UNIVERSITAT DE BARCELONA

ADVANCED MATHEMATICS
MASTER'S FINAL PROJECT

Abelian surfaces, Siegel modular forms, and the Paramodularity Conjecture

Author:
Enric Florit Zacarías

Supervisor:
Dr. Xavier Guitart Morales

Facultat de Matemàtiques i Informàtica

June 28, 2021

Contents

Abstract

This master's thesis studies the modularity of elliptic curves over the rationals and two generalizations. The first is a theorem of Ribet based on Serre's modularity conjecture, asserting that all abelian varieties of GL_2-type come from the Eichler-Shimura construction. The second is the Paramodularity Conjecture, which says that all abelian surfaces with trivial endomorphism ring have an associated Siegel paramodular form with coinciding L-function.

We give background on abelian varieties, Galois representations and classical modular forms, all necessary to state modularity. Further, we explain the Eichler-Shimura construction and relation. We then study the basic theory of Siegel modular forms with respect to the paramodular group. The final chapter gives the statement of the Paramodularity Conjecture, along with a commentary of what a generalization to GL_4-type abelian varieties could look like.

An important part of this project is centered on explicit computation of Fourier-Siegel coefficients, and special care has been taken to present computational principles which are scattered across the literature. We also provide the first public implementation of the specialization method that was used to prove the first instance of the Paramodularity Conjecture.

Acknowledgements

El màster de matemàtiques és un període d'estudi extremadament curt, i sorprèn que un treball com aquest pugui tenir més de tres o quatre frases d'agraïment. No obstant això, i després d'un any i mig de distanciament social i treball des de casa, no voldria deixar passar l'oportunitat de mencionar algunes persones sense les quals la realització d'aquest projecte hauria estat molt difícil, si no directament impossible.

Vull agrair al meu tutor Xevi per tot el que m'ha ensenyat. La seva ajuda m'ha permès introduir-me en un món complex, ple de matemàtiques noves i desconegudes per mi. En especial, agraeixo que m'hagi respost sempre les preguntes i dubtes interminables, que m'hagi escoltat quan feia volar coloms amb conjectures improbables i, en resum, agraeixo la seva paciència infinita.

Es diu que un viatge pot ser valorat pels qui t'hi acompanyen. Per aquest motiu, vull agrair als meus companys. A David, porque nos hemos ayudado siempre en este duro máster. En nada terminamos. A l'Ignasi, com va dir ell, per pensar junts. Al Gerard i l'Arnau, amb qui hem seguit acompanyant-nos malgrat la distància. A Dani, por su amistad, carácter, y su ayuda en todo momento. A Marta, porque ha sido un placer habernos conocido, y por leerte el trabajo entero en tan poco tiempo. A tots els companys del màster i del SIMBa, desitjant retrobar-nos en persona en un futur pròxim.

Vull agrair als meus pares, Toni i Loli, pel seu suport en uns temps tan difícils. Sé com és de complicat confiar en una activitat tan inexplicable i etèria com la que faig, i espero que aviat en puguem veure els fruits.

Tanco els agraïments amb la persona més important per mi. Gràcies, Ana, per tot el teu suport i tot el que fas per mi. Espero poder ajudar-te tant com tu m'ajudes a mi, durant molt de temps.

Introduction

Between the 1990s and the 2000s, the following result was proven:

Theorem (Modularity Theorem)**.** *All elliptic curves over* $\mathbb{Q}$ *are modular.*

This thesis gives an overview of the various topics involved in the Modularity Theorem and its generalizations to abelian varieties defined over $\mathbb{Q}$, both proven and conjectural. It will involve studying at least two kinds of objects, which a priori may seem unrelated: abelian varieties and modular forms. Abelian varieties are higher-dimensional analogues of elliptic curves, which are algebraic curves of genus 1. Each abelian variety has an associated meromorphic function, called its L-function, which encodes arithmetic data about it. On the other hand, a classical modular form is an holomorphic function on the upper half plane with some symmetries with respect to a matrix group. Modular forms also have L-functions, defined in terms of their eigenvalues for some linear operators called Hecke operators.

We say an abelian variety is modular if its L-function is equal (or more broadly, if it is related) to the L-function of a modular form. For instance, by the Modularity Theorem each elliptic curve defined over $\mathbb{Q}$ has a corresponding classical modular form with rational Hecke eigenvalues, and these eigenvalues coincide with arithmetic data coming from the curve. To extend the collection of modular abelian varieties, one has to consider modular forms with eigenvalues lying in some finite extension of $\mathbb{Q}$. This being said, our first goal is to explain the ingredients of modularity of a class of abelian varieties called of GL_2-type.

The correspondence with classical modular forms does not suffice to assert modularity for all abelian varieties. To add other types of varieties to the list one introduces Siegel paramodular forms, which are holomorphic functions in a certain space of 2-by-2 symmetric matrices. These have a theory analogue to that of classical modular forms, and Hecke operators and L-functions are also defined. The Paramodularity Conjecture states that certain abelian surfaces are paramodular, that is, their L-functions coincide with the L-functions of some paramodular forms. This conjecture is in its early stages, and very few cases have been proven so far. The second goal of this thesis is to explain the statement of the conjecture, the current progress, and how one can compute the necessary Hecke eigenvalues to verify examples of paramodularity.

Let us outline the ideas of modularity by looking at elliptic curves. An elliptic curve is given by the projectivization of a Weierstrass equation

$$E : y^2 = x^3 + Ax + B, \tag{1}$$

where A and B lie in some field. It is important that the curve is smooth, for that, we ask for its discriminant $\Delta = 4A^3 + 27B^2$ to be nonzero. We will be interested in curves defined either over finite extensions K of $\mathbb{Q}$ (which are called number fields), the complex numbers $\mathbb{C}$, or finite fields $\mathbb{F}_q$ with q a power of a prime p.

Elliptic curves are interesting for many reasons, but one of the most prominent is that their points form abelian groups. More specifically, if E is a curve defined over a field K and $E(K)$ denotes the set of points defined over K satisfying an equation of the form (1) together with the unique point at infinity, then $E(K)$ is an abelian group. The group law can be described geometrically, see for example [Sil09, § III.2].

The remarkable theorem of Mordell and Weil [Sil09, § VIII.4] tells us that if E is defined over $\mathbb{Q}$, then the group $E(\mathbb{Q})$ is finitely generated, so that

$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r \tag{2}$$

for some finite group T and some nonnegative integer r.

If an elliptic curve E is defined over $\mathbb{Q}$, then via a change of variables we can ensure that it has the form $E : y^2 = x^3 + Ax + B$ with A, B integers. We can then reduce modulo a prime p not dividing the discriminant to obtain a curve

$$\tilde{E} : y^2 = x^3 + \tilde{A}x + \tilde{B}$$

defined over $\mathbb{F}_p$. Clearly the group $\tilde{E}(\mathbb{F}_p)$ is finite. There is a straightforward way to count the number of points: for each $x \in \mathbb{F}_p$, we only need to count the number of solutions to $y^2 \equiv c \bmod p$, for $c = x^3 + \tilde{A}x + \tilde{B}$. This number of solutions is 0 or 2 with roughly the same probability. Accounting for the unique point “at infinity”, this means that $\#\tilde{E}(\mathbb{F}_p) \approx p + 1$. To measure the deviation from this approximation, one defines the quantity

$$a_p := p + 1 - \#\tilde{E}(\mathbb{F}_p).$$

When p divides the discriminant of E we can do a similar reduction, but the resulting curve over $\mathbb{F}_p$ will be singular. In that case, we define $a_p = -1, 0$ or 1 depending on the type of singularity that appears. The values a_p satisfy the Hasse bound,

$$|a_p| \leq 2\sqrt{p},$$

for all primes p. The L-function of E is then defined as the product

$$L(E, s) = \prod_{p \nmid \Delta_{min}} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p \mid \Delta_{min}} \frac{1}{1 - a_p p^{-s}},$$

where s is a complex variable and Δ_{min} is the minimal discriminant of E. Using the Hasse bound, one can prove that this product converges in the right half plane $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > \frac{3}{2}\}$. By expanding the product, we obtain an expression for the L-function as the Dirichlet series

$$L(E,s) = \sum_{n \geq 1} \frac{a_n}{n^s}$$

which may remind the reader of other L-functions, such as the Riemann zeta function. The values a_n are defined by this equality, in particular, the a_p for p prime remain unchanged. The L-function of E should give us information about E. This is the content of the weak Birch and Swinnerton-Dyer conjecture, which predicts that the rank in (2) should satisfy

$$r = \mathrm{ord}_{s=1} L(E,s),$$

the order of vanishing of L at 1.

A modular form is a holomorphic function

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

where $\mathcal{H}$ is the complex upper half plane,

$$\mathcal{H} = \{z \in \mathbb{C} \mid \mathrm{Im}(z) > 0\},$$

and f satisfies some symmetry conditions with respect to a finite index subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, and has some regularity conditions "at infinity". The precise definition of the symmetry with respect to Γ is given in Section 1.2, the only property needed here is the fact that, for all $z \in \mathcal{H}$,

$$f(z+1) = f(z).$$

This gives us a Fourier expansion for f, and the regularity conditions ensure that it has the form

$$f(z) = \sum_{n \geq 0} a_n(f) e^{2\pi i z}.$$

One defines, for every prime p, certain Hecke operators T_p on the spaces of modular forms. The Hecke operators can be diagonalized simultaneously, so that there are *eigenforms* f such that

$$T_p f = a_p(f) f$$

for all primes p. If $f(z) = \sum_{n \geq 0} a_n e^{2\pi i z}$ is an eigenform, then its L-function is defined to be the series

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

This is seen to extend to a meromorphic function on the whole complex plane. We say an elliptic curve is modular if its L-function equals that of a modular eigenform.

To each modular eigenform f (of weight 2) we can always associate an abelian variety. This will be an elliptic curve if all the Fourier coefficients of f are rationals, we denote it by E_f. The relation of Eichler and Shimura implies that the L-functions of f and E_f coincide, making this the first case of modular elliptic curves. The Shimura-Taniyama-Weil conjecture, now the Modularity Theorem, asserted that all elliptic curves over $\mathbb{Q}$ either appeared with this construction, or were isogenous to some E_f for an eigenform f.

In particular, if E is an elliptic curve defined over $\mathbb{Q}$, the Modularity Theorem says that $L(E,s)$ extends to a meromorphic function on all of $\mathbb{C}$. This gives us the first step to attack the Birch and Swinnerton-Dyer conjecture. In fact, the proofs of the only known cases of this conjecture ($\operatorname{ord}_{s=1} L(E,s) = 0$ and 1) rely heavily on the modularity of E.

We can ask for a generalization of the Modularity Theorem where we substitute elliptic curves by a higher-dimensional object. The relevant concept here is that of abelian varieties, which are projective algebraic varieties whose points have a group structure defined geometrically. A useful tool to work with abelian varieties are Jacobians: to each algebraic curve C of genus g, we associate an abelian variety $\operatorname{Jac}(C)$ and a morphism $C \to \operatorname{Jac}(C)$, such that every morphism to an abelian variety $C \to A$ factors through $\operatorname{Jac}(C)$.

Chapter 1 explains the case of abelian varieties over $\mathbb{Q}$ of GL_2-type, for which modularity is completely solved. These are varieties whose endomorphism algebra is a number field of degree coinciding with the dimension of the variety, which is also the case of elliptic curves. We first explain how to generalize the L-function to a higher-dimensional variety through Galois representations. After that, we give the relevant definitions and properties of classical modular forms. Then, we show how to associate a GL_2-type abelian variety to a modular eigenform, with what is known as the Eichler-Shimura construction. Finally we present the theorem of Ribet, which completes the construction in the reverse direction.

The first case of a variety which is not of GL_2-type is that of an abelian surface whose endomorphism ring is isomorphic to $\mathbb{Z}$. This case does not arise in the Eichler-Shimura construction, and the L-function of such a variety is given by a product of degree-4 factors which do not split into smaller, degree-2 factors.

To find the corresponding complex analytic functions we need to look at Siegel modular forms, which are holomorphic functions on the Siegel upper half space

$$\mathcal{H}_2 = \left\{ M \in \mathrm{Mat}_{2\times 2}^{sym}(\mathbb{C}) \mid \mathrm{Im}(M) \text{ is positive definite} \right\},$$

where $\mathrm{Mat}_{2\times 2}^{sym}(\mathbb{C})$ is the set of 2-by-2 complex symmetric matrices. We also ask for symmetry with respect to a matrix group and some regularity conditions.

Chapter 2 develops the theory of Siegel modular forms. In particular, we consider forms with respect to certain groups $K(N)$ of $\mathrm{Sp}_4(\mathbb{Z})$ called paramodular groups. We first show the properties of their Fourier expansions, and show they can be written as

$$f(Z) = \sum_{T \geq 0} a(T; f) e^{2\pi i \operatorname{Tr}(TZ)}$$

where T runs over positive semidefinite matrices of a certain level.

