pi_{f,q}$ of GL_2.
- $K = \mathbb{Q}_f\mathbb{Q}_F$ is the compositum of coefficient fields of f and F.
- Λ will be a "large prime" of K as in the statement of Harder's conjecture (the modulus of the congruence). Associated to this will be a completion K_Λ, valuation ring $\mathcal{O}_\Lambda$ and residue field $\mathbb{F}_\Lambda$ (which by assumption is of characteristic $l > j+2k-2 > 4$ for some prime $l \neq p$).
- ρ_f is the 2-dimensional Λ-adic Galois representation associated to f (realised over $\mathcal{O}_\Lambda$). The mod Λ semisimple reduction of this is $\overline{\rho}_F$. Also for each prime q we have the restriction $\rho_{f,q}$ to $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$.
- ρ_F is the 4-dimensional Λ-adic Galois representation associated to F (also realised over $\mathcal{O}_\Lambda$). Again we have a mod Λ semisimple reduction $\overline{\rho}_F$ and restrictions $\rho_{F,q}$ to $\mathrm{Gal}(\overline{\mathbb{Q}}_q/\mathbb{Q}_q)$.

We will assume in advance that the pair of forms (f,F) satisfy the congruence given in Conjecture 1.3.2.

The eventual aim is to prove that, given the above assumptions, $\pi_{F,p}$ is likely to contain new $K(p)$-fixed vectors. Hence F can be taken to be a new paramodular form of level p. In fact we will try and prove something stronger,

that $\pi_{F,p}$ is likely to be of type II_a in Roberts and Schmidt's tables. This will be done in three stages:

1. We will show that $\pi_{F,p}$ is parabolically induced from the Borel subgroup of $\mathrm{GSp}_4(\mathbb{Q}_p)$. This will mean that $\pi_{F,p}$ is of type I-VI in Schmidt's tables.
2. We will then show that $\pi_{F,p}$ is of type I or II unless p has certain orders mod Λ. We will do this by comparing L-parameters mod Λ of automorphic representations coming from the congruence.
3. Since type II representations fall into two categories it remains to show that $\pi_{F,p}$ is rarely of types I or II_b. We will do this by directly studying the Galois representations mentioned above.

We will approach these in reverse order since the arguments flow more naturally this way.

5.2.1 From types I and II to type II_a

First we translate the congruence into a result about Galois representations.

Lemma 5.2.1.
$$\overline{\rho}_F^{ss} \sim \overline{\rho}_f \oplus \overline{\chi}_l^{k-2} \oplus \overline{\chi}_l^{j+k-1},$$
where χ_l is the l-adic cyclotomic character.

Proof. For each $q \neq p$ we have the congruence:
$$b_q \equiv a_q + q^{k-2} + q^{j+k-1} \bmod \Lambda.$$
Note that in terms of Λ-adic representations this gives:
$$\mathrm{tr}(\rho_F(\phi_q)) \equiv \mathrm{tr}((\rho_f \oplus \chi_l^{k-2} \oplus \chi_l^{j+k-1})(\phi_q)) \bmod \Lambda$$
for all $q \neq p, l$.

Residually this means that $\mathrm{tr}(\overline{\rho}_F(\phi_q)) = \mathrm{tr}((\overline{\rho_f} \oplus \overline{\chi}_l^{k-2} \oplus \overline{\chi}_l^{j+k-1})(\phi_q))$ for all $q \neq p, l$.

By the Cebotarev density theorem we now deduce that
$$\mathrm{tr}(\overline{\rho}_F) = \mathrm{tr}(\overline{\rho}_f \oplus \overline{\chi}_l^{k-2} \oplus \overline{\chi}_l^{j+k-1}).$$
Then since l is a "large" prime we have $l > 4$ and the result follows by the Brauer-Nesbitt theorem. □

Note that we really do only know this up to semi-simplification since the trace doesn't detect off diagonal elements.

It will be handy to know when $\bar{\rho}_f$ is irreducible. Fortunately there is an easy condition which forces this.

Lemma 5.2.2. *Let $k' = j + 2k - 2$ (the weight of f). If $\overline{\rho}_f$ is reducible then $ord_\Lambda\left(\frac{B_{k'}(p^{k'}-1)}{2k'}\right) > 0$, where $B_{k'}$ is the k'-th Bernoulli number.*

Proof. Suppose $\overline{\rho}_f$ is reducible. Then after a suitable choice of basis:

$$\overline{\rho}_f = \begin{pmatrix} \alpha & \star \\ 0 & \beta \end{pmatrix},$$

where α, β are two characters $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\Lambda^\times$. Notice that the image of these characters is abelian.

Now it is known that $\overline{\rho}_f$ is unramified at all primes $q \nmid pl$ and so α and β must be unramified at the same primes. This forces $\alpha = \overline{\chi}_l^m \epsilon_1$ and $\beta = \overline{\chi}_l^n \epsilon_2$ where ϵ_1, ϵ_2 are unramified outside p.

To see this take an arbitrary character $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathbb{F}_\Lambda^\times$ unramified at all $q \nmid pl$. Note that by global class field theory α and β factor through $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty}, \mu_{l^\infty})/\mathbb{Q})$ (where μ_{p^∞} denotes the set of pth power roots of unity, similarly for l). The field $\mathbb{Q}(\mu_{p^\infty}, \mu_{l^\infty})$ is the maximal abelian extension of $\mathbb{Q}$ unramified outside pl.

We find that $\mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty}, \mu_{l^\infty})/\mathbb{Q}) \cong \mathrm{Gal}(\mathbb{Q}(\mu_{p^\infty})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\mu_{l^\infty})/\mathbb{Q})$ since p and l are coprime. Hence $\chi = \delta\epsilon$ where δ is unramified outside of l and ϵ is unramified outside of p.

To prove the claim that δ is a power of $\overline{\chi}_l$ note that $\mathrm{Gal}(\mathbb{Q}(\mu_{l^\infty})/\mathbb{Q}) \cong \mathbb{Z}_l^\times \cong (\mathbb{Z}/(l-1)\mathbb{Z}) \times \mathbb{Z}_l$ (using the fact that $l > 2$). By continuity of Galois representations we know that δ has to be trivial on $l^t\mathbb{Z}_l$ for some $t \geq 0$ and so δ induces a representation of $(\mathbb{Z}/(l-1)\mathbb{Z}) \times (\mathbb{Z}/l^t\mathbb{Z})$. But since l is coprime to $|\mathbb{F}_\Lambda^\times| = N(\Lambda) - 1$ the image of the second component must be trivial. The characters of $(\mathbb{Z}/(l-1)\mathbb{Z}) \cong (\mathbb{Z}/l\mathbb{Z})^\times$ are exactly the powers of $\overline{\chi}_l$. Thus $\chi = \overline{\chi}_l^s \epsilon$ for some integer s.

Continuing we now see that since $\det(\overline{\rho}_f(\phi_q)) \equiv q^{k'-1} \bmod \Lambda$ for all $q \nmid pl$ it must be that $\epsilon_2 = \epsilon_1^{-1}$.

Thus:

$$\overline{\rho}_f = \begin{pmatrix} \overline{\chi}_l^m \epsilon & \star \\ 0 & \overline{\chi}_l^n \epsilon^{-1} \end{pmatrix}.$$

A comparison of Artin conductors (p.39 of [69]) shows that ϵ is trivial. Indeed

the Artin conductor of $\overline{\rho}_f$ is known to be p whereas if ϵ is non-trivial then the Artin conductor would be at least $p^2 > p$.

Now since l is "large" we have $2 \leq k' \leq l+1$. Also it must be the case that $a_l \not\equiv 0 \bmod \Lambda$ (otherwise $\overline{\rho}_{f,l}$ is irreducible by Fontaine, contradicting the global reducibility of $\overline{\rho}_f$).

Thus by Deligne's theorem $\overline{\rho}_{f,l}$ must possess an unramified composition factor, hence one of $\overline{\chi}_l^m, \overline{\chi}_l^n$ must be unramified at l. Since all non-trivial powers of $\overline{\chi}_l$ are ramified at l this means one of the composition factors is trivial. It is then clear that the other composition factor must be $\overline{\chi}_l^{k'-1}$.

Hence:

$$\overline{\rho}_f = \begin{pmatrix} 1 & \star \\ 0 & \overline{\chi}_l^{k'-1} \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \overline{\chi}_l^{k'-1} & \star \\ 0 & 1 \end{pmatrix}.$$

In either case comparing traces gives for all primes $q \neq p, l$ the Ramanujan style congruence:

$$a_q \equiv 1 + q^{k'-1} \bmod \Lambda.$$

By Proposition 4.2 of [20] it must then be that $\mathrm{ord}_\Lambda\left(\frac{B_{k'}(p^{k'}-1)}{2k'}\right) > 0$. □

Proposition 5.2.3. *Suppose $\pi_{F,p}$ is of type I or II and that $ord_\Lambda\left(\frac{B_{k'}(p^{k'}-1)}{2k'}\right) = 0$. Then either $\pi_{F,p}$ is of type II_a or there exists a level one normalized newform $g \in S_{k'}(SL_2(\mathbb{Z}))$ that satisfies Harder's congruence with F.*

Proof. We know that $\overline{\rho}_f$ is irreducible by the previous result. However by Theorem 5.1.5 we have, under a suitable choice of basis:

$$\overline{\rho}_{f,p} = \begin{pmatrix} \overline{\lambda}_a & \star \\ 0 & \overline{\chi}_l\overline{\lambda}_a \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} \overline{\chi}_l\overline{\lambda}_a & \star \\ 0 & \overline{\lambda}_a \end{pmatrix}.$$

In either case the restriction of $\overline{\rho}_{f,p}$ to the inertia subgroup I_p of $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)$ is as follows:

$$\overline{\rho}_{f,p}|_{I_p} = \begin{pmatrix} 1 & \star' \\ 0 & 1 \end{pmatrix}.$$

We have two cases. First it could be the case that $\star' \equiv 0 \bmod \Lambda$. If this is the case then we may use Ribet's level lowering theorem for modular representations (Theorem 1.1 in [54]) to produce $g \in S_{k'}(\mathrm{SL}_2(\mathbb{Z}))$ such that $\overline{\rho}_g \sim \overline{\rho}_f$. We would then observe a level one version of Harder's congruence as required.

