Maeda's Conjecture on Elliptic and Siegel Modular Forms

October, 2013

Author:
Angus McAndrew

Supervisor:
Dr. Alex Ghitza

Submitted in partial fulfillment of the requirements of the degree of Master of Science

Department of Mathematics and Statistics, The University of Melbourne

Abstract

Consider the Hecke operator T_n acting on the space of level 1 cusp forms $S_k(\mathrm{SL}(2,\mathbb{Z}))$. This is conjectured to have irreducible characteristic polynomial, with Galois group of its splitting field equal to the full symmetric group. We begin with a study of this conjecture, describing some commonly used results. Further we provide an updated version of an algorithm originally introduced in [Buz96] and discuss its asymptotic advantages.

Building on this, we look to the case of the space of degree 2 *Siegel* cusp forms, $S_k(\mathrm{Sp}(4,\mathbb{Z}))$, and the Hecke operators T_n acting on it. We investigate how the conjecture behaves under new conditions and how one needs to modify it to arrive at a generalisation. With this we give an algorithm to find evidence for our new conjecture, and describe some of the computational disadvantages of the Siegel case and some methods by which one can overcome these.

Declaration

This is to certify that

(i) the thesis comprises only my original work towards the Master of Science (Mathematics and Statistics) except where indicated in the preface;

(ii) due acknowledgement has been made in the text to all other material used; and

(iii) the thesis is 60-80 pages in length, excluding references, appendices figures and tables.

Angus McAndrew

Preface

This thesis expects no more background than could be reasonably acquired throughout an undergraduate course in mathematics. There are several sections to cover background and necessary definitions to give the reader a sufficient understanding of the context of the work.

- Section 1 (Introduction) describes the problem we considered.
- Section 2 provides preliminaries for the theory of elliptic modular forms.
- Section 3 defines the Hecke operators and gives a formula for their effect on Fourier expansions, which is a large part of our computational approach.
- Section 4 is an empirical study of Maeda's conjecture in the elliptic case, looking at previous work that has been done and providing a new technique and some further evidence. The work in this section was done together with my supervisor Alex, and much of it has been previously published in [GM12].
- Section 5 introduces the theory of Siegel modular forms and how the definitions from the elliptic theory can be generalised. We generalise Maeda's conjecture and provide an algorithm to check it for various weights. Using this, we provide evidence to support our generalised conjecture.
- Section 6 describes some further directions the study of this conjecture can and has been taken.

Acknowledgements

I would like to thank Alex Ghitza for his role as my supervisor. For suggesting the project to me and giving me constant guidance and support throughout the last two years. I have learned a great deal and grown a lot as a mathematician as a result of this work, and I thank him for being a part of that growth. I would like to further thank him for pushing me to get a paper out with him between my first and second semesters. It made me work much harder than I ever had up to that point on the project and it was the pivotal moment at which everything became much more serious. The opportunity to present it at the AustMS conference that year in Ballarat is as yet the highlight of my mathematical career. Finally, I'd like to thank him for organising and involving me in a weekly Number Theory seminar. It is now clear to me that number theory is my mathematical passion, and it has been great to have a forum for people to discuss the interesting work they have been considering.

Thank you also to Alex, the Sage team, Martin Raum, Nathan C. Ryan, Nils-Peter Skoruppa, and Gonzalo Tornaría. It was as a result of them that I was able to implement the code and algorithms that led to the empirical studies of the conjecture explored throughout the last two years. Further, I'd like to thank the IT team in the maths department for maintaining our servers and allowing us to run our computations on them.

Thank you to Arun Ram, for the many questions he asked and answered. The time that was given up just to talk about the world of mathematics in general meant a lot to me, and allowed me to learn much. Thank you to Lawrence Reeves, for being the second examiner on my thesis. It meant a lot that you would give your time up for my sake, even though you weren't my supervisor. Further, thank you to you both and all the rest of the lecturers I have had over the last five years of my study at Melbourne University. Every one of you has contributed to my mathematical path, and I cherish that.

Thank you to my friends and family for your support throughout my life, leading up to this crowning mathematical achievement. I needed all of you and you were all always there. You have all guided me and grown alongside me. It means more than you may know. Finally, thank you to my partner Mai. To you I will simply say the following:

Without you, my space has no structure. You give definitions meaning, and theorems purpose. If you are not here, all my actions are trivial.

Contents

1 Introduction

Martin Eichler has been famously quoted as saying, "There are five elementary arithmetical operations: addition, subtraction, multiplication, division, and modular forms". What is certainly true is that modular forms are one of the most ubiquitous concepts in modern mathematics. A modular form is a holomorphic function on the upper half plane $\mathcal{H}$ which has a particular transformation under the action of the group $\mathrm{SL}(2,\mathbb{Z})$. Thus at first glance they seem to belong to the theory of Complex Analysis. However, they are in fact historically associated with Number Theory and related areas of mathematics.

Thus it is unsurprising that the theory of modular forms is a well-studied and rich one. Much is understood and well known, but as yet there still exist phenomena that are surprising and unexplained. Some of these arise in even the most elementary examples. The topic we are concerned with is one of these phenomena.

On the space of modular forms one can define an algebra of commuting linear operators called Hecke Operators. The subspace of cusp forms is invariant (but not pointwise) under the action of these operators. Regarding this action, Maeda has conjectured the following:

Conjecture 1.1 (See [HM97], Conjecture 1.2)**.** *The Hecke algebra over $\mathbb{Q}$ of $S_k(\mathrm{SL}(2,\mathbb{Z}))$ is simple (that is, a single number field) whose Galois closure over $\mathbb{Q}$ has Galois group isomorphic to the symmetric group $\mathfrak{S}_d$, where $d = \dim S_k(\mathrm{SL}(2,\mathbb{Z}))$.*

This has attracted much attention within the field of modular forms, and has been slightly reformulated since its conception. A more modern statement, first considered by J.B. Conrey and D.W. Farmer in 1999, is as follows:

Conjecture 1.2 (See [CF99], Theorem 3)**.** *Let $n, k \in \mathbb{Z}_{>0}$. Let f be characteristic polynomial of the Hecke Operator T_n acting on the space $S_k(\mathrm{SL}(2,\mathbb{Z}))$ of level 1 weight k cusp forms. Let K be the splitting field of f. Then*

(1) f is irreducible over $\mathbb{Q}$,

(2) the Galois group $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_d$, the symmetric group on d letters, where $d = \dim S_k(\mathrm{SL}(2,\mathbb{Z}))$.

This is the form in which the conjecture is most often considered. It is a slightly stronger statement than the original, which is equivalent to the above statement being true for at least one Hecke operator, rather than all of them simultaneously.

We provide some background to define some terms and to give some insight into the significance of this conjecture. We also describe some of the results that have arisen in its study, along with our work in extending these methods. Finally, we give a new result, which seeks to extend and generalise the conjecture by applying it as much as possible to the case of *Siegel* modular forms.

2 Classical Modular Forms

We cover some basic definitions and concepts in the theory of modular forms. This section follows [Ste07], [DS05] and [Zud13].

2.1 The modular group and the upper half plane

The *upper half plane*, $\mathcal{H}$, is the set of all complex numbers with strictly positive imaginary part; i.e. $\mathcal{H} = \{\tau \in \mathbb{C} \mid \operatorname{Im}(\tau) > 0\}$.

Note: We use the notation τ rather than z to avoid confusion with general elements of $\mathbb{C}$.

Consider the group of rational 2×2 matrices with strictly positive determinant,

$$\mathrm{GL}(2,\mathbb{Q})^+ = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Q}) \;\middle|\; ad - bc > 0 \right\}. \tag{2.1}$$

This acts on $\mathcal{H}$ by *fractional linear transformations*. i.e. let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then

$$\gamma\tau = \frac{a\tau + b}{c\tau + d}. \tag{2.2}$$

Lemma 2.1. *The formula given in equation (2.2) defines a group action of $GL(2,\mathbb{Q})^+$ on $\mathcal{H}$. That is:*

(1) if $\gamma_1, \gamma_2 \in \mathrm{GL}(2,\mathbb{Q})^+$ and $\tau \in \mathcal{H}$, then $\gamma_1(\gamma_2\tau) = (\gamma_1\gamma_2)\tau$,

(2) if $\gamma \in GL(2,\mathbb{Q})^+$ and $\tau \in \mathcal{H}$, then $\operatorname{Im}(\gamma\tau) > 0$.

Proof. (1) follows from an uninspiring computation of the left hand and right hand sides of the desired equality. As for (2), let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, then

$$\operatorname{Im}(\gamma\tau) = \operatorname{Im}\left(\frac{a\tau + b}{c\tau + d}\right) = \operatorname{Im}\left(\frac{(ad - bc)\tau}{|c\tau + d|^2}\right) = \frac{ad - bc}{|c\tau + d|^2}\operatorname{Im}(\tau). \tag{2.3}$$

Since $ad - bc > 0$, $|c\tau + d|^2 > 0$ and $\mathrm{Im}(\tau) > 0$, we have $\mathrm{Im}(\gamma\tau) > 0$, as desired. □

We will in fact wish to specialise to a subgroup of $GL(2, \mathbb{Q})^+$. We consider the group of integral 2×2 matrices with determinant 1,

$$\mathrm{SL}(2, \mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(\mathbb{Z}) \;\middle|\; ad - bc = 1 \right\}. \tag{2.4}$$

Since it is a subgroup of $\mathrm{GL}(2, \mathbb{Q})^+$, this also has a well defined action on $\mathcal{H}$ by fractional linear transformations. In this case, the formula given in equation (2.3) reduces to $\mathrm{Im}(\gamma\tau) = \frac{\mathrm{Im}(\tau)}{|c\tau+d|^2}$. In the context of modular forms, $\mathrm{SL}(2, \mathbb{Z})$ is known as the *modular group*, and is generated by the matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \; S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}. \tag{2.5}$$

The action of $\mathrm{SL}(2, \mathbb{Z})$ on $\mathcal{H}$ leads us to consider the space of $\mathrm{SL}(2, \mathbb{Z})$-orbits in $\mathcal{H}$, denoted $\mathrm{SL}(2, \mathbb{Z}) \setminus \mathcal{H}$. This allows us to consider the notion of a fundamental domain for this orbit space, as follows

Lemma 2.2. *The fundamental domain for the action of* $\mathrm{SL}(2, \mathbb{Z})$ *on* $\mathcal{H}$ *is given by*

$$\mathcal{F}_1 = \left\{ \tau \in \mathcal{H} \;\middle|\; \begin{array}{c} \textit{Either } |\,\mathrm{Re}(\tau)| < 1/2 \textit{ and } |\tau| > 1, \\ \textit{or } -1/2 \leq \mathrm{Re}(\tau) \leq 0 \textit{ and } |\tau| = 1 \end{array} \right\}. \tag{2.6}$$

The fundamental domain $\mathcal{F}_1$ is shown below in Figure 2.1 A, with B showing some exceptional points of the domain and C demonstrating the transformation of the domain under the actions of the matrices T and S, defined in equation (2.5).

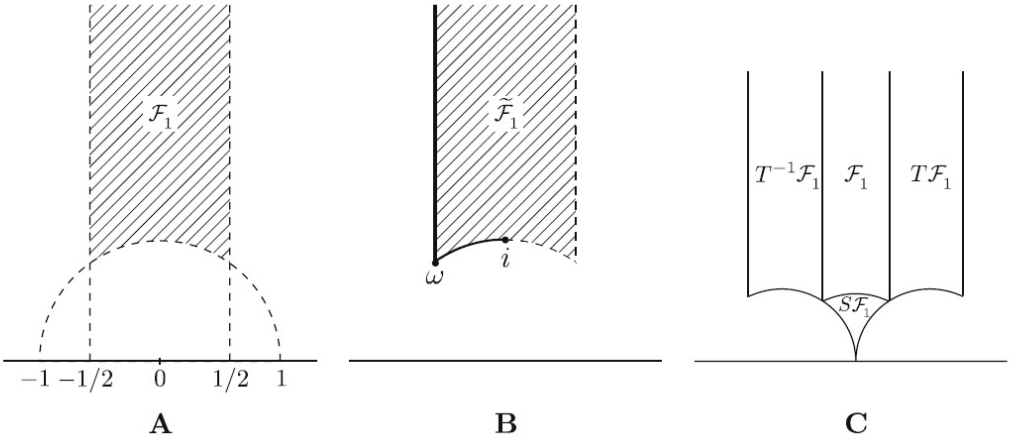

Figure 1: Fundamental domain for $\mathrm{SL}(2,\mathbb{Z}) \setminus \mathcal{H}$.

2.2 Weakly modular functions and modular forms

Definition 2.3 (Weakly modular function)**.** Let $k \in \mathbb{Z}$. A meromorphic function $f : \mathcal{H} \to \mathbb{C}$ is said to be *weakly modular of weight* k if

$$f(\gamma\tau) = (c\tau + d)^k f(\tau), \quad \text{for } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \text{ and } \tau \in \mathcal{H}. \tag{2.7}$$

A few things are immediately apparent from this definition.

First, to show a function is weakly modular of weight k, one only needs to check the transformation under the action of the matrices T and S defined in equation (2.5).

Second, one can apply the negative identity matrix $-I = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, to obtain

$$f(\tau) = f\left(\frac{-\tau}{-1}\right) = f\left(\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\tau\right) = (-1)^k f(\tau). \tag{2.8}$$

Thus if k is odd, we have $f(\tau) = -f(\tau)$ and thus $f(\tau) = 0$ for all $\tau \in \mathcal{H}$. So there are no nonzero weakly modular functions of odd weight.

Third, if one applies the matrix $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, one has

$$f(T\tau) = f\left(\frac{\tau+1}{1}\right) = f(\tau+1) = (1)^k f(\tau) = f(\tau). \tag{2.9}$$

So $f(\tau+1) = f(\tau)$, and thus a weakly modular function is $\mathbb{Z}$-periodic. As a periodic function, it has a Fourier expansion. This is given by

$$f(\tau) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi i n\tau} = \sum_{n=-\infty}^{\infty} a_n q^n, \quad \text{where } q = e^{2\pi i\tau}, \tag{2.10}$$

where the a_n are called the *Fourier coefficients*. For a weakly modular function f, let $a_n(f)$ denote the nth Fourier coefficient of f.

The association $\tau \mapsto q = e^{2\pi i\tau}$ is a map $\mathcal{H} \to D = \{z \in \mathbb{C} \mid |z| < 1\}$. This follows since if $\tau = x + iy$, with $y > 0$, then $|q| = |e^{-2\pi y} e^{2\pi i x}| < 1$. We may now observe that the preimage of the value $q = 0$ is given by $\tau = i\infty$. So one may wish to extend the requirement of meromorphicity on $\mathcal{H}$ to $\overline{\mathcal{H}} = \mathcal{H} \cup \{i\infty\}$. The point at infinity, $i\infty$, is known as the *cusp* of $\mathrm{SL}(2,\mathbb{Z})$. If f is meromorphic at ∞ (i.e. at $q = 0$), this corresponds to a finite number of negative index terms in the Fourier expansion.

With these concepts in mind, we may now turn to our main object of study:
Definition 2.4 (modular form)**.** A *modular form of weight k* is a function $f : \mathcal{H} \to \mathbb{C}$ such that:

(1) f is holomorphic,

(2) f is weakly modular of weight k,

(3) f is holomophic at the cusp.

As discussed above, this last condition corresponds to the Fourier coefficients $a_n = 0$ if $n < 0$. Thus a modular form is represented by a power series $f(q) = \sum_{n=0}^{\infty} a_n q^n$.

Note: Unless otherwise specified, we work exclusively with modular forms for $\mathrm{SL}(2,\mathbb{Z})$, i.e. level 1 (see section 2.4).

Recalling Conjecture 1.2, we in fact need to define the notion of a *cusp form*. A cusp form is a modular form that is not just holomorphic at the cusps, but indeed 0 at the cusp. i.e. $f(q=0) = \sum_{n=0}^{\infty} a_n(0)^n = 0$. Thus a cusp form is a modular form for which the Fourier coefficient $a_0 = 0$.

2.3 The space of modular forms

We may now wonder if any nonconstant modular forms or cusp forms even exist. The following are examples of each:

Example 2.5 (Eisenstein Series)**.** Let $k > 0$ be an even integer. The Eisenstein series of weight k is

$$G_k(\tau) = \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{(m\tau+n)^k}. \tag{2.11}$$

The holomorphicity follows from the convergence of the sequence. We will confirm that it is weakly modular of weight k.

$$\begin{aligned} G_k\left(\frac{a\tau+b}{c\tau+d}\right) &= \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{1}{\left(m\left(\frac{a\tau+b}{c\tau+d}\right)+n\right)^k} \\ &= \sum_{(m,n)\in\mathbb{Z}^2\setminus\{(0,0)\}} \frac{(c\tau+d)^k}{((am+cn)\tau+(bm+dn))^k} = (c\tau+d)^k G(\tau), \end{aligned}$$

where the last equality follows since if m and n vary over $\mathbb{Z}$, so too do $am+cn$ and $bm+dn$. The Fourier expansion is given by

$$G_k(q) = -\frac{B_k}{k!}(2\pi i)^k + 2\frac{(2\pi i)^k}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{k-1}(n)q^n, \quad \text{where } q = e^{2\pi i\tau}. \tag{2.12}$$

So this gives examples of modular forms for every possible weight. So we are well equipped with examples of modular forms. However, we still require cusp forms.

Given that we have modular forms represented by Fourier expansions, one could imagine taking products and sums of these expansions such that we

could force $a_0 = 0$. However, would this resulting function be a modular form? It would certainly be a holomorphic power series, but we would need to confirm that the function is weakly modular. In fact, we have the following:

Lemma 2.6. *Denote the set of modular forms of weight k as $M_k(\mathrm{SL}(2,\mathbb{Z}))$. Denote the subset of cusp forms as $S_k(\mathrm{SL}(2,\mathbb{Z}))$. Then*

(1) $M_k(\mathrm{SL}(2,\mathbb{Z}))$ is a complex vector space, and $S_k(\mathrm{SL}(2,\mathbb{Z}))$ is a subspace.

(2) The direct sum $M_*(\mathrm{SL}(2,\mathbb{Z})) = \bigoplus_{\substack{k\in\mathbb{Z}_{\geq 0}\\ k \text{ even}}} M_k(\mathrm{SL}(2,\mathbb{Z}))$ forms a graded complex algebra, and $S_*(\mathrm{SL}(2,\mathbb{Z})) = \bigoplus_{\substack{k\in\mathbb{Z}_{\geq 0}\\ k \text{ even}}} S_k(\mathrm{SL}(2,\mathbb{Z}))$ forms an ideal in $M_*(\mathrm{SL}(2,\mathbb{Z}))$.