On each space of Siegel paramodular forms, several Hecke operators are defined. An eigenform is a paramodular form $f : \mathcal{H}_2 \to \mathbb{C}$ which is an eigenvector with respect to all Hecke operators. From the eigenvalues of f, we can build a meromorphic L-function $L(f, s)$. The Paramodularity Conjecture predicts that, for every abelian surface $A_{/\mathbb{Q}}$ with endomorphism ring $\mathbb{Z}$, there is a Siegel paramodular form f_A such that

$$L(A, s) = L(f_A, s).$$

We also say A is paramodular.

The difficulty in working with Siegel modular forms is twofold: first, constructing them can be difficult; second, one needs very large amounts of Fourier coefficients to compute Hecke eigenvalues, requiring a lot of computational power. The last part of our second chapter focuses on the method of specialization outlined in [PY07] and refined in [Bru+19]. With this method, one can compute lots of Hecke eigenvalues without having to compute as many Fourier coefficients.

The first case of the Paramodularity Conjecture that was proven was given in [Bru+19, Theorem 1.2.1], and is as follows.

Theorem. *Consider the Jacobian $A = \operatorname{Jac}(C)$ of the curve*

$$C : y^2 + (x^3 + x^2 + x + 1)y = -x^2 - x,$$

which is an abelian surface of conductor 277. Then A is paramodular, that is, there is a Siegel paramodular form f_A of level 277 such that

$$L(A, s) = L(f_A, s).$$

We have implemented the method of specialization using Sage, and all the source code is now available in [Flo21]. This is the first public implementation of the method. With enough computational resources, it allows for an independent check of the Paramodularity Conjecture for level $N = 277$.

We give the current form of the conjecture in Chapter 3. We explain the current evidence towards its validity, a task involving techniques from representation theory, computational number theory, and the algorithms explained in Chapter 2. Finally, we discuss the generalization of the Paramodularity Conjecture to abelian varieties of GL_4-type.

At the end of this work, we will have given the full expected picture for abelian surfaces, including the Eichler-Shimura construction in the proven GL_2 case, and some of the known instances of the paramodular case.

Chapter 1

GL2-type abelian varieties

This chapter gives the Eichler-Shimura construction and the statements of the Modularity Theorem, as well as Ribet's theorem on GL_2-type abelian varieties. We first give the necessary background on abelian varieties, Jacobians and Galois representations, and we also give the theory of classical modular forms and their Hecke operators.

1.1 Abelian varieties

Let k be a field. We say an algebraic variety X over k is a group variety if it has at a point $e \in X(k)$ and two morphisms

$$\begin{aligned} i\colon X &\to X \\ m\colon X \times X &\to X \end{aligned}$$

inducing a group structure on the points $X(\bar{k})$ defined over an algebraic closure $\bar{k}$ of k. A group variety A is called an abelian variety if it is complete, in that case, one can prove A is projective. By the rigidity property abelian varieties are commutative groups. The (affine) group variety $\mathrm{GL}_n(k)$ is not an abelian variety for any field k. Elliptic curves, on the other hand, are the simplest examples of abelian varieties.

We will be interested in abelian varieties over $\mathbb{Q}$. Since $\mathbb{Q}$ injects in $\mathbb{C}$ it is convenient to study complex abelian varieties first. Any abelian variety $A_{/\mathbb{Q}}$ has a complex analytic structure, and the morphisms m and i give $A(\mathbb{C})$ the structure of a complex Lie group.

Definition 1.1. *A lattice is a discrete subgroup $\Lambda \subset \mathbb{C}^g$. Given a lattice Λ of maximal $\mathbb{Z}$-rank $2g$, the quotient $\mathbb{C}^g/\Lambda$ is called a g-dimensional complex torus.*

Theorem 1.2. *Let $A_{/\mathbb{C}}$ be a g-dimensional abelian variety. Then there is a lattice $\Lambda \subset \mathbb{C}^g$ such that, as complex Lie groups, $A \cong \mathbb{C}^g/\Lambda$.*

However, most complex tori are not abelian varieties, in the sense that they cannot be embedded in projective space. A complex torus $\mathbb{C}^g/\Lambda$ is an abelian variety if and only if admits a nondegenerate Riemann form, which we now define.

Definition 1.3. *We say a pairing $H\colon \mathbb{C}\times\mathbb{C}\to\mathbb{C}$ is a Hermitian form if it is linear in the first variable and $H(v,w)=\overline{H(w,v)}$. We say H is a Riemann form for Λ if, in addition, $\operatorname{Im} H$ takes integer values on $\Lambda\times\Lambda$. We say it is nondegenerate if it is positive definite.*

See [HS00, § A.5.2] for an account on the relation between Riemann forms, ample divisors and projective embeddings.

There is a natural correspondence between Hermitian forms $H:\mathbb{C}^g\times\mathbb{C}^g\to\mathbb{C}$ and real bilinear alternating forms $E:\mathbb{C}^g\times\mathbb{C}^g\to\mathbb{R}$ satisfying $E(ix,iy)=E(x,y)$. This correspondence is given by the maps

$$H\mapsto E=\operatorname{Im} H \qquad \text{and} \qquad E\mapsto H(x,y)=E(ix,y)+iE(x,y).$$

Example 1.4. *Let τ be a symmetric $g\times g$ matrix such that $\operatorname{Im}\tau$ is positive definite (from now on, we write $\operatorname{Im}\tau>0$). Then*

$$H(z,w)=z^t(\operatorname{Im}\tau)^{-1}\overline{w}$$

defines a nondegenerate Riemann form with respect to the lattice $\mathbb{Z}^g+\tau\mathbb{Z}^g$. Therefore $\mathbb{C}^g/(\mathbb{Z}^g+\tau\mathbb{Z}^g)$ is a complex abelian variety. A basis of the lattice is given by the columns of the block matrix

$$(Id_g \mid \tau)\,.$$

Given a lattice Λ and a nonzero $\alpha\in\mathbb{C}$, the homothety $\Lambda\mapsto\alpha\Lambda$ induces an isomorphism of complex tori $\mathbb{C}^g/\Lambda\to\mathbb{C}^g/\alpha\Lambda$. In the case of $g=1$, we may use an homothety to ensure that $\Lambda=\langle 1,\tau\rangle$ with $\operatorname{Im}(\tau)>0$. It follows that 1-dimensional tori are always abelian varieties. These are usually known as elliptic curves, and we can embed them into $\mathbb{P}^2$ via Weierstrass' $\wp$ function and its derivative.

Given a nondegenerate bilinear alternating form E taking integer values on a lattice Λ, a result of Frobenius says there is a basis of Λ such that the matrix of E has the form

$$\begin{pmatrix} 0 & D \\ -D & 0 \end{pmatrix}, \tag{1.1}$$

where $D=\operatorname{diag}(d_1,\dots,d_g)$, each d_i is an integer, and $d_i\mid d_{i+1}$. Two Riemann forms H_1, H_2 are called equivalent if $nH_1=mH_2$ for positive integers m,n.

Definition 1.5. *A polarization on an abelian variety $A_{/\mathbb{C}}$ is an equivalence class of Riemann forms on A, defining a particular projective embedding.*

If H is a class representative, and setting $E=\operatorname{Im} H$ and $D=\operatorname{diag}(d_1,\dots,d_g)$ as in (1.1), the vector $(d_1,\dots,d_g)$ is called the polarization type of A. We say A is principally polarized if $D=Id$.

We deal now with morphisms between abelian varieties.

Definition 1.6. *Let A and B be abelian varieties defined over k. A morphism of abelian varieties is a morphism $\phi : A \to B$ inducing a group homomorphism $A(\bar{k}) \to B(\bar{k})$.*

Given two such abelian varieties, $\mathrm{Hom}(A, B)$ denotes the group of morphisms between A and B which are defined over k. If l is an extension of k, the group of morphisms defined over l is notated $\mathrm{Hom}(A_l, B_l)$. Similarly, we write $\mathrm{End}(A)$, the endomorphism ring (with addition and composition), and $\mathrm{End}(A_l)$. In particular, if $\bar{k}$ is an algebraic closure of k then $\mathrm{End}(A_{\bar{k}})$ is the *full* endomorphism ring of A. We also write $\mathrm{End}^0(A)$ for the *endomorphism algebra* $\mathrm{End}(A) \otimes k$.

Definition 1.7. *A morphism of abelian varieties $\phi : A \to B$ is said to be an isogeny if:*

(i) *ϕ is surjective,*

(ii) $\ker \phi$ *is finite,*

(iii) $\dim A = \dim B$.

Note that any two of these conditions implies the third. The isogeny is defined over k if ϕ is given locally by rational functions with coefficients in k.

Being isogenous is an equivalence relation, this will appear several times in the rest of the chapter: all statements on L-functions, representations and modularity are always up to isogeny.

If A and B are elliptic curves, then any non-constant morphism of elliptic curves between them is an isogeny. This is not necessarily true in higher dimension. However, the image of an isogeny $\phi : A \to B$ is an abelian subvariety of B. Therefore, if we consider simple abelian varieties A and B of the same dimension (they have no proper abelian subvarieties), then either $\mathrm{Hom}(A, B) = 0$, or every non-constant morphism $A \to B$ is an isogeny.

For all nonzero integer n, the multiplication-by-n endomorphism $[n] : A \to A$ is an isogeny. It can be seen that there is an injection $\mathbb{Z} \hookrightarrow \mathrm{End}(A)$, in particular, the endomorphism ring of an abelian variety is a ring of characteristic zero.

A variety A defined over the finite field $\mathbb{F}_p$ always has an endomorphism σ_p (which is an isogeny) called the Frobenius endomorphism. This corresponds to raising every coordinate of a point to its pth power (for instance, it takes a point (x, y) on an elliptic curve to (x^p, y^p)). Being an endomorphism, we have a dual endomorphism σ_p^* satisfying

$$\sigma_p \circ \sigma_p^* = [p],$$

the multiplication-by-p endomorphism. The Frobenius σ_p is used to count points over $\mathbb{F}_p$, since $A(\mathbb{F}_p) = \ker(\sigma_p - [1])$.

Before moving on to Jacobians, we mention briefly the notion of conductor of an abelian variety $A_{/\mathbb{Q}}$. We explain the case of elliptic curves. Any elliptic curve $E_{/\mathbb{Q}}$ has an equation of the form

$$E : y^2 = x^3 + Ax + B$$

with A, B integers, and such that the (nonzero) discriminant $\Delta = 4A^3 + 27B^2$, A and B have minimal valuation at all primes. We can then reduce the equation modulo a prime p, and this will yield a projective curve $\tilde{E}$ over $\mathbb{F}_p$. We say E has good reduction at p if $\tilde{E}$ is nonsingular, otherwise, it has bad reduction. Depending on the type of singularity that appears we further say $\tilde{E}$ has multiplicative reduction (if the singular point is a node) or additive reduction (if the singular point is a cusp).

The conductor of E is defined to be the integer $N = \prod_p p^{f_p}$ where

$$f_p = \begin{cases} 0 & \text{if } E \text{ has good reduction at } p, \\ 1 & \text{if } E \text{ has multiplicative reduction at } p, \\ 2 & \text{if } E \text{ has additive reduction at } p \text{ and } p \notin \{2,3\}, \\ 2+\delta_p & \text{if } E \text{ has additive reduction at } p \text{ and } p \in \{2,3\}. \end{cases}$$

We have $\delta_2 \leq 6$ and $\delta_3 \leq 3$, although their precise computation requires quite more work. Similarly, one can define the reduction of a variety $A_{/\mathbb{Q}}$ modulo a prime by using equations with integer coefficients, and then we can also define a notion of the conductor. The conductor is an invariant of the isogeny class.

