KU LEUVEN

UNIVERSITÉ DU LUXEMBOURG

Computational Aspects of Classical and Hilbert Modular Forms

Jasper Van Hirtum

Computational Aspects of Classical and Hilbert Modular Forms

Jasper VAN HIRTUM

Examination committee:
Prof. dr. Walter Van Assche, chair
dr. Jan Tuitman, supervisor
Prof. dr. Wim Veys, supervisor
Prof. dr. Gabor Wiese, supervisor
(Université du Luxembourg)
Prof. dr. Martin Schlichenmaier
(Université du Luxembourg)
dr. Andrew V. Sutherland
(MIT)
dr. Lassina Dembélé
(Max-Planck Institute for Mathematics)

Dissertation presented in partial fulfilment of the requirements for the degree of Doctor of Science (PhD): Mathematics

Arenberg Doctoral School
Faculty of Science
KU Leuven

June 2017

PhD-FSTC-2017-33
The Faculty of Sciences, Technology and Communication

Computational Aspects of Classical and Hilbert Modular Forms

DISSERTATION
Presented on 15/06/2017
to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG
EN MATHÉMATIQUES

by
Jasper Van Hirtum
Born on 13 May 1990 in Leuven (Belgium)

Abstract

The main topic of this thesis is the study of classical and Hilbert modular forms and computational aspects of their q-expansions. The coefficients of q-expansions of eigenforms are particularly interesting because of their arithmetic significance. Most notably, modular forms are an essential ingredient in Andrew Wiles's proof of Fermat's last theorem.

This thesis consists of two parts: the first part concerns the distribution of the coefficients of a given classical eigenform; the second part studies computational aspects of the adelic q-expansion of Hilbert modular forms of weight 1.

Part I of this thesis is an adapted version of the article *On the Distribution of Frobenius of Weight* 2 *Eigenforms with Quadratic Coefficient Field* published in *Experimental Mathematics* [38]. It presents a heuristic model that settles the following question related to the Sato-Tate and Lang-Trotter conjectures: given a normalised eigenform of weight 2 with quadratic coefficient field, what is the asymptotic behaviour of the number of primes p such that the p-th coefficient of this eigenform is a rational integer? Our work contributes to this problem in two ways. First, we provide an explicit heuristic model that describes the asymptotic behaviour in terms of the associated Galois representation. Secondly, we show that this model holds under reasonable assumptions and present numerical evidence that supports these assumptions.

Part II concerns the study of (adelic) q-expansions of Hilbert modular forms. Our main achievements are the design, proof and implementation of several algorithms that compute the adelic q-expansions of Hilbert modular forms of weight 1 over $\mathbb{C}$ and over finite fields. One reason we are studying such q-expansions is that their coefficients (conjecturally) describe the arithmetic of Galois extensions of a totally real number field with Galois group in $\mathrm{GL}_2(\overline{\mathbb{F}}_p)$ that are unramified at p. Using the adelic q-expansions of Hilbert modular forms of higher weight, these algorithms enable the explicit computation of Hilbert modular forms of any weight over $\mathbb{C}$ and the computation of Hilbert modular forms of parallel weight both over $\mathbb{C}$ and in positive characteristics. The main improvement to existing methods is that this algorithm can be

applied in (partial) weight 1, which fills the gap left by standard computational methods. Moreover, the algorithm computes in all characteristics simultaneously. More precisely, we prove that, under certain conditions in higher weight, the output of the algorithm for given level $\mathfrak{N}$ and quadratic character $\mathcal{E}$ includes a finite set of primes $\mathcal{L}$ such that all Hilbert modular forms of given parallel weight, level $\mathfrak{N}$ and quadratic character $\mathcal{E}$ over $\overline{\mathbb{F}}_p$ are liftable for all primes p outside the set $\mathcal{L}$. In particular, testing primes in the set $\mathcal{L}$ enabled the computation of examples of non-liftable Hilbert modular forms of weight 1.

Both parts of the thesis start with a more elaborate introduction.

Samenvatting

Het hoofdthema van deze thesis is de studie van klassieke en Hilbert modulaire vormen en computationele aspecten van hun q-expansies. De coëfficiënten van deze q-expansies zijn interessant vanwege hun rekenkundige betekenis voor onder andere Galois representaties. In het bijzonder spelen modulaire vormen een essentiële rol in Andrew Wiles' bewijs van de laatste stelling van Fermat.

Deze thesis is opgebouwd uit twee delen: het eerste deel behandelt de verdeling van de coëfficiënten van een gegeven klassieke eigenvorm; het tweede deel betreft computationele aspecten van de adelische q-expansies van Hilbert modulaire vormen van gewicht 1.

Deel I is een aangepaste versie van het artikel *On the Distribution of Frobenius of Weight* 2 *Eigenforms with Quadratic Coefficient Field* dat in 2017 verscheen in *Experimental Mathematics*, zie [38]. In dit artikel beschrijven we een heuristisch model dat een antwoord biedt op de volgende vraag die nauw verband houdt met de conjecturen van Sato-Tate en Lang-Trotter: zij f een eigenvorm van gewicht 2 met kwadratisch coëfficiëntenveld en zonder inwendige twists, wat is het asymptotische gedrag van het aantal priemgetallen p zodat de p-de coëfficiënt van f een rationaal getal is? Wij verbeteren de bestaande theorie op twee manieren: ten eerste geven we een expliciet model dat het asymptotische gedrag beschrijft in functie van de Galois representatie geassocieerd aan de gegeven eigenvorm. Ten tweede bewijzen we ons model onder expliciete voorwaarden. In de laatste sectie van deel I, geven we numerieke data die ons model en de onderliggende voorwaarden ondersteunen.

In deel II bestuderen we de adelische q-expansies van Hilbert modulaire vormen. Bestaande algoritmen om de coëfficiënten van deze q-expansies te bepalen zijn enkel toepasbaar in gewicht groter dan 2. We ontwerpen, implementeren en bewijzen verschillende algoritmen die gebruik maken van de bestaande methodes in gewicht 2 om de adelische q-expansies van Hilbert modulaire vormen van gewicht 1 te berekenen. Meer precies, tonen we aan dat deze algoritmen toepasbaar zijn voor Hilbert modulaire vormen met coëfficiënten in $\mathbb{C}$ voor elk gewicht alsook voor Hilbert modulaire vormen

met coëfficiënten in eindige velden en met parallel gewicht. Bovendien tonen we aan dat ons algoritme in staat is om in alle karakteristieken tegelijk te rekenen. Dit wil zeggen, de uitvoer bevat een eindige lijst priemgetallen $\mathcal{L}$ zodat voor alle priemgetallen p niet in $\mathcal{L}$ alle Hilbert modulaire vormen van parallel gewicht 1, niveau $\mathfrak{N}$ en kwadratisch karakter $\mathcal{E}$ over $\overline{\mathbb{F}}_p$ ophefbaar zijn tot karakteristiek 0. In het bijzonder staat dit ons toe om expliciete voorbeelden van niet-ophefbare Hilbert modulaire vormen van gewicht 1 te vinden.

Acknowledgements

This thesis would not have been written without the help and support of many people.

First, I would like to express my gratitude to all members of the examination committee for taking the time to go through my thesis. In particular, I am grateful to Andrew Sutherland and Lassina Dembélé for the interesting and helpful remarks they provided.

I owe many thanks to all three of my supervisors. Wim, bedankt om me de kans te geven een doctoraat te beginnen en om mij de vrijheid te geven om zelfstandig rond te dwarrelen tussen Leuven en Luxembourg.

Jan, het onderwerp van mijn doctoraat is sinds het begin verder weg geslopen van jouw expertisegebied, maar toch stond jouw deur altijd open voor vragen over onder andere Magma, de matrix of algebraïsche meetkunde.

Gabor, bedankt voor al jouw steun, aanmoediging en advies gedurende de voorbije vier jaar. Jij zag in waar ik problemen had en stuurde bij precies daar waar ik het nodig had. Met een uitzonderlijk oog voor details heb je steeds mijn werk gelezen, gecorrigeerd en herlezen. Ik had me geen betere promotor kunnen inbeelden.

Next, I would like to thank all my colleagues from Leuven and Luxembourg for the nice atmosphere. I enjoyed the occasional lunch breaks playing cards, the walks to the chambre de commerce, the coffee breaks and any kind of break involving ice-cream or frisbee. To all those in the algebra section, thank you for the many evenings and nights enjoying one too many beers in the city center.

Thank you Alexander, Annelies, Christophe, Hans, Lore and Marta for all the distracting afternoons. The ground floor has lost much of its charm after most of you left.

Annelies, bedankt voor de vele gesprekken over politiek, feminisme en zowat alles behalve wiskunde. Ik heb oprecht genoten van onze discussies, vooral wanneer we vertrokken van tegenstrijdige meningen. Het was een plezier om dit avontuur met jou te starten.

Verder wil ik ook mijn ouders bedanken voor het warme nest waar zij steeds voor hebben gezorgd, voor de goulash op zondag en voor het nalezen van zowat alles dat ik ooit geschreven heb.

Bedankt Bregt, om me steeds uit te dagen en me te doen nadenken over het belang van fundamenteel onderzoek in de wiskunde. Als ik het ooit ontdek, laat ik het je weten.

Bedankt Tilde, voor de lange wandelingen op zoek naar virtuele monstertjes terwijl we ons beklag deden over ons doctoraat. Jouw ervaringen hebben me laten inzien dat het op de afdeling algebra nog niet zo slecht is.

Merci Ben, Ruben en Yennef, voor de zeldzame momenten waarop we alle vier tegelijk in Kumtich waren. Een avond wiezen, Kingen, spades en ja zelfs hartenjagen bij een Orval zullen altijd een trip vanuit Luxembourg waard zijn.

Asante Marie-claire, om je deur voor mij het voorbije jaar te openen, je hebt me steeds het gevoel gegeven dat ik welkom was.

Finally, I want to express how lucky I feel to have Mariagiulia in my life. I want to thank you for all the trains, flights and car rides you took to see me in the past two years and for the incredible patience you showed in the past months. You have made Luxembourg feel like home and I cannot wait to see what our future brings. Sei la cosa migliore che mi sia mai capitata, la mia principessa.

Jasper

Contents

Part I

Classical Modular Forms

Introduction

Let f be a weight 2 cuspidal Hecke eigenform of level $\Gamma_1(N)$ with quadratic coefficient field and without inner twist. Denote the p-th coefficient of the q-expansion of f by $a_p(f)$. Then the set of primes $\{p \mid a_p(f) \in \mathbb{Q}\}$ is known to be of density zero, cf. [17, Corollary 1.1]. Part of the conjecture that Kumar Murty posed based on earlier work of S. Lang and H. Trotter [20] is the following.

Conjecture 0.0.1 (Conjecture 3.4 [23])**.** *Let f be a weight 2 normalised cuspidal Hecke eigenform of level $\Gamma_1(N)$ with quadratic coefficient field and without inner twists. Then*

$$\#\{p < x \text{ prime} \mid a_p(f) \in \mathbb{Q}\} \sim c_f \frac{\sqrt{x}}{\log x},$$

with c_f a constant that depends on the eigenform.

In Part I, we present a heuristic model that makes this conjecture explicit. More precisely, we will prove the following theorem.

Theorem 1.5.3. *Let f be a weight 2 normalised cuspidal Hecke eigenform of level $\Gamma_1(N)$ with quadratic coefficient field $\mathbb{Q}(\sqrt{D})$ and without inner twists. Assume that there exists a positive integer m_0 such that Assumptions 1.3.4 and 1.2.1 hold for f and all positive integers in $m_0\mathbb{Z}$. Then there is an explicit constant $\widehat{F}$, depending on the images of the Galois representations attached to f, such that Conjecture 0.0.1 holds with*

$$c_f = \frac{16\sqrt{D}\widehat{F}}{3\pi^2}.$$

Our work is based on the methods used by S. Lang and H. Trotter in [20] where they derive a heuristic model for the behaviour of the coefficients of the L-polynomial of an elliptic curve, i.e. the coefficients of a weight 2 eigenform with rational coefficients.

Section 1.1 contains preliminaries concerning modular forms. In Section 1.2, we describe the assumptions needed to reduce our problem to the product of two functions:

one concerning the real absolute value and the other derived from the non-archimedean places. In Section 1.3, we will discuss the factor of the infinite place. For this factor we will use recent results on the Sato-Tate conjecture for abelian surfaces and one additional assumption. The factor at the finite places will be discussed in Section 1.4. We will derive this factor from the adelic representation attached to the eigenform. Section 1.5 contains the proof of our main result. In the final section, we compare our model to numerical data. Moreover, we check all assumptions and intermediate results numerically. All computations agree with our model and the assumptions we made to obtain these results. Therefore, we are led to believe that our heuristic model correctly predicts the asymptotic number of primes with rational integer coefficient.

Chapter 1

The Distribution of Frobenius

1.1 Preliminaries

In this section, we recall some definitions and properties of modular forms required for the remainder of this chapter.

Definition 1.1.1. *A* Congruence subgroup *of* $\mathrm{SL}_2(\mathbb{Z})$ *is any subgroup* Γ *of* $\mathrm{SL}_2(\mathbb{Z})$ *that contains*

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

for some positive integers N*. The smallest such* N *is called the* level *of* Γ*.*

Two important congruence subgroups are

$$\Gamma_1(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

and

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \middle| \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}.$$

Let $\mathcal{H}$ be the complex upper half plane. Let Γ be a congruence subgroup of $\mathrm{SL}_2(\mathbb{Z})$. Then Γ acts on $\mathcal{H}$ by

$$\gamma z = \gamma \cdot z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z := \frac{az+b}{cz+d}.$$

The group $\mathrm{SL}_2(\mathbb{Z})$ is generated by the following elements:

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \qquad \text{and} \qquad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Their actions are given by

$$Sz = -1/z \qquad \text{and} \qquad Tz = z + 1.$$

A fundamental domain of the action of $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane $\mathcal{H}$ is given by

$$D := \left\{ z \in \mathcal{H} \middle| |z| \geq 1 \text{ and } |\mathrm{Re}(z)| \leq \frac{1}{2} \right\}$$

by identifying the left and right half of the boundary, see [30, Chapter VII Theorem 1].

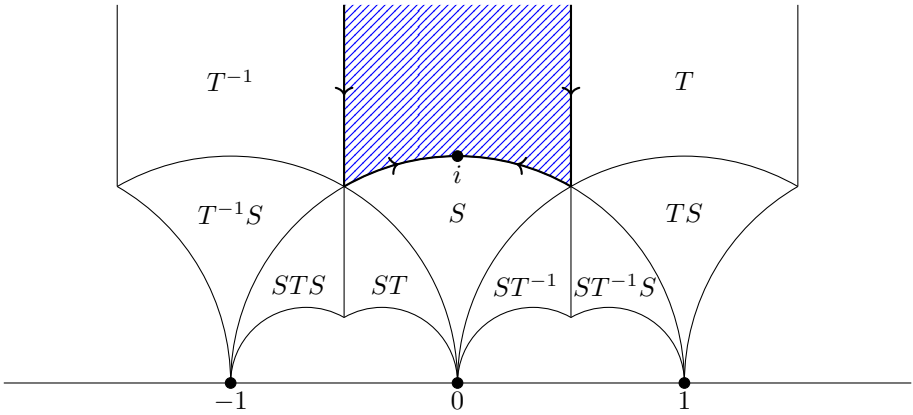


Figure 1.1: The fundamental domain of the action of $\mathrm{SL}_2(\mathbb{Z})$ on the complex upper half plane $\mathcal{H}$.

Definition 1.1.2. *Let k be a positive integer, Γ a congruence subgroup of level N and ε a Dirichlet character mod N.* A modular form of weight k, level N and nebentypus ε *is a function $f : \mathcal{H} \to \mathbb{C}$ such that:*

1. *The function f is holomorphic;*
2. *For all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$, the function f satisfies*

$$f(\gamma \cdot z) = \varepsilon(d)(cz + d)^k f(z).$$

This condition is known as the modularity condition*;*

3. *The function f is* holomorphic at the cusps*, see Definition 1.1.4.*

We denote the space of modular forms by $\mathcal{M}_k(\Gamma, \varepsilon)$.

Holomorphic at the Cusps

Let f be a holomorphic function on $\mathcal{H}$ that satisfies the modularity condition in Definition 1.1.2 for some congruence subgroup Γ of level N. Then, the modularity condition for $\gamma = \begin{pmatrix} 1 & N \\ 0 & 1 \end{pmatrix} \in \Gamma$, yields

$$\begin{aligned} f(z+N) &= f(\gamma \cdot z) \\ &= f(z). \end{aligned}$$

In other words, f is a periodic function of period N. In particular, f admits a Fourier expansion of the form

$$\begin{aligned} f &\sim \sum_{n \in \frac{1}{N}\mathbb{Z}} a_n e^{2\pi i n z} \\ &= \sum_{n \in \frac{1}{N}\mathbb{Z}} a_n q^n \end{aligned}$$

with $q = e^{2\pi i z}$, called the *q-expansion of f* (at ∞).

Remark 1.1.3. *If Γ is a congruence subgroup that contains the matrix $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, then f is periodic with period 1 so that the q-expansion can be taken over $\mathbb{Z}$ instead. The groups $\Gamma_0(N)$ and $\Gamma_1(N)$ both contain the element T. In the remainder of this thesis, we will only consider modular forms with these congruence subgroups so we only consider q-expansions indexed by integers. However, in the broader setting of modular forms one might encounter more general q-expansions.*

We extend the action of $\mathrm{SL}_2(\mathbb{Z})$ to $\mathbb{P}^1 = \mathbb{Q} \cup \{\infty\}$ in a natural way by

$$\gamma \cdot (x : y) = \gamma \cdot \begin{pmatrix} x \\ y \end{pmatrix}.$$

The set of *cusps of* Γ is the quotient $\Gamma \backslash \mathbb{P}^1$. One can check that $\mathrm{SL}_2(\mathbb{Z})$ has only one cusp, that is $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{P}^1 = \{\infty\}$.

Definition 1.1.4. *Let f be a holomorphic function on $\mathcal{H}$ that satisfies the modularity condition in Definition 1.1.2 and let C be a cusp of Γ. Let γ be an element of $\mathrm{SL}_2(\mathbb{Z})$ such that $\gamma \cdot C = \infty$. Then we say that f is* holomorphic at the cusp C *if the q-expansion of $f(\gamma \cdot z)$ is of the form $a_0 + a_1 q^1 + \cdots$.*

We say that f is holomorphic at the cusps *if f is holomorphic for all cusps.*

A modular form is a cusp form *(or cuspidal modular form) if $a_0 = 0$ in the q-expansion of $f(\gamma \cdot z)$ for all γ in $\mathrm{SL}_2(\mathbb{Z})$. We denote the space of cuspidal modular forms of weight k, level Γ and nebentypus ε by $\mathcal{S}_k(\Gamma, \varepsilon)$.*

Lemma 1.1.5. *For any weight k, congruence subgroup Γ and Dirichlet character ε the space of modular forms $\mathcal{M}_k(\Gamma, \varepsilon)$ is finite dimensional.*

Proof. See [4, Proposition 3]. □

Hecke Operators

Definition 1.1.6. *Let m be a positive integer. The* Hecke operator T_m *on the space of modular forms $\mathcal{M}_k(N, \varepsilon)$ is*

$$T_m : \mathcal{M}_k(N, \varepsilon) \to \mathcal{M}_k(N, \varepsilon) : f \mapsto \sum_{\gamma} \varepsilon(d) \frac{\det \gamma^{k-1}}{(cz + d)^k} f(\gamma \cdot z)$$

where the sum is taken over all $\gamma = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z})$ such that $\det(\gamma) = m$ and a, d and b are positive integers with $d > b \geq 0$.

The set of Hecke operators on a given space of modular forms is a finitely generated commutative algebra, see [30, Chapter VII Corollary 5.2] and [34, Theorem 9.23]. Moreover, the following relations show that it is finitely generated by operators T_p with p a prime number

$$T_{a \cdot b} = T_a T_b \qquad \text{if } (a, b) = 1 \text{ and}$$

$$T_{p^r} = \begin{cases} T_p T_{p^{r-1}} & \text{if } p \mid n \\ T_p T_{p^{r-1}} - \varepsilon(p) p^{k-1} T_{p^{r-2}} & \text{else .} \end{cases}$$

One checks that the action of the Hecke operator on the q-expansion of a modular form is given by

$$a_n(T_m(f)) = \sum_{r \mid (n,m)} r^{k-1} \varepsilon(r) a_{mn/r^2}(f).$$

Definition 1.1.7. *We say that a modular form is an* eigenform *if it is a simultaneous eigenvector for all Hecke operators. We say that a modular form is* normalised *if* $a_1(f) = 1$.

Definition 1.1.8. *Let* f *be a normalised eigenform, the field* $\mathbb{Q}(a_n(f) \mid n \in \mathbb{Z}_{\geq 0})$ *is called the coefficient field of* f *and denoted* K_f.

Lemma 1.1.9. *Let* f *be a normalised eigenform, then* $K_f = \mathbb{Q}(a_p(f) \mid p \text{ prime})$. *Moreover,* $[K_f : \mathbb{Q}]$ *is finite.*

Proof. This follows from the fact that the Hecke algebra is generated by a finite number of Hecke operators T_p with p-prime. □

Inner Twists

Definition 1.1.10. *Let* f *be a modular form and* χ *a Dirichlet character, we say that* f *has* complex multiplication by χ *if*

$$\chi(p)a_p(f) = a_p(f)$$

for almost all primes p. *We say that* f *has an* inner twist *by* χ *and* $\sigma \in Aut_{\mathbb{Q}}(K_f)$ *if*

$$\chi(p)a_p(f) = \sigma(a_p(f))$$

for almost all primes p.

Lemma 1.1.11. *Let* f *be a weight* 2 *eigenform of level* $\Gamma_1(N)$ *and trivial nebentypus. If* N *is square-free, then* f *does not have inner twists.*

Proof. This follows from [28, Theorem 3.9 bis]. □

Lemma 1.1.12. *Let* f *be a normalised cuspidal Hecke eigenform of level* $\Gamma_1(N)$.

1. *If* f *has trivial nebentypus, then the coefficient field of* f *is totally real.*
2. *If* f *does not have any inner twist, then* f *has trivial nebentypus.*

Proof. Let K_f be the coefficient field of f, N the level and ε the nebentypus of f. Let $< \cdot, \cdot >$ be the Petersson scalar product. The Hecke operators are self adjoint with respect to $< \cdot, \cdot >$ up to the character ε, see [19, Theorem 5.1], i.e.

$$< T_p \cdot, \cdot >= \varepsilon(p) < \cdot, T_p \cdot >,$$

for all primes p not dividing N. Hence, for any such prime p we obtain

$$\begin{aligned} a_p(f) < f, f > &=< T_p f, f > \\ &= \varepsilon(p) < f, T_p f > \\ &= \varepsilon(p)\widehat{a_p(f)} < f, f >, \end{aligned}$$

where $\widehat{a_p(f)}$ denotes the complex conjugate of $a_p(f)$. In particular,

$$\varepsilon^{-1}(p)a_p(f) = \widehat{a_p(f)}$$

for all primes p not dividing N.

1. If the nebentypus of f is trivial, then by the above
$$a_p(f) = \widehat{a_p(f)},$$
for all primes p not dividing N. In particular, $K_f \subset \mathbb{R}$.
2. Note that $\widehat{\cdot}|_{K_f} \in \mathrm{Aut}_{\mathbb{Q}}(K_f)$ so if ε is not the trivial character, then f has inner twist by ε^{-1}.

□

Remark 1.1.13. *Let f be a cuspidal Hecke eigenform of level $\Gamma_1(N)$.*

1. *If f has complex multiplication by the Dirichlet character χ, then $\chi(p)a_p(f) = a_p(f)$ for almost all primes. If p is a prime such that $\chi(p) \neq 0, 1$ then $a_p(f) = 0$. By Dirichlet's theorem of arithmetic progression the density of the set $\{p \text{ prime } | a_p(f) = 0\}$ is at least $\frac{1}{2}$.*
2. *Suppose that f has quadratic coefficient field K_f and an inner twist by the Dirichlet character χ and non-trivial automorphism $\sigma \in Gal(K_f/\mathbb{Q})$. Let p be a prime such that $\chi(p) = 1$, then $\sigma(a_p(f)) = \chi(p) \cdot a_p(f) = a_p(f)$ so $a_p(f) \in \mathbb{Q}$. If n is the modulus of the character χ and p is a prime such that $p \equiv 1 \mod n$, then $\chi(p) = 1$ and $a_p(f) \in \mathbb{Q}$. Again by Dirichlet's theorem of arithmetic progression the density of the set $\{p \text{ prime } | a_p(f) \in \mathbb{Q}\}$ is at least $\frac{1}{\phi(n)}$.*
3. *Let f be a weight k form without inner twists and let d be the extension degree of K_f over $\mathbb{Q}$. Then Kumar Murty conjectured the following [23, Conjecture 3.4]*
$$\#\{p < x \text{ prime } \mid a_p(f) \in \mathbb{Q}\} \sim c_f \cdot \begin{cases} \sqrt{x}/\log x & \text{if } k = d = 2, \\ \log\log x & \text{if } k = 2 \text{ and } d = 3, \\ & \text{or } k = 3 \text{ and } d = 2, \\ 1 & \text{else.} \end{cases}$$

1.2 The Heuristic Model

For the remainder of this chapter, f will be a normalised cuspidal Hecke eigenform of weight 2 and level $\Gamma_1(N)$ without inner twist and with quadratic coefficient field K_f. By Lemma 1.1.12 K_f is totally real and f has trivial nebentypus. Let D be the positive square-free integer such that $K_f = \mathbb{Q}(\sqrt{D})$. Denote by $\bar{\cdot}$ the unique non-trivial element of the Galois group of $K_f/\mathbb{Q}$. Define

$$Z_p := a_p(f) - \overline{a_p(f)}.$$

Note that $Z_p \in \sqrt{D}\mathbb{Z}$ since $a_p(f)$ is an algebraic integer in K_f. Moreover,

$$\begin{aligned} a_p(f) \in \mathbb{Q} \Leftrightarrow & Z_p = 0 \\ \Leftrightarrow & \frac{-m\sqrt{D}}{2} < Z_p < \frac{m\sqrt{D}}{2} \text{ and} \\ & Z_p \equiv 0 \mod m\sqrt{D}\mathbb{Z} \text{ for all } m \in \mathbb{Z}_{>0}. \end{aligned}$$

In other words, the condition $a_p(f) \in \mathbb{Q}$ is equivalent to a condition on the real and ℓ-adic absolute value of Z_p for finite places ℓ dividing m for any positive integer m. Denote $\pi(x) := \#\{p < x \text{ prime}\}$ and

$$P(x) := \frac{\#\{p < x \text{ prime} \mid Z_p = 0\}}{\pi(x)},$$

$$P_m(x) := \frac{\#\{p < x \text{ prime} \mid Z_p \equiv 0 \mod m\sqrt{D}\mathbb{Z}\}}{\pi(x)},$$

$$P^m(x) := \frac{\#\left\{p < x \text{ prime} \mid Z_p \in \left]\frac{-m\sqrt{D}}{2}, \frac{m\sqrt{D}}{2}\right[\right\}}{\pi(x)}.$$

Since $|a_p(f)| = \mathcal{O}(\sqrt{p})$ (cf. [19, Lemma 2]),

$$\lim_{m\to\infty} P_m(x) = P(x) \text{ and } \lim_{m\to\infty} P^m(x) = 1$$

for all $x > 2$. In particular,

$$\lim_{m\to\infty} \frac{P^m(x) \cdot P_m(x)}{P(x)} = 1 \text{ for all } x > 2$$

so

$$\lim_{x\to\infty} \lim_{m\to\infty} \frac{P^m(x) \cdot P_m(x)}{P(x)} = 1.$$

Our first assumption states that the order of the double limit can be reversed.

Assumption 1.2.1. *Let f be as above. Then*

$$\lim_{m\to|\infty}\lim_{x\to\infty}\frac{P^m(x)\cdot P_m(x)}{P(x)}=1,$$

where $\lim_{m\to|\infty}$ denotes the limit over m taken by divisibility.

We say that a is the limit of a series $(a_m)_m$ by divisibility if for all $\varepsilon>0$ there exists a positive integer m_0 such that for all $m\in m_0\mathbb{Z}_{>0}$

$$|a_m-a|<\varepsilon.$$

In Section 1.5, we will show that the convergence of the double limit in Assumption 1.2.1 follows from the weaker condition that there exists at least one positive integer m satisfying the following assumption.

Assumption 1.2.2. *Let f be as above and m a positive integer. Then*

$$\lim_{x\to\infty}\frac{P^m(x)\cdot P_m(x)}{P(x)}=\alpha_m,$$

with $0<\alpha_m<\infty$.

Note that the '$0<\alpha_m$' part of the statement will follow immediately from Lemma 1.4.1. Assumption 1.2.2 is enough to prove the asymptotic behaviour of $\#\{p<x \text{ prime} \mid a_p\in\mathbb{Q}\}$. However, to prove Theorem 1.5.3 we will need the stronger Assumption 1.2.1.

By deriving suitable expressions for the arithmetic part $P_m(x)$ and the real part $P^m(x)$, respectively, we will obtain the asymptotic behaviour of $P(x)$ predicted by Conjecture 0.0.1 from Assumption 1.2.2. Additionally, under the stronger condition of Assumption 1.2.1 we will obtain an explicit constant. In Section 1.4, we use Chebotarev's density theorem to prove an explicit formula for the factor $P_m(x)$. For the factor at the infinite place we will need an additional assumption. We describe this assumption and the results that follow in the next section.

1.3 The Place at Infinity

In this section, we describe a heuristic formula for the factor

$$P^m(x)=\frac{\#\{p<x \text{ prime} \mid Z_p\in]\frac{-m\sqrt{D}}{2},\frac{m\sqrt{D}}{2}[\}}{\pi(x)},$$

which we derive from a natural assumption. We use results from a recent paper by F. Fité, K. Kedlaya, V. Rotger and A. Sutherland that describes the joint distribution of the coefficients of the normalised L_p-polynomial of hyperelliptic curves of genus 2 under the assumption of the Sato-Tate conjecture for abelian varieties (cf. [12]). Note that we use the Sato-Tate conjecture for abelian varieties rather than the Sato-Tate distribution for modular forms. The latter describes the distribution of the real absolute value of the coefficients but claims nothing about the coefficients as elements of the number field K_f.

Let f be as above. Then one can associate via Shimura's construction (cf. [10, section 1.7]) an abelian variety $\mathcal{A}_f$ of dimension $[K_f : \mathbb{Q}]$ to the eigenform f. For every prime p the L_p-polynomial associated to the variety $\mathcal{A}_f$ splits as the L_p-polynomial of the eigenform and its Galois conjugate over K_f. More precisely, let $L_p(T) := p^2T^4 + pX_pT^3 + Y_pT^2 + X_pT + 1$ be the L_p-polynomial of $\mathcal{A}_f$, then

$$L_p(T) = \big(pT^2 - a_p(f)T + 1\big)\big(pT^2 - \overline{a_p(f)}T + 1\big).$$

Hence,

$$a_p(f) = -\frac{X_p}{2} \pm \sqrt{2p - Y_p + \frac{X_p^2}{4}}.$$

Note that from the L_p-polynomial of $\mathcal{A}_f$ we cannot deduce $a_p(f)$ completely. Indeed, we only obtain its Galois orbit. However, we can decide whether or not Z_p lies in a symmetrical interval around zero since

$$|Z_p| = \sqrt{8p - 4Y_p + X_p^2}.$$

Let $a_{1,p} = \frac{X_p}{\sqrt{p}}$ and $a_{2,p} = \frac{Y_p}{p}$ be the coefficients of the normalised L_p-polynomial $L_p(T/\sqrt{p})$. Then

$$Z_p \in \Big]-\frac{m\sqrt{D}}{2}, \frac{m\sqrt{D}}{2}\Big[\Leftrightarrow \sqrt{2 - a_{2,p} + a_{1,p}^2/4} < \frac{m\sqrt{D}}{4\sqrt{p}}.$$

The generalised Sato-Tate conjecture states that the joint distribution of $(a_{1,p}, a_{2,p})$ is completely determined by the so called Sato-Tate group. In [12] Fité et al. study the joint distribution of $(a_{1,p}, a_{2,p})$ for abelian surfaces. More precisely, they prove the following theorem.

Theorem 1.3.1. *Let $\mathcal{A}$ be an abelian surface. There exist exactly 52 Sato-Tate groups for abelian surfaces, of which only 34 occur over $\mathbb{Q}$. Moreover, the conjugacy class of the Sato-Tate group of $\mathcal{A}$ is uniquely determined by its Galois type (cf. [12, Def. 1.3]) and vice versa.*

Proof. This is Theorem 1.4 in [12]. □

Corollary 1.3.2. *Let f and $\mathcal{A}_f$ be as above. The generalised Sato-Tate conjecture holds for A_f and the joint distribution of $(a_{1,p}, a_{2,p})$ is given by*

$$\Phi : T \to \mathbb{R} : (x, y) \mapsto \frac{1}{2\pi^2}\sqrt{\frac{(y - 2x + 2)(y + 2x + 2)}{x^2 - 4y + 8}},$$

where T is the following subset of the plane (Fig. 1.2)

$$T := \left\{(x, y) |\, y + 2 > |2x| \text{ and } 4y < x^2 + 8\right\}.$$

Moreover, let δ be the measure with density Φ and let S be a measurable set. Then

$$\delta(S) \sim \frac{\#\{p < x \text{ prime} \mid (a_{1,p}, a_{2,p}) \in S\}}{\pi(x)}.$$

Proof. The $\mathbb{Q}$-algebra of endomorphisms of $\mathcal{A}_f$ over $\mathbb{Q}$ is K_f. Moreover, the $\mathbb{Q}$-algebra of endomorphisms of $\mathcal{A}_f$ over $\overline{\mathbb{Q}}$ is also K_f since f does not have any inner twists (cf. [26, Theorem 5]). So all endomorphisms of $\mathcal{A}_f$ over $\overline{\mathbb{Q}}$ are already defined over $\mathbb{Q}$. In particular, the Galois type of $\mathcal{A}_f$ is

$$[\mathrm{Gal}(\mathbb{Q}/\mathbb{Q}), K_f \otimes_{\mathbb{Z}} \mathbb{R}] = [1, \mathbb{R} \times \mathbb{R}],$$

since K_f is a real quadratic number field. The generalised Sato-Tate conjecture is proven for abelian surfaces of this Galois type by Christian Johansson in [15, Proposition 22]. It follows from Tables 8 and 11 in [12] that the Sato-Tate group of $\mathcal{A}_f$ is $SU(2) \times SU(2)$. Finally, the joint distribution function of this group is given by [12, Table 5]. □

The following result is proven by K. Koo, W. Stein and G. Wiese (cf. [17, Corollary 1.1]). We give an alternative proof using recent results on Sato-Tate equidistribution.

Corollary 1.3.3. *Let f be as above. The set $\{p < x \text{ prime} \mid a_p(f) \in \mathbb{Q}\}$ has density zero.*

Proof. Let $S = \{(x, y) \mid \sqrt{x^2 - 4y + 8} = 0\}$ by Corollary 1.3.2

$$\frac{\#\{p < x \text{ prime} \mid a_p(f) \in \mathbb{Q}\}}{\pi(x)} = \frac{\#\{p < x \text{ prime} \mid (a_{1,p}, a_{2,p}) \in S\}}{\pi(x)} \sim \delta(S).$$

Clearly, $\delta(S) = 0$. □

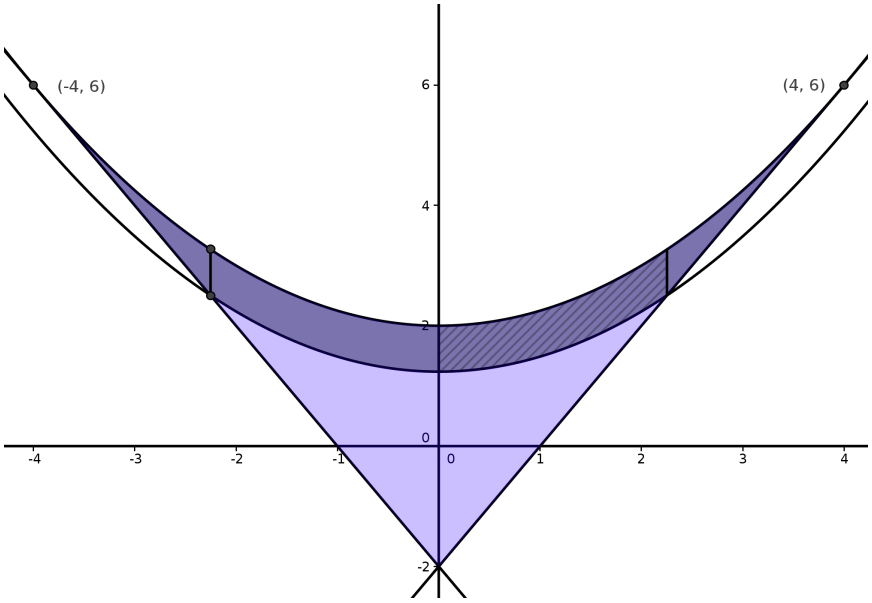


Figure 1.2: The areas T (dark and light blue), T_ε (dark blue) and T_ε^1 (hatched).

Define for any $\varepsilon > 0$

$$T_\varepsilon := \left\{ (x,y) \in T \mid \sqrt{x^2/4 - y + 2} < \varepsilon \right\}.$$

Then

$$Z_p \in \left] -\frac{m\sqrt{D}}{2}, \frac{m\sqrt{D}}{2} \right[\Leftrightarrow (a_{1,p}, a_{2,p}) \in T_{m\sqrt{D}/(4\sqrt{p})}.$$

By Corollary 1.3.2

$$\delta(T_{m\sqrt{D}/(4\sqrt{p})}) \sim \frac{\#\left\{ q < x \text{ prime} \mid \sqrt{2 - a_{2,q} + a_{1,q}^2/4} < \frac{m\sqrt{D}}{4\sqrt{p}} \right\}}{\pi(x)}$$

since $T_{m\sqrt{D}/(4\sqrt{p})}$ is a measurable set. We will need the following heuristic assumption.

Assumption 1.3.4. *Let m be a positive integer. Then*

$$P^m(x) \sim \frac{1}{\pi(x)} \sum_{p=2}^{x} \delta(T_{m\sqrt{D}/(4\sqrt{p})})$$

where the sum is taken only over primes.

The idea behind this assumption is that approximating the probability of $\left|\frac{Z_p}{2\sqrt{p}}\right| < \frac{m\sqrt{D}}{4\sqrt{p}}$ (which is either 1 or 0) by the probability that $\left|\frac{Z_q}{2\sqrt{q}}\right| < \frac{m\sqrt{D}}{4\sqrt{p}}$ for any prime q is 'good on average'. Note that for each individual prime p this approximation is bad. However, the assumption states that summing over all primes p does yield a good approximation.

Lemma 1.3.5. *The measure of the set T_ε is*

$$\delta(T_\varepsilon) = \frac{32}{3\pi^2}\varepsilon + o(\varepsilon).$$

Proof. It suffices to determine the integral $\delta(T_\varepsilon) = \int_{T_\varepsilon} \Phi \mathrm{d}A$ up to quadratic terms in ε. Since the density function Φ is even with respect to the first variable x we can restrict to positive x. We split the integration domain T_ε in two parts (Fig. 1.2)

$$T_\varepsilon^1 := \{(x,y) \in T_\varepsilon \mid 0 < x < 4 - 2\varepsilon\} \text{ and}$$

$$T_\varepsilon^2 := \{(x,y) \in T_\varepsilon \mid 4 - 2\varepsilon < x < 4\}.$$

So

$$\delta(T_\varepsilon) = 2\int_{T_\varepsilon^1} \Phi \mathrm{d}A + 2\int_{T_\varepsilon^2} \Phi \mathrm{d}A.$$

Parametrisations of both sets are given, respectively, by

$$T_\varepsilon^1 = \{(u, u^2/4 + 2 - v^2) \mid 0 < u < 4 - 2\varepsilon \ \wedge \ 0 < v < \varepsilon\} \text{ and}$$

$$T_\varepsilon^2 = \{(u, u^2/4 + 2 - v^2) \mid 4 - 2\varepsilon < u < 4 \ \wedge \ 0 < v < 2 - u/2\}.$$

The determinant of the Jacobian of the parametrisation, $\mathrm{d}A$, is $2v\mathrm{d}v\mathrm{d}u$ so

$$\begin{aligned}
&2\Phi(u, u^2/4 + 2 - v^2)\mathrm{d}A \\
&= \frac{2}{2\pi^2}\sqrt{\frac{(u^2/4 + 2 - v^2 - 2u + 2)(u^2/4 + 2 - v^2 + 2u + 2)}{u^2 - u^2 - 8 + 4v^2 + 8}}2v\mathrm{d}v\mathrm{d}u \\
&= \frac{1}{4\pi^2}\sqrt{(u^2 + 16 - 4v^2 - 8u)(u^2 + 16 - 4v^2 + 8u)}\mathrm{d}v\mathrm{d}u \\
&= \frac{1}{4\pi^2}\sqrt{(u^2 + 16 - 4v^2)^2 - 64u^2}\mathrm{d}v\mathrm{d}u.
\end{aligned}$$

First we show that

$$2\int_{T_\varepsilon^2} \Phi \mathrm{d}A = \mathcal{O}(\varepsilon^2).$$

It suffices to show that the limit of $\frac{1}{\varepsilon^2}2\int_{T^2_\varepsilon}\Phi \mathrm{d}A$ is finite if ε tends to zero. Let us compute

$$\lim_{\varepsilon\to 0}\frac{1}{\varepsilon^2}2\int_{T^2_\varepsilon}\Phi \mathrm{d}A = \lim_{\varepsilon\to 0}\frac{1}{\varepsilon^2}\frac{1}{4\pi^2}\int_{4-2\varepsilon}^{4}\int_0^{2-u/2}\sqrt{(u^2+16-4v^2)^2-64u^2}\mathrm{d}v\mathrm{d}u.$$

Then by l'Hôpital's rule we obtain

$$\begin{aligned}
\lim_{\varepsilon\to 0}\frac{1}{\varepsilon^2}2\int_{T^2_\varepsilon}\Phi \mathrm{d}A &\overset{\text{H}}{=} \lim_{\varepsilon\to 0}\frac{1}{\varepsilon}\frac{1}{2\pi^2}\int_0^{\varepsilon}\sqrt{(\varepsilon^2+16-4v^2)^2-64\varepsilon^2}\mathrm{d}v \\
&< \lim_{\varepsilon\to 0}\frac{1}{\varepsilon}\frac{1}{2\pi^2}\int_0^{\varepsilon}\sqrt{(\varepsilon^2+16)^2-64\varepsilon^2}\mathrm{d}v \\
&= \lim_{\varepsilon\to 0}\frac{1}{2\pi^2}\sqrt{(\varepsilon^2+16)^2-64\varepsilon^2} \\
&= \frac{8}{\pi^2} < \infty.
\end{aligned}$$

In particular, we obtain

$$\delta(T_\varepsilon) = 2\int_{T^1_\varepsilon}\Phi \mathrm{d}A + \mathcal{O}(\varepsilon^2).$$

Finally, denote $\phi(u,v) = 2\Phi\frac{\mathrm{d}A}{\mathrm{d}v\mathrm{d}u} = \frac{1}{4\pi^2}\sqrt{(u^2+16-4v^2)^2-64u^2}$. Then, again by l'Hôpital's rule and Leibniz rule for double integration

$$\begin{aligned}
\lim_{\varepsilon\to 0}\frac{\frac{32}{3\pi^2}\varepsilon-\delta(T_\epsilon)}{\varepsilon} &= \lim_{\varepsilon\to 0}\frac{1}{\varepsilon}\left(\frac{32}{3\pi^2}\varepsilon-\int_0^{4-2\varepsilon}\int_0^{\varepsilon}\phi(u,v)\mathrm{d}v\mathrm{d}u\right) \\
&\overset{\text{H}}{=} \lim_{\varepsilon\to 0}\frac{32}{3\pi^2}-\int_0^{4-2\varepsilon}\phi(u,\varepsilon)\mathrm{d}u+2\int_0^{\varepsilon}\phi(4-2\varepsilon,v)\mathrm{d}v \\
&= \frac{32}{3\pi^2}-\int_0^4\phi(u,0)\mathrm{d}u+0 \\
&= \frac{32}{3\pi^2}-\frac{1}{4\pi^2}\int_0^4\sqrt{(u^2+16)^2-64u^2}\mathrm{d}u \\
&= \frac{32}{3\pi^2}-\frac{1}{4\pi^2}\int_0^4(16-u^2)\mathrm{d}u \\
&= \frac{32}{3\pi^2}-\frac{1}{4\pi^2}\left[16u-\frac{u^3}{3}\right]_0^4 \\
&= 0.
\end{aligned}$$

□

Corollary 1.3.6. *For all $m > 0$ satisfying Assumption 1.3.4*

$$P^m(x) \sim \frac{16m\sqrt{D}}{3\pi^2\sqrt{x}}.$$

Proof. By Assumption 1.3.4, Lemma 1.3.5 with $\varepsilon = m\sqrt{D}/(4\sqrt{p})$ and the fact that $\sum_{p=2}^{x} \frac{1}{2\sqrt{p}} \sim \frac{\sqrt{x}}{\log x}$, respectively, we obtain

$$\begin{aligned} P^m(x) &\sim \frac{1}{\pi(x)} \sum_{p=2}^{x} \delta(T_{m\sqrt{D}/(4\sqrt{p})}) \\ &\sim \frac{1}{\pi(x)} \frac{16m\sqrt{D}}{3\pi^2} \sum_{p=2}^{x} \frac{1}{2\sqrt{p}} \\ &\sim \frac{16m\sqrt{D}}{3\pi^2} \frac{\sqrt{x}}{\pi(x)\log x} \\ &\sim \frac{16m\sqrt{D}}{3\pi^2\sqrt{x}}. \end{aligned}$$

□

1.4 The Finite Places

In this section, we describe the remaining factor $P_m(x)$. No heuristic is needed to obtain the results of this section. For each positive integer m, the factor P_m can be computed by Chebotarev's density theorem and the image of the mod m Galois representation attached to f.