Proof. (1) Let $f_1, f_2 \in M_k(\mathrm{SL}(2,\mathbb{Z}))$ and $\alpha_1, \alpha_2 \in \mathbb{C}$. Let $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Then

$$\begin{aligned}(\alpha_1 f_1 + \alpha_2 f_2)\left(\frac{a\tau+b}{c\tau+d}\right) &= \alpha_1 f_2\left(\frac{a\tau+b}{c\tau+d}\right) + \alpha_2 f_2\left(\frac{a\tau+b}{c\tau+d}\right)\\ &= \alpha_1(c\tau+d)^k f_1(\tau) + \alpha_2(c\tau+d)^k f_2(\tau)\\ &= (c\tau+d)^k(\alpha_1 f_1 + \alpha_2 f_2)(\tau)\end{aligned}$$

So $M_k(\mathrm{SL}(2,\mathbb{Z}))$ is a complex vector space, and if $a_0(f_1) = a_0(f_2) = 0$, then $a_0(\alpha_1 f_1 + \alpha_2 f_2) = \alpha_1 a_0(f_1) + \alpha_2 a_0(f_2) = 0$, so $S_k(\mathrm{SL}(2,\mathbb{Z}))$ is a subspace.

(2) Let $f_1 \in M_{k_1}(\mathrm{SL}(2,\mathbb{Z}))$ and $f_2 \in M_{k_2}(\mathrm{SL}(2,\mathbb{Z}))$, with $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ as above. Then

$$\begin{aligned}(f_1 f_2)\left(\frac{a\tau+b}{c\tau+d}\right) &= f_1\left(\frac{a\tau+b}{c\tau+d}\right) f_2\left(\frac{a\tau+b}{c\tau+d}\right)\\ &= (c\tau+d)^k f_1(\tau)(c\tau+d)^k f_2(\tau) = (c\tau+d)^{k_1+k_2}(f_1 f_2)(\tau).\end{aligned}$$

So $f_1 f_2 \in M_{k_1+k_2}(\mathrm{SL}(2,\mathbb{Z}))$ and thus $M_*(\mathrm{SL}(2,\mathbb{Z}))$ is a graded complex algebra. Further, if $a_0(f_1) = 0$ and $a_0(f_2) = \beta$, then $a_0(f_1 f_2) = a_0(f_1)a_0(f_2) = 0$. Thus $S_*(\mathrm{SL}(2,\mathbb{Z}))$ is an ideal in $M_*(\mathrm{SL}(2,\mathbb{Z}))$. □

Example 2.7 (Modular Discriminant)**.** The modular discriminant is defined as

$$\Delta(\tau) = (60G_4(\tau))^3 - 27(140G_6(\tau))^2. \tag{2.13}$$

This is a modular form of weight 12, by Lemma 2.6.

Further, we have that

$$\begin{aligned} a_0(\Delta) &= (60a_0(G_4))^3 - 27(140a_0(G_6))^2 \\ &= \left(60\frac{\pi^4}{45}\right)^3 - 27\left(140\frac{2\pi^6}{27\cdot 35}\right)^2 = 0, \end{aligned}$$

thus we have that $\Delta(\tau)$ is a cusp form of weight 12.

By Lemma 2.6, we have that $G_k(\tau)\Delta(\tau)$ is also a cusp form (where $k \in 2\mathbb{Z}_{\geq 0}$). Thus we have examples for cusp forms for all weights $k \geq 12$. In fact, it transpires that all examples of modular forms will arise from finite combinations of the examples we have seen. However, before that result we require a certain technical Theorem. First we require the following:

Definition 2.8 (Order of a function)**.** Let f be a meromorphic function. The *order of f at s*, denoted $v_s(f)$ is $n \in \mathbb{Z}$ such that $f(\tau)/(\tau - s)^n$ is holomorphic and $f(s)/(s-s)^n \neq 0$.

In fact, for modular forms, the functional equation $f(\frac{a\tau+b}{c\tau+d}) = (c\tau+d)^k f(\tau)$ implies that the integer $v_s(f)$ depends only on the orbit of s in $\mathrm{SL}(2,\mathbb{Z}) \setminus \mathcal{H}$. We now may state the desired result:

Theorem 2.9. *Let f be a non-zero modular form of weight k, for $k \geq 2\mathbb{Z}_{\geq 0}$. Then*

$$v_\infty(f) + \frac{1}{2}v_i(f) + \frac{1}{3}v_\rho(f) + \sum_{s\in\Omega} v_s(f) = \frac{k}{12}, \tag{2.14}$$

where $\rho = e^{2\pi i/3}$ and $\Omega = \{\tau \in \mathrm{SL}(2,\mathbb{Z}) \setminus \mathcal{H} \mid \gamma\tau \neq i, \rho \quad \forall \gamma \in \mathrm{SL}(2,\mathbb{Z})\}$.

Proof. See [Zag08], Proposition 2. □

The factors 1/2 and 1/3, along with the slightly odd summation index, come from the stabilisers of the points i and ρ in $\mathrm{SL}(2,\mathbb{Z})$.

The use to us of Theorem 2.9 is the following result:

Corollary 2.10. *The dimension of $M_k(\mathrm{SL}(2,\mathbb{Z}))$ is 0 for $k \in 2\mathbb{Z}+1$ or $k \in \mathbb{Z}_{<0}$, while for $k \in 2\mathbb{Z}_{\geq 0}$ we have*

$$\dim M_k(\mathrm{SL}(2,\mathbb{Z})) = \begin{cases} [k/12]+1, & \text{if } k \not\equiv 2 \pmod{12} \\ [k/12], & \text{if } k \equiv 2 \pmod{12}. \end{cases} \tag{2.15}$$

Proof. First, we have seen that $\dim M_k(\mathrm{SL}(2,\mathbb{Z})) = 0$ for $k \in 2\mathbb{Z}+1$ in equation (2.8). Second, note that the left hand side of equation (2.14) is non-negative, so we have that $k < 0$ would imply that $f = 0$, and thus $\dim M_k(\mathrm{SL}(2,\mathbb{Z})) = 0$ for $k \in \mathbb{Z}_{<0}$.

We now find dimensions for the spaces $M_k(\mathrm{SL}(2,\mathbb{Z}))$ for $k = 0, 2, 4, 6, 8, 10$ and show that multiplication by $\Delta(\tau)$ defines an isomorphism

$$M_{k-12}(\mathrm{SL}(2,\mathbb{Z})) \xrightarrow{\sim} S_k(\mathrm{SL}(2\mathbb{Z})). \tag{2.16}$$

Since $S_k(\mathrm{SL}(2,\mathbb{Z}))$ is the kernel of the following linear map:

$$\begin{array}{ccc} M_k(\mathrm{SL}(2,\mathbb{Z})) & \longrightarrow & \mathbb{C} \\ f = \sum_{n=0}^{\infty} a_n q^n & \longmapsto & a_0, \end{array} \tag{2.17}$$

we have that $\dim\left(M_k(\mathrm{SL}(2,\mathbb{Z}))/S_k(\mathrm{SL}(2,\mathbb{Z}))\right) = 1$, in particular

$$M_k(\mathrm{SL}(2,\mathbb{Z})) = S_k(\mathrm{SL}(2,\mathbb{Z})) \oplus \{cG_k(\tau) \mid c \in \mathbb{C}\}. \tag{2.18}$$

Consider solutions $(\ell, m, n) \in \mathbb{Z}^3_{\geq 0}$ to $\ell + \frac{1}{2}m + \frac{1}{3}n = \frac{k}{12}$. For $k = 0, 2, 4, 6, 8, 10$, there exist unique solutions. This shows that $\dim M_k(\mathrm{SL}(2,\mathbb{Z})) = 1$ for $k = 0, 2, 4, 6, 8, 10$.

Solutions for $k = 4$ and $k = 6$ show that $v_\rho(G_4) = 1, v_i(G_6) = 1$ and $v_s(G_k) = 0$ for $k = 4, 6$ and $\gamma s \neq \rho$ for $\gamma \in \mathrm{SL}(2,\mathbb{Z})$. This implies that $\Delta(i) \neq 0$ and thus Δ is nonzero and we can apply theorem 2.9. This implies that $v_\infty(\Delta) = 1$ and $v_s(\Delta) \neq 0$. Thus if $f \in S_k(\mathrm{SL}(2,\mathbb{Z}))$ we have that $g(\tau) = f(\tau)/\Delta(\tau)$ is well-defined and an element of $M_{k-12}(\mathrm{SL}(2,\mathbb{Z}))$, as required.

Thus, using the isomorphism as induction, we have the desired result. □

Thus if we fix k, we have that $M_k(\mathrm{SL}(2,\mathbb{Z}))$ is a finite-dimensional vector space. Thus we can find a finite basis and compute matrices and characteristic polynomials of any linear operator. In the context of Conjecture 1.2, we are interested particularly in Hecke Operators. These are covered in Section 3. However, first we wish to explain the term *level* appearing in the conjecture.

2.4 Congruence subgroups

In the definition of a weakly modular function of weight k, we could consider other groups than $\mathrm{SL}(2,\mathbb{Z})$ allowing for more examples of weakly modular functions. Consider the following group:

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Note first that $\Gamma(1) = \mathrm{SL}(2,\mathbb{Z})$. In fact, in general we have that $\Gamma(N) = \ker\left(\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{Z}/N\mathbb{Z})\right)$. This implies that $[\mathrm{SL}(2,\mathbb{Z}) : \Gamma(N)]$ is finite for all $N \in \mathbb{Z}_{>0}$. This leads us to the following notion:

Definition 2.11 (Congruence Subgroup)**.** Let $\Gamma \subseteq \mathrm{SL}(2,\mathbb{Z})$. If $\Gamma(N) \subseteq \Gamma$ for some $N \in \mathbb{Z}_{>0}$, then Γ is a *congruence subgroup*. It is denoted a congruence subgroup of *level* N.

The most important examples (besides $\Gamma(N)$ itself) are the following:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}, \text{ and}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \;\middle|\; \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

Now we must in general define a modular form with respect to a group of this form rather than $\mathrm{SL}(2,\mathbb{Z})$. For this, we introduce the notion of a *weight* k $\mathrm{GL}(2,\mathbb{Q})^+$*-action* on functions $f : \mathcal{H} \to \mathbb{C}$ as follows:

Let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2,\mathbb{Q})^+$, and $k \in \mathbb{Z}$. Then define

$$(\gamma, f) \longmapsto (f|_k\gamma)(\tau) = (\det\gamma)^{k/2}(c\tau+d)^{-k} f\left(\frac{a\tau+b}{c\tau+d}\right). \tag{2.19}$$

We can now extend the definition of a modular from $\mathrm{SL}(2,\mathbb{Z})$ to any congruence subgroup as follows:

Definition 2.12 (modular form)**.** Let $\Gamma \subseteq \mathrm{SL}(2,\mathbb{Z})$ be a congruence subgroup of level N. A *modular form of weight k with respect to* Γ is a function $f : \mathcal{H} \to \mathbb{C}$ such that:

(1) f is holomorphic,

(2) f is invariant under the weight k action of Γ, i.e. $f(z) = (f|_k\gamma)(z)$ for $\gamma \in \Gamma$,

(3) $f|_k\gamma$ is holomorphic at the cusp for all $\gamma \in \mathrm{SL}(2,\mathbb{Z})$.

Then f is said to be a modular form of weight k and level N.

In relation to the motivating Conjecture 1.2, we see that level 1 corresponds to the case $\Gamma(1) = \Gamma_0(1) = \Gamma_1(1) = \mathrm{SL}(2,\mathbb{Z})$, so the condition that the cusp forms be level 1 simply corresponds to the standard $\mathrm{SL}(2,\mathbb{Z})$ case.

One may wonder the need for having the factor of $\det\gamma$ in equation (2.19). This is relevant for section 3.

3 Hecke Operators

The Hecke operators are a large area of the study within the theory of modular forms. Historically, one of the reasons for their study was considering the question of how to find a suitable basis for the vector space of modular forms of a fixed weight k. Specifically, a consideration of this problem for the subspace of cusp forms is one of the motivating reasons for the theory of Hecke Operators. This follows since there exists an inner product on the space, the *Petersson Inner Product*, for which the operators arising from the action of the double coset $\Gamma_1(N) \setminus \mathrm{GL}(2,\mathbb{Q})^+/\Gamma_1(N)$ are Hermitian. This allows us, by linear algebra, to find an orthogonal basis of forms which are eigenvectors for every operator of this form.

First we recall the action of $\mathrm{GL}(2,\mathbb{Q})^+$ on $\mathcal{H}$, as defined in equation (2.19), that is

$$(\gamma, f) \longmapsto (f|_k\gamma)(\tau) = (\det\gamma)^{k/2}(c\tau+d)^{-k} f\left(\frac{a\tau+b}{c\tau+d}\right). \tag{3.1}$$

Using this we will define the Hecke Operators as the action of a double coset, defined in terms of the above. Specifically, we will consider the double cosets given by $\mathrm{SL}(2,\mathbb{Z}) \setminus \mathrm{GL}(2,\mathbb{Q})^+/\mathrm{SL}(2,\mathbb{Z})$. First we have the following:

Definition 3.1 (Double Coset)**.** Let G be a group, with H and K subgroups. An (H,K) double coset in G is an equivalence class of the equivalence relation defined by

$$x \sim y \text{ if there exists } h \in H \text{ and } k \in K \text{ such that } hxk = y.$$

This double coset is denoted HxK.

As stated above, we are interested in the case $G = \mathrm{GL}(2,\mathbb{Q})^+$ and $H = K = \mathrm{SL}(2,\mathbb{Z})$. In this case, we have the following result:

Proposition 3.2. *Let $\alpha \in \mathrm{GL}(2,\mathbb{Q})^+$. The double coset $\mathrm{SL}(2,\mathbb{Z})\alpha\mathrm{SL}(2,\mathbb{Z})$ is a finite union of right cosets:*

$$\mathrm{SL}(2,\mathbb{Z})\alpha\mathrm{SL}(2,\mathbb{Z}) = \bigcup_{i=1}^{N} \mathrm{SL}(2,\mathbb{Z})\alpha_i, \qquad \textit{where } \alpha_i \in \mathrm{GL}(2,\mathbb{Q})^+. \tag{3.2}$$

We may now define the Hecke Operator arising from a double coset as follows:

Definition 3.3 (Hecke Operator)**.** Let $\alpha \in \mathrm{GL}(2,\mathbb{Q})^+$. The *Hecke Operator* $T_\alpha : M_k(\mathrm{SL}(2,\mathbb{Z})) \to M_k(\mathrm{SL}(2,\mathbb{Z}))$ is given by

$$f \longmapsto f|T_\alpha = \sum_{i=1}^{N} f|_k \alpha_i, \tag{3.3}$$

where α_i are such that $\mathrm{SL}(2,\mathbb{Z})\alpha\mathrm{SL}(2,\mathbb{Z}) = \cup_{i=1}^{N}\mathrm{SL}(2,\mathbb{Z})\alpha_i$.

The fact that f is a modular form implies that $f|T_\alpha$ is independent of the choice of representatives of α_i. Further, for any $\gamma \in \mathrm{SL}(2,\mathbb{Z})$, the cosets $\mathrm{SL}(2,\mathbb{Z})\alpha_i\gamma$ are just permutations of the cosets $\mathrm{SL}(2,\mathbb{Z})\alpha_i$. Thus there exist $\gamma_i \in \mathrm{SL}(2,\mathbb{Z})$ such that $(\alpha_i\gamma)$ is just a permutation of $(\gamma_i\alpha_i)$. We can compute

$$(f|T_\alpha)\gamma = \sum_{i=1}^{N} f|\alpha_i\gamma = \sum_{i=1}^{N} f|\gamma_i\alpha_i = \sum_{i=1}^{n} f|\alpha_i = f|T_\alpha, \tag{3.4}$$

which demonstrates that $f|T_\alpha$ is also a modular form of weight k. One can also confirm that the operators T_α are linear on $M_k(\mathrm{SL}(2,\mathbb{Z}))$, and that the subspace $S_k(\mathrm{SL}(2,\mathbb{Z}))$ is invariant under the action. We wish to endow the collection of Hecke Operators with the structure of an algebra. For this, we will define the *product* of two Hecke Operators $T_\alpha T_\beta$ to satisfy

$$f|(T_\alpha T_\beta) = (f|T_\alpha)|T_\beta. \tag{3.5}$$

The right side of the above we compute as follows

$$(f|T_\alpha)|T_\beta = \sum_{j=1}^{M}\sum_{i=1}^{N} f|(\alpha_i\beta_j) = \sum_{\sigma\in\mathrm{SL}(2,\mathbb{Z})\backslash\mathrm{GL}(2,\mathbb{Q})^+} m(\alpha,\beta;\sigma) f|\sigma, \tag{3.6}$$

where

$$m(\alpha,\beta;\sigma) = \left|\{(i,j) \mid \sigma \in \mathrm{SL}(2,\mathbb{Z})\alpha_i\beta_j\}\right|. \tag{3.7}$$

One can confirm that $m(\alpha,\beta;\sigma)$ only depends on the coset $\mathrm{SL}(2,\mathbb{Z})\sigma\mathrm{SL}(2,\mathbb{Z})$ so we can write

$$f|T_\alpha T_\beta = \sum_{\sigma\in\mathrm{SL}(2,\mathbb{Z})\backslash\mathrm{GL}(2,\mathbb{Q})^+/\mathrm{SL}(2,\mathbb{Z})} m(\alpha,\beta;\sigma) f|\sigma. \tag{3.8}$$

We now have the following result:

Theorem 3.4. *The algebra generated by the Hecke Operators T_α for $\alpha \in \mathrm{GL}(2,\mathbb{Q})^+$ is commutative.*

Sketch of Proof. Consider the map

$$\begin{array}{rccc} \varphi: & \mathrm{GL}(2,\mathbb{Q})^+ & \longrightarrow & \mathrm{GL}(2,\mathbb{Q})^+ \\ & g & \longmapsto & g^\top, \end{array} \tag{3.9}$$

and the map φ_* it induces on the Hecke Algebra. One can prove that

$$\mathrm{SL}(2,\mathbb{Z})\alpha\mathrm{SL}(2,\mathbb{Z}) = \mathrm{SL}(2,\mathbb{Z})\alpha^\top\mathrm{SL}(2,\mathbb{Z}), \tag{3.10}$$

by showing that a minimal set of representatives is given by certain diagonal matrices. Thus the map φ_* is in fact the identity map, but also has the property that

$$\varphi_*(T_\alpha T_\beta) = \varphi_*(T_\alpha)\varphi_*(T_\beta). \tag{3.11}$$

A map with this property is often referred to as an *antiautomorphism*. The above, along with the fact that φ_* is the identity morphism, shows that

$$T_\alpha T_\beta = T_\beta T_\alpha, \tag{3.12}$$

and thus the algebra is commutative, as required. □

Note that the above implies that there is no need to differentiate between a right- or left-action. So this leads to the more commonly used notation of $T_\alpha f$ for the Hecke action.