1.1.1 Jacobians

If $C_{/\mathbb{Q}}$ is a projective algebraic curve, its $\mathbb{C}$-points have a complex analytic structure, so C is also a Riemann surface. Given a base point $P_0 \in C$, we will now construct the Jacobian $\mathrm{Jac}(C)$ of C, a complex abelian variety with a map $C \to \mathrm{Jac}(C)$ sending P_0 to the identity of $\mathrm{Jac}(C)$. The construction will have the universal property that given another abelian variety X and a morphism of complex varieties $C \to X$ sending P_0 to the identity of X, there will be a unique morphism of complex abelian varieties $\mathrm{Jac}(C) \to X$ making the following diagram commute:

$$\begin{tikzcd} C \arrow[r] \arrow[dr] & \mathrm{Jac}(C) \arrow[d, dashed] \\ & X \end{tikzcd}$$

The Jacobian $\mathrm{Jac}(C)$ is an abelian variety of dimension equal to the genus g of the curve. If $H_1(C, \mathbb{Z})$ is the singular homology of $C(\mathbb{C})$, and $\Omega^1(C)$ are the holomorphic differentials on $C(\mathbb{C})$, then

$$\mathrm{rank}_{\mathbb{Z}} H_1(C, \mathbb{Z}) = 2g \qquad \text{and} \qquad \dim_{\mathbb{C}}(\Omega^1(C))) = g.$$

We let $\gamma_1, \ldots, \gamma_{2g}$ be a basis of paths on C, and let $\omega_1, \ldots, \omega_g$ be a basis of holomorphic differentials. We integrate each differential ω_j against each path γ_i to obtain the period matrix of C,

$$\Omega = \left(\Omega_i^j\right)_{\substack{1 \leq i \leq 2g \\ 1 \leq j \leq g}} = \left(\int_{\gamma_i} \omega_j\right)_{\substack{1 \leq i \leq 2g \\ 1 \leq j \leq g}}.$$

Theorem 1.8 (Riemann's period relations)**.** *Choose the paths $\gamma_1, \ldots, \gamma_{2g}$ so that the intersection property*

$$\gamma_i \cdot \gamma_j = \begin{cases} 1, & \text{if } j = i + g, \\ 0, & \text{otherwise.} \end{cases} \tag{1.2}$$

is satisfied. Then the period matrix Ω, written by square blocks as $\Omega = (\Omega_1 \mid \Omega_2)$, satisfies

$$\begin{cases} \Omega_1 \Omega_2^t = \Omega_2 \Omega_1^t \\ -\sqrt{-1} \left(\bar{\Omega}_1 \Omega_2^t - \bar{\Omega}_2 \Omega_1^t \right) > 0. \end{cases}$$

In particular the basis of differentials $\omega_1, \ldots, \omega_g$ can be chosen so that the period matrix is of the form

$$\Omega = (Id \mid \tau)$$

with $\tau = \Omega_1^{-1}\Omega_2$, $\operatorname{Im} \tau$ is positive definite, and the column vectors of Ω generate the lattice $L_\Omega = \mathbb{Z}^g + \tau \mathbb{Z}^g$.

Definition 1.9. *The Jacobian of a Riemann surface C is the complex torus*

$$\operatorname{Jac}(C) := \mathbb{C}^g / L_\Omega.$$

Together with the intersection pairing given by (1.2)*, it is a principally polarized abelian variety. If the lattice L_Ω is of the form $\mathbb{Z}^g + \tau\mathbb{Z}^g$, then the Riemann form is equivalently given by $H(z, w) = z^t (\operatorname{Im} \tau)^{-1} \bar{w}$.*

Sometimes is also convenient to define the Jacobian in an equivalent, more intrinsic way. We inject $H_1(C, \mathbb{Z})$ into the dual space $\Omega^1(C)^\vee$ with the map $\gamma \mapsto \int_\gamma$. Then we can set

$$\operatorname{Jac}(C) := \Omega^1(C)^\vee / H_1(C, \mathbb{Z}). \tag{1.3}$$

Recall that the divisor group $\operatorname{Div}(C)$ of C is the formal abelian group generated by the points of C,

$$\operatorname{Div}(C) = \bigoplus_{P \in C} \mathbb{Z}[P].$$

The degree-0 part of the divisor group, $\operatorname{Div}^0(C)$, is the group of formal sums $\sum_{P \in C} n_P[P]$ such that $\sum_{P \in C} n_P = 0$. The divisors which are zeros of some function on C form a subgroup of $\operatorname{Div}^0(C)$ called the group of principal divisors. The Picard group $\operatorname{Pic}^0(C)$ is the quotient of $\operatorname{Div}^0(C)$ by the principal divisors.

We can embed the curve C in its Jacobian as follows. We fix a base point $P_0 \in C$, and for each point $P \in C$ we define the Abel-Jacobi map

$$P \mapsto \left(\int_{P_0}^P \omega_1, \cdots \int_{P_0}^P \omega_g \right).$$

This map is not well-defined, since the integrals are path-dependent. In fact, given two points P and Q on C and two different paths α and β between them, we can form a loop on C by concatenating α with the reverse of β, this is homologous to $\sum_{i=1}^{2g} n_i\gamma_i \in H_1(C,\mathbb{Z})$ for some integers n_i. Therefore the map $C \to \mathrm{Jac}(C)$ is well-defined. We extend it by linearity to $\Phi_{P_0} : \mathrm{Div}^0(C) \to \mathrm{Jac}(C)$.

Theorem 1.10 (Abel-Jacobi)**.** *The map Φ_{P_0} is surjective, and its kernel is exactly the subgroup of principal divisors. Hence, Φ_{P_0} induces a group isomorphism* $\mathrm{Pic}^0(C) \cong \mathrm{Jac}(C)$.

Corollary 1.11. *If C is a curve of genus $g \geq 1$, the map $\Phi_{P_0} : C \to \mathrm{Jac}(C)$ is an embedding. In particular every elliptic curve is isomorphic to its Jacobian.*

Although we won't need the material, the Jacobian of a curve C defined over a field of arbitrary characteristic also exists, and there still is an Abel-Jacobi map $C \to \mathrm{Jac}(C)$ inducing a bijection $\mathrm{Pic}^0(C) \cong \mathrm{Jac}(C)$.[1] See [HS00, § A.8] for further detail.

Definition 1.12. *A smooth curve $C_{/\mathbb{Q}}$ of genus $g \geq 2$ is called hyperelliptic if it admits a double cover $C \to \mathbb{P}^1$ of the projective line. Such a curve has an affine equation $C : y^2 + H(x)y = F(x)$ for some polynomials $H(x)$, $F(x)$.*

All curves $C_{/\mathbb{Q}}$ of genus 2 are hyperelliptic. When $H(x) = 0$ (and so $F(x)$ is a polynomial of degree 5 or 6), a basis of $\Omega^1(C)$ is $\{dx/y, xdx/y\}$. If $\{\alpha_1, \alpha_2, \beta_1, \beta_2\}$ are loops generating $H_1(C,\mathbb{Z})$ (remember that $C(\mathbb{C})$ is topologically a two-holed torus), the period lattice L_C of C is spanned by the vectors

$$\left(\int_\gamma \frac{dx}{y}, \int_\gamma \frac{xdx}{y}\right) = \left(\int_\gamma \frac{dz}{\sqrt{F(z)}}, \int_\gamma \frac{zdz}{\sqrt{F(z)}}\right), \qquad \gamma \in \{\alpha_1, \alpha_2, \beta_1, \beta_2\},$$

these are called Abelian integrals. The complex torus $\mathbb{C}^2/L_C$ is the Jacobian of C, and it comes equipped with the intersection pairing defined above, so $\mathrm{Jac}(C)$ is principally polarized. Every principally polarized abelian surface over $\mathbb{C}$ is either of this form, or it is isomorphic to a product of elliptic curves $E_1 \times E_2$.

1.1.2 Galois representations

Let $\bar{\mathbb{Q}}$ be a fixed algebraic closure of $\mathbb{Q}$. The group of field automorphisms of $\bar{\mathbb{Q}}$ form the absolute Galois group of $\mathbb{Q}$, which we write from now on $G_\mathbb{Q} := \mathrm{Aut}(\bar{\mathbb{Q}})$. An automorphism $\sigma \in G_\mathbb{Q}$ fixes $\mathbb{Q}$ point-wise and restricts to an automorphism

$$\sigma|_F \in \mathrm{Gal}(F/\mathbb{Q})$$

for every Galois number field F. This restriction is surjective. If $E \supset F \supset \mathbb{Q}$ is a tower of number fields, we have $\sigma|_F = \sigma|_E|_F$, so the restrictions are compatible.

[1] We do not require the field k to be algebraically closed, but we do need $C(k) \neq \emptyset$.

Conversely, every compatible system $\{\sigma_F\}_F$, where F runs over every finite Galois extension of $\mathbb{Q}$, defines an element of $G_{\mathbb{Q}}$. This description is summarized with the projective limit

$$G_{\mathbb{Q}} = \varprojlim_{\substack{F/\mathbb{Q} \\ \text{finite, Galois}}} \mathrm{Gal}(F/\mathbb{Q}).$$

We endow $G_{\mathbb{Q}}$ with the Krull topology by means of a basis of open sets, consisting of

$$\sigma \cdot (\ker : G_{\mathbb{Q}} \twoheadrightarrow \mathrm{Gal}(F/\mathbb{Q}))$$

for all $\sigma \in G_{\mathbb{Q}}$ and every Galois number field F. For $\sigma = id_{\bar{\mathbb{Q}}}$, these sets are the collection of normal subgroups with finite index in $G_{\mathbb{Q}}$. This topology is equivalent to the one given by the projective limit, if we consider each $\mathrm{Gal}(F/\mathbb{Q})$ to have the discrete topology. As the inverse limit of finite groups, $G_{\mathbb{Q}}$ is a compact topological group.

Let $A_{/\mathbb{Q}}$ be an abelian variety of dimension g. Given a positive integer n, the group of n-torsion points $A[n](\mathbb{C})$ is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$, since $A(\mathbb{C}) \cong \mathbb{C}^g/\Lambda$ for some lattice $\Lambda \subset \mathbb{C}^g$. Note that every point $P \in A[n](\mathbb{C})$ is defined over $\bar{\mathbb{Q}}$, because addition on A is defined by $\mathbb{Q}$-rational maps. Hence $G_{\mathbb{Q}}$ acts on $A[n] = A[n](\bar{\mathbb{Q}})$, and by choosing a $\mathbb{Z}/n\mathbb{Z}$-basis of $A[n]$ we obtain a representation

$$\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{Aut}(A[n]) \cong \mathrm{GL}_{2g}(\mathbb{Z}/n\mathbb{Z}).$$

If $n = \ell$ is a prime, we have a representation with values in $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$. It is convenient to have a representation over a ring of characteristic zero, this motivates the use of ℓ-adic numbers.

Recall that given a prime number ℓ, $\mathbb{Z}_\ell$ is the ring of ℓ-adic integers, with elements given by sequences $(a_1, a_2, a_3, \dots)$ such that $a_n \in \mathbb{Z}/\ell^n\mathbb{Z}$ and $a_{n+1} \equiv a_n \bmod \ell^n$ for all $n \geq 1$. Thus it is the projective limit

$$\mathbb{Z}_\ell = \varprojlim_n \mathbb{Z}/\ell^n\mathbb{Z}.$$

Like $G_{\mathbb{Q}}$, $\mathbb{Z}_\ell$ has a topology with a basis of open sets given by $x + \ell^n\mathbb{Z}_\ell$ for all $x \in \mathbb{Z}_\ell$ and $n > 0$. This topology is equivalent to the one given by the metric induced by the ℓ-adic valuation. With it, $\mathbb{Z}_\ell$ is a compact topological ring. The field $\mathbb{Q}_\ell$ of ℓ-adic numbers is the fraction field of $\mathbb{Z}_\ell$, its topology is also given by the ℓ-adic valuation.

The vector spaces $\mathbb{Q}_\ell^d$ have the product topology, and the group $\mathrm{GL}_d(\mathbb{Q}_\ell)$ has the induced topology from being a subset of $\mathbb{Q}_\ell^{d^2}$. The operations of $\mathbb{Q}_\ell$, $\mathbb{Q}_\ell^d$ and $\mathrm{GL}_d(\mathbb{Q}_\ell)$ are all continuous.

We are now ready to build ℓ-adic representations out of abelian varieties. Let $A_{/\mathbb{Q}}$ be an abelian variety, and let ℓ be any prime. First, note that for each positive integer n, the multiplication-by-ℓ map $[\ell] : A[\ell^{n+1}] \to A[\ell^n]$ is surjective.

Definition 1.13. *The ℓ-adic Tate module of $A_{/\mathbb{Q}}$ is defined to be*

$$\mathrm{T}_\ell(A) := \varprojlim_n A[\ell^n].$$

We also define $\mathrm{V}_\ell(A) := \mathrm{T}_\ell(A) \otimes \mathbb{Q}$.

From the isomorphism $A[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^{2g}$, where $g = \dim A$, it is immediate to see that $\mathrm{T}_\ell(A)$ is a $\mathbb{Z}_\ell$-module of rank $2g$, and that $\mathrm{V}_\ell(A) \cong \mathbb{Q}_\ell^{2g}$. The group $G_\mathbb{Q}$ acts on each of the $A[\ell^n]$, and the action commutes with the maps $[\ell]$. Hence $G_\mathbb{Q}$ acts on $\mathrm{T}_\ell(A)$, and the action is in fact continuous. This yields a representation $G_\mathbb{Q} \to \mathrm{Aut}(\mathrm{T}_\ell(A))$. By choosing a basis of $\mathrm{V}_\ell(A)$, we have the ℓ-adic representation associated to A,

$$\rho_{A,\ell} : G_\mathbb{Q} \to \mathrm{GL}_{2g}(\mathbb{Q}_\ell).$$

More generally, ℓ-adic Galois representations have the following definition.