Let f be as above and denote the ring of integers of its coefficient field by $\mathcal{O}_f$. Let m be a positive integer and denote $\mathcal{O}_m := \mathcal{O}_f \otimes_{\mathbb{Z}} \mathbb{Z}/m\mathbb{Z}$. Denote the absolute Galois group of $\mathbb{Q}$ by $G_{\mathbb{Q}}$. Then the action of $G_{\mathbb{Q}}$ on the m-torsion points of $\mathcal{A}_f$ induces a mod-m representation

$$\rho_m : G_{\mathbb{Q}} \to GL_2(\mathcal{O}_m).$$

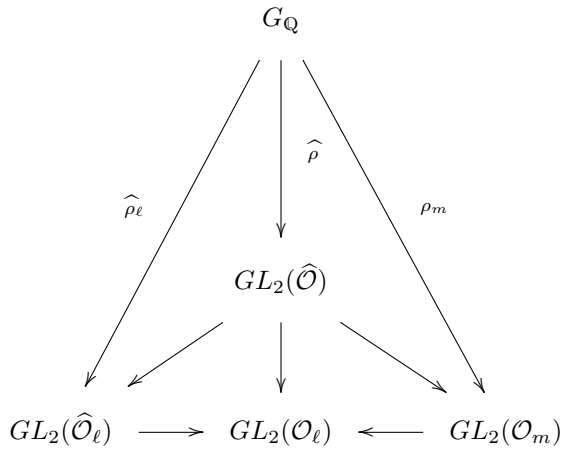
By taking the inverse limit over all integers m we obtain an adelic representation

$$\widehat{\rho} := \varprojlim_m \rho_m : G_{\mathbb{Q}} \to GL_2(\widehat{\mathcal{O}}),$$

where $\widehat{\mathcal{O}} = \mathcal{O}_f \otimes_{\mathbb{Z}} \widehat{\mathbb{Z}}$ is the ring of finite adèles of K_f. If ℓ is a prime, we obtain an ℓ-adic representation by taking the limit over all powers of ℓ torsion points

$$\widehat{\rho}_\ell := \varprojlim_k \rho_{\ell^k} : G_{\mathbb{Q}} \to GL_2(\widehat{\mathcal{O}}_\ell),$$

with $\widehat{\mathcal{O}}_\ell = \mathcal{O}_f \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Note that by definition $\widehat{\rho} = \prod_\ell \widehat{\rho}_\ell$. Moreover, for any positive integer m and any prime ℓ dividing m the following diagram commutes.



Let $\overline{\cdot}$ be the unique non-trivial element of the Galois group of K_f over $\mathbb{Q}$. Then $\overline{\cdot}$ induces by the tensor product endomorphisms on $\widehat{\mathcal{O}}$, $\widehat{\mathcal{O}}_\ell$ and $\mathcal{O}_m$. By abuse of notation we denote each of these morphisms by $\overline{\cdot}$. Hence, we obtain the following maps

$$Z : GL_2(\widehat{\mathcal{O}}) \to \widehat{\mathcal{O}} : \sigma \mapsto \operatorname{tr}\sigma - \overline{\operatorname{tr}\sigma},$$

$$Z : GL_2(\widehat{\mathcal{O}}_\ell) \to \widehat{\mathcal{O}}_\ell : \sigma \mapsto \operatorname{tr}\sigma - \overline{\operatorname{tr}\sigma} \text{ and}$$

$$Z : GL_2(\mathcal{O}_m) \to \mathcal{O}_m : \sigma \mapsto \operatorname{tr}\sigma - \overline{\operatorname{tr}\sigma}.$$

Consider the following (subsets) of the images of the representations:

$$\widehat{\mathcal{G}} := \operatorname{Im}\widehat{\rho}, \qquad \widehat{\mathcal{G}}^t := \{\sigma \in \widehat{\mathcal{G}} \mid Z(\sigma) = 0\},$$

$$\widehat{\mathcal{G}}_\ell := \operatorname{Im}\widehat{\rho}_\ell, \qquad \widehat{\mathcal{G}}_\ell^t := \{\sigma \in \widehat{\mathcal{G}}_\ell \mid Z(\sigma) = 0\},$$

$$\mathcal{G}_m := \operatorname{Im}\rho_m, \qquad \mathcal{G}_m^t := \{\sigma \in \mathcal{G}_m \mid Z(\sigma) = 0\}.$$

Define for each positive integer m

$$F_m := m\frac{\#\mathcal{G}_m^t}{\#\mathcal{G}_m}.$$

Lemma 1.4.1. *Let m be a positive integer, then*

$$P_m(x) \sim \frac{1}{m}F_m.$$

Proof. Let m be a positive integer. Then by Chebotarev's density theorem the conjugacy class of Frob_p is equidistributed in $\mathcal{G}_m$ where p varies over all primes not dividing mN, i.e. for all conjugacy classes Cl of $\mathcal{G}_m$ we have

$$\#\{p < x \text{ prime } \mid p \nmid mN \text{ and } \rho_m(\mathrm{Frob}_p) \in Cl\} \sim \frac{\#Cl}{\#\mathcal{G}_m}\pi(x).$$

Denote by $\imath$ the morphism of $\mathcal{O}_f$ to $\mathcal{O}_m$ given by sending z to $z \otimes 1$. If p is a prime that does not divide mN, then $\mathrm{tr}\,(\rho_m(\mathrm{Frob}_p)) = \imath(a_p(f)) \in \mathcal{O}_m$ (cf. [7, Theorem 3.1.a]). Note that $Z(\sigma)$ only depends on the conjugacy class of the matrix σ so $Z(\rho_m(\mathrm{Frob}_p))$ is well defined. Moreover,

$$\imath(Z_p) = Z(\rho_m(\mathrm{Frob}_p)) \in \mathcal{O}_m,$$

since $Z_p = a_p(f) - \overline{a_p(f)}$ by definition. In particular, $Z_p \equiv 0 \mod m\sqrt{D}\mathbb{Z}$ if and only if $Z(\rho_m(\mathrm{Frob}_p)) = 0$ as an element of $\mathcal{O}_m$. Hence,

$$\begin{aligned} P_m(x) &= \frac{\#\{p < x \text{ prime} \mid Z_p \equiv 0 \mod m\sqrt{D}\mathbb{Z}\}}{\pi(x)} \\ &\sim \frac{\#\{p < x \text{ prime } \mid p \nmid mN \text{ and } Z(\rho_m(\mathrm{Frob}_p)) = 0\}}{\pi(x)} \\ &\sim \frac{\#\{\sigma \in \mathcal{G}_m \mid Z(\sigma) = 0\}}{\#\mathcal{G}_m} \\ &= \frac{\#\mathcal{G}_m^t}{\#\mathcal{G}_m}. \end{aligned}$$

□

The following theorem will enable us to give explicit formulas for the cardinalities of $\mathcal{G}_{\ell^k}$ and $\{\mathcal{G}_{\ell^k} \mid Z(\sigma) = 0\}$ for almost all primes.

Define

$$\widehat{\mathcal{A}}_\ell = \{\sigma \in GL_2(\widehat{\mathcal{O}}_\ell) \mid \det\sigma \in \mathbb{Z}_\ell^\times\}.$$

Theorem 1.4.2. *Let f be a weight 2 normalised cuspidal Hecke eigenform without inner twists. Then for all primes ℓ the image of the ℓ-adic representation, $\widehat{\mathcal{G}}_\ell$, is an open subgroup of $\widehat{\mathcal{A}}_\ell$. Moreover, $\widehat{\mathcal{G}}_\ell = \widehat{\mathcal{A}}_\ell$ for almost all primes. We say that the prime ℓ has large image if the inclusion is an equality, and we say that ℓ is exceptional otherwise.*

Proof. This is a special case of [27, Theorem 0.1]. □

Let ℓ be a prime and k a positive integer. Denote $\mathcal{A}_{\ell^k}$ for the image of $\widehat{\mathcal{A}}_\ell$ under the natural projection modulo ℓ^k and $\mathcal{A}_{\ell^k}^t = \{\sigma \in \mathcal{A}_{\ell^k} \mid Z(\sigma) = 0\}$. If ℓ is a prime with

large image, then $\mathcal{A}_{\ell^k} = \mathcal{G}_{\ell^k}$ so

$$F_{\ell^k} = \ell^k \frac{\#\mathcal{A}^t_{\ell^k}}{\#\mathcal{A}_{\ell^k}}.$$

Note that $\widehat{\mathcal{O}}_\ell \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ if ℓ splits in $\mathcal{O}_f$. If ℓ is inert in $\mathcal{O}_f$, then $\widehat{\mathcal{O}}_\ell$ is the ring of integers of the unique unramified quadratic extension of $\mathbb{Q}_\ell$, denoted by $\mathbb{Z}_{\ell^2}$. In the next two sections, we describe the cardinalities of $\mathcal{A}_{\ell^k}$ and $\mathcal{A}^t_{\ell^k}$ in the inert and split case, respectively. For both cases we will need the following lemma and its corollary.

Lemma 1.4.3. *Let R be a finite local ring with maximal ideal $\mathfrak{m}$. Denote $r = \#R$ and $m = \#\mathfrak{m}$. Then*

$$\#GL_2(R) = (r^2 - m^2) \cdot r \cdot (r - m).$$

Proof. Let $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_{2\times 2}(R)$. Then

$$\sigma \in GL_2(R) \Leftrightarrow ad \not\equiv bc \mod \mathfrak{m}.$$

The vector (a, b) can be any vector not contained in $\mathfrak{m} \times \mathfrak{m}$. There are $r^2 - m^2$ such vectors. We consider two cases depending on the valuation of b in R.

First, if $b \in \mathfrak{m}$, then $a \in R^\times$ so

$$ad \not\equiv bc \mod \mathfrak{m} \Leftrightarrow d \not\equiv bca^{-1} \mod \mathfrak{m}$$

$$\Leftrightarrow d \not\equiv 0 \mod \mathfrak{m}.$$

Hence, c can be any element of R and d any element of $R^\times$. There are $r \cdot (r - m)$ such vectors (c, d).

Second, if $b \notin \mathfrak{m}$, then

$$ad \not\equiv bc \mod \mathfrak{m} \Leftrightarrow adb^{-1} \not\equiv c \mod \mathfrak{m}.$$

Hence, d can be any element of R and c any element not contained in $adb^{-1} + \mathfrak{m}$. There are $r \cdot (r - m)$ such vectors.

In either case we obtain $r \cdot (r - m)$ possibilities for the second vector. Hence, $\#GL_2(R) = (r^2 - m^2) \cdot r \cdot (r - m)$. □

Corollary 1.4.4. *Let ℓ be a prime and k a positive integer. Then*

$$\#GL_2(\mathbb{Z}/\ell^k\mathbb{Z}) = \ell^{4k-3}(\ell^2 - 1)(\ell - 1).$$

Inert Primes

Let f be as above, suppose that ℓ is an odd inert prime in $\mathcal{O}_f$, the ring of integers of the coefficient field of f. Then

$$\widehat{\mathcal{O}}_\ell \cong \mathcal{O}_f \otimes_{\mathbb{Z}} \mathbb{Z}_\ell \cong \mathbb{Z}_{\ell^2}.$$

Recall that $\mathbb{Z}_{\ell^2}$ is the ring of integers of the unique unramified quadratic extension of $\mathbb{Q}_\ell$. If $\alpha \in \overline{\mathbb{Q}}$ with α^2 a square-free integer that is congruent to a non-quadratic residue modulo ℓ, then $\mathbb{Q}_\ell(\alpha)$ is an unramified quadratic extension of $\mathbb{Q}_\ell$ with ring of integers $\mathbb{Z}_\ell[\alpha]$, hence

$$\mathbb{Z}_{\ell^2} \cong \mathbb{Z}_\ell[\alpha].$$

Moreover, the morphism $\bar{\cdot}$ is given by

$$\bar{\cdot} : \mathbb{Z}_\ell[\alpha] \to \mathbb{Z}_\ell[\alpha] : a + \alpha b \mapsto a - \alpha b.$$

If ℓ is an inert prime in $\mathcal{O}_f$, then we can take $\alpha = \sqrt{D}$ with D the square-free integer such that $K_f = \mathbb{Q}(\sqrt{D})$. If moreover the ℓ-adic representation attached to f has large image in the sense of Theorem 1.4.2, the sets $\mathcal{G}_{\ell^k}$ and $\{\sigma \in \mathcal{G}_{\ell^k} \mid Z(\sigma) = 0\}$ are, respectively,

$$\mathcal{A}_{\ell^k,I} := \left\{\sigma \in GL_2(\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]) \mid \det\sigma \in \mathbb{Z}/\ell^k\mathbb{Z}^\times\right\} \text{ and}$$

$$\mathcal{A}^t_{\ell^k,I} := \left\{\sigma \in GL_2(\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]) \mid \det\sigma \in \mathbb{Z}/\ell^k\mathbb{Z}^\times \wedge\ \operatorname{tr}\sigma \in \mathbb{Z}/\ell^k\mathbb{Z}\right\}.$$

Proposition 1.4.5. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#\mathcal{A}_{\ell^k,I} = \ell^{7k-5}(\ell^4-1)(\ell-1).$$

Proof. There are $(\ell^2-1)\ell^{2k-2}$ units $\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$, of which $(\ell-1)\ell^{k-1}$ units are embedded in $\mathbb{Z}/\ell^k\mathbb{Z}$. By Lemma 1.4.3

$$\#GL_2(\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]) = \ell^{8k-6}(\ell^4-1)(\ell^2-1).$$

Since any unit occurs equally many times as the determinant of a matrix in $GL_2(\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha])$ we obtain

$$\begin{aligned}\#\mathcal{A}_{\ell^k,I} &= \#GL_2(\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha])\frac{\#\mathbb{Z}/\ell^k\mathbb{Z}^\times}{\#\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]^\times}\\ &= \ell^{8k-6}(\ell^4-1)(\ell^2-1)\frac{(\ell-1)\ell^{k-1}}{(\ell^2-1)\ell^{2k-2}}\\ &= \ell^{7k-5}(\ell^4-1)(\ell-1).\end{aligned}$$

□

Proposition 1.4.6. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#\mathcal{A}^t_{\ell^k,I} = \frac{(\ell-1)}{(\ell+1)}\ell^{6k-2}\left(\ell^2+\ell+1-\ell^{-2k}\right).$$

Proof. See Section 1.B. □

Split Primes

Let f be as above, suppose that ℓ is an odd split prime in $\mathcal{O}_f$. Then

$$\widehat{\mathcal{O}}_\ell \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$$

and the morphism induced by the unique non-trivial element of the Galois group of K_f over $\mathbb{Q}$ by the tensor product over $\mathbb{Z}$ with $\mathbb{Z}_\ell$ is

$$\bar{\cdot} : \mathbb{Z}_\ell \times \mathbb{Z}_\ell \to \mathbb{Z}_\ell \times \mathbb{Z}_\ell : (a,b) \mapsto (b,a).$$

In particular, the embedding of $\mathbb{Z}$ into $\widehat{\mathcal{O}}_\ell$ is diagonal. Suppose that ℓ has large image in the sense of Theorem 1.4.2. Then the image of the Galois representation modulo ℓ^k and its subset $\{\sigma \in \mathcal{G}_{\ell^k} \mid \operatorname{tr}\sigma \in \mathbb{Z}/\ell^k\mathbb{Z}\}$ are, respectively,

$$\mathcal{A}_{\ell^k,S} := \{(\tau,\tau') \in GL_2(\mathbb{Z}/\ell^k\mathbb{Z})^2 \mid \det\tau = \det\tau'\} \text{ and}$$

$$\mathcal{A}^t_{\ell^k,S} := \{(\tau,\tau') \in GL_2(\mathbb{Z}/\ell^k\mathbb{Z})^2 \mid \text{char. poly. } \tau = \text{char. poly. } \tau'\},$$

where char. poly. $\tau = X^2 - \operatorname{tr}\tau X + \det\tau$ denotes the characteristic polynomial of τ.

Proposition 1.4.7. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#\mathcal{A}_{\ell^k,S} = \ell^{7k-5}(\ell^2-1)^2(\ell-1).$$

Proof. The determinant is equidistributed in the units of $(\mathbb{Z}/\ell^k\mathbb{Z})^2$. By Corollary 1.4.4 $\#GL_2(\mathbb{Z}/\ell^k\mathbb{Z})^2 = \left(\ell^{4k-3}(\ell^2-1)(\ell-1)\right)^2$. Moreover, there are $\left(\ell^{k-1}(\ell-1)\right)^2$ units in $(\mathbb{Z}/\ell^k\mathbb{Z})^2$ and $\ell^{k-1}(\ell-1)$ of those units are contained in $\mathbb{Z}/\ell^k\mathbb{Z}$. Hence,

$$\begin{aligned}\#\mathcal{A}_{\ell^k,S} &= \#GL_2(\mathbb{Z}/\ell^k\mathbb{Z})^2 \frac{\#\mathbb{Z}/\ell^k\mathbb{Z}^\times}{\#(\mathbb{Z}/\ell^k\mathbb{Z}^\times)^2} \\ &= \left(\ell^{4k-3}(\ell^2-1)(\ell-1)\right)^2 \frac{\ell^{k-1}(\ell-1)}{\left(\ell^{k-1}(\ell-1)\right)^2} \\ &= \ell^{7k-5}(\ell^2-1)^2(\ell-1).\end{aligned}$$

□

Proposition 1.4.8. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#\mathcal{A}^t_{\ell^k,S} = \frac{(\ell-1)}{(\ell+1)}\ell^{6k-4}\left(\ell^4+\ell^3-\ell^2-2\ell-\ell^{-2k+2}\right).$$

Proof. See Section 1.B. □

The Limit of F_m

In this section, we describe the behaviour of the factor F_m and its limit by divisibility.

Lemma 1.4.9. *Let ℓ be a prime. Then*

$$\widehat{F}_\ell := \lim_{k\to\infty} \ell^k \frac{\#\mathcal{G}^t_{\ell^k}}{\#\mathcal{G}_{\ell^k}} < \infty.$$

Moreover, if ℓ is odd, unramified and has large image,

$$\widehat{F}_\ell = \begin{cases} \dfrac{\ell^3(\ell^2+\ell+1)}{(\ell+1)(\ell^4-1)} & \text{if } \ell \text{ is inert} \\ \dfrac{\ell^2(\ell^3+\ell^2-\ell-2)}{(\ell^2-1)^2(\ell+1)} & \text{if } \ell \text{ is split.} \end{cases}$$

Proof. First we show that $\widehat{F}_\ell$ is finite if ℓ is a prime with large image by deducing an upper bound on $\#\mathcal{A}^t_{\ell^k}$ and a lower bound on $\#\mathcal{A}_{\ell^k}$.

Let D be the positive square-free integer such that $K_f = \mathbb{Q}(\sqrt{D})$. Then $\mathcal{O}_f = \mathbb{Z}[X]/(X^2-D)$ and

$$\mathcal{O}_{\ell^k} \cong (\mathbb{Z}/\ell^k\mathbb{Z}[X])/(X^2-D).$$

In particular, we can embed $\mathcal{A}^t_{\ell^k}$ into

$$M^t_{\ell^k} :=$$

$$\left\{\sigma \in M_{2\times 2}\big((\mathbb{Z}/\ell^k\mathbb{Z}[X])/(X^2-D)\big) \mid \operatorname{tr}\sigma \in \mathbb{Z}/\ell^k\mathbb{Z} \text{ and } \det\sigma \in \mathbb{Z}/\ell^k\mathbb{Z}\right\}.$$

We deduce an upper bound on the size of the latter set. Let a_1, a_2, ... and d_2 be elements of $\mathbb{Z}/\ell^k\mathbb{Z}$ and $\sigma = \begin{pmatrix} a_1+Xa_2 & b_1+Xb_2 \\ c_1+Xc_2 & d_1+Xd_2 \end{pmatrix}$, then

$$\operatorname{tr}\sigma \in \mathbb{Z}/\ell^k\mathbb{Z} \Leftrightarrow a_2+d_2 = 0 \text{ and}$$

$$\det\sigma \in \mathbb{Z}/\ell^k\mathbb{Z} \Leftrightarrow a_1d_2+a_2d_1-b_1c_2-b_2c_1 = 0.$$

In particular, there is a bijection of sets between $M_{\ell^k}^t$ and the 7-tuples $(a_1, a_2, ..., d_1)$ satisfying

$$a_1a_2 - a_2d_1 + b_1c_2 + b_2c_1 = 0. \tag{1.1}$$

Denote by ν the ℓ-adic valuation on $\mathbb{Z}/\ell^k\mathbb{Z}$. Let $t = \min\{k, \nu(a_2), \nu(b_2), \nu(c_2)\}$. If $t = k$, then (1.1) holds for any a_1, b_1, c_1 and d_1 in $\mathbb{Z}/\ell^k\mathbb{Z}$. So there are at most ℓ^{4k} matrices in $M_{\ell^k}^t$ with $a_2 = b_2 = c_2 = 0$.

Suppose that t is strictly smaller than k. Take a_2', b_2' and c_2' such that $a_2\ell^t = a_2'\ell^t$, $b_2 = b_2'\ell^t$ and $c_2 = c_2'\ell^t$. By construction at least one of a_2', b_2' or c_2' is invertible in $\mathbb{Z}/\ell^{k-t}\mathbb{Z}$. Suppose that a_2' is a unit. Then

$$(1.1) \Leftrightarrow d_1 \equiv a_2'^{-1}\big(a_1a_2' + b_1c_2' + b_2'c_1\big) \mod \ell^{k-t}.$$

Hence, for every $0 \leq t < k$ there are at most $\ell^{6k-2t-1}(\ell-1)$ matrices in $M_{\ell^k}^t$ with $\nu(a_2) = t$, $\nu(b_2) \geq t$ and $\nu(c_2) \geq t$. If b_2' or c_2' is invertible we obtain at most $\ell^{6k-2t-1}(\ell-1)$ matrices in $M_{\ell^k}^t$ by a similar argument. So for every $t < k$ there are at most $3\ell^{6k-2t-1}(\ell-1)$ matrices in $M_{\ell^k}^t$ with $t = \min\{\nu(a_2), \nu(b_2), \nu(c_2)\}$. Summing over all t yields

$$\begin{aligned}
\#\mathcal{A}_{\ell^k}^t \leq \#M_{\ell^k}^t &\leq \ell^{4k} + 3\sum_{t=0}^{k-1} \ell^{6k-2t-1}(\ell-1) \\
&= \ell^{4k} + 3(\ell-1)\ell^{4k-1}\big(\ell^{2k} + \ell^{2k-2} + \cdots + \ell^2\big) \\
&= \ell^{4k}\left(1 + 3(\ell-1)\ell\frac{(\ell^{2k}-1)}{(\ell^2-1)}\right) \\
&\leq 3\ell^{6k}.
\end{aligned}$$

Next we deduce a lower bound on $\#\mathcal{A}_{\ell^k}$. Let u and v be units in $\mathbb{Z}/\ell^k\mathbb{Z}$, b and c elements of $(\mathbb{Z}/\ell^k\mathbb{Z}[X])/(X^2 - D)$ and $m \in \ell\mathbb{Z}/\ell^k\mathbb{Z}$. Then $a = (v + mX)$ is a unit in $(\mathbb{Z}/\ell^k\mathbb{Z}[X])/(X^2 - D)$. Indeed, the inverse is given by $(v^2 - m^2D)^{-1}(v - mX)$. If $d = (u + bc)a^{-1}$ the matrix $\sigma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has determinant u so belongs to $\mathcal{A}_{\ell^k}$. In particular, there are at least $\ell^{7k-3}(\ell-1)^2$ elements in $\mathcal{A}_{\ell^k}$. Using the upper bound on $\#\mathcal{A}_{\ell^k}^t$ and the lower bound on $\#\mathcal{A}_{\ell^k}$ we obtain

$$\widehat{F}_\ell = \lim_{k\to\infty} \ell^k \frac{\#\mathcal{A}_{\ell^k}^t}{\#A_{\ell^k}} \leq \lim_{k\to\infty} \ell^k \frac{3\ell^{6k+1}}{\ell^{7k-3}(\ell^2-1)} \leq 4\ell^2.$$

If ℓ is an exceptional prime, then $\widehat{\mathcal{G}}_\ell$ is an open subgroup of $\widehat{\mathcal{A}}_\ell$ by Theorem 1.4.2. So that

$$\lim_{k\to\infty} \frac{\#\mathcal{A}_{\ell^k}}{\#\mathcal{G}_{\ell^k}} = \#\left(\widehat{\mathcal{A}}_\ell/\widehat{\mathcal{G}}_\ell\right) < \infty.$$

Moreover, $\mathcal{G}^t_{\ell^k} \subset \mathcal{A}^t_{\ell^k}$ so

$$\begin{aligned}\widehat{F}_\ell = \lim_{k\to\infty} \ell^k \frac{\#\mathcal{G}^t_{\ell^k}}{\#\mathcal{G}_{\ell^k}} &\leq \lim_{k\to\infty} \ell^k \frac{\#\mathcal{A}^t_{\ell^k}}{\#\mathcal{G}_{\ell^k}} \\ &= \lim_{k\to\infty} \ell^k \frac{\#\mathcal{A}^t_{\ell^k}}{\#\mathcal{A}_{\ell^k}} \cdot \lim_{k\to\infty} \frac{\#\mathcal{A}_{\ell^k}}{\#\mathcal{G}_{\ell^k}} \\ &< \infty.\end{aligned}$$

Finally, from Propositions 1.4.5 and 1.4.7 we obtain

$$\#\mathcal{A}_{\ell^k} = \begin{cases} \ell^{7k-5}(\ell^4-1)(\ell-1) & \text{if } \ell \text{ is inert} \\ \ell^{7k-5}(\ell^2-1)^2(\ell-1) & \text{if } \ell \text{ is split.} \end{cases}$$

Moreover, from Propositions 1.4.6 and 1.4.8

$$\#\mathcal{A}^t_{\ell^k} = \begin{cases} \frac{\ell-1}{\ell+1}\ell^{6k-2}\left(\ell^2+\ell+1-\ell^{-2k}\right) & \text{if } \ell \text{ is inert} \\ \frac{\ell-1}{\ell+1}\ell^{6k-4}\left(\ell^4+\ell^3-\ell^2-2\ell-\ell^{-2k+2}\right) & \text{if } \ell \text{ is split.} \end{cases}$$

So that

$$\lim_{k\to\infty} \ell^k \frac{\#\mathcal{A}^t_{\ell^k}}{\#\mathcal{A}_{\ell^k}} = \begin{cases} \dfrac{\ell^3(\ell^2+\ell+1)}{(\ell+1)(\ell^4-1)} & \text{if } \ell \text{ is inert} \\ \dfrac{\ell^2(\ell^3+\ell^2-\ell-2)}{(\ell^2-1)^2(\ell+1)} & \text{if } \ell \text{ is split.} \end{cases}$$

□

Corollary 1.4.10. *Let f be as above. Then the limit of F_m by divisibility exists, i.e.*

$$\widehat{F} := \lim_{m\to|\infty} F_m < \infty.$$

Proof. First note that for any sequence a_n

$$\begin{aligned}\sum_n a_n < \infty \Rightarrow \sum_n \log(a_n+1) &< \infty \\ \Leftrightarrow \prod_n (a_n+1) &< \infty.\end{aligned}$$

Moreover, if ℓ is an odd unramified prime with large image, Lemma 1.4.9 yields

$$\widehat{F}_\ell = \begin{cases} 1 + \dfrac{\ell^3 + \ell + 1}{(\ell+1)(\ell^4-1)} & \text{if } \ell \text{ is inert} \\ \\ 1 + \dfrac{\ell^3 - \ell - 1}{(\ell^2-1)^2(\ell+1)} & \text{if } \ell \text{ is split.} \end{cases}$$

In particular, the product $\prod \widehat{F}_\ell$ taken over all odd unramified primes with large image is finite. Since almost all primes are odd, are unramified and have large image the product taken over all primes is finite by Lemma 1.4.9. Finally, Serre's adelic open image theorem [21, Theorem 3.3.1] states that $\widehat{\mathcal{G}}$ is an open subgroup of $\prod_\ell \widehat{\mathcal{G}}_\ell$, hence

$$\begin{aligned} \lim_{m\to|\infty} F_m &= \lim_{m\to|\infty} m \frac{\#\mathcal{G}_m^t}{\#\mathcal{G}_m} \\ &\leq \lim_{m\to|\infty} \frac{\prod_{\ell^k\|m} \ell^k \#\mathcal{G}_{\ell^k}^t}{\#\mathcal{G}_m} \\ &= \lim_{m\to|\infty} \frac{\prod_{\ell^k\|m} \ell^k \#\mathcal{G}_{\ell^k}^t}{\prod_{\ell^k\|m} \#\mathcal{G}_{\ell^k}} \cdot \frac{\prod_{\ell^k\|m} \#\mathcal{G}_{\ell^k}}{\#\mathcal{G}_m} \\ &= \lim_{m\to|\infty} \prod_{\ell^k\|m} \ell^k \frac{\#\mathcal{G}_{\ell^k}^t}{\#\mathcal{G}_{\ell^k}} \cdot \lim_{m\to|\infty} \frac{\#\prod_{\ell^k\|m} \mathcal{G}_{\ell^k}}{\#\mathcal{G}_m} \\ &= \prod_\ell \widehat{F}_\ell \cdot \#\left(\prod_\ell \widehat{\mathcal{G}}_\ell / \widehat{\mathcal{G}}\right) \\ &< \infty. \end{aligned}$$

□

1.5 The Main Result

In this section, we state and prove our main result.

Lemma 1.5.1. *Let f be a weight 2 normalised cuspidal Hecke eigenform of level $\Gamma_1(N)$, with quadratic coefficient field without inner twist. Let m be a positive integer such that Assumptions 1.3.4 and 1.2.2 hold. Then*

$$\#\{p < x \text{ prime} \mid a_p \in \mathbb{Q}\} \sim \frac{F_m}{\alpha_m} \frac{16\sqrt{D}}{3\pi^2} \frac{\sqrt{x}}{\log x},$$

with $0 < \alpha_m < \infty$ as in Assumption 1.2.2.

Proof. Denote $N_f(x) = \#\{p < x \text{ prime } \mid a_p(f) \in \mathbb{Q}\} = P(x) \cdot \pi(x)$ and let $\varepsilon > 0$. By Assumption 1.2.2 there exists $x_1 > 0$ such that for all $x > x_1$

$$\left| \frac{P^m(x) P_m(x)}{\alpha_m P(x)} - 1 \right| < \varepsilon/6.$$

Let x_2 be such that for all $x > x_2$ we have

$$\left| \frac{F_m}{m P_m(x)} - 1 \right| < \frac{\varepsilon}{6}.$$

Such an x_2 exists by Lemma 1.4.1. By Corollary 1.3.6 under Assumption 1.3.4 there exists an x_3 such that for all $x > x_3$

$$\left| \frac{16m\sqrt{D}}{3\pi^2 \sqrt{x} P^m(x)} - 1 \right| < \frac{\varepsilon}{6}.$$

Finally, let x_4 be such that for all $x > x_4$

$$\left| \frac{x}{\pi(x) \log(x)} - 1 \right| < \frac{\varepsilon}{6}.$$

Then for any $x > \max\{x_1, x_2, x_3, x_4\}$ we obtain

$$\begin{aligned}
&\left| \frac{1}{\alpha_m} \frac{16\sqrt{D} F_m \sqrt{x}}{3\pi^2 \log x N_f(x)} - 1 \right| \\
=&\left| \frac{P^m(x) P_m(x)}{\alpha_m P(x)} \cdot \frac{16\sqrt{D} m}{3\pi^2 \sqrt{x} P^m(x)} \cdot \frac{F_m}{m P_m(x)} \cdot \frac{x}{\pi(x) \log x} - 1 \right| \\
<&\left| \left(1 + \frac{\varepsilon}{6}\right)^4 - 1 \right| \\
<&\varepsilon.
\end{aligned}$$

□

Corollary 1.5.2. *Let f be as above. Suppose that there exists a positive integer m_0 such that Assumptions 1.3.4 and 1.2.2 hold for m_0.*

1. *Then Assumption 1.3.4 implies 1.2.2 for any positive integer m.*
2. *If Assumption 1.3.4 is true for all positive integers $m \in m_0\mathbb{Z}$, then*

$$0 < \lim_{m \to |\infty} \lim_{x \to \infty} \frac{P^m(x) \cdot P_m(x)}{P(x)} =: \alpha < \infty.$$

Moreover,

$$\#\{p < x \text{ prime } \mid a_p(f) \in \mathbb{Q}\} \sim \frac{\widehat{F}}{\alpha} \frac{16\sqrt{D}}{3\pi^2} \frac{\sqrt{x}}{\log x}.$$

Proof. If such an m_0 exists, then by Lemma 1.5.1 there exists a positive non-zero constant C_{m_0} such that $P(x) \sim C_{m_0}\sqrt{x}/\log x$.

1. Let m be a positive integer satisfying Assumption 1.3.4. By Corollary 1.3.6 and Lemma 1.4.1 $P^m(x) \cdot P_m(x) \sim C'\sqrt{x}/\log x$ with $0 < C' = \frac{16\sqrt{D}F_m}{3\pi^2} < \infty$. Hence,

$$\begin{aligned}\lim_{x\to\infty} \frac{P^m(x)\cdot P_m(x)}{P(x)} &= \lim_{x\to\infty} \frac{C'\sqrt{x}/\log x}{C_{m_0}\sqrt{x}/\log x} \\ &= \frac{C'}{C_{m_0}}.\end{aligned}$$

2. By the first point we can apply Lemma 1.5.1 to any pair of positive integers m and m' in $m_0\mathbb{Z}$ and obtain that

$$\frac{\alpha_m}{F_m} = \frac{\alpha_{m'}}{F_{m'}}.$$

So the following definition of α does not depend on the choice of m.

$$0 < \alpha := \frac{\alpha_m \widehat{F}}{F_m} < \infty.$$

In particular,

$$\begin{aligned}\lim_{m\to|\infty}\lim_{x\to\infty} \frac{P^m(x)\cdot P_m(x)}{P(x)} &= \lim_{m\to|\infty} \alpha_m \\ &= \lim_{m\to|\infty} \frac{\alpha F_m}{\widehat{F}} \\ &= \alpha.\end{aligned}$$

By Lemma 1.5.1 we obtain for every positive integer m divisible by m_0 that

$$1 = \lim_{x\to\infty} \frac{F_m 16\sqrt{D}\sqrt{x}}{\alpha_m 3\pi^2 \log x N_f(x)}.$$

Taking the limit by divisibility of m yields

$$1 = \lim_{m\to|\infty}\lim_{x\to\infty} \frac{F_m 16\sqrt{D}\sqrt{x}}{\alpha_m 3\pi^2 \log x N_f(x)}.$$

Since F_m and α_m do not depend on x we obtain

$$1 = \lim_{m\to|\infty} \frac{F_m}{\alpha_m} \lim_{x\to\infty} \frac{16\sqrt{D}\sqrt{x}}{3\pi^2 \log x N_f(x)}$$

$$= \lim_{x\to\infty} \frac{\widehat{F}16\sqrt{D}\sqrt{x}}{\alpha 3\pi^2 \log x N_f(x)}. \qquad \square$$

Theorem 1.5.3. *Let f be a weight 2 normalised cuspidal Hecke eigenform of level $\Gamma_1(N)$ with quadratic coefficient field $\mathbb{Q}(\sqrt{D})$ and without inner twist. Suppose that there exists a positive integer m_0 such that Assumptions 1.3.4 and 1.2.1 hold for f and all positive integers in $m_0\mathbb{Z}$. Then*

$$\#\{p < x \text{ prime } \mid a_p(f) \in \mathbb{Q}\} \sim \frac{16\sqrt{D}\widehat{F}}{3\pi^2} \frac{\sqrt{x}}{\log x}.$$

Proof. From Corollary 1.5.2 we obtain

$$\#\{p < x \text{ prime } \mid a_p(f) \in \mathbb{Q}\} \sim \frac{\widehat{F}}{\alpha} \frac{16\sqrt{D}}{3\pi^2} \frac{\sqrt{x}}{\log x}.$$

The claim of Assumption 1.2.1 is precisely that $\alpha = 1$. Hence, the theorem follows. $\square$

1.6 Numerical Results

In this section, we provide numerical results that support the assumptions made and the results deduced from these assumptions. Moreover, we describe the method used to obtain these results.

All computations are done using the following six new Hecke eigenforms $f_N \in S_2(\Gamma_0(N))$:

$$f_{29} = q + (-1+\sqrt{2})q^2 + (1-\sqrt{2})q^3 + (1-2\sqrt{2})q^4 - q^5 + \cdots$$

$$f_{43} = q + \sqrt{2}q^2 - \sqrt{2}q^3 + (2-\sqrt{2})q^5 + \cdots$$

$$f_{55} = q + (1+\sqrt{2})q^2 - 2\sqrt{2}q^3 + (1+2\sqrt{2})q^4 - q^5 \cdots$$

$$f_{23} = q + \frac{-1+\sqrt{5}}{2}q^2 - \sqrt{5}q^3 - \frac{1+\sqrt{5}}{2}q^4 + (-1+\sqrt{5})q^5 + \cdots$$

$$f_{87} = q + \frac{1+\sqrt{5}}{2}q^2 + q^3 + \frac{-1+\sqrt{5}}{2}q^4 + (1-\sqrt{5})q^5 \cdots$$

$$f_{167} = q + \frac{-1+\sqrt{5}}{2}q^2 - \frac{1+\sqrt{5}}{2}q^3 - \frac{1+\sqrt{5}}{2}q^4 - q^5 + \cdots .$$

Note that the level for each of the eigenforms is square-free and the nebentypus is trivial so by Lemma 1.1.11 none of these eigenforms have inner twists. Moreover, the coefficient field of f_{29}, f_{43} and f_{55} is $\mathbb{Q}(\sqrt{2})$ and the coefficient field of f_{23}, f_{87} and f_{167} is $\mathbb{Q}(\sqrt{5})$. In this section, we will denote $\mathcal{A}_{f_N}$, c_{f_N},... by $\mathcal{A}_N$, c_N, ..., respectively.

As described in Section 1.3 the Galois orbit of the p-th coefficient of a eigenform f_N can be computed from the L_p-polynomial of the abelian variety $\mathcal{A}_N$ associated to f_N. For each eigenform f_N we give an equation for a hyperelliptic curve C_N such that the Jacobian $J(C_N)$ is isomorphic to the abelian variety $\mathcal{A}_N$. Obtaining such an equation is a non-trivial problem. For levels 29, 43 and 55 the equations are found in [2, page 42] and the remaining three equations are found in [39, page 137]. The equations are:

$$C_{29} : y^2 = x^6 - 2x^5 + 7x^4 - 6x^3 + 13x^2 - 4x + 8,$$

$$C_{43} : y^2 = -3x^6 - 2x^5 + 7x^4 - 4x^3 - 13x^2 + 10x - 7,$$

$$C_{55} : y^2 = -3x^6 + 4x^5 + 16x^4 - 2x^3 - 4x^2 + 4x - 3,$$

$$C_{23} : y^2 = x^6 + 2x^5 - 23x^4 + 50x^3 - 58x^2 + 32x - 11,$$

$$C_{87} : y^2 = -x^6 + 2x^4 + 6x^3 + 11x^2 + 6x + 3,$$

$$C_{167} : y^2 = -x^6 + 2x^5 + 3x^4 - 14x^3 + 22x^2 - 16x + 7.$$

Next we use Andrew Sutherlands smalljac algorithm described in [16] to compute the coefficients of the L_p-polynomial of each hyperelliptic curve C_N. This algorithm is implemented in C and is available at Sutherland's web page. With this method we are able to compute the Galois orbit of the coefficients of one eigenform for all primes up to 10^8 in less than 50 hours. All computations are done on a Dell Latitude E6540 laptop with Intel i7-4610M processor (3.0 GHz, 4MB cache, Dual Core). The processing of the data and the creation of the graphs was done using Sage Mathematics Software [35] on the same machine. The running time of this is negligible compared to the smalljac algorithm.

Murty's Conjecture

First we check Conjecture 0.0.1. For each eigenform we plot the number of primes $p < x$ such that the p-th coefficient is a rational integer for 50 values of x up to 10^8.

According to this conjecture there exists a constant c_N such that

$$\#\{p < x \text{ prime} \mid a_p(f_N) \in \mathbb{Q}\} \sim c_N \frac{\sqrt{x}}{\log x}.$$

To check the conjecture we approximate c_N using least squares fitting. Denote this estimate by $\widetilde{c}_N$. Figure 1.3 provides numerical evidence for the behaviour of $N(x)$ and column 2 of Table 1.1 list the values of $\widetilde{c}_N$ found by least squares fitting.