The more usual type of the Hecke Operators is those of the form T_n. For these, we must consider the set

$$\Delta_n = \{\gamma \in \mathrm{GL}(2,\mathbb{Q})^+ \mid \det\gamma = n\}, \tag{3.13}$$

which has a decomposition given by the following result:

Lemma 3.5. *We have*

$$\Delta_n = \bigcup_{\substack{a,d>0,\ ad=n \\ 0\le b<n}} \mathrm{SL}(2,\mathbb{Z}) \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}. \tag{3.14}$$

If we denote the above decomposition as $\Delta_n = \cup_j \mathrm{SL}(2,\mathbb{Z})\delta_{n,j}$, we then define

$$f \longmapsto T_n f = \sum_j f|\delta_{n,j}. \tag{3.15}$$

We now wish to know the effect of the Hecke Operators on the Fourier expansions. For this, let $f(z) = \sum_n A(n)q^n$. By the definition of the operator T_n we can compute

$$\begin{aligned} T_n f(z) &= \sum_{ad=n} \sum_{b \pmod d} \left(\frac{a}{d}\right)^{k/2} f\left(\frac{az+b}{d}\right) \\ &= \sum_{ad=n} \sum_{b \pmod d} \left(\frac{a}{d}\right)^{k/2} \sum_{m=1}^{\infty} A(m) e^{2\pi i \frac{amz}{d}} e^{2\pi i \frac{mb}{d}} \end{aligned}$$

Note that $\sum_b e^{2\pi i \frac{mb}{d}} = d$ if $d|m$, and 0 otherwise. It follows that

$$(T_n f)(z) = \sum_{m=1}^{\infty} \sum_{\substack{ad=n \\ d|m}} \left(\frac{a}{d}\right)^{k/2} d e^{2\pi i \frac{amz}{d}} A(m) \tag{3.16}$$

Thus if we write $(T_n f)(z) = \sum_{m=1}^{\infty} B(m)q^m$, then

$$\sum_{\substack{ad=n \\ a|m}} \left(\frac{a}{d}\right)^{k/2} dA\left(\frac{md}{a}\right). \tag{3.17}$$

In the study of Conjecture 1.2, we are generally concerned with the action of T_n specifically on cusp forms. In this case, we may rewrite the above as follows:

Proposition 3.6. *Let $f = \sum a_n q^n \in S_k(\mathrm{SL}(2,\mathbb{Z}))$, and let T_m be the mth Hecke operator. Then we have*

$$(T_m f)(q) = \sum_{n=1}^{\infty} \left(\sum_{d|\gcd(m,n)} d^{k-1} a_{mn/d^2} \right) q^n. \tag{3.18}$$

This leads to the following remarkable result

Proposition 3.7. *Let $f(z) = \sum_n A(n)q^n$ be a Hecke eigenform (that is a simultaneous eigenvector for all the Hecke operators T_n), with eigenvalues $\lambda(n)$ normalised such that*

$$T_n f = n^{1-k/2}\lambda(n) f. \tag{3.19}$$

Then

(1) $A(1) \neq 0$.

(2) If $A(1) = 1$, *then* $\lambda(n) = A(n)$ *for all* n.

(3) If $A(1) = 1$ *and* $\gcd(n, m) = 1$, *then* $A(nm) = A(n)A(m)$.

Proof. We have

$$n^{1-k/2}\lambda(n)A(m) = \sum_{\substack{ad=n \\ a|m}} \left(\frac{a}{d}\right)^{k/2} dA\left(\frac{md}{a}\right) \tag{3.20}$$

(1) Suppose $\gcd(n, m) = 1$. Since $a|m$ and $a|n$, we have $a = 1$. Thus the above sum is just $d = n$, so

$$\lambda(n)A(m) = A(nm). \tag{3.21}$$

If $m = 1$, $\gcd(n, m) = 1$ for all n, so we have

$$\lambda(n)A(1) = A(n), \quad \text{for all } n. \tag{3.22}$$

Thus if $A(1) = 0$, $A(n) = 0$ for all n. So we have $A(1) \neq 0$.

(2) If $A(1) = 1$, then $\lambda(n) = A(n)$ by the above formula.

(3) If $A(1) = 1$, then $\lambda(n) = A(n)$, so we have from above

$$A(n)A(m) = A(nm), \tag{3.23}$$

as required.

□

4 Studying Maeda's Conjecture

Since Maeda originally posed the conjecture in [HM97], it has received much attention, both for applications of the conjecture, and for attempting to confirm it for various weights. Although studying the latter does not actually prove the conjecture, the examples considered have greatly helped in understanding the structure of the Hecke algebra.

The following is a summary of weights k for which the conjecture has been confirmed for the Hecke operator T_2:

Source	weights
Lee-Hung	$k \leq 62$, $k \neq 60$
Buzzard	$k = 12\ell$, ℓ prime, $2 \leq \ell \leq 19$
Maeda	$k \leq 468$
Conrey-Farmer	$k \leq 500$, $k \equiv 0 \pmod 4$
Farmer-James	$k \leq 2000$
Buzzard-Stein, Kleinerman	$k \leq 3000$
Chu-Wee Lim	$k \leq 6000$
Ghitza-McAndrew	$k \leq 14000$

Figure 2: Empirical evidence for Maeda's conjecture

Why choose the Hecke operator T_2? This is due to the computational difficulty of appealing to T_n for larger n. To perform computations with modular forms, their Fourier coefficients must be stored computationally. One chooses a precision, N, which defines the maximum index q^N for which the Fourier coefficient is computed. Now, consider the formula given in equation (3.18). To compute the nth Fourier coefficient of the image of a form $f = \sum a_j q^j$ under T_m, at most we need the coefficient a_{mn}.

How do the Fourier coefficients of these forms come into the computation of the characteristic polynomial of the Hecke Operator? We know that $S_k(\mathrm{SL}(2,\mathbb{Z}))$ is a finite dimensional vector space. So to compute the ma-

trix of the operator, we need to express the images of a set of basis vectors under that operator with respect to that basis. Given that the space is finite dimensional, it suffices to consider only a number of coefficients equal to the dimension. Further, it occurs that the first $d = \dim S_k(\mathrm{SL}(2,\mathbb{Z}))$ coefficients will distinguish these forms. We need to be able to compute the first d coefficients for all forms f and their images $T_m f$. So we need to at most compute the coefficient a_{md} for each basis element.

Thus, computationally, it is best to use the operator T_2 and vary the weight k. This has been the choice of the authors above. However, this is not to say that no work has been done examining the effect of increasing the index m of the Hecke Operator. Much theoretical work has been done in this regard. We present some of the results below:

Theorem 4.1 (Conrey-Farmer-Wallace)**.** *Let k be a positive even integer. Suppose there exists $n \geq 2$ such that the operator T_n acting on $S_k(\mathrm{SL}(2,\mathbb{Z}))$ satisfies Conjecture 1.2. Then so does T_p acting on $S_k(\mathrm{SL}(2,\mathbb{Z}))$ for every prime p in the set of density $5/6$ defined by the conditions*

$$p \not\equiv \pm 1 \pmod 5 \qquad \textit{and} \qquad p \not\equiv \pm 1 \pmod 7.$$

Theorem 4.2 (Baba-Murty)**.** *Let k be a positive even integer. Suppose there exists a prime p such that the characteristic polynomial of T_p acting on $S_k(\mathrm{SL}(2,\mathbb{Z}))$ is irreducible over $\mathbb{Q}$. Then there exists $\delta > 0$ such that*

$$|\{\ell \leq N \textit{ prime} \mid \mathrm{charpoly}(T_\ell) \textit{ is reducible}\}| \ll \frac{N}{(\log N)^{1+\delta}}. \tag{4.1}$$

Theorem 4.3 (Ahlgren)**.** *Let k be such that $d = \dim S_k(\mathrm{SL}(2,\mathbb{Z})) \geq 2$. Suppose there exists $n \geq 2$ such that the operator T_n acting on $S_k(\mathrm{SL}(2,\mathbb{Z}))$ satisfies Conjecture 1.2. Then*

(1) T_p acting on $S_k(\mathrm{SL}(2,\mathbb{Z}))$ satisfies Conjecture 1.2 for all primes $p \leq 4000000$,

(2) T_n acting on $S_k(\mathrm{SL}(2,\mathbb{Z}))$ satisfies Conjecture 1.2 for all $n \leq 10000$.

Our results are as stated above in Figure 2, focusing on the computational aspects of the operator T_2 on the spaces $S_k(\mathrm{SL}(2,\mathbb{Z}))$ for various weights k. Our approach is based on those introduced by Buzzard in [Buzzard 96] and refined by Conrey-Farmer in [CF99]. The technique comes from the observation that the Fourier coefficients a_n grow very quickly with the index n. Furthermore, in the study of this conjecture, what sort of questions are we asking? We are investigating some polynomial, and determining irreducibility and facts about its Galois group.

Given this problem, it is a standard technique to work over a finite field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ rather than $\mathbb{Z}$ itself. First we have the following definition:
Definition 4.4 (Reduced Polynomial)**.** Let $F \in \mathbb{Z}[X]$ and $p \in \mathbb{Z}$ a prime, such that we can write

$$F = a_n X^n + a_{n-1} + X^{n-1} + \ldots + a_1 X + a_0. \tag{4.2}$$

Then the *reduction of* F mod p, denoted $F_p \in \mathbb{F}_p[X]$ is

$$F = \overline{a}_n X^n + \overline{a}_{n-1} + X^{n-1} + \ldots + \overline{a}_1 X + \overline{a}_0, \tag{4.3}$$

where $\overline{a}_i \in \mathbb{F}_p$ is unique such that $\overline{a_i} \equiv a_i \pmod{p}$ for all $i \in \{1, \ldots, n\}$.

Now, it is a standard result that given a polynomial $F \in \mathbb{Z}[X]$, if the reduction F_p is irreducible then F is also irreducible. However, what can be said of the Galois group? For this, we first have the following group theoretic result
Lemma 4.5. *Let $G < \mathfrak{S}_d$ be a subgroup of the symmetric group on d symbols such that there exist elements $\tau_1, \tau_2 \in G$ such that τ_1 is a 2-cycle and τ_2 is a p-cycle, where p is a prime with $p > d/2$. Then $G = \mathfrak{S}_d$.*

Proof. For $i, j \in S = \{1, \ldots, d\}$, write $i \sim j$ if $i = j$ or if the transposition $(i\ j)$ is in G. This is an equivalence relation on S. Since G is transitive, each equivalence class has the same number n of elements and it follows that $n|d$, since $d = |S|$. Note that $n > 1$ since G contains at least one transposition, namely τ_1. Let T be the subset of S permuted by τ_2, and let G_T be the subgroup of G fixing $S \setminus T$. Define an equivalence relation on T by $i \simeq j$ if

$i = j$ or if the transposition $(i\ j) \in G_T$. As before, each equivalence class has the same number m of elements and $m|p$, since $p = |T|$. Since $n > 1$, we have $m > 1$, so $m = p$ since p is prime. But $n \geq m$ because $G_T \subset G$. Thus $n > d/2$, so $n = d$. This implies $G = \mathfrak{S}_d$. □

This allows us prove that the Galois Group of a given characteristic polynomial F is equal to $\mathfrak{S}_d$ for $d = \dim S_k(\mathrm{SL}(2, \mathbb{Z}))$ if we can exhibit the existence of just two elements, a transposition and a p-cycle, where $p > d/2$ is prime. We wish to infer this from the existence of certain factorization patterns in F_p for various p. The connection between these concepts is given by the *Frobenius elements* of the Galois Group. This is a central concept in Algebraic Number Theory, and is a common tool for gaining information about various Galois Groups by looking at finite or local fields (i.e. $\mathbb{F}_p$, $\mathbb{Q}_p$, etc.).

First we define some terminology:

Definition 4.6 (Cycle pattern)**.** Let $\tau \in \mathfrak{S}_d$ be a permutation on d symbols. Then it can be decomposed into a product of disjoint cycles. The *cycle pattern of* τ is

$$d_1^{m_1} d_2^{m_2} \dots d_t^{m_t} \tag{4.4}$$

if its decomposition contains exactly m_i cycles of length d_i for all $i \in \{1, \dots, t\}$.

Definition 4.7 (Factorization pattern, Separable)**.** Let $\mathbb{K}$ be a field and let $H \in \mathbb{K}[X]$ be a polynomial. The *factorization pattern of* H is

$$d_1^{m_1} d_2^{m_2} \dots d_t^{m_t} \tag{4.5}$$

if H has exactly m_i irreducible factors of degree d_i for all $i \in \{1, \dots, t\}$. We say H is *separable* if it has distinct roots over $\overline{\mathbb{K}}$, the algebraic closure of $\mathbb{K}$.

We can now state the main result that we wish to use, with a proof due to John Tate:

Theorem 4.8. *Let $F \in \mathbb{Z}[X]$ be monic, let p be a prime and let $F_p \in \mathbb{F}_p[X]$ be the reduction of F* mod p*. If F_p is separable, then there exists an element σ of the Galois group of F such that the cycle pattern of σ is the same as the factorization pattern of F_p.*

Proof. Let $x_1, \ldots, x_n$ be the roots of F. Let $\mathbb{K} = \mathbb{Q}(x_1, \ldots, x_n)$ be the splitting field of F. Let $G_F = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Let $A_F = \mathbb{Z}[x_1, \ldots, x_n]$ and let $\mathfrak{p}$ be a prime ideal of A_F such that $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$. Since F is monic, A_F is integral over $\mathbb{Z}$. Thus p is not invertible in A_F and we can therefore find such an ideal $\mathfrak{p}$. Further, this ideal is maximal since $\mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$ is maximal in $\mathbb{Z}$. Further, the field $E_{F_p} = A_F/\mathfrak{p} = \mathbb{F}_p[\overline{x}_1, \overline{x}_2, \ldots, \overline{x}_n]$, where $\overline{x}_i \in \mathbb{F}_p$ is unique such that $\overline{x}_i \equiv x_i \pmod{P}$, is the splitting field of F_p.

Since E_{F_p} is a finite extension of the finite field F_p, the Galois group $G_{F_p} = \mathrm{Gal}(E_{F_p}/\mathbb{F}_p)$ is cyclic generated by the automorphism $\overline{x} \mapsto \overline{x}^p$. Let $D_\mathfrak{p} = \{\sigma \in G_F \mid \sigma(\mathfrak{p}) = \mathfrak{p}\}$. $D_\mathfrak{p}$ is a subgroup of G_F called the *decomposition group at* P. Given an automorphism $\sigma \in D_\mathfrak{p}$ we can construct an automorphism $\overline{\sigma} \in G_{F_p} = \mathrm{Gal}(E_{F_p})$, where $\overline{\sigma}(\overline{x}) = \overline{\sigma(x)}$. Since $\sigma(\mathfrak{p}) = \mathfrak{p}$, we have that $\overline{\sigma}$ is well defined and further that this association is injective. We can thus define an injective homomorphism

$$\begin{array}{rccc} \phi: & D_\mathfrak{p} & \longrightarrow & G_{F_p} \\ & \sigma & \longmapsto & \overline{\sigma}. \end{array} \tag{4.6}$$

We wish to show that this is in fact an isomorphism. Thus we must show that it is surjective.

First, we will demonstrate that the fixed field of $\phi(D_\mathfrak{p})$ is $\mathbb{F}_p$. Let $a \in A_F$. Then by the Chinese Remainder Theorem, there exists an element $x \in A_F$ such that $x \equiv a \pmod{\mathfrak{p}}$ and $x \equiv 0 \pmod{\sigma^{-1}(\mathfrak{p})}$ for all $\sigma \in G_F \setminus D_\mathfrak{p}$. Then

$$\prod_{\sigma \in G_F} (X - \sigma(x)) \in \mathbb{Z}[X] \qquad \text{and} \qquad X^m \prod_{\sigma \in D_\mathfrak{p}} (X - \overline{\sigma}(\overline{a})) \in \mathbb{F}_p[X].$$

Thus all the conjugates of $\overline{a}$ are of the form $\overline{\sigma}(\overline{a}$, which implies that the fixed field of $\phi(D_\mathfrak{p})$ is $\mathbb{F}_p$, as desired.

Let $\sigma_\mathfrak{p} \in D_\mathfrak{p}$ be the unique element such that $\overline{\sigma}_\mathfrak{p}(\overline{x}) = \overline{x}^p$, which we can find by injectivity. Then $\sigma_\mathfrak{p}$ is the unique element of G_F such that $\sigma_\mathfrak{p}(x) \equiv x^p$ for every $x \in A_F$. Since the homomorphism $x \mapsto \overline{x}$ is a bijection between the roots of F and F_p, we thus have that the groups $D_\mathfrak{p}$ and G_{F_p} are isomorphic, as desired.

Then, since the cycle pattern of $\overline{\sigma}_{\mathfrak{p}}$ is determined by the orbits of the action of G_{F_p} on the roots of F_p, and since the group G_{F_p} acts transitively on the roots of each irreducible factor in the factorization pattern of F_p, we have that the cycle pattern of $\sigma_{\mathfrak{p}}$ is equal to the factorization pattern of F_p, as desired. □

In the literature, this is often referred to as follows:

Definition 4.9 (Frobenius Element)**.** Let $F \in \mathbb{Z}[X]$ be a monic polynomial with splitting field $\mathbb{K}$, Galois group $G_F = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$ and let p be a prime such that F_p is separable. Let $\mathfrak{p} \in \mathcal{O}_{\mathbb{K}}$ be a prime above p. The *Frobenius Element* $\mathrm{Frob}_{\mathfrak{p}} \in G_F$ is the unique element with cycle pattern equal to the factorisation pattern of F_p as determined by Theorem 4.8.

This leads to the following important result:

Lemma 4.10. *Let $F \in \mathbb{Z}[X]$ be a monic polynomial of degree d. Suppose that there exists primes p_1, p_2, p_3 such that*

- *F_{p_1} is irreducible over $\mathbb{F}_{p_1}$ (denoted a prime of type* I*),*
- *$F_{p_2} = g_1 g_2 \dots g_r$, where g_i is irreducible for all $i \in \{1, \dots, r\}$, $\deg g_1 = 2$, and $\deg g_i$ is odd for $i \in \{2, \dots, r\}$ (denoted a prime of type* II*),*
- *$F_{p_3} = h_1 h_2 \dots h_s$, where h_i is irreducible for all $i \in \{1, \dots, s\}$ and $\deg h_1 = \ell$ with $\ell > d/2$ a prime (denoted a prime of type* III*).*

Then F is irreducible over $\mathbb{Z}$ and the splitting field has Galois group equal to the full symmetric group $\mathfrak{S}_d$.

Proof. Since there exists a prime p_1 such that F_{p_1} is irreducible over $\mathbb{F}_{p_1}$, we immediately have that F is irreducible over $\mathbb{Z}$.