Definition 1.14. *Let d be a positive integer. A d-dimensional ℓ-adic Galois representation is a continuous homomorphism*

$$\rho : G_\mathbb{Q} \to \mathrm{GL}_d(L)$$

where L is a finite extension of $\mathbb{Q}_\ell$. If $\rho' : G_\mathbb{Q} \to \mathrm{GL}_d(L)$ is another such representation, it is said to be equivalent to ρ, written $\rho \sim \rho'$, if there is some $m \in \mathrm{GL}_d(L)$ such that $\rho'(\sigma) = m^{-1}\rho(\sigma)m$ for all $\sigma \in G_\mathbb{Q}$.

We write $\bar{\mathbb{Z}}$ for the ring of algebraic integers, that is, all the roots inside $\bar{\mathbb{Q}}$ of monic polynomials in $\mathbb{Z}[x]$. Given a maximal ideal $\mathfrak{p}$ of $\bar{\mathbb{Z}}$, its intersection with $\mathbb{Z}$ is a maximal ideal $p\mathbb{Z}$ for some prime number p. The field $\bar{\mathbb{Z}}/\mathfrak{p}$ is an algebraic closure of $\mathbb{F}_p$, denoted as usual by $\bar{\mathbb{F}}_p$.

The decomposition group of $\mathfrak{p}$ is

$$D_\mathfrak{p} = \{\sigma \in G_\mathbb{Q} \mid \mathfrak{p}^\sigma = \mathfrak{p}\}.$$

By definition, each $\sigma \in D_\mathfrak{p}$ satisfies $(x + \mathfrak{p})^\sigma = x^\sigma + \mathfrak{p}$ for all $x \in \bar{\mathbb{Q}}$, inducing a reduction map

$$D_\mathfrak{p} \to G_{\bar{\mathbb{F}}_p}$$

where $G_{\bar{\mathbb{F}}_p} = \mathrm{Aut}(\bar{\mathbb{F}}_p)$. This morphism is surjective. An absolute Frobenius element $\mathrm{Frob}_\mathfrak{p}$ is any preimage of the Frobenius automorphism $\sigma_p \in G_{\bar{\mathbb{F}}_p}$ sending x to x^p. Such an element is defined up to the kernel of the reduction map, called the inertia group of $\mathfrak{p}$,

$$I_\mathfrak{p} = \ker\left(D_\mathfrak{p} \to G_{\bar{\mathbb{F}}_p}\right) = \{\sigma \in D_\mathfrak{p} \mid x^\sigma \equiv x \bmod \mathfrak{p}\ \forall x \in \bar{\mathbb{Z}}\}.$$

Theorem 1.15 (Čebotarev)**.** *Let S be a finite set of rational primes. For each maximal ideal $\mathfrak{p}$ of $\bar{\mathbb{Z}}$ lying over any rational prime p outside S, choose an absolute Frobenius element* $\mathrm{Frob}_\mathfrak{p}$*. The set of such elements forms a dense subset of $G_\mathbb{Q}$.*

Given a Galois representation ρ, we usually want to know its values at absolute Frobenius elements. However, each $\mathrm{Frob}_{\mathfrak{p}}$ is only defined up to an inertia group $I_{\mathfrak{p}}$, so $\rho(\mathrm{Frob}_{\mathfrak{p}})$ is well defined if and only if $I_{\mathfrak{p}} \subset \ker\rho$. This motivates the following definition.

Definition 1.16. *Let ρ be a Galois representation and let p be prime. Then ρ is unramified at p if $I_{\mathfrak{p}} \subset \ker\rho$ for any maximal ideal $\mathfrak{p} \subset \bar{\mathbb{Z}}$ containing $p\mathbb{Z}$.*

As long as our representation is unramified at all but a finite number of primes, Theorem 1.15 implies the values $\rho(\mathrm{Frob}_{\mathfrak{p}})$ for $\mathfrak{p}$ over unramified p determine ρ everywhere by continuity. This situation applies to abelian varieties.

Theorem 1.17. *Let $A_{/\mathbb{Q}}$ be an abelian variety of conductor N and let ℓ be a prime. The ℓ-adic representation $\rho_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{Aut}(\mathrm{T}_\ell(A))$ is unramified at every prime $p \nmid \ell N$.*

1.1.3 L-functions

Given an abelian variety $A_{/\mathbb{Q}}$, we consider its associated ℓ-adic representation

$$\rho_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_{2g}(\mathbb{Q}_\ell).$$

For any prime p we define the pth Euler factor of A to be the characteristic polynomial of an absolute Frobenius element $\mathrm{Frob}_{\mathfrak{p}}$ over p,

$$L_p(A,T) := \det\left(1 - T\rho_{A,\ell}(Frob_{\mathfrak{p}})|\,\mathrm{T}_\ell(A)^{I_{\mathfrak{p}}}\right).$$

This definition is independent of the choice of a maximal ideal $\mathfrak{p}$ over p: if $\mathfrak{p}'$ is another such ideal, then $\mathrm{Frob}_{\mathfrak{p}}$ is the conjugate of $\mathrm{Frob}_{\mathfrak{p}'}$ by some automorphism $\sigma \in G_{\mathbb{Q}}$, so $\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}})$ and $\rho_{A,\ell}(\mathrm{Frob}_{\mathfrak{p}'})$ have the same characteristic polynomial.

Note that we need the restriction to the $I_{\mathfrak{p}}$-invariant part of $\mathrm{T}_\ell(A)$ for $\rho(\mathrm{Frob}_{\mathfrak{p}})$ to be well-defined. Theorem 1.17 asserts that $\mathrm{T}_\ell(A)^{I_{\mathfrak{p}}}$ is the full Tate module for all $p \nmid \ell N_A$. In this case, if A is an elliptic curve then one can see that

$$L_p(A,T) = 1 - a_pT + pT^2.$$

If A is a surface, then L_p is a degree-4 polynomial

$$L_p(A,T) = 1 - a_pT + b_{p^2}T^2 - pa_pT^3 + p^2T^4. \tag{1.4}$$

The choice of notation will make sense once we consider Siegel paramodular forms in Chapter 2. In all cases $L_p(A,T) \in 1 + \mathbb{Z}[T]$. We package all the factors into the L-function of A,

$$L(A,s) := \prod_p L_p(A,p^{-s})^{-1}. \tag{1.5}$$

This function can be seen to converge in a suitable right half plane.

Assume $A = \operatorname{Jac}(C)$ for some curve $C_{/\mathbb{Q}}$. For a prime p of good reduction for C (i.e., such that the mod p curve $\tilde{C}_{/\mathbb{F}_p}$ is smooth), we may define a generating function

$$Z(\tilde{C}_{/\mathbb{F}_p}, T) = \exp\left(\sum_{n=1}^{\infty} \#\tilde{C}(\mathbb{F}_{p^n})\frac{T^n}{n}\right).$$

By the Weil conjectures [Sil09, Theorem V.2.2], this turns out to be the rational function

$$Z(\tilde{C}_{/\mathbb{F}_p}, T) = \frac{L_p(A,T)}{P(T)}$$

for some integer polynomial $P(T)$, and all the complex roots α_i of L_p satisfy $|\alpha_i| \leq p^{-1/2}$. It follows that $L(A,s)$ converges in the right half plane $\{s \in \mathbb{C} \mid \operatorname{Re}(s) > \frac{3}{2}\}$.

1.2 Modular curves and modular forms

We consider the complex upper half plane,

$$\mathcal{H} = \{z \in \mathbb{C} \mid \operatorname{Im} z > 0\}.$$

We have an action of the group $\mathrm{SL}_2(\mathbb{R})$ on $\mathcal{H}$; a matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $ad - bc = 1$ acts as $\tau \mapsto \frac{a\tau+b}{c\tau+d}$. This action is transitive, and is also valid if we take some matrix $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$.

Definition 1.18. *Let $\mathcal{O}(\mathcal{H})$ be the set of holomorphic functions on $\mathcal{H}$. The weight-k slash operator of $\gamma \in \mathrm{GL}_2^+(\mathbb{R})$ on a function $f \in \mathcal{O}(\mathcal{H})$ is given by*

$$(f|_k\gamma)(\tau) := (\det\gamma)^{k-1} j(\gamma,\tau)^{-k} f(\gamma\tau),$$

where $j(\gamma,\tau) := c\tau + d$ for $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

Let $N \geq 1$ be an integer. The principal congruence subgroup of level N is defined as

$$\Gamma(N) := \ker(\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})),$$

it is a finite index subgroup of $\mathrm{SL}_2(\mathbb{Z})$. A subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ is a congruence subgroup if it contains some $\Gamma(N)$.

Definition 1.19. *Given any congruence subgroup $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$, we say a holomorphic function $f \in \mathcal{O}(\mathcal{H})$ is a modular form of weight k on Γ if*

1. *$f(\gamma\tau) = (c\tau + d)^k f(\tau)$, for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$,*

2. *For any $\gamma \in \mathrm{SL}_2(\mathbb{Z})$, there exists a positive integer h such that the function $f|_k\gamma(\tau) = (c\tau + d)^{-k} f(\tau)$ can be written as a series*

$$\sum_{n=0}^{\infty} a_n^\gamma q^{n/h}, \text{ where } q = e^{2\pi i\tau}.$$

A modular form is called a cusp form if $a_0^\gamma = 0$ for all γ. The $\mathbb{C}$-vector space of modular forms of weight k for Γ is denoted by $M_k(\Gamma)$. The vectors subspace of cusp forms is denoted by $S_k(\Gamma)$.

Given a congruence subgroup Γ, its open modular curve is the quotient

$$Y_\Gamma := \Gamma\backslash\mathcal{H},$$

the notation coming from the fact that we have a left action of Γ on $\mathcal{H}$. It is useful to compactify these by adding a finite set of points called cusps: we set $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$, then Γ acts on $\mathbb{P}^1(\mathbb{Q})$ and $\Gamma\backslash\mathbb{P}^1(\mathbb{Q})$ is finite. We then define the quotient

$$X_\Gamma := \Gamma\backslash\mathcal{H}^*,$$

which is a compact Riemann surface. We call X_Γ the modular curve corresponding to Γ; we can apply to it the theory of complex Jacobians. We will mostly focus on weight-2 modular forms, because they give us the cohomology of the various modular curves X_Γ.

Take a cusp form $f \in S_2(\Gamma)$ and let $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Then

$$d(\gamma\tau) = \frac{a(c\tau + d) - c(a\tau + b)}{(c\tau + d)^2} d\tau = \frac{d\tau}{(c\tau + d)^2},$$

so $2\pi i f(\gamma\tau)d(\gamma\tau) = 2\pi i f(\tau)d\tau$, and $2\pi i f(\tau)d\tau$ is a Γ-invariant holomorphic differential. The definition $q = e^{2\pi i\tau}$ implies $2\pi i d\tau = dq/q$, so ω_f is holomorphic at $i\infty$ because $a_0(f) = 0$, f being a cusp form. Continuing with this reasoning, one can prove the following.

Proposition 1.20. *The map $f(\tau) \mapsto \omega_f := 2\pi i f(\tau)d\tau$ is an isomorphism between the space $S_2(\Gamma)$ and the space $\Omega^1(X_\Gamma)$ of holomorphic differentials on the curve X_Γ.*

In particular, the Riemann-Roch theorem [HS00, Theorem A.4.2.1] implies $S_2(\Gamma)$ has finite dimension equal to the genus g of X_Γ.

This identifies the $\mathrm{Jac}(X_\Gamma)$ with the quotient $S_2(\Gamma)^\vee/H_1(X_\Gamma, \mathbb{Z})$, it is an abelian variety of dimension g.

From now on we will only use the congruence subgroup $\Gamma_0(N)$ of level N, given by the matrices that become upper triangular modulo N:

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

We shall write $X_0(N) := X_{\Gamma_0(N)}$ and $J_0(N) := \mathrm{Jac}(X_0(N))$ for the corresponding modular curve and its Jacobian. It can be proved that both $X_0(N)$ and $\mathrm{Jac}(X_0(N))$ are not only complex varieties, but they can also be defined over $\mathbb{Q}$.

1.2.1 Hecke operators

The space $S_2(\Gamma_0(N))$ comes equipped with an action of certain linear operators T_p for each prime p, called the Hecke operators.

To reduce the notation load we set momentarily $\Gamma = \Gamma_0(N)$. For each matrix $\alpha \in \mathrm{GL}_2(\mathbb{Q})^+$ we have a corresponding double coset

$$\Gamma\alpha\Gamma = \{\gamma_1\alpha\gamma_2 \mid \gamma_1, \gamma_2 \in \Gamma\},$$

defining a Hecke operator $T(\Gamma\alpha\Gamma) : M_2(\Gamma) \to M_2(\Gamma)$ as follows. The group Γ acts on $\Gamma\alpha\Gamma$ on the left. By [DS05, Lemmas 5.1.1 and 5.1.2] we can take a finite set of class representatives $\{\beta_j\}$ of $\Gamma\backslash\Gamma\alpha\Gamma$. Then, we can set

$$T(\Gamma\alpha\Gamma)(f) := \sum_j f|_2\beta_j,$$

which is well-defined and independent of representatives. We shall use the particular case of

$$T_p := T\left(\Gamma\begin{pmatrix}1 & 0\\ 0 & p\end{pmatrix}\Gamma\right)$$

for any prime p.