The place at Infinity

Corollary 1.3.6 states that under Assumption 1.3.4

$$\#\left\{p < x \text{ prime} \mid Z_p \in]-m\sqrt{D}/2, m\sqrt{D}/2[\right\} \sim \frac{16\sqrt{D}m}{3\pi^2}\frac{\pi(x)}{\sqrt{x}}.$$

For m equal to 100, 500 and 1000 Figure 1.4 indicates that $\frac{16m\sqrt{D}}{3\pi^2}\frac{\pi(x)}{\sqrt{x}}$ is in fact a good approximation for $\#\{p < x \text{ prime} \mid Z_p \in]-m\sqrt{D}/2, m\sqrt{D}/2[\}$. Although this does not prove Assumption 1.3.4 , it does confirm that $P_m(x)$ depends on the coefficient field of the eigenform.

Finite Places

In [3] Nicolas Billerey and Luis Dieulefait provide explicit bounds on the primes ℓ that do not have large image for a given eigenform $f \in S_2(\Gamma_0(N))$ with square-free level N. In fact they provide a more general result. We only state the lemma for square-free level.

Lemma 1.6.1. *Let f be a eigenform in $S_2(\Gamma_0(N))$. Assume that $N = p_1p_2\cdots p_t$, where $p_1, ..., p_t$ are $t \geq 1$ distinct primes and ℓ is exceptional. Then ℓ divides $15N$ or $p_i^2 - 1$ for some $1 \leq i \leq t$.*

Proof. This is the statement of [3, Theorem 2.6] in the weight 2 case. □

The eigenforms in our computations have weight 2 and square-free level so we can apply the lemma and obtain a list of primes that are possibly exceptional for each eigenform (Table 1.1).

If ℓ is an odd unramified prime with large image Lemmas 1.4.1 and 1.4.9 yield

$$\#\{p < x \text{ prime} \mid Z_p \equiv 0 \mod \ell^k\} \sim \pi(x) \cdot \begin{cases} \dfrac{\ell^2+\ell+1-\ell^{-2k}}{(\ell+1)(\ell^4-1)\ell^{k-3}} & \text{if } \ell \text{ is inert} \\ \dfrac{\ell^4+\ell^3-\ell^2-2\ell-\ell^{-2k+2}}{(\ell^2-1)^2\ell^{k-1}} & \text{if } \ell \text{ is split.} \end{cases}$$

For each prime that is possibly exceptional and each eigenform we can confirm that the prime is exceptional by comparing $\#\{p < x \text{ prime} \mid Z_p \equiv 0 \mod \ell^k\}$ with the expected value for a prime with large image for x up to 10^8 (Fig. 1.5). For $\ell = 2$ we do not have a theoretic result for large image. Therefore, none is plotted. The same holds for $\ell = 5$ and eigenforms f_{23}, f_{87} and f_{167} since 5 ramifies in $\mathbb{Q}(\sqrt{5})$.

Some primes are inert in $\mathbb{Q}(\sqrt{5})$ and split in $\mathbb{Q}(\sqrt{2})$ or vice versa. So a priori we have two possibilities for the behaviour of $\#\{p < x \text{ prime} \mid Z_p \equiv 0 \mod \ell^k\}$ for a prime ℓ with large image. However, the first prime for which this occurs is 7. Indeed, 7 splits in $\mathbb{Q}(\sqrt{2})$ and is inert in $\mathbb{Q}(\sqrt{5})$. For $\ell = 7$ one can hardly distinguish the inert and split case visually.

Figure 1.5 indicates which odd unramified primes are exceptional for a given eigenform. If the plot of $\#\{p < x \mid Z_p \equiv 0 \mod \ell^k\}$ differs from that of the large image case, we can expect the image to be exceptional. Moreover, for any prime ℓ we can expect that the image of the ℓ-adic representation attached to different eigenforms are distinct by comparing the corresponding plots. Note that the converse does not hold. Indeed, the fact that two eigenforms exhibit the same behaviour with respect to $\#\{p < x \text{ prime} \mid Z_p \equiv 0 \mod \ell^k\}$ is no reason to believe that their ℓ-adic representations are the same.

For example if $\ell^k = 2$ (Fig. 1.5a), then all eigenforms except f_{167} exhibit the same behaviour. But for $\ell^k = 8$ (Fig. 1.5b) we clearly distinguish five different representations. Note that we do not observe this behaviour for any other prime. From $\ell^k = 3$ (Fig. 1.5c) we can suspect that 3 is an exceptional prime for the 3-adic representation attached to f_{43} and f_{55}. The primes that are marked in bold in the last column of Table 1.1 are the primes for which Figure 1.5 hints that the prime is exceptional.

Main Result

Next we test Theorem 1.5.3 by comparing the behaviour of $\#\{p < x \text{ prime} \mid a_p \in \mathbb{Q}\}$ with $c_N\sqrt{x}/\log x$ where c_N is the constant predicted by Theorem 1.5.3. Recall that

according to our main theorem under Assumptions 1.3.4 and 1.2.1 we have

$$c_N = \frac{16\sqrt{D}}{3\pi^2}\widehat{F}.$$

Since $\widehat{F}$ is a limit by divisibility we approximate it numerically. In order to do so we use the following assumption.

Assumption 1.6.2. *Let m and m' be co-prime integers. Then*

$$P_m(x) \cdot P_{m'}(x) \sim P_{m\cdot m'}(x).$$

If $\widehat{\rho}$ is an independent system of representations in the sense of [31, Section 3], the assumption holds. However, $\widehat{\rho}$ is in general not an independent system and the assumption is a much weaker claim. Moreover, this assumption is only needed to get a numerical result and our main theorem holds even if this assumption is false. All computations support the assumption (see Figure 1.6).

Under Assumption 1.6.2 we can compute an approximation of $\widehat{F}$ by taking the product over all primes

$$\widehat{F} = \prod_{\ell} \widehat{F}_\ell.$$

For odd unramified primes with large image the factor $\widehat{F}_\ell$ is given by Lemma 1.4.9. Let $\{\ell_1, ..., \ell_t\}$ be the set of primes that are even, ramified or possibly exceptional. For every prime ℓ_i we apply Lemma 1.4.1 for $\ell_i^{k_i}$ with k_i the largest integer such that $\ell_i^{k_i}$ is less than $\sqrt{10^8}/20$, i.e.

$$k_i = \lfloor \log_{\ell_i}(\sqrt{10^8}/20) \rfloor.$$

So we use the following approximation for c_N

$$\widehat{c}_N = \frac{16\sqrt{D}}{3\pi^2} \prod_{i=1}^{t} \ell^{k_i} P_{\ell_i^{k_i}}(10^8) \prod_{\substack{\ell \text{ unramified} \\ \text{with large image}}} \widehat{F}_\ell.$$

For every eigenform f_N we plot $\widehat{c}_N\sqrt{c}/\log x$, $\widehat{c}_N \pi(x)/\sqrt{x}$ and $\#\{p < x \text{ prime} \mid a_p \in \mathbb{Q}\}$ (see figure 1.7).

Comparing the values of $\widehat{c}_N$ to the previously found $\widetilde{c}_N$ by least square fitting yields $1.025 < \widetilde{c}_N/\widehat{c}_N < 1.149$ (Table 1.1). This error is to be expected for this small a bound on the primes. For example in the proof of Corollary 1.3.6 we use $\frac{\sqrt{x}}{\log x}$ to approximate $\sum_{p=2}^{x} \frac{1}{2\sqrt{p}}$. For $x = 10^8$ this estimate yields a similar error

$$\frac{\log 10^8}{\sqrt{10^8}} \cdot \sum_{p=2}^{10^8} \frac{1}{2\sqrt{p}} = 1.146\cdots.$$

Table 1.1: For each eigenform f_N the table contains the level N, the constant $\widetilde{c}_N$ obtained by least square fitting, the constant $\widehat{c}_N$ according to Theorem 1.5.3, the error $\widetilde{c}_N/\widehat{c}_N$ and the possibly exceptional primes according to Corollary 1.6.1, respectively. The expected exceptional primes are marked in bold.

N	$\widetilde{c}_N$	$\widehat{c}_N$	$\widetilde{c}_N/\widehat{c}_N$	Pos. exc. primes
29	4.990	4.517	1.104	2, 3, 5, **7**, 29
43	4.588	4.204	1.109	2, **3**, 5, **7**, 11, 43
55	10.515	9.958	1.056	2, **3**, 5,11
23	5.490	4.982	1.102	2, 3, 5, **11**, 23
87	4.972	4.413	1.127	2, 3, **5**, 7, 29
167	2.066	1.833	1.127	2, 3, 5, 7, 83, 167

Final Assumption

The final assumptions we check are Assumptions 1.2.1 and 1.2.2. Recall that Assumption 1.2.1 states that for every eigenform f_N and every $\varepsilon > 0$ there exists an m_0 such that for all m with $m_0|m$ there exists an x_0 such that for all $x > x_0$

$$\left| \frac{P^m(x) \cdot P_m(x)}{P(x)} - 1 \right| < \varepsilon.$$

Assumption 1.2.2 is a much weaker claim and states that the limit

$$\lim_{x \to \infty} \frac{P^m(x) \cdot P_m(x)}{P(x)}$$

exists for a given positive m. For all eigenforms we can find various m such that

$$\left| \frac{P^m(x) \cdot P_m(x)}{P(x)} - 1 \right| < 0.2$$

for all x larger than $5 \cdot 10^7$. For every eigenform we choose different values for m and plot $\frac{P^m(x) \cdot P_m(x)}{P(x)}$ and the constant functions 1 and $\frac{P^{m_N}(10^8) \cdot P_{m_N}(10^8)}{P(10^8)}$ (Fig. 1.8). Where m_N is the largest positive integer used for every eigenform f_N. The values of m are chosen so that they increase by divisibility and so that the confirmed exceptional primes divide m.

Additionally figure 1.8 provides numerical evidence for Assumption 1.2.2 which implies the existence of the double limit of $P_m(x) \cdot P^m(x)/P(x)$ by Corollary 1.5.2. However, one could argue that the figure suggests that the double limit does not converge to 1. Let us denote for every N

$$\alpha_N = \lim_{m \to |\infty} \lim_{x \to \infty} \frac{P^m(x) \cdot P_m(x)}{P(x)}$$

as in Corollary 1.5.2. Then the corollary states that

$$\#\{p < x \text{ prime } \mid a_p(f_N) \in \mathbb{Q}\} \sim \frac{1}{\alpha_N} \frac{16\sqrt{D}\widehat{F}}{3\pi^2} \frac{\sqrt{x}}{\log x}.$$

We have a convincing estimate $\widehat{c}_N$ for c_N. Moreover, the best approximation of α_N available is

$$\alpha_{m_N} = P^{m_N}(10^8) \cdot P_{m_N}(10^8)/P(10^8).$$

So we can check this last statement by plotting both functions (Fig. 1.9). In this figure $1/\alpha_{m_N}\widehat{c}_N \frac{\pi(x)}{\sqrt{x}}$ clearly yields an overestimate when we in fact expect a slight underestimate. This is an indication that, although the convergence might be slow, the double limit equals 1.

1.A List of Figures

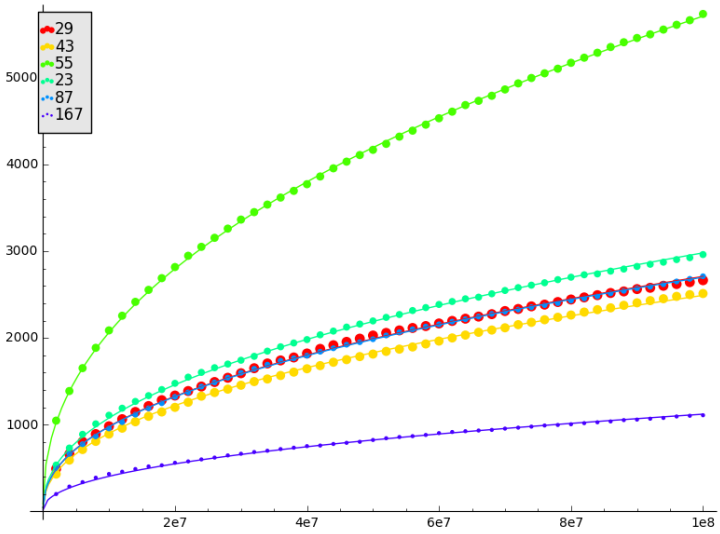
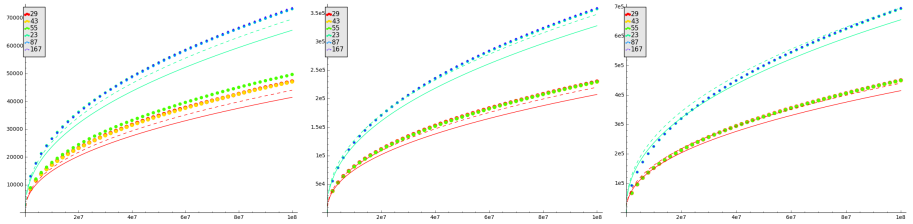
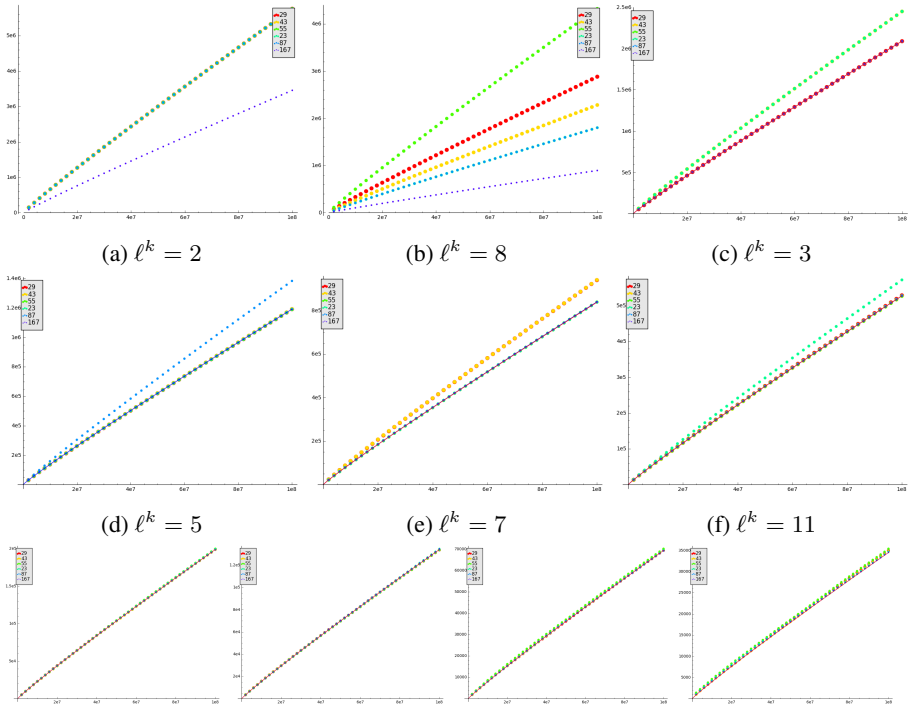


Figure 1.3: Plot of $\#\{p < x \text{ prime } \mid a_p(f_N) \in \mathbb{Q}\}$ (dots) and $\widetilde{c}_N\sqrt{x}/\log x$ (line) using least squares fitting to compute $\widetilde{c}_N$ for x up to 10^8.



(a) $m = 100$ (b) $m = 500$ (c) $m = 1000$

Figure 1.4: Plots of $\#\{p < x \text{ prime} \mid Z_p \in]-m\sqrt{D}/2, m\sqrt{D}/2[\}$ (dots), $\frac{16\sqrt{D}m}{3\pi^2}\frac{\pi(x)}{\sqrt{x}}$ (dashed) and $\frac{16\sqrt{D}m}{3\pi^2}\frac{\sqrt{x}}{\log x}$ (full line) for $\sqrt{D} = \sqrt{5}$ (cyan) and $\sqrt{D} = \sqrt{2}$ (red) for each eigenform f_N and $m = 100, 500, 1000$.

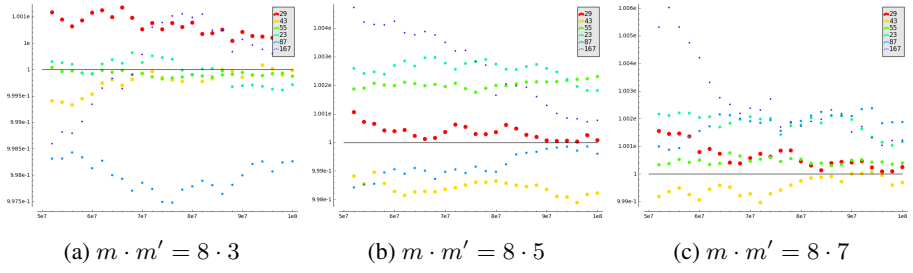


(a) $\ell^k = 2$ (b) $\ell^k = 8$ (c) $\ell^k = 3$

(d) $\ell^k = 5$ (e) $\ell^k = 7$ (f) $\ell^k = 11$

(g) $\ell^k = 29$ (h) $\ell^k = 43$ (i) $\ell^k = 83$ (j) $\ell^k = 167$

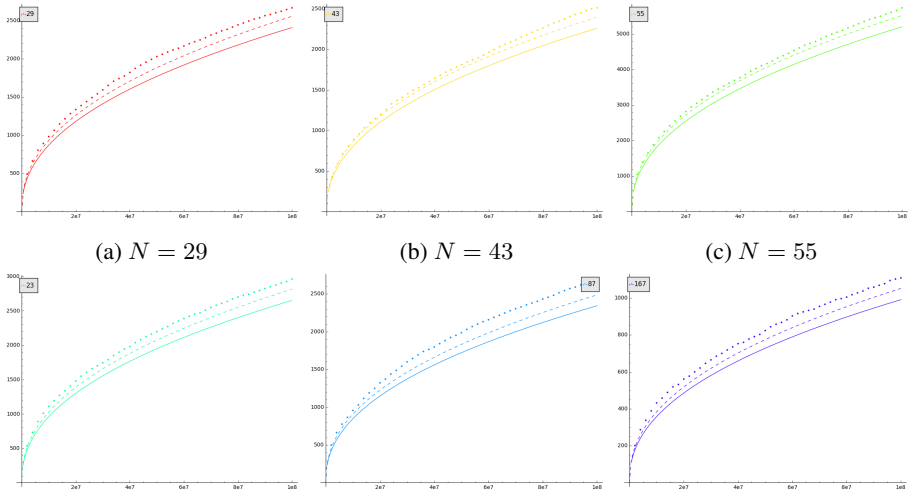
Figure 1.5: Plots of $\#\{p < x \text{ prime} \mid Z_p \equiv 0 \mod \ell^k\}$ for large image (line) and actual value (dots) for all eigenforms. If $\ell = 2$ no function is plotted for large image.



(a) $m \cdot m' = 8 \cdot 3$ (b) $m \cdot m' = 8 \cdot 5$ (c) $m \cdot m' = 8 \cdot 7$

(d) $m \cdot m' = 3 \cdot 5$ (e) $m \cdot m' = 3 \cdot 7$ (f) $m \cdot m' = 5 \cdot 7$

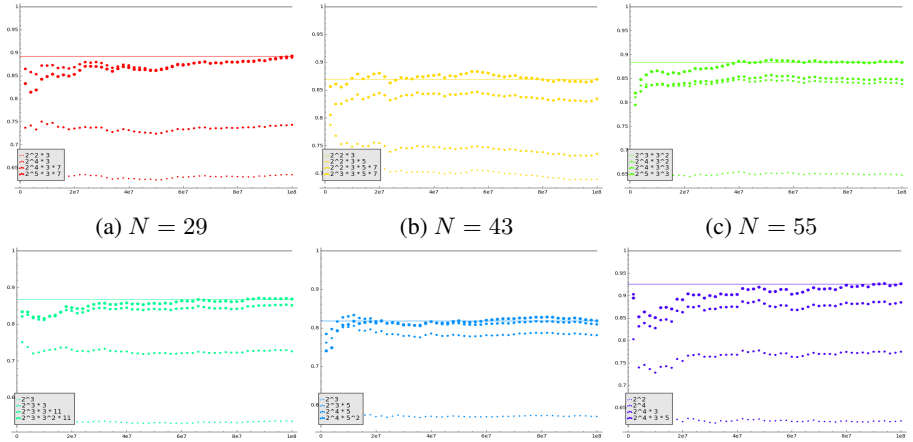
Figure 1.6: Plots of $P_m(x) \cdot P_{m'}(x)/P_{m \cdot m'}(x)$ (dots) and the constant function 1 (line)
.



(a) $N = 29$ (b) $N = 43$ (c) $N = 55$

(d) $N = 23$ (e) $N = 87$ (f) $N = 167$

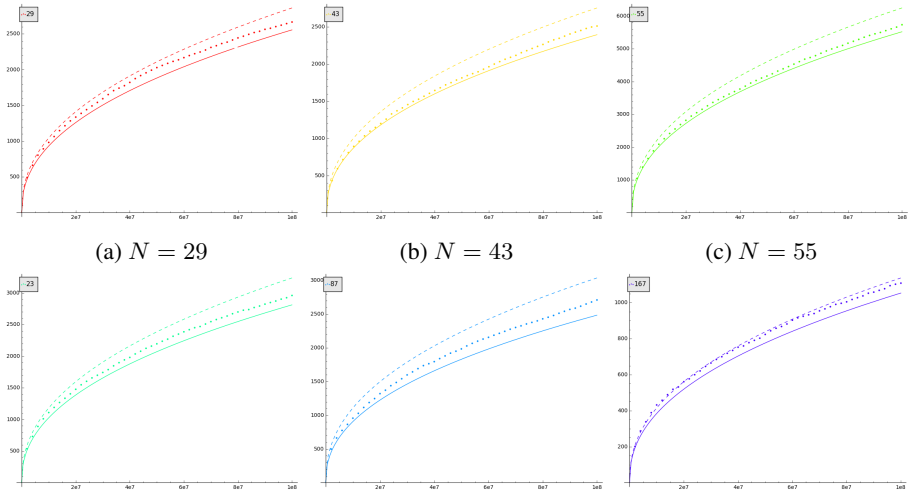
Figure 1.7: Plots of $\#\{p < x \text{ prime} \mid a_p \in \mathbb{Q}\}$ (dots), $\widehat{c}_N \frac{\sqrt{x}}{\log x}$ (full line) and $\widehat{c}_N \frac{\pi(x)}{\sqrt{x}}$ (dashed line) for all eigenforms f_N with $\widehat{c}_N$ based on Theorem 1.5.3 .



(a) $N = 29$ (b) $N = 43$ (c) $N = 55$

(d) $N = 23$ (e) $N = 87$ (f) $N = 167$

Figure 1.8: Plots of $P^m(x) \cdot P_m(x)/P(x)$ (dots), the constant function 1 (black line) and the constant functions $P^{m_0}(10^8) \cdot P_{m_0}(10^8)/P(10^8)$ (coloured line) for each eigenform f_N and various divisors m of m_0 for x up to 10^8.



(a) $N = 29$ (b) $N = 43$ (c) $N = 55$

(d) $N = 23$ (e) $N = 87$ (f) $N = 167$

Figure 1.9: Plots of $\#\{p < x \text{ prime} \mid a_p \in \mathbb{Q}\}$ (dots), $\widehat{c}_N \frac{\pi(x)}{\sqrt{x}}$ (full line) and $1/\alpha_{m_N} \widehat{c}_N \frac{\pi(x)}{\sqrt{x}}$ (dashed line) for all eigenforms f_N with $\widehat{c}_N$ based on Theorem 1.5.3 .

1.B Counting Traces

In this section, we prove Propositions 1.4.6 and 1.4.8.

Proof of Proposition 1.4.6

In this section, we give the proof of the following proposition.

Proposition 1.4.6. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#\mathcal{A}^t_{\ell^k,I} = \frac{(\ell-1)}{(\ell+1)}\ell^{6k-2}\left(\ell^2+\ell+1-\ell^{-2k}\right).$$

Before we give the proof we need a lemma. Let

$$\nu : \mathbb{Z}[\alpha] \to \mathbb{Z}$$

be the ℓ-adic valuation. By abuse of notation we will also use ν to denote the induced valuation on $\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$.

Lemma 1.B.1. *Consider for any $k \geq r \geq 1$ the following two conditions on pairs $(a,d) \in (\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha])^2$*

$$\begin{cases} a \cdot d \in \mathbb{Z}/\ell^k\mathbb{Z}^\times + \alpha\ell^r\mathbb{Z}/\ell^k\mathbb{Z} & \text{(1.2a)} \\ a + d \in \mathbb{Z}/\ell^k\mathbb{Z}. & \text{(1.2b)} \end{cases}$$

1. *Let $b \in \mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$ with $\min\{\nu(b), k\} = r$. Then there exists an element $c \in \mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$ such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{A}^t_{\ell^k,I}$ if and only if both* (1.2a) *and* (1.2b) *hold. Moreover, there exist precisely ℓ^{k+r} distinct such c.*
2. *There are*
$$\ell^{3k-r-2}(\ell-1)(r\ell-r+\ell)$$
pairs $(a,d) \in (\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha])^2$ satisfying (1.2a) *and* (1.2b).

Proof. 1. The 'only if' statement is immediate. Conversely suppose that a and d are elements of $\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$ satisfying (1.2a) and (1.2b). Let $b \in \mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$ and $k \geq r \geq 1$ with $r = \min \nu(b)k$. For every c in $\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$ denote

$$\sigma_c := \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Condition (1.2b) is equivalent with $\operatorname{tr}\sigma_c \in \mathbb{Z}/\ell^k\mathbb{Z}$. So it suffices to show that there are ℓ^{k+r} distinct c such that $\det\sigma_c \in \mathbb{Z}/\ell^k\mathbb{Z}^\times$.

Let e_1, e_2, b_1, b_2, c_1 and c_2 be elements of $\mathbb{Z}/\ell^k\mathbb{Z}$ such that

$$a \cdot d = e_1 + \ell^r e_2\alpha,$$

$$b = \ell^r(b_1 + b_2\alpha),$$

$$c = c_1 + c_2\alpha.$$

Then $\det\sigma_c \in \mathbb{Z}/\ell^k\mathbb{Z}^\times$ if and only if

$$e_1 - \ell^r(b_1c_1 + b_2c_2\alpha^2) \in \mathbb{Z}/\ell^k\mathbb{Z}^\times \text{ and}$$

$$\ell^r(e_2 - b_2c_1 - b_1c_2) = 0.$$

Note that (1.2a) implies that e_1 is invertible. So the first condition is satisfied. Moreover, $\nu(b) \geq r$ so either b_1 or b_2 is a unit. Without loss of generality suppose that b_1 is a unit. Then $\det\sigma_c \in \mathbb{Z}/\ell^k\mathbb{Z}$ if and only if

$$c_2 \in b_1^{-1}(e_2 - b_2c_1) + \ell^{k-r}\mathbb{Z}/\ell^k\mathbb{Z}.$$

In particular, there exist ℓ^{k+r} distinct such c such that $\sigma_c \in \mathcal{A}^t_{\ell^k,I}$.

2. Let a_1, a_2, d_1 and d_2 be elements of $\mathbb{Z}/\ell^k\mathbb{Z}$ such that $a = a_1 + a_2\alpha$ and $d = d_1 + d_2\alpha$. Then conditions (1.2a) and (1.2b) hold if and only if

$$\begin{cases} a_1d_1 + a_2d_2\alpha^2 \in \mathbb{Z}/\ell^k\mathbb{Z}^\times \\ a_1d_2 + a_2d_1 \in \ell^r\mathbb{Z}/\ell^k\mathbb{Z} \\ a_2 + d_2 = 0. \end{cases}$$

Using $d_2 = -a_2$ in the first expressions we obtain

$$\begin{cases} a_1d_1 - a_2^2\alpha^2 \in \mathbb{Z}/\ell^k\mathbb{Z}^\times & \text{(1.3a)} \\ a_2(a_1 - d_1) \in \ell^r\mathbb{Z}/\ell^k\mathbb{Z}. & \text{(1.3b)} \end{cases}$$

We distinguish three cases depending on the valuation of a_2.

(a) If $a_2 = 0$, then (1.3b) is satisfied and

$$\text{(1.3a)} \Leftrightarrow a_1d_1 \in \mathbb{Z}/\ell^k\mathbb{Z}^\times.$$

So there are $\ell^{2k-2}(\ell-1)^2$ such pairs (a, d).

(b) If $r \leq \nu(a_2) = s < k$, then $a_2 \in \ell^r\mathbb{Z}/\ell^k\mathbb{Z}$ so (1.3b) is satisfied and

$$(1.3a) \Leftrightarrow a_1 d_1 \in \mathbb{Z}/\ell^k\mathbb{Z}^\times.$$

So for every $r \leq s < k$ there are $\ell^{3k-3-s}(\ell-1)^3$ pairs (a,d) with $\nu(a_2) = s$ that satisfy (1.2a) and (1.2b).

(c) If $0 < \nu(a_2) = s < r$ then

$$\begin{cases} (1.3a) \Leftrightarrow a_1 d_1 \in \mathbb{Z}/\ell^k\mathbb{Z}^\times \\ (1.3b) \Leftrightarrow a_1 - d_1 \in \ell^{r-s}(\mathbb{Z}/\ell^k\mathbb{Z}^\times). \end{cases}$$

These conditions are equivalent to

$$\begin{cases} a_1 \in \mathbb{Z}/\ell^k\mathbb{Z}^\times \\ d_1 \in a_1 + \ell^{r-s}\mathbb{Z}/\ell^k\mathbb{Z}. \end{cases}$$

So for every $0 < s < r$ there are $\ell^{3k-2-r}(\ell-1)^2$ such pairs (a,d) with $\nu(a_2) = s$.

(d) Finally, suppose that a_2 is invertible. If $a_1 \in \ell\mathbb{Z}/\ell^k\mathbb{Z}$, then (1.3b) implies (1.3a). Hence, the remaining condition is

$$d_1 \in a_1 + \ell^r\mathbb{Z}/\ell^k\mathbb{Z}.$$

So there are $\ell^{3k-2-r}(\ell-1)$ pairs (a,d) with a_2 a unit and a_1 not invertible. If a_1 is an invertible element we have

$$\begin{cases} (1.3a) \Leftrightarrow d_1 \notin a_1^{-1}a_2^2\alpha^2 + \ell\mathbb{Z}/\ell^k\mathbb{Z} \\ (1.3b) \Leftrightarrow d_1 \in a_1 + \ell^r\mathbb{Z}/\ell^k\mathbb{Z}. \end{cases}$$

Note that the intersection of $a_1^{-1}a_2^2\alpha^2 + \ell\mathbb{Z}/\ell^k\mathbb{Z}$ and $a_1 + \ell^r\mathbb{Z}/\ell^k\mathbb{Z}$ is empty. Indeed, otherwise $a_1 \equiv a_1^{-1}a_2^2\alpha^2 \mod \ell$ or $(a_1a_2^{-1})^2 \equiv \alpha^2 \mod \ell$. Which contradicts the fact that α^2 is a quadratic non-residue modulo ℓ. Hence

$$(1.3b) \Leftrightarrow d_1 \in a_1 + \ell^r\mathbb{Z}\ell^k\mathbb{Z} \Rightarrow (1.3a).$$

In particular, there are $\ell^{3k-2-r}(\ell-1)^2$ pairs (a,d) with both a_1 and a_2 invertible elements.

Adding the two cases, a_1 being a unit and a_1 not being a unit, yields

$$\begin{aligned} \ell^{3k-2-r}(\ell-1)^2 + \ell^{3k-2-r}(\ell-1) &= \ell^{3k-2-r}(\ell-1)(\ell-1+1) \\ &= \ell^{3k-1-r}(\ell-1) \end{aligned}$$

distinct pairs (a,d) satisfying (1.2a) and (1.2b) with a_1 invertible.

Finally, we sum over all cases

$$\ell^{2k-2}(\ell-1)^2+\sum_{s=r}^{k-1}\ell^{3k-3-s}(\ell-1)^3+\sum_{s=1}^{r-1}\ell^{3k-2-r}(\ell-1)^2+\ell^{3k-1-r}(\ell-1)$$

$$=\ell^{2k-2}(\ell-1)\Big(\ell-1+(\ell-1)\sum_{s=r}^{k-1}\ell^{k-1-s}(\ell-1)$$

$$+\sum_{s=1}^{r-1}\ell^{k-r}(\ell-1)+\ell^{k-r+1}\Big).$$

Note that the first summation is telescopic so the total sum yields

$$\ell^{2k-2}(\ell-1)\Big(\ell-1+(\ell-1)(\ell^{k-r}-1)+(r-1)(\ell-1)\ell^{k-r}+\ell^{k-r+1}\Big)$$

$$=\ell^{2k-2}(\ell-1)\Big(r(\ell-1)\ell^{k-r}+\ell^{k-r+1}\Big)$$

$$=\ell^{3k-2-r}(\ell-1)\Big(r(\ell-1)+\ell\Big).$$ □

Proof of Proposition 1.4.6 .
Let $\sigma=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in GL_2(\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha])$. Then $\sigma\in\mathcal{A}^t_{\ell^k,I}$ if and only if

$$\begin{cases} ad-bc\in\mathbb{Z}/\ell^k\mathbb{Z}^\times & \text{(1.4a)}\\ a+d\in\mathbb{Z}/\ell^k\mathbb{Z}. & \text{(1.4b)}\end{cases}$$

We distinguish three cases depending on the valuation of b.

1. If b is a unit then

$$\begin{cases}\text{(1.4a)}\Leftrightarrow c\in adb^{-1}+\mathbb{Z}/\ell^k\mathbb{Z}^\times\\ \text{(1.4b)}\Leftrightarrow d\in -a+\mathbb{Z}/\ell^k\mathbb{Z}.\end{cases}$$

So there are

$$\ell^{2k}\cdot\ell^{2k-2}(\ell^2-1)\cdot\ell^{k-1}(\ell-1)\cdot\ell^k=\ell^{6k-3}(\ell-1)(\ell^2-1)$$

matrices $\sigma\in\mathcal{A}^t_{\ell^k,I}$ with b a unit.

2. If $b = 0$, then
$$\begin{cases} \text{(1.4a)} \Leftrightarrow ad \in \mathbb{Z}/\ell^k\mathbb{Z}^\times \\ \text{(1.4b)} \Leftrightarrow d + a \in \mathbb{Z}/\ell^k\mathbb{Z}. \end{cases}$$
By Lemma 1.B.1 with $r = k$ there are $\ell^{2k-2}(\ell-1)(k\ell-k+\ell)$ such pairs (a,d). Again by Lemma 1.B.1 there are ℓ^{2k} elements c in $\mathbb{Z}_{\ell^2}$ for every such pair (a,d) so that $\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$ is an element of $\mathcal{A}^t_{\ell^k,I}$. In particular, we obtain
$$\ell^{4k-2}(\ell-1)(k\ell-k+\ell)$$
elements of $\mathcal{A}^t_{\ell^k,I}$ with $b = 0$.

3. Let $0 < \nu(b) = r < k$. Then by part 1 of Lemma 1.B.1 there exists ℓ^{k+r} elements c for each b and each pair (1.2a) and (1.2b) such that $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathcal{A}^t_{\ell^k,I}$. By part 2 of the same lemma there exist $\ell^{3k-2-r}(\ell-1)(r\ell-r+\ell)$ such pairs (a,d). Moreover, there are $\ell^{2k-2-2r}(\ell^2-1)$ elements b in $\mathbb{Z}[\alpha]/\ell^k\mathbb{Z}[\alpha]$ with $\nu(b) = r$. So there are
$$\begin{aligned} &\ell^{3k-2-r}(\ell-1)(r\ell-r+\ell)\cdot\ell^{2k-2-2r}(\ell^2-1)\cdot\ell^{k+r} \\ &\qquad = \ell^{4(k-1)+2(k-r)}(\ell-1)(\ell^2-1)(r\ell-r+\ell) \end{aligned}$$
elements in $\mathcal{A}^t_{\ell^k,I}$ with $\nu(b) = r$ for each $0 < r < k$.

It remains to take the sum over all three cases. Note that
$$\begin{aligned} \#\mathcal{A}^t_{\ell^k,I} &= \ell^{6k-3}(\ell-1)(\ell^2-1) \\ &\quad + \sum_{r=1}^{k-1} \ell^{4(k-1)+2(k-r)}(\ell-1)(\ell^2-1)(r\ell-r+\ell) \\ &\quad + \ell^{4k-2}(\ell-1)(k\ell-k+\ell) \\ &= \ell^{4(k-1)}(\ell-1)\Big(k\ell-k+\ell+\sum_{r=0}^{k}\ell^{2(k-r)}(\ell^2-1)(r(\ell-1)+\ell)\Big). \end{aligned}$$
We split the summation in two terms
$$\begin{aligned} \#\mathcal{A}^t_{\ell^k,I} =& \ell^{4(k-1)}(\ell-1)\Big(k(\ell-1)+\ell \\ &+ (\ell-1)\sum_{r=0}^{k} r\ell^{2(k-r)}(\ell^2-1) + \sum_{r=0}^{k}\ell^{2(k-r)+1}(\ell^2-1)\Big). \end{aligned}$$

Expand the first summation and note that the second summation is telescopic

$$\begin{aligned}
\#\mathcal{A}^t_{\ell^k,I} =&\ell^{4(k-1)}(\ell-1)\Big(k(\ell-1)+\ell \\
&+(\ell-1)(\ell^{2k}+\ell^{2k-2}+\cdots+\ell^2-k)+(\ell^{2k+3}-\ell)\Big) \\
=&\ell^{4(k-1)}(\ell-1)\Big(k(\ell-1)+\ell \\
&+(\ell-1)\frac{\ell^{2(k+1)}-1}{\ell^2-1}-(\ell-1)(1+k)+\ell^{2k+3}-\ell\Big) \\
=&\ell^{4(k-1)}(\ell-1)\Big(\frac{\ell^{2(k+1)}-1}{\ell+1}-(\ell-1)+\ell^{2k+3}\Big) \\
=&\ell^{4(k-1)}\frac{(\ell-1)}{(\ell+1)}\Big(\ell^{2(k+1)}-1-(\ell+1)(\ell-1)+\ell^{2k+4}+\ell^{2k+3}\Big) \\
=&\ell^{4(k-1)}\frac{(\ell-1)}{(\ell+1)}\Big(\ell^{2k+4}-\ell^2+\ell^{2k+3}+\ell^{2k+2}\Big) \\
=&\ell^{6k-2}\frac{(\ell-1)}{(\ell+1)}\Big(\ell^2+\ell+1-\ell^{-2k}\Big).
\end{aligned}$$

□

Proof of Proposition 1.4.8

In this section, we prove Proposition 1.4.8.

Proposition 1.4.8. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#\mathcal{A}^t_{\ell^k,S}=\frac{(\ell-1)}{(\ell+1)}\ell^{6k-4}\left(\ell^4+\ell^3-\ell^2-2\ell-\ell^{-2k+2}\right).$$

Before we prove this proposition we need three intermediate results.

Lemma 1.B.2. *Let ℓ be an odd prime and k a positive integer. Let f be a quadratic monic polynomial in $\mathbb{Z}/\ell^k\mathbb{Z}[X]$ and D be the discriminant of f. Then*

$$\#\big\{r\in\mathbb{Z}/\ell^k\mathbb{Z}\mid f(r)=0\big\}=\begin{cases}\ell^{\lfloor k/2\rfloor} & \text{if } D=0\\ 2\ell^i & \text{if } D=u^2\ell^{2i} \text{ with } u\in\mathbb{Z}/\ell^k\mathbb{Z}^\times \\ & \text{and } 0\le i\le k/2\\ 0 & \text{else.}\end{cases}$$

Proof. Let $f = X^2 + bX + c$ be a polynomial in $\mathbb{Z}/\ell^k\mathbb{Z}[X]$.

If f has at least one zero, say a, then

$$f(a) = 0 \Leftrightarrow 4a^2 + 4ba + 4c = 0$$

$$\Leftrightarrow (2a + b)^2 = b^2 - 4c.$$

In particular, the discriminant of f is a square. Let $D = b^2 - 4c$ be the discriminant of f. We distinguish two cases based on the valuation of D.

If D is an invertible element, the result follows from Hensel's lemma. So we may assume that the valuation of D is at least one. Let $\widehat{f}$ be the reduction of f modulo ℓ. Then $\widehat{f}$ has $-b/2$ as a double zero. In particular, any zero of f in $\mathbb{Z}/\ell^k\mathbb{Z}$ is of the form $-b/2 + a$ with $a \in \ell\mathbb{Z}/\ell^k\mathbb{Z}$. Let us compute

$$f\left(-\frac{b}{2} + a\right) = 0 \Leftrightarrow (-\frac{b}{2} + a)^2 + b(-\frac{b}{2} + a) + c = 0$$

$$\Leftrightarrow \frac{b^2}{4} - \frac{b^2}{2} + c + a^2$$

$$\Leftrightarrow -\frac{D}{4} + a^2 = 0.$$

If $D = 0$, the zeros of f are precisely the elements of $-\frac{b}{2} + \ell^{\lceil k/2 \rceil}\mathbb{Z}/\ell^k\mathbb{Z}$. In particular, f has $\ell^{\lfloor k/2 \rfloor}$ zeros.

Finally, suppose that $D = u^2\ell^{2i}$ with u an invertible element. Then the zeros of f are

$$-\frac{b}{2} \pm \frac{u}{2}\ell^i + \ell^{k-i}\mathbb{Z}/\ell^k\mathbb{Z}.$$

This set has cardinality $2\ell^i$. □

For every $0 \leq i \leq k$ let P_i be the set of monic quadratic polynomials with coefficients in $\mathbb{Z}/\ell^k\mathbb{Z}$ with invertible constant term and $\min \nu(\text{Disc } f)k = i$. Moreover, consider the following subsets of P_i

$$P_{i,0} = \Big\{ f \in P_i \mid \text{Disc } f \text{ not a quadratic residue in } \mathbb{Z}/\ell^k\mathbb{Z} \Big\},$$

$$P_{i,2} = \Big\{ f \in P_i \mid \text{Disc } f \text{ a quadratic residue in } \mathbb{Z}/\ell^k\mathbb{Z} \Big\},$$

where Disc f denotes the discriminant of the quadratic polynomial f. Note that the set $P_{i,2}$ is empty for every odd i moreover, so is $P_{k,0}$ since 0 is a quadratic residue.

Lemma 1.B.3. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#P_{i,j} = \begin{cases} \frac{(\ell-1)}{2}\ell^{2k-1} & \text{if } i=0 \text{ and } j=0 \\ \frac{(\ell-1)(\ell-2)}{2}\ell^{2k-2} & \text{if } i=0 \text{ and } j=2 \\ (\ell-1)^2\ell^{2k-2t-1} & \text{if } i=2t-1<k \text{ and } j=0 \\ \frac{(\ell-1)^2}{2}\ell^{2k-2t-2} & \text{if } i=2t<k \\ (\ell-1)\ell^{k-1} & \text{if } i=k \text{ and } j=2 \\ 0 & \text{else.} \end{cases}$$

Proof. Let ℓ be an odd prime and k a positive integer. Let $f = X^2 + bX + c$ be a quadratic monic polynomial. We distinguish three cases depending on the valuation of the discriminant D of f.