As for the Galois group, the existence of the primes p_2 and p_3 allows us to find elements of the Galois group $\mathrm{Frob}_{\mathfrak{p}_2}$ and $\mathrm{Frob}_{\mathfrak{p}_3}$, where $\mathfrak{p}_2$ and $\mathfrak{p}_3$ are primes lying above p_2 and p_3, respectively. These elements have cycle pattern equal to the factorisation pattern of F_{p_2} and F_{p_3}. Thus, let $n_1 =$

$\deg(g_2)\deg(g_3)\ldots\deg(g_r)$ and $n_2 = \deg(h_2)\deg(h_3)\ldots\deg(h_s)$. Then $\mathrm{Frob}_{\mathfrak{p}_2}^{n_1}$ is a 2-cycle and $\mathrm{Frob}_{\mathfrak{p}_3}^{n_2}$ is a ℓ-cycle, where $\ell > d/2$ is a prime.

Then, since the Galois group is a subset of the symmetric group $\mathfrak{S}_d$ which contains a 2-cycle and a ℓ-cycle, where $\ell > d/2$ is a prime, by Lemma 4.5 we have that the Galois group is equal to the symmetric group $\mathfrak{S}_d$, as desired. □

So what does this all mean for us? It allows us to confirm that the Galois group of a given polynomial F is equal to the full symmetric group by only looking at factorization patterns of F_p for various primes p. We can now fully describe the algorithm we used to study Maeda's conjecture, for the operator T_2 on the space $S_k(\mathrm{SL}(2,\mathbb{Z}))$ for a given weight k:

(1) Compute the Victor Miller basis $\mathcal{B}$ for $S_k(\mathrm{SL}(2,\mathbb{Z}))$ up to precision $2(d+2)$, where d is the dimension of $S_k(\mathrm{SL}(2,\mathbb{Z}))$.

(2) Compute the matrix M of the Hecke operator T_2 with respect to the basis $\mathcal{B}$: this is very efficient since the basis $\mathcal{B}$ is echelonized.

(3) Pick a random prime $p < 2^{20}$, uniformly over this range. (This choice of upper bound gives a large enough range so that it is likely to contain primes of type we are looking for, but not so large that the arithmetic over $\mathbb{F}_p$ gets too expensive.)

(4) Reduce M mod p and compute the characteristic polynomial $F_p \in \mathbb{F}_p[X]$. The characteristic polynomial is computed by the Linbox library (see [DGG+02]).

(5) Is F_p irreducible? If so, p is a prime of type *I*. The irreducibility test uses FLINT (see [Har10]).

(6) Factor F_p over $\mathbb{F}_p$ and use this factorization to decide whether p is a prime of type *II* or *III*. The factorization is done by FLINT.

(7) Repeat from step (3) until we have found at least one prime of each type.

This algorithm is based on the algorithm originally employed by Buzzard and

later refined by Conrey-Farmer. Our main input was to improve the choice of prime to a random method. The original method was a consecutive method, in which to find the primes of each type one would simply test the primes in order. It turns out that significant time savings can be made by using a random approach, suggesting that low primes are generally unsuitable for this purpose.

The code that we used and the data we gathered are available at

`http://bitbucket.org/aghitza/maeda_data`.

We will now make this precise by looking at the expected length of time to find primes of the desired types by a random method. That is, we must determine the density of primes of the right types within the set of all primes. For this purpose there is a very precise result known as the Theorem of Frobenius, which can be stated as follows:

Theorem 4.11 (Frobenius)**.** *Let $F \in \mathbb{Z}[X]$ be monic, let $\mathbb{K}$ be the splitting field of F and let $G = \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Then the density of primes p for which F_p has factorization pattern $d_1^{m_1} \dots d_t^{m_t}$ is equal to*

$$\frac{|\{\sigma \in G \mid \text{the cycle pattern of } \sigma \text{ is } d_1^{m_1} \dots d_t^{m_t}\}|}{|G|}. \tag{4.7}$$

In fact, when we have a specified cycle pattern, there is a specific formula for the number of elements of $\mathfrak{S}_d$ with that cycle pattern, which is given in the following:

Lemma 4.12. *Let an element σ of $\mathfrak{S}_d$ have cycle pattern $d_1^{m_1} d_2^{m_2} \dots d_t^{m_t}$, where m_i is the number of times a cycle of length d_i appears in the cycle decomposition of σ. The number of elements of $\mathfrak{S}_d$ of cycle pattern $d_1^{m_1} d_2^{m_2} \dots d_t^{m_t}$ is equal to*

$$C(d_1^{m_1} d_2^{m_2} \dots d_t^{m_t}) = \frac{d!}{\prod_{j=1}^{t} \left(d_j^{m_j} m_j!\right)}. \tag{4.8}$$

However, in many of our cases, we do not know the precise cycle pattern, only certain restrictions which still could correspond to multiple patterns.

For example, for a prime of type II we only have one cycle specified (a 2-cycle), while the others could be anything as long as they are odd order. Still, we can find precise statements for the density of each type of prime as follows. We provide a proof of the formula for primes of type I as an example of how one can use Lemma 4.12. Proofs of the formulas for the other prime types can be found in [GM12].

Proposition 4.13. *The density of primes of type I is*

$$D_I(d) = \frac{1}{d}. \tag{4.9}$$

Proof. Primes of type I correspond to d-cycles in $\mathfrak{S}_d$. Each such cycle can be written uniquely as a sequence $1, a_1, \ldots, a_{d-1}$, where $a_1, \ldots, a_{d-1} \in \{2, \ldots, d\}$ can appear in any order. Therefore there are $(d-1)!$ d-cycles, and by Theorem 4.11, the density of primes of type I is

$$\frac{(d-1)!}{d!} = \frac{1}{d}. \tag{4.10}$$

□

In order to state our result on primes of type II, we will use the *double factorial* $n!!$ of n, which is defined to be the product of all the odd positive integers less than or equal to n.

Proposition 4.14. *Let $d > 2$ and let $\tilde{d}$ be the largest even integer such that $\tilde{d} \leq d$. The density of primes of type II is given by*

$$D_{II}(d) = \frac{[(\tilde{d}-3)!!]^2}{2(\tilde{d}-2)!} \tag{4.11}$$

and satisfies the inequality

$$D_{II}(d) > \frac{1}{4\sqrt{d}}. \tag{4.12}$$

Proposition 4.15. *The density of primes of type III is*

$$D_{III}(d) = \sum_{d/2 < \ell \leq d,\, \ell \text{ prime}} \frac{1}{\ell}. \tag{4.13}$$

If $d > 2$, then

$$D_{III}(d) > \frac{1}{d}. \tag{4.14}$$

We can get a much better lower bound on the density D_{III} by using some recent results of Dusart on explicit estimates for sums over primes.

Theorem 4.16 (Dusart, Theorem 6.10 in [Dus10])**.** *Let $B \approx 0.26149$ denote the Meissel-Mertens constant. For all $x > 1$ we have*

$$\log\log x + B - \left(\frac{1}{10\log^2 x} + \frac{4}{15\log^3 x}\right) \leq \sum_{p \leq x} \frac{1}{p}. \tag{4.15}$$

We will also need an upper bound on the sum of the reciprocals of primes up to x, but Dusart's upper bound only holds for $x \geq 10372$. For our purposes, the following weaker result is sufficient: for all $x > 1$ we have

$$\sum_{p \leq x} \frac{1}{p} \leq \log\log x + B + \frac{1}{\log^2 x}. \tag{4.16}$$

(This inequality can be found in Theorem 8.8.5 of [BS96].)

Proposition 4.17. *If $d > 10$, then*

$$D_{III}(d) > \frac{1}{3\log d}. \tag{4.17}$$

We now state the main result we have achieved through this algorithm

Theorem 4.18. *Let $k \leq 14\,000$ and let*

$$\begin{aligned} n \in &\{2, ..., 10\,000\} \cup \{p \text{ prime} \mid 2 \leq p \leq 4\,000\,000\} \\ &\cup \{p \text{ prime} \mid p \equiv 1 \pmod 5\} \cup \{p \text{ prime} \mid p \equiv 1 \pmod 7\}. \end{aligned}$$

Let F be the characteristic polynomial of the Hecke operator T_n acting on the space $S_k(\mathrm{SL}(2,\mathbb{Z}))$ of cusp forms of weight k and level 1. Then F is irreducible over $\mathbb{Q}$ and the Galois group of its splitting field is the full symmetric group $\mathfrak{S}_d$, where d is the dimension of the space $S_k(\mathrm{SL}(2,\mathbb{Z}))$.

Proof. The statement for T_2 is the result of our computations. The statement for T_n for other values of n follows from applying Theorem 4.1 and Theorem 4.3. □

5 Siegel Modular Forms

5.1 Introduction

We are interested in how conjecture 1.2 behaves as we modify the conditions. It transpires that there exist modular forms attached to groups other than $\mathrm{SL}(2,\mathbb{Z})$). The theory of Siegel modular forms replaces the group $\mathrm{SL}(2,\mathbb{Z})$ with the group $\mathrm{Sp}(2g,\mathbb{Z})$. In this case Maeda's Conjecture displays some interesting properties.

5.2 Preliminaries

We begin with the basic definitions in the theory of Siegel modular forms.

The *symplectic group* is the matrix group

$$\mathrm{Sp}(2g,\mathbb{Z}) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M_{2g\times 2g}(\mathbb{Z}) \;\middle|\; \begin{array}{l} A,B,C,D \in M_g(\mathbb{Z}) \\ AB^\top = BA^\top,\ CD^\top = DC^\top, \\ \text{and } AD^\top - BC^\top = I \end{array} \right\}. \tag{5.1}$$

This group does not act on the upper half plane $\mathcal{H}$ as the group $\mathrm{SL}(2,\mathbb{Z})$ does. It acts on what is called the *Siegel upper half space*, which is defined as

$$\mathcal{H}_g = \{Z \in M_g(\mathbb{C}) \mid Z^\top = Z,\ \mathrm{Im}(Z) > 0\}. \tag{5.2}$$

In the above, the notation $\mathrm{Im}(Z) > 0$ is taken to mean that the matrix made by taking the imaginary part of each entry of Z is positive-definite.

The action of an element $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}(2g,\mathbb{Z})$ on $Z \in \mathcal{H}_g$ is defined by

$$Z \;\longmapsto\; \gamma Z = (AZ+B)(CZ+D)^{-1}. \tag{5.3}$$

In the theory of classical modular forms, we have a factor of automorphy $(cz+d)^k$. To generalise this, we introduce the following notion:

Definition 5.1 (Representation)**.** A *representation* ρ of a group G on a vector space V is a group homomorphism

$$\rho : G \longrightarrow \mathrm{GL}(V) \tag{5.4}$$

where $\mathrm{GL}(V)$ is the group of automorphisms of V.

We can now define the focal object of study in the theory:

Definition 5.2 (Siegel modular form)**.** Let $\rho : \mathrm{GL}(g, \mathbb{C}) \to \mathrm{GL}(V)$ be a representation of $\mathrm{GL}(g, \mathbb{C})$ on a finite dimensional $\mathbb{C}$-vector space V. A *Siegel modular form of weight* ρ is a holomorphic function $f : \mathcal{H}_g \to V$ such that

(1) $f(\gamma Z) = \rho(CZ + D)f(Z)$ for all $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}(2g, \mathbb{Z})$ and $Z \in \mathcal{H}_g$,

(2) if $g = 1$ then f is holomorphic at ∞.

Note that condition (2) is only required if $g = 1$. If $g > 1$, this is immediately satisfied, due to the Koecher principle (Theorem 4.4 in [vdG06]).

An interesting special case is that of *scalar-valued* Siegel modular forms. These arise by restricting our attention to powers of the determinant representation, i.e.

$$\begin{array}{rccc} \det^k : & \mathrm{GL}(g, \mathbb{C}) & \longrightarrow & \mathbb{C}^* \\ & M & \longmapsto & \det(M)^k \end{array} \tag{5.5}$$

where $\mathbb{C}^*$ is the multiplicative group of nonzero complex numbers. From this we get the following:

Definition 5.3 (Scalar-Valued Siegel modular form)**.** A *scalar-valued Siegel modular form of weight* k *and genus* g is a holomorphic $f : \mathcal{H}_g \to \mathbb{C}$ such that

(1) $f(\gamma Z) = \det(CZ + D)^k f(Z)$ for all $\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}(2g, \mathbb{Z})$ and $Z \in \mathcal{H}_g$,

(2) if $g = 1$ then f is holomorphic at ∞.

Note that these forms again form a vector space for a fixed weight. On this vector space, there is in fact an inner product, given by the following:

Definition 5.4 (Petersson Inner Product)**.** Let $F_1, F_2 \in M_k(\mathrm{Sp}(2g, \mathbb{Z}))$ such that at least one is a cusp form. Then the *Petersson inner product* of F_1 and F_2 is given by

$$\langle F_1, F_2 \rangle = \int_{\mathrm{Sp}(2g,\mathbb{Z})\backslash\mathcal{H}_g} \det(Y)^k F_1(Z)\overline{F_2(Z)}dZ, \tag{5.6}$$

where

- $Z = X + iY$, $X = (x_{ij})$, $Y = (y_{ij})$,
- $dZ = \det(y)^{-(g+1)} \prod_{i \leq j} dx_{ij} dy_{ij}$ is an $\mathrm{Sp}(2g, \mathbb{Z})$-invariant measure on $\mathcal{H}_g$ (see proposition 2.9 in Chapter 1 of [AZ95]), and
- the integral converges absolutely because of our assumption that at least one of F_1 and F_2 is a cusp form (see Lemma 5.2 and Theorem 5.3 in Chapter 2 of [AZ95]).

In fact, there is a similar inner product on the space of elliptic modular forms. We did not define it in our discussion of elliptic modular forms since our use will be to look at the orthogonal complement of certain subspaces of the space of Siegel cusp forms (defined below). However, in the elliptic case we simply looked at the whole of $S_k(\mathrm{SL}(2, \mathbb{Z}))$ at once.

5.3 Genus two

5.3.1 Definition and generators

In the above definition, if we consider $g = 1$, we get $\mathrm{Sp}(2, \mathbb{Z}) = \mathrm{SL}(2, \mathbb{Z})$ and $\mathcal{H}_1 = \mathcal{H}$. Thus this reduces to the case of classic elliptic modular forms. So the first case of the theory in which we see something new occurs for genus $g = 2$. Specifically, we wish to consider the case of genus 2 *scalar-valued* Siegel modular forms.

In this case there is a large body of results and computational techniques. We primarily follow [Sko92]. As in the elliptic case, for a fixed weight k we get a finite dimensional vector space $M_k(\mathrm{Sp}(4,\mathbb{Z}))$ with a subspace of cusp forms $S_k(\mathrm{Sp}(4,\mathbb{Z}))$. Taking a direct sum over even weights, these forms form a graded algebra

$$M_* = \bigoplus_{k \text{ even}} M_k(\mathrm{Sp}(4,\mathbb{Z})). \tag{5.7}$$

As with the elliptic case, we have a finite algebraic generating set for the algebra. This is given in the following theorem of Igusa:

Theorem 5.5 (Igusa)**.** *Let $\psi_4, \psi_6, \chi_{10}, \chi_{12}$ be nonzero forms in the one-dimensional spaces $M_4(\mathrm{Sp}(4,\mathbb{Z})), M_6(\mathrm{Sp}(4,\mathbb{Z})), S_{10}(\mathrm{Sp}(4,\mathbb{Z})), S_{12}(\mathrm{Sp}(4,\mathbb{Z}))$, respectively. Then*

$$M_*(\mathrm{Sp}(4,\mathbb{Z})) = \bigoplus_{k \text{ even}} M_k(\mathrm{Sp}(4,\mathbb{Z})) = \mathbb{C}[\psi_4, \psi_6, \chi_{10}, \chi_{12}], \tag{5.8}$$

i.e. the modular forms $\psi_4, \psi_6, \psi_{10}, \psi_{12}$ are algebraically independent and any element of $M_*(\mathrm{Sp}(4,\mathbb{Z}))$ can be written as a polynomial in these functions.

An immediate consequence of the theorem is that $\dim M_k(\mathrm{Sp}(4,\mathbb{Z})) = 0$ for $k = 0, 2$.

Remark 5.6. Unlike the elliptic case, there do exist Siegel modular forms of odd weight in level 1, which occur if and only if the genus g is even. For genus 2, the form of odd weight in the generating set is χ_{35}, and there exists a polynomial R in the even weight generators such that $\chi_{35}^2 = R$. Thus if we wish to consider only even weight forms, we do not need to worry about χ_{35}.

5.3.2 Fourier expansion

As in the elliptic case, we look to express forms as a series expansion. In the case $g = 1$, this follows from the action of the matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ implying that the forms are $\mathbb{Z}$-periodic and allowing us to make use of Fourier analysis. This gives us an expression for the form as a series indexed over $\mathbb{Z}$.

In the genus 2 case we consider the matrix

$$\gamma = \left(\begin{array}{cc|cc} 1 & 0 & \multicolumn{2}{c}{\multirow{2}{*}{S}} \\ 0 & 1 & & \\ \hline 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \tag{5.9}$$

which is an element of $\mathrm{Sp}(4,\mathbb{Z})$ if and only if $S \in M_{2\times 2}(\mathbb{Z})$ is symmetric. Then let $f \in M_k(\mathrm{Sp}(4,\mathbb{Z}))$. Substituting this into the modularity condition for f, we have that

$$f(Z+S) = f(\gamma Z) = \det(\mathbf{0}Z + I)^k f(Z) = f(Z) \tag{5.10}$$

where

$$\mathbf{0} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \quad \text{and} \quad I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{5.11}$$

So we have that f is periodic in all the individual entries of the argument Z. In fact, the restrictions on $\mathcal{H}_2$ and the symmetric matrices in $M_{2\times 2}(\mathbb{Z})$ mean that these entries form a space of dimension 3, so the Fourier expansion is indexed over triples $A = [a,b,c] \in \mathbb{Z}^3$ corresponding to semi-positive definite quadratic forms $aX^2 + bXY + cY^2$. So we have the conditions $a \geq 0$ and $b^2 - 4ac \leq 0$. Thus we let

$$Q = \{A = [a,b,c] \in \mathbb{Z}^3 \mid b^2 - 4ac \leq 0,\ a \geq 0\}. \tag{5.12}$$

So we have that a Siegel modular form $f \in M_k(\mathrm{Sp}(4,\mathbb{Z}))$ has a Fourier expansion given by

$$f(Z) = \sum_{A=[a,b,c]\in Q} C_f(A) e(a\tau + bz + c\tau') \tag{5.13}$$

where

- $e(x) = e^{2\pi i x}$,
- $C_f(A) \in \mathbb{C}$, and
- $Z = \begin{pmatrix} \tau & z \\ z & \tau' \end{pmatrix}$ with $\tau, \tau' \in \mathcal{H}$ and $z \in \mathbb{C}$.