The effect of T_p on the q-expansion of a form $f(\tau) = \sum a_n q^n$ is given by the formulas

$$T_p(f) = \begin{cases} \sum_{p|n} a_n q^{n/p} + p\sum a_n q^{pn}, & \text{if } p \nmid N,\\ \sum_{p|n} a_n q^{n/p}, & \text{if } p \mid N.\end{cases}$$

In particular, T_p maps cusp forms to cusp forms. The definition of Hecke operators is extended to T_n for arbitrary positive integers n by the formal Dirichlet series

$$\sum_{n=1}^{\infty} T_n n^{-s} := \prod_{p\nmid N}(1 - T_p p^{-s} + p^{1-2s})^{-1} \prod_{p|N}(1 - T_p p^{-s})^{-1}. \tag{1.6}$$

Definition 1.21. *The Hecke algebra over $\mathbb{Z}$ is the algebra of endomorphisms of $S_2(\Gamma_0(N))$ generated over $\mathbb{Z}$ by the Hecke operators,*

$$\mathbb{T}_{\mathbb{Z}} = \mathbb{Z}[\{T_n; n \in \mathbb{Z}_{\geq 1}\}].$$

The Hecke algebra $\mathbb{T}_{\mathbb{C}}$ over $\mathbb{C}$ is defined similarly. We remark that both these algebras are commutative.

By duality, $\mathbb{T}_{\mathbb{Z}}$ acts on $S_2(\Gamma_0(N))^\vee$, and in particular it stabilizes the finite $\mathbb{Z}$-module $H_1(X_0(N), \mathbb{Z})$. It follows that $\mathbb{T}_{\mathbb{Z}}$ has also finite $\mathbb{Z}$-rank, and it is in fact equal to $g = \dim_{\mathbb{C}} S_2(\Gamma_0(N))$.

A form $f \in S_2(\Gamma_0(N))$ is an eigenform for all of $\mathbb{T}_{\mathbb{C}}$ if and only if f is an eigenform for all Hecke operators T_p. If f is also normalized so that $a_1(f) = 1$, then the identity $T_n(f) = a_n(f)f$ gives a ring homomorphism

$$\lambda_f : \mathbb{T}_{\mathbb{Z}} \to \mathbb{C}.$$

The image of λ_f is the subring $\mathbb{Z}[\{a_n(f) \mid n \in \mathbb{Z}_{\geq 1}\}]$ of $\mathbb{C}$, which is finitely generated as a $\mathbb{Z}$-module, because $\mathbb{T}_{\mathbb{Z}}$ is. In particular, the image consists of algebraic integers.

We define a non-degenerate Hermitian inner product for any two cusp forms $f, g \in S_2(\Gamma_0(N))$,

$$\langle f, g \rangle := \int_{\Gamma_0(N)\backslash\mathcal{H}} f(\tau)\overline{g(\tau)}dxdy,$$

called the Petersson scalar product.

Lemma 1.22. *Let $\mathbb{T}^0_{\mathbb{Z}}$ be the $\mathbb{Z}$-submodule of $\mathbb{T}_{\mathbb{Z}}$ generated by all T_n with n coprime to N. If $T \in \mathbb{T}^0_{\mathbb{Z}}$, then it is self-adjoint with respect to the Petersson scalar product,*

$$\langle Tf, g \rangle = \langle f, Tg \rangle,$$

for all forms $f, g \in S_2(\Gamma_0(N))$.

After the lemma, the Spectral theorem plus the fact that all Hecke operators commute imply the space $S_2(\Gamma_0(N))$ has an orthogonal basis of simultaneous eigenforms for the Hecke operators T_n, for all n coprime to N. More succintly, $\mathbb{T}^0_{\mathbb{Z}}$ acts semi-simply on $S_2(\Gamma_0(N))$; however, this is not the case for $\mathbb{T}_{\mathbb{Z}}$: $S_2(\Gamma_0(N))$ does not decompose into a direct sum of eigenspaces corresponding to homomorphisms $\lambda : \mathbb{T}_{\mathbb{Z}} \to \mathbb{C}$. This problem is solved by introducing newforms. We consider integers $M \mid N$ and d such that $d \mid \frac{N}{M}$, and define a level-raising operator

$$V_d : S_2(\Gamma_0(M)) \to S_2(\Gamma_0(N)) \tag{1.7}$$

by

$$(V_d f)(\tau) := \frac{1}{d}\left(f\Big|_2 \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} \right)(\tau) = f(d \cdot \tau).$$

This operator satisfies $V_d T_n = T_n V_d$ for n coprime to d. Note also that the inclusion of groups $\Gamma_0(N) \subset \Gamma_0(M)$ implies the reverse inclusion of spaces $S_2(\Gamma_0(M)) \subset S_2(\Gamma_0(N))$.

Definition 1.23. *The old subspace is defined as*

$$S_2(\Gamma_0(N))^{old} := \mathrm{span}_{\mathbb{C}}\{V_d(S_2(\Gamma_0(M))) \ : \ dM \mid N, M \neq N\}.$$

The new subspace is then defined as the orthogonal complement of $S_2(\Gamma_0(N))^{old}$ in $S_2(\Gamma_0(N))$ with respect to the Petersson scalar product,

$$S_2(\Gamma_0(N))^{new} := \left(S_2(\Gamma_0(N))^{old}\right)^{\perp}.$$

We say $f \in S_2(\Gamma_0(N))^{new}$ is a newform if it is a simultaneous eigenform for $\mathbb{T}_{\mathbb{Z}}$ and it is normalized so that $a_1(f) = 1$.

Both the actions of $\mathbb{T}_{\mathbb{Z}}$ and $\mathbb{T}_{\mathbb{Z}}^0$ leave the old and new subspaces invariant. Assume now that $f \in S_2(\Gamma_0(N))^{new}$ is a nonzero eigenform for all Hecke operators T_n with n coprime to N. The identity $a_n(f) = \lambda_f(T_n)a_1(f)$ plus [DS05, Theorem 5.7.1] imply that $a_1(f) \neq 0$, and we may further assume f is normalized.

For any positive $m \in \mathbb{Z}$ we let $g_m = T_m f - a_m(f)f$, which is an element of the new space and an eigenform for all T_n with n coprime to N. Then

$$\begin{aligned} a_1(g_m) &= a_1(T_m f) - a_1(a_m(f)f) \\ &= a_m(f) - a_m(f) = 0, \end{aligned}$$

so again by [DS05, Theorem 5.7.1] we have $g_m \in S_2(\Gamma_0(N))^{old}$. It follows that $g_m = 0$, so $T_m f = a_m(f)f$. This discussion can be completed [AL70] to show the following.

Theorem 1.24 (Strong Multiplicity One)**.** *Let $N \geq 1$.*

1. *If $f \in S_2(\Gamma_0(N))^{new}$ is a simultaneous eigenform for the action of $\mathbb{T}_{\mathbb{Z}}^0$ then f is a simultaneous eigenform for all of $\mathbb{T}_{\mathbb{Z}}$.*
2. *If $f \in S_2(\Gamma_0(N))^{new}$ and $g \in S_2(\Gamma_0(M))^{new}$ are both newforms satisfying $a_p(f) = a_p(g)$ for all but finitely many primes p, then $N = M$ and $f = g$.*

In particular, the space $S_2(\Gamma_0(N))^{new}$ has an orthogonal basis of newforms, and $T_n f = a_n(f)f$ for every newform, so that the Fourier coefficients of f are its T_n-eigenvalues.

Theorem 1.25. *There is a direct sum decomposition*

$$S_2(\Gamma_0(N)) = \bigoplus_{M|N} \bigoplus_{dM|N} V_d(S_2(\Gamma_0(M))^{new}).$$

In other words, the set

$$\mathcal{B}_2(N) = \{f(d\tau) \ : \ f \text{ is a newform of level } M \text{ and } dM \mid N\}$$

is a basis of $S_2(\Gamma_0(N))$.

1.2.2 L-functions

Given an eigenform $f(\tau) = \sum a_n q^n \in S_2(\Gamma_0(N))$, its L-function is defined as the Dirichlet series

$$L(f,s) := \sum_n \frac{a_n}{n^s}.$$

By the formal series (1.6), $L(f,s)$ has an expression as an Euler product

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

The function $L(f,s)$ converges in the right half plane $\{s \in \mathbb{C} \mid \mathrm{Re}(s) > 2\}$. However, we can do better. Given a function $g : \mathbb{R}^+ \to \mathbb{C}$, its Mellin transform is the complex function

$$\tilde{g}(s) = \int_0^\infty g(t)t^s \frac{dt}{t}.$$

We define the completed L-function of f to be

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

where $\Gamma(s) = \int_0^\infty t^{s-1}e^{-t}dt$ is the usual Gamma function satisfying $\Gamma(n+1) = n!$ for natural n (note that $\Gamma(s)$ is the Mellin transform of e^t). We have the equality

$$\Lambda(f,s) = \int_0^\infty f(it)t^s \frac{dt}{t},$$

where the right hand-side is the Mellin transform of the function of real variable $f(it) : \mathbb{R}^+ \to \mathbb{C}$. Moreover, one can prove the functional equation

$$N^{s/2}\Lambda(f,s) = \varepsilon_f N^{s/2}\Lambda(f,2-s)$$

where $\varepsilon_f \in \{1,-1\}$. It follows that $L(f,s)$ has an analytic continuation to the whole complex plane.

1.3 The Eichler-Shimura relation

Let $f(\tau) = \sum_{n\geq 1} a_n q^n$ be a normalized eigenform in $S_2(\Gamma_0(N))$ corresponding to an algebra homomorphism

$$\lambda_f : \mathbb{T}_{\mathbb{Z}} \to \mathbb{C}$$

given by $\lambda_f(T_n) = a_n(f)$. Let $I_f \subset \mathbb{T}_{\mathbb{Z}}$ be the ideal

$$I_f = \ker(\lambda_f) = \{T \in \mathbb{T}_{\mathbb{Z}} \mid Tf = 0\}.$$

We have the $\mathbb{Z}$-module isomorphism $\mathbb{T}_{\mathbb{Z}}/I_f \cong \mathbb{Z}[\{a_n(f)\}_n]$.

Definition 1.26. *The number field of f is defined to be the extension of $\mathbb{Q}$ generated by the Fourier coefficients of f,*

$$K_f := \mathbb{Q}(\{a_n(f)\}).$$

In particular, the $\mathbb{Z}$-rank of $\mathbb{T}_{\mathbb{Z}}/I_f$ is equal to the extension degree $[K_f : \mathbb{Q}]$.

Any embedding $\sigma : K_f \hookrightarrow \mathbb{C}$ conjugates f by acting on its coefficients, so that

$$f^\sigma(\tau) = \sum_{n\geq 1} a_n^\sigma q^n.$$

One shows that f^σ is another normalized eigenform, and if f is a newform f^σ is also a newform (see [DS05, Theorem 6.5.4] for a proof). It is clear that

$K_f = K_{f^\sigma}$ whenever the extension $K_f/\mathbb{Q}$ is Galois, and $\mathrm{Aut}(K_f/\mathbb{Q})$ divides the set of newforms of level N in equivalence classes.

The image $I_f(J_0(N))$ is an abelian subvariety of $J_0(N)$ which is stable under $\mathbb{T}_\mathbb{Z}$, allowing to make the following definition.

Definition 1.27. *The abelian variety associated to f is the quotient*

$$A_f := J_0(N)/I_f J_0(N).$$

Clearly the ring $\mathbb{Z}[\{a_n(f)\}] \cong \mathbb{T}_\mathbb{Z}/I_f$ acts on A_f, so the field K_f injects into the endomorphism algebra $\mathrm{End}^0(A_{f,\mathbb{C}})$. It can be shown that A_f is defined over $\mathbb{Q}$, and so K_f also lies in the algebra of endomorphisms of A_f defined over $\mathbb{Q}$, $\mathrm{End}^0(A_f)$. Additionally, the dimension of A_f is equal to the degree $[K_f : \mathbb{Q}]$.

By using Theorem 1.25, one proves the following.

Theorem 1.28. *The Jacobian $J_0(N)$ associated to $\Gamma_0(N)$ is isogenous over $\mathbb{Q}$ to the product*

$$\prod_{[f]} A_f^{m_f}$$

where the product is taken over a set of equivalence class representatives $f \in S_2(\Gamma_0(M_f))$ at levels M_f dividing N, and each m_f is the number of divisors of N/M_f.