1. Suppose that D is a unit. Then D is a square modulo $\mathbb{Z}/\ell^k\mathbb{Z}$ if and only if D is a quadratic residue modulo ℓ. So it suffices to count quadratic polynomials $f \in \mathbb{F}_\ell[X]$ with $f(0)$ a unit and D a quadratic residue or non-residue mod ℓ. There are $\frac{(\ell-1)\ell}{2}$ monic quadratic irreducible polynomials with $f(0) \neq 0$ in $\mathbb{F}_\ell[X]$ and $\frac{(\ell-1)(\ell-2)}{2}$ monic quadratic polynomials with $f(0) \neq 0$ and distinct roots. The result for $\nu(D) = 0$ follows from Hensel's lemma.

2. Let $0 < i < k$. Then

$$f \in P_i \Leftrightarrow c \in (b/2)^2 + \ell^i(\mathbb{Z}/\ell^k\mathbb{Z}^\times).$$

   In particular, b is a unit. For each of the $(\ell-1)\ell^{k-1}$ different choices of b, there are $(\ell-1)\ell^{k-i-1}$ choices for c. Hence, $\#P_i = (\ell-1)^2\ell^{2k-i-2}$. If $i = 2t-1$ is odd, then $P_{2t-1,2}$ is empty so $\#P_{2t-1,0} = (\ell-1)^2\ell^{2k-2t-1}$. If $i = 2t$ is even, then the discriminant is a square for half of the polynomials. Hence, $\#P_{2t,0} = \#P_{2t,2} = \frac{(\ell-1)^2}{2}\ell^{2k-2t-2}$.

3. Finally, suppose that $i = k$, then $D = 0$ if and only if $c = \frac{b^2}{4}$. Hence, for every unit b there is precisely one polynomial in the set P_k with discriminant zero. □

For every non-empty set $P_{i,j}$ fix a polynomial $f_{i,j} \in P_{i,j}$. Denote

$$M_{i,j} := \{\sigma \in GL_2(\mathbb{Z}/\ell^k\mathbb{Z}) \mid \text{char. poly. } \sigma = f_{i,j}\}.$$

If no such polynomial $f_{i,j}$ exists, $M_{i,j}$ is defined as the empty set.

Lemma 1.B.4. *Let ℓ be an odd prime and k a positive integer. Then*

$$\#M_{i,j} = \begin{cases} (\ell-1)\ell^{2k-1} & \text{if } i=0 \text{ and } j=0 \\ (\ell+1)\ell^{2k-1} & \text{if } i=0 \text{ and } j=2 \\ (\ell^{t+1}+\ell^t-\ell-1)\ell^{2k-t-1} & \text{if } i=2t-1 \text{ and } j=0 \\ (\ell^{t+1}+\ell^t-2)\ell^{2k-t-1} & \text{if } i=2t \text{ and } j=0 \\ (\ell+1)\ell^{2k-1} & \text{if } i=2t \text{ and } j=2 \\ (\ell^{m+1}+\ell^m-1)\ell^{3m-1} & \text{if } i=k=2m \text{ and } j=2 \\ (\ell^{m+1}+\ell^m-1)\ell^{3m+1} & \text{if } i=k=2m+1 \text{ and } j=2 \\ 0 & \text{else.} \end{cases}$$

In particular, $\#M_{i,j}$ does not depend on the polynomial $f_{i,j}$.

Proof. If $j=2$ and i is odd, the set $M_{i,j}$ is empty by definition and so is the set $M_{k,0}$. We prove the remaining cases.

Let ℓ be an odd prime and k a positive integer. Let $f = X^2 - TX + S \in \mathbb{Z}/\ell^k\mathbb{Z}[X]$ with S invertible. Let $D = T^2 - 4S$ be the discriminant of f. A matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ has characteristic polynomial f if and only if

$$\begin{cases} d = T - a \\ a^2 - aT + S + bc = 0. \end{cases}$$

So for every pair (b,c) and every zero of $X^2 - TX + S + bc$ there exists precisely one matrix with characteristic polynomial f. By Lemma 1.B.2 the number of zeros of $f + bc$ depends only on the discriminant of $f + bc$. The discriminant of $f + bc$ is $D - 4bc$. We distinguish three cases depending on the valuation of bc. Define

$$M_{i,j}^{<} := \{\sigma \in M_{i,j} \mid \nu(bc) < i\},$$

$$M_{i,j}^{=} := \{\sigma \in M_{i,j} \mid \min \nu(bc)k = i\},$$

$$M_{i,j}^{>} := \{\sigma \in M_{i,j} \mid \min \nu(bc)k > i\}.$$

Then for every pair i and j

$$\#M_{i,j} = \#M_{i,j}^{<} + \#M_{i,j}^{=} + \#M_{i,j}^{>}.$$

First we compute the cardinality of each of the sets $M_{i,j}^{<}$, $M_{i,j}^{=}$ and $M_{i,j}^{>}$ for all pairs i and j.

1. Suppose that $0 \leq \nu(bc) < \min \nu(D)k = i \leq k$. Then $\nu(D - 4bc) = \nu(bc)$. We need only consider tuples (b, c) such that the valuation of bc is even. Indeed, by Lemma 1.B.2 monic quadratic polynomials with odd valuated discriminant have no zeros. For each integer s with $0 \leq 2s < i$ there exist $(2s+1)(\ell-1)^2\ell^{2k-2s-2}$ pairs (b, c) such that $\nu(bc) = 2s$. Moreover, for exactly half of these pairs $D - 4bc$ is a square. In this case there exist $2\ell^s$ solution for the polynomial $f + bc$ by Lemma 1.B.2.

   So for each $0 \leq s < \lceil i/2 \rceil - 1$ we obtain $(2s + 1)(\ell - 1)^2\ell^{2k-s-2}$ different matrices with characteristic polynomial f. Summing over all s yields

$$\begin{aligned}
&\sum_{s=0}^{\lceil i/2 \rceil - 1} (2s + 1)(\ell - 1)^2\ell^{2k-s-2} \\
&= 2(\ell - 1) \sum_{s=0}^{\lceil i/2 \rceil - 1} s(\ell - 1)\ell^{2k-s-2} + (\ell - 1) \sum_{s=0}^{\lceil i/2 \rceil - 1} (\ell - 1)\ell^{2k-s-2} \\
&= 2(\ell - 1)\Big(\ell^{2k-2} + \ell^{2k-3} + \cdots + \ell^{2k-\lceil i/2 \rceil} - (\lceil i/2 \rceil - 1)\ell^{2k-\lceil i/2 \rceil - 1}\Big) \\
&\quad + (\ell - 1)\Big(\ell^{2k-1} - \ell^{2k-\lceil i/2 \rceil - 1}\Big) \\
&= (\ell - 1)\ell^{2k-\lceil i/2 \rceil - 1}\Big(2\frac{(\ell^{\lceil i/2 \rceil} - 1)}{\ell - 1} - 2\lceil i/2 \rceil + \ell^{\lceil i/2 \rceil} - 1\Big) \\
&= \ell^{2k-\lceil i/2 \rceil - 1}\Big(2\ell^{\lceil i/2 \rceil} - 2 - 2\lceil i/2 \rceil(\ell - 1) + \ell^{\lceil i/2 \rceil}(\ell - 1) - (\ell - 1)\Big) \\
&= \ell^{2k-\lceil i/2 \rceil - 1}\Big(\ell^{\lceil i/2 \rceil}(\ell + 1) - 2\lceil i/2 \rceil(\ell - 1) - \ell - 1\Big).
\end{aligned}$$

   So we obtain

$$\#M^{<}_{i,j} = \begin{cases} 0 & \text{if } i = 0 \\ \ell^{2k-\lceil i/2 \rceil - 1}\Big(\ell^{\lceil i/2 \rceil}(\ell + 1) - 2\lceil i/2 \rceil(\ell - 1) - \ell - 1\Big) & \text{else.} \end{cases}$$

2. Suppose that $0 \leq \min \nu(bc)k = i = \min \nu(D)k \leq k$. Then the valuation of $D - 4bc$ will be at least i and may be bigger depending on bc.

   If $i < k$ there are $(i + 1)(\ell - 1)^2\ell^{2k-i-2}$ pairs (b, c) such that $\nu(bc) = i$. Since every element of $D + \ell^i(\mathbb{Z}/\ell^k\mathbb{Z}^\times)$ occurs an equal amount of times as $D - 4bc$ for all b and c in $\mathbb{Z}/\ell^k\mathbb{Z}$ with $\nu(bc) = i$ it suffices to count the number of squares with given valuation. In particular, each element of $D + \ell^i(\mathbb{Z}/\ell^k\mathbb{Z}^\times)$ will occur

precisely

$$\frac{\#\left\{(b,c)\in(\mathbb{Z}/\ell^k\mathbb{Z})^2 \mid \nu(bc)=i\right\}}{\#-D+\ell^i(\mathbb{Z}/\ell^k\mathbb{Z}^\times)} = \frac{(i+1)(\ell-1)^2\ell^{2k-i-2}}{(\ell-1)\ell^{k-i-1}}$$

$$= (i+1)(\ell-1)\ell^{k-1}$$

times as the discriminant of $f+bc$ for all pairs (b,c) with $\min\nu(bc)k=i$.

If D is not a square, then for any $i\leq 2s<k$ there are $\frac{1}{2}(\ell-1)\ell^{k-2s-1}$ squares in $D+\ell^i\mathbb{Z}/\ell\mathbb{Z}^\times$ with valuation $2s$. Each square with valuation $2s<k$ induces $2\ell^s$ distinct zeros and discriminant equal to zero induces $\ell^{\lfloor k/2\rfloor}$ zeros. Summing over all cases yields

$$\begin{aligned}\#M_{i,0}^{=} &= (i+1)(\ell-1)\ell^{k-1}\Big(\ell^{\lfloor k/2\rfloor}+\sum_{s=\lceil i/2\rceil}^{\lceil k/2\rceil-1}\frac{(\ell-1)}{2}\ell^{k-2s-1}\cdot 2\ell^s\Big)\\ &= (i+1)(\ell-1)\ell^{k-1}\big(\ell^{\lfloor k/2\rfloor}+\ell^{k-\lceil i/2\rceil}-\ell^{k-\lceil k/2\rceil}\big)\\ &= (i+1)(\ell-1)\ell^{2k-\lceil i/2\rceil-1}.\end{aligned}$$

If D is a square, then there are only $\frac{1}{2}(\ell-3)\ell^{k-i-1}$ squares with valuation i as all elements in $D+\ell^{i+1}\mathbb{Z}/\ell^k\mathbb{Z}$ are quadratic residues modulo ℓ^k with valuation i and

$$\Big(D+\ell^{i+1}\mathbb{Z}/\ell^k\mathbb{Z}\Big)\cap\Big(D+\ell^i(\mathbb{Z}/\ell\mathbb{Z}^\times)\Big)=\varnothing.$$

The number of squares with valuation $2s>i$ is the same as in the case that D is a quadratic non-residue modulo ℓ^k. So summing over all s with $i\leq 2s\leq k$ yields

$$\begin{aligned}&\#M_{i,2}^{=}\\ &= (i+1)(\ell-1)\ell^{k-1}\Big(\ell^{\lfloor k/2\rfloor}+(\ell-3)\ell^{k-i/2-1}+\sum_{s=i/2+1}^{\lceil k/2\rceil-1}(\ell-1)\ell^{k-s-1}\Big)\\ &= (i+1)(\ell-1)\ell^{k-1}\Big(\ell^{\lfloor k/2\rfloor}+\ell^{k-i/2}-3\ell^{k-i/2-1}+\ell^{k-i/2-1}-\ell^{\lfloor k/2\rfloor}\Big)\\ &= (i+1)(\ell-1)(\ell-2)\ell^{2k-i/2-2}.\end{aligned}$$

Finally, suppose that $D=0=bc$. Then one checks that the number of pairs (b,c) such that $bc=0$ is $\big((k+1)\ell-k\big)\ell^{k-1}$. For each of these pairs the discriminant of the polynomial $f+bc$ equals the discriminant of the polynomial

f which is zero. In particular, every pair (b,c) induces $\ell^{\lfloor k/2 \rfloor}$ distinct matrices with characteristic polynomial f.

So the number of matrices with characteristic polynomial f and $0 \leq \min \nu(bc)k = \min \nu(D)k = i \leq k$ is

$$\#M^{=}_{i,j} = \begin{cases} (i+1)(\ell-1)(\ell-2)\ell^{2k-i/2-2} & \text{if } i < k \text{ and } j = 2 \\ \big((k+1)\ell - k\big)\ell^{k+\lfloor k/2 \rfloor - 1} & \text{if } i = k \\ (i+1)(\ell-1)\ell^{2k-\lceil i/2 \rceil - 1} & \text{else.} \end{cases}$$

3. Suppose that $0 \leq i = \nu(D) < \min \nu(bc)k \leq k$. If D is not a square in $\mathbb{Z}/\ell^k\mathbb{Z}$, then $D - 4bc$ is not a square since $D - 4bc \equiv D \mod \ell^{\nu(bc)}$ and D is a quadratic non-residue modulo $\ell^{\nu(bc)}$. So if D is not a square, no matrices exists.

   If D is a square with even valuation i one checks that there exists $\ell^{2k-i-2}\big((i+2)\ell - i - 1\big)$ pairs (b,c) such that $i < \min \nu(bc)k \leq k$. For each pair there exists $2\ell^{i/2}$ zeros of the polynomial $f + bc$. Hence, we find

$$\#M^{>}_{i,j} = \begin{cases} 2\ell^{2k-i/2-2}\big((i+2)\ell - i - 1\big) & \text{if } i < k \text{ and } j = 2 \\ 0 & \text{else.} \end{cases}$$

We compute the sum $\#M_{i,j} = \#M^{<}_{i,j} + \#M^{=}_{i,j} + \#M^{>}_{i,j}$ for each pair i and j.

1. Suppose that $\nu(D) = 0$ and D is a quadratic non-residue. Then there exist no matrices with characteristic polynomial f unless $\nu(bc) = 0$. In this case

$$\#M_{0,0} = (\ell-1)\ell^{2k-1}.$$

2. If $\nu(D) = 0$ and D is a quadratic residue. There exist $(\ell-1)(\ell-2)\ell^{2k-2}$ matrices with $\nu(bc) = 0$ and $2\ell^{2k-2}(2\ell-1)$ with $\nu(bc) > 0$. Hence, we obtain

$$\#M_{0,2} = (\ell+1)\ell^{2k-1}.$$

3. If $0 < i < k$ is odd, say $i = 2t-1$. Then

$$\begin{aligned} \#M_{2t-1,0} &= \ell^{2k-t-1}\Big(\ell^t(\ell+1) - 2t(\ell-1) - \ell - 1\Big) + 2t(\ell-1)\ell^{2k-t-1} \\ &= (\ell^{t+1} + \ell^t - \ell - 1)\ell^{2k-t-1}. \end{aligned}$$

4. If i is even say $i = 2t$ and D is not a square. We obtain

$$\begin{aligned} \#M_{2t,0} &= \ell^{2k-t-1}\big(\ell^t(\ell+1) - 2t(\ell-1) - \ell - 1\big) \\ &\quad + (2t+1)(\ell-1)\ell^{2k-t-1} \\ &= (\ell^{t+1} + \ell^t - 2)\ell^{2k-t-1}. \end{aligned}$$

5. If $i = 2t$ and D is a square. Then summing over all cases yields

$$\begin{aligned}\#M_{2t,2} &= \ell^{2k-t-1}\big(\ell^t(\ell+1) - 2t(\ell-1) - \ell - 1\big)\\ &\quad + \ell^{2k-t-2}(2t+1)(\ell-1)(\ell-2) + 2\ell^{2k-t-2}\big((2t+2)\ell - 2t - 1\big)\\ &= (\ell+1)\ell^{2k-1}.\end{aligned}$$

6. If $D = 0$ and $k = 2m$. We obtain

$$\begin{aligned}\#M_{k,2} &= \ell^{4m-m-1}\big(\ell^m(\ell+1) - 2m(\ell-1) - \ell - 1\big)\\ &\quad + \ell^{2m+m-1}\big((2m+1)\ell - 2m\big)\\ &= \ell^{3m-1}(\ell^{m+1} + \ell^m - 1).\end{aligned}$$

7. If $D = 0$ and $k = 2m+1$. Then

$$\begin{aligned}\#M_{k,2} &= \ell^{4m+2-m-1-1}\big(\ell^{m+1}(\ell+1) - 2(m+1)(\ell-1) - \ell - 1\big)\\ &\quad + \ell^{2m+1+m-1}\big((2m+2)\ell - 2m - 1\big)\\ &= \ell^{3m+1}(\ell^{m+1} + \ell^m - 1).\end{aligned}$$

In particular, the cardinality of $M_{i,j}$ does not depend on the choice of $f_{i,j}$. □

Proof of Proposition 1.4.8. Recall that

$$\mathcal{A}^t_{\ell^k,S} = \{(\tau,\tau') \in GL_2(\mathbb{Z}/\ell^k\mathbb{Z})^2 \mid \text{char. poly. } \tau = \text{char. poly. } \tau'\}.$$

So

$$\begin{aligned}\#\mathcal{A}^t_{\ell^k,S} &= \sum_{f\in\mathbb{Z}/\ell^k\mathbb{Z}[X]} \big(\#\{\tau \in GL_2(\mathbb{Z}/\ell^k\mathbb{Z}) \mid \text{char. poly. } \tau = f\}\big)^2\\ &= \sum_{i,j} \#P_{i,j}\cdot(\#M_{i,j})^2\end{aligned}$$

where the sum is taken over all pairs (i,j) with $0 \le i < k$ and $j = 0, 2$ and the pair $(i,j) = (k,2)$. The factors $\#P_{i,j}$ and $\#M_{i,j}$ are computed in Lemmas 1.B.3 and 1.B.4, respectively. We will only give the proof if k is odd. If k is even the computation

is similar. Suppose that $k = 2m + 1$. Then

$$\begin{aligned}
\#\mathcal{A}^t_{\ell^k,S} =& \frac{(\ell-1)}{2}\ell^{2k-1}\cdot(\ell-1)^2\ell^{4k-2} + \frac{(\ell-1)(\ell-2)}{2}\ell^{2k-2}\cdot(\ell+1)^2\ell^{4k-2} \\
&+ \sum_{t=1}^{m}\Big((\ell-1)^2\ell^{2k-2t-1}\cdot\big(\ell^t(\ell+1)-(\ell+1)\big)^2\ell^{4k-2t-2} \\
&+ \frac{(\ell-1)^2}{2}\ell^{2k-2t-2}\cdot\big(\ell^t(\ell+1)-2\big)^2\ell^{4k-2t-2} \\
&+ \frac{(\ell-1)^2}{2}\ell^{2k-2t-2}\cdot(\ell+1)^2\ell^{4k-2}\Big) \\
&+ (\ell-1)\ell^{2m}\cdot\big(\ell^m(\ell+1)-1\big)^2\ell^{6m+2} \\
=& \frac{(\ell-1)}{2}\ell^{6k-4}\big((\ell-1)^2\ell+(\ell+1)^2(\ell-2)\big) \\
&+ \sum_{t=1}^{m}\ell^{6k-4t-4}\Bigg(\\
&\frac{(\ell-1)^2}{2}\big(2\ell^{2t+1}(\ell+1)^2-4\ell^{t+1}(\ell+1)^2+2\ell(\ell+1)^2\big) \\
&+ \frac{(\ell-1)^2}{2}\big(\ell^{2t}(\ell+1)^2-4\ell^t(\ell+1)+4\big) \\
&+ \frac{(\ell-1)^2}{2}\ell^{2t}(\ell+1)^2\Bigg) \\
&+ (\ell-1)\ell^{8m+2}\big(\ell^{2m}(\ell+1)^2-2\ell^m(\ell+1)+1\big) \\
=& \frac{(\ell-1)}{2}\ell^{6k-4}(2\ell^3-2\ell^2-2\ell-2) \\
&+ \frac{(\ell-1)^2}{2}\sum_{t=1}^{m}\Bigg(\\
&\ell^{6k-4t-4}\Big(2\ell^{2t}(\ell+1)^3-4\ell^t(\ell+1)(\ell^2+\ell+1)+2(\ell^2+1)(\ell+2)\Big)\Bigg) \\
&+ (\ell-1)\big((\ell+1)^2\ell^{10m+2}-2(\ell+1)\ell^{9m+2}+\ell^{8m+2}\big).
\end{aligned}$$

Splitting the summation into three sums yields

$$\begin{aligned}
\#\mathcal{A}^t_{\ell^k,S} =&(\ell-1)\ell^{6k-4}(\ell^3-\ell^2-\ell-1)\\
&+(\ell-1)(\ell+1)^2\sum_{t=1}^{m}(\ell^2-1)\ell^{6k-2t-4}\\
&-2(\ell-1)(\ell+1)\sum_{t=1}^{m}(\ell^3-1)\ell^{6k-3t-4}\\
&+\frac{(\ell-1)(\ell+2)}{(\ell+1)}\sum_{t=1}^{m}(\ell^4-1)\ell^{6k-4t-4}\\
&+(\ell-1)\big((\ell+1)^2\ell^{10m+2}-2(\ell+1)\ell^{9m+2}+\ell^{8m+2}\big).
\end{aligned}$$

Computing the telescopic sums and using that $k=2m+1$

$$\begin{aligned}
\#\mathcal{A}^t_{\ell^k,S} =&(\ell-1)\ell^{12m+2}(\ell^3-\ell^2-\ell-1)\\
&+(\ell-1)(\ell+1)^2(\ell^{12m+2}-\ell^{10m+2})\\
&-2(\ell-1)(\ell+1)(\ell^{12m+2}-\ell^{9m+2})\\
&+\frac{(\ell-1)(\ell+2)}{(\ell+1)}(\ell^{12m+2}-\ell^{8m+2})\\
&+(\ell-1)\big((\ell+1)^2\ell^{10m+2}-2(\ell+1)\ell^{9m+2}+\ell^{8m+2}\big).
\end{aligned}$$

By sorting the powers of ℓ^m we obtain

$$\begin{aligned}
\#\mathcal{A}^t_{\ell^k,S} =&(\ell-1)\ell^{12m+2}\Big((\ell^3-\ell^2-\ell-1)+(\ell+1)^2-2(\ell+1)+\frac{(\ell+2)}{(\ell+1)}\Big)\\
&+(\ell-1)(\ell+1)^2\ell^{10m+2}(-1+1)\\
&-2(\ell-1)(\ell+1)\ell^{9m+2}(-1+1)\\
&+(\ell-1)\ell^{8m+2}\Big(-\frac{(\ell+2)}{(\ell+1)}+1\Big)\\
=&(\ell-1)\ell^{12m+2}\Big(\ell^3-\ell-2+\frac{(\ell+2)}{(\ell+1)}\Big)-\frac{(\ell-1)}{(\ell+1)}\ell^{8m+2}\\
=&\frac{(\ell-1)}{(\ell+1)}\ell^{12m+2}(\ell^4+\ell^3-\ell^2-2\ell-\ell^{-4m}).
\end{aligned}$$

Using that $k = 2m + 1$ yields

$$\#\mathcal{A}^t_{\ell^k,S} = \frac{(\ell-1)}{(\ell+1)}\ell^{6k-4}(\ell^4 + \ell^3 - \ell^2 - 2\ell - \ell^{-2k+2}). \qquad \square$$

Part II

Hilbert Modular Forms

Introduction

Hilbert modular forms are a generalisation of classical modular forms to holomorphic functions in more than one variable. David Hilbert was the first to consider these objects, even if he did not publish on this subject. However, his first PhD student, Otto Blumenthal, published *Zum Eliminationsproblem bei analytischen Funktionen mehrerer Veränderlicher* on the topic in 1903.

Established methods to compute Hilbert modular forms are restricted to weight larger than 2. As with classical modular forms, the weight 1 case is more intricate. However, one can use the graded algebra of Hilbert modular forms to compute the adelic q-expansion of a Hilbert modular form of (partial) weight 1 as the quotient of modular forms of higher weights.

If f and E are Hilbert modular forms of level $\mathfrak{N}$, weights k and k' and characters $\mathcal{E}$ and $\mathcal{E}'$ respectively, then their product $f \cdot E$ is a Hilbert modular form of weight $k + k'$ and character $\mathcal{E} \cdot \mathcal{E}'$. So, if the adelic q-expansion of E is invertible, then any Hilbert modular form of weight k is the quotient of a Hilbert modular form of weight $k + k'$ by the form E, i.e.

$$\mathcal{M}_k(\mathfrak{N}, \mathcal{E}) \subset \frac{1}{E}\mathcal{M}_{k+k'}(\mathfrak{N}, \mathcal{E} \cdot \mathcal{E}').$$

Moreover, the left hand side is stable under the action of the Hecke algebra of weight k, so we can shrink the right hand side by taking the largest subspace of $\frac{1}{E}\mathcal{M}_{k+k'}(\mathfrak{N}, \mathcal{E} \cdot \mathcal{E}')$ that is stable under the action of the Hecke algebra. The underlying philosophy is that we can shrink this candidate space until it only contains Hilbert modular forms of weight k. This philosophy was used for the first time for classical modular forms in 1978 by Joe Buhler in [5] and later by Kevin Buzzard in [6] and George Schaeffer in [29], and for classical Hilbert modular forms over quadratic fields with narrow class number 1 by Richard Moy and Joel Specter in [22].

The key observation that enables these results to extend to Hilbert modular forms is that we can verify whether or not a candidate fraction of Hilbert modular forms is indeed a Hilbert modular form by using its truncated adelic q-expansion. That is, we prove that the square of the truncated adelic q-expansion of such a fraction g/E coincides with

the adelic q-expansion of a Hilbert modular form (of higher weight) if and only if the the quotient of the truncated adelic q-expansions of g and E coincides with the adelic q-expansion of a Hilbert modular form (of lower weight).

We apply this approach to compute Hilbert modular forms with coefficients in $\mathbb{C}$ and any weight as well as Hilbert modular forms over finite fields with parallel weight. In particular, we prove that our algorithm computes in almost all characteristics simultaneously, in the sense that the output of our algorithm with given level $\mathfrak{N}$ and character $\mathcal{E}$ includes a finite set of primes $\mathcal{L}$ such that for all primes p not contained in $\mathcal{L}$ satisfying certain conditions in higher weight, all Hilbert modular forms in $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; \overline{\mathbb{F}}_p)$ lift to characteristic zero. Finally, we use our algorithm to find explicit examples of non-liftable Hilbert modular forms of parallel weight 1 by running the algorithms for primes contained in $\mathcal{L}$.

In Chapter 2, we introduce notation and preliminaries concerning characters used in later chapters

Chapter 3 provides an introduction to the basics of Hilbert modular forms of (partial) weight over $\mathbb{C}$, their adelic and geometric q-expansions and the Hecke operators acting on them. We give a detailed description of the algorithms that can be used to compute the spaces of Hilbert modular forms of (partial) weight 1 and the conditions required to apply the different algorithms.

In Chapter 4 we show how we extended the algorithm to the module of parallel weight Hilbert modular forms with adelic q-expansions in more general rings, specifically with integer coefficients and with coefficients in finite fields. In particular, we describe how to use these algorithms to determine precisely which level, characters and characteristics admit non-liftable Hilbert modular forms. The last part of this chapter contains explicit numerical examples.

Chapter 2

Preliminaries

Notation

In Part II, the field K will denote a totally real number field of degree $n > 1$, and $\mathcal{O}_K$ its ring of integers. If a is an element of K we will denote by $a^{(1)}, ..., a^{(n)}$ the n distinct embeddings of K into $\mathbb{R}$. An element a of K is said to be *totally positive*, denoted $a \gg 0$, if $a^{(i)} > 0$ for all embeddings of K into $\mathbb{R}$. If $\mathfrak{a}$ is a subset of K, we will denote $\mathfrak{a}^+$ the subset of totally positive elements of $\mathfrak{a}$. For example $\mathcal{O}_K^{\times,+}$ is the set of totally positive units in $\mathcal{O}_K$. We will use the notation $\mathfrak{p} \mid \infty$ and $\mathfrak{p} < \infty$ to denote that a place of K is archimedean or non-archimedean, respectively.

Let I_K be the group of fractional ideals of K. The *class group of* K, denoted Cl, is the quotient of I_K by the subgroup of principal ideals in K. The *narrow class group of* K, denoted Cl^+, is the quotient of I_K by the subgroup of principal ideals in K that are generated by a totally positive element of $\mathcal{O}_K$. Both the class group and the narrow class group are finite. Their cardinalities are called the *class number* and the *narrow class number*, and denoted by h and h^+, respectively.

For n-tuples $z = (z_1, ..., z_n) \in \mathbb{C}^n$ and $k = (k_1, ..., k_n) \in \mathbb{Z}^n$ we write

$$z^k = \prod_{i=1}^{n} z_i^{k_i} \qquad \text{and} \qquad \mathrm{tr}(z) = \sum_{i=1}^{n} z_i.$$

We extend this notation to K by identifying $\xi \in K$ with the n-tuple $\left(\xi^{(1)}, ..., \xi^{(n)}\right)$ in $\mathbb{R}^n$, i.e.

$$\xi^k = \prod_{i=1}^{n} \left(\xi^{(i)}\right)^{k_i} \qquad \text{and} \qquad \mathrm{tr}(\xi) = \sum_{i=1}^{n} \xi^{(i)}.$$

Moreover, we write $k_0 = \max_i\{k_i\}$ and $\underline{k}$ to denote the parallel vector $\underline{k} = (k, ..., k)$ for an integer k. Note that under these conventions we have that

$$\mathrm{N}(\xi) = \xi^{\underline{1}} \qquad \text{and} \qquad \mathrm{tr}_{K/\mathbb{Q}}(\xi) = \mathrm{tr}(\xi).$$

Finally, we write

$$\mathrm{sgn}(\cdot)^k : (\mathbb{R}^\times)^n \to \{\pm 1\} : x \mapsto \left(\frac{x}{|x|}\right)^k$$

for the multiplicative character on $(\mathbb{R}^\times)^n$ and its extension to K by the n real embeddings as above.

Adèles and Idèles

The notion of idèle is a modification of the notion of ideal. It was first introduced by the French mathematician Claude Chevalley in the 20th century. Chevalley used the term ideal element, which was abbreviated as id.el., hence the name idèle.

Let $\mathfrak{p}$ be any place of K. Then we denote the completion of K with respect to $\mathfrak{p}$ by $K_\mathfrak{p}$. Note that $K_\mathfrak{p} = \mathbb{R}$ for all infinite places. If $\mathfrak{p}$ is a finite place of K, then $\mathcal{O}_\mathfrak{p}$ denotes the ring of integers of $K_\mathfrak{p}$ and $\nu_\mathfrak{p}$ denotes the $\mathfrak{p}$-adic valuation on $K_\mathfrak{p}$.

The group of *adèles* of K, denoted $\mathbb{A}_K$, is the restricted product indexed by the set of all places

$$\mathbb{A}_K = \widehat{\prod_\mathfrak{p}} K_\mathfrak{p}$$

with respect to the subgroups $\mathcal{O}_\mathfrak{p}$. In other words, an adèle is an element $\alpha = (\alpha_\mathfrak{p})_\mathfrak{p} \in \prod_\mathfrak{p} K_\mathfrak{p}$ indexed by all the places $\mathfrak{p}$ of K such that $\alpha_\mathfrak{p}$ is an element of $\mathcal{O}_\mathfrak{p}$ for all but finitely many finite places $\mathfrak{p}$.

The *idèle group of* K is defined as the unit group of the adèles and denoted $\mathbb{A}_K^\times$. The inclusion $K \subset K_\mathfrak{p}$ allows us to view $K^\times$ as a subgroup of $\mathbb{A}_K$ by the diagonal embedding

$$K^\times \to \mathbb{A}_K : a \to (a)_\mathfrak{p}.$$

As a subset of the product of $K_\mathfrak{p}^\times$ the idèles inherit a natural topology. However, with this topology the set of idèles is not a topological group. Instead, we use the so called restricted topology. A basis is given by the open sets of the form

$$\prod_\mathfrak{p} V_\mathfrak{p},$$

where $V_\mathfrak{p}$ is an open in $K_\mathfrak{p}$ and $V_\mathfrak{p} = O_\mathfrak{p}^\times$ for almost all finite places $\mathfrak{p}$. The group of idèles equipped with the restricted topology is a locally compact topological group, see [24, VI.I].

Given an idèle $\alpha \in \mathbb{A}_K^\times$ there are only finitely many places $\mathfrak{p}$ such that $\nu_\mathfrak{p}(\alpha_\mathfrak{p}) \neq 0$. Hence, we can associate to every idèle α a fractional ideal of K by

$$\mathbb{A}_K^\times \to I_K : \alpha \mapsto \prod_{\mathfrak{p}<\infty} \mathfrak{p}^{\nu_\mathfrak{p}(\alpha_\mathfrak{p})}.$$

Moreover, this map induces surjective morphisms to both the class group and the narrow class group of K. In particular, we can consider any idèle in $\mathbb{A}_K^\times$ as a fractional ideal of K. Therefore, we will not distinguish notation between an idèle and its associated fractional ideal. For more details on adèles see [24, Section VI.1].

Characters

In this section, we will discuss Hecke characters, Größencharakters and characters of the narrow class group. They were introduced in the PhD dissertation of Erich Hecke under the supervision of David Hilbert, as a generalisation of Dirichlet characters on $\mathbb{Z}$. The names Größencharakter and Hecke characters are often used interchangeable. However, we will follow the approach of Jürgen Neukirch's *Algebraic Number Theory*, see [24, VII Section 6]. That is, we will define both Hecke characters and Größencharakters and show how to obtain one from the other and vice versa. Finally, we will show how characters of the narrow class group form a subset of Hecke characters.

Let $\mathfrak{m}$ be an integral ideal of K. We will denote by $I^\mathfrak{m}$ the group of all fractional ideals of K that are relatively prime to $\mathfrak{m}$ in the following sense, the fractional ideal with factorisation into prime ideals $\prod_\mathfrak{p} \mathfrak{p}^{r_\mathfrak{p}}$ is coprime to $\mathfrak{m}$ if $r_\mathfrak{p} = 0$ for all prime ideals $\mathfrak{p}$ dividing $\mathfrak{m}$.

Definition 2.0.1. *A* Größencharakter mod $\mathfrak{m}$ *is a character* $\chi : I^\mathfrak{m} \to \mathbb{C}^\times$ *such that there exists a pair of characters*

$$\chi_f : (\mathcal{O}/\mathfrak{m})^\times \to \mathbb{C}^\times, \qquad \chi_\infty : (\mathbb{R}^\times)^n \to \mathbb{C}^\times$$

satisfying

$$\chi\big((a)\big) = \chi_f(a) \cdot \chi_\infty(a)$$

for every algebraic integer $a \in \mathcal{O}$ *such that* (a) *is relatively prime to* $\mathfrak{m}$*. The character* χ_f *is called the* finite part *of* χ *and* χ_∞ *is called the* infinite part *of* χ*.*

A character χ of $I^\mathfrak{m}$ is a Größencharakter mod $\mathfrak{m}$ as soon as there exists a character χ_∞ such that

$$\chi\big((a)\big) = \chi_\infty(a)$$

for all $a \in \mathcal{O}_K$ such that $a \equiv 1 \mod \mathfrak{m}$. Indeed, we can define the finite part of the character by $\chi_f(a) := \chi\big((a)\big)\chi_\infty(a)^{-1}$.

Proposition 2.0.2. *Let χ be a Größencharakter mod $\mathfrak{m}$ and let $\mathfrak{m}'$ be an integral ideal dividing $\mathfrak{m}$. Then the following are equivalent:*

1. *The character χ is the restriction of a Größencharakter χ' mod $\mathfrak{m}'$;*
2. *The character χ_f factors through $(\mathcal{O}/\mathfrak{m}')^\times$.*

Proof. See [24, VII Proposition 6.2]. □

A Größencharakter mod $\mathfrak{m}$ is called *primitive* if it is not the restriction of a Größencharakter χ' mod $\mathfrak{m}'$ for any proper divisor $\mathfrak{m}' \mid \mathfrak{m}$. According to Proposition 2.0.2 this is the case if and only if the character χ_f of $(\mathcal{O}/\mathfrak{m})^\times$ is primitive, i.e. if χ_f does not factor through $(\mathcal{O}/\mathfrak{m}')^\times$ for any proper divisor $\mathfrak{m}' \mid \mathfrak{m}$. The *Conductor of* χ is the smallest divisor $\mathfrak{f}$ of $\mathfrak{m}$ such that χ is the restriction of a Größencharakter mod $\mathfrak{f}$. Again by Proposition 2.0.2, it is the conductor of χ_f.

Definition 2.0.3. *A* Hecke character *is a character of the idèle class group of the number field K, i.e. a continuous homomorphism*

$$\mathcal{E} : \mathbb{A}_K^\times \to \mathbb{C}^\times$$

of the idèle group such that $\mathcal{E}(K^\times) = 1$.

Let $\mathfrak{p}$ be a finite place and $r \geq 1$ an integer. Consider the following subsets of $K_\mathfrak{p}^\times$

$$U_\mathfrak{p}^{(0)} = \mathcal{O}_\mathfrak{p}^\times \qquad \text{and} \qquad U_\mathfrak{p}^{(r)} = 1 + \mathfrak{p}^r.$$

Let $\mathfrak{m}$ be an integral ideal of K and $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{r_\mathfrak{p}}$ its factorisation into prime ideals. We associate to this ideal the subgroup $\bar{I}_K^\mathfrak{m}$ of $\mathbb{A}_K^\times$,

$$\bar{I}_K^\mathfrak{m} = \prod_{\mathfrak{p} \nmid \infty} U_\mathfrak{p}^{(r_\mathfrak{p})} \times \prod_{\mathfrak{p} \mid \infty} K_\mathfrak{p}^\times = I_f^\mathfrak{m} \times I_\infty.$$

We call the ideal $\mathfrak{m}$ a *module of definition* of the Hecke character $\mathcal{E}$ if

$$\mathcal{E}(I_f^\mathfrak{m}) = 1.$$

Every Hecke character admits a module of definition. Indeed, the image $\mathcal{E}\left(\prod_{\mathfrak{p}\nmid\infty} \mathcal{O}_\mathfrak{p}^\times\right)$ is a compact and totally disconnected subgroup of $\mathbb{C}^\times$, hence finite. In particular, the kernel of $\mathcal{E}$ contains a subgroup of the form $\prod_{\mathfrak{p}\nmid\infty} U_\mathfrak{p}^{(r_\mathfrak{p})}$ where $n_\mathfrak{p} = 0$ for almost all finite places $\mathfrak{p}$. So $\mathfrak{m} = \prod_{\mathfrak{p}\nmid\infty} \mathfrak{p}^{r_\mathfrak{p}}$ will be a module of definition.

Given a Hecke character $\mathcal{E}$ with module of definition $\mathfrak{m}$, we will construct a Größencharakter mod $\mathfrak{m}$ as follows. For every finite place $\mathfrak{p}$, we fix a prime element $\pi_\mathfrak{p}$ of K_p and construct a homomorphism

$$c : I^\mathfrak{m} \to \mathbb{A}_K^\times / I_f^\mathfrak{m} K^\times : \mathfrak{p} \mapsto [\pi_\mathfrak{p}] = (..., 1, 1, \pi_\mathfrak{p}, 1, 1, ...).$$

This mapping does not depend on the choices of the prime elements. The prime elements in the local field $K_\mathfrak{p}$ are unique up to a unit in $\mathcal{O}_\mathfrak{p}$ and the idèles of the form $(u_\mathfrak{p})_\mathfrak{p}$ with all $u_\mathfrak{p}$ in $\mathcal{O}_K^\times$ lie in $I_f^\mathfrak{m}$.

Proposition 2.0.4. *Taking the composite map*

$$I^\mathfrak{m} \xrightarrow{c} \mathbb{A}_K^\times / I_f^\mathfrak{m} K^\times \xrightarrow{\mathcal{E}} \mathbb{C}^\times$$

yields a 1-1 *correspondence between Hecke characters with module of definition* $\mathfrak{m}$ *and Größencharakter mod* $\mathfrak{m}$.

Proof. See [24, VII Corollary 6.14]. □

Let $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{r_\mathfrak{p}}$ be an integral ideal and recall that $I^\mathfrak{m}$ denotes the group of all fractional ideals of K that are relatively prime to $\mathfrak{m}$, that is, those ideals with no common factors in the unique factorisation into prime ideals. The *narrow ray*, $P^{\mathfrak{m},+}$ is the subgroup of principal ideals generated by totally positive elements a, with $\nu_\mathfrak{p}(a-1) \geq r_\mathfrak{p}$ for all $\mathfrak{p}$ dividing $\mathfrak{m}$. The *narrow ray class group mod* $\mathfrak{m}$ is the quotient $I^\mathfrak{m}/P^{\mathfrak{m},+}$. Note that the narrow ray class group mod $\mathfrak{m}$ is simply called the ray class group in [24]. However, Neukirch himself remarks that the name ray class group is generally used for another group.

Definition 2.0.5. *A* Dirichlet character mod $\mathfrak{m}$ *is a character*

$$\chi : I^\mathfrak{m}/P^{\mathfrak{m},+} \to \mathbb{C}^\times$$

of the narrow ray class group mod $\mathfrak{m}$.

The following proposition redefines the narrow ray class group in an idèlic language.

Proposition 2.0.6. *Let* $\mathfrak{m} = \prod_\mathfrak{p} \mathfrak{p}^{r_\mathfrak{p}}$ *be an integral ideal. Then the identification of idèles and ideals induces an isomorphism*

$$\mathbb{A}_K^\times / \left(\prod_{\mathfrak{p}<\infty} U_\mathfrak{p}^{r_\mathfrak{p}} \times \prod_{\mathfrak{p}|\infty} \mathbb{R}^{\times,+} \right) \cong I^\mathfrak{m}/P^{\mathfrak{m},+}.$$

Proof. See [24, I Proposition 1.9] □

Corollary 2.0.7. *Let $\mathcal{E}$ be a Hecke character with module of definition $\mathfrak{N}$, and χ the associated Größencharakter mod $\mathfrak{N}$. Then the following are equivalent:*

1. *The Hecke character $\mathcal{E}$ is a Dirichlet character mod $\mathfrak{m}$, i.e. $\mathcal{E}(P^{\mathfrak{m},+}) = 1$.*
2. *There exists an element r of $(\mathbb{Z}/2\mathbb{Z})^n$ such that*

$$\chi_\infty = \mathrm{sgn}(\cdot)^r.$$

The definition of Hecke characters varies between authors and the distinction between Hecke and Größencharakter is not always made. Because of Proposition 2.0.4 there is no need to make a distinction. From now on we only consider Dirichlet characters $\mathcal{E}$, that is, Hecke characters with infinity type of the form $\mathrm{sgn}(\cdot)^r$ for some r in $\mathbb{Z}/2\mathbb{Z}^n$ and consider $\mathcal{E}$ as a map from the set of all ideals to $\mathbb{C}^\times$ by using the above correspondence and setting $\mathcal{E}(\mathfrak{a}) = 0$ if $\mathfrak{a}$ and $\mathfrak{m}$ are not relatively prime. We will denote such a character simply by *a character mod* $\mathfrak{N}$.

L-series

Let $\mathfrak{m}$ be an integral ideal and $\mathcal{E} : I^{\mathfrak{m}} \to \mathbb{C}^\times$ a Hecke character mod $\mathfrak{m}$. The L-series of the character $\mathcal{E}$ is

$$L(\mathcal{E}, s) = \sum_{\mathfrak{a}} \mathcal{E}(\mathfrak{a})\mathrm{N}(\mathfrak{a})^{-s}.$$

Proposition 2.0.8. *The L-series $L(\mathcal{E}, s)$ converges absolutely and uniformly in the domain $Re(s) > 1 + \delta$ for all $\delta > 0$. Moreover, one has*

$$L(\mathcal{E}, s) = \prod_{\mathfrak{p}} \frac{1}{1 - \mathcal{E}(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{-s}},$$

where the product varies over the prime ideals of K.