Further, these can be represented by matrices $M_A = \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix}$. Thus we have

$$f(Z) = \sum_{A \in Q} C_f(A) e(\mathrm{tr}(Z M_A)). \tag{5.14}$$

5.3.3 Important forms

We now wish to construct some useful examples of Siegel modular forms, motivated by the classical examples of the elliptic case. Specifically, we would like to know if there are analogous theories for cusp forms and Eisenstein series.

One way to define cusp forms is to say that $f \in M_k(\mathrm{Sp}(4,\mathbb{Z}))$ is a cusp form if $C_f(A) = 0$ for all singular (i.e. non-invertible) matrices A. However, the coefficients $C_f(A)$ are not independent. In fact we have

$$C_f(B \cdot A) = \det(B)^k B \cdot C_f(A), \tag{5.15}$$

for all $A \in \mathrm{GL}(2,\mathbb{Z})$ such that $\begin{pmatrix} (A^{-1})^T & \mathbf{0} \\ \mathbf{0} & A \end{pmatrix} \in \mathrm{Sp}(4,\mathbb{Z})$. So a more common approach is to define the following function, called the *Siegel* Φ*-operator* which maps Siegel modular forms of genus 2 to genus 1 (i.e. elliptic) modular forms. It is given by the following formula:

$$\begin{array}{ccccc} \Phi: & M_k(\mathrm{Sp}(4,\mathbb{Z})) & \longrightarrow & M_k(\mathrm{SL}(2,\mathbb{Z})) \\ & f(Z) = \sum_{A \in Q} C_f(A) e^{\mathrm{tr}(Z M_A)} & \longmapsto & \Phi(f)(q) = \displaystyle\sum_{n=0}^{\infty} C_f([0,0,n]) q^n. \end{array} \tag{5.16}$$

A *cusp form* $f \in M_k(\mathrm{Sp}(4,\mathbb{Z}))$ is then a Siegel modular form such that $\Phi(f) = 0$. That is, it lies in the kernel of the Siegel Φ-operator. The subspace of weight k cusp forms is denoted $f \in S_k(\mathrm{Sp}(4,\mathbb{Z}))$. In fact, there is an alternative characterization given as follows

Proposition 5.7. *Let $f \in M_k(\mathrm{Sp}(4,\mathbb{Z}))$. Then $f \in S_k(\mathrm{Sp}(4,\mathbb{Z}))$ if and only if there exist modular forms $g \in M_{k-10}(\mathrm{Sp}(4,\mathbb{Z}))$ and $h \in M_{k-12}(\mathrm{Sp}(4,\mathbb{Z}))$*

such that

$$f = g\chi_{10} + h\chi_{12}. \tag{5.17}$$

Proof. First we note that of the Igusa generators, χ_{10} and χ_{12} are cusp forms, while ψ_4 and ψ_6 are not. This is a result of Theorem 5.11, Proposition 5.12 and the formulae given in equation (5.29).

($\Leftarrow$) : We have that $f = g\chi_{10} + h\chi_{12}$. We thus compute the desired Fourier coefficients by

$$\begin{aligned} C_f([0,0,n]) &= \sum_{k=0}^{n} (C_g([0,0,k])C_{\chi_{10}}([0,0,n-k]) + C_h([0,0,k])C_{\chi_{12}}([0,0,n-k])) \\ &= \sum_{k=0}^{n} (C_g([0,0,k])0 + C_h([0,0,k])0) = 0. \end{aligned}$$

Thus $f \in S_k(\mathrm{Sp}(4,\mathbb{Z}))$, as required.

($\Rightarrow$) : Assume it is not the case that f can be represented as stated above. Then we will have that

$$f = g_1\chi_{10} + g_2\chi_{12} + g_3 \tag{5.18}$$

where $g_1 \in M_{k-10}(\mathrm{Sp}(4,\mathbb{Z}))$, $g_2 \in M_{k-12}(\mathrm{Sp}(4,\mathbb{Z}))$ and g_3 is a polynomial expression in the generators ψ_4 and ψ_6. However, we have that

$$\begin{aligned} C_f([0,0,n]) &= C_{g_1\chi_{10}}([0,0,n]) + C_{g_2\chi_{12}}([0,0,n]) + C_{g_3}([0,0,n]) \\ &= 0 + 0 + C_{g_3}([0,0,n]) = C_{g_3}([0,0,n]), \end{aligned}$$

and based on the Fourier expansions of ψ_4 and ψ_6, there exists no polynomial such that you can have the $[0,0,n]$ coefficient equal to zero for all $n \in \mathbb{Z}_{\geq 0}$. Thus $f \notin S_k(\mathrm{Sp}(4,\mathbb{Z}))$, as required.

□

As for Eisenstein Series, they are defined in a completely analogous way to elliptic modular forms. That is, for $M_k(\mathrm{Sp}(4,\mathbb{Z}))$, $k \geq 4$, the *weight-k*

Eisenstein Series is defined by

$$E_k(Z) = \sum_{\{C,D\}} \det(CZ + D)^{-k}, \tag{5.19}$$

where the sum is indexed over $C, D \in M_{2\times 2}(\mathbb{Z})$ such that C and D are coprime and nonassociated (under left multiplication by $\mathrm{GL}(2,\mathbb{Z})$). Two integral matrices are said to be *coprime* if whenever GC and GD are both integral, then G is an integral matrix.

We can also compute the Fourier expansions of these Eisenstein Series. First we must define *Cohen's function*, which is given by

$$H(k-1,N) = \begin{cases} 0, & \text{if } N \not\equiv 0,3 \pmod 4 \\ \zeta(3-2k), & \text{if } N = 0 \\ L(2-k, \left(\frac{-N_0}{\cdot}\right))H_0(k-1,N), & \text{if } N \equiv 0,3 \pmod 4 \text{ and } N \neq 0 \end{cases} \tag{5.20}$$

where

$$H_0(k-1,N) = \sum_{d|f} \mu(d) \left(\frac{-N_0}{d}\right) d^{k-2}\sigma_{2k-3}(f/d) \tag{5.21}$$

and N has been written $N = N_0 f^2$ with $f \in \mathbb{N}$, where N_0 is the discriminant of $\mathbb{Q}(\sqrt{-N})$. Further, $\sigma_k(n) = \sum_{d|n} d^k$ is the divisor function and $L(s,\chi)$ is the Dirichlet L-function, attached to the Dirichlet character χ,

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}. \tag{5.22}$$

The character χ appearing in equations (5.20) and (5.21) is the quadratic character of $\mathbb{Q}(\sqrt{-N})$, i.e. the quadratic residue symbol $\left(\frac{N_0}{\cdot}\right)$.

Now we have that the Fourier coefficients of the Eisenstein series E_k are given by

$$C_{E_k}([a,b,c]) = \sum_{d|\gcd(a,b,c)} d^{k-1} H\left(k-1, \frac{4ac-b^2}{d^2}\right). \tag{5.23}$$

Remark 5.8. If we consider the image of E_k under the Siegel Φ-operator, we note that $C_{E_k}([0,0,n]) = \zeta(3-2k)\sigma_k(n)$, which is precisely the nth coefficient

of the weight-k Eisenstein series in degree 1. In fact, for any genus we have that the Siegel Φ-operator maps Eisenstein series to Eisenstein series.

5.3.4 Maaß lifts

At this stage we would like to know the extent to which we are able to use classical results from the theory of elliptic modular forms in the theory of Siegel modular forms. In fact, many examples of Siegel modular forms arise as "lifts" of elliptic modular forms. That is, they lie in the image of Hecke equivariant linear embeddings from elliptic to Siegel forms.

To define these lifts, we first require the following notion:
Definition 5.9 (Jacobi Form)**.** A *Jacobi form* of level 1, weight k and index 1 is a function $\phi : \mathcal{H}_1 \times \mathbb{C} \to \mathbb{C}$ such that

1. $\phi\left(\frac{a\tau+b}{c\tau+d}, \frac{z}{c\tau+d}\right) = (c\tau+d)^k e^{\frac{2\pi i c z^2}{c\tau+d}} \phi(\tau, z)$ for $\tau \in \mathcal{H}_1$, $z \in \mathbb{C}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$;
2. $\phi(\tau, z + \lambda\tau + \mu) = e^{-2\pi i(\lambda^2\tau + 2\lambda z)} \phi(\tau, z)$ for all $\lambda, \mu \in \mathbb{Z}$; and
3. ϕ has a Fourier expansion of the form

$$\phi(\tau, z) = \sum_{n=0}^{\infty} \sum_{r^2 \leq 4n} d(n, r) q^n \zeta^r, \tag{5.24}$$

where $q = e^{2\pi i\tau}$ and $\zeta = e^{2\pi iz}$.

We write $J_k(\mathrm{SL}(2, \mathbb{Z}))$ to mean the space of such Jacobi forms of weight k and index 1 (we do not need to be concerned with higher index forms for our purposes). Let the subspace of Jacobi cusp forms, which are forms in which the Fourier coefficients $d(n, r) = 0$ whenever $r^2 = 4mn$, be denoted $S_k^J(\mathrm{SL}(2, \mathbb{Z}))$. Note that any Jacobi form $\phi \in J_k(\mathrm{SL}(2, \mathbb{Z}))$ can have their series expansion represented by:

$$\phi(\tau, z) = \sum_{\substack{D, r \in \mathbb{Z}, D \leq 0 \\ D \equiv r^2 \bmod 4}} C_\phi(D) q^{(r^2 - D)/4} \zeta^r, \tag{5.25}$$

where $q^{2\pi i\tau}$, $\zeta = e^{2\pi iz}$, for $\tau \in \mathcal{H}$ and $z \in \mathbb{C}$.

We now define a Maaß lift as follows:

Definition 5.10 (Maaß Lift, see [Sko92], p. 384)**.** For any integer $k \geq 0$, let the *Maaß Lift*, V, be the map

$$\begin{array}{ccccc} V: & J_k(\mathrm{SL}(2,\mathbb{Z})) & \longrightarrow & M_k(\mathrm{Sp}(4,\mathbb{Z})) \\ \phi = & \sum\limits_{\substack{D,r\in\mathbb{Z},D\leq 0\\ D\equiv r^2 \bmod 4}} C_\phi(D) q^{(r^2-D)/4}\zeta^r & \longmapsto & \sum\limits_{\substack{n,r,m\in\mathbb{Z}\\ r^2-4mn\leq 0\\ n,m\geq 0}} a(n,r,m) q^n \zeta^r (q')^m, \end{array} \tag{5.26}$$

where $q = e^{2\pi i\tau}$, $\zeta = e^{2\pi iz}$, $q' = e^{2\pi i\tau'}$, and

$$a(n,r,m) = \sum_{a\,|\,\gcd(n,r,m)} a^{k-1} C_\phi\left(\frac{r^2-4mn}{a^2}\right) \tag{5.27}$$

and $a(0,0,0) = -(B_{2k}/4k)C_\phi(0)$.

Theorem 5.11. *V defines a Hecke invariant embedding which maps cusp forms to cusp forms, and Eisenstein series to Eisenstein series.*

For this theorem, we need to know what the Hecke Operators are on the spaces $J_k(\mathrm{SL}(2,\mathbb{Z}))$ and $M_k(\mathrm{Sp}(4,\mathbb{Z}))$, this is outlined in subsection 5.4.

Any Siegel modular form which is the image of a Jacobi form under the above embedding is called a *Maaß Spezialform*. However, we needn't concern ourselves too greatly with the theory of Jacobi forms. The following proposition allows us to construct $J_k(\mathrm{SL}(2,\mathbb{Z}))$ from elliptic modular forms, and thus bypass the theory entirely in favour of the elliptic case:

Proposition 5.12 (See [Sko92], p. 384)**.** *Let*

$$A = \Delta^{-1/4} \sum_{\substack{r,s\in\mathbb{Z}\\ r\not\equiv \bmod 2}} s^2(-1)^r q^{(s^2+r^2)/4}\zeta^r,$$

$$B = \Delta^{-1/4} \sum_{\substack{r,s\in\mathbb{Z}\\ r\not\equiv \bmod 2}} (-1)^r q^{(s^2+r^2)/4}\zeta^r,$$

where $\Delta = q\prod_{n=1}^{\infty}(1-q^n)^{24}$. *Then, for any integer* k, *the map*

$$\begin{array}{rccc} I: & M_k(\mathrm{SL}(2,\mathbb{Z}))\oplus S_{k+2}(\mathrm{SL}(2,\mathbb{Z})) & \xrightarrow{\sim} & J_k(\mathrm{SL}(2,\mathbb{Z})) \\ & (f,g) & \longmapsto & \dfrac{k}{2}fA-\left(q\dfrac{d}{dq}f\right)B+gB \end{array} \tag{5.28}$$

is a Hecke equivariant isomorphism of $\mathbb{C}$*-vector spaces.*

An important remark is that the Jacobi form $I(f,g)$ is a cusp form if and only if f is a cusp form. Thus we have an isomorphism between $S_k(\mathrm{SL}(2,\mathbb{Z}))\oplus S_{k+2}(\mathrm{SL}(2,\mathbb{Z}))$ and the space of Jacobi cusp forms.

Thus the composition map $V\circ I$ is a linear Hecke invariant embedding of elliptic modular forms attached to $\mathrm{SL}(2,\mathbb{Z})$ into Siegel modular forms attached to $\mathrm{Sp}(4,\mathbb{Z})$. In fact, the generators given in Theorem 5.5 are all Maaß Spezialformen, given as follows:

$$\begin{array}{ll} \psi_4 = V(I(E_4,0)), & \psi_6 = V(I(E_6,0)), \\ \chi_{10} = V(I(0,-\Delta)), & \chi_{12} = V(I(\Delta,0)). \end{array} \tag{5.29}$$

Remark 5.13. The composition map $V\circ I$ is linear (i.e. a morphism of vector spaces), but not a ring morphism. That is, the product of two Maaß Spezialformen need not be a Maaß Spezialform itself.

We now have some good fundamentals for explicit computation of Siegel modular forms. Coefficients in the Fourier expansion of any form can be computed via multiplication of the above generators. The Fourier expansions of these generators are computed via composition of the formulas given in Theorem 5.11 and Proposition 5.12.

5.4 Hecke operators for ...

5.4.1 ... Elliptic modular forms

This is the classical case of the Hecke Operators. It is covered in greater depth in section 3.

We start with the action of an element of $\mathrm{GL}(2,\mathbb{Q})^+$ on an elliptic modular form, which is given by

$$f|_\gamma(z) = (\det\gamma)^{k/2}(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right). \tag{5.30}$$

This allows us to define the action of a double coset in $\mathrm{SL}(2,\mathbb{Z})\backslash\mathrm{GL}(2,\mathbb{Q})^+/\mathrm{SL}(2,\mathbb{Z})$. First, we have the following result.

Lemma 5.14. *Let $\alpha \in \mathrm{GL}(2,\mathbb{Q})^+$. Then the double coset $\mathrm{SL}(2,\mathbb{Z})\alpha\mathrm{SL}(2,\mathbb{Z})$ is a finite union of right cosets*

$$\mathrm{SL}(2,\mathbb{Z})\alpha\mathrm{SL}(2,\mathbb{Z}) = \bigcup_{i=1}^{n} \mathrm{SL}(2,\mathbb{Z})\alpha_i, \qquad \alpha_i \in \mathrm{GL}(2,\mathbb{Q})^+. \tag{5.31}$$

Proof. See [Bum98], Proposition 1.4.1. □

Now we define the Hecke Operator T_α attached to an element $\alpha \in \mathrm{GL}(2,\mathbb{Q})^+$ by

$$T_\alpha f = \sum_{i=1}^{n} f|_{\alpha_i}, \tag{5.32}$$

where the α_i are as given in Lemma 5.14. To define Hecke Operators of the type T_n, we will first consider the set

$$\Delta_n = \{\gamma \in \mathrm{GL}(2,\mathbb{Q})^+ \mid \det\gamma = n\}, \tag{5.33}$$

which has a decomposition given by the following result.

Lemma 5.15. *We have*

$$\mathrm{SL}(2,\mathbb{Z})\Delta_n\mathrm{SL}(2,\mathbb{Z}) = \bigcup_{\substack{a,d>0, ad=n \\ 0\le b<n}} \mathrm{SL}(2,\mathbb{Z}) \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}. \tag{5.34}$$

If we express the above decomposition as $\mathrm{SL}(2,\mathbb{Z})\Delta_n\mathrm{SL}(2,\mathbb{Z}) = \bigcup_j \mathrm{SL}(2,\mathbb{Z})\delta_{n,j}$, we then see that

$$T_n f = \sum_j f|_{\delta_{n,j}}. \tag{5.35}$$

The ideal of cusp forms is invariant under the action of the Hecke Operators.