Now suppose that $\star' \not\equiv 0 \bmod \Lambda$. Then $\overline{\rho}_{f,p}$ is ramified (since the restriction to I_p is non-trivial). But if $\pi_{F,p}$ is of type I or II_b then $\pi_{F,p}$ is unramified (it contains $\mathrm{GSp}_4(\mathbb{Z}_p)$ fixed vectors). By the Local Langlands Correspondence for

GSp_4 (which has been proved in [26]) we would have that $\rho_{F,p}$ is unramified so that $\overline{\rho}_{F,p}$ is unramified, giving a contradiction. The only other possibility for $\pi_{F,p}$ is to be of type II_a as required. □

Note the intuition here. Given $\pi_{F,p}$ is of type I or II then either:

- f itself satisfies a simpler Ramanujan congruence (detected by a simple divisibility criterion),
- a replacement level 1 elliptic form satisfies Harder's congruence with F (which could be level 1 since we only assumed π_F is unramified outside of p),
- or $\pi_{F,p}$ is of type II_a (so gives rise to the fact that a form satisfying the congruence can be found in $S_{j,k}^{\mathrm{new}}(K(p))$).

The first two of these are rare occurrences and are easy to check for in practice (especially the first). We will see in Section 5.3 that the second possibility rarely occurs for paramodular F (so was unobserved in my previous calculations). Also testing for F of level 1 can be done (this is the classical Harder conjecture).

5.2.2 From I-VI to I or II

Let us now assume that $\pi_{F,p}$ is induced from the Borel subgroup of $\mathrm{GSp}_4(\mathbb{Q}_p)$. Then $\pi_{F,p}$ must be of type I-VI in Schmidt's tables. It is our aim in this subsection to prove that $\pi_{F,p}$ is likely to be of type I or II.

Let $W'_{\mathbb{Q}_p} = \mathbb{C} \rtimes W_{\mathbb{Q}_p}$ be the Weil-Deligne group of $\mathbb{Q}_p$. The multiplication on this group is given by $(z, w)(z', w') = (z + \nu(w)z', ww')$, where $\nu : W_{\mathbb{Q}_p} \longrightarrow \mathbb{C}^\times$ is the character corresponding to $|\cdot|_p$ by local class field theory.

By the Local Langlands Correspondence for GSp_4 we may associate to each irreducible admissible representation of $\mathrm{GSp}_4(\mathbb{Q}_p)$ a certain representation:

$$W'_{\mathbb{Q}_p} \longrightarrow \mathrm{GSp}_4(\mathbb{C})$$

called an L-parameter. Omitting the rigorous definition one can view them as pairs (ρ_0, N) where:

$$\rho_0 : W_{\mathbb{Q}_p} \longrightarrow \mathrm{GSp}_4(\mathbb{C})$$

is a continuous homomorphism and $N \in M_n(\mathbb{C})$ is a nilpotent matrix such that:

$$\rho_0(w) N \rho_0(w)^{-1} = \nu(w) N,$$

for all $w \in W_{\mathbb{Q}_p}$. The corresponding representation of $W'_{\mathbb{Q}_p}$ is then given by:

$$(z, w) \longmapsto \rho_0(w)\exp(zN).$$

As a brief remark it should be noted that under the Local Langlands Correspondence, irreducible admissible representations of $\mathrm{GSp}_4(\mathbb{Q}_p)$ that are isomorphic should give rise to the same L-parameter. However a fixed L-parameter can arise from different isomorphism classes, but only finitely many (those in the same "L-packet").

Roberts and Schmidt have classified the L-parameters of all non-supercuspidal representations of $\mathrm{GSp}_4(\mathbb{Q}_p)$ in [56]. For representations parabolically induced from the Borel subgroup of $\mathrm{GSp}_4(\mathbb{Q}_p)$ it turns out that the L-parameters are quite simple. The ρ_0 part is semisimple given by four characters of $W_{\mathbb{Q}_p}$ (which by local class field theory correspond to four characters of $\mathbb{Q}_p^\times$).

Fixing a uniformizer ω of $\mathbb{Q}_p^\times$ and evaluating these four characters at ω gives four complex numbers called Satake parameters. Unramified representations are uniquely determined by their Satake parameters (much in the same way as unramified local Galois representations are determined by the image of Frobenius).

The following table has been extracted from p.283 of Roberts and Schmidt [56]. It uses the same classification as given in Appendix A.1:

Type	ρ_0	Central character
I	$\chi_1\chi_2\sigma, \chi_1\sigma, \chi_2\sigma, \sigma$	$\chi_1\chi_2\sigma^2$
II	$\chi^2\sigma, \nu^{\frac{1}{2}}\chi\sigma, \nu^{-\frac{1}{2}}\chi\sigma, \sigma$	$(\chi\sigma)^2$
III	$\nu^{\frac{1}{2}}\chi\sigma, \nu^{-\frac{1}{2}}\chi\sigma, \nu^{\frac{1}{2}}\sigma, \nu^{-\frac{1}{2}}\sigma$	$\chi\sigma^2$
IV	$\nu^{\frac{3}{2}}\sigma, \nu^{\frac{1}{2}}\sigma, \nu^{-\frac{1}{2}}\sigma, \nu^{-\frac{3}{2}}\sigma$	σ^2
V	$\nu^{\frac{1}{2}}\sigma, \nu^{\frac{1}{2}}\xi\sigma, \nu^{-\frac{1}{2}}\xi\sigma, \nu^{-\frac{1}{2}}\sigma$	σ^2
VI	$\nu^{\frac{1}{2}}\sigma, \nu^{\frac{1}{2}}\sigma, \nu^{-\frac{1}{2}}\sigma, \nu^{-\frac{1}{2}}\sigma$	σ^2

The matrices N will not be needed so have been omitted.

Let us now return to our congruence between f and F. We have already seen that the existence of this congruence for all $q \neq p$ leads to a residual equivalence of global Galois representations:

$$\overline{\rho}_F \sim \overline{\rho}_f \oplus \overline{\chi}_l^{k-2} \oplus \overline{\chi}_l^{j+k-1}.$$

In particular we can compare these representations locally at p, the level of f. Since we have the local equality $\chi_l|_{W_{\mathbb{Q}_p}} = \nu^{-1}$ it follows that:

$$\overline{\rho}_{F,p}|_{W_{\mathbb{Q}_p}} \sim \overline{\rho}_{f,p}|_{W_{\mathbb{Q}_p}} \oplus \overline{\nu}^{2-k} \oplus \overline{\nu}^{1-j-k}.$$

So given the existence of the congruence we see that the local representations

of $\rho_{F,p}|_{W_{\mathbb{Q}_p}}$ and $\rho_{f,p}|_{W_{\mathbb{Q}_p}} \oplus \nu^{2-k} \oplus \nu^{1-j-k}$ of $W_{\mathbb{Q}_p}$ have the same composition factors mod Λ.

Recall that to F we have a "global" Galois representation ρ_F and a "global" automorphic representation π_F. Similarly for f. By local-global compatibility (see [61] for GSp_4 and [64] for GL_2) we know that $\rho_{F,p}|_{W_{\mathbb{Q}_p}}$ corresponds to $\pi_{F,p}$ and $\rho_{f,p}|_{W_{\mathbb{Q}_p}}$ corresponds to $\pi_{f,p}$ under the corresponding local Langlands correspondences.

Tying all of this together we expect the mod Λ L-parameters of $\pi_{F,p}$ to match those of $\pi_{f,p}$ and $|\cdot|_p^{2-k}, |\cdot|_p^{1-j-k}$ collectively (up to scaling by $p^{\frac{k'-1}{2}} = p^{\frac{j+2k-3}{2}}$). In particular the Satake parameters should match mod Λ.

Since f is a newform of level p it is known that $\pi_{f,p} \cong \mathrm{St}$ or $\pi_{f,p} \cong \epsilon\mathrm{St}$ where St is the Steinberg representation of $\mathrm{GL}_2(\mathbb{Q}_p)$ and ϵ is the unique unramified non-trivial quadratic character of $\mathbb{Q}_p^\times$. In either case the Satake parameters are known to be α_p and α_p^{-1} where $\alpha_p = p^{\frac{1}{2}}$ or $\epsilon(p)p^{\frac{1}{2}} = -p^{\frac{1}{2}}$.

Tying the above together we find that the required Satake parameters are

$$[a,b,c,d] = \left[\pm p^{\frac{j+2k-2}{2}}, \pm p^{\frac{j+2k-4}{2}}, p^{k-2}, p^{j+k-1}\right]$$

(where the sign is the same for a and b). Note that these are all integral powers of p.