Proof. See [24, VII Proposition 8.1]. □

Corollary 2.0.9. *The L-series $L(\mathcal{E}, s)$ has a meromorphic continuation to the whole complex plane.*

Proof. This follows from [24, VII Theorem 8.5] applied to $\mathcal{E}$. □

Chapter 3

Hilbert Modular Forms

3.1 Hilbert Modular Forms

In this section, we give a brief introduction to Hilbert modular forms. For more details see [1], [13] and [33].

Let K be a totally real number field of degree $n > 1$ as above. Let $\mathcal{H}^n$ be n-copies of the complex upper half plane, i.e.

$$\mathcal{H}^n = \{z = (z_1, ..., z_n) \in \mathbb{C}^n \mid \mathrm{Im}(z_i) > 0\}.$$

We define the action of the group

$$\mathrm{GL}_2^+(K) := \left\{\gamma \in \mathrm{GL}_2(K) \mid \det \gamma \gg 0\right\}$$

on $\mathcal{H}^n$ by coordinate-wise linear fractional transformations

$$\gamma \cdot z := \frac{az+b}{cz+d} = \left(\frac{a^{(i)}z_i + b^{(i)}}{c^{(i)}z_i + d^{(i)}}\right)_{i=1}^{n}$$

with $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $z = (z_1, ..., z_n)$.

Classical Hilbert Modular Forms

Definition 3.1.1. *A* congruence subgroup *of* $\mathrm{GL}_2^+(K)$ *is a subgroup of* $\mathrm{GL}_2^+(K)$ *that contains the kernel of the reduction morphism*

$$\pi : \mathrm{SL}_2(\mathcal{O}_K) \to \mathrm{SL}_2(\mathcal{O}_K/\mathfrak{N}\mathcal{O}_K)$$

for some integral ideal $\mathfrak{N}$ of K and such that $\Gamma/(\Gamma \cap K^\times)$ is commensurable with $\mathrm{SL}_2(\mathcal{O}_K)/\{\pm 1\}$.

Example 3.1.2. *For any integral ideal $\mathfrak{N}$ and fractional ideal $\mathfrak{c}$ the subgroups*

$$\Gamma_0(\mathfrak{c},\mathfrak{N}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \begin{pmatrix} \mathcal{O}_K & \mathfrak{c}^{-1} \\ \mathfrak{c}\mathfrak{N} & \mathcal{O}_K \end{pmatrix} \;\middle|\; ad - cd \in \mathcal{O}_K^{\times,+} \right\} \text{ and}$$

$$\Gamma_1(\mathfrak{c},\mathfrak{N}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \begin{pmatrix} \mathcal{O}_K & \mathfrak{c}^{-1} \\ \mathfrak{c}\mathfrak{N} & 1+\mathfrak{N} \end{pmatrix} \;\middle|\; ad - cd \in \mathcal{O}_K^{\times,+} \right\},$$

are both congruence subgroups. These are the only type of congruence subgroups we will consider.

Definition 3.1.3. *Let $k = (k_1, ..., k_n)$ be an element of $\mathbb{Z}^n$, Γ a congruence subgroup and $\mathcal{E}$ a character mod $\mathfrak{N}$. A* classical Hilbert modular form of weight k, level Γ and character $\mathcal{E}$ *is a holomorphic function*

$$f : \mathcal{H}^n \to \mathbb{C}$$

such that

$$f(\gamma \cdot z) = \mathcal{E}_f(d) \cdot \frac{(cz+d)^k}{\det(\gamma)^{k/2}} f(z),$$

for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ in Γ. We denote the space of classical Hilbert modular forms of weight k, level Γ and character $\mathcal{E}$ by $\mathcal{M}_k^c(\Gamma, \mathcal{E})$.

Remark 3.1.4. *Note that the definition of a classical Hilbert modular form differs from the definition of a classical modular form as defined in 1.1.2. We do not require the form to be holomorphic at the cusp. That is because this condition is automatically satisfied if $K \neq \mathbb{Q}$. This result is known as* Koechers principle *and we will give a full statement and proof later, see 3.3.2.*

Hilbert Modular Forms

For the remainder of Part II, we fix $\mathfrak{t}_1, ..., \mathfrak{t}_{h^+}$ elements of $\mathbb{A}_K^\times$ such that their associated fractional ideals form a complete set of representatives of the narrow class group of K. We will use the same notation, $\mathfrak{t}_\lambda$, for both the idèle and the associated fractional ideal.

Definition 3.1.5. *Let $k = (k_1, ..., k_n)$ be an element of $\mathbb{Z}^n$, $\mathfrak{N}$ an integral ideal of K and $\mathcal{E}$ a character mod $\mathfrak{N}$. A* Hilbert modular form of weight k, level $\mathfrak{N}$ and character $\mathcal{E}$ *is an h^+-tuple of holomorphic functions*

$$f_\lambda : \mathcal{H}^n \to \mathbb{C}$$

such that for all $\lambda = 1, ..., h^+$ *and all* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *in* $\Gamma_0(\mathfrak{t}_\lambda, \mathfrak{N})$*,* f_λ *satisfies*

$$f_\lambda(\gamma \cdot z) = \mathcal{E}_f(d) \cdot \frac{(cz+d)^k}{\det(\gamma)^{k/2}} f_\lambda(z).$$

We denote the space of Hilbert modular forms of weight k*, level* $\mathfrak{N}$ *and character* $\mathcal{E}$ *by* $\mathcal{M}_k(\mathfrak{N}, \mathcal{E})$*.*

Note that by definition of the space of Hilbert modular forms we have an isomorphism of complex vector spaces

$$M_k(\mathfrak{N}, \mathcal{E}) \cong \bigoplus_{\lambda=1}^{h^+} \mathcal{M}_k^c\big(\Gamma_0(\mathfrak{t}_\lambda, \mathfrak{N}), \mathcal{E}\big).$$

Remark 3.1.6. *Not all authors make the distinction in terminology between classical Hilbert modular forms and Hilbert modular forms. This is because there is no difference, if the narrow class group is trivial. We will show in the next section that there is no good Hecke theory on the space of classical Hilbert modular forms, unless the narrow class number is* 1*. This is one of the main reasons one switches to more complicated Hilbert modular forms.*

Some authors refer to Hilbert modular forms as adelic Hilbert modular forms*, this is because one can define Hilbert modular forms as functions from* $\mathrm{GL}_2(\mathbb{A}_K)$ *to* $\mathbb{C}$ *satisfying certain modularity conditions. For more details, see [32, Section 2].*

Lemma 3.1.7. *If* $\mathcal{M}_k(\mathfrak{N}, \mathcal{E}) \neq 0$*, then either* $k = (0, 0, ..., 0)$ *or all* k_i *are strictly positive.*

Proof. See [37, Lemma 6.3]. □

Theorem 3.1.8. *Let* k *be a weight vector,* $\mathfrak{N}$ *a level and* $\mathcal{E}$ *a character mod* $\mathfrak{N}$*. Then the space* $\mathcal{M}_k(\mathfrak{N}, \mathcal{E})$ *is finite dimensional.*

Proof. See [13, Theorem I.6.1]. □

It is easy to see that the set of classical Hilbert modular forms of given level Γ and arbitrary weight and character admits the structure of a graded algebra. More precisely, if $f \in \mathcal{M}_{k_1}(\Gamma, \mathcal{E}_1)$ and $g \in M_{k_2}(\Gamma, \mathcal{E}_2)$ are classical Hilbert modular forms with the same level, then $f \cdot g$ is a classical Hilbert modular form of weight $k_1 + k_2$, level $\mathfrak{N}$ and character $\mathcal{E}_1 \cdot \mathcal{E}_2$. Moreover, this grading extends to the set of Hilbert modular forms of given level $\mathfrak{N}$. We will denote the graded algebra of classical Hilbert modular forms of level Γ by $\mathcal{M}_\star^c(\Gamma, \star)$, and the graded algebra of Hilbert modular forms of level $\mathfrak{N}$

by $\mathcal{M}_\star(\Gamma, \star)$. We will denote the graded algebra of Hilbert modular forms of parallel weight and level $\mathfrak{N}$ by $\mathcal{M}_{\underline{\star}}(\mathfrak{N}, \star)$. Under this notation we have

$$\mathcal{M}_\star(\mathfrak{N}, \star) = \bigoplus_{k \in \mathbb{Z}^n} \mathcal{M}_k(\mathfrak{N}, \star) \text{ and}$$

$$\mathcal{M}_{\underline{\star}}(\mathfrak{N}, \star) = \bigoplus_{k \in \mathbb{Z}} \mathcal{M}_{\underline{k}}(\mathfrak{N}, \star).$$

3.2 Hecke Operators

In this section, we introduce Hecke operators on the space of Hilbert modular forms. They were first introduced by Erich Hecke, but the topic remained relatively unexplored until the development of complex manifolds. We follow Shimura's *Special values of certain zeta functions*, cf [32, Section 2].

In the next section, we will introduce the q-expansion of a Hilbert modular form and show how one can see a Hecke operator as a linear operator on the q-expansion of a Hilbert modular form. In fact, after the next section we will identify a Hilbert modular form with its q-expansion, so for the purpose of this part of the thesis, one could take the Hecke operators on the q-expansions as the definition of a Hecke operator and skip this section. However, we include this section for the sake of completeness and to highlight the similarities between Hilbert modular forms and classical modular forms.

The fractional ideal

$$\delta^{-1} := \{x \in K \mid \operatorname{tr}(x\mathcal{O}_K) \subset \mathcal{O}\}$$

is called the *Dedekind's complementary module* or the *inverse different*. Its inverse

$$\delta := (\delta^{-1})^{-1}$$

is called the *different of* K. Since $\mathcal{O}_K \subset \delta^{-1}$ the fractional ideal δ is in fact an integral ideal of K. Let $\mathfrak{N}$ be an integral ideal of K. We define subsets $W_P(\mathfrak{N}) \subset Y_\mathfrak{p}(\mathfrak{N}) \subset \mathrm{GL}_2(K_\mathfrak{p})$ and $W(\mathfrak{N}) \subset Y(\mathfrak{N}) \subset \mathrm{GL}_2(\mathbb{A}_K)^+$, respectively, by

$$Y_\mathfrak{p}(\mathfrak{N}) := \left\{ y = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \begin{pmatrix} \mathcal{O}_\mathfrak{p} & \delta^{-1}\mathcal{O}_\mathfrak{p} \\ \mathfrak{N}\delta\mathcal{O}_\mathfrak{p} & \mathcal{O}_\mathfrak{p} \end{pmatrix} \;\middle|\; \det(y) \in K_\mathfrak{p}^\times \text{ and } a\mathcal{O}_\mathfrak{p} + \mathfrak{N} = 1 \right\},$$

$$W_\mathfrak{p}(\mathfrak{N}) := \left\{ w = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \begin{pmatrix} \mathcal{O}_\mathfrak{p} & \delta^{-1}\mathcal{O}_\mathfrak{p} \\ \mathfrak{N}\delta\mathcal{O}_\mathfrak{p} & \mathcal{O}_\mathfrak{p} \end{pmatrix} \;\middle|\; \det(w) \in \mathcal{O}_\mathfrak{p}^\times \text{ and } a\mathcal{O}_\mathfrak{p} + \mathfrak{N} = 1 \right\},$$

$$Y(\mathfrak{N}) := \mathrm{GL}_2(\mathbb{A}_K) \cap \left(\mathrm{GL}_2^+(\mathbb{R})^n \times \prod_{\mathfrak{p} < \infty} Y_\mathfrak{p}(\mathfrak{N}) \right) \text{ and}$$

$$W(\mathfrak{N}) := \mathrm{GL}_2^+(\mathbb{R})^n \times \prod_{\mathfrak{p}<\infty} W_{\mathfrak{p}}(\mathfrak{N}).$$

Note that $W_p(\mathfrak{N})$ and $W(\mathfrak{N})$ are in fact subgroups of $\mathrm{GL}_2(K_{\mathfrak{p}})$ and $\mathrm{GL}_2(\mathbb{A}_K)$, respectively, while $Y_{\mathfrak{p}}(\mathfrak{N})$ and $Y(\mathfrak{N})$ are only semi-groups.

Given a character $\mathcal{E}$ mod $\mathfrak{N}$, we define a character $\mathcal{E}_Y$ on $Y(\mathfrak{N})$ by

$$\mathcal{E}_Y : Y(\mathfrak{N}) \to \mathbb{C} : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \mathcal{E}_f(d_{\mathfrak{N}})$$

where $d_{\mathfrak{N}}$ denotes the $\mathfrak{N}$-part of d.

Consider for each of the idèles $\mathfrak{t}_\lambda$ an element x_λ in $\mathrm{GL}_2(\mathbb{A}_K)$ as follows

$$x_\lambda = \begin{pmatrix} 1 & 0 \\ 0 & \mathfrak{t}_\lambda \end{pmatrix}.$$

If $\mathfrak{m}$ is an integral ideal of K, then there exists a $y \in Y(\mathfrak{N})$ such that $\mathfrak{m} = \det(y)$. Moreover, for each λ there exists an element α_λ of $x_\lambda Y x_\mu^{-1} \cap \mathrm{GL}_2(K)$ such that

$$W(\mathfrak{N}) y W(\mathfrak{N}) = W(\mathfrak{N})(x_\lambda^{-1}\alpha_\lambda x_\mu) W(\mathfrak{N}),$$

where μ is the index such that $[\mathfrak{m}\mathfrak{t}_\lambda] = [\mathfrak{t}_\mu]$ in the narrow class group of K. By abuse of notation we denote this as

$$\alpha_{[\mathfrak{t}_\lambda]} \in x_{[\mathfrak{t}_\lambda]} Y x_{[\mathfrak{t}_\lambda/\mathfrak{m}]}^{-1} \bigcap \mathrm{GL}_2(K),$$

i.e. for any fractional ideal $\mathfrak{a}$ the subscript $[\mathfrak{a}]$ is the subscript λ such that $[\mathfrak{a}] = [\mathfrak{t}_\lambda]$ in the narrow class group of K.

Since $\alpha_\lambda \in x_\lambda Y(\mathfrak{N}) x_\mu^{-1} \cap \mathrm{GL}_2(K)$, we have a disjoint coset decomposition of the double coset

$$\Gamma_0(\mathfrak{t}_\lambda, \mathfrak{N}) \alpha_\lambda \Gamma_0(\mathfrak{t}_\mu, \mathfrak{N}) = \bigsqcup_{j=1}^{n_{\lambda,\mu}} \Gamma_0(\mathfrak{t}_\lambda, \mathfrak{N}) \alpha_{\lambda,j,\mu}$$

with finitely many $\alpha_{\lambda,j,\mu}$. Given such a decomposition we can define a morphism $T_{\lambda,\alpha_\lambda,\mu}$ by

$$T_{\lambda,\alpha_\lambda,\mu} : \mathcal{M}_k\big(\Gamma_0(\mathfrak{t}_\lambda, \mathfrak{N}), \mathcal{E}\big) \to \mathcal{M}_k\big(\Gamma_0(\mathfrak{t}_\mu, \mathfrak{N}), \mathcal{E}\big) :$$

$$f_\lambda \mapsto \sum_{j=1}^{n_{\lambda,\mu}} \mathcal{E}_Y(x_\lambda^{-1}\alpha_{\lambda,j,\mu} x_\mu)(f_\lambda|_k \alpha_{\lambda,j,\mu}),$$

where we define $f_\lambda|_k\alpha := \frac{\det \alpha^{k/2}}{(cz+d)^k} f(\alpha \cdot z)$ for $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

The fact that the classical Hilbert modular form $T_{\lambda,\alpha_\lambda,\mu}(f_\lambda)$ has a different level than f_λ itself is the key obstruction to a good Hecke theory on classical Hilbert modular forms. This obstruction is (one of) the reason(s) why we are working with Hilbert modular forms rather than classical Hilbert modular forms.

Given y in Y with $\det(y) = \mathfrak{m}$ as above, take elements $\alpha_1, ..., \alpha_{h^+}$ and decompositions

$$\Gamma_0\big([\mathfrak{t}_\mu/\mathfrak{m}], \mathfrak{N}\big)\alpha_{[\mathfrak{t}_\mu/\mathfrak{m}]}\Gamma_0\big([\mathfrak{t}_\mu], \mathfrak{N}\big) = \bigsqcup_{j=1}^{n_{[\mathfrak{t}_\mu/\mathfrak{m}],[\mathfrak{t}_\mu]}} \Gamma_0\big([\mathfrak{t}_\mu/\mathfrak{m}], \mathfrak{N}\big)\alpha_{[\mathfrak{t}_\mu/\mathfrak{m}],j,[\mathfrak{t}_\mu]}$$

as above. Then we can define an operator T_y on $\mathcal{M}_k(\mathfrak{N}, \mathcal{E})$ by

$$\begin{aligned} T_y &: \mathcal{M}_k(\mathfrak{N}, \mathcal{E}) \to \mathcal{M}_k(\mathfrak{N}, \mathcal{E}) : \\ &(f_1, ..., f_{h^+}) \mapsto \Big(T_{[\mathfrak{t}_\mu/\mathfrak{m}],\alpha_{[\mathfrak{t}_\mu/\mathfrak{m}]},[\mathfrak{t}_\mu]}(f_{[\mathfrak{t}_\mu/\mathfrak{m}]})\Big)_{\mu=1}^{h^+} \\ &= \left(\sum_{j=1}^{n_{[\mathfrak{t}_\mu/\mathfrak{m}],[\mathfrak{t}_\mu]}} \mathcal{E}_Y\big(x_{[\mathfrak{t}_\mu/\mathfrak{m}]}^{-1}\alpha_{[\mathfrak{t}_\mu/\mathfrak{m}],j,[\mathfrak{t}_\mu]}x_{[\mathfrak{t}_\mu]}\big)\big(f_{[\mathfrak{t}_\mu/\mathfrak{m}]}\big|_k\alpha_{[\mathfrak{t}_\mu/\mathfrak{m}],j,[\mathfrak{t}_\mu]}\big)\right)_{\mu=1}^{h^+}. \end{aligned}$$

Finally, we are able to define the Hecke operator $T_\mathfrak{m}$ of weight k for an integral ideal $\mathfrak{m}$. Recall that for a weight vector k in $\mathbb{Z}^n$ we write k_0 for the integer $\max_i\{k_i\}$ and $\underline{k}_0$ for the parallel weight vector $(k_0, ..., k_0)$.

Definition 3.2.1. *Let $\mathfrak{m}$ be an integral ideal of K. The* Hecke operator $T_\mathfrak{m}$ *on the space of Hilbert modular forms of weight k, level $\mathfrak{N}$ and character $\mathcal{E}$ is defined as*

$$T_\mathfrak{m} : \mathcal{M}_k(\mathfrak{N}, \mathcal{E}) \to \mathcal{M}_k(\mathfrak{N}, \mathcal{E}) : f \mapsto \mathrm{N}(\mathfrak{m})^{(k_0-2)/2} \cdot \sum_{\substack{y \in Y \\ \det(y) = \mathfrak{m}}} T_y(f).$$

The Hecke algebra $\mathbb{T}_k(\mathfrak{N}, \mathcal{E})$ *is the $\mathbb{C}$-algebra generated by the operators $T_\mathfrak{m}(f)$ for all integral ideals $\mathfrak{m}$ of K. It is a sub $\mathbb{C}$-algebra of the endomorphism ring of $\mathcal{M}_k(\mathfrak{N}, \mathcal{E})$.*

Lemma 3.2.2. *The Hecke algebra $\mathbb{T}_k(\mathfrak{N}, \mathcal{E})$ is finite dimensional as a $\mathbb{C}$-vector space. Moreover, as a $\mathbb{C}$-algebra, $\mathbb{T}_k(\mathfrak{N}, \mathcal{E})$ is finitely generated by elements of the form $T_\mathfrak{p}$ with $\mathfrak{p}$ prime.*

Proof. By Theorem 3.1.8 the space of Hilbert modular forms is finite dimensional, so we can choose a basis $\beta = \{\beta_1, ..., \beta_\ell\}$ of $\mathcal{M}_k(\mathfrak{N}, \mathcal{E})$. The choice of the basis induces an injective morphism of $\mathbb{T}_k(\mathfrak{N})$ into the space of $\ell \times \ell$-matrices with coefficients in $\mathbb{C}$. Hence, $\mathbb{T}_k(\mathfrak{N})$ is a finite dimensional $\mathbb{C}$-vector space.

By [32, Section 2] we have

$$T_{\mathfrak{a}\mathfrak{b}} = T_{\mathfrak{a}} \cdot T_{\mathfrak{b}} \qquad \text{if } \mathfrak{a} + \mathfrak{b} = \mathcal{O}_K \text{ and}$$

$$T_{\mathfrak{p}^r} = \begin{cases} T_{\mathfrak{p}} \cdot T_{\mathfrak{p}^r - 1} & \text{if } \mathfrak{p} | \mathfrak{N} \\ T_{\mathfrak{p}} \cdot T_{\mathfrak{p}^r - 1} - \mathcal{E}(\mathfrak{p}) \mathrm{N}(\mathfrak{p})^{k_0 - 1}\, T_{\mathfrak{p}^{r-2}} & \text{else.} \end{cases}$$

This proves the second claim of the lemma. □

Proposition 3.2.3. *The eigenvalues of $T_{\mathfrak{p}}$ are algebraic numbers. Moreover, if the weight vector k is parallel, then the eigenvalues of $T_{\mathfrak{p}}$ are algebraic integers.*

Proof. See [32, Proposition 2.2]. □

Definition 3.2.4. *Let f be a Hilbert modular form of weight k, level $\mathfrak{N}$ and character $\mathcal{E}$. We say that f is an* eigenform *if f is an eigenvector for all operators $T_{\mathfrak{m}}$ in $\mathbb{T}_k(\mathfrak{N}, \mathcal{E})$.*

3.3 Geometric and Adelic q-Expansions

In this section, we explain how to obtain a Fourier expansion from a classical Hilbert modular form. We will use this Fourier expansion to define both the geometric q-expansion and the adelic q-expansion of a Hilbert modular form. Then we will introduce the graded algebra of formal adelic power series and show how Hilbert modular forms form subalgebras by means of the adelic q-expansion. Finally, we will define the action of the Hecke operators on the adelic q-expansion.

Geometric q-Expansions

Let $f = (f_1, ..., f_{h^+}) \in \mathcal{M}_k(\mathfrak{N}, \mathcal{E})$ be a Hilbert modular form. Let a be an element of $\mathfrak{t}_\lambda^{-1}$ and $\gamma_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$. Then $\gamma_a \in \Gamma_0(\mathfrak{t}_\lambda, \mathfrak{N})$, so we obtain

$$f_\lambda(\gamma_a \cdot z) = \mathcal{E}_f(1) \cdot \frac{(0+1)^k}{1^{k/2}} f_\lambda(z)$$

$$= f_\lambda(z).$$

Moreover, $\gamma_a \cdot z = z + a$, hence

$$f_\lambda(z + a) = f_\lambda(z).$$

So f_λ is a multivariate periodic function with respect to the lattice $\mathfrak{t}_\lambda^{-1}$. In particular, we obtain the following proposition.

Proposition 3.3.1. *Let $f = (f_1, ..., f_{h^+}) \in \mathcal{M}_k(\mathfrak{N}, \mathcal{E})$ be a Hilbert modular form. Then each $f_\lambda(z)$ admits a Fourier expansion of the form*

$$f_\lambda = a_{\lambda,0} + \sum_{\xi \in \mathfrak{t}_\lambda} a_{\lambda,\xi}\, e^{2\pi i tr(\xi z)}.$$

Moreover, $a_{\lambda,\varepsilon\cdot\xi} = \varepsilon^{k/2} \cdot a_{\lambda,\xi}$ for all totally positive units ε.

Proof. Since $f_\lambda(z + a) = f_\lambda(a)$ for all $a \in \mathfrak{t}_\lambda^{-1}$, Lemma 4.1 in [13] yields a Fourier expansion over the dual lattice of $\mathfrak{t}_\lambda^{-1}$, i.e. a power series

$$f_\lambda = a_{\lambda,0} + \sum_{\xi \in \mathfrak{t}_\lambda} a_{\lambda,\xi}\, e^{2\pi i \mathrm{tr}(\xi z)}$$

indexed by elements of the fractional ideal $\mathfrak{t}_\lambda$.

Let ε be a totally positive unit in $\mathcal{O}_K$. Then $\begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(\mathfrak{t}_\lambda, \mathfrak{N})$. So by the modularity condition we obtain

$$f(\varepsilon \cdot z) = \varepsilon^{-k/2} \cdot f(z).$$

Comparing the Fourier expansions of the left-hand side and the right-hand side of the equation yields

$$a_{\lambda,\xi} = \varepsilon^{-k/2} \cdot a_{\lambda,\varepsilon\cdot\xi}$$

proving the last claim of the proposition. □

Lemma 3.3.2 (Koecher's Principle)**.** *Let f be a Hilbert modular form. Then f is* holomorphic at the cusps *in the sense that $a_{\lambda,\xi} \neq 0$ implies that $\xi = 0$ or $\xi \gg 0$.*

Proof. Let ξ_0 be an element of $\mathfrak{t}_\lambda$ that is not totally positive and such that a_{λ,ξ_0} is non-zero. Without loss of generality, we assume $\xi_0^{(1)} < 0$. By Dirichlet's unit theorem there exists ε, a totally positive unit such that $\varepsilon^{(1)} > 1$ and $\varepsilon^{(j)} < 1$ for all $j > 1$ and such that $\mathrm{tr}(\varepsilon \cdot \xi_0) < 0$. We now evaluate the above power series at $\underline{i}$

$$f_\lambda(\underline{i}) = a_{\lambda,0} + \sum_{\xi \in \mathfrak{t}_\lambda} a_{\lambda,\xi}\, e^{2\pi i \mathrm{tr}(\xi \underline{i})}$$

and consider the terms indexed by $\xi_0\varepsilon^m$ for positive integers m

$$a_{\lambda,\xi_0\varepsilon^m}\, e^{2\pi i \mathrm{tr}(\xi_0\varepsilon^m \underline{i})} = \varepsilon^{-km/2} a_{\lambda,\xi_0}\, e^{2\pi |\mathrm{tr}(\xi_0\varepsilon^m)|}.$$

The exponential term ensures that the right-hand side approaches infinity as m grows. In particular, the Fourier expansion of f_λ cannot converge unless a_{λ,ξ_0} vanishes.

□

Definition 3.3.3. *Let $f \in \mathcal{M}_k(\mathfrak{N}, \mathcal{E})$ be a Hilbert modular form. The h^+-tuple of Fourier expansions of each f_λ is called the* geometric q-expansion of f. *We denote it by*

$$f = \left(a_{\lambda,0} + \sum_{\xi \in \mathfrak{t}_\lambda^+} a_{\lambda,\xi}\, q^\xi \right)_{[\mathfrak{t}_\lambda] \in \mathrm{Cl}^+}$$

with $q^\xi = e^{2\pi i \mathrm{tr}(\xi z)}$.

Definition 3.3.4. *We say that $f \in \mathcal{M}_k(\mathfrak{N}, \mathcal{E})$ is* a cuspidal Hilbert modular form *if the constant terms $a_{\lambda,0}$ of the Fourier expansion of $f_\lambda(\gamma z)$ are zero for all $\gamma \in \mathrm{GL}_2^+(\mathcal{O}_K)$. We denote the space of cuspidal Hilbert modular forms by $\mathcal{S}_k(\mathfrak{N}, \mathcal{E})$.*

Proposition 3.3.5. *Let k be a non-parallel weight vector, then*

$$\mathcal{S}_k(\mathfrak{N}, \mathcal{E}) = \mathcal{M}_k(\mathfrak{N}, \mathcal{E}).$$

Proof. Suppose that $f \in \mathcal{M}_k(\mathfrak{N}, \mathcal{E})$ is non-cuspidal. Without loss of generality f is non-vanishing at ∞, i.e. $a_{\lambda,0} \neq 0$ for some λ. From Proposition 3.3.1 we obtain that

$$a_{\lambda,0} = \varepsilon^{k/2} \cdot a_{\lambda,0}$$

for all $\varepsilon \in \mathcal{O}_K^{\times,+}$. Since $a_{\lambda,0}$ is non-zero we find

$$\varepsilon^{k/2} = 1$$

for all totally positive units ε. Let $\mathcal{L}$ be the image of $\mathcal{O}_K^{\times,+}$ in $\mathbb{R}^n$ under the logarithmic embedding, i.e. $\mathcal{L}$ is the image of the mapping

$$\log : \mathcal{O}_K^{\times,+} \to \mathbb{R}^n : \varepsilon \mapsto \left(\log \varepsilon^{(1)}, ..., \log \varepsilon^{(n)} \right).$$

If k is not a parallel weight vector, then $\mathcal{L}$ is contained in the $n-2$-dimensional sub space of solutions of the linear system given by $X_1 + ... + X_n = 0$ and $k_1 X + ... + k_n X_n = 0$. This is in contradiction with Dirichlet's unit theorem which implies that $\mathcal{L}$ is a free $\mathbb{Z}$-module of rank $n-1$. □

Lemma 3.3.6 (Sturm bound for geometric q-expansion)**.** *Let k be a weight vector, $\mathfrak{N}$ an integral ideal and $\mathcal{E}$ a character mod $\mathfrak{N}$. There exists an element $b \in O_K^+$ with $b \ll k_0 \mathrm{N}(\mathfrak{N})^3$ such that*

$$a_{\lambda,\xi}(f) = 0 \text{ for all } \xi \ll b \text{ if and only if } f_\lambda = 0$$

for all Hilbert modular forms $f = (f_1, ..., f_{h^+})$ in $\mathcal{M}_k(\mathfrak{N}, \mathcal{E})$.

Proof. See [36, Theorem 1]. □

Adelic q-Expansion

Let $\mathfrak{b}$ be a non trivial integral ideal of K and f a Hilbert modular form of weight k. Let ξ be a totally positive element of $\mathcal{O}_K$ such that $\mathfrak{b} = \xi\,\mathfrak{t}_\lambda^{-1}$. Then

$$a_\mathfrak{b} := a_{\lambda,\xi}\,\xi^{(\underline{k}_0-k)/2}$$

does not depend on the choice of ξ. Indeed, if ξ' is another totally positive generator of $\mathfrak{b}\,\mathfrak{t}_\lambda$, then there exists a totally positive unit ε such that $\xi' = \varepsilon\cdot\xi$, hence

$$\begin{aligned} a_{\lambda,\varepsilon\xi}\cdot(\varepsilon\,\xi)^{(\underline{k}_0-k)/2} &= \varepsilon^{k/2} a_{\lambda,\xi}\,(\varepsilon\,\xi)^{(\underline{k}_0-k)/2} \\ &= a_{\lambda,\xi}\,\varepsilon^{\underline{k}_0}\,\xi^{(\underline{k}_0-k)/2} \\ &= a_{\lambda,\xi}\,\mathrm{N}(\varepsilon)^{k_0}\xi^{(\underline{k}_0-k)/2} \\ &= a_{\lambda,\xi}\,\xi^{(\underline{k}_0-k)/2}. \end{aligned}$$

Moreover, we define

$$a_{(0)} := \big(a_{(0),[\mathfrak{t}_\lambda]}\big)_{[\mathfrak{t}_\lambda]\in\mathrm{Cl}^+} = \big(a_{\lambda,0}\big)_{[\mathfrak{t}_\lambda]\in\mathrm{Cl}^+}$$

where the index is over the narrow class group of K. If the weight k is parallel, then the above formula simplifies to

$$a_\mathfrak{b} = a_{\lambda,\xi}.$$

Definition 3.3.7. *Let f be a Hilbert modular form. The formal power series*

$$f \sim a_{(0)} + \sum_{0\neq\mathfrak{b}\lhd\mathcal{O}_K} a_\mathfrak{b} q^\mathfrak{b},$$

with all $a_\star$ defined as above, is called the adelic q-expansion of f.

Definition 3.3.8. *Let f be a Hilbert modular form. We say that f is normalised if its adelic q-expansion is normalised, i.e.*

$$a_{\mathcal{O}_K}(f) = 1.$$

Power Series

We define the $\mathbb{C}$-vector space of *adelic power series over* $\mathbb{C}$ as the formal power series with coefficients indexed by the non trivial ideals of $\mathcal{O}_K$ and with constant coefficient

$a_{(0)}$ in $\mathbb{C}^{\mathrm{Cl}^+}$. Formally, we write

$$\mathbb{C}_{\mathbb{A}}[\![q]\!] := \mathbb{C}^{\mathrm{Cl}^+} \oplus \prod_{0\neq\mathfrak{b}\lhd\mathcal{O}_K} \mathbb{C}\cdot q^{\mathfrak{b}}$$

$$= \Big\{ \big(a_{(0),[\mathfrak{t}_\lambda]}\big)_{[\mathfrak{t}_\lambda]\in\mathrm{Cl}^+} + \sum_{0\neq\mathfrak{b}\lhd\mathcal{O}_K} a_{\mathfrak{b}} q^{\mathfrak{b}} \;\Big|\; \text{with all } a_\star \in \mathbb{C} \Big\}.$$

Let k be a weight vector and $(\mathfrak{t}_\lambda)_{\mathrm{Cl}^+}$ a full set of representatives of the narrow class group of K. We define the $\mathbb{C}$-vector space of *geometric power series of weight k over $\mathbb{C}$*, as the $\mathbb{C}$-vector space of h^+-tuples of formal power series where the coefficients of the power series at λ are indexed by totally positive elements in $\mathfrak{t}_\lambda$. Formally, we write

$$\mathbb{C}_{k,(\mathfrak{t}_\lambda)}[\![q]\!] := \Big\{ \Big(a_{\lambda,0} + \sum_{\xi\in\mathfrak{t}_\lambda^+} a_{\lambda,\xi} q^{\xi}\Big)_{\mathrm{Cl}^+} \;\Big|\; a_{\lambda,\varepsilon\xi} = \varepsilon^{k/2} a_{\lambda,\xi} \text{ for all } \varepsilon \in \mathcal{O}_K^{\times,+} \Big\},$$

where all $a_\star$ lie in $\mathbb{C}$. Note that the space of adelic power series does not depend on the choice of representatives. The space of geometric power series over $\mathbb{C}$ does depend on the choice of representatives $(\mathfrak{t}_\lambda)$. However, we will show the different spaces are isomorphic. Note that $\bigoplus_{k\in\mathbb{Z}^n_{\geq 0}} \mathbb{C}_{k,(\mathfrak{t}_\lambda)}[\![q]\!]$ has a natural structure of a graded ring by componentwise multiplication. The following proposition will allow us to view the adelic power series as a graded ring.

Proposition 3.3.9. *The choice of representatives $\mathfrak{t}_1, ..., \mathfrak{t}_{h^+}$ induces a bijection $\Psi_{k,(\mathfrak{t}_\lambda)}$ between geometric power series and adelic power series.*

Proof. This is precisely the map given in the construction of the adelic q-expansion of a Hilbert modular form, i.e.

$$\Psi_{k,(\mathfrak{t}_\lambda)} : \mathbb{C}_{k,(\mathfrak{t}_\lambda)}[\![q]\!] \to \mathbb{C}_{\mathbb{A}}[\![q]\!] :$$

$$\Big(a_{\lambda,0} + \sum_{\xi\in\mathfrak{t}_\lambda^+} a_{\lambda,\xi} q^{\xi}\Big)_{\mathrm{Cl}^+} \mapsto (a_{\lambda,0})_{\mathrm{Cl}^+} + \sum_{0\neq\mathfrak{b}\lhd\mathcal{O}_K} a_{\mathfrak{b}} q^{\mathfrak{b}}$$

$$\text{with } a_{\mathfrak{b}} = a_{\lambda,\xi}\, \xi^{(\underline{k}_0 - k)/2} \text{ such that } \mathfrak{b} = \xi\mathfrak{t}_\lambda^{-1}.$$

Its inverse is given by

$$\Phi_{k,(\mathfrak{t}_\lambda)} : \mathbb{C}_{\mathbb{A}}[\![q]\!] \to \mathbb{C}_{k,(\mathfrak{t}_\lambda)}[\![q]\!] :$$

$$(a_{(0),[\mathfrak{t}_\lambda]})_{\mathrm{Cl}^+} + \sum_{0\neq\mathfrak{b}\lhd\mathcal{O}_K} a_{\mathfrak{b}} q^{\mathfrak{b}} \mapsto \Big(a_{(0),[\mathfrak{t}_\lambda]} + \sum_{\xi\in\mathfrak{t}_\lambda^+} a_{\lambda,\xi} q^{\xi}\Big)_{\mathrm{Cl}^+}$$

$$\text{with } a_{\lambda,\xi} = a_{\xi\,\mathfrak{t}_\lambda^{-1}} \cdot \xi^{(k-\underline{k}_0)/2}.$$

Note that $a_{\xi\mathfrak{t}_\lambda^{-1}}$ is defined as 0 when $\xi\mathfrak{t}_\lambda^{-1}$ is not an integral ideal.

□

Definition 3.3.10. *The graded* $\mathbb{C}$*-algebra of* adelic power series *is the* $\mathbb{C}$*-vector space*

$$\mathbb{C}[\![q]\!]^K := \bigoplus_{k\in\mathbb{Z}^n_{\geq 0}} \mathbb{C}_{\mathbb{A}}[\![q]\!]$$

equipped with the graded $\mathbb{C}$*-algebra structure induced by the isomorphisms* $\Psi_{k,(\mathfrak{t}_\lambda)}$ *and* $\Phi_{k,(\mathfrak{t}_\lambda)}$.

Theorem 3.3.11. *The graded* $\mathbb{C}$*-algebra* $\mathbb{C}[\![q]\!]^K$ *is independent of the choice of representatives* $(\mathfrak{t}_\lambda)_{\mathrm{Cl}^+}$.

Proof. Let $(\mathfrak{t}_\lambda)_{\mathrm{Cl}^+}$ and $(\mathfrak{t}'_\lambda)_{\mathrm{Cl}^+}$ be two choices of representatives of the narrow class group of K and let $(\xi_\lambda)_{\mathrm{Cl}^+}$ be totally positive elements of K such that

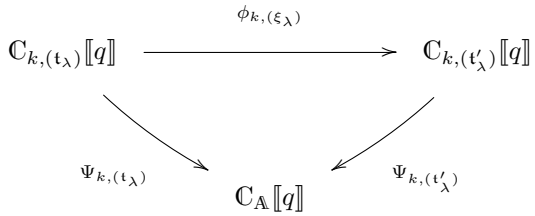
$$\xi_\lambda\mathfrak{t}_\lambda = \mathfrak{t}'_\lambda \text{ for all } [\mathfrak{t}_\lambda] \text{ in } \mathrm{Cl}^+.$$

We define an isomorphism of $\mathbb{C}$-vector spaces as follows

$$\phi_{k,(\xi_\lambda)} : \mathbb{C}_{k,(\mathfrak{t}_\lambda)}[\![q]\!] \to \mathbb{C}_{k,(\mathfrak{t}'_\lambda)}[\![q]\!] :$$

$$\Big(\sum_{\xi'\in\mathfrak{t}_\lambda^+} a_{\lambda,\xi'}q^{\xi'}\Big)_{\mathrm{Cl}^+} \mapsto \Big(\sum_{\xi'\in\mathfrak{t}_\lambda^+} a_{\lambda,\xi'}\xi_\lambda^{(k-\underline{k}_0)/2}q^{\xi_\lambda\xi'}\Big)_{\mathrm{Cl}^+}.$$

By construction of $\phi_{k,(\xi_\lambda)}$ the following diagram commutes.



Finally, one checks that the isomorphism $\phi_{k,(\xi_\lambda)}$ induces an isomorphism of graded $\mathbb{C}$-algebras. □

Corollary 3.3.12. *The adelic* q*-expansion induces an injective morphism of graded* $\mathbb{C}$*-algebras from* $\mathcal{M}_\star(\mathfrak{N},\star)$ *to* $\mathbb{C}[\![q]\!]^K$. *Moreover, the image of* $\mathcal{M}_\star(\mathfrak{N},\star)$ *in* $\mathbb{C}[\![q]\!]^K$ *is independent of the choice of representatives* $(\mathfrak{t}_\lambda)_{\mathrm{Cl}^+}$.

Remark 3.3.13. *Corollary 3.3.12 can be summarised by the following slogan:* "The product of adelic q-expansions is the adelic q-expansion of the product". *In fact the multiplication of adelic q-power series is precisely defined such that this slogan is true.*

Corollary 3.3.14 (Sturm bound for adelic q-expansion)**.** *Let $\mathfrak{N}$ be an integral ideal, $\mathcal{E}$ a character mod $\mathfrak{N}$ and weight k. There exists a positive integer $B \leq k_0 \mathrm{N}(\mathfrak{N})^3$ such that*

$$a_{\mathfrak{b}}(f) = 0 \text{ for all } \mathrm{N}(\mathfrak{b}) \leq B \text{ if and only if } f = 0$$

for all Hilbert modular forms f in $\mathcal{M}_k(\mathfrak{N}, \mathcal{E})$.

Proof. This follows from Proposition 3.3.9 and Lemma 3.3.6. □

Definition 3.3.15. *We define the $\mathbb{C}$-vector space of* fractional Hilbert modular forms of weight k, level $\mathfrak{N}$ and character $\mathcal{E}$ *as follows:*

$$\mathcal{M}_k^f(\mathfrak{N}, \mathcal{E}) := \left\{ \frac{f}{g} \;\middle|\; \begin{array}{c} k_1 - k_2 = k,\ \mathcal{E}_1/\mathcal{E}_2 = \mathcal{E},\ f \in \mathcal{M}_{k_1}(\mathfrak{N}, \mathcal{E}_1), \\ 0 \neq g \in \mathcal{M}_{k_2}(\mathfrak{N}, \mathcal{E}_2) \text{ and } g|f \text{ in } \mathbb{C}[\![q]\!]^K \end{array} \right\},$$

where we consider f/g as a meromorphic function on $\mathcal{H}^n$.

Note that the condition $g|f$ in $\mathbb{C}[\![q]\!]^K$ means precisely that $\frac{f}{g}$ has a well defined adelic q-expansion in $\mathbb{C}[\![q]\!]^K$, i.e. the q-expansion is over integral ideals rather than fractional ideals. Moreover, the set of Hilbert modular forms can be characterised as the set of holomorphic fractional Hilbert modular forms.