For computation purposes, we wish to know the explicit effect of the T_n operators on the Fourier expansions of Cusp Forms. This is given as follows

Theorem 5.16. *Let $f \in S_k(\mathrm{SL}(2,\mathbb{Z}))$ have Fourier expansion $f(z) = \sum_{m=1}^{\infty} a_m q^m$. Then*

$$(T_n f)(z) = \sum_{m=1}^{\infty} \left(\sum_{d \mid \gcd(m,n)} d^{k-1} a_{mn/d^2} \right) q^m \tag{5.36}$$

5.4.2 ... Siegel modular forms

We will begin with the purely general definition for vector-valued Siegel modular forms of any genus and then restrict to the scalar-valued genus 2 case when it comes to finding an expression for the action on the Fourier coefficients. Analogously to the case of elliptic modular forms, we have the action of a Hecke Algebra. In this case, we consider the Hecke Algebra of double cosets of $\mathrm{Sp}(2g,\mathbb{Z})$ in the matrix group

$$\mathrm{GSp}(2g,\mathbb{Q}) = \left\{ \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in M_{2g}(\mathbb{Q}) \;\middle|\; \begin{array}{l} A,B,C,D \in M_g(\mathbb{Q}) \\ AB^\top = BA^\top, \text{ and } CD^\top = DC^\top \end{array} \right\}. \tag{5.37}$$

Within this, there is a subgroup

$$\mathrm{GSp}(2g,\mathbb{Q})^+ = \{\gamma \in \mathrm{GSp}(2g,\mathbb{Q}) \mid \det\gamma > 0\}. \tag{5.38}$$

The operators are defined in a completely analogous way to those acting on the space of elliptic modular forms. That is, we define the action of an element $\gamma \in \mathrm{GSp}(2g,\mathbb{Q})^+$ by

$$f|_\gamma(Z) = \rho(CZ+D)^{-1} f(\gamma Z), \quad \text{where } \gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix}. \tag{5.39}$$

As in the elliptic case, for $\gamma \in \mathrm{GSp}(2g,\mathbb{Q})^+$, there exist $\{\gamma_i\}_{i=1}^N \subseteq \mathrm{GSp}(2g,\mathbb{Q})^+$ such that

$$\mathrm{Sp}(2g,\mathbb{Z})\gamma\mathrm{Sp}(2g,\mathbb{Q}) = \bigcup_{i=1}^{N} \mathrm{Sp}(2g,\mathbb{Z})\gamma_i. \tag{5.40}$$

(See [vdG06], Lemma 16.1) So we now define the action of the Hecke Operator T_γ by

$$T_\gamma f = \sum_{i=1}^{N} f|_{\gamma_i}, \tag{5.41}$$

where the γ_i are as in equation (5.40). Now we define

$$T_n f = \sum_{j=1}^{N} f|_{\delta_{n,j}}, \tag{5.42}$$

where $\mathrm{Sp}(2g,\mathbb{Z})\Delta_n\mathrm{Sp}(2g,\mathbb{Q}) = \bigcup_j \mathrm{SL}(2,\mathbb{Z})\delta_{n,j}$, where

$$\Delta_n = \{\gamma \in \mathrm{GSp}(2g,\mathbb{Q})^+ \mid \det\gamma = n\}. \tag{5.43}$$

In the scalar-valued genus 2 case, we would like a formula for the Fourier coefficients of the image of a form under the action of a Hecke Operator, in terms of the coefficients of the original form. In this case we have the following result:

Theorem 5.17 (See [Sko92], p. 386)**.** *Let $k, \ell \in \mathbb{Z}$ and $\ell \geq 1$. Let*

$$F = \sum_{Q=[n,r,m]\geq 0} a(Q)q^n\zeta^r(q')^m \quad \textit{and} \quad T_\ell F = \sum_{Q=[n,r,m]\geq 0} a^*(Q)q^n\zeta^r(q')^m, \tag{5.44}$$

where $F \in M_k(\mathrm{Sp}(4,\mathbb{Z}))$ and T_ℓ denotes the ℓth Hecke operator on this space. Then

$$a^*(Q) = \sum_{t_2|t_1|\ell} t_1^{k-2}t_2^{k-1} \sum_{\substack{V\in\Gamma_0(t_1/t_2)\backslash\mathrm{SL}(2,\mathbb{Z}) \\ Q((X,Y)V)=[n',r',m'] \\ t_1|n',t_2|r',m'}} a\left(\left[\frac{\ell n'}{t_1^2}, \frac{\ell r'}{t_1t_2}, \frac{\ell m'}{t_2^2}\right]\right) \tag{5.45}$$

where the inner sum is over a set of representatives for $\Gamma_0(t_1/t_2) \setminus \mathrm{SL}(2,\mathbb{Z})$ satisfying the stated conditions, and where

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \;\middle|\; c \equiv 0 \pmod{N} \right\}. \tag{5.46}$$

As in the elliptic case, the ideal of cusp forms is invariant under the action of the Hecke Operators.

5.4.3 ... Jacobi modular forms

We include this case of Hecke Theory so that one may confirm the Hecke equivariance of the Maass lifts from Elliptic modular forms to Siegel modular forms. To that end, we will directly provide the definition of T_ℓ for $\ell \in \mathbb{Z}_{>0}$

and then provide the formula for the Fourier coefficients of the image of a Jacobi form under the action of a Hecke Operator.

Definition 5.18 (Hecke Operator on $J_{k,m}(\mathrm{SL}(2,\mathbb{Z}))$)**.** Let $\phi \in J_{k,m}(\mathrm{SL}(2,\mathbb{Z}))$. We define the Hecke Operator T_ℓ by

$$T_\ell \phi = \ell^{k-4} \sum_{\substack{M \in \Gamma_1 \backslash M_2(\mathbb{Z}) \\ \det M = \ell^2 \\ \exists n \in \mathbb{Z} \text{ s.t. } \gcd(M) = n^2}} \sum_{X \in \mathbb{Z}^2/\ell\mathbb{Z}^2} (\phi|_{k,m} M)|_m X, \tag{5.47}$$

where

$$\left(\phi|_{k,m} \begin{pmatrix} a & b \\ c & d \end{pmatrix}\right)(\tau, z) = (c\tau + d)^{-k} e^m \left(\frac{-cz^2}{c\tau + d}\right) \phi\left(\frac{a\tau + b}{c\tau + d}, \frac{z}{c\tau + d}\right),$$
$$(\phi|_m \begin{pmatrix} \lambda & \mu \end{pmatrix})(\tau, z) = e^m(\lambda^2\tau + 2\lambda z)\phi(\tau, z + \lambda\tau + \mu).$$

To give the formula for the Fourier coefficients, we must first define the following functions. Consider $D \in \mathbb{Z}_{\geq 0}$. This can be written as $D = D_0 f^2$ where $f \in \mathbb{Z}_{>0}$ and D_0 is the discriminant of $\mathbb{Q}(\sqrt{D})$. Let χ be the primitive Dirichlet character $(\mathrm{mod}\, D_0)$ corresponding to $\mathbb{Q}(\sqrt{D})$, i.e. the multiplicative function defined by

$$\chi(p) = \begin{cases} \left(\frac{D_0}{p}\right), & \text{if } p \text{ odd}, \\ 1, & \text{if } p = 2,\ D \equiv 1 \pmod 8, \\ -1, & \text{if } p = 2,\ D \equiv 5 \pmod 8, \\ 0, & \text{if } p = 2,\ D \equiv 0 \pmod 4 \end{cases}$$
$$\chi(-1) = \operatorname{sign} D,$$

and we now can define

$$\varepsilon_D(n) = \begin{cases} \chi(n_0)g, & \text{if } n = n_0 g^2,\ g|f,\ \gcd\left(\frac{f}{g}, n_0\right) = 1, \\ 0, & \text{if } \gcd(n, f^2) \neq \end{cases} \tag{5.48}$$

We now have the following result:

Theorem 5.19 (See [EZ85], p. 50)**.** *Let* $f(\tau, z) = \sum_{n=0}^{\infty} \sum_{r^2 \leq 4mn} d(n,r) q^n \zeta^r$ *be a Jacobi form of weight* k*, index* m*. Let* $\ell \in \mathbb{Z}_{>0}$ *be such that* $\gcd(\ell, m) = 1$*. Then we write*

$$(T_\ell f)(\tau, z) = \sum_{n=0}^{\infty} \sum_{r^2 \leq 4mn} c^*(n,r) q^n \zeta^r \tag{5.49}$$

where

$$c^*(n,r) = \sum_{a \text{ satisfying (5.51)}} \varepsilon_{r^2-4mn}(a) a^{k-2} c(n', r'), \tag{5.50}$$

and

$$\begin{aligned} a | \ell^2, \qquad & a^2 | \ell^2 (r^2 - 4mn), \\ a^{-2}\ell^2(r^2 - 4mn) &\equiv 0, 1 \pmod 4, \\ (r')^2 - 4n'm &= \ell^2 (r^2 - 4mn)/a^2, \\ ar' &\equiv \ell r \pmod{2m}. \end{aligned} \tag{5.51}$$

5.5 Studying the conjecture

5.5.1 Hecke invariant splittings

For an analogue to the conjecture, we would like to consider the characteristic polynomial of the Hecke Operator T_n on the subspace of cusp forms. In the elliptic case we have that the characteristic polynomial is irreducible. However even just in the genus 2 case, we have that there are Hecke invariant splittings due to the Maaß lifts.

Specifically, if $f \in S_k(\mathrm{Sp}(4, \mathbb{Z}))$ is a Maaß Spezialform, then $T_n f$ is also a Maaß Spezialform. Within this space is the subspace $V(S_k^J(\mathrm{SL}(2, \mathbb{Z})))$ of such forms which are also cusp forms. Since V is Hecke equivariant (that is, the map commutes with any Hecke operator T_n), we have that the subspace is fixed (but not pointwise) by the Hecke operators. This follows since if $F = V(f) \in V(S_k^J(\mathrm{SL}(2, \mathbb{Z})))$ with $f \in S_k^J(\mathrm{SL}(2, \mathbb{Z}))$, then

$$T_n F = T_n \circ V(f) = V \circ T_n(f) = V(T_n f) \in V(S_k^J(\mathrm{SL}(2, \mathbb{Z}))). \tag{5.52}$$

One can decompose the space of Siegel cusp forms as:

$$S_k(\mathrm{Sp}(4,\mathbb{Z})) = V(S_k^J(\mathrm{SL}(2,\mathbb{Z}))) \oplus S_k^?(\mathrm{Sp}(4,\mathbb{Z})), \tag{5.53}$$

where $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$ is often referred to as the space of *interesting Siegel modular forms*. The leading notation (i.e. use of a question mark) gives some insight to the lack of understanding of this subspace in the theory thus far.

We would like to say that $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$ is also fixed (again, not pointwise) under the Hecke operators. This follows from the existence of a Hecke invariant inner product with respect to which the above subspaces are orthogonal. Such an inner product is given by the *Petersson Inner Product*, see Definition 5.4. We now have the following result regarding this inner product

Lemma 5.20. *The Hecke operators are Hermitian with respect to the Petersson Inner product, and the spaces* $V(S_k^J(\mathrm{SL}(2,\mathbb{Z})))$ *and* $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$ *are orthogonal with respect to the inner product.*

Thus $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$ is also fixed under the Hecke operators and thus the decomposition

$$S_k(\mathrm{Sp}(4,\mathbb{Z})) = V(S_k^J(\mathrm{SL}(2,\mathbb{Z}))) \oplus S_k^?(\mathrm{Sp}(4,\mathbb{Z})), \tag{5.54}$$

is Hecke invariant.

Since the space $S_k(\mathrm{Sp}(4,\mathbb{Z}))$ has (in general) nontrivial Hecke invariant subspaces, the characteristic polynomial will certainly not be irreducible. This follows since if T is an operator on a vector space W with $W = A \oplus B$ and $TA \subseteq A$, $TB \subseteq B$, then with the correct choice of basis for W the matrix of T can be written as:

$$M_T = \left(\begin{array}{c|c} M_T|_A & \mathbf{0} \\ \hline \mathbf{0} & M_T|_B \end{array}\right), \tag{5.55}$$

where $\mathbf{0}$ is the zero matrix. Then the characteristic polynomial of T will be

$$\begin{aligned}\operatorname{charpoly}(T) = \operatorname{charpoly}(M_T) &= \operatorname{charpoly}\left(\begin{array}{c|c} M_T|_A & \mathbf{0} \\ \hline \mathbf{0} & M_T|_B \end{array}\right) \\ &= \operatorname{charpoly}(M_T|_A)\operatorname{charpoly}(M_T|_B) \\ &= \operatorname{charpoly}(T|_A)\operatorname{charpoly}(T|_B).\end{aligned}$$

So the characteristic polynomial will factor into a product of the characteristic polynomials of the operator restricted to the subspaces, so it will certainly be reducible. However, it is of interest to note what the circumstances for the reducibility of $\operatorname{charpoly}(T)$ are. If this is the only reason for the polynomial to be reducible, then it is in some sense "as irreducible as possible".

Thus, to remove the trivial factorisation over this splitting, we will restrict our attention to the space $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$. This leads us to suggest the following as the correct analogy for Maeda's conjecture when considering Siegel modular forms of genus 2:

Conjecture 5.21. *Let $n \in \mathbb{Z}_{>0}$, $k \in \mathbb{Z}_{>0} \setminus \{24, 26\}$[1]. Let $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$ be the space of weight k Siegel cusp forms of genus 2 which are not Maaß Spezialformen. Let f be the characteristic polynomial of the Hecke Operator T_n acting on $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$. Let K be the splitting field of f. Then*

(1) f is irreducible over $\mathbb{Q}$,

(2) the Galois group $\mathrm{Gal}(K/\mathbb{Q}) \cong \mathfrak{S}_d$, the symmetric group on d letters, where $d = \dim S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$.

5.5.2 Computing the Hecke matrix

We considered two approaches to this, which will be referred to as the "naive approach" and "Skoruppa's approach", with the second being in reference to the methods used by Skoruppa in [Sko92]. All computations were done using

[1] The reason for avoiding 24 and 26 is covered in section 5.5.2

the Siegel modular forms package for Sage currently under construction by Martin Raum, Nathan C. Ryan, Nils-Peter Skoruppa, and Gonzalo Tornaría.

Naive approach

We wish to find the characteristic polynomial of the Hecke Operator T_n acting on the space $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$. This space cannot be computed directly, since it is defined to be "the part of $S_k(\mathrm{Sp}(4,\mathbb{Z}))$ not coming from $V(S_k^J(\mathrm{SL}(2,\mathbb{Z})))$". Given this definition, we compute the space $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$ by first computing the spaces $S_k(\mathrm{Sp}(4,\mathbb{Z}))$ and $V(S_k^J(\mathrm{SL}(2,\mathbb{Z})))$. Given these, we have

$$S_k^?(\mathrm{Sp}(4,\mathbb{Z})) = S_k(\mathrm{Sp}(4,\mathbb{Z})) \Big/ V(S_k^J(\mathrm{SL}(2,\mathbb{Z}))). \tag{5.56}$$

In Sage, we compute a basis for $S_k(\mathrm{Sp}(4,\mathbb{Z}))$ using products of the Igusa generators, noting that the form $\psi_4^a\psi_6^b\chi_{10}^c\chi_{12}^d$ is a cusp form if and only if $c \geq 1$ or $d \geq 1$. Further, using Definition 5.10 and Proposition 5.12, we have explicit formulas for the Maaß lift of elliptic forms, so we can compute a basis for $V(S_k^J(\mathrm{SL}(2,\mathbb{Z})))$. This is implemented in the Sage package.

Then, for each basis element, take a number of Fourier coefficients equal to $n = \dim S_k(\mathrm{Sp}(4,\mathbb{Z}))$ (note that these are integral after a renormalisation), and treat the space as a formal $\mathbb{Q}$-vector space isomorphic to $\mathbb{Q}^n$. This allows us to compute the vector space quotient and find the space $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$.

Here we come across a difficulty. That is, Sage is rather over-zealously "helpful" when it comes to formal vector spaces, and will automatically reset your basis to something of the form $\{(1,0,0,\ldots),\ (0,1,0,\ldots),\ \ldots\}$. This is a difficulty, because we need to keep track of the Fourier coefficients so we can find which forms these arbitrary vectors actually correspond to.

Naivest approach

The difficulty above is keeping track of your basis of coefficients when you compute the quotient space. This makes it impossible to find what linear combinations of the forms we know gives us a basis for $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$. However, we needn't fully compute this space and the operator acting upon it, as all

we require is the characteristic polynomial of T_n. As observed in subsection 5.5.1, we have that

$$\text{charpoly}\left(T_n|_{S_k(\mathrm{Sp}(4,\mathbb{Z}))}\right) = \text{charpoly}\left(T_n|_{S_k^?(\mathrm{Sp}(4,\mathbb{Z}))}\right) \times \text{charpoly}\left(T_n|_{V(S_k^J(\mathrm{SL}(2,\mathbb{Z})))}\right), \tag{5.57}$$

and so rearranging this allows us to directly compute

$$\text{charpoly}\left(T_n|_{S_k^?(\mathrm{Sp}(4,\mathbb{Z}))}\right) = \frac{\text{charpoly}\left(T_n|_{S_k(\mathrm{Sp}(4,\mathbb{Z}))}\right)}{\text{charpoly}\left(T_n|_{V(S_k^J(\mathrm{SL}(2,\mathbb{Z})))}\right)}. \tag{5.58}$$

So, in full, the algorithm to find the characteristic polynomial of T_n on the space $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$ is as follows:

(1) Compute the Igusa generators $\psi_4, \psi_6, \chi_{10}, \chi_{12}$ to a precision *prec*.

(2) Find all multiples that give rise to weight k cusp forms (i.e. solve $4a + 6b + 10c + 12d = k$ for $a, b \in \mathbb{Z}_{\geq 0}$ and $c, d \in \mathbb{Z}_{>0}$).

(3) Compute these products to find a basis for the space $S_k(\mathrm{Sp}(4,\mathbb{Z}))$.

(4) Compute bases for the spaces $S_k(\mathrm{SL}(2,\mathbb{Z}))$ and $S_{k+2}(\mathrm{SL}(2,\mathbb{Z}))$.

(5) Compute the Maaß subspace $V(S_k^J(\mathrm{SL}(2,\mathbb{Z})))$ by computing $V(I(f,0))$ and $V(I(0,g))$ for each $f \in S_k(\mathrm{SL}(2,\mathbb{Z}))$ and $g \in S_{k+2}(\mathrm{SL}(2,\mathbb{Z}))$.

(6) Compute the images of the basis elements for $S_k(\mathrm{Sp}(4,\mathbb{Z}))$ and $V(S_k^J(\mathrm{SL}(2,\mathbb{Z})))$ under the action of the Hecke Operator T_n.

(7) Compute the matrices of $T_n|_{S_k(\mathrm{Sp}(4,\mathbb{Z}))}$ and $T_n|_{V(S_k^J(\mathrm{SL}(2,\mathbb{Z})))}$. To do this, we perform the following steps

   (a) Compute a number of coefficients a_i for each form f in the basis of $S_k(\mathrm{Sp}(4,\mathbb{Z}))$ equal to $n = \dim S_k(\mathrm{Sp}(4,\mathbb{Z})$ such that the vectors $(a_1, \ldots, a_n)$ are linearly independent. If too few coefficients have been computed to do this successfully, restart and increase precision.

   (b) Repeat the above for the basis of $V(S_k^J(\mathrm{SL}(2,\mathbb{Z})))$. If too few coefficients have been computed to do this successfully, restart and increase precision.

(c) Repeat the above for $T_n f$ for f in the basis of $S_k(\mathrm{Sp}(4,\mathbb{Z}))$ and $V(S_k^J(\mathrm{SL}(2,\mathbb{Z})))$, respectively. If too few coefficients have been computed to do this successfully, restart and increase precision.

(d) Consider the matrices M with columns the coefficient vectors of the forms $T_n f$, and F with columns the coefficient vectors of the forms f, for f in the basis of $S_k(\mathrm{Sp}(4,\mathbb{Z}))$. Then the matrix of $T_n|_{S_k(\mathrm{Sp}(4,\mathbb{Z}))}$ is given by MF^{-1}.

(e) Repeat the above for f in the basis of $V(S_k^J(\mathrm{SL}(2,\mathbb{Z})))$ to compute the matrix of $T_n|_{S_k(\mathrm{Sp}(4,\mathbb{Z}))}$. If too few coefficients have been computed to do this successfully, restart and increase precision.

(8) Compute charpoly $\left(T_n|_{S_k(\mathrm{Sp}(4,\mathbb{Z}))}\right)$ and charpoly $\left(T_n|_{V(S_k^J(\mathrm{SL}(2,\mathbb{Z})))}\right)$ and from that charpoly $\left(T_n|_{S_k^?(\mathrm{Sp}(4,\mathbb{Z}))}\right)$ by equation (5.58).