Theorem 5.2.4. *Suppose $\pi_{F,p}$ is of type I-VI and $p^{j+2t-2} \not\equiv 1 \bmod \Lambda$ for $t = 0,1,2,3$. Then $\pi_{F,p}$ cannot be of type III,IV,V or VI.*

Proof. We show that the Satake parameters of representations of type III, IV, V or VI can be congruent mod Λ to those given above only if $p^{j+2t-2} \equiv 1 \bmod \Lambda$ for some $t = 0,1,2,3$. Then the result follows.

We work in reverse order. Here ϵ_0 will stand for the trivial character. Whenever there is a choice of sign this will be fixed by a choice of upper or lower row.

Type VI The L-parameter here is given by the four characters

$$\nu^{\frac{1}{2}}\sigma, \nu^{\frac{1}{2}}\sigma, \nu^{-\frac{1}{2}}\sigma, \nu^{-\frac{1}{2}}\sigma.$$

Since the central character is trivial we have $\sigma^2 = \epsilon_0$, so that σ is trivial or quadratic.

Thus in some order the Satake parameters are given by

$$\pm p^{\frac{1}{2}}, \pm p^{\frac{1}{2}}, \pm p^{-\frac{1}{2}}, \pm p^{-\frac{1}{2}}.$$

Scaling by $p^{\frac{k'-1}{2}}$ gives

$$\pm p^{\frac{j+2k-2}{2}}, \pm p^{\frac{j+2k-2}{2}}, \pm p^{\frac{j+2k-4}{2}}, \pm p^{\frac{j+2k-4}{2}}.$$

Notice that there are two equal pairs here. Thus for $[a,b,c,d]$ to be congruent to these four numbers mod Λ we would have to have that a is equivalent to one of b,c or d mod Λ.

Setting $a \equiv b \bmod \Lambda$ gives $p \equiv 1 \bmod \Lambda$.

Setting $a \equiv c \bmod \Lambda$ gives $p^{\frac{j+2}{2}} \equiv \pm 1 \bmod \Lambda$.

Setting $a \equiv d \bmod \Lambda$ gives $p^{\frac{j}{2}} \equiv \pm 1 \bmod \Lambda$.

Type V The L-parameter here is given by the four characters

$$\nu^{\frac{1}{2}}\sigma, \nu^{\frac{1}{2}}\xi\sigma, \nu^{-\frac{1}{2}}\xi\sigma, \nu^{-\frac{1}{2}}\sigma.$$

Since the central character is trivial we have $\sigma^2 = \epsilon_0$, so that σ is trivial or quadratic.

Thus in some order the Satake parameters are given by

$$\pm p^{\frac{1}{2}}, \mp p^{\frac{1}{2}}, \mp p^{-\frac{1}{2}}, \pm p^{-\frac{1}{2}}.$$

Scaling by $p^{\frac{k'-1}{2}}$ gives

$$\pm p^{\frac{j+2k-2}{2}}, \mp p^{\frac{j+2k-2}{2}}, \mp p^{\frac{j+2k-4}{2}}, \pm p^{\frac{j+2k-4}{2}}.$$

Notice that there are two pairs of the form $(\alpha, -\alpha)$. Thus for $[a,b,c,d]$ to be congruent to these four numbers mod Λ we would have to have that a is equivalent to one of $-b,-c$ or $-d$ mod Λ.

Setting $a \equiv -b \bmod \Lambda$ gives $p \equiv 1 \bmod \Lambda$.

Setting $a \equiv -c \bmod \Lambda$ gives $p^{\frac{j+2}{2}} \equiv \mp 1 \bmod \Lambda$.

Setting $a \equiv -d \bmod \Lambda$ gives $p^{\frac{j}{2}} \equiv \mp 1 \bmod \Lambda$.

Type IV The L-parameter here is given by the four characters

$$\nu^{\frac{3}{2}}\sigma, \nu^{\frac{1}{2}}\sigma, \nu^{-\frac{1}{2}}\sigma, \nu^{-\frac{3}{2}}\sigma.$$

Since the central character is trivial we have $\sigma^2 = \epsilon_0$, so that σ is trivial or quadratic.

Thus in some order the Satake parameters are given by

$$\pm p^{\frac{3}{2}}, \pm p^{\frac{1}{2}}, \pm p^{-\frac{1}{2}}, \pm p^{-\frac{3}{2}}.$$

Scaling by $p^{\frac{k'-1}{2}}$ gives

$$\pm p^{\frac{j+2k}{2}}, \pm p^{\frac{j+2k-2}{2}}, \pm p^{\frac{j+2k-4}{2}}, \pm p^{\frac{j+2k-6}{2}}.$$

If $[a,b,c,d]$ are congruent to these numbers mod Λ then there are four possibilities for c.

Setting $c \equiv \pm p^{\frac{j+2k}{2}} \bmod \Lambda$ gives $p^{\frac{j+4}{2}} \equiv \pm 1 \bmod \Lambda$.

Setting $c \equiv \pm p^{\frac{j+2k-2}{2}} \bmod \Lambda$ gives $p^{\frac{j+2}{2}} \equiv \pm 1 \bmod \Lambda$.

Setting $c \equiv \pm p^{\frac{j+2k-4}{2}} \bmod \Lambda$ gives $p^{\frac{j}{2}} \equiv \pm 1 \bmod \Lambda$.

Setting $c \equiv \pm p^{\frac{j+2k-6}{2}} \bmod \Lambda$ gives $p^{\frac{j-2}{2}} \equiv \pm 1 \bmod \Lambda$.

Type III The L-parameter here is given by the four characters

$$\nu^{\frac{1}{2}}\chi\sigma, \nu^{-\frac{1}{2}}\chi\sigma, \nu^{\frac{1}{2}}\sigma, \nu^{-\frac{1}{2}}\sigma.$$

Since the central character is trivial we have $\chi\sigma^2 = \epsilon_0$, so that $\chi\sigma = \sigma^{-1}$.

Thus in some order the Satake parameters are given by

$$p^{\frac{1}{2}}\beta^{-1}, p^{-\frac{1}{2}}\beta^{-1}, p^{\frac{1}{2}}\beta, p^{-\frac{1}{2}}\beta,$$

where $\beta = \sigma(p)$. Scaling by $p^{\frac{k'-1}{2}}$ gives

$$p^{\frac{j+2k-2}{2}}\beta^{-1}, p^{\frac{j+2k-4}{2}}\beta^{-1}, p^{\frac{j+2k-2}{2}}\beta, p^{\frac{j+2k-4}{2}}\beta.$$

If $[a,b,c,d]$ are congruent to these numbers mod Λ then there are four possibilities for a (each giving the value of β mod Λ). However replacing β by β^{-1} gives the same Satake parameters, so it suffices to set a congruent to just the last two Satake parameters.

Setting $a \equiv p^{\frac{j+2k-2}{2}}\beta \bmod \Lambda$ gives $\beta \equiv \pm 1 \bmod \Lambda$. This gives Satake parameters equivalent to

$$\pm p^{\frac{j+2k-2}{2}}, \pm p^{\frac{j+2k-2}{2}}, \pm p^{\frac{j+2k-4}{2}}, \pm p^{\frac{j+2k-4}{2}}.$$

However we have already dealt with these in Type VI.

Setting $a \equiv p^{\frac{j+2k-4}{2}}\beta \bmod \Lambda$ gives $\beta \equiv \pm p \bmod \Lambda$. This gives Satake parameters equivalent to

$$\pm p^{\frac{j+2k}{2}}, \pm p^{\frac{j+2k-2}{2}}, \pm p^{\frac{j+2k-4}{2}}, \pm p^{\frac{j+2k-6}{2}}.$$

However we have already dealt with these in Type IV.

Suppose now that none of the following holds:

$$p^{j-2} \equiv 1 \bmod \Lambda$$
$$p^{j} \equiv 1 \bmod \Lambda$$
$$p^{j+2} \equiv 1 \bmod \Lambda$$
$$p^{j+4} \equiv 1 \bmod \Lambda.$$

Then none of the conditions found above hold and so we must have that $\pi_{F,p}$ is of type I or II, as required. □

Note that the conditions above are not the strongest conditions but are sufficient for our purposes. It is expected that these weak conditions are still quite rare since p, j are generally small in comparison to l.

Also if one compares the Satake parameters $[a, b, c, d]$ to those from a representation of type I or II then no conditions arise. It is always possible for them to be congruent mod Λ.

5.2.3 $\pi_{F,p}$ is induced from the Borel

We now move on to our final task, showing that $\pi_{F,p}$ must be induced from the Borel subgroup of $\mathrm{GSp}_4(\mathbb{Q}_p)$. In this section Λ' will be an arbitrary prime of $K = \mathbb{Q}_F\mathbb{Q}_f$, lying above a rational prime l'.

Recall that $\pi_{F,p}$ corresponds via Local Langlands to a representation of the Weil-Deligne group W'_p, which itself is parametrized by a continuous representation $\rho_0 : W_{\mathbb{Q}_p} \to \mathrm{GSp}_4(\mathbb{C})$ and a nilpotent matrix $N \in \mathrm{M}_4(\mathbb{C})$ with certain properties (mentioned in the previous subsection). However if we fix a choice of embeddings $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$ and $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_{l'}$ then one can convert these representations into l'-adic representations with open kernel.

It is also known that local Galois representations give rise to Weil-Deligne representations.