Lemma 3.3.16. *Let f be a fractional Hilbert modular form. Then f^2 is a Hilbert modular form if and only if f is a Hilbert modular form.*

Proof. This follows form the fact that for each $\lambda = 1, ..., h^+$ the meromorphic function f_λ is holomorphic if and only if f_λ^2 is holomorphic. □

Hecke Operators on Adelic Power Series

Let k be a weight vector, $\mathfrak{N}$ and integral ideal and $\mathcal{E}$ a character mod $\mathfrak{N}$. We extend the action of the Hecke algebra $\mathbb{T}_k(\mathfrak{N}, \mathcal{E})$ to the k-part of the graded algebra $\mathbb{C}[\![q]\!]^K$ by

$$a_{(0),[\mathfrak{t}_\lambda]}\big(T_{\mathfrak{p}}(f)\big) = a_{(0),[\mathfrak{t}_\lambda \mathfrak{p}]}(f) + \mathcal{E}(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{(k_0-1)} a_{(0),[\mathfrak{t}_\lambda/\mathfrak{p}]}(f)$$

$$a_{\mathfrak{m}}\big(T_{\mathfrak{p}}(f)\big) = a_{\mathfrak{m}\mathfrak{p}}(f) + \mathcal{E}(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{(k_0-1)} a_{\mathfrak{m}/\mathfrak{p}}(f)$$

for prime ideals $\mathfrak{p}$ and extend to all integral ideals $\mathfrak{m}$ by

$$T_{\mathfrak{ab}} = T_{\mathfrak{a}} \cdot T_{\mathfrak{b}} \qquad \text{if } \mathfrak{a}+\mathfrak{b} = \mathcal{O}_K \text{ and}$$

$$T_{\mathfrak{p}^r} = \begin{cases} T_{\mathfrak{p}} \cdot T_{\mathfrak{p}^{r-1}} & \text{if } \mathfrak{p} | \mathfrak{N} \\ T_{\mathfrak{p}} \cdot T_{\mathfrak{p}^{r-1}} - \mathcal{E}(\mathfrak{p})\mathrm{N}(\mathfrak{p})^{k_0-1}\, T_{\mathfrak{p}^{r-2}} & \text{else.} \end{cases}$$

One can check that under these definitions we have

$$a_{(0),[\mathfrak{t}_\lambda]}\big(T_{\mathfrak{a}}(f)\big) = \sum_{\mathfrak{a}\subset\mathfrak{b}} \mathcal{E}(\mathfrak{b})\mathrm{N}(\mathfrak{b})^{k_0-1} a_{(0),[\mathfrak{t}_\lambda \mathfrak{a}/\mathfrak{b}^2]}(f),$$

$$a_{\mathfrak{m}}\big(T_{\mathfrak{a}}(f)\big) = \sum_{\mathfrak{m}+\mathfrak{a}\subset\mathfrak{b}} \mathcal{E}(\mathfrak{b})\mathrm{N}(\mathfrak{b})^{k_0-1} a_{\mathfrak{m}\mathfrak{a}/\mathfrak{b}^2}(f)$$

for all integral ideals $\mathfrak{a}$ in K.

Lemma 3.3.17. *The Hecke operators on power series are well defined, that is the following diagram commutes.*

$$\begin{array}{ccc} \mathcal{M}_k(\mathfrak{N},\mathcal{E}) & \xrightarrow{T_{\mathfrak{m}}} & \mathcal{M}_k(\mathfrak{N},\mathcal{E}) \\ \downarrow & & \downarrow \\ \mathbb{C}[\![q]\!]_k^K & \xrightarrow[T_{\mathfrak{m}}]{} & \mathbb{C}[\![q]\!]_k^K \end{array}$$

Proof. See [32, Section 2]. □

Corollary 3.3.18. *Let f be a normalised eigenform in $\mathcal{M}_k(\mathfrak{N},\mathcal{E})$. Then,*

$$T_{\mathfrak{m}}(f) = a_{\mathfrak{m}}(f) \cdot f$$

for all Hecke operators $T_{\mathfrak{m}}$ in $\mathbb{T}_k(\mathfrak{N})$.

For completeness and later use, we formally state the formula for multiplication in the graded ring $\mathbb{C}[\![q]\!]^K$.

Proposition 3.3.19. *Let f_1 and f_2 be power series in $\mathbb{C}[\![q]\!]^K$ of weight k_1 and k_2, respectively. Let $\mathfrak{m}$ be an integral ideal and ξ a totally positive generator of $\mathfrak{m}\mathfrak{t}_\lambda$ as*

above. Then we have the following

$$a_{(0)}(f_1 f_2) = a_{(0)}(f_1) \cdot a_{(0)}(f_2), \text{ (component-wise)}$$

$$\begin{aligned} a_{\mathfrak{m}}(f_1 f_2) = \xi^{m_{1+2}} \Big(& a_{(0),[\mathfrak{t}_\lambda]}(f_1) a_{\xi \mathfrak{t}_\lambda^{-1}}(f_2) \xi^{-m_2} \\ & + \sum_{0 \ll \nu \ll \xi} a_{\nu \mathfrak{t}_\lambda^{-1}}(f_1)\, a_{(\xi-\nu)\mathfrak{t}_\lambda^{-1}}(f_2)\, \nu^{-m_1} (\xi-\nu)^{-m_2} \\ & + a_{\xi \mathfrak{t}_\lambda^{-1}}(f_1) \xi^{-m_1} a_{(0),[\mathfrak{t}_\lambda]}(f_2) \Big) \end{aligned}$$

where we define

$$m_j := (\underline{k_j}_0 - k_j)/2 \quad \text{for } j \in \{1,2\},$$

$$m_{1+2} := \left(\underline{(k_1+k_2)}_0 - (k_1+k_2) \right)/2.$$

If all entries of $a_{(0)}(f_2)$ are invertible and $k_1 \gg k_2$, then

$$a_{(0)} \left(\frac{f_1}{f_2} \right) = \frac{a_{(0)}(f_1)}{a_{(0)}(f_2)}, \text{ (component-wise)}$$

$$\begin{aligned} a_{\mathfrak{m}} \left(\frac{f_1}{f_2} \right) = \frac{\xi^{m_{1-2}}}{a_{(0),[\mathfrak{t}_\lambda]}(f_2)} \Big(& a_{\xi \mathfrak{t}_\lambda^{-1}}(f_1) \xi^{-m_1} - a_{(0),[\mathfrak{t}_\lambda]} \left(\frac{f_1}{f_2} \right) a_{\xi \mathfrak{t}_\lambda^{-1}}(f_2) \xi^{-m_2} \\ & - \sum_{0 \ll \nu \ll \xi} a_{\nu \mathfrak{t}_\lambda^{-1}} \left(\frac{f_1}{f_2} \right) a_{(\xi-\nu)\mathfrak{t}_\lambda^{-1}}(f_2)\, \nu^{-m_{1-2}} (\xi-\nu)^{-m_2} \Big) \end{aligned}$$

where we define

$$m_{1-2} := \left(\underline{(k_1-k_2)}_0 - (k_1-k_2) \right)/2.$$

Proof. This follows from the definition of the multiplication on adelic power series. □

Truncated Adelic Power Series

Let B be a positive integer, then by the definition of multiplication of adelic power series (3.3.19), the following subgroup is an ideal of $\mathbb{C}[\![q]\!]^K$

$$(q^B) = \left\{ \sum_{\mathfrak{m} \lhd \mathcal{O}_K} a_{\mathfrak{m}} q^{\mathfrak{m}} \;\middle|\; a_{\mathfrak{m}} = 0 \text{ for all } \mathrm{N}(\mathfrak{m}) < B \right\}.$$

We call its quotient, $\mathbb{C}[\![q]\!]^K/(q^B)$, *the ring of adelic power series mod q^B*.

Definition 3.3.20. *Let k be a weight vector, $\mathfrak{N}$ an integral ideal of K and $\mathcal{E}$ a character mod $\mathfrak{N}$. The* Sturm bound of weight k, level $\mathfrak{N}$ and character $\mathcal{E}$ *is the smallest positive integer B such that the adelic q-expansion map followed by the natural projection*

$$\mathcal{M}_k(\mathfrak{N}, \mathcal{E}) \to \mathbb{C}[\![q]\!]^K/(q^B)$$

is an injective morphism of $\mathbb{C}$-vector spaces.

Recall that such a B exists by Corollary 3.3.14.

The following theorem is the principle that will allow us to verify that a computed adelic power series is in fact the adelic q-expansion of a Hilbert modular form.

Theorem 3.3.21. *Let k and k' be weight vectors, $\mathfrak{N}$ an integral ideal of K and $\mathcal{E}$ and $\mathcal{E}'$ characters mod $\mathfrak{N}$. Let E be a Hilbert modular form in $\mathcal{M}_{k'}(\mathfrak{N}, \mathcal{E}')$. Let B be the Sturm bound of weight $2k + 2k'$, level $\mathfrak{N}$ and character $\mathcal{E}^2\mathcal{E}'^2$. Let $\tilde{f}$ be the mod q^B-truncated adelic q-expansion of a fractional Hilbert modular form in $E^{-1}\mathcal{M}_{k+k'}(\mathfrak{N}, \mathcal{E}\mathcal{E}')$.*

Then $\tilde{f}^2$ agrees with the adelic q-expansion mod q^B of a Hilbert modular form in $\mathcal{M}_{2k}(\mathfrak{N}, \mathcal{E}^2)$ if and only if $\tilde{f}$ agrees with the adelic q-expansion mod q^B of a Hilbert modular form in $\mathcal{M}_k(\mathfrak{N}, \mathcal{E})$.

Proof. The 'only if' part is immediate. Conversely, let $g \in \mathcal{M}_{k+k'}(\mathfrak{N}, \mathcal{E}\mathcal{E}')$ and $h \in \mathcal{M}_{2k}(\mathfrak{N}, \mathcal{E}^2)$ such that

$$\tilde{f} \equiv \frac{g}{E} \mod q^B \qquad \text{and} \qquad \tilde{f}^2 \equiv h \mod q^B.$$

Then $\frac{g^2}{E^2}E^2$ and hE^2 are Hilbert modular forms in $\mathcal{M}_{2k+2k'}(\mathfrak{N}, \mathcal{E}^2\mathcal{E}'^2)$. Moreover, the adelic q-expansions of g^2 and hE^2 agree up to q^B, indeed

$$g^2 \equiv \tilde{f}^2E^2 \equiv hE^2 \mod q^B.$$

So by Definition 3.3.20 we obtain

$$g^2 = hE^2,$$

so that $\frac{g^2}{E^2} = h$ is a Hilbert modular form in $\mathcal{M}_{2k}(\mathfrak{N}, \mathcal{E}^2)$. Now $\frac{g}{E}$ is a fractional Hilbert modular form such that $(\frac{g}{E})^2$ is a Hilbert modular form. So by Lemma 3.3.16 $\frac{g}{E}$ is a Hilbert modular form whose adelic q-expansion agrees with $\tilde{f}$. □

Let $\mathfrak{m}$ be an integral ideal, then the Hecke operators on adelic power series do not act on the ring of truncated power series mod q^B. Instead, the Hecke operator $T_\mathfrak{m}$ loses exactly a factor $\mathrm{N}(\mathfrak{m})$ of precision. Formally, we have the following proposition.

Proposition 3.3.22. *Let k be a weight vector and $\mathfrak{m}$ an integral ideal, then $\mathbb{C}[\![q]\!]^K/(q^{B/\mathrm{N}(\mathfrak{m})})$ is the largest truncated power series ring such that the operator $T_\mathfrak{m}$ from $\mathbb{C}[\![q]\!]_k^K/(q^B)$ to $\mathbb{C}[\![q]\!]_k^K/(q^{B/\mathrm{N}(\mathfrak{m})})$ is well defined, i.e. such that the following diagram commutes.*

$$\begin{array}{ccc} \mathbb{C}[\![q]\!]_k^K & \xrightarrow{T_\mathfrak{m}} & \mathbb{C}[\![q]\!]_k^K \\ \Big\downarrow{\scriptstyle \pi_B} & & \Big\downarrow{\scriptstyle \pi_{B/\mathrm{N}(\mathfrak{m})}} \\ \mathbb{C}[\![q]\!]_k^K/(q^B) & \xrightarrow[T_\mathfrak{m}]{} & \mathbb{C}[\![q]\!]_k^K/(q^{B/\mathrm{N}(\mathfrak{m})}) \end{array}$$

Proof. This follows from the definition of the Hecke operators on adelic power series. □

Definition 3.3.23. *Let V be a subspace of $\mathbb{C}[\![q]\!]^K/(q^B)$ and $T_\mathfrak{m}$ a Hecke operator in $\mathbb{T}_k(\mathfrak{N},\mathcal{E})$. We say that V is* $T_\mathfrak{m}$-stable *if V is contained in the k-part of $\mathbb{C}[\![q]\!]^K/(q^B)$ and*

$$T_\mathfrak{m}(V) \subset \pi_{B/\mathrm{N}(\mathfrak{m})}(V).$$

If $\widetilde{\mathbb{T}}$ is a subset of $\mathbb{T}_k(\mathfrak{N},\mathcal{E})$, we say V is $\widetilde{\mathbb{T}}$-stable *if V is $T_\mathfrak{m}$-stable for all Hecke operators in $\widetilde{\mathbb{T}}$. We say that V is* Hecke stable *if V is $T_\mathfrak{m}$-stable for all Hecke operators $T_\mathfrak{m}$ in $\mathbb{T}_k(\mathfrak{N},\mathcal{E})$. The* Hecke-stable subspace *(resp. $T_\mathfrak{m}$-stable subspace or $\widetilde{\mathbb{T}}$-stable subspace) of a subspace W of $\mathbb{C}[\![q]\!]^K/(q^B)$ is the largest subspace of W that is Hecke-stable (resp. $T_\mathfrak{m}$-stable or $\widetilde{\mathbb{T}}$-stable) and we denote it by $W^{\mathbb{T}}$ (resp. $W^{T_\mathfrak{m}}$ or $W^{\widetilde{\mathbb{T}}}$).*

Note that the space of adelic q-expansions mod q^B of $\mathcal{M}_k(\mathfrak{N},\mathcal{E})$ is a Hecke stable subspace for any weight, level and character. We will use this to compute the adelic q-expansions in the next section.

3.4 Algorithms

In this section, we will describe an algorithm to compute a space of truncated adelic power series that contains the truncated q-expansions of the space of Hilbert modular forms of (partial) weight 1. The algorithm follows the same philosophy as the algorithms used by Joe Buhler in [5],by Kevin Buzzard in [6] and George Schaeffer in [29] for classical modular forms and by Richard Moy and Joel Specter in [22]

for classical Hilbert modular forms. The idea is that a finite dimensional space of meromorphic functions that satisfy the modularity condition and which is stable under the action of Hecke operators, should be modular. Moreover, we will give conditions under which the candidate space equals the space of Hilbert modular forms. Although the algorithm can be used in arbitrary weight, the interesting applications are to compute spaces of Hilbert modular forms of (partial) weight 1 since there are other algorithms known and implemented in higher weights, and we will make use of these algorithms to compute in weight 1.

Outline of the Algorithm

Let k be a weight vector of (partial) weight 1. That is a vector $k \in \mathbb{Z}^n$ such that at least one of the components $k_i = 1$. Let $\mathfrak{N}$ be an integral ideal of K and $\mathcal{E}$ a character mod $\mathfrak{N}$. A Hilbert modular form E in $M_{k'}(\mathfrak{N}, \mathcal{E}')$ induces a morphism of $\mathbb{C}$-vector spaces

$$- \cdot E : \mathcal{M}_k(\mathfrak{N}, \mathcal{E}) \to \mathcal{M}_{k+k'}(\mathfrak{N}, \mathcal{E}\mathcal{E}') : f \mapsto f \cdot E.$$

Suppose that E has an invertible adelic q-expansion, then we can consider the vector space $E^{-1}\mathcal{M}_{k+k'}(\mathfrak{N}, \mathcal{E}\mathcal{E}')$. The elements of this space are not Hilbert modular forms since their components are not necessarily holomorphic functions. They do, however, satisfy the modularity condition. Moreover, this space contains the space of Hilbert modular forms

$$\mathcal{M}_k(\mathfrak{N}, \mathcal{E}) \subset E^{-1}\mathcal{M}_{k+k'}(\mathfrak{N}, \mathcal{E}\mathcal{E}').$$

So that we have a finite dimensional candidate space. We then use the Hecke operators to shrink this candidate space.

The space of Hilbert modular forms is Hecke stable, that is $T_{\mathfrak{m}}\mathcal{M}_k(\mathfrak{N}, \mathcal{E}) \subset \mathcal{M}_k(\mathfrak{N}, \mathcal{E})$ for all Hecke operators $T_{\mathfrak{m}}$. So the largest Hecke-stable subspace of $E^{-1}\mathcal{M}_{k+k'}(\mathfrak{N}, \mathcal{E}\mathcal{E}')$ will contain the space of Hilbert modular forms. In fact the philosophy is that $\mathcal{M}_k(\mathfrak{N}, \mathcal{E})$ is the largest Hecke-stable subspace. To show this equality it suffices to show that all forms in this subspace are holomorphic. The final algorithm will consist of two steps

First, we compute the largest Hecke-stable subspace of $E^{-1}\mathcal{M}_{k+k'}(\mathfrak{N}, \mathcal{E}\mathcal{E}')$ as truncated power series. This will be our candidate space. Then, we verify that all power series in this candidate space are in fact the q-expansion of holomorphic Hilbert modular forms.

Existing Results

Theorem 3.4.1. *There exists an algorithm that, given a totally real field K, a weight $k \gg 1$, a non-zero ideal $\mathfrak{N}$ of K and a character mod $\mathfrak{N}$ computes the space $\mathcal{S}_k(\mathfrak{N}, \mathcal{E})$*

of cuspidal Hilbert modular forms of weight k and level $\mathfrak{N}$ and character $\mathcal{E}$ as a Hecke module.

Proof. This is the main result of [9]. □

Corollary 3.4.2. *There exists an algorithm that, given a totally real field K, a weight $k \gg 1$, a non-zero ideal $\mathfrak{N}$, a character $\mathcal{E}$ mod $\mathfrak{N}$ and a positive integer B, computes a $\mathbb{C}$-basis of the image of $\mathcal{S}_k(\mathfrak{N}, \mathcal{E})$ in $\mathbb{C}[\![q]\!]^K/(q^B)$.*

Proof. The image of $\mathcal{S}_k(\mathfrak{N})$ in $\mathbb{C}[\![q]\!]^K/(q^B)$ is given by the dual space of the space of the Hecke operators given by 3.4.1. □

Proposition 3.4.3. *Let $k \geq 1$ be an integer and let $\mathcal{E}_1$ and $\mathcal{E}_2$ be characters mod $\mathfrak{N}_1$ and $\mathfrak{N}_2$, respectively. Then there exists an element $E_k(\mathcal{E}_1, \mathcal{E}_2) \in \mathcal{M}_{\underline{k}}(\mathfrak{N}_1\mathfrak{N}_2, \mathcal{E}_1\mathcal{E}_2)$ such that*

$$a_{\mathfrak{b}}\big(E_k(\mathcal{E}_1, \mathcal{E}_2)\big) = \sum_{\mathfrak{a}|\mathfrak{b}} \mathcal{E}_1(\mathfrak{b}/\mathfrak{a})\psi(\mathfrak{a})\mathrm{N}(\mathfrak{a})^{k-1}$$

for all nonzero ideals $\mathfrak{b}$ in $\mathcal{O}_K$.When $k > 1$ we have

$$a_{(0),[\mathfrak{t}_\lambda]}\big(E_k(\mathcal{E}_1, \mathcal{E}_2)\big) = \begin{cases} 2^{-n}\mathcal{E}_1^{-1}(\mathfrak{t}_\lambda)\mathrm{L}(\mathcal{E}_2\mathcal{E}_1^{-1}, 1-k) & \text{if } \mathfrak{N}_1 = \mathcal{O}_K \\ 0 & \text{otherwise.} \end{cases}$$

Moreover, $E_1(\mathcal{E}_1, \mathcal{E}_2) = E_1(\mathcal{E}_2, \mathcal{E}_1)$, and

$$a_{(0),[\mathfrak{t}_\lambda]}\big(E_1(\mathcal{E}_1, \mathcal{E}_2)\big) = \begin{cases} \mathcal{E}_1^{-1}(\mathfrak{t}_\lambda)\mathrm{L}(\mathcal{E}_2\mathcal{E}_1^{-1}, 0) & \\ \quad + \mathcal{E}_2^{-1}(\mathfrak{t}_\lambda)\mathrm{L}(\mathcal{E}_1\mathcal{E}_2^{-1}, 0) & \text{if } \mathfrak{N}_1 = \mathcal{O}_K = \mathfrak{N}_2, \\ \mathcal{E}_1^{-1}(\mathfrak{t}_\lambda)\mathrm{L}(\mathcal{E}_2\mathcal{E}_1^{-1}, 0) & \text{if } \mathfrak{N}_1 = \mathcal{O}_K \neq \mathfrak{N}_2, \\ \mathcal{E}_2^{-1}(\mathfrak{t}_\lambda)\mathrm{L}(\mathcal{E}_1\mathcal{E}_2^{-1}, 0) & \text{if } \mathfrak{N}_1 \neq \mathcal{O}_K = \mathfrak{N}_2 \\ 0 & \text{if } \mathfrak{N}_1 \neq \mathcal{O}_K \neq \mathfrak{N}_2. \end{cases}$$

Proof. This is [8, Proposition 2.1]. □

Hecke Stable Subspace

Lemma 3.4.4. *Let V be a subspace of $\mathbb{C}[\![q]\!]^K/(q^B)$ and $\widetilde{\mathbb{T}}$ a finite set of Hecke operators. Then the following algorithm computes the $\widetilde{\mathbb{T}}$-stable subspace of V in finite time.*

Algorithm 1 Given a subspace V of $\mathbb{C}[\![q]\!]^K/(q^B)$ and a set of Hecke operators $\widetilde{\mathbb{T}}$, computes the $\widetilde{\mathbb{T}}$-stable subspace $V^{\widetilde{\mathbb{T}}}$ of V.

while V is not $T_{\mathfrak{m}}$-stable for some $T_{\mathfrak{m}}$ in $\widetilde{\mathbb{T}}$ **do**
  $V \leftarrow \big(T_{\mathfrak{m}}|_V\big)^{-1}\big(\pi_{B/\mathrm{N}(\mathfrak{m})}(V)\big)$
end while
return V

Proof. Let $V^{\widetilde{\mathbb{T}}}$ be the largest $\widetilde{\mathbb{T}}$-stable subspace of V. In each step of the algorithm

$$V^{\widetilde{\mathbb{T}}} \subset \big(T_{\mathfrak{m}}|_V\big)^{-1}\big(\pi_{B/\mathrm{N}(\mathfrak{m})}(V)\big).$$

Hence, if the algorithm terminates, the result is the largest $\widetilde{\mathbb{T}}$-stable subspace of V.

Note that, in every iteration the dimension of V decreases, indeed

$$\dim_{\mathbb{C}}\big(T_{\mathfrak{m}}|_V\big)^{-1}\big(\pi_{B/\mathrm{N}(\mathfrak{m})}(V)\big) \leq \dim_{\mathbb{C}} V,$$

with equality if and only if V is $T_{\mathfrak{m}}$-stable. Moreover, V is finite dimensional and $\widetilde{\mathbb{T}}$ is a finite set, hence the algorithm will terminate after a finite number of iterations. □

Candidate Spaces

Theorem 3.4.5. *Let k be a weight vector, $\mathfrak{N}$ an integral ideal and $\mathcal{E}$ a character mod $\mathfrak{N}$. Then the following algorithm computes a candidate space V mod q^B that contains the space of adelic q-expansions mod q^B of $\mathcal{M}_k(\mathfrak{N},\mathcal{E})$ given the following information:*

1. *The adelic q-expansion mod q^B of a Hilbert modular form E in $\mathcal{M}_{k'}(\mathfrak{N},\mathcal{E}')$ such that $a_{(0)}(E)$ is invertible;*
2. *The adelic q-expansions mod q^B of a basis of the space $\mathcal{M}_{k+k'}(\mathfrak{N},\mathcal{E}\mathcal{E}')$.*

Moreover, if the bound B is larger than the Sturm bound for $\mathcal{M}_{2k+2k'}(\mathfrak{N},\mathcal{E}^2\mathcal{E}'^2)$, then the space of adelic q-expansions mod q^B of $\mathcal{M}_k(\mathfrak{N},\mathcal{E})$ is precisely the space of mod q^B-adelic power series v in V such that v^2 agrees with the adelic q-expansion of a Hilbert modular form in $M_{2k}(\mathfrak{N},\mathcal{E}^2)$. Finally, the analogous statement holds for spaces of cuspidal Hilbert modular forms.

Algorithm 2 Given $E^{-1}\mathcal{M}_{k+k'}(\mathfrak{N}, \mathcal{E}\mathcal{E}')$ as a subspace of $\mathbb{C}[\![q]\!]^K/(q^B)$ returns a candidate subspace of $\mathbb{C}[\![q]\!]^K/(q^B)$ that contains the truncated adelic q-expansions of $\mathcal{M}_k(\mathfrak{N}, \mathcal{E})$.

$V \leftarrow E^{-1}\mathcal{M}_{k+k'}(\mathfrak{N}, \mathcal{E}\mathcal{E}')$ as a subspace of $\mathbb{C}[\![q]\!]^K/(q^B)$
$\widetilde{\mathbb{T}} \leftarrow \{T_{\mathfrak{m}} \in \mathbb{T}_k(\mathfrak{N}, \mathcal{E}) \mid \mathrm{N}(\mathfrak{m}) \leq B/\mathrm{N}(\mathfrak{N})\}$
return $V^{\widetilde{\mathbb{T}}}$

Proof. It is clear that the space of q-expansions mod q^B of $\mathcal{M}_k(\mathfrak{N}, \mathcal{E})$ is a subspace of the output of the algorithm. The second claim follows from Theorem 3.3.21. □

Corollary 3.4.6. *There exists an explicit algorithm that given an integral ideal $\mathfrak{N}$ and a quadratic character $\mathcal{E}$ mod $\mathfrak{N}$ such that $L(\mathcal{E}, 0) \neq 0$, computes a candidate space V mod q^B that contains the space of adelic q-expansions of $\mathcal{S}_{\underline{1}}(\mathfrak{N}, \mathcal{E})$. Moreover, if the bound B is larger than the Sturm bound for $\mathcal{S}_{\underline{4}}(\mathfrak{N})$ then the space of adelic q-expansions mod q^B of $\mathcal{S}_{\underline{1}}(\mathfrak{N}, \mathcal{E})$ is precisely the space of mod q^B-adelic power series v in V such that v^2 agrees with the adelic q-expansion of a Hilbert modular form in $S_{\underline{2}}(\mathfrak{N})$.*

Proof. By Proposition 3.4.3 there exists an Eisenstein series $E_{\underline{1}}(\mathcal{E})$ in $\mathcal{M}_{\underline{1}}(\mathfrak{N}, \mathcal{E})$ with invertible constant term. By Corollary 3.4.2 we can compute the adelic q-expansion of a basis of the space $\mathcal{M}_{\underline{2}}(\mathfrak{N})$. In particular, we can apply Theorem 3.3.21. □

Eigenforms

Theorem 3.4.7. *Let k be a weight vector, $\mathfrak{N}$ an integral ideal and $\mathcal{E}$ a character mod $\mathfrak{N}$. Then the following algorithm computes the adelic q-expansion mod q^B of all normalised Hilbert eigenforms of $\mathcal{M}_k(\mathfrak{N}, \mathcal{E})$ given the following information:*

1. *The adelic q-expansion mod q^B of a Hilbert modular form E in $\mathcal{M}_{k'}(\mathfrak{N}, \mathcal{E}')$ such that $a_{(0)}(E)$ is invertible;*
2. *The adelic q-expansions mod q^B of a basis of the space $\mathcal{M}_{k+k'}(\mathfrak{N}, \mathcal{E}\mathcal{E}')$,*

such that the bound B is larger than the Sturm bound for $\mathcal{M}_{2k+2k'}(\mathfrak{N}, \mathcal{E}^2\mathcal{E}'^2)$ and the Hecke algebra $\mathbb{T}_k(\mathfrak{N}, \mathcal{E})$ is generated by all Hecke operators $T_{\mathfrak{m}}$ with $\mathrm{N}(\mathfrak{m}) \leq B$. Finally, the analogous statement holds for cuspidal eigenforms.

Algorithm 3 Given $E^{-1}\mathcal{M}_{k+k'}(\mathfrak{N}, \mathcal{E}\mathcal{E}')$ as a subspace of $\mathbb{C}[\![q]\!]^K/(q^B)$ returns the q-expansion mod q^B of all normalised eigenforms in $\mathcal{M}_k(\mathfrak{N}, \mathcal{E})$.

$V \leftarrow E^{-1}\mathcal{M}_{k+k'}(\mathfrak{N}, \mathcal{E}\mathcal{E}')$ as a subspace of $\mathbb{C}[\![q]\!]^K/(q^B)$
$\widetilde{\mathbb{T}} \leftarrow \left\{\mathbb{T}_{\mathfrak{m}} \mid \mathrm{N}(\mathfrak{m}) \leq B\right\}$
$< \beta_1 >, ..., < \beta_\ell > \leftarrow$ simultaneous eigenspaces of $\widetilde{\mathbb{T}}$ in $V^{\widetilde{\mathbb{T}}}$
return $\left\{\frac{1}{a_1(\beta_i)}\beta_i \;\middle|\; \beta_i^2 \in \mathcal{M}_{2k+2k'}(\mathfrak{N}, \mathcal{E}^2\mathcal{E}'^2)\right\}$

Proof. To prove the algorithm is well defined, we need to show that under the conditions of the Theorem the simultaneous eigenspaces of $\widetilde{\mathbb{T}}$ in $V^{\widetilde{\mathbb{T}}}$ are 1-dimensional. Recall that by Corollary 3.3.18, any normalised eigenvector f in $\mathbb{C}[\![q]\!]^K/(q^B)$ satisfies

$$T_{\mathfrak{m}}(f) = a_{\mathfrak{m}}(f) \cdot f.$$

So if β and β' are normalised simultaneous eigenvectors in the same simultaneous eigenspace of $\widetilde{\mathbb{T}}$, then $a_{\mathfrak{m}}(\beta) = a_{\mathfrak{m}}(\beta')$ for all ideals $\mathfrak{m}$. In particular, $\beta = \beta'$ since $\beta^2 \in \mathcal{M}_{2k+2k'}(\mathfrak{N}, \mathcal{E}^2\mathcal{E}'^2)$ for all β in the output of the algorithm and since the B is larger than the Sturm bound for $\mathcal{M}_{2k+2k'}(\mathfrak{N}, \mathcal{E}^2\mathcal{E}'^2)$. We can conclude by Theorem 3.3.21 that each of the adelic power series mod q^B in the output of the algorithm agrees with the adelic q-expansion of some normalised Hilbert modular form f in $\mathcal{M}_k(\mathfrak{N}, \mathcal{E})$, with f an eigenvector for all Hecke operators $T_{\mathfrak{m}}$ with $\mathrm{N}(B) \leq \mathfrak{m}$. Since these Hecke operators generate the full Hecke algebra $\mathbb{T}_k(\mathfrak{N})$, the form f is an eigenform. □

Corollary 3.4.8. *There exists an explicit algorithm that given an integral ideal $\mathfrak{N}$ and a quadratic character $\mathcal{E}$ mod $\mathfrak{N}$ such that $L(\mathcal{E}, 0) \neq 0$, computes the adelic power series of all eigenforms in $\mathcal{S}_{\underline{1}}(\mathfrak{N}, \mathcal{E})$.*

We will give explicit examples computed with the implementations of these algorithms in Sections 4.4 and 4.5.

Chapter 4

Non-liftable Hilbert Modular Forms of Parallel Weight 1

In this chapter we extend the definition of Hilbert modular forms of parallel weight to more general fields and rings. In particular, we show that the algorithms of Chapter 3, with appropriate modifications, remain valid in $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebras for Hilbert modular forms of parallel weight. In the last section we use these algorithms to calculate examples of (non-liftable) Hilbert modular forms of parallel weight 1.

This chapter contains a lot of 'black boxes'. It would require almost another PhD thesis to properly define all the objects involved. Therefore, we only include a minimum of theory required to show that the formulas and algorithms of the previous Chapter remain valid if one changes the coefficient ring.

4.1 Geometric Hilbert Modular Forms

In this section, we give a short overview of the geometric definition of Hilbert modular forms and their properties. We do not include any proofs in this section. For a more detailed approach see for example [1], [14] or [37].

Definition 4.1.1. *Let k be a weight vector, $\mathfrak{N}$ an integral ideal of K, R a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra and $\mathcal{E}$ an R-valued character mod $\mathfrak{N}$. The R-module of* Hilbert modular forms of weight k, level $\mathfrak{N}$ and character $\mathcal{E}$ over R *is defined as*

$$\mathcal{M}_k(\mathfrak{N}, \mathcal{E}; R) := H^0\big(X_1(\mathfrak{N}) \times \mathrm{Spec}(R), \underline{\omega}_{\mathcal{E}}^{\otimes k}\big),$$

with $X_1(\mathfrak{N})$ the so called Hilbert modular variety of level $\Gamma_1(\mathfrak{N})$ *and $\underline{\omega}_{\mathcal{E}}^k$ the* modular line bundle *of weight k and character $\mathcal{E}$, see [1, Definition 5.4].*

Remark 4.1.2. *The Hilbert modular variety can be defined as the solution to the moduli problem parametrising the polarised abelian varieties with real multiplication by $\mathcal{O}_K$ and certain level structure satisfying the Deligne-Pappas condition. For the purpose of this thesis, it suffices that $X_1(\mathfrak{N})$ is a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-scheme and that the modular line bundle is an invertible sheaf on this scheme.*

Proposition 4.1.3. *For any weight vector k, level $\mathfrak{N}$ and character $\mathcal{E}$ mod $\mathfrak{N}$, the geometric and analytic definition of Hilbert modular forms over $\mathbb{C}$ are equivalent, i.e.*

$$\mathcal{M}_k(\mathfrak{N}, \mathcal{E}; \mathbb{C}) \cong \mathcal{M}_k(\mathfrak{N}, \mathcal{E}).$$

Proof. See the proof of [25, Lemma 6.12]. □

For a given R-valued character $\mathcal{E}$ mod $\mathfrak{N}$ the global sections of the invertible sheaves $\underline{\omega}_{\mathcal{E}}^{\otimes \underline{k}}$ on $X_1(\mathfrak{N})$ are endowed with a natural graded R-algebra structure. So we can define the graded R-algebra of Hilbert modular forms of parallel weight and character $\mathcal{E}$ by

$$\mathcal{M}_{\underline{\star}}(\mathfrak{N}, \mathcal{E}^\star; R) := \bigoplus_{k \in \mathbb{Z}_{\geq 0}} \mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}^k; R).$$

Lemma 4.1.4. *Let k be a weight vector, $\mathfrak{N}$ an integral ideal, R a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra and $\mathcal{E}$ an R-valued character mod $\mathfrak{N}$. Then the R-module $\mathcal{M}_k(\mathfrak{N}, \mathcal{E}; R)$ is finitely generated. Moreover, if R is a subring of $\mathbb{C}$, then*

$$\mathcal{M}_k\Big(\mathfrak{N}, \mathcal{E}; R\Big) \otimes_{\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]} \mathbb{C} \cong \mathcal{M}_k(\mathfrak{N}, \mathcal{E}).$$

Proof. This follows from Proposition 6.6 and Theorem 6.12 [25], respectively. □

Lifting

Let $\mathfrak{N}$ be an integral ideal of K and p a prime that does not divide $\mathrm{N}(\mathfrak{N})$. Fix an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_p$ and consider the induced projection morphism

$$\pi_p : \mathcal{M}_k\left(\mathfrak{N}, \mathcal{E}; \overline{\mathbb{Z}}[\tfrac{1}{\mathrm{N}(\mathfrak{N})}]\right) \to \mathcal{M}_k(\mathfrak{N}, \mathcal{E}; \overline{\mathbb{F}}_p)$$

for any weight vector k and character $\mathcal{E}$ mod $\mathfrak{N}$. An open question is which Hilbert modular forms are so called liftable, that is, for which level $\mathfrak{N}$, weight k, character $\mathcal{E}$ and prime p this projection is surjective. The following definition will make the notion of lifting more precise.

Definition 4.1.5. *Let k be a weight vector, $\mathfrak{N}$ an integral ideal of K, p a prime that does not divide $\mathrm{N}(\mathfrak{N})$ and $\mathcal{E}$ a character mod $\mathfrak{N}$. We say that a Hilbert modular form $\bar{f}$ in $\mathcal{M}_k(\mathfrak{N},\mathcal{E};\overline{\mathbb{F}}_p)$ is* liftable *if there exists a Hilbert modular form f in $\mathcal{M}_k(\mathfrak{N},\mathcal{E};\overline{\mathbb{Z}}[\frac{1}{\mathrm{N}(\mathfrak{N})}])$ such that*

$$\pi_p(f)=\bar{f}.$$

There exist partial results proving that Hilbert modular forms always lift for specific weight, level, character and characteristic. One of those is the following theorem. It is, to the best of our knowledge, the most general statement known in the literature.

Theorem 4.1.6. *Let $\underline{k}\gg 2$ be a parallel weight vector, $\mathfrak{N}$ an integral ideal of K, $p\geq[K:\mathbb{Q}]$ a prime not dividing $\mathrm{N}(\mathfrak{N})$ and $\mathcal{E}$ a character mod $\mathfrak{N}$. Then all Hilbert modular forms in $\mathcal{M}_{\underline{k}}(\mathfrak{N},\mathcal{E};\mathbb{F}_p[\mathcal{E}])$ are liftable.*

Proof. This follows from the main result in [18]. □

4.2 Adelic Power Series over Rings

In this section, we extend the q-expansion principle to Hilbert modular forms of parallel weight over R. That is, we show that we can identify a Hilbert modular form of parallel weight with an adelic q-expansion over R.

Let R be a ring, then we define the R-module of *adelic power series over R* formally as

$$\begin{aligned}R_{\mathbb{A}}[\![q]\!] &:= R^{\mathrm{Cl}^+}\oplus\prod_{0\neq\mathfrak{b}\lhd\mathcal{O}_K}R\cdot q^{\mathfrak{b}}\\ &:=\Big\{(a_{(0),[\mathfrak{t}_\lambda]})_{\mathrm{Cl}^+}+\sum_{0\neq\mathfrak{b}\lhd\mathcal{O}_K}a_{\mathfrak{b}}q^{\mathfrak{b}}\;\Big|\;\text{with all } a_\star\in R\Big\},\end{aligned}$$

Recall that $\mathfrak{t}_1,\dots\mathfrak{t}_{h^+}$ are fixed fractional ideals forming a complete set of representatives of the narrow class group of K. We define the R-algebra of *geometric power series* as

$$R_{(\mathfrak{t}_\lambda)}[\![q]\!]:=\Big\{\Big(a_{\lambda,0}+\sum_{\xi\in\mathfrak{t}_\lambda^+}a_{\lambda,\xi}q^\xi\Big)_{[\mathfrak{t}_\lambda]\in\mathrm{Cl}^+}\;\Big|\;a_{\lambda,\varepsilon\xi}=a_{\lambda,\xi}\text{ for all }\varepsilon\in\mathcal{O}_K^{\times,+}\Big\},$$

where all $a_\star$ lie in R, i.e. an element of $R_{(\mathfrak{t}_\lambda)}[\![q]\!]$ is an h^+-tuple indexed by the representatives $\mathfrak{t}_\lambda$ of the narrow class group of K, such that the entry at $\mathfrak{t}_\lambda$ is a formal power series indexed by the elements ξ of $\mathfrak{t}_\lambda^+$ and such that $a_{\lambda,\varepsilon\xi}=a_{\lambda,\xi}$ for all ε in $\mathcal{O}_K^{\times,+}$.

Proposition 4.2.1. *The choice of representatives* $\mathfrak{t}_1, ..., \mathfrak{t}_{h^+}$ *induces an isomorphism of* R*-modules*

$$\Psi_{(\mathfrak{t}_\lambda)} : R_{(\mathfrak{t}_\lambda)}[\![q]\!] \cong R_{\mathbb{A}}[\![q]\!].$$

Proof. Consider the R-module morphisms $\Psi_{(\mathfrak{t}_\lambda)}$ and $\Phi_{(\mathfrak{t}_\lambda)}$:

$$\Psi_{(\mathfrak{t}_\lambda)} : R_{(\mathfrak{t}_\lambda)}[\![q]\!] \to R_{\mathbb{A}}[\![q]\!] :$$

$$\Big(a_{\lambda,0} + \sum_{\xi \in \mathfrak{t}_\lambda^+} a_{\lambda,\xi} q^{\xi}\Big)_{\mathrm{Cl}^+} \mapsto (a_{\lambda,0})_{\mathrm{Cl}^+} + \sum_{0 \neq \mathfrak{b} \lhd \mathcal{O}_K} a_{\mathfrak{b}} q^{\mathfrak{b}}$$

with $a_{\mathfrak{b}} = a_{\lambda,\xi}$ such that $\mathfrak{b} = \xi \mathfrak{t}_\lambda^{-1}$

$$\Phi_{(\mathfrak{t}_\lambda)} : R_{\mathbb{A}}[\![q]\!] \to R_{(\mathfrak{t}_\lambda)}[\![q]\!] :$$

$$(a_{(0),[\mathfrak{t}_\lambda]})_{\mathrm{Cl}^+} + \sum_{0 \neq \mathfrak{b} \lhd \mathcal{O}_K} a_{\mathfrak{b}} q^{\mathfrak{b}} \mapsto \Big(a_{(0),[\mathfrak{t}_\lambda]} + \sum_{\xi \in \mathfrak{t}_\lambda^+} a_{\lambda,\xi} q^{\xi}\Big)_{\mathrm{Cl}^+}$$

with $a_{\lambda,\xi} = a_{\xi\, \mathfrak{t}_\lambda^{-1}}$.

One checks that both are R-module morphism and each other's inverse for any ring R. □

Definition 4.2.2. *The* R*-algebra of* parallel weight adelic power series over R *is the* R*-module* $R_{\mathbb{A}}[\![q]\!]$ *equipped with the ring structure induced by the isomorphisms* $\Psi_{(\mathfrak{t}_\lambda)}$ *and* $\Phi_{(\mathfrak{t}_\lambda)}$*. We denote this* R*-algebra by* $R[\![q]\!]^{\underline{K}}$*.*

The following corollary shows that this R-algebra is well defined.

Corollary 4.2.3. *The* R*-algebra* $R[\![q]\!]^{\underline{K}}$ *is independent of the choice of representatives.*

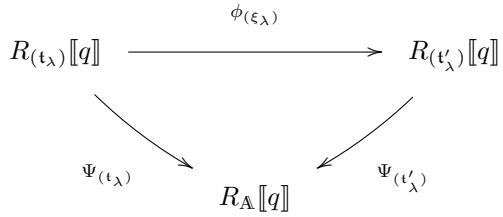
Proof. Let $(\mathfrak{t}_\lambda)_{\mathrm{Cl}^+}$ and $(\mathfrak{t}'_\lambda)_{\mathrm{Cl}^+}$ be two choices of representatives of the narrow class group of K and let $(\xi_\lambda)_{\mathrm{Cl}^+}$ be totally positive element of K such that

$$\xi_\lambda \mathfrak{t}_\lambda = \mathfrak{t}'_\lambda \text{ for all } [\mathfrak{t}_\lambda] \text{ in } \mathrm{Cl}^+.$$

We define an isomorphism of R-algebras by

$$\phi_{(\xi_\lambda)} : R_{(\mathfrak{t}_\lambda)}[\![q]\!] \to R_{(\mathfrak{t}'_\lambda)}[\![q]\!] : \Big(\sum_{\xi' \in \mathfrak{t}_\lambda^+} a_{\lambda,\xi'} q^{\xi'}\Big)_{\mathrm{Cl}^+} \mapsto \Big(\sum_{\xi' \in \mathfrak{t}_\lambda^+} a_{\lambda,\xi'} q^{\xi_\lambda \xi'}\Big)_{\mathrm{Cl}^+}.$$

By construction of $\phi_{(\xi_\lambda)}$, the following diagram commutes.