As for confirming irreducibility and that the Galois group is equal to the full symmetric group, we make use of Lemma 4.10, as in the elliptic case. We have implemented this algorithm in Sage, and are currently running it over a series of weights. This leads to our current result

Theorem 5.22. *Conjecture 5.21 is true for*

$$n = 2 \quad \textit{and} \quad k \in \{20, 22\} \cup ([28, 110] \cap 2\mathbb{Z}).$$

The above theorem was confirmed using a slight upgrade of the above algorithm in which we reduced the number of multiplications required for step (3). This is outlined in 5.5.3.

Weight 24 and 26

One may note that in the Theorem above, we do not claim that Conjecture 5.21 holds for weights 24 and 26. This is due to the rationality of the Fourier coefficients of the Hecke eigenforms in $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$. For weights up to 26, all the Hecke eigenforms have coefficients (and eigenvalues) in $\mathbb{Q}$, while for weights $k \geq 28$ the coefficients lie in some number field (i.e. a finite field extension of $\mathbb{Q}$).

For weights $k \leq 22$, we have $\dim S_k^?(\mathrm{Sp}(4,\mathbb{Z})) = 0$ or 1. However, for $k > 22$, we have $\dim S_k^?(\mathrm{Sp}(4,\mathbb{Z})) \geq 2$. However, we know from above that the eigenvalues are in $\mathbb{Q}$. Thus since the characteristic polynomial will be a quadratic over $\mathbb{Q}$ with roots in $\mathbb{Q}$, it will certainly be reducible.

This is the only case in which this particular phenomena is observed. This, along with the Hecke invariant splitting of $S_k(\mathrm{Sp}(4,\mathbb{Z}))$ outlined in subsection 5.5.1, is what has lead some authors to use the phrase "as irreducible as possible". Since it is not entirely accurate to say that the characteristic polynomial is always irreducible, but the only reasons why it would factorise generally occur in isolation (i.e. the issue in weights 24 and 26), or are otherwise well understood and one can make a more precise statement that avoids the issue (i.e. the Hecke invariant splitting, for which one restricts to the subspace $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$.

5.5.3 The computational price of products

In the algorithm presented in subsection 5.5.2, by far the most computationally expensive part is step (3). That is, computing the products of the Igusa generators which give rise to the basis for the space $S_k(\mathrm{Sp}(4,\mathbb{Z}))$. This is simply due to the fact that taking the products of series indexed over three variables is long. For example, when computing the above algorithm for weight 80 with precision 1600, computing the products took 3.5 hours, while everything else took in total 84 seconds.

The question then is how best to reduce the number of products required to compute this basis.

Method 1: Precompute powers

The first method was based on the observation that a lot of the products had common terms between them, which one could compute in advance so as not to have to compute said product many times over. For example, consider

weight 30, in which the products

$$A^2B^2C \qquad B^5C \qquad B^2CD \qquad AB^3D$$

all have the term B^2 in common. So in the algorithm outlined above, at the point where we computed the products, one could precompute $E = B^2$ and reduce the above to

$$A^2EC \qquad BE^2C \qquad ECD \qquad ABED,$$

which would reduce the total number of products required by 3.

Extending this, we updated the algorithm as follows: Once one has determined the required products to form a basis for $S_k(\mathrm{Sp}(4,\mathbb{Z}))$, we precompute all powers of the individual Igusa generators that will be needed for the products. Here is a comparison of the required number of products for this method and the original method over various weights:

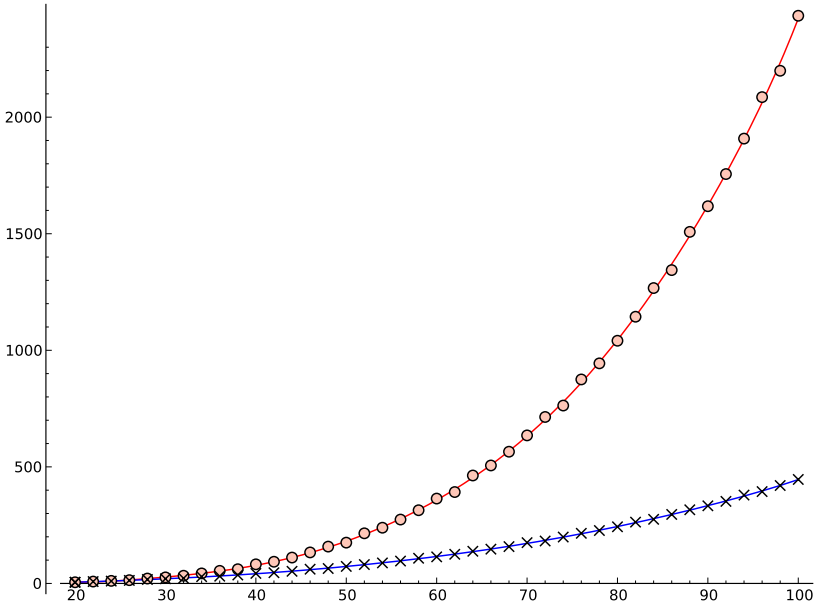

Figure 3: The circles and red line correspond to the original method, the crosses and blue line correspond to the method of precomputing powers.

A better method would be to completely determine all repeated products so they need not be done more than once. In the above example, the product B^2 may appear four times, but even the product B^2C appears three times. So to be able to make use of the minimal number of products would be ideal, but as of the moment a method of identifying all repeated products in advance is not clear.

Method 2: Use general Maaß forms, rather than just the Igusa generators

This is based on a conjecture of Martin Raum in [Rau10]. Raum has conjectured that for any k, any $f \in M_k(\mathrm{Sp}(4,\mathbb{Z}))$ can be computed as the product of no more than 2 elements of the Maaß Spezialschar. Formally,

Conjecture 5.23. *Let $k \in \mathbb{Z}_{\geq 0}$, and $f \in M_k(\mathrm{Sp}(4,\mathbb{Z}))$. Then either*

(1) $f \in V(J_k(\mathrm{SL}(2,\mathbb{Z})))$, or

(2) there exist $k_1, k_2 \in \mathbb{Z}_{\geq 0}$ such that $k_1 + k_2 = k$ and there exist $g \in V(J_{k_1}(\mathrm{SL}(2,\mathbb{Z})))$ and $h \in V(J_{k_2}(\mathrm{SL}(2,\mathbb{Z})))$ such that $f = gh$.

Raum has confirmed this up to weight 172. However, what has not yet been determined is a method to identify the Maaß Spezialformen which will give rise to $S_k(\mathrm{Sp}(4,\mathbb{Z}))$ for a given k. Using this method, Raum has achieved the following result:

Theorem 5.24. *Let $n \in \mathbb{Z}_{>0}$, $k \in \{20, 22\} \cap ([28, 150] \cap 2\mathbb{Z})$. Let $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$ be the space of weight k Siegel cusp forms of genus 2 which are not Maaß Spezialformen. Let f be the characteristic polynomial of the Hecke Operator T_n acting on $S_k^?(\mathrm{Sp}(4,\mathbb{Z}))$. Then f is irreducible over $\mathbb{Q}$.*

One will note that this is precisely part (1) of Conjecture 5.21.

6 A Look to the Future

6.1 Higher genus and vector-valued Siegel modular forms

We have been interested in extending Maeda's conjecture to the case of Siegel modular forms. Thanks to the package in Sage provided by the work of Raum, Ryan, Skoruppa, Tornaría we have been able to establish an algorithm to explore Maeda's Conjecture in the case of scalar-valued Siegel modular forms attached to the group $\mathrm{Sp}(4,\mathbb{Z})$. However, as one may have noted from the definition above, there are many more cases of Siegel modular forms.

Our definition of Hecke Operators was already in the general setting of vector-valued forms of any genus g. Further, we can extend the definitions of Fourier expansions as follows:

Consider a vector-valued Siegel modular form f and the matrix

$$\gamma = \left(\begin{array}{c|c} I & S \\ \hline \mathbf{0} & I \end{array}\right), \tag{6.1}$$

where I is the $g \times g$ identity matrix, $\mathbf{0}$ is the $g \times g$ zero matrix, and S is a symmetric integral matrix. Substituting this in to the modularity condition for f, we see

$$f(Z+S) = f(\gamma Z) = \rho(\mathbf{0}Z + I)f(Z) = f(Z), \tag{6.2}$$

so again we have periodicity in the coordinates of $\mathcal{H}_g$. Recall that in the genus 2 case, we had that the Fourier expansion was indexed over triples $[a,b,c]$ corresponding to semi-positive definite quadratic forms. The generalisation begins with the following definition

Definition 6.1 (Half-integral matrix)**.** A symmetric $g \times g$ matrix $m \in \mathrm{GL}(g,\mathbb{Q})$ is *half-integral* if m has integral diagonal entries, and $2m$ is integral.

From such a matrix m, we can define a linear form on the coordinates Z_{ij} of

$\mathcal{H}_g$ (for $i, j \in \{1, \ldots, g\}$) by

$$\mathrm{Tr}(mZ) = \sum_{i=1}^{g} m_{ii} Z_{ii} + 2 \sum_{1 \leq i < j \leq g} m_{ij} Z_{ij}. \tag{6.3}$$

In this way, we can now write

$$f(Z) = \sum_{m \text{ half-integral}} a(m) e^{2\pi i \,\mathrm{Tr}(mZ)}. \tag{6.4}$$

So we have defined Hecke Operators and Fourier expansions fully, however there are some features that make this more difficult to study in the full breath of cases:

- Examples of Siegel modular forms are only known for very low genus.
- Further, even in the cases where some examples are known, the full structure of the ring of Siegel modular forms for a fixed group $\mathrm{Sp}(2g, \mathbb{Z})$, including generators, is not know for any cases beyond $\mathrm{Sp}(4, \mathbb{Z})$.
- Even when the ring structure is known, not a great deal is known regarding lifting maps to higher genus, or other Hecke invariant splittings of the space.

One case in which some work has been done is the case of vector-valued Siegel modular forms attached to $\mathrm{Sp}(4, \mathbb{Z})$. This work has been carried out by Ghitza, Ryan, Sulon in [GRS13]. In this case, we are considering representations of $\mathrm{GL}(2, \mathbb{C})$, which are given by

$$\rho = \mathrm{Sym}^j(W) \otimes \det(W)^k, \tag{6.5}$$

where W is the standard representation of $\mathrm{GL}(2, \mathbb{C})$. So we can write that the weight of such a Siegel modular form is given by a pair (k, j).The Siegel modular forms of this weight are functions $f : \mathcal{H}_2 \to \mathbb{C}[X, Y]_j$, the space of homogeneous polynomials of degree j. This space has a $\mathrm{GL}(2, \mathbb{Q})^+$ action given by

$$(A, p) \longmapsto A \cdot p := p((X, Y)A). \tag{6.6}$$

The work done was specifically looking at the case $j = 2$, that is forms of weight $(k, 2)$, given by

$$\rho = \mathrm{Sym}^2(W) \otimes \det(W)^k. \tag{6.7}$$

In this case, the work of Satoh gives an explicit generating set. However, we first need the following construction.

Definition 6.2 (Satoh bracket)**.** Let $F \in M_k(\mathrm{Sp}(4,\mathbb{Z})), G \in M_{k'}(\mathrm{Sp}(4,\mathbb{Z}))$ be *scalar-valued* Siegel modular forms of weight k and k' respectively, and let $M_{k+k',2}(\mathrm{Sp}(4,\mathbb{Z}))$ be the space of weight $(k+k',2)$ *vector-valued* Siegel modular forms. The *Satoh bracket* of F and G is

$$[F,G]_2 = \frac{1}{2\pi i}\left(\frac{1}{k}G\partial_Z F - \frac{1}{k'}F\partial_Z G\right) \in M_{k+k',2}(\mathrm{Sp}(4,\mathbb{Z})), \tag{6.8}$$

where

$$\partial_Z = \begin{pmatrix} \partial_{Z_{11}} & 1/2\partial_{Z_{12}} \\ 1/2\partial_{Z_{12}} & \partial_{Z_{22}} \end{pmatrix}, \tag{6.9}$$

and

$$\partial_{Z_{ii}} = Z_{ii}\frac{d}{dZ_{ii}}. \tag{6.10}$$

The use here is that we can construct an explicit basis for $M_{k,2}(\mathrm{Sp}(4,\mathbb{Z}))$. Before we give the decomposition of the space, we will make the note that the notation $\mathbb{C}[A_1,\ldots,A_n]_m$ refers to the space of weight m Modular Forms that can be expressed in terms of the generators $A_1,\ldots,A_n$. The decomposition is given as follows:

$$\begin{aligned} M_{k,2}(\mathrm{Sp}(4,\mathbb{Z})) = {} & [\psi_4,\psi_6]_2 \cdot M_{k-10}(\mathrm{Sp}(4,\mathbb{Z})) \oplus [\psi_4,\ chi_{10}]_2 \cdot M_{k-14}(\mathrm{Sp}(4,\mathbb{Z})) \\ & \oplus [\psi_4,\chi_{12}]_2 \cdot M_{k-16}(\mathrm{Sp}(4,\mathbb{Z})) \cdot [\psi_6,\chi_{10}]_2 \cdot \mathbb{C}[\psi_6,\chi_{10},\chi_{12}]_{k-16} \\ & \oplus [\psi_6,\chi_{12}]_2 \cdot \mathbb{C}[\psi_6,\chi_{10},\chi_{12}]_{k-18} \oplus [\chi_{10},\chi_{12}]_2 \cdot \mathbb{C}[\chi_{10},\chi_{12}]_{k-22}, \end{aligned}$$

where $\psi_4,\psi_6,\chi_{10},\chi_{12}$ are the Igusa generators for the space $M_*(\mathrm{Sp}(4,\mathbb{Z}))$.

In this setting we can write the Fourier expansion as

$$F(Z) = \sum_{A=[a,b,c]\in Q} C_F(A)e\left(a\tau + bz + c\tau'\right), \tag{6.11}$$

where

- $Q = \{[a,b,c] \in \mathbb{Z}^3 \mid b^2 - 4ac \leq 0, a \geq 0\}$,
- $e(x) = e^{2\pi i x}$,
- $C_F(A) \in \mathbb{C}[X,Y]_2$, and
- $Z = \begin{pmatrix} \tau & z \\ z & \tau' \end{pmatrix}$.

Further, we can generalise the notion of a *cusp form* as being any form F such that $C_F(A) = 0$ for all A which are not positive-definite. Denote the space of such forms of weight k by $S_{k,j}(\mathrm{Sp}(4,\mathbb{Z}))$.

While we have expressed the definition for the Hecke Operators in full generality, for computational purposes we have to find a new expression for their action on the Fourier coefficients in this new setting. Given Hecke operators T_n, T_m with m and n coprime, we have that $T_{nm} = T_n T_m$, so it is common restrict to the case T_{p^δ} for $\delta \in \mathbb{Z}_{\geq 0}$ and p prime. We have not done this in previous cases, but this is desirable here due the complexity of the formula. The action on Fourier coefficients is given by the following:

Theorem 6.3. *Let $F \in M_{k,2}(\mathrm{Sp}(4,\mathbb{Z}))$ with Fourier coefficients given by $C_F([a,b,c])$. Consider the Hecke operator T_{p^δ} with $\delta \in \mathbb{Z}_{\geq 0}$ and p prime. Let the Fourier coefficients of $T_{p^\delta}F$ be given by $C_{T_{p^\delta}}([a,b,c])$. then*

$$C_{T_{p^\delta}}([a,b,c]) = \sum_{\alpha+\beta+\gamma=\delta} p^{\beta k+\gamma(2k-1)} \sum_{\substack{U \in R(p^\beta) \\ a_U \equiv 0 \pmod{p^{\beta+\gamma}} \\ b_U \equiv c_U \equiv 0 \pmod{p^\gamma}}} (d_{0,\beta}U) \cdot C_F\left(p^\alpha \left[\frac{a_U}{p^{\beta+\gamma}}, \frac{b_U}{p^\gamma}, \frac{c_U}{p^{\gamma-\beta}}\right]\right), \tag{6.12}$$

where

- *$R(p^\beta)$ is a complete set of representatives for $\mathrm{SL}(2,\mathbb{Z})/\Gamma_0(p^\beta)$ where $\Gamma_0(p^\beta)$ is the congruence subgroup of $\mathrm{SL}(2,\mathbb{Z})$ of level p^β,*
- *for $f = [a,b,c]$, $f := [a_U, b_U, c_U] = f((X,Y)^T U)$,*
- *$d_{0,\beta} = \begin{pmatrix} 1 & 0 \\ 0 & p^\beta \end{pmatrix}$, and*

- *the $\cdot$ is given by the action defined in equation 6.6.*

Using this as a computational basis, the authors have arrived at the following:
Proposition 6.4 (See [GRS13], Prop 3.2)**.** *Let $k \in \{14, 16, 18, 22, 24, 26, 28, 30\}$. Then the characteristic polynomial of the Hecke operator T_2 acting on $S_{k,2}(\mathrm{Sp}(4,\mathbb{Z}))$ is irreducible over $\mathbb{Q}$. If $k = 20$, the characteristic polynomial of the Hecke operator T_2 decomposes over $\mathbb{Q}$ into a linear factor and a quadratic factor.*

6.2 Higher level

As opposed to looking to Siegel modular forms and increasing the genus, another avenue by which one can extend the conjecture is to look at the case of elliptic modular forms attached to $\Gamma_0(N) \subseteq \mathrm{SL}(2,\mathbb{Z})$ for $N \in \mathbb{N}$, that is modular forms of level N (see 2.4). There has been some interest in this particular generalisation of Maeda's Conjecture of late, with much work being done by Tsaknias in [Tsa12] and by Chow, Ghitza, Withers (in preparation).

Again, here there exists a Hecke invariant splitting of the space $S_k(\Gamma_0(N))$ coming from a phenomenon which is quite analogous to the liftings we see in the Siegel case. This is given by the following definition:
Definition 6.5 (Oldform)**.** Let $M, N \in \mathbb{Z}_{>0}$ such that $M|N$, and let $t \,\big|\, \frac{M}{N}$. Consider the function

$$\begin{array}{rccc} \alpha_{M,t}: & S_k(\Gamma_0(M)) & \longrightarrow & S_k(\Gamma_0(N)) \\ & f & \longmapsto & f\left|\begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix}\right. \end{array} \tag{6.13}$$

An *oldform* is a modular form $f \in S_k^{\mathrm{old}}(\Gamma_0(N))$, where

$$S_k^{\mathrm{old}}(\Gamma_0(N)) = \bigoplus_{M|N \text{ and } t\left|\frac{N}{M}\right.} \alpha_{M,t}\left(S_k(\Gamma_0(M))\right). \tag{6.14}$$

We can decompose the space $S_k(\Gamma_0(N))$ as follows:

$$S_k(\Gamma_0(N)) = S_k^{\text{old}}(\Gamma_0(N)) \oplus S_k^{\text{new}}(\Gamma_0(N)). \tag{6.15}$$

As in the Siegel case (see definition 5.4), we can define the *Petersson inner product* on the space of modular forms of level N. Given $f, g \in S_k(\Gamma_0(N))$ we define the product by

$$\langle f, g \rangle = \int_F f(z)\overline{g(z)}y^k \frac{dxdy}{y^2}, \tag{6.16}$$

where F is a fundamental domain for the action of $\Gamma_0(N)$ on $\mathcal{H}$. Here again we have that the Hecke operators are Hermitian with respect to the Petersson inner product, and the decomposition

$$S_k(\Gamma_0(N)) = S_k^{\text{old}}(\Gamma_0(N)) \oplus S_k^{\text{new}}(\Gamma_0(N)). \tag{6.17}$$

is Hecke invariant.