Theorem 5.2.5. *(Grothendieck-Deligne) Let $p \neq l'$ and fix a continuous n-dimensional Λ'-adic representation:*

$$\rho : Gal(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \longrightarrow GL_n(K_{\Lambda'}).$$

Then associated to ρ is a unique l'-adic representation of $W'_{\mathbb{Q}_p}$, given by a pair (ρ'_0, N') satisfying:

- *$\rho'_0 : W_{\mathbb{Q}_p} \longrightarrow GL_n(K_{\Lambda'})$ is continuous with respect to the discrete topology on $GL_n(K_{\Lambda'})$. In particular $\rho'_0(I_p)$ is finite.*
- *$\rho'_0(\phi_p)$ has characteristic polynomial defined over $GL_n(\mathcal{O}_{\Lambda'})$ with constant term a unit.*
- *$N' \in M_n(K_{\Lambda'})$ is nilpotent and satisfies*

  $$\rho'_0(\sigma)N'\rho'_0(\sigma)^{-1} = \nu(\sigma)N',$$

  for all $\sigma \in W_{\mathbb{Q}_p}$.

Fixing the tamely ramified character $t_{l'} : I_p \to \mathbb{Z}_{l'}$, the relationship between ρ and ρ_0' is:

$$\rho(\phi_p^n u) = \rho_0'(\phi_p^n u) exp(t_{l'}(u)N'),$$

for all $n \in \mathbb{Z}$, $u \in I_p$.

Now consider the local Galois representation $\rho_{F,p}$. By the above theorem it has an associated Weil-Deligne representation, given by a pair (ρ_0', N'). A Local-Global Compatibility conjecture of Sorensen (pages 3-4 of [61], proved in certain cases by Mok in Theorem 4.14 of [52]) predicts that the Weil-Deligne representations attached to $\pi_{F,p}$ and $\rho_{F,p}$ are isomorphic (up to Frobenius semi-simplification). In particular this implies that $\rho_0 \cong \rho_0'$ up to Frobenius semi-simplification. We make this identification from now on and use ρ_0 to denote both representations.

A useful corollary of the above theorem is the following:

Corollary 5.2.6. *(Grothendieck Monodromy Theorem) With the above setup there exists a finite index subgroup $J_{\Lambda'} \subseteq I_p$ such that $\rho(\sigma) = exp(t_{l'}(\sigma)N)$ for each $\sigma \in J_{\Lambda'}$, i.e. each element of $J_{\Lambda'}$ acts unipotently.*

See the appendix of [58] for a proof of this.

By the Grothendieck Monodromy Theorem there exists a (maximal) finite index subgroup $J_{\Lambda'} \subseteq I_p$ acting by unipotent matrices, i.e. if $\sigma \in J_{\Lambda'}$ then:

$$\rho_{F,p}(\sigma) = \exp(t_{l'}(\sigma)N).$$

Note then that as a consequence, for each $\sigma \in J_{\Lambda'}$:

$$\rho_0(\sigma) = \rho_{F,p}(\sigma)\exp(-t_{l'}(\sigma)N) = I.$$

Thus ρ_0 factors through $I_p/J_{\Lambda'}$:

$$\rho_0 : I_p \longrightarrow I_p/J_{\Lambda'} \longrightarrow \mathrm{GL}_4(\mathcal{O}_{\Lambda'}).$$

Note that $\rho_0(I_p/J_{\Lambda'})$ is finite. It is conjectured that the size of this image is independent of Λ' (by Conjecture 1.3 on p.81 − 82 of [63] one expects a compatible system of Galois representations).

A generalization of an argument on p.46−48 of [11] tells us about the possible sizes of this image.

Lemma 5.2.7. *Suppose G is a finite subgroup of $GL_n(\mathcal{O}_{\Lambda'})$ and that $l' > e+1$ (where e is the ramification index of $K_{\Lambda'}/\mathbb{Q}_{l'}$). Then $|G|$ divides $|GL_n(\mathbb{F}_{\Lambda'})|$.*

Proof. We claim that the kernel of the reduction map $\mathrm{GL}_n(\mathcal{O}_{\Lambda'}) \to \mathrm{GL}_n(\mathbb{F}_{\Lambda'})$ is torsion-free (i.e. every non-identity element in the kernel is of infinite order).

Then restricting to G we must have trivial kernel (since G is finite), hence G injects into $\mathrm{GL}_n(\mathbb{F}_{\Lambda'})$.

To prove the claim we take $A \in \mathrm{GL}_n(\mathcal{O}_{\Lambda'})$ with $A \neq I$ and $A \equiv I \bmod \Lambda'$. We wish to prove that $A^m \neq I$ for each m. We already know this for $m = 1$.

Suppose that A has finite order $m > 1$. Then choosing a prime $q \mid m$ we see that $(A^k)^q = I$ (where $m = qk$). Letting $B = A^k$ we see that $B \neq I$ (since A has order bigger than k) and that $B \equiv I \bmod \Lambda'$. We have found a matrix with the same conditions as A with prime order. Thus it suffices to show that no such matrix can have prime order.

To this end we write $A = I + M$ with $M \neq 0$ and M having entries in Λ' (since $A \equiv I \bmod \Lambda'$). Choose an entry $m_{u,v}$ of M such that $|m_{u,v}|_{\Lambda'} = \delta$ is maximal among all entries of M. Then $0 < \delta \leq \frac{1}{N(\Lambda')}$ (normalizing the absolute value in the usual fashion).

Note that:

$$A^q = (I + M)^q = I + qM + \binom{q}{2} M^2 + ... + \binom{q}{q-1} M^{q-1} + M^q.$$

Case 1: Suppose $q \neq l'$. Then the entries of $\binom{q}{j} M^j$ for $j \geq 2$ all have Λ'-adic absolute value less than or equal to δ^2. However qM contains the entry $qm_{u,v}$ of absolute value $\delta > \delta^2$ (since $q \neq l'$). Hence $A^q - I$ must contain an entry of absolute value $\delta > 0$ and so $A^q - I \neq 0$ as required.

Case 2: $q = l'$. We need sharper inequalities for this case since qM has no entry of absolute value δ. However it does contain the entry $qm_{u,v}$ of absolute value $\frac{\delta}{N(\Lambda')^e}$ (since by definition the ramification index of the extension is e).

For $2 \leq j \leq q-1$ we know that q divides $\binom{q}{j}$ so the matrices $\binom{q}{j} M^j$ have entries of maximal absolute value $\frac{\delta^2}{N(\Lambda')^e} \leq \frac{\delta}{N(\Lambda')^{e+1}} < \frac{\delta}{N(\Lambda')^e}$.

(We did not need to take into account divisibility of binomial coefficients in Case 1, weaker inequalities were enough.)

The matrix M^q has entries of absolute value greater than or equal to $\delta^q < \delta^{e+1} \leq \frac{\delta}{N(\Lambda')^e}$ (using here the condition $q = l' > e + 1$).

Thus we see that $A^q - I$ contains an entry of absolute value $\frac{\delta}{N(\Lambda')^e} > 0$ and so $A^q - I \neq 0$ as required. □

Set $N(\Lambda') = l'^f$. Then a simple linear algebra argument shows:

$$\begin{aligned} |\mathrm{GL}_4(\mathbb{F}_{\Lambda'})| &= (l'^{4f} - l'^{3f})(l'^{4f} - l'^{2f})(l'^{4f} - l'^f)(l'^{4f} - 1) \\ &= l'^{6f}(l'^f - 1)(l'^{2f} - 1)(l'^{3f} - 1)(l'^{4f} - 1). \end{aligned}$$

Now by using what we know about $\rho_{F,p}$ from the congruence we may prove the following.

Theorem 5.2.8. *If $J_{\Lambda'} \neq I_p$ and $m_{\Lambda'} = |\rho_0(I_p/J_{\Lambda'})|$ then $l | m_{\Lambda'}$.*

Proof. Note that $m_{\Lambda'} = |\rho_{F,p}(I_p/J_{\Lambda'})|$.

As mentioned it is conjectured that $m_{\Lambda'}$ has order independent of Λ'. Thus we may make the choice $\Lambda' = \Lambda$.

Now $G = \rho_{F,p}(I_p/J_\Lambda)$ is a finite subgroup of $\mathrm{GL}_4(\mathcal{O}_\Lambda)$. It must embed into $\mathrm{GL}_4(\mathbb{F}_\Lambda)$ by reduction (since by the proof of the above lemma G cannot contain any non-trivial elements in the kernel of reduction). Thus $|G| = |\overline{\rho}_{F,p}(I_p/J_{\Lambda'})|$.

However by the congruence we already know that the mod Λ reduction $\overline{\rho}_{F,p}$ has composition factors $\overline{\rho}_{f,p}, \overline{\chi}_l^{k-2}, \overline{\chi}_l^{j+k-1}$.

Then since $\overline{\rho}_{f,p} = \begin{pmatrix} 1 & \star \\ 0 & 1 \end{pmatrix}$ and χ_l is unramified at p we have:

$$\overline{\rho}_{F,p}(I_p/J_\Lambda) \subseteq \left\{ \begin{pmatrix} 1 & \star & \star & \star \\ 0 & 1 & \star & \star \\ 0 & 0 & 1 & \star \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\}.$$

However $J_\Lambda \neq I_p$, so that $\overline{\rho}_{F,p}(I_p/J_\Lambda)$ is non-trivial, showing that $N(\Lambda)$ divides $|G|$. Thus l divides $|G|$. Then by the independence of Λ' mentioned above $l | m_{\Lambda'}$ for any Λ'. □

Corollary 5.2.9. *Let $K_\Lambda/\mathbb{Q}_l$ have ramification index e and residue degree f. If $l \geq max\{6f+2, e+2\}$ then $J_{\Lambda'} = I_p$ for some Λ'.*

Proof. Suppose $J_{\Lambda'} \neq I_p$ for all Λ'. Then we know that $l | m_{\Lambda'}$ for all Λ'. But for each Λ' we know that $\rho_0(I_p/J_{\Lambda'})$ is a finite subgroup of $\mathrm{GL}_4(\mathcal{O}_{\Lambda'})$ and so (restricting to those extensions such that $l' > e+1$):

$$l | l'^{6f}(l'^f - 1)(l'^{2f} - 1)(l'^{3f} - 1)(l'^{4f} - 1),$$

for all such l'.