Since $\phi_{(\xi_\lambda)}$ is an R-algebra isomorphism the Corollary follows.

□

Remark 4.2.4. *The formulas and results from this section coincide with the results from Section 3.3 if the ring R is $\mathbb{C}$ and the weight is parallel. That is, the $\mathbb{C}$-algebra $\mathbb{C}[\![q]\!]^{\underline{K}}$ is precisely the parallel weight part of the graded $\mathbb{C}$ algebra $\mathbb{C}[\![q]\!]^K$ defined in Section 3.3.10.*

One can extend the notion of an adelic and geometric power series module of partial weight over a ring R under certain conditions on R. However, if the characteristic of R is non-zero and the weight k is not parallel, then the morphisms $\Phi_{k,(\mathfrak{t}_\lambda)}$ and $\Psi_{k,(\mathfrak{t}_\lambda)}$ defined in the proof of Proposition 3.3.9 are not isomorphisms. In particular, we cannot use them to define the R-algebra $R[\![q]\!]^K$. Since the goal of this chapter is to use the adelic q-expansion to obtain non-liftable forms with coefficients in finite fields we restrict to Hilbert modular forms of parallel weight.

Proposition 4.2.5. *Let $\underline{k}$ be a parallel weight vector, $\mathfrak{N}$ an integral ideal of K, R a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra and $\mathcal{E}$ an R-valued character mod $\mathfrak{N}$. Then there exists a natural injective* geometric q-expansion map*, i.e. each Hilbert modular form f in $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R)$ admits a unique geometric q-expansion in $R_{(\mathfrak{t}_\lambda)}[\![q]\!]$. Moreover, if R is a ring contained in $\mathbb{C}$ this q-expansion principle agrees with the geometric q-expansion of f as in Definition 3.3.7.*

Proof. See [1, Section 6]. □

Corollary 4.2.6. *Let $R \subset R'$ be an inclusion of $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebras. Then*

$$\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R) = \left\{ f \in \mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R') \;\middle|\; a_{\lambda,\xi}(f) \in R \text{ for all } \xi \in \mathfrak{t}_\lambda^+ \right\}.$$

Proof. See [1, Theorem 6.10.ii]. □

Corollary 4.2.7. *Let $\mathfrak{N}$ be an integral ideal of K, R a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra and $\mathcal{E}$ an R-valued character mod $\mathfrak{N}$. The geometric q-expansion map induces an injective adelic q-expansion map*

$$\mathcal{M}_{\underline{\star}}(\mathfrak{N}, \mathcal{E}^\star; R) \to R[\![q]\!]^{\underline{K}}.$$

Moreover, the image of $\mathcal{M}_{\underline{\star}}(\mathfrak{N}, \mathcal{E}^\star; R)$ in $R[\![q]\!]^{\underline{K}}$ is independent of the choice of representatives $(\mathfrak{t}_\lambda)$.

Proof. This follows from Corollary 4.2.6 and Proposition 4.2.1. □

Hecke Operators

Proposition 4.2.8. *Let $\underline{k}$ be a parallel weight vector, $\mathfrak{N}$ be an integral ideal of K, R a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra and $\mathcal{E}$ be an R-valued character mod $\mathfrak{N}$. Then the action of the Hecke operators on the adelic q-expansion of $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R)$ is given by*

$$a_{(0),[\mathfrak{t}_\lambda]}\big(T_{\mathfrak{a}}(f)\big) = \sum_{\mathfrak{a}\subset\mathfrak{b}} \mathcal{E}(\mathfrak{b})\mathrm{N}(\mathfrak{b})^{k_0-1} a_{(0),[\mathfrak{t}_\lambda \mathfrak{a}/\mathfrak{b}^2]}(f),$$

$$a_{\mathfrak{m}}\big(T_{\mathfrak{a}}(f)\big) = \sum_{\mathfrak{m}+\mathfrak{a}\subset\mathfrak{b}} \mathcal{E}(\mathfrak{b})\mathrm{N}(\mathfrak{b})^{k_0-1} a_{\mathfrak{m}\mathfrak{a}/\mathfrak{b}^2}(f).$$

Proof. See [11, Section 3]. □

We can summarise the above results in the following theorem.

Theorem 4.2.9 (The adelic q-expansion principle)**.** *Let $\underline{k}$ be a parallel weight vector, $\mathfrak{N}$ an integral ideal of K, R a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra and $\mathcal{E}$ an R-valued character mod $\mathfrak{N}$. The adelic q-expansion map induces an injective morphism of graded R-algebras from $\mathcal{M}_{\underline{\star}}(\mathfrak{N}, \mathcal{E}^\star; R)$ to $R[\![q]\!]^{\underline{K}}$ that commutes with the action of the Hecke operators. Moreover, If R' is a ring that contains R, then*

$$\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R) = \left\{ f \in \mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R') \;\middle|\; \begin{array}{c} a_{(0)}(f) \in R^{h^+} \text{ and} \\ a_{\mathfrak{b}} \in R \text{ for all } 0 \neq \mathfrak{b} \lhd \mathcal{O}_K \end{array} \right\}$$

for any weight vector $\underline{k}$ and any R-valued character $\mathcal{E}$ mod $\mathfrak{N}$.

Proof. The first statement follows from Proposition 4.2.8 and Corollary 4.2.6. The second part follows from Proposition 4.2.1 and Corollary 4.2.6. □

Remark 4.2.10. *We will write $\mathbb{T}_{\underline{k}}(\mathfrak{N},\mathcal{E})$ to indicate the $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-module generated by the Hecke operators $T_{\mathfrak{m}}$ for all integral ideals $\mathfrak{m}$ of K. We will write $\mathbb{T}_{\underline{k}}(\mathfrak{N},\mathcal{E};R)$ to indicate the R-algebra generated by the Hecke operators $T_{\mathfrak{m}}$ for all integral ideals $\mathfrak{m}$ seen as a subalgebra of $\mathrm{End}_R\big(\mathcal{M}_k(\mathfrak{N},\mathcal{E};R)\big)$.*

Corollary 4.2.11. *Let $\underline{k}$ be a parallel weight vector, $\mathfrak{N}$ be an integral ideal of K, R a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra and $\mathcal{E}$ be an R-valued character mod $\mathfrak{N}$. Let R' be a ring that contains R and let B be a positive integer such that the $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-module $\mathbb{T}_{\underline{k}}(\mathfrak{N},\mathcal{E})$ is generated by the Hecke operators $T_{\mathfrak{b}}$ with $\mathrm{N}(\mathfrak{b})\leq B$. Then*

$$\mathcal{M}_{\underline{k}}(\mathfrak{N},\mathcal{E};R)=\left\{f\in\mathcal{M}_{\underline{k}}(\mathfrak{N},\mathcal{E};R')\;\middle|\;\begin{array}{c}a_{(0)}(f)\in R^{h^+}\text{ and }a_{\mathfrak{b}}\in R\\ \text{for all } 0\neq\mathfrak{b}\lhd\mathcal{O}_K \text{ with } \mathrm{N}(\mathfrak{m})\leq B\end{array}\right\}.$$

Proof. Let f be a Hilbert modular form in $\mathcal{M}_k(\mathfrak{N},\mathcal{E};R')$ such that $a_{(0)}(f)\in R^{h^+}$ and $a_{\mathfrak{b}}(f)\in R$ for all non trivial ideals $\mathfrak{b}$ with $\mathrm{N}(\mathfrak{b})\leq B$. By Theorem 4.2.9 it suffices to show that $a_{\mathfrak{m}}(f)\in R$ for all non trivial ideals $\mathfrak{m}$. Let $\mathfrak{m}$ be an ideal with $\mathrm{N}(\mathfrak{m})\geq 0$. Then $T_{\mathfrak{m}}$ is a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-linear combination of Hecke operators $T_{\mathfrak{b}_i}$ with $\mathrm{N}(\mathfrak{b}_i)\leq B$, hence

$$a_{\mathfrak{m}}(f)=a_{\mathcal{O}_K}(T_{\mathfrak{m}}f)=a_{\mathcal{O}_K}\left(\sum_i r_iT_{\mathfrak{b}_i}f\right)=\sum_i r_ia_{\mathfrak{b}_i}(f).$$

Since all $a_{\mathfrak{m}_i}$ are elements of R, so is $a_m(f)$. □

Definition 4.2.12. *Let f be a Hilbert modular form in $\mathcal{M}_k(\mathfrak{N},\mathcal{E};R)$. We say that f is an* eigenform *if f is an eigenvector for all operators $T_{\mathfrak{m}}$ in $\mathbb{T}_k(\mathfrak{N},\mathcal{E})$. We say that f is normalised if $a_{\mathcal{O}_K}(f)=1$.*

Corollary 4.2.13. *Let f be a normalised eigenform in $\mathcal{M}_k(\mathfrak{N},\mathcal{E};R)$. Then,*

$$T_{\mathfrak{m}}(f)=a_{\mathfrak{m}}(f)\cdot f$$

for all Hecke operators $T_{\mathfrak{m}}$ in $\mathbb{T}_k(\mathfrak{N},\mathcal{E};R)$.

Remark 4.2.14. *Theorem 4.2.9 allows us to identify Hilbert modular forms of parallel weight over R with adelic q-expansions. Moreover, it ensures that the formulas for multiplication on the adelic q-expansion of Hilbert modular forms of parallel weight and the action of the Hecke operators are precisely those introduced in Chapter 3. From now on we will always identify a Hilbert modular form of parallel weight with its adelic q-expansion.*

Truncated power series

Let R be a ring and B be a positive integer, then by the definition of multiplication of adelic power series, Definition 4.2.2, the following subgroup is an ideal of $R[\![q]\!]^{\underline{K}}$

$$\left(q^B\right) = \left\{ \sum_{\mathfrak{m} \lhd \mathcal{O}_K} a_{\mathfrak{m}} q^{\mathfrak{m}} \;\middle|\; a_{\mathfrak{m}} = 0 \text{ for all } \mathrm{N}(\mathfrak{m}) < B \right\}.$$

We call the quotient, $R[\![q]\!]^{\underline{K}}/(q^B)$, *the ring of parallel weight adelic power series mod* q^B.

Definition 4.2.15. *Let $\underline{k}$ be a parallel weight vector, $\mathfrak{N}$ an integral ideal of K, R a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra and $\mathcal{E}$ an R-valued character mod $\mathfrak{N}$. The* Sturm bound of weight $\underline{k}$, level $\mathfrak{N}$ and character $\mathcal{E}$ over R *is the smallest positive integer B such that adelic q-expansion map followed by the natural projection of q-expansions*

$$\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R) \to R[\![q]\!]^{\underline{K}}/(q^B)$$

is an injective morphism of R-modules.

Lemma 4.2.16. *Let $\underline{k}$ be a parallel weight vector, $\mathfrak{N}$ an integral ideal of K, R a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra and $\mathcal{E}$ an R-valued character mod $\mathfrak{N}$. The Sturm bound of weight $\underline{k}$, level $\mathfrak{N}$ and character $\mathcal{E}$ over R is finite and less than $k_0 \mathrm{N}(\mathfrak{N})^3$.*

Proof. Lemma 4.1.4 implies that the Sturm bound exists, i.e. is finite. The explicit bound is the main result of [36]. □

Definition 4.2.17. *We define the R-module of* fractional Hilbert modular forms of weight $\underline{k}$, level $\mathfrak{N}$, character $\mathcal{E}$ over R *as follows:*

$$\mathcal{M}^f_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R) := \left\{ \frac{f}{g} \;\middle|\; \begin{array}{c} \underline{k}_1 - \underline{k}_2 = \underline{k},\ \mathcal{E}_1/\mathcal{E}_2 = \mathcal{E},\ f \in \mathcal{M}_{\underline{k}_1}(\mathfrak{N}, \mathcal{E}_1), \\ 0 \neq g \in \mathcal{M}_{\underline{k}_2}(\mathfrak{N}, \mathcal{E}_2) \text{ and } g|f \text{ in } R[\![q]\!]^{\underline{K}} \end{array} \right\},$$

where we consider f/g as an element of $H^0\big(X_1(\mathfrak{N}) \times \mathit{Spec}(R), \underline{\omega}_{\mathcal{E}}^{\otimes \underline{k}} \otimes \mathcal{K}\big)$ with $\mathcal{K}$ the sheaf of meromorphic functions on $X_1(\mathfrak{N}) \times \mathit{Spec}(R)$).

The condition $g|f$ in $R[\![q]\!]^K$ means precisely that f/g has a well defined adelic q-expansion in $R[\![q]\!]^{\underline{K}}$. In particular, the q-expansion is over integral ideals of K rather than fractional ideals. The following lemma and corollary will give necessary and sufficient conditions on a fractional Hilbert modular form to be a Hilbert modular form.

Lemma 4.2.18. *Let f be a fractional Hilbert modular form over R. Then f^2 is a Hilbert modular form if and only if f is a Hilbert modular form.*

Proof. This follows from the fact that the R-module of Hilbert modular forms is precisely the R-submodule of the fractional Hilbert modular forms that do not admit any poles. □

Corollary 4.2.19. *Let $\underline{k}$ and $\underline{k}'$ be parallel weight vectors, $\mathfrak{N}$ an integral ideal of K, R a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra and let $\mathcal{E}$ and $\mathcal{E}'$ be R-valued characters mod $\mathfrak{N}$. Let E be a Hilbert modular form in $\mathcal{M}_{\underline{k}'}(\mathfrak{N}, \mathcal{E}'; R)$. Let B be the Sturm bound of weight $2\underline{k} + 2\underline{k}'$, level $\mathfrak{N}$ and character $\mathcal{E}^2\mathcal{E}'^2$. Let $\tilde{f}$ be the truncated adelic q-expansion mod q^B of a fractional Hilbert modular form in $E^{-1}\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; R)$.*

Then $\tilde{f}^2$ agrees with the adelic q-expansion mod q^B of a Hilbert modular form in $\mathcal{M}_{2\underline{k}}(\mathfrak{N}, \mathcal{E}^2; R)$ if and only if $\tilde{f}$ agrees with the adelic q-expansion mod q^B of a Hilbert modular form in $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R)$.

Proof. The argument is analogous to the proof of 3.3.21. □

Let $\mathfrak{m}$ be an integral ideal, then the Hecke operators on adelic power series do not act on the R-module of truncated weight $\underline{k}$ power series mod q^B. Instead, the Hecke operator $T_{\mathfrak{m}}$ loses exactly a factor $\mathrm{N}(\mathfrak{m})$ of precision. Formally, we have the following proposition.

Proposition 4.2.20. *Let $\underline{k}$ be a weight vector, $\mathfrak{N}$ an integral ideal of K, R a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra and $\mathcal{E}$ an R-valued character mod $\mathfrak{N}$. Let $\mathfrak{m}$ be an integral ideal of K, then $R[\![q]\!]^{\underline{K}}/(q^{B/\mathrm{N}(\mathfrak{m})})$ is the largest truncated power series R-module such that the operator $T_{\mathfrak{m}}$ from $R[\![q]\!]^{\underline{K}}_{\underline{k}}/(q^B)$ to $R[\![q]\!]^{\underline{K}}_{\underline{k}}/(q^{B/\mathrm{N}(\mathfrak{m})})$ is well defined, i.e. such that the following diagram commutes.*

$$\begin{array}{ccc} R[\![q]\!]^{\underline{K}}_{\underline{k}} & \xrightarrow{T_{\mathfrak{m}}} & R[\![q]\!]^{\underline{K}}_{\underline{k}} \\ \Big\downarrow{\scriptstyle \pi_B} & & \Big\downarrow{\scriptstyle \pi_{B/\mathrm{N}(\mathfrak{m})}} \\ R[\![q]\!]^{\underline{K}}_{\underline{k}}/(q^B) & \xrightarrow[T_{\mathfrak{m}}]{} & R[\![q]\!]^{\underline{K}}_{\underline{k}}/(q^{B/\mathrm{N}(\mathfrak{m})}) \end{array}$$

Proof. This follows from the definition of the Hecke operators on adelic power series. □

Let V be a submodule of $R[\![q]\!]^{\underline{K}}/(q^B)$ and $T_{\mathfrak{m}}$ a Hecke operator in $\mathbb{T}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R)$. We say that V is $T_{\mathfrak{m}}$-*stable*

$$T_{\mathfrak{m}}(V) \subset \pi_{B/\mathrm{N}(\mathfrak{m})}(V).$$

If $\widetilde{\mathbb{T}}$ is a subset of $\mathbb{T}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R)$, we say that V is $\widetilde{\mathbb{T}}$-*stable* if V is $T_{\mathfrak{m}}$-stable for all Hecke operators in $\widetilde{\mathbb{T}}$. We say that V is *Hecke stable* if V is $T_{\mathfrak{m}}$-stable for all Hecke operators $T_{\mathfrak{m}}$ in $\mathbb{T}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R)$. The *Hecke-stable subspace* (resp. $T_{\mathfrak{m}}$-stable subspace or $\widetilde{\mathbb{T}}$-stable subspace) of a subspace W of $R[\![q]\!]^{\underline{K}}/(q^B)$ is the largest subspace of W that is Hecke-stable (resp. $T_{\mathfrak{m}}$-stable or $\widetilde{\mathbb{T}}$-stable) and we denote it by $W^{\mathbb{T}}$ (resp. $W^{T_{\mathfrak{m}}}$ or $W^{\widetilde{\mathbb{T}}}$).

4.3 Algorithms (Again)

Existing Results

Corollary 4.3.1. *Let $\underline{k} \gg 1$ be a weight vector, $\mathfrak{N}$ an integral ideal of K, R a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra and $\mathcal{E}$ an R-valued character mod $\mathfrak{N}$. If*

$$\mathcal{S}_{\underline{k}}\big(\mathfrak{N}, \mathcal{E}; \mathbb{Z}[\tfrac{1}{\mathrm{N}(\mathfrak{N})}, \mathcal{E}]\big) \otimes_{\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]} R \cong \mathcal{S}_{\underline{k}}\big(\mathfrak{N}, \mathcal{E}; R\big),$$

then there exists an explicit algorithm that computes a finite set of R-generators of the image of $\mathcal{S}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R)$ in $R[\![q]\!]^{\underline{K}}/(q^B)$.

Proof. Theorem 3.4.1 shows the existence of an algorithm to compute the adelic q-expansion mod q^B of a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-basis of $\mathcal{S}_{\underline{k}}\big(\mathfrak{N}, \mathcal{E}; \mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}, \mathcal{E}]\big)$. If

$$\mathcal{S}_{\underline{k}}\big(\mathfrak{N}, \mathcal{E}; \mathbb{Z}[\tfrac{1}{\mathrm{N}(\mathfrak{N})}, \mathcal{E}]\big) \otimes_{\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]} R \cong \mathcal{S}_{\underline{k}}\big(\mathfrak{N}, \mathcal{E}; R\big),$$

then the image of the q-expansion of this basis will generate the image of $\mathcal{S}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R)$ in $R[\![q]\!]^{\underline{K}}/(q^B)$ as an R-module. □

Hecke Stable Submodule

In practice there are two types of rings we will consider, namely the ring R will either be a field or $R = \mathcal{O}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$ with $\mathcal{O}$ the ring of integers of some number field. In the second case, R need not be a principal ideal domain. Linear algebra over rings that are not PID's could, a priori, cause complications. However, the ring $\mathcal{O}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$ is free of finite rank as a module over the PID $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$. To avoid any such complications, computations will be done as $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-modules. The following corollary formalises this condition in a more general setting.

Corollary 4.3.2. *Let R be a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra such that there exists a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra S that is a* PID *and such that R is a free S-module of finite rank. Then $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}, R)$ is a free S-module of finite rank, for any R-valued character $\mathcal{E}$ mod $\mathfrak{N}$.*

Proof. By Lemma 4.1.4 $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}, R)$ is finitely generated as an R-module. Since R is free of finite rank as an S-module, $\mathcal{M}_{k}(\mathfrak{N}, \mathcal{E}, R)$ is finitely generated. Moreover, $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}, R)$ injects into the torsion-free S-module $R[\![q]\!]^{\underline{K}}$. In particular, $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}, R)$ is torsion free as an S-module. Since S is a PID, the structure theorem for finitely generated modules over principal ideal domains implies that $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}, R)$ is free of finite rank as an S-module. □

The following lemma shows that we can compute Hecke stable submodules of those types that we will actually need for the later algorithms in $R[\![q]\!]^{\underline{K}}/(q^B)$ in finite time, given that the bound B is sufficiently large.

Lemma 4.3.3. *Let $\underline{k}$ be a parallel weight vector, $\mathfrak{N}$ an integral ideal of K, R a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra and $\mathcal{E}$ an R-valued character mod $\mathfrak{N}$. Let $\widetilde{\mathbb{T}}$ be a finite set of Hecke operators in $\mathbb{T}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R)$ and V an R-submodule of $R[\![q]\!]^{\underline{K}}/(q^B)$. Then the following algorithm computes the $\widetilde{\mathbb{T}}$-stable R-submodule of V in finite time if either R is a field or the following three conditions are satisfied:*

1. *The ring R is free of finite rank as an S-module for some $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra S that is a* PID*;*
2. *The R-submodule V is the R-submodule of $R[\![q]\!]^{\underline{K}}/(q^B)$ consisting of the adelic q-expansion mod q^B of all fractional Hilbert modular forms in $E^{-1}\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; R)$, with E a Hilbert modular form in $\mathcal{M}_{\underline{k}'}(\mathfrak{N}, \mathcal{E}'; R)$ whose adelic q-expansion mod q^B is invertible in $R[\![q]\!]^{\underline{K}}/(q^B)$;*
3. *The bound B is such that the $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-module $\mathbb{T}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}')$ is generated by the Hecke operators $T_{\mathfrak{b}}$ with $\mathrm{N}(\mathfrak{b})^2 \leq B$ and such that $\mathrm{N}(\mathfrak{m})^2 \leq B$ for all operators $T_{\mathfrak{m}}$ in $\widetilde{\mathbb{T}}$.*

Algorithm 4 Given a submodule V of $R[\![q]\!]^{\underline{K}}/(q^B)$ and a set of Hecke operators $\widetilde{\mathbb{T}}$, computes the $\widetilde{\mathbb{T}}$-stable submodule $V^{\widetilde{\mathbb{T}}}$ of V.

$V_0 \leftarrow V$
while V_i is not $T_{\mathfrak{m}}$-stable for some $T_{\mathfrak{m}}$ in $\widetilde{\mathbb{T}}$ **do**
  $i \leftarrow i + 1$
  $V_i \leftarrow \left(T_{\mathfrak{m}}|_{V_{i-1}}\right)^{-1}\left(\pi_{B/\mathrm{N}(\mathfrak{m})}(V_{i-1})\right)$
end while
return V_i

Proof. As in the algorithm, we define

$$V_0 := V \text{ and}$$

$$V_{i+1} := \left(T_{\mathfrak{m}}|_{V_i}\right)^{-1}\left(\pi_{B/\mathrm{N}(\mathfrak{m})}(V_i)\right) \subset V_i.$$

Clearly, the largest $\widetilde{\mathbb{T}}$-stable submodule $V^{\widetilde{\mathbb{T}}}$ is contained in each of the spaces V_i. Hence, if the algorithm terminates, the result is the largest $\widetilde{\mathbb{T}}$-stable subspace of V. It remains to show that the algorithm does terminate after a finite number of iterations.

Note that by construction, each of the inclusion $V_{i+1} \subset V_i$ is strict, so we obtain a descending chain of R-modules

$$V_0 \supset V_1 \supset ... \supset V_i \supset V_{i+1} \supset ... \supset V^{\widetilde{\mathbb{T}}}.$$

If R is a field we obtain a strictly decreasing sequence of positive integers

$$\dim_R(V_0) > \dim_R(V_1) > \cdots > \dim_R(V_i) > \dim_R(V_{i+1}) > .... > \dim_R(V^{\widetilde{\mathbb{T}}}).$$

Since, V_0 is finite dimensional, the descending chain V_i terminates after at most $\dim_R(V_0)$ iterations.

If condition 1 in the statement of the lemma holds, then Corollary 4.3.2 implies that the module V is a free S-module of finite rank, so by the above argument, it suffices to show that

$$\mathrm{rank}_S(V_i) = \mathrm{rank}_S(V_{i+1}) \text{ if and only if } V_i = V_{i+1}.$$

Let us denote the image of the q-expansion map composed with the natural projection mod q^B, by $q^B(-)$. Then, condition 2 states that

$$V_0 = V = q^B\left(E^{-1}\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; R)\right).$$

We will show that the following two statements hold for any bound B satisfying condition 3 of the statement of the lemma.

(i) For all v_0 in $\mathrm{Frac}(S) \otimes_S R[\![q]\!]^{\underline{K}}/(q^B)$ and all $s \in S \setminus \{0\}$,

$$s \cdot v_0 \in V_0 \text{ and } \pi_{\sqrt{B}}(v_0) \in R[\![q]\!]^{\underline{K}}/(q^{\sqrt{B}}) \text{ if and only if } v_0 \in V_0.$$

(ii) For all v in $R[\![q]\!]^{\underline{K}}/(q^B)$, all $s \in S \setminus \{0\}$ and all integers $i \geq 0$,

$$s \cdot v \in V_i \text{ if and only if } v \in V_i.$$

The 'only if' part of (i) is immediate. Conversely, let v_0 be an element of $\mathrm{Frac}(S) \otimes_S R[\![q]\!]^{\underline{K}}/(q^B)$ and s a non-zero element of S such that $s \cdot v_0 \in V_0$ and $\pi_{\sqrt{B}}(v_0) \in R[\![q]\!]^{\underline{K}}/(q^{\sqrt{B}})$. By definition of V_0, there exists a Hilbert modular form f in $\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; R)$ such that

$$s \cdot v_0 \cdot E \equiv f \mod q^B.$$

Now f/s is a Hilbert modular form in $\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}', \mathrm{Frac}(S) \otimes_S R)$ whose coefficients mod q^B agree with those of $v_0 \cdot E$. The coefficients of v_0 mod $q^{\sqrt{B}}$ are elements of R, hence the coefficients of f/s mod $q^{\sqrt{B}}$ are contained in R. Since the $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-module $\mathbb{T}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}')$ is generated by the Hecke operators $T_{\mathfrak{b}}$ with $\mathrm{N}(\mathfrak{b}) \leq \sqrt{B}$, Corollary 4.2.11 implies that f/s is a Hilbert modular form in $\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; R)$. So $f/(s \cdot E)$ is a fractional Hilbert modular form in $E^{-1}\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; R)$ whose adelic q-expansion mod q^B agrees with v_0, i.e. v_0 is an element of $V_0 = q^B\big(E^{-1}\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; R)\big)$.

Next, we prove statement (ii) by induction on i. Again, the 'only if' part is immediate. Conversely, the case $i = 0$ is a special case of statement (i). Let $i > 0$ be an integer, $v \in R[\![q]\!]^{\underline{K}}/(q^B)$ and $s \in S \setminus \{0\}$ such that $s \cdot v \in V_i$. By construction of V_i this means that $s \cdot v \in V_{i-1}$ and $T_{\mathfrak{m}}(s \cdot v) \in \pi_{B/\mathrm{N}(\mathfrak{m})}(V_{i-1})$, i.e. $s \cdot v \in V_{i-1}$ and there exists an element v' in V_{i-1} such that

$$T_{\mathfrak{m}}(s \cdot v) = \pi_{B/\mathrm{N}(\mathfrak{m})}(v').$$

The element v'/s is an element of $\mathrm{Frac}(S) \otimes_S V_{i-1} \subset \mathrm{Frac}(S) \otimes_S V_0$ such that $\pi_{\sqrt{B}}(v'/s) = \pi_{\sqrt{B}} \circ T_{\mathfrak{m}}(v) \in R[\![q]\!]^{\underline{K}}/(q^{\sqrt{B}})$. Note that the projection $\pi_{\sqrt{B}}$ of $T_{\mathfrak{m}}(v)$ is well defined since $B > \mathrm{N}(\mathfrak{m})^2$. So by statement (i), v'/s is an element of V_0. In particular, v'/s is an element of $R[\![q]\!]^{\underline{K}}/(q^B)$ and $s \cdot v'/s = v' \in V_{i-1}$, the induction hypothesis implies that v'/s is an element of V_{i-1}. So

$$T_{\mathfrak{m}}(v) = \pi_{B/\mathrm{N}(\mathfrak{m})}(v'/s) \in \pi_{B/\mathrm{N}(\mathfrak{m})}(V_{i-1})$$

and $v \in V_{i-1}$, hence v is an element of V_i. This completes the proof by induction of part (ii).

Finally, we show that (ii) implies that

$$\mathrm{rank}_S(V_i) = \mathrm{rank}_S(V_{i+1}) \text{ if and only if } V_i = V_{i+1}$$

for all $i \geq 0$. Suppose that $\mathrm{rank}_S(V_i) = \mathrm{rank}_S(V_{i+1})$, then $\mathrm{Frac}(S) \otimes_S V_i = \mathrm{Frac}(S) \otimes_S V_{i+1}$. Let v be an element of V_i, then there exists an element s in S such that $s \cdot v \in V_{i+1}$. By statement (ii), this implies that $v \in V_{i+1}$. □

Candidate Spaces

The following theorem is the analogue of Theorem 3.4.5 and the algorithm is the analogue of Algorithm 2. The underlying idea is the same, that is, we first compute the q-expansions of the R-module of Hilbert modular forms of weight $\underline{k} + \underline{k}'$. By dividing by the adelic q-expansion of a suitable Hilbert modular form of weight $\underline{k}'$ we obtain a candidate space that contains the adelic q-expansions of Hilbert modular forms of weight $\underline{k}$. We then decrease the size of the candidate R-module by taking the Hecke stable submodules. Finally, we hope that the resulting candidate module equals the R-module of Hilbert modular forms. We can verify that it is by checking that the squares of our candidates are Hilbert modular forms of weight $2\underline{k}$.

In practice we do not use all Hecke operators available. Rather, we only use the first few and increase the number of Hecke operators and/or the precision if our candidate space is too big.

Theorem 4.3.4. *Let $\underline{k}$ and $\underline{k}'$ be parallel weight vectors, $\mathfrak{N}$ an integral ideal, R a $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-algebra and $\mathcal{E}$ and $\mathcal{E}'$ R-valued characters mod $\mathfrak{N}$. Then the following algorithm computes a candidate R-submodule V of $R[\![q]\!]^{\underline{K}}/(q^B)$ that contains the R-module of adelic q-expansions mod q^B of $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R)$ given the following information:*

1. *The adelic q-expansion mod q^B of a Hilbert modular form E in $\mathcal{M}_{\underline{k}'}(\mathfrak{N}, \mathcal{E}'; R)$ such that $a_{(0)}(E)$ is invertible in R;*
2. *The adelic q-expansions mod q^B of a finite generating set of the R-module $\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; R)$.*

Moreover, if the bound B is larger than the Sturm bound for $\mathcal{M}_{2\underline{k}+2\underline{k}'}(\mathfrak{N}, \mathcal{E}^2\mathcal{E}'^2; R)$, then the R-module of adelic q-expansions mod q^B of $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R)$ is precisely the R-module of mod q^B-adelic power series v in V such that v^2 agrees with the adelic q-expansion of a Hilbert modular form in $M_{2\underline{k}}(\mathfrak{N}, \mathcal{E}^2; R)$. Finally, the analogous statement holds for R-modules of cuspidal Hilbert modular forms.

Algorithm 5 Given an invertible adelic q-expansion mod q^B of a Hilbert modular form in $\mathcal{M}_{\underline{k}'}(\mathfrak{N}, \mathcal{E}'; R)$ and the adelic q-expansion mod q^B of a basis of $\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; R)$ computes an R-module mod q^B that contains the adelic q-expansions of $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R)$.

$V \leftarrow E^{-1}\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; R)$ as a submodule of $R[\![q]\!]^{\underline{K}}/(q^B)$
$\widetilde{\mathbb{T}} \leftarrow \{T_{\mathfrak{m}} \in \mathbb{T}_k(\mathfrak{N}, \mathcal{E}; R) \mid \mathrm{N}(\mathfrak{m}) \leq B/\mathrm{N}(\mathfrak{N})\}$
return $V^{\widetilde{\mathbb{T}}}$

Proof. It is clear that the R-module of q-expansions mod q^B of $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; R)$ is a submodule of the output of the algorithm. The second claim follows from Corollary 4.2.19. □

Corollary 4.3.5. *There exists an explicit algorithm that given an integral ideal $\mathfrak{N}$, a prime number p not dividing $\mathrm{N}(\mathfrak{N})$ and a quadratic character $\mathcal{E}$ mod $\mathfrak{N}$ such that p does not divide the nominator of $L(\mathcal{E}, 0)$, computes a candidate space V mod q^B that contains the space of adelic q-expansions of $\mathcal{S}_{\underline{1}}(\mathfrak{N}, \mathcal{E}; \mathbb{F}_p)$ provided that all Hilbert modular forms in $\mathcal{S}_{\underline{2}}(\mathfrak{N}, \mathcal{E}^2; \mathbb{F}_p)$ are liftable. Moreover, if the bound B is larger than the Sturm bound for $\mathcal{S}_{\underline{4}}(\mathfrak{N}, \mathcal{E}^4; \mathbb{F}_p)$, then the space of adelic q-expansions mod q^B of $\mathcal{S}_{\underline{1}}(\mathfrak{N}, \mathcal{E}; \mathbb{F}_p)$ is precisely the space of mod q^B-adelic power series v in V such that v^2 agrees with the adelic q-expansion of a Hilbert modular form in $S_{\underline{2}}(\mathfrak{N}, \mathcal{E}^2; \mathbb{F}_p)$.*

Proof. By Proposition 3.4.3 there exists an Eisenstein series $E_{\underline{1}}(\mathcal{E})$ in $\mathcal{M}_{\underline{1}}(\mathfrak{N}, \mathcal{E}; \mathbb{F}_p)$ with invertible constant term. By Corollary 3.4.2 we can compute the adelic q-expansion of a basis of the space $\mathcal{S}_{\underline{2}}(\mathfrak{N}, \mathcal{E}^2; \mathbb{F}_p)$. Since all weights are parallel we can apply Corollary 4.2.19. □

Eigenforms

The following theorem is the equivalent of Theorem 3.4.7 and the algorithm is the equivalent of Algorithm 3. The underlying idea is the same, that is, we first compute a candidate space using Algorithm 5. Then we compute the simultaneous eigenvectors of the Hecke operators in the candidate space.

Theorem 4.3.6. *Let $\underline{k}$ and $\underline{k}'$ be parallel weight vectors, $\mathfrak{N}$ an integral ideal, F an algebraically closed field such that $\mathrm{N}(\mathfrak{N})$ is invertible in F and $\mathcal{E}$ and $\mathcal{E}'$ F-valued characters mod $\mathfrak{N}$. Then the following algorithm computes the adelic q-expansion mod q^B of all normalised Hilbert eigenforms of $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; F)$ given the following information:*

1. *The adelic q-expansion mod q^B of a Hilbert modular form E in $\mathcal{M}_{\underline{k}'}(\mathfrak{N}, \mathcal{E}'; F)$ such that $a_{(0)}(E)$ is invertible;*
2. *The adelic q-expansions mod q^B of a basis of the space $\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; F)$,*

such that the bound B is larger than the Sturm bound for $\mathcal{M}_{2\underline{k}+2\underline{k}'}(\mathfrak{N}, \mathcal{E}^2\mathcal{E}'^2; F)$ and the Hecke algebra $\mathbb{T}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; F)$ is generated by all Hecke operators $T_{\mathfrak{m}}$ with $\mathrm{N}(\mathfrak{m}) \leq B$. Finally, the analogous statement holds for cuspidal eigenforms.

Algorithm 6 Given an invertible adelic q-expansion mod q^B of a Hilbert modular form in $\mathcal{M}_{\underline{k}'}(\mathfrak{N}, \mathcal{E}'; F)$ and the adelic q-expansion mod q^B of a basis of $\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; F)$ computes the adelic q-expansion mod q^B of all normalised eigenforms in $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; F)$.

$V \leftarrow E^{-1}\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}')$ as a subspace of $F[\![q]\!]^{\underline{K}}/(q^B)$
$\widetilde{\mathbb{T}} \leftarrow \left\{\mathbb{T}_{\mathfrak{m}} \mid \mathrm{N}(\mathfrak{m}) \leq B\right\}$
$< \beta_1 >, ..., < \beta_\ell > \leftarrow$ simultaneous eigenspaces of $\widetilde{\mathbb{T}}$ in $V^{\widetilde{\mathbb{T}}}$
return $\left\{\frac{1}{a_1(\beta_i)}\beta_i \;\middle|\; \beta_i^2 \in \mathcal{M}_{2\underline{k}+2\underline{k}'}(\mathfrak{N}, \mathcal{E}^2\mathcal{E}'^2; F)\right\}$

Proof. To prove that the algorithm is well defined, we need to show that under the conditions of the Theorem the simultaneous eigenspaces of $\widetilde{\mathbb{T}}$ in $V^{\widetilde{\mathbb{T}}}$ are 1-dimensional. Recall that by Corollary 4.2.13 any normalised eigenvector f in $F[\![q]\!]^{\underline{K}}/(q^B)$ satisfies

$$T_{\mathfrak{m}}(f) = a_{\mathfrak{m}}(f) \cdot f.$$

So if β and β' are normalised simultaneous eigenvectors in the same simultaneous eigenspace of $\widetilde{\mathbb{T}}$, then $a_{\mathfrak{m}}(\beta) = a_{\mathfrak{m}}(\beta')$ for all ideals $\mathfrak{m}$. In particular, $\beta = \beta'$, since $\beta^2 \in \mathcal{M}_{2\underline{k}+2\underline{k}'}(\mathfrak{N}, \mathcal{E}^2\mathcal{E}'^2; F)$ for all β in the output of the algorithm and since the B is larger than the Sturm bound for $\mathcal{M}_{2\underline{k}+2\underline{k}'}(\mathfrak{N}, \mathcal{E}^2\mathcal{E}'^2; F)$ we can conclude by Corollary 4.2.19 that each of the adelic power series mod q^B in the output of the algorithm agrees with the adelic q-expansion of some normalised Hilbert modular form f in $\mathcal{M}_k(\mathfrak{N}, \mathcal{E}; F)$, with f an eigenvector for all Hecke operators $T_{\mathfrak{m}}$ with $\mathrm{N}(B) \leq \mathfrak{m}$. Since these Hecke operators generate the full Hecke algebra $\mathbb{T}_{\underline{k}}(\mathfrak{N})$, the form f is an eigenform. □

Corollary 4.3.7. *There exists an explicit algorithm that given an integral ideal $\mathfrak{N}$, a quadratic character $\mathcal{E}$ mod $\mathfrak{N}$ such that p does not divide the denominator of $L(\mathcal{E}, 0)$ and a prime p not dividing $\mathrm{N}(\mathfrak{N})$, computes the adelic power series of all eigenforms in $\mathcal{S}_{\underline{1}}(\mathfrak{N}, \mathcal{E}; \overline{\mathbb{F}}_p)$.*

Non-liftable Forms

One application of our algorithm is to compute examples of non-liftable Hilbert modular forms of parallel weight 1. The following corollary to Theorem 4.3.4 will enable us to compute the q-expansion of Hilbert modular forms with coefficients in $\mathbb{F}_p$ for almost all primes p simultaneously, under certain conditions. That is, it will compute a space of Hilbert modular forms $\mathcal{M}_{\underline{1}}\left(\mathfrak{N}, \mathcal{E}; \mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]\right)$ and a finite list of primes such that the projection morphism is surjective for all primes p not in the list. We can then find explicit non-liftable Hilbert modular forms by rerunning the algorithm in characteristic

p for primes in the finite list. This procedure will enable us to find all non-liftable Hilbert modular forms provided the precision is sufficiently high and the forms in the higher weight are liftable.

Corollary 4.3.8. *Let $\underline{k}$ and $\underline{k}'$ be parallel weight vectors, $\mathfrak{N}$ an integral ideal and let $\mathcal{E}$ and $\mathcal{E}'$ be quadratic characters mod $\mathfrak{N}$. If Algorithm 5 for $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$ yields a candidate submodule V of $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}][\![q]\!]^{\underline{K}}$ such that the adelic q-expansion map followed by the natural projection mod q^B is an isomorphism of $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-modules from $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; \mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}])$ to V, then it also yields a finite set of primes $\mathcal{L}$ such that for all primes p not contained in $\mathcal{L}$ the conditions*

1. *The projection morphism $\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; \mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]) \to \mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; \mathbb{F}_{\mathfrak{p}})$ is surjective;*
2. *The Sturm bound for $\mathcal{M}_k(\mathfrak{N}, \mathcal{E}; \mathbb{F}_p)$ is smaller than the precision B,*

imply that the projection $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; \mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]) \to \mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; \mathbb{F}_p)$ is surjective.

Proof. Recall that Algorithm 5 requires a Hilbert modular form E of weight $\underline{k}'$, level $\mathfrak{N}$ and character $\mathcal{E}'$ with invertible constant term $a_{(0)}(E)$ in $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]^n$. We define $\mathcal{L}_1$ to be the set of primes containing all primes p such that $a_{(0)}(E)$ is not invertible in $\mathbb{F}_p^n$ as well as any prime p dividing $\mathrm{N}(\mathfrak{N})$.

Let $V(\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}])$ be the output of Algorithm 5. Note that by construction $V(\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}])$ is the solution of a system of linear equations defined over $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$. Let us denote $V(\mathbb{F}_p)$ for the $\mathbb{F}_p$-space of solutions of the mod p-reduced linear system. Then for almost all primes p we have

$$V(\mathbb{F}_p) = V(\mathbb{Z}[\tfrac{1}{\mathrm{N}(\mathfrak{N})}])/(p),$$

i.e. for almost all primes p the solution of the reduced system is the reduction of the solution of the system. We define $\mathcal{L}_2$ to be the set of primes for which equality does not hold. Note that $\mathcal{L}_2$ is contained in the set of primes dividing the pivot elements of the Hermite normal form of the matrix representation of the linear system of equations defining V, hence we can explicitly determine all primes p such that $V(\mathbb{F}_p) \neq V(\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}])/(p)$. We define the set $\mathcal{L}$ as the union of $\mathcal{L}_1$ and $\mathcal{L}_2$. By construction the set $\mathcal{L}$ is finite.

Let p be a prime not contained in $\mathcal{L}$ and such that the projection morphism

$$\mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; \mathbb{Z}[\tfrac{1}{\mathrm{N}(\mathfrak{N})}]) \to \mathcal{M}_{\underline{k}+\underline{k}'}(\mathfrak{N}, \mathcal{E}\mathcal{E}'; \mathbb{F}_{\mathfrak{p}})$$

is surjective, then the first part of Theorem 4.3.4 implies that the candidate space $V(\mathbb{F}_p)$ contains the adelic q-expansions mod q^B of $\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}, \mathbb{F}_p)$.