So here one restricts to the space $S_k^{\text{new}}(\Gamma_0(N))$, and rather remarkable phenomena occur in this context. Essentially, it is difficult to say anything directly about the nature of the characteristic polynomial. What is easier to get a hold of is the nature of the space as a Hecke module. That is, as a module over the Hecke algebra (recall that this is the $\mathbb{C}$-algebra generated by the Hecke operators T_n for $n \in \mathbb{Z}_{\geq 0}$).

This is a common way to study Maeda's conjecture, since as observed in section 5.5.1, it cannot be the case that the characteristic polynomial of an operator is irreducible if the space it acts upon is not itself irreducible. This is the method used in [Tsa12], and the conjecture can be stated as follows

Conjecture 6.6. *Let $k, N \in \mathbb{Z}_{\geq 0}$. Consider $S_k(\Gamma_0(N))$ as a Hecke module, and let its decomposition into irreducible modules be written as*

$$S_k(\Gamma_0(N)) = \bigoplus_{i=1}^{m_{k,N}} V_i. \tag{6.18}$$

Then

(1) $m_{k,N}$ *is bounded as* $k \to \infty$ *and in fact* $m_{k,N}$ *will tend towards a constant* quickly*,*

(2) if $N = p_1 p_2 \dots p_r$ *is squarefree, then* $m_{k,N} = 2^r$*, and*

(3) if N *and* M *are coprime, then* $m_{k,NM} = m_{k,N} m_{k,M}$*.*

James Withers has data supporting this conjecture for $N \leq 200$ and $k \leq 30$.

References

[Ahl08] Scott Ahlgren. On the irreducibility of Hecke polynomials. *Mathematics of Computation*, 77(263):1725–1731, 2008.

[AZ95] Anatolii Andrianov and Vladimir Zhuravlev. *Modular Forms and Hecke Operators*. American Mathematical Society, 1995.

[BJX11] Jeffrey Beyerl, Kevin James, and Hui Xue. Divisibility of an eigenform by another eigenform. 2011.

[BM03] Srinath Baba and M. Ram Murty. Irreducibility of Hecke polynomials. *Mathematical Research Letters*, 10(5-6):709–715, 2003.

[BS96] Eric Bach and Jeffrey Shallit. *Algorithmic number theory. Vol. 1.* MIT Press, Cambridge, MA, 1996.

[Bum98] Daniel Bump. *Automorphic Forms and Representations*. Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1998.

[Buz96] Kevin Buzzard. On the eigenvalues of the Hecke operator T_2. *Journal of Number Theory*, 57(1):130–132, 1996.

[Buz12] Kevin Buzzard. Notes on Siegel modular forms. 2012.

[CF99] J. B. Conrey and D. W. Farmer. Hecke operators and the nonvanishing of L-functions. In *Topics in number theory (University Park, PA, 1997)*, volume 467 of *Math. Appl.*, pages 143–150. Kluwer Acad. Publ., Dordrecht, 1999.

[CFW00] J. B. Conrey, D. W. Farmer, and P. J. Wallace. Factoring Hecke polynomials modulo a prime. *Pacific J. Math.*, 196(1):123–130, 2000.

[DGG+02] Dumas, Gautier, Giesbrecht, Giorgi, Hovinen, Kaltofen, Saunders, Turner, and Villard. Linbox: a generic library for exact

linear algebra. In A. Cohen, X-S Gao, and N. Takayama, editors, *Mathematical software: ICMS 2002*, pages 40–50, Beijing, 2002. World Scientific.

[DS05] Fred Diamond and Jerry Shurman. *A First Course in Modular Forms*, volume 228 of *Graduate Texts in Mathematics*. Springer, 2005.

[Dus10] Pierre Dusart. Estimates of some functions over primes without R.H. arXiv:1002.0442, 2010.

[EZ85] Martin Eichler and Don Zagier. *The Theory of Jacobi Forms*, volume 55 of *Progress in Mathematics*. Birkhäuser, Boston, 1985.

[Fel68] William Feller. *An Introduction to Probability Theory and Its Applications*, volume 1. Wiley, New York, 1968.

[FJ02] D. W. Farmer and K. James. The irreducibility of some level 1 Hecke polynomials. *Mathematics of Computation*, 71(239):1263–1270, 2002.

[Ghi11] Alexandru Ghitza. Distinguishing Hecke eigenforms. *International Journal of Number Theory*, 7(5):1247–1253, 2011.

[GM12] Alexandru Ghitza and Angus McAndrew. Experimental evidence for Maeda's conjecture on modular forms. *Tbilisi Mathematical Journal*, Vol. 5(2):55–69, 2012.

[Gro96] Benedict H. Gross. On the Satake isomorphism. In *Galois Representations in Arithmetic Algebraic Geometry*, pages 223–237. Cambridge University Press, Durham, England, 1996.

[GRS13] Alexandru Ghitza, Nathan C. Ryan, and David Sulon. Computations of vector-valued siegel modular forms. *Journal of Number Theory*, Volume 133(11):3921–3940, November 2013.

[Har10] William Hart. Fast library for number theory: an introduction. In *Mathematical Software – ICMS 2010*, volume 6327 of *Lecture notes in computer science*, pages 88–91. Springer, Heidelberg, 2010.

[HM97] Haruzo Hida and Yoshitaka Maeda. Non-abelian base change for totally real fields. *Pacific Journal of Mathematics*, (Special Issue):189–217, 1997.

[Kil08] Lloyd Kilford. *Modular Forms: A Classical and Computational Introduction*. Imperial College Press, 2008.

[Kle04] Seth Kleinerman. Some computations in support of Maeda's conjecture. 2004.

[LH95] Hong-Chang Lee and Wan-Hui Hung. Galois groups of Hecke eigenforms. *Chinese Journal of Mathematics*, 23(4):329–342, 1995.

[Lim05] *Decomposition of spaces of cusp forms over Q, and variants of partial Nim*. ProQuest LLC, Ann Arbor, MI, 2005.

[NR03] Kendra Nelsen and Arun Ram. Kostka-Foulkes polynomials and Macdonald spherical functions. *Surveys in Combinatorics*, 2003.

[Rau10] Martin Raum. Efficiently generated spaces of classical Siegel modular forms and the Boecherer conjecture. *J. Aust. Math.*, 98(3):393–405, 2010.

[Rio58] John Riordan. *An introduction to combinatorial analysis*. John Wiley & Sons Inc., New York, 1958.

[Rob55] Herbert Robbins. A remark on Stirling's formula. *The American Mathematical Monthly*, 62:26–29, 1955.

[RRST12] Martin Raum, Nathan Ryan, Nils-Peter Skoruppa, and Gonzalo Tornaría. Explicit computations of Siegel modular forms of degree

two. arXiv:1205.6255, 2012.

[S+13] W.A. Stein et al. *Sage Mathematics Software (Version 5.8)*. The Sage Development Team, 2013.

[Sea12] N. J. A. Sloane et al. The on-line encyclopedia of integer sequences, sequence a000246. 2012.

[Sko92] Nils-Peter Skoruppa. Computations of siegel modular forms of genus two. *Math. Comp.*, 58:381–398, 1992.

[SL96] P. Stevenhagen and H. W. Lenstra, Jr. Chebotarëv and his density theorem. *The Mathematical Intelligencer*, 18(2):26–37, 1996.

[Sta97] Richard P. Stanley. *Enumerative combinatorics. Vol. 1*, volume 49 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1997.

[Ste07] William Stein. *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, 2007.

[Tsa12] Panagiotis Tsaknias. A possible generalization of Maeda's conjecture. 2012.

[vdG06] Gerard van der Geer. Siegel modular forms. In *The 1-2-3 of Modular Forms*. Springer, 2006. arXiv:math/0605346.

[Zag08] Don Zagier. Elliptic modular forms and their applications. In *The 1-2-3 of Modular Forms*. Springer, 2008.

[Zud13] Wadim Zudilin. AMSI summer school 2013: Modular forms, January 2013.

Appendix: Siegel Code

```
1  def siegel_maeda(weight, n_hecke, prec = 0, verbose = False,
       writeout = False, charpoly = False, PRIME_BOUND =
2  2^12):
3
4          if writeout:
5                  doc = open('/home/hs/stude/mcandrew/sage_stuff/
       siegel_computations/computations%d_%d_%d.txt'
6  %(weight,n_hecke,prec),'w')
7                  doc.write('Space of weight %d Siegel Cusp forms' % (
       weight) + '\n')
8                  doc.write('Hecke Operator T_{%d}' % (n_hecke) + '\n'
       )
9                  doc.write('Using precision prec = %d' % (prec) + '\n
       ' + '\n')
10
11         # start timing
12
13         import time
14         t0 = time.time()
15
16         # Find which products of generators are cusp forms in a
       given weight
17
18         spanlst = []
19         k = weight - 10
20         for a in range((k/4).floor() + 1):
21                 for b in range((k/6).floor() + 1):
22                         for c in range((k/10).floor() + 1):
23                                 for d in range((k/12).floor() + 1):
24                                         if 4*a + 6*b + 10*c + 12*d == k:
25                                                 spanlst.append((a, b, c+1, d
       ))
26         k = weight - 12
27         for a in range((k/4).floor() + 1):
28                 for b in range((k/6).floor() + 1):
29                         for c in range((k/10).floor() + 1):
```

```
30                          for d in range((k/12).floor() + 1):
31                              if 4*a + 6*b + 10*c + 12*d == k:
32                                  spanlst.append((a, b, c, d
    +1))
33
34      spanlst = uniq(spanlst)
35      spanlst.reverse()
36      print(len(spanlst))
37      print(spanlst)
38
39      # Set precision and generators
40
41      if prec == 0:
42          prec = weight*10
43      A,B,C,D = SiegelModularFormsAlgebra().gens(prec=prec)
44      spanset = []
45
46      Apow = [1]
47      for j in range(1, max([x[0] for x in spanlst]) + 1):
48          Apow.append(Apow[j-1] * A)
49
50      Bpow = [1]
51      for j in range(1, max([x[1] for x in spanlst]) + 1):
52          Bpow.append(Bpow[j-1] * B)
53
54      Cpow = [1]
55      for j in range(1, max([x[2] for x in spanlst]) + 1):
56          Cpow.append(Cpow[j-1] * C)
57
58      Dpow = [1]
59      for j in range(1, max([x[3] for x in spanlst]) + 1):
60          Dpow.append(Dpow[j-1] * D)
61
62      spanset = [Apow[a] * Bpow[b] * Cpow[c] * Dpow[d] for (a, b
    , c, d) in spanlst]
63      # this is called spanset, but it seems to actually be a
    basis for the
64      # space of all cusp forms of that weight
```

```
65
66          t1 = time.time()
67          st = "finding spanset took %f seconds" % (t1 - t0) + '\n'
68          if verbose:
69                  print st
70          if writeout:
71                  doc.write(st + '\n')
72
73          Sk = CuspForms(1,weight).basis()
74          Sk2 = CuspForms(1,weight+2).basis()
75          Maass = [SiegelModularForm(f,0,prec=prec) for f in Sk]
76          Maass = Maass + [SiegelModularForm(0,g,prec=prec) for g in
        Sk2]
77
78          CuspImages = [f.hecke_image(n_hecke) for f in spanset]
79          MaassImages = [f.hecke_image(n_hecke) for f in Maass]
80
81          # find support for all forms
82
83          coeffs = spanset[0].coeffs().keys()
84          dlst = sorted([(4*a*c-b**2, a, b, c) for (a, b, c) in
       coeffs])
85          coeffs = [(a, b, c) for (d, a, b, c) in dlst]
86
87          m = matrix(QQ, [[f[x] for x in coeffs] for f in spanset])
88          if verbose:
89                  print(m.pivots())
90          support = [coeffs[j] for j in m.pivots()]
91          if verbose:
92                  print(support)
93          if len(support) < len(spanset):
94                  if writeout:
95                          doc.write('prec too low' + '\n')
96                          doc.close()
97                  raise RuntimeError("support too small; increase
       precision")
98
99          coeffs = Maass[0].coeffs().keys()
```

```
100         dlst = sorted([(4*a*c-b**2, a, b, c) for (a, b, c) in
    coeffs])
101         coeffs = [(a, b, c) for (d, a, b, c) in dlst]
102
103         m = matrix(QQ, [[f[x] for x in coeffs] for f in Maass])
104         if verbose:
105                 print(m.pivots())
106         supportmaass = [coeffs[j] for j in m.pivots()]
107         if verbose:
108                 print(supportmaass)
109         if len(supportmaass) < len(Maass):
110                 if writeout:
111                         doc.write('prec too low' + '\n')
112                         doc.close()
113                 raise RuntimeError("support too small; increase
    precision")
114
115         t2 = time.time()
116         st = "finding support took %f seconds" % (t2 - t1) + '\n'
117         if verbose:
118                 print st
119         if writeout:
120                 doc.write(st + '\n')
121
122         # Compute full Hecke matrix
123
124         v = [support[i] for i in range(len(spanset))]
125
126         T = matrix([[f[x] for f in CuspImages] for x in v])
127         F = matrix([[f[x] for f in spanset] for x in v])
128         if det(F) == 0:
129                 if writeout:
130                         doc.write('prec too low' + '\n')
131                         doc.close()
132                 raise RuntimeError("det F = 0; increase precision")
133
134         MT = T*(F.inverse())
135
```

```
136         v = [supportmaass[i] for i in range(len(Maass))]
137
138         TMas = matrix([[f[x] for f in MaassImages] for x in v])
139         FMas = matrix([[f[x] for f in Maass] for x in v])
140         if det(FMas) == 0:
141                 if writeout:
142                         doc.write('prec too low' + '\n')
143                         doc.close()
144                 raise RuntimeError("det FMas = 0; increase precision
    ")
145
146         MTMas = TMas*(FMas.inverse())
147
148         if charpoly:
149                 poly1 = MT.charpoly()
150                 poly2 = MTMas.charpoly()
151                 f = poly1/poly2
152                 return f.numerator()
153
154         t3 = time.time()
155         st = "computing Hecke matrices took %f seconds" % (t3 - t2
    ) + '\n'
156         if verbose:
157                 print st
158         if writeout:
159                 doc.write(st + '\n')
160
161         # Compute charpoly mod p to determine Galois group an
    irreducibility
162
163         p = 1
164         type1_prime = None
165         type2_prime = None
166         type3_prime = None
167         Gal = None
168         irred = None
169         denom = MT.denominator()*MTMas.denominator()
170
```

```
171     while (((type1_prime is None) or (type2_prime is None) or
    (type3_prime is None)) and (p < PRIME_BOUND)):
172             p = next_prime(p)
173             while (denom % p == 0):
174                     p = next_prime(p)
175
176             MTp = MT.change_ring(GF(p))
177             poly1 = MTp.charpoly()
178             MTMasp = MTMas.change_ring(GF(p))
179             poly2 = MTMasp.charpoly()
180             poly = (poly1/poly2).numerator()
181
182             if poly.degree() < 2:
183                     irred = True
184                     Gal = True
185                     break
186             if verbose:
187                     print p, '\n', poly
188             if (type1_prime is None) and poly.is_irreducible():
189                     irred = True
190                     type1_prime = p
191                     if (type3_prime is None) and is_prime(poly.
    degree()):
192                             type3_prime = p
193                             continue
194             if not poly.is_squarefree():
195                     continue
196             fact = poly.factor()
197             lst = sorted([g[0].degree() for g in fact])
198             if (type2_prime is None) and is_type_II(lst):
199                     type2_prime = p
200             if (type3_prime is None) and is_type_III(lst):
201                     type3_prime = p
202     if ((type1_prime is None) or (type2_prime is None) or (
    type3_prime is None)) and (Gal is None):
203             print "Prime bound exceeded without finding primes
    of each type"
204     else:
```

```
205             #print "Galois group equal to the full symmetric
    group S_{%d}" % poly.degree()
206             Gal = True
207
208         t4 = time.time()
209         st = "computing characteristic polynomials took %f seconds
    " % (t4 - t3) + '\n'
210         if verbose:
211             print st
212         if writeout:
213             doc.write(st + '\n')
214
215         if writeout:
216             doc.write('charpoly irreducible = %s' % (irred) + '\
    n')
217             doc.write('Gal(charpoly) is S_{%d} = %s' % (poly.
    degree(), Gal) + '\n' + '\n')
218             doc.close()
219         return 'Gal(charpoly) is S_{%d} = %s' % (poly.degree(),
    Gal)
220
221
222
223 def galois_group(poly, PRIME_BOUND=2^12, verbose=False):
224         if poly.degree() < 2:
225             return True
226         ZP.<x> = ZZ[]
227         type1_prime = None
228         type2_prime = None
229         type3_prime = None
230         p = 1
231         while (((type1_prime is None) or (type2_prime is None) or
    (type3_prime is None)) and (p < PRIME_BOUND)):
232             p = next_prime(p)
233             f = poly.change_ring(GF(p))
234             if verbose:
235                 print f
236             if (type1_prime is None) and f.is_irreducible():
```

```
237                     type1_prime = p
238                     if (type3_prime is None) and is_prime(f.degree
    ()):
239                         type3_prime = p
240                         continue
241             if not f.is_squarefree():
242                 continue
243             fact = f.factor()
244             lst = sorted([g[0].degree() for g in fact])
245             if (type2_prime is None) and is_type_II(lst):
246                 type2_prime = p
247             if (type3_prime is None) and is_type_III(lst):
248                 type3_prime = p
249         if ((type1_prime is None) or (type2_prime is None) or (
    type3_prime is None)):
250             print "Prime bound exceeded without finding primes
    of each type"
251         else:
252             print "Galois group equal to the full symmetric
    group S_{%d}" % f.degree()
253         return True
254
255 def is_type_II(lst):
256         mylst = copy(lst)
257         if mylst.count(2) != 1:
258             return False
259         mylst.remove(2)
260         for l in mylst:
261             if (l % 2) == 0:
262                 return False
263         return True
264
265 def is_type_III(lst):
266         return (is_prime(lst[-1]) and (lst[-1] > sum(lst)/2))
```