It remains to prove that l' can be chosen to contradict this. To contradict the divisibility condition it suffices to choose $l' \neq l$ such that $l'^{3f} \not\equiv 1 \bmod l$ and $l'^{4f} \not\equiv 1 \bmod l$. To do this we will show that, under the condition on l, there exists a non-zero class mod l that does not have order dividing $3f$ or $4f$.

Note that since l is prime there are at most n solutions to the congruence $x^n \equiv 1 \bmod l$, hence at most n classes mod l of order dividing n. Thus there are at most $3f + 4f = 7f$ classes that have order dividing $3f$ or $4f$. However

note that the classes of order dividing $\mathrm{hcf}(3f, 4f) = f$ are counted twice and so there must be at most $7f - f = 6f$ classes of order dividing $3f$ and $4f$.

But since $l \geq 6f+2$ there must be a non-zero class mod l that doesn't satisfy these congruences. By Dirichlet's theorem there are infinitely many primes in this class mod l.

It suffices to choose l' to be in this class with $l' \geq e+2$ (so that $l' > e+1$ too). □

Of course it is highly likely that $l \geq \max\{6f+2, e+2\}$ in practice since l is a "large" prime. The result will still hold true for certain $l \leq \max\{6f+2, e+2\}$ but it is not so easy to find a good choice for l'.

It remains to prove that the case $J_{\Lambda'} = I_p$ (known as "semi-stable" in Wiese [69]) implies that $\pi_{F,p}$ is induced from the Borel subgroup of $\mathrm{GSp}_4(\mathbb{Q}_p)$.

Proposition 5.2.10. *If Λ' satisfies $J_{\Lambda'} = I_p$ then $\pi_{F,p}$ is induced from the Borel subgroup of $GSp(\mathbb{Q}_p)$.*

Proof. It suffices to show that there is a basis of $K^4_{\Lambda'}$ such that

$$\rho_0 \cong \begin{pmatrix} \chi_1 & \star & \star & \star \\ 0 & \chi_2 & \star & \star \\ 0 & 0 & \chi_3 & \star \\ 0 & 0 & 0 & \chi_4 \end{pmatrix},$$

for four unramified characters $\chi_1, \chi_2, \chi_3, \chi_4$ of $W_{\mathbb{Q}_p}$. Then since the image of ρ_0 lies in GSp_4 we must have that $\chi_3 = \chi_1^{-1}$ and $\chi_4 = \chi_2^{-1}$. Then by Local Langlands for GSp_4 it must be that $\pi_{F,p}$ is induced from the Borel subgroup.

To this end we already know that I_p acts unipotently and so it remains to study the action of Frobenius ϕ_p. Recall the condition $\rho_0(\phi_p)N\rho_0(\phi_p)^{-1} = p^{-1}N$. We will rewrite this as $\rho_0(\phi_p)N = p^{-1}N\rho_0(\phi_p)$.

By Theorem 5.2.5 the characteristic polynomial of $\rho_0(\phi_p)$ has constant term in $\mathcal{O}^\times_{\Lambda'}$ we may choose an eigenvector v of $\rho_0(\phi_p)$ with non-zero eigenvalue $\alpha \in \mathcal{O}_{\Lambda'}$. Then notice that

$$\rho_0(\phi_p)(Nv) = p^{-1}N\rho_0(\phi_p) = \alpha p^{-1}(Nv).$$

This shows that if $Nv \neq 0$ then Nv is another eigenvector of $\rho_0(\phi_p)$ with eigenvalue $\alpha p^{-1} \neq \alpha$.

Consider the list v, Nv, N^2v, N^3v. If all of these vectors are non-zero then we have a basis of eigenvectors for $\rho_0(\phi_p)$. Then $\rho_0(\phi_p)$ is diagonal.

If for some $i \leq 3$ we have $N^iv = 0$ then we can quotient out by the subspace generated by $v, Nv, ..., N^{i-1}v$ and choose another eigenvector w for $\rho_0(\phi_p)$ acting on this quotient by a non-zero eigenvalue.

We may generate the list w, Nw, N^2w. If there are $4-i$ non-zero vectors here then we are done, since we can lift to $K^4_{\Lambda'}$ and couple with the $N^k v$'s to make a basis such that $\rho_0(\phi_p)$ is upper triangular.

If there are not enough non-zero vectors then we may quotient out again and repeat the same process with a new eigenvector y. Continuing in this fashion we then construct a basis of $K^4_{\Lambda'}$ such that:

$$\rho_0(\phi_p) = \begin{pmatrix} \alpha_1 & \star & \star & \star \\ 0 & \alpha_2 & \star & \star \\ 0 & 0 & \alpha_3 & \star \\ 0 & 0 & 0 & \alpha_4 \end{pmatrix}.$$

It is then clear that ρ_0 is of the required form with unramified characters defined by $\chi_i(\phi_p) = \alpha_i$ for $i = 1, 2, 3, 4$ (since I_p acts unipotently). □

5.3 Congruences of local origin

One can use similar techniques to Subsection 5.2.2 to explain why the methods used in this thesis do not produce congruences of "local origin", also predicted by Harder [32].

To explain the meaning of this term we first briefly consider such congruences between elliptic modular forms. One may find a more in depth discussion in [20].

Recall that for all primes p we have the Ramanujan congruence:

$$\tau(p) \equiv 1 + p^{11} \bmod 691.$$

This shows a congruence between Hecke eigenvalues of a level 1 cuspform of weight 12 and the Hecke eigenvalues of the weight 12 Eisenstein series.

The modulus 691 can be interpreted in many ways. Naively this prime just happens to appear in the q-expansion of E_{12}. A better interpretation is that it divides the numerator of $\frac{B_{12}}{24}$ (the relevant quantity in the coefficients of E_{12}). However the best interpretation is that it divides the numerator of $\frac{\zeta(12)}{\pi^{12}}$.

One can ask whether such Ramanujan congruences arise for elliptic modular forms of higher level. Indeed they do but a mysterious phenomenon occurs.

Consider the question of finding a normalized eigenform $f \in S_k(\Gamma_0(p))$ satisfying for all $q \neq p$:

$$a_q \equiv 1 + q^{k-1} \bmod \lambda$$

where λ is some prime of $\mathbb{Q}_f$. For technical reasons we must demand that $k \neq 2$ and that λ does not lie above 2 or 3.

Of course if $\mathrm{ord}_\lambda\left(\frac{B_k}{2k}\right) > 0$ then we can manipulate the Eisenstein series E_k mod λ to find a level 1 cuspform that satisfies the congruence (i.e. an oldform in $S_k(\Gamma_0(p))$). However newforms can satisfy such congruences too. How do we account for these?

It turns out that instead of looking for primes dividing (global) zeta values we can instead look for primes dividing incomplete zeta values. Let:

$$\zeta_{\{p\}}(s) = \prod_{q \neq p}\left(1 - \frac{1}{q^s}\right)^{-1} = \left(1 - \frac{1}{p^s}\right)\zeta(s) = \frac{(p^k - 1)}{p^s}\zeta(s).$$

Then if $\mathrm{ord}_\lambda\left(\frac{\zeta_{\{p\}}(k)}{\pi^k}\right) > 0$ we expect to find a Ramanujan congruence of the above form for some $f \in S_k(\Gamma_0(p))$. The ones arising from newforms are predicted to come from those λ such that $\mathrm{ord}_\lambda(p^k - 1) > 0$ and $\mathrm{ord}_\lambda\left(\frac{\zeta(k)}{\pi^k}\right) = 0$ (i.e. $\mathrm{ord}_\lambda\left(\frac{B_k}{2k}\right) = 0$). This motivates the term "local origin", since such congruences are observed from divisibility of a (local) Euler factor.

We can do this in more generality. Let Σ be a finite set of primes and set

$$\zeta_\Sigma(s) = \prod_{p \notin \Sigma}\left(1 - \frac{1}{p^s}\right)^{-1} = \prod_{p \in \Sigma}\left(1 - \frac{1}{p^s}\right)\zeta(s) = \prod_{p \in \Sigma}\frac{(p^k - 1)}{p^s}\zeta(s).$$

Then one can predict congruences of higher level from divisibility of special values $\frac{\zeta_\Sigma(k)}{\pi^k}$.

Naturally we may ask if there are any Harder style congruences of "local origin". Indeed these are also predicted to occur and a plentiful supply of evidence has been found [5]. However, unlike the Ramanujan congruences of local origin these are still conjectural.