Proof. See Theorem 6.6.6 and the subsequent discussion in [DS05]. □

The interest of this construction goes further, because the L-function of each A_f is related to the L-function of the corresponding newform f. To see the idea why this is true we give an interpretation of the modular curve $X_0(N)$, called the moduli space interpretation: each point on $\Gamma_0(N)\backslash\mathcal{H}$ corresponds to an isomorphism class of elliptic curves with some "level structure".

We define the following set of enhanced elliptic curves:

$$S_0(N) = \{(E, C) \mid E_{/\mathbb{C}},\ C \text{ is a cyclic subgroup of order } N \text{ of } E\}/\sim,$$

where $\sim$ means the equivalence relation of isomorphism of structure: $(E, C) \sim (E', C')$ whenever there exists an isomorphism $E \to E'$ taking C to C'. The set $S_0(N)$ is a space of moduli of isomorphism classes of complex elliptic curves. Sometimes we want to exclude the curves with j-invariants 0 and 1728 (these correspond to curves with extra automorphisms), in that case, we write $S_0(N)'$.

Proposition 1.29. *There is a bijection*

$$\begin{aligned} \psi_0 : S_0(N) &\longrightarrow \Gamma_0(N)\backslash\mathcal{H} \\ [\mathbb{C}/\Lambda_\tau, \langle 1/N + \Lambda_\tau\rangle] &\longmapsto \Gamma_0(N)\tau. \end{aligned}$$

The Hecke operator T_p on $J_0(N)$ induced by duality is made explicit as an operator on $\mathrm{Div}(S_0(N))$. Indeed, if $[E, C]$ is an enhanced elliptic curve, we have

$$T_p[E, C] = \sum_{D \subset E \text{ cyclic of order } p} [E/D, C + D].$$

Here the quotient E/D corresponds to the image of the unique isogeny (up to isomorphism) $E \to E'$ with kernel D [Sil09, Theorem III.4.12]. The endomorphism $T_p : J_0(N) \to J_0(N)$ resulting from conjugation with ψ_0 is algebraic.

We now look at the reduction of a modular curve mod p, and the moduli space for elliptic curves over $\bar{\mathbb{F}}_p$. We begin by taking a prime $\mathfrak{p} \subset \bar{\mathbb{Z}}$ over p and we define the moduli space of curves with good reduction at $\mathfrak{p}$,

$$S_0(N)'_{gd} = \big\{[E,C] \in S_0(N) \mid E \text{ is defined over } \bar{\mathbb{Q}}, \text{ has good reduction at } \mathfrak{p}, \\ \text{and } j(E) \bmod \mathfrak{p} \notin \{0, 1728\}\big\}.$$

Next, we define $\tilde{S}_0(N)$ to be the moduli space over $\bar{\mathbb{F}}_p$: the set of equivalence classes $[E,C]$ where E is an elliptic curve over $\bar{\mathbb{F}}_p$ and C is a cyclic subgroup of order N. The reduction map $S_0(N)'_{gd} \to \tilde{S}_0(N)'$ is surjective.

Theorem 1.30 (Igusa). *Let N be a positive intger and let p be a prime not dividing N. The modular curve $X_0(N)$ has good reduction at p. Letting $\tilde{X}_0(N)_{/\mathbb{F}_p}$ be the reduction of $X_0(N)$ modulo p, we have a commutative diagram*

$$\begin{tikzcd} S_0(N)'_{gd} \arrow[r, "\psi_0"] \arrow[d] & X_0(N)_{/\mathbb{Q}} \arrow[d] \\ \tilde{S}_0(N)' \arrow[r, "\tilde{\psi}_0"'] & \tilde{X}_0(N)_{/\mathbb{F}_p}. \end{tikzcd}$$

The horizontal arrows are the identification of isomorphism classes in the moduli spaces with points on the modular curves, while the vertical arrows correspond to reduction modulo p.

The morphisms in this diagram extend to divisors, so that we have a similar diagram with $\mathrm{Div}^0(S_0(N)'_{gd})$, $\mathrm{Div}^0(\tilde{S}_0(N)')$, $\mathrm{Pic}^0(X_0(N)) \cong J_0(N)$ and $\mathrm{Pic}^0(\tilde{X}_0(N)) \cong \tilde{J}_0(N)$.

The Hecke operator T_p on $\mathrm{Pic}^0(X_0(N))$ reduces modulo p to give a commutative diagram

$$\begin{tikzcd} \mathrm{Pic}^0(X_0(N)) \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}^0(X_0(N)) \arrow[d] \\ \mathrm{Pic}^0(\tilde{X}_0(N)) \arrow[r, "\tilde{T}_p"'] & \mathrm{Pic}^0(\tilde{X}_0(N)), \end{tikzcd}$$

We compute $\tilde{T}_p$ by interpreting $\tilde{X}_0(N)$ as a moduli space. We take an elliptic curve $E_{/\bar{\mathbb{Q}}}$ with good reduction at $\mathfrak{p}$ and let C be a subgroup of order N. We also let Frob_p be an absolute Frobenius element at $\mathfrak{p}$. Note that, by definition, $\sigma_p(\tilde{E}) = \widetilde{E^{\mathrm{Frob}_p}}$, where σ_p is the Frobenius morphism $\tilde{E} \to \tilde{E}^{(p)}$.

We let D_0 be the kernel of the reduction map $E[p] \to \tilde{E}[p]$, which is of order p or p^2 (depending on whether $\tilde{E}$ is ordinary or supersingular modulo p). In both cases we have:

Lemma 1.31. *For any order p subgroup D of E,*

$$[\widetilde{E/D}, \widetilde{C+D}] = \begin{cases} [\sigma_p(\tilde{E}), \sigma_p(\tilde{C})], & \text{if } D = D_0, \\ [\sigma_p^{-1}(\tilde{E}), [p]\sigma_p^{-1}(\tilde{C})], & \text{if } D \neq D_0. \end{cases}$$

Proof. See [DS05, Lemma 8.7.1.]. □

Summing over the order-p subgroups of $E[p]$, it follows that the Hecke operator $\tilde{T}_p$ applied to the enhanced curve $[\tilde{E}, \tilde{C}]$ yields

$$\tilde{T}_p[\tilde{E}, \tilde{C}] = \sum_{D \subset E \text{ cyclic of order } p} [\widetilde{E/D}, \widetilde{C+D}] = (\sigma_p + p\sigma_p^{-1})[\tilde{E}, \tilde{C}].$$

By considering the objects $X_0(N)$, $S_0(N)'_{gd}$, their Picard groups and their respective reductions, we have the main result of this section.

Theorem 1.32 (Eichler-Shimura Relation)**.** *Let $p \nmid N$. We have $\tilde{T}_p = \sigma_{p,*} + \sigma_p^*$, so that the following diagram commutes:*

$$\begin{tikzcd}
\mathrm{Pic}^0(X_0(N)) \arrow[r, "T_p"] \arrow[d] & \mathrm{Pic}^0(X_0(N)) \arrow[d] \\
\mathrm{Pic}^0(\tilde{X}_0(N)) \arrow[r, "\sigma_{p,*}+\sigma_p^*"'] & \mathrm{Pic}^0(\tilde{X}_0(N)).
\end{tikzcd}$$

Here the superscript and subscript $*$ denote pushforward and pullback from the Frobenius endomorphism σ_p of the modular curve $\tilde{X}_0(N)$ to its Picard group, as explained in [Sil09, § II.3].

Proof. See [DS05, § 8.7] for further details. □

We now apply the Eichler-Shimura relation to a newform $f \in S_2(\Gamma_0(N))$ with integer coefficients.

Theorem 1.33. *Let $f \in S_2(\Gamma_0(N))$ be a normalized eigenform with integer coefficients, so that $K_f = \mathbb{Q}$ and $E = A_f$ is an elliptic curve. Then*

$$L(f, s) = L(E, s).$$

In particular, the L-function of E has an analytic continuation to the whole complex plane.

Sketch of proof. Let p be a prime not dividing either the level N or the conductor of the curve N_E. The following considerations (and some additional diagram chasing, showcased in [DS05, Theorem 8.8.2]) show that $a_p(f) = a_p(E)$.

1. From the isogeny $J_0(N) \sim \prod_g A_g$, the Hecke operator T_p on A_g for each newform g is given by $a_p(g)$.

2. The Hecke operator T_p on $\mathrm{Pic}^0(X_0(N)) \cong J_0(N)$ reduces to $\sigma_{p,*} + \sigma_p^*$ on $\mathrm{Pic}^0(\tilde{X}_0(N))$ by the Eichler-Shimura relation.

3. The endomorphism $\sigma_{p,*} + \sigma_p^*$ commutes with the projection $\prod_g A_g \to E$ to become $\sigma_{p,*} + \sigma_p^*$ on $\mathrm{Pic}^0(\tilde{E}) \cong \tilde{E}$.

4. The number $a_p(E)$ is precisely the trace of Frobenius on $\tilde{E}$, that is, $a_p(E) = \mathrm{Tr}(\sigma_p) = \sigma_{p,*} + \sigma_p^*$. Note further that $\mathrm{Tr}(\sigma_p) = \mathrm{Tr}(\rho_{E,\ell}(\mathrm{Frob}_p))$ for any prime $\ell \neq p$ and any absolute Frobenius element at p.

The equality for the remaining primes $p \mid N_E N$ is out of the scope of this project. □

Definition 1.34. *We say an elliptic curve $E_{/\mathbb{Q}}$ is modular if it is isogenous to an elliptic curve E_f coming from a normalized eigenform $f \in S_2(\Gamma_0(N))$. Equivalently, we say $E_{/\mathbb{Q}}$ is modular if*

$$L(E,s) = L(f,s)$$

for some normalized eigenform $f \in S_2(\Gamma_0(N))$.

With this result we can give the notion of the representation associated to a newform f with integer coefficients. Indeed, given such a newform we take its associated elliptic curve E_f, then the ℓ-adic representation associated to f is

$$\rho_{f,\ell} = \rho_{E_f,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(\mathbb{Q}_\ell).$$

If we take the pth Euler factor of L to be

$$L_p(f,T) = \det\left(1 - T\rho_{f,\ell}(\mathrm{Frob}_{\mathfrak{p}}) \middle| \, \mathrm{T}_\ell(E_f)^{I_{\mathfrak{p}}}\right),$$

then the product $\prod_p L_p(f, p^{-s})$ does indeed coincide, in a suitable right half plane, with the L-function we defined for f.

We will generalize this theorem in the next section.

1.4 Modularity of GL_2-type abelian varieties

Recall that the variety A_f associated to a newform f has an action by the ring of integers of the number field K_f, and $\dim A_f = [K_f : \mathbb{Q}] = \mathrm{rank}_{\mathbb{Z}} \mathcal{O}_{K_f}$. Forgetting about the newform for a moment, we let $A_{/\mathbb{Q}}$ be an abelian variety and suppose that K is a number field acting on A up to isogeny over $\mathbb{Q}$,

$$K \hookrightarrow \mathrm{End}^0(A).$$

Then K acts on the tangent space of A at 0, which is a $\mathbb{Q}$-vector space of dimension $\dim A$. The dimension of this vector space is therefore a multiple of $[K : \mathbb{Q}]$, so that we have $[K : \mathbb{Q}] \mid \dim A$, and in particular $[K : \mathbb{Q}] \leq \dim A$.

Proposition 1.35. *If K is a number field of degree $\dim A$ which is contained in $\mathrm{End}^0(A)$, then the Tate modules $\mathrm{V}_\ell(A)$ associated with A are free of rank two over $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Accordingly, the action of $G_{\mathbb{Q}}$ on $\mathrm{V}_\ell(A)$ defines a representation with values in $\mathrm{GL}_2(K \otimes \mathbb{Q}_\ell)$, and every prime λ of $\mathcal{O}_K$ lying over ℓ gives a representation*

$$\rho_\lambda : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_\lambda),$$

where K_λ is the completion of K with respect to the λ-adic valuation.

Proof. We can see A as a complex torus $\mathbb{C}^d/\Lambda$, where $d = \dim A$. Then Λ is an $\mathcal{O}_K$-module of $\mathbb{Z}$-rank $2d$. Since K is a number field of degree d, $\Lambda \otimes \mathbb{Q}$ is a free K-module of rank 2, and so $\Lambda \otimes \mathbb{Q}_\ell$ is free of rank 2 over $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. The isomorphism $\mathrm{T}_\ell(A) \cong \Lambda \otimes \mathbb{Z}_\ell$ is immediate, and so

$$\mathrm{V}_\ell(A) = \mathrm{T}_\ell(A) \otimes \mathbb{Q} \cong \Lambda \otimes \mathbb{Z}_\ell \otimes \mathbb{Q} \cong \Lambda \otimes \mathbb{Q}_\ell$$

shows $\mathrm{V}_\ell(A)$ is free of rank 2 over $K \otimes \mathbb{Q}_\ell$.