Let us write $q^B(-)$ for the image of the adelic q-expansion map followed by the natural projection mod q^B. Then, the first condition of the corollary says that

$$q^B(-) : \mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}, \mathbb{Z}[\tfrac{1}{\mathrm{N}(\mathfrak{N})}]) \to V(\mathbb{Z}[\tfrac{1}{\mathrm{N}(\mathfrak{N})}])$$

is an isomorphims of $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-modules. Hence, we obtain the following commutative diagram

$$\begin{array}{ccccc} q^B\big(\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}, \mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}])\big)/(p) & \hookrightarrow & q^B\big(\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}, \mathbb{F}_p])\big) & \hookrightarrow & V(\mathbb{F}_p) \\ & \searrow & & \nearrow & \\ & & V\big(\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]\big)/(p) & & \end{array}$$

where all injections are inclusions. In particular, we obtain

$$q^B\big(\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}, \mathbb{Z}[\tfrac{1}{\mathrm{N}(\mathfrak{N})}])\big)/(p) = q^B\big(\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}, \mathbb{F}_p)\big).$$

Finally, if p is a prime such that the Sturm bound for weight $\underline{k}$, level $\mathfrak{N}$ and character $\mathcal{E}$ over $\mathbb{F}_p$ is less than the precision B, then this implies the projection

$$\mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; \mathbb{Z}[\tfrac{1}{\mathrm{N}(\mathfrak{N})}]) \to \mathcal{M}_{\underline{k}}(\mathfrak{N}, \mathcal{E}; \mathbb{F}_p)$$

is surjective.

□

4.4 Numerical Examples

In this section, we discuss explicit results obtained by our implementation of the above algorithms in Magma.

Limitations

Recall that in order to apply Theorems 3.4.5, 3.4.7, 4.3.4 and 4.3.6 and their corollaries to prove that an adelic power series obtained from algorithms 5 or 6 corresponds to the adelic q-expansion of a Hilbert modular form in $S_{\underline{k}}(\mathfrak{N}, \mathcal{E}, \overline{\mathbb{F}}_p)$ the precision B must be larger than the Sturm bound for $S_{\underline{2}k+2\underline{k}'}(\mathfrak{N}, \mathcal{E}^4, \overline{\mathbb{F}}_3)$. However, the best known bound

on the Sturm bound, $2(k+k')\mathrm{N}(\mathfrak{N})^3$, is beyond what we can compute in a reasonable time with the available computing power.

A second obstruction to proving that the computed space of adelic power series agrees with the adelic q-expansions of Hilbert modular forms arises from the condition in Corollaries 4.3.1 and 4.3.8. Both corollaries require that the projection morphism

$$S_{\underline{2}}(\mathfrak{N}, \mathcal{E}^2, \mathbb{Z}[\tfrac{1}{\mathrm{N}(\mathfrak{N})}]) \to S_{\underline{2}}(\mathfrak{N}, \mathcal{E}^2, \mathbb{F}_p)$$

is surjective. So the above claim in positive characteristic is only conditional.

This remark holds in all weights, levels and characters. More precisely, our computations in characteristic 0 yield a candidate space that is a upper bound, i.e. the output of the algorithm contains the space of adelic q-expansions of Hilbert modular forms, but this inclusion could be strict if the precision is lacking. Moreover, in positive characteristic this depends on the surjective of the projection morphism

$$M_{\underline{2}}(\mathfrak{N}, \mathcal{E}^2, \mathbb{Z}[\tfrac{1}{\mathrm{N}(\mathfrak{N})}, \mathcal{E}]) \to M_{\underline{2}}(\mathfrak{N}, \mathcal{E}^2, \mathbb{F}_p[\mathcal{E}]).$$

If the projection morphism is not surjective for a given prime p, the computed candidate space is only a lower bound, i.e. there could, a priori, exist more Hilbert modular forms in $S_{\underline{1}}(\mathfrak{N}, \mathcal{E}, \mathbb{F}_p)$.

Given enough time and computational power, one could use our algorithms to compute a bound on the Sturm bound in individual cases. One could also use Corollary 4.3.8 to verify that the projection morphism in parallel weight 2 is indeed surjective for all primes p since all Hilbert modular forms in parallel weight larger than 2 are liftable by Theorem 4.1.6. These computations would then yield proven adelic q-expansions. However, the time required is beyond reasonable.

Instead, we run our algorithm with increasing precision in steps of 500. If the number of linearly independent eigenforms remains the same after increasing the bound we are lead to believe that we have computed enough precision. In the examples that follow, using coefficients with ideals up to norm at most 2000 sufficed.

A First Non-liftable Example

The real quadratic field $\mathbb{Q}(\sqrt{6})$ has class number 1 and narrow class number 2. Let ω denote $\sqrt{6}$, let $\mathfrak{N}_{331} = (25+7\omega)$ be a prime ideal above 331 and let $\mathcal{E}$ be the unique quadratic character mod $\mathfrak{N}_{331}$.

The Eisenstein series $E_{\underline{1}}(\mathcal{E}, 1)$ obtained from Proposition 3.4.3 is cuspidal. However, the Eisenstein series $E_{\underline{1}}(\mathcal{E}', 1)$ with $\mathcal{E}'$ the primitive character inducing $\mathcal{E}$ has constant term $a_{\mathcal{O}} = [\frac{1}{12}, \frac{1}{12}]$. In particular, $12 \cdot E_{\underline{1}}(\mathcal{E}', 1)$ is an (old) Hilbert modular form in

$\mathcal{M}_{\underline{1}}(\mathfrak{N}_{331}, \mathcal{E}, \mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N}_{331})}])$ whose adelic q-expansion is invertible in $\mathbb{F}_p[\![q]\!]^{\underline{K}}$ for all primes p.

So we can apply algorithms 5 and 6 to obtain

$$\dim\big(\mathcal{S}_{\underline{1}}(\mathfrak{N}_{331}, \mathcal{E}, \mathbb{C})\big) = 0 \text{ and}$$

$$\dim\big(\mathcal{S}_{\underline{1}}(\mathfrak{N}_{331}, \mathcal{E}, \overline{\mathbb{F}}_p)\big) = \begin{cases} 2 & \text{if } p = 3 \\ 0 & \text{else.} \end{cases}$$

Moreover, we can compute normalised eigenforms f and f^σ with coefficients in $\mathbb{F}_9 = \mathbb{F}_3(\zeta)$ where $\zeta^4 = 1$. The eigenform f and its Galois conjugate f^σ span the space $\mathcal{S}_{\underline{1}}(\mathfrak{N}_{331}, \mathcal{E}, \overline{\mathbb{F}}_3)$. For primes $\mathfrak{p}$ with norm up to 25 we list the norm of the prime, a generator $\alpha_\mathfrak{p}$ of the prime and the coefficient, hence Hecke eigenvalue, of the normalised eigenforms $a_\mathfrak{p}(f)$ and $a_\mathfrak{p}(f^\sigma)$ in Table 4.1.

The absolute and relative frequencies of elements of $\mathbb{F}_9$ occurring as a Hecke eigenvalue for primes up to norm 2000 are given in Table 4.2. These frequencies suggest that the image of the associated Galois representation in $\mathrm{GL}_2(\mathbb{F}_9)$ is one of the following subgroups $H_1 \cong \mathbb{Z}_8 \times \mathbb{Z}_2$, $H_2 = \text{SmallGroup}(48, 33)$ or $H_3 = \text{SmallGroup}(144, 130)$. The images of these subgroups in $\mathrm{PGL}_2(\mathbb{F}_9)$ are respectively isomorphic to $\mathbb{Z}_4$, A_4 and Smallgroup$(36, 9)$.

Table 4.1: The Hecke eigenvalues for primes $\mathfrak{p} = (\alpha_\mathfrak{p})$ with norm less than 25 for the normalised eigenforms f and f^σ spanning the space $\mathcal{S}_{\underline{1}}(\mathfrak{N}_{331}, \mathcal{E}, \overline{\mathbb{F}}_3)$.

$\mathrm{N}(\mathfrak{p})$	2	3	5	5	19	19	23	23
$\alpha_\mathfrak{p}$	$2-\omega$	$3-\omega$	$1+\omega$	$1-\omega$	$5-\omega$	$5+\omega$	$1+2\omega$	$1-2\omega$
$a_\mathfrak{p}(f)$	$-\zeta$	1	ζ	0	2	0	ζ	0
$a_\mathfrak{p}(f^\sigma)$	ζ	1	$-\zeta$	0	2	0	$-\zeta$	0

Table 4.2: The absolute and relative frequencies of elements $x \in \mathbb{F}_9 = \mathbb{F}_3(\zeta)$ occurring as the Hecke eigenvalues for primes $\mathfrak{p}$ with norm less than 2000 for the normalised eigenforms f and f^σ spanning the space $\mathcal{S}_{\underline{1}}(\mathfrak{N}_{331}, \mathcal{E}, \overline{\mathbb{F}}_3)$.

x	$a_\mathfrak{p}(f)$ abs. freq.	$a_\mathfrak{p}(f)$ rel. freq.	$a_\mathfrak{p}(f^\sigma)$ abs. freq.	$a_\mathfrak{p}(f^\sigma)$ abs. freq.
0	71	0.24	71	0.24
1	56	0.19	56	0.19
-1	52	0.18	52	0.18
ζ	63	0.21	53	0.18
$-\zeta$	53	0.18	63	0.21

A Second Non-liftable Example

The real quadratic field $\mathbb{Q}(\sqrt{2})$ has narrow class number 1. Let ω be the generator of the integers of $\mathbb{Q}(\sqrt{2})$, i.e. $\omega^2 = 2$. Let $\mathfrak{N}_{484} = (22)$ be the unique ideal of norm 484 and let $\mathcal{E}$ be the unique quadratic character mod $\mathfrak{N}_{484}$ satisfying $\mathcal{E}(17 + 8\omega) = 1$. The Eisenstein series obtained from the primitive character $\mathcal{E}'$ inducing $\mathcal{E}$ has constant term $a_\mathcal{O} = \frac{1}{8}$. Multiplying this Eistensteinseries by 8 yields a Hilbert modular form with invertible adelic q-expansion in every characteristic. By applying algorithms 5 and 6 we obtain

$$\dim\big(\mathcal{S}_{\underline{1}}(\mathfrak{N}_{484}, \mathcal{E}, \mathbb{C})\big) = 0 \text{ and}$$

$$\dim\big(\mathcal{S}_{\underline{1}}(\mathfrak{N}_{484}, \mathcal{E}, \overline{\mathbb{F}}_p)\big) = \begin{cases} 1 & \text{if } p = 5 \\ 0 & \text{else.} \end{cases}$$

Morevover, we obtain a normalised eigenform g with coefficients in $\mathbb{F}_5$ that spans the space $\mathcal{S}_{\underline{1}}(\mathfrak{N}_{484}, \mathcal{E}, \overline{\mathbb{F}}_5)$ as a $\overline{\mathbb{F}}_5$ vector space.

For primes $\mathfrak{p}$ with norm less than 25 we list the norm of the prime, a generator $\alpha_\mathfrak{p}$ of the prime and the coefficient, hence Hecke eigenvalue, of the normalised eigenform $a_\mathfrak{p}(g)$ in Table 4.3. The absolute and relative frequencies of elements of $\mathbb{F}_5$ occurring as a Hecke eigenvalue for primes up to norm 2000 are given in Table 4.4. These frequencies suggest that the associated Galois representation is reducible.

Table 4.3: The Hecke eigenvalues for primes $\mathfrak{p} = (\alpha_p)$ with norm less than 25 for the normalised eigenform g spanning the space $\mathcal{S}_{\underline{1}}(\mathfrak{N}_{484}, \mathcal{E}, \overline{\mathbb{F}}_5)$.

$\mathrm{N}(\mathfrak{p})$	2	7	7	9	17	17	23	23
$\alpha_\mathfrak{p}$	$2-\omega$	$1-2\omega$	$1+2\omega$	3	$1-3\omega$	$1+3\omega$	$5+\omega$	$5-\omega$
$a_\mathfrak{p}(g)$	1	0	0	2	2	2	0	0

Table 4.4: The absolute and relative frequencies of elements $x \in \mathbb{F}_5$ occurring as the Hecke eigenvalues for primes $\mathfrak{p}$ with norm less than 2000 for the normalised eigenform g spanning the space $\mathcal{S}_{\underline{1}}(\mathfrak{N}_{484}, \mathcal{E}, \overline{\mathbb{F}}_5)$.

x	$a_\mathfrak{p}(g)$ abs. freq.	$a_\mathfrak{p}(g)$ rel. freq.
0	156	0.52
1	2	0.01
2	143	0.47

4.5 Tables of Numerical Results

In this section we list some numerical results obtained by our implementations of the algorithms in Magma for Hilbert modular forms of parallel weight 1 over the number fields $\mathbb{Q}(D)$ with $D = 2, 3, 5, 6$ respectively. We compute for all ideals $\mathfrak{N}$ with norm up to a given bound depending on the number field and all quadratic characters $\mathcal{E}$ mod $\mathfrak{N}$.

To keep the tables somewhat readable we omit any line corresponding to an ideal $\mathfrak{N}$ and quadratic character $\mathcal{E}$ mod $\mathfrak{N}$ for which we either cannot apply the algorithms or the algorithms return the zero space in all characteristics. More precisely, we do not list entries corresponding to an ideal $\mathfrak{N}$ and character $\mathcal{E}$ mod $\mathfrak{N}$ such that either one of the following conditions hold:

1. The constant term of the Eisenstein series given by 3.4.3 with character $\mathcal{E}$ and the associated primitive character $\mathcal{E}$ equals zero, i.e. the Eisenstein series does not have an invertible adelic q-expansion in any characteristic;

2. The candidate space given by Algorithm 5 is the zero space in all characteristics, i.e. $\mathcal{S}_{\underline{1}}(\mathfrak{N}, \mathcal{E}; \star) = \{0\}$.

Note that the results are valid under the assumption that the conditions of Theorem 4.3.4, Theorem 4.3.6 and Corollary 4.3.8 are satisfied. If these conditions do not hold the listed results are an upper (or lower) bound as discussed in the previous section.

In every table the first four columns identify the level $\mathfrak{N}$ and the quadratic character $\mathcal{E}$ mod $\mathfrak{N}$. In the first column we list the norm of the level. The second columns lists a generator of the ideal $\mathfrak{N}$. For the third column we fix the ordering of all ideals up to given norm provided by Magma, the number in the third column indicates the ordinal number of the ideal $\mathfrak{N}$ amongst ideals of the given norm using this order. In the fourth column we list the ordinal number of the character $\mathcal{E}$ among the quadratic characters mod $\mathfrak{N}$, again by using the ordering given by Magma. These two numbers have no intrinsic mathematical meaning, they are used to identify the level $\mathfrak{N}$ and quadratic character $\mathcal{E}$ in Magma.

Columns five to seven contain the results of computations in characteristic 0. That is the fifth column lists the $\mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}]$-rank of $\mathcal{S}_{\underline{2}}(\mathfrak{N}, \mathcal{E}^2, \mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}])$ obtained by applying the existing algorithms in Magma. The sixth column tabulates the rank of the candidate $\mathbb{Z}$-module $V_{\mathbb{Z}}$ containing the adelic q-expansions of $\mathcal{S}_{\underline{1}}(\mathfrak{N}, \mathcal{E}, \mathbb{Z}[\frac{1}{\mathrm{N}(\mathfrak{N})}])$ given by Algorithm 5. Column seven contains the number of linearly independent eigenforms in $\mathcal{S}_{\underline{1}}(\mathfrak{N}, \mathcal{E}, \overline{\mathbb{Q}})$ given by Algorithm 6.

Note that the candidate space $V_{\mathbb{Z}}$ includes adelic power series whose square does not agree with the adelic q-expansion of a weight 2 Hilbert modular form. Checking this condition on a basis of $V_{\mathbb{Z}}$ is not sufficient since this could dependent on the choice of the basis. Instead, our algorithms only check this condition on the eigenforms. In almost all examples, this information suffices to determine the rank of the submodule of adelic power series in the candidate space $V_{\mathbb{Z}}$ whose square agrees with the q-expansion of a Hilbert modular form.

Columns eight and nine contain the $\mathbb{F}_2$-dimension of the candidate space $V_{\mathbb{F}_2}$ containing $\mathcal{S}_{\underline{1}}(\mathfrak{N}, \mathcal{E}, \mathbb{F}_2)$ given by Algorithm 5 and the number of linearly independent eigenform in $\mathcal{S}_{\underline{1}}(\mathfrak{N}, \mathcal{E}, \overline{\mathbb{F}}_2)$ given by Algorithm 6. Columns ten and eleven contain the corresponding data in characteristic 3. If the level $\mathfrak{N}$ is not invertible in characteristic 2 (or 3), the space of Hilbert modular forms of level $\mathfrak{N}$ is not defined, we indicate this by listing a "-" in the corresponding columns.

The last column contains a list of primes p that divide the numerator of the Eisenstein series. For these primes no data was computed mod p.

Examples over $\mathbb{Q}(\sqrt{2})$

The field $\mathbb{Q}(\sqrt{2})$ has narrow class number 1, its ring of integers is $\mathbb{Z} \oplus \omega\mathbb{Z}$ with $\omega^2 = 2$. We include data for ideals up to norm 500.

N($\mathfrak{N}$)	gen.	$\mathfrak{N}$	$\mathcal{E}$	$\mathcal{S}_2$	$V_{\mathbb{Z}}$	$\mathrm{E}_{\mathbb{Z}}$	$V_{\mathbb{F}_2}$	$\mathrm{E}_{\mathbb{F}_2}$	$V_{\mathbb{F}_3}$	$\mathrm{E}_{\mathbb{F}_3}$	Notes
49	7	2	2	3	1	0	1	0	1	0	
97	$7\omega - 1$	1	1	5	1	1	1	1	1	1	[3, 97]
98	7ω	1	2	7	2	0	-	-	2	0	[2]
100	10	1	3	7	1	0	-	-	1	0	[2, 5]
112	$-8\omega - 4$	2	7	7	1	0	-	-	1	0	[2]
119	$\omega - 11$	3	3	5	0	0	1	0	0	0	
119	$\omega + 11$	1	3	5	0	0	1	0	0	0	
146	$-9\omega - 4$	1	1	10	0	0	-	-	1	0	[2]
153	$9\omega - 3$	2	1	9	0	0	1	0	-	-	[3]
153	$9\omega - 3$	2	3	9	0	0	1	0	-	-	
161	$2\omega - 13$	3	3	7	2	1	2	1	2	1	[2]
161	$2\omega + 13$	2	3	7	2	1	2	1	2	1	[2]
164	$-4\omega + 14$	2	3	11	1	0	-	-	1	0	[2]
178	$-3\omega + 14$	1	1	12	0	0	-	-	1	0	[2]
193	$-4\omega - 15$	2	1	9	2	2	2	2	2	2	[5]
194	$\omega + 14$	1	1	13	2	2	-	-	2	2	[2, 3]
196	14	1	3	15	0	0	-	-	1	0	[2]
196	14	1	7	15	3	0	-	-	3	0	[2]
200	-10ω	1	3	13	2	0	-	-	2	0	[2, 5]
207	$-3\omega - 15$	1	3	9	0	0	1	0	-	-	[3]
217	$-11\omega + 5$	4	3	11	1	0	1	0	1	0	
217	$11\omega + 5$	3	2	11	1	0	1	0	1	0	
224	$4\omega - 16$	2	14	15	1	0	-	-	1	0	[2]
224	$4\omega - 16$	2	15	15	2	0	-	-	2	0	[2]
225	15	1	1	13	0	0	1	1	-	-	[3, 5]
225	15	1	3	13	2	1	2	1	-	-	[2, 3, 5]
241	$11\omega - 1$	1	1	11	2	2	2	2	2	2	[5]
242	-11ω	1	1	16	0	0	-	-	1	0	[11, 2]
288	-12ω	1	7	19	0	0	-	-	-	-	[2, 3]
288	-12ω	1	15	19	1	0	-	-	-	-	[2, 3]
289	17	3	1	15	0	0	1	0	1	0	
289	17	3	3	15	0	0	1	0	1	0	
292	$4\omega - 18$	2	3	19	1	1	-	-	2	1	[2]
328	$-14\omega + 8$	2	3	21	2	0	-	-	2	0	[2]
329	$-4\omega + 19$	4	3	15	1	0	1	0	1	0	
343	$-14\omega + 7$	1	2	19	1	0	1	0	1	0	[7]
356	$-14\omega - 6$	2	3	23	1	1	-	-	2	1	[2]
361	19	1	1	16	1	1	1	1	1	1	[3, 19]
368	$-4\omega + 20$	2	6	23	0	0	-	-	2	0	[2]
368	$-4\omega + 20$	2	7	23	1	0	-	-	1	0	[2]
369	$6\omega - 21$	1	1	19	0	0	3	1	-	-	[3]
369	$6\omega - 21$	1	3	19	3	2	3	1	-	-	[3]
386	$15\omega + 8$	2	1	25	4	4	-	-	4	4	[2, 5]
388	$-14\omega - 2$	2	3	25	3	3	-	-	3	3	[2, 3]
392	14ω	2	3	31	0	0	-	-	2	0	[2]

392	14ω	2	7	31	4	0	-	-	4	0	[2, 7]
400	20	1	7	25	3	1	-	-	3	1	[2, 5]
401	$-15\omega + 7$	1	1	17	3	3	3	3	3	3	[7]
423	$3\omega + 21$	1	3	19	0	0	1	0	-	-	[3]
425	$15\omega + 5$	1	1	21	0	0	1	0	0	0	
425	$15\omega + 5$	1	3	21	1	0	1	0	1	0	[5]
433	$-2\omega - 21$	1	1	19	3	3	3	3	3	3	[7]
434	$-5\omega - 22$	3	2	31	2	0	-	-	3	0	[2]
434	$-5\omega + 22$	2	3	31	2	0	-	-	3	0	[2, 7]
441	21	2	3	27	0	0	2	1	-	-	[3, 7]
441	21	2	7	27	2	0	2	1	-	-	[3, 7]
448	$-16\omega - 8$	1	14	31	2	0	-	-	2	0	[2]
448	$-16\omega - 8$	1	15	31	4	0	-	-	4	0	[2]
449	$-15\omega - 1$	1	1	19	2	2	2	2	2	2	[5]
450	-15ω	1	3	35	4	2	-	-	-	-	[2, 3, 5]
452	$4\omega - 22$	2	3	29	2	1	-	-	2	1	[2]
466	$3\omega + 22$	2	1	30	0	0	-	-	1	0	[2]
482	$\omega + 22$	2	1	31	4	4	-	-	4	4	[2, 5]
484	22	1	1	31	0	0	-	-	0	0	[11, 2] (*)
484	22	1	2	31	1	1	-	-	2	1	[11, 2]
496	$16\omega - 4$	2	7	31	2	1	-	-	2	1	[2]
497	$4\omega - 23$	2	3	23	3	2	3	1	3	2	[3]
497	$-4\omega - 23$	4	3	23	3	2	3	1	3	2	[3]

(*) The candidate space $V_{\mathbb{F}_5}$ is 1-dimensional and generated by a normalised eigenform. This is the only example of a non-liftable Hilbert modular form in characteristic 5 in the range in which we computed. This example is discussed in more detail in the previous section.

Examples over $\mathbb{Q}(\sqrt{3})$

The field $\mathbb{Q}(\sqrt{3})$ has narrow class number 2, its ring of integers is $\mathbb{Z} \oplus \omega\mathbb{Z}$ with $\omega^2 = 3$. We include data for ideals up to norm 350.

N($\mathfrak{N}$)	gen.	$\mathfrak{N}$	$\mathcal{E}$	$\mathcal{S}_2$	$V_{\mathbb{Z}}$	$\mathrm{E}_{\mathbb{Z}}$	$V_{\mathbb{F}_2}$	$\mathrm{E}_{\mathbb{F}_2}$	$V_{\mathbb{F}_3}$	$\mathrm{E}_{\mathbb{F}_3}$	Notes
25	5	1	1	4	0	0	1	1	0	0	
25	5	1	3	4	0	0	1	1	0	0	
33	$-\omega - 6$	2	3	4	0	0	2	0	-	-	
49	7	1	1	6	0	0	1	1	0	0	
49	7	1	2	6	0	0	1	1	0	0	[7]
52	$-4\omega + 10$	2	2	8	0	0	-	-	1	1	[2]
73	$-3\omega - 10$	1	2	8	0	0	2	1	0	0	
73	$-3\omega - 10$	1	3	8	1	1	1	1	1	1	[2]
75	-5ω	1	1	10	0	0	2	1	-	-	[3]

75	-5ω	1	3	10	0	0	2	1	-	-	[3, 5]
97	$\omega - 10$	1	1	10	0	0	1	1	0	0	
97	$\omega - 10$	1	2	10	0	0	1	1	0	0	
99	$6\omega - 3$	1	3	12	0	0	2	0	-	-	[3]
100	10	1	1	14	0	0	-	-	1	1	[2]
104	$-14\omega + 22$	1	1	14	0	0	-	-	2	1	[2]
117	$3\omega + 12$	1	1	14	0	0	1	1	-	-	[3]
121	11	3	2	12	0	0	2	0	0	0	[11]
146	$13\omega - 19$	1	3	20	2	2	-	-	2	2	[2]
147	-7ω	1	1	18	0	0	2	1	-	-	[3]
148	$-22\omega + 40$	1	2	20	0	0	-	-	1	1	[2]
167	$8\omega - 5$	2	3	12	0	0	2	1	0	0	
169	13	2	1	20	0	0	1	1	1	1	
169	13	2	3	20	1	1	1	1	1	1	[2, 13]
177	$4\omega - 15$	1	3	20	0	0	2	0	-	-	
181	$-5\omega - 16$	1	1	16	0	0	0	0	1	1	
193	$\omega - 14$	2	1	18	0	0	2	1	0	0	
193	$\omega - 14$	2	3	18	1	1	1	1	1	1	[2]
194	$9\omega - 7$	1	2	26	0	0	-	-	2	0	[2]
196	14	1	1	26	0	0	-	-	1	1	[2]
200	$-30\omega + 50$	1	1	26	0	0	-	-	2	1	[2]
208	$-92\omega + 160$	2	2	28	0	0	-	-	3	1	[2]
208	$-92\omega + 160$	2	3	28	0	0	-	-	0	0	[2]
208	$-92\omega + 160$	2	6	28	1	1	-	-	1	1	[2]
219	$10\omega - 9$	2	1	26	0	0	4	1	-	-	[3]
219	$10\omega - 9$	2	3	26	2	2	2	2	-	-	[2, 3]
225	15	1	1	28	0	0	3	2	-	-	[3]
225	15	1	3	28	1	1	3	2	-	-	[3, 5]
241	$-4\omega - 17$	1	1	22	0	0	4	1	0	0	
241	$-4\omega - 17$	1	3	22	3	3	3	3	3	3	[2]
242	$-11\omega + 11$	2	2	36	0	0	-	-	2	0	[11, 2]
244	$-20\omega + 38$	2	2	32	0	0	-	-	1	1	[2]
249	$5\omega - 18$	1	2	28	0	0	2	1	-	-	[3]
249	$5\omega - 18$	1	3	28	2	2	4	1	-	-	[3]
256	16	1	7	30	1	1	-	-	1	1	[2]
275	$10\omega - 5$	2	1	26	0	0	2	1	0	0	
275	$10\omega - 5$	2	3	26	0	0	0	0	2	0	[2, 5]
276	$10\omega - 24$	2	7	46	2	0	-	-	-	-	[2, 3]
286	$-\omega - 17$	2	3	40	0	0	-	-	2	2	[2]
286	$5\omega - 19$	1	3	40	0	0	-	-	2	2	[2]
286	$19\omega - 37$	4	3	40	0	0	-	-	2	2	[2]
289	17	1	1	26	0	0	2	1	0	0	
289	17	1	3	26	1	1	1	1	1	1	[2, 17]
291	$10\omega - 3$	1	1	34	0	0	2	1	-	-	[3]
291	$10\omega - 3$	1	3	34	0	0	2	1	-	-	[3]
292	$32\omega - 58$	1	1	38	0	0	-	-	1	1	[2]

292	$32\omega - 58$	1	3	38	3	3	-	-	3	3	[2]
296	$-22\omega + 34$	1	1	38	0	0	-	-	2	1	[2]
297	$3\omega - 18$	2	1	36	0	0	2	1	-	-	[3]
297	$3\omega - 18$	2	3	36	2	2	4	1	-	-	[3]
313	$4\omega - 19$	2	1	28	0	0	3	2	0	0	
313	$4\omega - 19$	2	3	28	2	2	3	2	2	2	[3]
321	$\omega + 18$	2	3	36	0	0	2	0	-	-	
324	18	1	3	52	1	1	-	-	-	-	[2, 3]
325	$-5\omega + 20$	1	1	34	0	0	2	1	1	1	
325	$-5\omega + 20$	1	3	34	0	0	0	0	2	0	[2, 5]
333	$6\omega + 21$	2	1	38	0	0	1	1	-	-	[3]
337	$-7\omega - 22$	1	1	30	0	0	5	3	0	0	
337	$-7\omega - 22$	1	2	30	4	4	5	3	4	4	[5]
338	$-13\omega + 13$	2	1	52	0	0	-	-	2	2	[2]
338	$-13\omega + 13$	2	3	52	2	2	-	-	2	2	[2, 13]

Examples over $\mathbb{Q}(\sqrt{5})$

The field $\mathbb{Q}(\sqrt{5})$ has narrow class number 1, its ring of integers is $\mathbb{Z} \oplus \omega\mathbb{Z}$ with $\omega = \frac{1+\sqrt{5}}{2}$. We include data for ideals up to norm 500.

N($\mathfrak{N}$)	gen.	$\mathfrak{N}$	$\mathcal{E}$	$\mathcal{S}_2$	$V_{\mathbb{Z}}$	$\mathrm{E}_{\mathbb{Z}}$	$V_{\mathbb{F}_2}$	$\mathrm{E}_{\mathbb{F}_2}$	$V_{\mathbb{F}_3}$	$\mathrm{E}_{\mathbb{F}_3}$	Notes
45	$-6\omega + 3$	1	1	1	0	0	1	0	-	-	[3]
45	$-6\omega + 3$	1	3	1	0	0	1	0	-	-	[5]
95	$2\omega + 9$	2	3	1	0	0	1	0	0	0	[5]
99	$-9\omega + 6$	1	3	1	0	0	1	0	-	-	[3]
121	11	1	3	3	1	0	1	0	1	0	
145	$-11\omega + 3$	2	1	3	0	0	1	0	1	0	[5]
145	$-11\omega + 3$	2	3	3	1	0	1	0	1	0	
176	$-12\omega + 4$	2	6	3	0	0	-	-	1	0	[2]
176	$-12\omega + 4$	2	7	3	1	0	-	-	1	0	[2]
205	$-13\omega + 4$	1	1	5	0	0	1	1	0	0	[5, 41]
205	$-13\omega + 4$	1	3	5	0	0	1	1	0	0	[5]
209	$-\omega + 15$	1	3	3	1	0	1	0	1	0	
209	$\omega + 14$	2	3	3	1	0	1	0	1	0	
225	15	1	1	5	0	0	1	0	-	-	[3, 5]
225	15	1	3	5	0	0	1	0	-	-	[5]
241	$-14\omega + 9$	2	1	5	1	1	1	1	1	1	[3]
244	$-14\omega + 6$	2	1	6	0	0	-	-	1	0	[2]
245	$14\omega - 7$	1	1	5	0	0	1	0	1	0	[5]
245	$14\omega - 7$	1	3	5	0	0	1	0	1	0	[7]
261	$3\omega + 15$	1	1	5	0	0	1	0	-	-	[3]
261	$3\omega + 15$	1	3	5	1	0	1	0	-	-	
275	$15\omega - 5$	1	1	5	0	0	1	1	0	0	[11, 5]

281	$-15\omega+8$	1	1	5	1	1	1	1	1	1	[3]
295	$-3\omega+19$	1	3	5	0	0	1	0	1	0	[5]
304	$-16\omega+4$	2	3	7	0	0	-	-	1	0	[2]
304	$-16\omega+4$	2	7	7	1	0	-	-	1	0	[2]
305	$\omega-18$	2	1	7	0	0	1	1	0	0	[5, 61]
305	$\omega-18$	2	3	7	0	0	1	1	0	0	[5]
320	$16\omega-8$	1	7	7	0	0	-	-	1	0	[2]
320	$16\omega-8$	1	15	7	1	0	-	-	1	0	[2]
341	$\omega-19$	2	2	7	1	0	1	0	1	0	
361	19	1	2	7	2	1	2	1	2	1	[2]
369	$3\omega-21$	2	1	7	0	0	1	0	-	-	[3]
369	$3\omega-21$	2	3	7	0	0	1	0	-	-	
380	$-4\omega-18$	2	1	9	0	0	-	-	1	0	[2, 5]
395	$2\omega-21$	1	3	7	0	0	1	0	0	0	[5]
405	$-18\omega+9$	1	1	9	0	0	1	0	-	-	[3]
405	$-18\omega+9$	1	3	9	0	0	1	0	-	-	[3, 5]
409	$3\omega-22$	2	1	7	1	1	1	1	1	1	[3]
421	$4\omega+19$	1	1	8	1	1	1	1	1	1	[3]
436	$2\omega+20$	2	1	10	0	0	-	-	1	0	[2]
441	21	1	1	9	0	0	1	1	-	-	[3, 7]
441	21	1	3	9	0	0	1	1	-	-	[3, 7]
445	$-19\omega+7$	2	1	9	0	0	1	0	1	0	[5]
445	$-19\omega+7$	2	3	9	1	0	1	0	1	0	
464	$4\omega-24$	2	7	9	1	0	-	-	1	0	[2]
475	$-20\omega+5$	2	3	9	0	0	1	0	0	0	[5]
484	22	3	3	11	2	0	-	-	2	1	[11, 2]
495	$-3\omega+24$	1	7	11	0	0	1	1	-	-	[11, 3, 5]
496	$20\omega-8$	1	3	11	0	0	-	-	1	0	[2]
496	$20\omega-8$	1	7	11	2	1	-	-	2	1	[2]

Examples over $\mathbb{Q}(\sqrt{6})$

The field $\mathbb{Q}(\sqrt{6})$ has narrow class number 2, its ring of integers is $\mathbb{Z}\oplus\omega\mathbb{Z}$ with $\omega^2=6$. We include data for ideals up to norm 100.

N($\mathfrak{N}$)	gen.	$\mathfrak{N}$	$\mathcal{E}$	$\mathcal{S}_2$	$V_{\mathbb{Z}}$	$\mathrm{E}_{\mathbb{Z}}$	$V_{\mathbb{F}_2}$	$\mathrm{E}_{\mathbb{F}_2}$	$V_{\mathbb{F}_3}$	$\mathrm{E}_{\mathbb{F}_3}$	Notes
25	5	3	1	12	0	0	2	0	0	0	[5]
25	5	3	3	12	0	0	2	0	0	0	[5]
49	7	1	1	16	0	0	1	1	0	0	
49	7	1	2	16	0	0	1	1	0	0	[7]
57	$2\omega+9$	2	2	24	0	0	1	1	-	-	[3]
57	$2\omega+9$	2	3	24	1	1	1	1	-	-	[2]
73	$-4\omega-13$	1	2	22	0	0	3	2	0	0	
73	$-4\omega-13$	1	3	22	2	2	3	2	2	2	[3]
75	$13\omega+33$	1	3	28	0	0	1	1	-	-	[3]

75	$5\omega + 15$	3	3	34	0	0	2	1	-	-	[3]
75	$\omega + 9$	2	3	28	0	0	1	1	-	-	[3]
76	$2\omega + 10$	1	2	32	0	0	-	-	1	1	[2]
76	$2\omega + 10$	1	3	32	0	0	-	-	0	0	[2]
97	$-2\omega - 11$	1	1	28	0	0	2	1	0	0	
97	$-2\omega - 11$	1	3	28	1	1	1	1	1	1	[2]
100	$48\omega + 118$	1	2	46	1	1	-	-	1	1	[2]
100	$20\omega + 50$	3	2	58	0	0	-	-	2	2	[2, 5]
100	$20\omega + 50$	3	7	58	4	2	-	-	4	2	[2, 5]

Thoughts for the Future

In its current form, our algorithm handles adelic q-expansions with complex coefficients both in parallel and partial weight, and q-expansions with coefficients in positive characteristic, but only in parallel weight. As discussed in the thesis, there are obstructions to a direct generalisation of our algorithm to q-expansions of Hilbert modular form of partial weight in finite fields. Specifically, the multiplication and division of adelic power series as defined in the thesis do not extend directly to positive characteristic.

A future step could attempt to resolve this and other possible obstructions in order to extend the code to partial weight in positive characteristic. Furthermore, one wonders if this obstruction could be a symptom of a more fundamental flaw of the adelic q-expansion of Hilbert modular forms of partial weight over finite fields.

Even though the algorithm described in this thesis is able to produce plenty of examples of non-liftable Hilbert modular eigenforms, in the future we would like to find a non-liftable Hilbert modular eigenform of weight 1 such that the associated Galois representation has so called big image. So far our brute force approach of computing in all levels and all characters has not yielded such an example. However, if such an example exists, our algorithms will (eventually) compute it.

Bibliography

[1] F. Andreatta and E. Z. Goren. Hilbert modular forms: mod p and p-adic aspects. *Mem. Amer. Math. Soc.*, 173(819):vi+100, 2005.

[2] Peter R. Bending. Curves of genus 2 with $\sqrt{2}$ multiplication. 1999.

[3] Nicolas Billerey and Luis V. Dieulefait. Explicit large image theorems for modular forms. *J. Lond. Math. Soc. (2)*, 89(2):499–523, 2014.

[4] Jan Hendrik Bruinier, Gerard van der Geer, Günter Harder, and Don Zagier. *The 1-2-3 of modular forms*. Universitext. Springer-Verlag, Berlin, 2008. Lectures from the Summer School on Modular Forms and their Applications held in Nordfjordeid, June 2004, Edited by Kristian Ranestad.

[5] Joe P. Buhler. *Icosahedral Galois representations*. Lecture Notes in Mathematics, Vol. 654. Springer-Verlag, Berlin-New York, 1978.

[6] Kevin Buzzard. Computing weight one modular forms over $\mathbb{C}$ and $\overline{\mathbb{F}}_p$. In *Computations with modular forms*, volume 6 of *Contrib. Math. Comput. Sci.*, pages 129–146. Springer, Cham, 2014.

[7] Henri Darmon, Fred Diamond, and Richard Taylor. Fermat's last theorem. In *Elliptic curves, modular forms & Fermat's last theorem (Hong Kong, 1993)*, pages 2–140. Int. Press, Cambridge, MA, 1997.

[8] Samit Dasgupta, Henri Darmon, and Robert Pollack. Hilbert modular forms and the Gross-Stark conjecture. *Ann. of Math. (2)*, 174(1):439–484, 2011.

[9] Lassina Dembélé and John Voight. Explicit methods for Hilbert modular forms. In *Elliptic curves, Hilbert modular forms and Galois deformations*, Adv. Courses Math. CRM Barcelona, pages 135–198. Birkhäuser/Springer, Basel, 2013.

[10] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2005.

[11] Mladen Dimitrov and Gabor Wiese. Unramifiedness of Galois representations attached to weight 1 Hilbert modular eigenforms mod p.

[12] Francesc Fité, Kiran S. Kedlaya, Víctor Rotger, and Andrew V. Sutherland. Sato-Tate distributions and Galois endomorphism modules in genus 2. *Compos. Math.*, 148(5):1390–1442, 2012.

[13] Eberhard Freitag. *Hilbert modular forms*. Springer-Verlag, Berlin, 1990.

[14] Haruzo Hida. *p-Adic automorphic forms on Shimura varieties*. Springer Monographs in Mathematics. Springer-Verlag, New York, 2004.

[15] Christian Johansson. On the Sato-Tate conjecture for non-generic abelian surfaces. *arXiv:1307.6478v5*, 2015.

[16] Kiran S. Kedlaya and Andrew V. Sutherland. Computing L-series of hyperelliptic curves. In *Algorithmic number theory*, volume 5011 of *Lecture Notes in Comput. Sci.*, pages 312–326. Springer, Berlin, 2008.

[17] Koopa Tak-Lun Koo, William Stein, and Gabor Wiese. On the generation of the coefficient field of a newform by a single Hecke eigenvalue. *J. Théor. Nombres Bordeaux*, 20(2):373–384, 2008.

[18] Kai-Wen Lan and Junecue Suh. Liftability of mod p cusp forms of parallel weights. *Int. Math. Res. Not. IMRN*, (8):1870–1879, 2011.

[19] Serge Lang. *Introduction to modular forms*, volume 222 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1995. With appendixes by D. Zagier and Walter Feit, Corrected reprint of the 1976 original.

[20] Serge Lang and Hale Trotter. *Frobenius distributions in GL_2-extensions*. Lecture Notes in Mathematics, Vol. 504. Springer-Verlag, Berlin-New York, 1976. Distribution of Frobenius automorphisms in GL_2-extensions of the rational numbers.

[21] D. Loeffler. Images of adelic Galois representations for modular forms. *ArXiv e-prints*, November 2014.

[22] Richard A. Moy and Joel Specter. There exist non-CM Hilbert modular forms of partial weight 1. *Int. Math. Res. Not. IMRN*, (24):13047–13061, 2015.

[23] V. Kumar Murty. Frobenius distributions and Galois representations. In *Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996)*, volume 66 of *Proc. Sympos. Pure Math.*, pages 193–211. Amer. Math. Soc., Providence, RI, 1999.

[24] Jürgen Neukirch. *Algebraic number theory*, volume 322 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1999. Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[25] M. Rapoport. Compactifications de l'espace de modules de Hilbert-Blumenthal. *Compositio Math.*, 36(3):255–335, 1978.

[26] K. A. Ribet. Endomorphism algebras of abelian varieties attached to newforms of weight 2. In *Seminar on Number Theory, Paris 1979–80*, volume 12 of *Progr. Math.*, pages 263–276. Birkhäuser, Boston, Mass., 1981.

[27] Kenneth A. Ribet. On l-adic representations attached to modular forms. *Invent. Math.*, 28:245–275, 1975.

[28] Kenneth A. Ribet. Twists of modular forms and endomorphisms of abelian varieties. *Math. Ann.*, 253(1):43–62, 1980.

[29] George Johann Schaeffer. *The Hecke Stability Method and Ethereal Forms*. ProQuest LLC, Ann Arbor, MI, 2012. Thesis (Ph.D.)–University of California, Berkeley.

[30] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York-Heidelberg, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[31] Jean-Pierre Serre. Un critère d'indépendance pour une famille de représentations ℓ-adiques. *Comment. Math. Helv.*, 88(3):541–554, 2013.

[32] Goro Shimura. The special values of the zeta functions associated with Hilbert modular forms. *Duke Math. J.*, 45(3):637–679, 1978.

[33] Goro Shimura. Corrections to: "On the Eisenstein series of Hilbert modular groups" [Rev. Mat. Iberoamericana **1** (1985), no. 3, 1–42; MR0836282 (87h:11038)]. *Duke Math. J.*, 55(4):838, 1987.

[34] William Stein. *Modular forms, a computational approach*, volume 79 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2007. With an appendix by Paul E. Gunnells.

[35] W. A. Stein et al. *Sage Mathematics Software (Version 6.3)*. The Sage Development Team, 2014. `http://www.sagemath.org`.

[36] Yuuki Takai. An analogue of Sturm's theorem for Hilbert modular forms. *Algebra Number Theory*, 7(4):1001–1018, 2013.

[37] Gerard van der Geer. *Hilbert modular surfaces*, volume 16 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1988.

[38] Jasper Van Hirtum. On the Distribution of Frobenius of Weight 2 Eigenforms with Quadratic Coefficient Field. *Experimental Mathematics*, 26(2):165–188, 2017.

[39] John Wilson. Explicit moduli for curves of genus 2 with real multiplication by $\mathbb{Q}(\sqrt{5})$. *Acta Arith.*, 93(2):121–138, 2000.