Let us make more precise what these congruences are. We seek genus 2 eigenforms, new at level p, such that:

$$b_q \equiv a_q + q^{k-2} + q^{j+k-1} \bmod \lambda$$

for all $q \neq p$. Here the a_q are eigenvalues of a level 1 elliptic eigenform (rather than the traditional level p as discussed earlier in this thesis). The modulus λ is now expected to arise from divisibility of (local) Euler factors of $L(f, j+k)$, i.e. $\mathrm{ord}_\lambda(p^{2(j+k)} - a_p p^{j+k} + p^{k'-1}) > 0$, where $k' = j + 2k - 2$.

As mentioned above we will use arguments similar to Subsection 5.2.2 in order to prove that such congruences are rarely found for paramodular forms on the Siegel side. To this end suppose an eigenform $F \in S_{j,k}^{\mathrm{new}}(K(p))$ satisfies a Harder type congruence of local origin with a normalized eigenform $f \in S_{k'}(\mathrm{SL}_2(\mathbb{Z}))$.

Recall that, by discussions in Subsection 5.2.2, the existence of the congruence forces $\pi_{F,p}$ to have Satake parameters congruent to $\alpha_p, \alpha_p^{-1}, p^{\frac{j+3}{2}}, p^{-\frac{j+3}{2}}$ mod λ. However now that f is of level 1 the values of α_p, α_p^{-1} are different.

Fortunately we only need to know these values mod λ and the divisibility of the Euler factor at p gives this. Indeed if:

$$\lambda \mid (p^{2(j+k)} - a_p p^{j+k} + p^{k'-1}) = (p^{j+k} + \alpha_p p^{\frac{k'+1}{2}})(p^{j+k} + \alpha_p^{-1} p^{\frac{k'+1}{2}})$$

then we see immediately that $\alpha_p \equiv p^{\pm(\frac{j+3}{2})}$ mod λ.

So working mod λ the relevant Satake parameters are (after scaling by $p^{\frac{j+2k-3}{2}}$

$$[a, b, c, d] = [p^{j+k}, p^{j+k-1}, p^{k-2}, p^{k-3}].$$

Theorem 5.3.1. *If a local origin congruence occurs for $F \in S_{j,k}^{new}(K(p))$ then $p^{j+2t} \equiv 1$ mod Λ for some $t = 0, 1, 2, 3$.*

Proof. We of course know that $F \in S_{j,k}^{\text{new}}(K(p))$ and so $\pi_{F,p}$ must have new paramodular fixed vectors, hence is of type II_a, IV_c, V_b, V_c, VI_c.

It is then a case of comparing Satake parameters in exactly the same fashion as Theorem 5.2.4. The details are omitted. □

The above theorem explains why no such congruences are found among my computations. Of course $p = 2, 3, 5, 7, 11$ are small primes and so we expect it to be rare for the conditions above to be satisfied. Indeed one may check explicitly that no local origin congruences arise.

Appendix A

Tables

A.1 Borel induced representations of GSp_4

The following table is adapted from p.297 of Roberts and Schmidt [56]. It lists the classification of all non-supercuspidal irreducible admissible representations of $\mathrm{GSp}_4(\mathbb{Q}_p)$ induced from the Borel subgroup. See Roberts and Schmidt's book [56] for a classification of representations induced from the Klingen and Siegel parabolics. For simplicity only the induced representations are given, rather than their irreducible constituents.

Contained in the table is information about $\dim(V^K)$ for certain interesting open compact subgroups K of $\mathrm{GSp}_4(\mathbb{Q}_p)$ (i.e. $\mathrm{GSp}_4(\mathbb{Z}_p)$ and the local paramodular group $K(p)$).

Here ϵ_0 is the trivial character and ξ is the unique unramified quadratic character of $\mathbb{Q}_p$. Recall also that χ_1, χ_2, σ are unramified characters.

Type	Constituent of	Conditions	$\dim(V^{\mathrm{GSp}_4(\mathbb{Z}_p)})$	$\dim(V^{K(p)})$
I	$\chi_1 \times \chi_2 \rtimes \sigma$	$\chi_1, \chi_2 \neq \lvert\cdot\rvert_p^{\pm 1}, \chi_1 \neq \lvert\cdot\rvert_p^{\pm 1}\chi_2^{\pm 1}$	1	2
II_a	$\lvert\cdot\rvert_p^{\frac{1}{2}}\chi \times \lvert\cdot\rvert_p^{-\frac{1}{2}}\chi \rtimes \sigma$	$\chi \neq \lvert\cdot\rvert_p^{\pm\frac{3}{2}}, \chi^2 \neq \lvert\cdot\rvert_p^{\pm 1}$	0	1
II_b			1	1
III_a	$\chi \times \lvert\cdot\rvert_p \rtimes \lvert\cdot\rvert_p^{-\frac{1}{2}}\sigma$	$\chi \neq \epsilon_0, \lvert\cdot\rvert_p^{\pm 2}$	0	0
III_b			1	2
IV_a	$\lvert\cdot\rvert_p \times \lvert\cdot\rvert_p^2 \rtimes \lvert\cdot\rvert_p^{-\frac{3}{2}}\sigma$		0	0
IV_b			0	0
IV_c			0	1
IV_d			1	1
V_a	$\lvert\cdot\rvert_p\xi \times \xi \rtimes \lvert\cdot\rvert_p^{-\frac{1}{2}}\sigma$	$\xi^2 = \epsilon_0, \xi \neq \epsilon_0$	0	0
V_b			0	1
V_c			0	1
V_d			1	0
VI_a	$\lvert\cdot\rvert_p \times \epsilon_0 \rtimes \lvert\cdot\rvert_p^{-\frac{1}{2}}\sigma$		0	0
VI_b			0	0
VI_c			0	1
VI_d			1	1

A.2 Newform dimensions

For each prime $p = 2, 3, 5, 7, 11$ the following tables give values of $\dim(A^{\text{new}}_{j,k}(D))$ for $0 \leq j \leq 20$ even and $0 \leq k \leq 15$. We use the specific quaternion algebras given at the end of Chapter 4. Note that Ibukiyama conjectures that these values are equal to $\dim(S^{\text{new}}_{j,k+3}(K(p)))$.

$p=2$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	0	0	0	1	1	1	0	2	1	2	1	3	2	3	2
2	0	0	0	0	0	0	0	1	1	1	1	2	4	2	4	5
4	0	0	0	0	1	1	1	1	3	3	4	4	7	7	9	9
6	0	0	0	0	1	0	2	2	4	3	5	7	10	9	13	14
8	0	0	0	1	2	2	2	4	7	7	9	10	15	17	20	22
10	0	0	0	1	3	4	4	6	10	10	14	17	21	23	29	33
12	0	0	1	1	3	5	6	8	12	14	17	21	28	30	37	41
14	0	0	1	3	5	6	9	12	17	19	24	29	37	40	49	56
16	0	1	2	4	8	9	13	16	23	26	32	38	48	53	63	70
18	0	0	2	5	9	11	15	20	28	31	39	46	58	64	76	86
20	0	2	3	7	12	16	20	26	35	41	50	58	71	81	94	106
$p=3$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	0	0	1	1	1	2	1	2	3	3	3	5	4	5	8
2	0	0	0	0	0	1	1	2	2	4	4	6	8	9	11	14
4	0	0	0	1	0	2	3	3	5	8	8	12	15	17	22	27
6	0	0	1	2	2	3	7	7	10	14	16	21	27	30	37	45
8	0	0	1	3	4	6	8	12	16	20	25	31	38	46	54	64
10	0	0	1	4	5	10	13	16	23	30	35	45	54	63	76	90
12	0	1	4	7	8	15	20	25	32	43	49	62	75	86	102	121
14	0	1	5	9	13	19	27	34	44	55	67	81	97	113	133	154
16	0	2	6	13	17	25	36	44	57	72	84	104	124	142	167	194
18	1	3	10	18	24	35	47	58	75	93	109	131	157	180	209	242
20	0	6	12	22	31	45	58	74	92	114	136	162	189	221	254	292

$p=5$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	0	1	1	2	2	3	3	5	5	7	8	10	11	14	16
2	0	0	0	0	1	2	3	5	7	10	13	17	22	27	33	40
4	0	1	1	3	4	7	10	14	18	25	31	39	48	59	70	84
6	0	0	3	4	7	11	17	22	31	39	50	63	77	92	112	131
8	0	3	5	9	15	21	28	40	51	64	81	99	119	144	169	198
10	0	2	6	12	20	29	41	54	71	90	112	136	165	196	231	270
12	1	6	14	22	31	48	62	81	104	130	157	193	228	269	316	366
14	0	7	17	27	44	60	82	107	136	167	207	247	294	346	404	465
16	3	13	24	43	61	84	113	145	180	224	269	322	381	445	514	594
18	3	14	34	53	78	109	143	181	230	279	336	401	472	548	636	727
20	4	26	45	72	105	143	183	236	289	352	423	500	582	680	779	890
$p=7$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	1	1	2	3	4	5	6	8	10	13	15	18	22	26	31
2	0	0	1	1	3	5	8	12	16	22	29	37	47	57	70	84
4	0	1	1	5	7	12	18	26	34	47	59	75	93	114	136	164
6	1	3	7	11	18	26	38	50	67	85	107	133	162	194	232	272
8	0	6	10	19	29	43	57	80	102	130	162	199	239	289	339	398
10	1	5	14	26	42	60	85	111	145	183	228	276	334	396	467	545
12	4	15	29	47	67	98	128	168	212	265	321	391	463	546	638	740
14	4	18	38	60	93	127	171	221	280	344	422	504	599	703	819	943
16	5	27	49	86	122	170	226	291	361	449	539	646	762	892	1030	1189
18	13	37	76	116	168	228	299	377	473	573	690	818	962	1116	1291	1475
20	13	54	94	150	214	291	373	477	585	712	852	1008	1174	1367	1567	1791

$p = 11$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	1	2	3	4	6	8	11	15	19	24	31	38	46	56	67
2	0	1	2	4	9	14	21	31	43	57	75	95	119	147	178	213
4	1	4	6	15	22	35	51	71	93	125	157	197	243	296	353	422
6	3	5	18	27	44	66	94	124	168	212	268	332	405	484	581	681
8	2	17	28	49	77	111	149	205	261	331	413	506	607	730	858	1005
10	7	20	43	75	115	161	225	293	377	475	586	709	856	1012	1189	1386
12	11	38	74	120	170	248	342	422	536	667	808	983	1163	1372	1603	1857
14	15	53	103	159	243	329	439	567	714	875	1072	1278	1515	1778	2068	2379
16	26	78	138	230	324	444	586	749	928	1147	1377	1642	1937	2261	2610	3008
18	38	100	198	298	428	582	759	954	1195	1447	1738	2063	2421	2806	3246	3707
20	44	148	252	390	554	745	954	1215	1487	1804	2157	2547	2966	3448	3951	4509

A.3 Congruences

The following table gives information on congruences found. These congruences were checked for Hecke eigenvalues at $q = 3$ when $p = 2$ and $q = 2$ when $p = 3, 5, 7, 11$.