The representation with values in $\mathrm{GL}_2(K \otimes \mathbb{Q}_\ell)$ follows from choosing a basis of $\mathrm{V}_\ell(A)$. Finally, we can use the isomorphism $K \otimes \mathbb{Q}_\ell \cong \prod_{\lambda|\ell} K_\lambda$ to get a 2-dimensional λ-adic representation for each prime λ over ℓ. □

Definition 1.36. *We say that an abelian variety $A_{/\mathbb{Q}}$ is of GL_2-type if its endomorphism algebra $\mathrm{End}^0(A)$ contains a number field of degree $\dim A$.*

We say that an abelian variety $A_{/\mathbb{Q}}$ of GL_2-type is primitive if it is not isogenous to some abelian variety B^n with $B_{/\mathbb{Q}}$ of GL_2-type.

Theorem 1.37. *Let $A_{/\mathbb{Q}}$ be an abelian variety of GL_2-type. Then the following are equivalent:*

(i) A is primitive,

(ii) A is simple over $\mathbb{Q}$,

(iii) The endomorphism algebra $\mathrm{End}^0(A)$ is a number field whose degree coincides with the dimension of A.

Proof. See [Rib04], Theorem 2.1. □

We remark that this does not say $\mathrm{End}^0(A_{\bar{\mathbb{Q}}})$ could not grow if we consider endomorphisms defined over an extension of $\mathbb{Q}$, the simplest example of this behavior is given by a CM elliptic curve.

Going back to modular curves, we now consider the representation associated to the Jacobian $J_0(N)$. We have already used that $J_0(N)$ has a model over $\mathbb{Q}$, and so its ℓ^n-torsion is defined over $\bar{\mathbb{Q}}$. This gives a $2g$-dimensional ℓ-adic Galois representation

$$\rho_{J_0(N),\ell} : G_{\mathbb{Q}} \to \mathrm{Aut}(\mathrm{V}_\ell(J_0(N))) \cong \mathrm{GL}_{2g}(\mathbb{Q}_\ell).$$

Since $J_0(N)$ has good reduction at any prime $p \nmid N$, by Theorem 1.17 $\rho_{J_0(N),\ell}$ is unramified at every prime $p \nmid \ell N$. In addition, if $p \nmid \ell N$ then the reduction modulo p

$$J_0(N)[\ell^n] \to \tilde{J}_0(N)[\ell^n]$$

is an isomorphism. Taking an absolute Frobenius element $\mathrm{Frob}_{\mathfrak{p}}$ over p, the Eichler-Shimura relation restricted to the ℓ-torsion

$$\begin{tikzcd} J_0(N)[\ell^n] \arrow[r, "T_p"] \arrow[d, "\sim"'] & J_0(N)[\ell^n] \arrow[d, "\sim"] \\ \tilde{J}_0(N)[\ell^n] \arrow[r, "\sigma_{p,*}+\sigma_p^*"'] & \tilde{J}_0(N)[\ell^n] \end{tikzcd}$$

implies that T_p equals $\mathrm{Frob}_{\mathfrak{p}} + p \, \mathrm{Frob}_{\mathfrak{p}}^{-1}$ on $J_0(N)[\ell^n]$, hence $\rho_{J_0(N),\ell}(\mathrm{Frob}_{\mathfrak{p}})$ satisfies the polynomial equation

$$\det(1 - X \, \mathrm{Frob}_{\mathfrak{p}} \mid \mathrm{T}_\ell(J_0(N))^{I_{\mathfrak{p}}}) = 1 - T_p X + p X^2 = 0. \tag{1.8}$$

Now fix some normalized eigenform $f \in S_2(\Gamma_0(N))$. Composing the isogeny $J_0(N) \to \prod_{[g]} A_g^{m_g}$ with the projection onto A_f, the maps $J_0(N)[\ell^n] \to A_f[\ell^n]$ are surjective. Moreover, the projection is defined over $\mathbb{Q}$, so the kernel is stable under the action of $G_{\mathbb{Q}}$. This allows us to project onto $\mathrm{T}_\ell(A_f)$ to get an ℓ-adic representation of dimension $2d = 2 \dim A_f$,

$$\rho_{A_f,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_{2d}(\mathbb{Q}_\ell).$$

This is the ℓ-adic representation we would associate normally to A_f, but the detour through $J_0(N)$ will be useful shortly. First, because $\rho_{A_f,\ell}$ factorizes through $\rho_{J_0(N),\ell}$, we obtain immediately that the former is unramified at all primes $p \nmid \ell N$.

What is more, the Eichler-Shimura relation goes through to A_f. If we choose a particular prime λ of K_f over ℓ, the fact that T_p acts as $a_p(g)$ on each A_g and (1.8) imply that $\rho_{A_f,\lambda}(\mathrm{Frob}_{\mathfrak{p}})$ satisfies the polynomial equation

$$1 - a_p(f) T + p T^2 = 0.$$

But the ℓ-adic representation of A_f splits as the product of many 2-dimensional ℓ-adic representations,

$$\rho_{A_f,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_2(K_f \otimes \mathbb{Q}_\ell) \cong \prod_{\lambda' \mid \ell} \mathrm{GL}_2(K_{f,\lambda'}).$$

Therefore, by considering the embeddings of K_f in $\mathbb{C}$, the characteristic polynomial of Frobenius $\det(1 - T \, \mathrm{Frob}_{\mathfrak{p}} \mid \mathrm{T}_\ell(A_f)^{I_{\mathfrak{p}}})$ will split as a product of the d factors corresponding to each piece of the representation,

$$\prod_{\sigma : K_f \hookrightarrow \mathbb{C}} (1 - a_p(f)^\sigma T + p T^2) = \prod_{\sigma : K_f \hookrightarrow \mathbb{C}} (1 - a_p(f^\sigma) T + p T^2).$$

After doing some more work on the bad primes, one arrives at the following generalization of Theorem 1.33.

Theorem 1.38. *Let N be a positive integer and let $f = \sum_{n>0} a_n q^n \in S_2(\Gamma_0(N))$ be a normalized eigenform. Then the L-functions of A_f and f are related by*

$$L(A_f, s) = \prod_{\sigma : K_f \hookrightarrow \mathbb{C}} L(f^\sigma, s).$$

Definition 1.39. *An abelian variety $A_{/\mathbb{Q}}$ is said to be modular if it is isogenous to A_f for eigenform $f \in S_2(\Gamma_0(N))$. In that case, we have the equality of L-functions*

$$L(A, s) = \prod_{\sigma : K_f \hookrightarrow \mathbb{C}} L(f^\sigma, s).$$

We end this chapter by stating two converse statements. The first one is a particular case of the second, but we separate them due to historical precedence.

Theorem 1.40 (Wiles,Taylor-Wiles,Breuil-Conrad-Diamond-Taylor)**.** *Let $E_{/\mathbb{Q}}$ be an elliptic curve of conductor N. Then there exists some newform $f \in S_2(N)$ with integer coefficients such that*

$$L(E, s) = L(f, s).$$

Moreover, E is isogenous to the elliptic curve E_f obtained by the Eichler-Shimura construction.

The class of GL_2-type abelian varieties is the target of the generalized version of this result. However, we have made our construction of the varieties A_f only for modular forms with respect to groups $\Gamma_0(N)$. In this case, the field K_f is always totally real [Rib04, Lemma 3.4], and there are GL_2-type varieties whose endomorphism algebra is a CM field (an imaginary quadratic extension of a totally real field). For those, one needs to consider modular forms with respect to the groups

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\},$$

and some details in our theory have to be completed by introducing characters of the group $(\mathbb{Z}/N\mathbb{Z})^\times$. Ribet [Rib04] proved the modularity theorem for GL_2-type varieties:

Theorem 1.41 (Ribet)**.** *Let A be an abelian variety over $\mathbb{Q}$ of GL_2-type. Assuming Serre's conjecture on representations of $G_{\mathbb{Q}}$, there is a newform $f \in S_2(\Gamma_1(N))$ such that*

$$L(A, s) = \prod_{\sigma : K_f \hookrightarrow \mathbb{C}} L(f^\sigma, s),$$

and moreover A is isogenous to the factor A_f of $\mathrm{Jac}(X_1(N))$ obtained by the Eichler-Shimura construction.

This became an unconditional result with the proof of Serre's modularity conjecture by Dieulefait [Die07] and Khare and Wintenberger [KW09a; KW09b].

A good survey on the various conjectures on modularity of representations can be found in [DS05, § 9.6].

We are now interested in abelian varieties over $\mathbb{Q}$ which are not of GL_2-type. The simplest case we have to look at is that of a surface $A_{/\mathbb{Q}}$ with

$$\mathrm{End}(A) = \mathbb{Z}.$$

The remaining two chapters propose a substitute for the classical, one-variable modular forms.

Chapter 2

Siegel modular forms

We now give the theory of Siegel modular forms with respect to the paramodular group. We have tried to parallel the exposition of Section 1.2 on classical modular forms, and many concepts follow a perfect analogy. However, we have not given the details of level-raising operators and newforms, since we do not need them for the purposes of the current project.

The second part of the chapter gives details on the construction of paramodular forms through theta blocks and the Gritsenko lift. We give the example of the nonlift of level 277. Finally, we explain the specialization method to compute Hecke eigenvalues given in [Bru+19].

2.1 Definitions and Fourier coefficients

Definition 2.1. *The Siegel upper half space is the matrix space*

$$\mathcal{H}_2 = \{Z \in \mathrm{Mat}_{2\times 2}^{sym}(\mathbb{C}) \mid \mathrm{Im}(Z) > 0\}$$

where $\mathrm{Im}(Z) > 0$ *means that the imaginary part of* Z *is positive definite as a real* $n \times n$ *symmetric matrix.*

We will sometimes write $\mathcal{H}_1 = \mathcal{H}$ to distinguish the upper half plane from $\mathcal{H}_2$. The real symplectic group of genus n is given by

$$\mathrm{Sp}_{2n}(\mathbb{R}) = \{M \in \mathrm{GL}_{2n}(\mathbb{R}) \mid M^T J M = J\},$$

where J is the block matrix $\begin{pmatrix} 0 & I_n \\ -I_n & 0 \end{pmatrix}$. A short computation shows that $\mathrm{Sp}_2(\mathbb{R}) = \mathrm{SL}_2(\mathbb{R})$. We will focus on the genus-2 case, $\mathrm{Sp}_4(\mathbb{R})$. The symplectic group $\mathrm{Sp}_4(\mathbb{R})$ acts transitively on $\mathcal{H}_2$ as

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \langle Z \rangle = (AZ + B)(CZ + D)^{-1},$$

where $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}_4(\mathbb{R})$. A slightly larger group is the general real positive symplectic group,

$$\mathrm{GSp}_4^+(\mathbb{R}) = \{M \in \mathrm{GL}_4(\mathbb{R}) \mid M^T JM = \mu(M)J,\ \mu(M) > 0\}.$$

The number $\mu(M)$ is called the multiplier of M, it satisfies $\mu(M) = \det(M)^{1/2}$. We define $\mathrm{Sp}_4(\mathbb{Q})$ and $\mathrm{GSp}_4^+(\mathbb{Q})$ in a similar manner.

Definition 2.2. *We denote by $\mathcal{O}(\mathcal{H}_2)$ the set of holomorphic functions on $\mathcal{H}_2$. The weight k slash operator of $M \in \mathrm{GSp}_4^+(\mathbb{R})$ on a function $f \in \mathcal{O}(\mathcal{H}_2)$ is given by*

$$(f|_k M)(Z) := \mu(M)^{2k-3} j(M\langle Z\rangle)^{-k} f(M\langle Z\rangle),$$

where $j(M\langle Z\rangle) := \det(CZ + D)$.

Let $\Gamma \subset \mathrm{Sp}_4(\mathbb{R})$ be a discrete subgroup commensurable with $\mathrm{Sp}_4(\mathbb{Z})$ (i.e. such that $\Gamma \cap \mathrm{Sp}_4(\mathbb{Z})$ has finite index in $\mathrm{Sp}_4(\mathbb{Z})$).