In all cases $\dim(S^{\text{new}}_{j,k}(K(p))) = 1$.

Also included is the congruence expected at level 11. Note that the large prime here lies above 11 itself.

Whenever a_q is rational we give the Hecke eigenvalue explicitly. When it lies in a bigger number field we give the minimal polynomial $f(x)$ defining $\mathbb{Q}_f$ (then the Hecke eigenvalue a_2 in all of our cases is exactly a root α of this polynomial).

The large primes given are the rational primes lying below the prime for which the congruence holds.

	(j,k)	$j+2k-2$	Large prime	$\dim(S^{\text{new}}_{j+2k-2}(\Gamma_0(p)))$	$\text{tr}(T_q)$	$\text{tr}(T_q)^{\text{new}} = b_q$	a_q
$p=2$	$(0,14)$	26	37	3	2223720	2223720	97956
	$(2,10)$	20	61	2	18360	18360	-13092
	$(2,11)$	22	71	2	-57528	-57528	59316
	$(2,12)$	24	29	1	-122040	-122040	-505908
	$(4,10)$	22	61	2	-189720	-189720	71604
	$(6,7)$	18	29	1	1872	3240	6084
	$(10,6)$	20	109	2	216	216	-13092
	$(12,5)$	20	79	2	77544	-7560	-53028
	$(12,6)$	22	23	2	-275688	30600	71604
	$(14,5)$	22	379	2	102960	63000	59316
	$(16,4)$	22	37	2	-97488	-23400	71604
$p=3$	$(2,8)$	16	109	2	-312	-312	-234
	$(4,6)$	14	23	3	-36	-36	-12
	$(6,5)$	14	47	3	72	72	$x^2+54x-16992$
	$(8,5)$	16	67	2	300	12	-72
	$(10,5)$	18	433	3	120	24	$x^2-594x-42912$
	$(12,4)$	18	23	3	-1716	132	204
	$(14,4)$	20	617	3	-240	72	$x^2-702x-664128$
$p=5$	$(2,7)$	14	61	5	-76	-76	$x^3-142x^2-11144x+901248$
$p=7$	$(2,5)$	10	263	5	-44	-44	$x^3-21x^2-1326x+19080$
	$(4,4)$	10	101	5	-2	-2	$x^2+6x-184$
	$(4,5)$	12	43	5	-70	10	$x^2+54x-2640$
$p=11$	$(2,4)$	8	11	6	-20	-20	N/A

Appendix B

Future efforts

There are many ways to extend the work done in this thesis. Here are a few particular avenues that I would like to consider in more detail:

- Strengthen the validity of the congruences already found by calculating higher index Hecke eigenvalues. This would be a case of making my programs run more efficiently and if possible improving my algorithms.
- Find examples of congruences from spaces of paramodular forms that are 2-dimensional. A simplifying assumption in this thesis, made only for computational purposes, was that $\dim(S_{j,k}^{\text{new}}(K(p))) = 1$.

  It can be noted from the tables found in Appendix A.2 that there are plenty of 2-dimensional spaces to look at. Quite a few of these spaces contain eigenforms with suspected congruences (since large primes dividing $\Lambda_{\text{alg}}(f, j+k)$ are found).

  Theoretically we are able to use the exact same algorithms to find the necessary Hecke eigenvalues but computationally this is now a heftier task. When testing in 1-dimensional spaces (for a class number 1 prime) we had to find $|\Gamma^{(2)}|\deg(T_q) = \frac{5760(q^2+1)(q+1)}{p^2-1}$ character values in order to find $b_q = \text{tr}(T_q)$. However for a 2-dimensional space we need both $\text{tr}(T_q)$ and $\text{tr}(T_q^2)$ to find b_q. Finding $\text{tr}(T_q^2)$ requires the calculation of an extra $|\Gamma^{(2)}|^2\deg(T_q) = \frac{32148900(q^2+1)(q+1)}{(p^2-1)^2}$ character values. This is significantly bigger.
- I wish to study situations where the class number is not 1. In these cases the Hecke representatives can not necessarily be taken to be rational but I imagine my algorithms can be modified to tackle this.

  Also there is more than one Γ-group (but note that I already have algorithms to calculate $\Gamma^{(2)}$ so a small piece of the work has already been

done).

I can use Ibukiyama's class number formula to find primes such that the class number is 2. These should be the most fruitful to start with.

- It is also a possibility to consider extending Ibukiyama's results to composite square-free levels. I imagine this would be a case of allowing more ramification in the quaternion algebra and would allow computation of Hecke eigenvalues of Siegel forms for $K(N)$.

  Again this would involve generalizing most of the work done in this thesis but it should be possible to guess the results. Once achieved this allows the possibility of finding other new congruences.

- I could study congruences for higher genus Siegel modular forms. We should still have some sort of Ibukiyama correspondence here but this would require a lot of thought (e.g. replacements for the paramodular group and U_2 on the algebraic side).

  Also the newform theory for algebraic forms would need to be considered. However once this is done I imagine the descriptions of the Γ-groups and the Hecke representatives should be similar to what we have seen.

- I could change the base field $\mathbb{Q}$ to some other real quadratic field, studying Hilbert-Siegel modular forms. Work in this area has already been done by Cunningham and Dembelé [16].

  In this case the analogue of Ibukiyama's correspondence has actually been proved by Sorensen [60].

  Here the descriptions of the Γ-groups and Hecke representatives would change but hopefully not too much from the rational case.

- I could change the group $G = \mathrm{GSp}_4$ to some other reductive split group. Recently many congruences have been predicted for unitary and orthogonal groups amongst others [5].

  Automorphic forms for such groups can also be linked with algebraic modular forms and so it is possible that I can check some of these congruences via similar methods.

- Investigate algebraic forms for orthogonal groups and special orthogonal groups. These groups are more suitable for generalizations of the Paramodular group than symplectic groups.

Bibliography

[1] R. Apéry, *Irrationalité de $\zeta(2)$ et $\zeta(3)$*. Astérisque 61, 1113, 1979.

[2] M. Asgari, R. Schmidt, *Siegel modular forms and representations*. Manuscripta math. 104, 173 – 200, 2001.

[3] A. O. Atkin, J. Lehner, *Hecke operators on $\Gamma_0(N)$*. Mathematische Annalen, 185, 134 – 160, 1970.

[4] J. Bergström, C. Faber, G. van der Geer, *Siegel Modular Forms of Genus 2 and Level 2: Cohomological Computations and Conjectures*. Int. Math. Res. Not. IMRN, 2008.

[5] J. Bergström, N. Dummigan, *Eisenstein congruences for split reductive groups*. 2014.

`http://people.su.se/~jonab/eiscong1.pdf`.

[6] J. Bernstein, P. Deligne, D. Kazhdan, M. -F Vignras, *Reprsentations des groupes rductifs sur un corps local*. Travaux en Cours, Paris: Hermann, 33 – 117, 1984.

[7] J. Bernstein, S. Gelbart at al, *An introduction to the Langlands Program*. Birkhauser Basel, 2004.

[8] S. Böcherer, R. Schulze-Pillot, *Vector valued theta series and Waldspurgers theorem*. Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg, Volume 64, Issue 1, pp 211 – 233, 1994.

[9] J. H. Bruinier, G. van der Geer, G. Harder, D. Zagier, *The* 1-2-3 *of Modular Forms*. Springer, Universitext, 2008.

[10] K. Buzzard, *Computing modular forms on definite quaternion algebras*.

`http://wwwf.imperial.ac.uk/~buzzard/maths/research/notes/old_notes_about_computing_modular_forms_on_def_quat_algs.pdf`

[11] J. W. S. Cassels, *Local Fields*. Cambridge University Press, London Mathematical Society Student Texts (No. 3), 1986.

[12] J. H. Conway, S. P. Norton, *Monstrous Moonshine*. Bull. London Math. Soc. 11, 308 – 339, 1979.

[13] G. Chenevier, *The infinite fern and families of quaternionic modular forms* `http://gaetan.chenevier.perso.math.cnrs.fr/coursIHP/chenevier_lecture6.pdf`

[14] G. Chenevier, J. Lannes, *Formes automorphes et voisins de Kneser des rseaux de Niemeier*. `http://arxiv.org/pdf/1409.7616v2.pdf`.

[15] N. Childress, *Class Field Theory*. Springer, Universitext, 2008.

[16] C. Cunningham, L. Dembelé, *Computing genus* 2 *Hilbert-Siegel modular forms over* $\mathbb{Q}(\sqrt{5})$ *via the Jacquet-Langlands correspondence*. Experiment. Math. 18, no. 3, 337 – 345, 2009.

[17] P. Deligne, *Values of L-Functions and Periods of Integrals*. Proc. Symp. Pure Math. AMS 33, 313 – 346, 1979.

[18] L. Dembelé, *On the computation of algebraic modular forms on compact inner forms of* GSp_4. Math. Comp. 83, 288, 1931 – 1950, 2014.

[19] F. Diamond, J. Shurman, *A first course in Modular Forms*. Springer, GTM 228, 2005.

[20] N. Dummigan, D. Fretwell, *Ramanujan style congruences of local origin*. Journal of Number Theory, Volume 143, Pages 248 – 261, 2014.

[21] N. Dummigan, *Symmetric square L-functions and Shafarevich-Tate groups*. Int. J. Number Theory, 5, 1321 – 1345, 2009.

[22] N. Dummigan, *A simple trace formula for algebraic modular forms*. Experimental Mathematics, 22, 123 – 131, 2013.

[23] B. Edixhoven, *The weight in Serre's conjectures on modular forms*. Inventiones mathematicae, Volume 109, Issue 1, 563 – 594, 1992.

[24] W. Fulton, J. Harris, *Representation Theory*. Springer, GTM 129, 2004.

[25] W. T. Gan, J. P. Hanke, J. Yu, *On an exact mass formula of Shimura*. Duke Math. J. Volume 107, 1, 103 – 133, 2001.

[26] W. T. Gan, S. Takeda, *The Local Langlands Conjecture for* $GSp(4)$. Annals of Mathematics, Pages 1841 – 1882, Volume 173, Issue 3, 2011.

[27] A. Ghitza, *Hecke eigenvalues of Siegel modular forms (mod p) and of algebraic modular forms*. Journal of Number Theory 106, 2, 345 – 384, 2004.

[28] A. Ghitza, N. Ryan, D. Sulon, *Computations of vector-valued Siegel modular forms*. Journal of Number Theory, Volume 133, Issue 11, Pages 3921 – 3940, 2013.

[29] M. Greenberg, J. Voight, *Lattice methods for algebraic modular forms on classical groups*. Computations with Modular Forms, Contributions in Mathematical and Computational Sciences Volume 6, 147 – 179, 2014.

[30] B. Gross, *Algebraic Modular Forms* Israel Journal of Mathematics, Volume 113, Issue 1, 61 – 93, 1999.

[31] G. Harder, *A congruence between a Siegel and an Elliptic Modular Form*. Featured in "The 1-2-3 of Modular Forms".

[32] G. Harder, *Secondary Operations in the Cohomology of Harish-Chandra modules*, 2013.

`http://www.math.uni-bonn.de/people/harder/Manuscripts/Eisenstein/SecOPs.pdf`.

[33] G. Harder, *Cohomology in the language of Adeles*.

`http://www.math.uni-bonn.de/people/harder/Manuscripts/buch/chap3-2014.pdf`.

[34] K. Hashimoto and T. Ibukiyama, *On class numbers of positive definite binary quaternion harmitian forms*. J.Fac.Sci.Univ.Tokyo Sect.IA Math., 27, 549 – 601, 1980.

[35] K. Hashimoto and T. Ibukiyama, *On class numbers of positive definite binary quaternion harmitian forms (II)*. J.Fac.Sci.Univ.Tokyo SectIA Math., 28, 695 – 699, 1982.

[36] H. Hida, *Geometric Modular Forms and Elliptic Curves*. World Scientific publishing, 2000.

[37] T. Ibukiyama, *On symplectic Euler factors of genus* 2. Proc. Japan Acad. Ser. A Math. Sci. Volume 57, Number 5, 271 – 275, 1981.

[38] T. Ibukiyama, *On maximal orders of division quaternion algebras over the rational number field with certain optimal embeddings*. Nagoya Math. J. Volume 88, 181 – 195, 1982.

[39] T. Ibukiyama, *On Automorphic Forms on the Unitary Symplectic Group* $Sp(n)$ *and* $SL_2(\mathbb{R})$. Mathematische Annalen, Volume 278, Issue $1-4$, $307-327$, 1987.

[40] T. Ibukiyama, T. Katsura, F. Oort, *Supersingular curves of genus* 2 *and class numbers*. Compositio Mathematica, Volume 57, Issue 2, 127 – 152, 1986.

[41] T. Ibukiyama, *Paramodular forms and compact twist*. Automorphic Forms on GSp(4), Proceedings of the 9th Autumn Workshop on Number Theory, Ed. M. Furusawa, 37 – 48, 2007.

[42] J.-I. Igusa, *On the ring of modular forms of degree two over* $\mathbb{Z}$. Amer. J. Math. 101, 149 – 183, 1979.

[43] Y. Ihara, *On certain arithmetical Dirichlet series*. J. Math. Soc. Japan, 16, 214 – 225, 1964.

[44] F. Jarvis, *Level lowering for modular mod l representations over totally real fields*. Mathematische Annalen 12; 313(1) : 141 – 160, 1998.

[45] A. Jorza, *Galois representations for holomorphic Siegel modular forms*. Mathematische Annalen, Volume 355, Issue 1, pp 381 – 400, 2013.

[46] L. Kilford, *Modular Forms: A classical and computational introduction*. Imperial College Press, 2008.

[47] D. H. Lehmer, *The vanishing of Ramanujans function* $\tau(n)$. Duke Math. J. 14: 429433, 1947.

[48] D. Loeffler, *Computing with algebraic automorphic forms*. Computations with Modular Forms: Proceedings of a Summer School and Conference, Heidelberg, August/September 2011 (ed. G. Bckle and G. Wiese), vol. 6 of Contributions in Mathematical and Computational Sciences, Springer, 2014, 47 – 68.

[49] J. I. Manin, *Periods of parabolic forms and p-adic Hecke series*. Mathematics of the USSR-Sbornik, Volume 21, Number 3, p.371, 1973.

[50] J. Milne, *Introduction to Shimura varieties*.

`http://www.jmilne.org/math/xnotes/svi.pdf`.

[51] J. Milne, *Reductive groups*.

`http://www.jmilne.org/math/CourseNotes/RG.pdf`.

[52] C. P. Mok, *Galois representations attached to automorphic forms on GL2 over CM fields*. Compositio Math. 150, 523-567, 2014.

[53] C. Poor, D. Yuen, *Paramodular cusp forms*. Journal Math. Comp. 84, 1401 – 1438, 2015.

[54] K. Ribet, *On Modular Representations of Gal(Q/Q) arising from modular forms*. Invent. Math. 100, 431476, 1990.

[55] J. D. Rogawski, *Representations of GL(n) and division algebras over a p-adic field*. Duke Mathematical Journal 50(1) : 161 – 196, 1983.

[56] B. Roberts, R. Schmidt, *Local Newforms for* GSp_4. Springer, Lecture notes in mathematics 1918, 2007.

[57] B. Roberts, R. Schmidt, *On modular forms for the paramodular group*. Automorphic Forms and Zeta Functions. Proceedings of the Conference in Memory of Tsuneo Arakawa. World Scientific, 2006.

[58] J. P. Serre, J. Tate, *Good reduction of Abelian varieties*. Annals of Mathematics, Vol 88, 3, 492 – 517, 1968.

[59] G. Shimura, *Arithmetic of alternating forms and quaternion hermitian forms*. J. Math. Soc. Japan, Volume 15, Number 1, 33 – 65, 1963.

[60] C. M. Sorensen, *Potential level-lowering for GSp*(4). J. Inst. Math. Jussieu, Volume 8, no 3, 595 – 622. 2009..

[61] C. M. Sorensen, *Galois representations and Hilbert-Siegel modular forms*. Doc. Math. 15, 623 – 670, 2010.

[62] W. Stein, *Modular Forms, a Computational Approach*. American Mathematical Society, GSM 79, 2007.

[63] R. Taylor, *Galois Representations*.
`http://math.stanford.edu/~lekheng/flt/taylor-long.pdf`.

[64] R. Taylor, T. Yoshida, *Compatibility of local and global Langlands correspondences*. J. Amer. Math. Soc., 20 – 2, 467 – 493, 2007.

[65] R. Tshushima, *An Explicit Dimension Formula for the Spaces of Generalized Automorphic Forms with Respect to Sp*$(2, \mathbb{Z})$. Proc. Japan Acad. Ser. A Math. Sci.Volume 59, Number 4, 139 – 142, 1983.

[66] S. Tsuyumine, *On Siegel modular forms of degree three*. Amer. J. Math.108, 755 – 862, 1986.

[67] J. Voight, *The arithmetic of Quaternion Algebras*.
`https://math.dartmouth.edu/~jvoight/crmquat/book/quat-modforms-041310.pdf`

[68] R. Weissauer, *Four dimensional Galois representations*. 2000.

[69] G. Wiese *Galois Representations*
`http://math.uni.lu/~wiese/notes/GalRep.pdf`

[70] `http://mathoverflow.net/questions/159604/integral-elements-of-quaternion-algebras-with-predescribed-properties`.