Definition 2.3. *We say that an holomorphic function $f : \mathcal{H}_2 \to \mathbb{C}$ is a Siegel modular form of weight k for Γ if*

1. *$f|_k M = f$ for all $M \in \Gamma$,*
2. *For all matrices $M \in \mathrm{Sp}_4(\mathbb{Q})$ and for all $Y_0 > 0$, $f|_k M$ is bounded on $\{Z \in \mathcal{H}_2 \mid \mathrm{Im}(Z) \geq Y_0\}$. The inequality $\mathrm{Im}(Z) \geq Y_0$ here means the matrix $\mathrm{Im}(Z) - Y_0$ is positive semidefinite.*

In our case, we are interested in the space of paramodular forms, which are the Siegel modular forms for the paramodular group $\Gamma = K(N)$, for $N \in \mathbb{Z}_{\geq 1}$. The paramodular group of level N is the group

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

Example 2.4. *An abelian surface A with polarization type $(1, N)$, $N \in \mathbb{N}$, can we written as a complex torus*

$$A \cong \mathbb{C}^2/(Z \mid T)\mathbb{Z}^4$$

where $(Z \mid T)$ is called the period matrix and $T = \mathrm{diag}(1, N)$. The matrix Z is symmetric and $\mathrm{Im}\, Z$ is positive definite, so Z belongs to the Siegel upper half space $\mathcal{H}_2$. The Riemann form associated to A in this basis is given by the matrix

$$J_N = \begin{pmatrix} 0 & T \\ -T & 0 \end{pmatrix}.$$

The group $\mathrm{Sp}_4(J_N, \mathbb{Z}) = \{M \in \mathrm{Mat}_{4\times 4}(\mathbb{Z}) \mid MJ_NM^t = J_N\}$ is called the parasymplectic (or paramodular) group, and it is indeed a conjugate of the *paramodular group $K(N)$. More specifically, we have $K(N)^t = I_N^{-1}\operatorname{Sp}_4(J_N, \mathbb{Z}) I_N$, where $I_N = \operatorname{diag}(1,1,1,N)$.*

The quotient space $\mathcal{A}_N = K(N)^t\mathcal{H}_2$ is the coarse moduli space of abelian surfaces with polarization type $(1, N)$. This generalises the bijection

$$S_0(N) \leftrightarrow X_0(N)$$

given in Proposition 1.29. Unfortunately, we will not able to push this analogy further, because we cannot relate the Siegel paramodular forms of our interest (weight 2) with the cohomology of $\mathcal{A}_N$.

As with classical modular forms, we are able to work with Fourier expansions, which are a major computational tool. We shall prove Koecher's principle for Siegel paramodular forms, which gives their Fourier expansion and proves that we do not need to check the boundedness condition at infinity.

We work with the following set of matrices:

$$\mathcal{X}_2(N) := \left\{ \begin{pmatrix} n & r/2 \\ r/2 & Nm \end{pmatrix} \mid n, r, m \in \mathbb{Z} \right\}.$$

As usual we let $e(\tau) = e^{2\pi i \tau}$. For 2-by-2 matrices T and Z, we define $\langle T, Z\rangle := \operatorname{Tr}(TZ)$, which is a symmetric bilinear form.

Lemma 2.5. *A paramodular form $f \in M_k(K(N))$ has a Fourier expansion*

$$f(Z) = \sum_{T \in \mathcal{X}_2(N)} a(T; f) e(\langle T, Z\rangle).$$

Proof. Given any real symmetric matrix S, the block matrix

$$M_S = \begin{pmatrix} I_2 & S \\ 0 & I_2 \end{pmatrix}$$

belongs to $\operatorname{Sp}_4(\mathbb{R})$. If we take $S = \begin{pmatrix} 1 & 1 \\ 1 & \frac{1}{N} \end{pmatrix}$, then $M_S \in K(N)$, so for all $Z \in \mathcal{H}_2$ we have $f(Z + S) = f(Z)$. Letting $Z = \begin{pmatrix} \tau & z \\ z & \omega \end{pmatrix}$, the Fourier expansion of f will have terms of the form $ae^{2\pi i (n\tau + rz + Nm\omega)}$ with $n, r, m \in \mathbb{Z}$, and the form in the exponent can be expressed by the trace

$$\langle T, Z \rangle = \operatorname{Tr}(TZ),\ T = \begin{pmatrix} n & r/2 \\ r/2 & Nm \end{pmatrix} \in \mathcal{X}_2(N).$$

□

The set of matrices $\mathcal{X}_2(N)$ is fairly intractable, and storing Fourier coefficients of a given modular form without further simplification would be inefficient. To be able to perform computations, we introduce an invariance of coefficients borrowing from the theory of binary quadratic forms. We say a matrix

$$\begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} \in M_2(\mathbb{R})$$

representing a quadratic form $ax^2 + bxy + cy^2$ is Legendre reduced if $0 \leq b \leq a \leq c$. Let

$$\Gamma^0_{\pm}(N) = \left\{ \begin{pmatrix} a & Nb \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}) \right\}$$

act on $\mathcal{X}_2(N)$ by $T[U] = U^t T U$, so that $\mathrm{GL}_2(\mathbb{Z}) = \Gamma^0_{\pm}(1)$ acts on $\mathcal{X}_2(1)$.

Lemma 2.6. *Given a matrix $T \in \mathcal{X}_2(N)$, there is a unique Legendre reduced matrix $\tilde{T} \in \mathcal{X}_2(1)$ and some $U \in \mathrm{GL}_2(\mathbb{Z})$ such that $T[U] = \tilde{T}$. Moreover, there is an algorithm to determine whether two definite matrices $T, S \in \mathcal{X}_2(N)$ are in the same $\Gamma^0_{\pm}(N)$-orbit.*

Proof. The first statement is Theorem 2.8 in [Cox89], modified to allow equivalence up to integral matrices of determinant -1. Algorithm 1 in Appendix A computes the Legendre reduced form of T.

For the second statement, we let $\mathrm{GL}_2(\mathbb{Z})$ act on $\mathcal{X}_2(1) \times \mathbb{P}(\mathbb{Z}/N\mathbb{Z})$ as $(T, v) \mapsto (T[U], U^{-1}v)$. We can identify $\mathcal{X}_2(N)$ with

$$\mathcal{X}_2(N) \times \left\{ \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \subseteq \mathcal{X}_2(1) \times \mathbb{P}(\mathbb{Z}/N\mathbb{Z}),$$

which is invariant under the action of $\Gamma^0_{\pm}(N)$.

Therefore, $(T, (0,1)^t)$ and $(S, (0,1)^t)$ are in the same $\mathrm{GL}_2(\mathbb{Z})$-orbit if and only if T and S are in the same $\Gamma^0_{\pm}(N)$-orbit. Given $S, T \in \mathcal{X}_2(N)$, we reduce $(T, (0,1)^t)$ and $(S, (0,1)^t)$ with algorithm A.1 to obtain $(\tilde{T}, u)$ and $(\tilde{S}, v)$ respectively, with $\tilde{T}$ and $\tilde{S}$ Legendre reduced. By the uniqueness of the reduced form, S and T are in the same $\Gamma^0_{\pm}(N)$-orbit as long as $\tilde{S} = \tilde{T}$ and $u = Mv$ for some $M \in \mathrm{Aut}_{\mathbb{Z}}(T)$. The automorphism group of T is computable and finite as long as T is definite, so we indeed have the claimed algorithm. □

It is worth noting that given a pair $(T, v) \in \mathcal{X}_2(1) \times \mathbb{P}(\mathbb{Z}/N\mathbb{Z})$ with both components of the vector v coprime and T Legendre reduced, we may take a matrix $U \in \mathrm{GL}_2(\mathbb{Z})$ with v as its second column, and then $T[U]$ will be a matrix in $\mathcal{X}_2(N)$.

Lemma 2.7. *Let $f \in M_k(K(N))$. For all $T \in \mathcal{X}_2(N)$ and $U \in \Gamma^0_{\pm}(N)$, $a(T[U]; f) = \det(U)^k a(T; f)$.*

Proof. For any $U \in \Gamma^0_{\pm}(N)$ the block matrix $\begin{pmatrix} U^{-1} & 0 \\ 0 & U^t \end{pmatrix}$ is in $K(N)$, so setting $U^* = (U^{-1})^t$ we have $f(Z[U^*]) = \det(U)^k f(Z)$. Looking at the Fourier expansion,

$$\begin{aligned}
f(Z[U^*]) &= \sum_{T\in\mathcal{X}_2(N)} a(T;f)e(\mathrm{Tr}(TU^{-1}ZU^*)) = \sum_{T\in\mathcal{X}_2(N)} a(T;f)e(\mathrm{Tr}(U^*TU^{-1}Z)) \\
&= \sum_{T\in\mathcal{X}_2(N)[U]} a(T[U];f)e(\langle T,Z\rangle) = \det(U^t)^k f(Z) \\
&= \det(U)^k \sum_{T\in\mathcal{X}_2(N)} a(T;f)e(\langle T,Z\rangle).
\end{aligned}$$

This shows that $a(T[U];f) = \det(U)^k a(T;f)$ for any $T \in \mathcal{X}_2(N)$ and $U \in \Gamma^0_\pm(N)$. □

Corollary 2.8. *Let D be a positive integer and $f \in M_k(K(N))$. Then the set*

$$\{a(T;f) \mid T \in \mathcal{X}_2(N) \text{ positive definite with } \det(2T) = D\}$$

is finite.

Proof. Let $T \in \mathcal{X}_2(N)$ with $\det(2T) = D$ and let $\tilde{T}$ be the Legendre reduced form of T. According to Lemma 2.6, the $\Gamma^0_\pm(N)$-orbit of T is represented by at least one element of $\{\tilde{T}\} \times \mathbb{P}(\mathbb{Z}/N\mathbb{Z})$, and by Lemma 2.7 this bounds the number of possible values of $a(T;f)$. □

Proposition 2.9 (Koecher principle)**.** *A paramodular form $f \in M_2(K(N))$ has a Fourier expansion of the form*

$$f(Z) = \sum_{T\geq 0} a(T;f)e(\langle T,Z\rangle),$$

where T runs over positive semidefinite symmetric matrices in the set $\mathcal{X}_2(N)$. In particular, $f(Z)$ is bounded in every region $\{Z \in \mathcal{H}_2 \mid Y = \mathrm{Im}(Z) \geq Y_0 > 0\}$.

Proof. We have already seen that f has a Fourier expansion

$$f(Z) = \sum_{T\in\mathcal{X}_2(N)} a(T;f)e(\langle T,Z\rangle).$$

We only need to show that this sum concerns only those T which are positive semidefinite. We use the invariance $a(T[U];f) = a(T;f)$ for $U \in \Gamma^0_\pm(N)$. If $a(T;f)$ is not zero, then for any symmetric positive definite Y the series

$$\sum_S e^{-2\pi\langle S,Y\rangle},$$

where S ranges through all the different matrices $S = T[U]$ for $U \in \Gamma^0_\pm(N)$, must converge. We shall show that this series diverges for $Y = I_2$ if T is not positive semidefinite. In this case there is a vector $g = (a,b) \in \mathbb{Z}^2$ with coprime coordinates such that $T[g] < 0$. After changing g by $(1 + kaN, kbN)$ for a suitable integer k, we can also assume that $\gcd(a, N) = 1$. Hence there is a matrix

$$U = \begin{pmatrix} a & Nx \\ b & y \end{pmatrix} \in \Gamma^0_{\pm}(N)$$

such that $T[U] = \begin{pmatrix} n & r/2 \\ r/2 & Nm \end{pmatrix}$ satisfies $n < 0$. Now for any

$$V = \begin{pmatrix} 1 & Nx \\ 0 & 1 \end{pmatrix} \in \Gamma^0_{\pm}(N)$$

the matrix $S = T[V]$ satisfies $\langle S, I_2 \rangle = \mathrm{Tr}(S) = nN^2x^2 + rNx + n + Nm$. We can let x vary, and in particular $\langle S, I_2 \rangle \to -\infty$ as $x \to \infty$. Therefore

$$e^{-2\pi \langle S, I_2 \rangle} \to \infty \text{ for } x \to \infty,$$

and the series has to diverge. It follows that $a(T; f) = 0$ whenever T is not positive semidefinite. □

The three lemmas prior to the Koecher principle give us the proper way of storing Fourier coefficients of a given form f. If we want to store the coefficients $a(T; f)$ with $\det(2T)$ in a given range, we only have to store finitely many of them, corresponding to matrices representing the finitely many $\Gamma^0_{\pm}(N)$-orbits in $\mathcal{X}_2(N)$ with this determinant bound.

Definition 2.10. *We define the Siegel map $\Phi : M_k(\Gamma) \to \mathcal{O}(\mathcal{H}_1)$ by*

$$\Phi(f)(z) = \lim_{\lambda \to +\infty} f \begin{pmatrix} z & 0 \\ 0 & i\lambda \end{pmatrix}.$$

We say that f vanishes at the cusps if for all matrices $M \in \mathrm{Sp}_4(\mathbb{Q})$, $\Phi(f|_k M) = 0$.

The space $S_k(\Gamma)$ of cusp forms is precisely the set of $f \in M_k(\Gamma)$ that vanish at the cusps. The space of paramodular cusp forms of weight k and level N is $S_k(K(N)) \subset M_k(K(N))$.

If $T \in \mathcal{X}_2(N)$ is a positive semidefinite matrix with lower right entry equal to zero, then it needs to be of the form $T = \begin{pmatrix} t & 0 \\ 0 & 0 \end{pmatrix}$. From the limit

$$\lim_{t \to \infty} e(\langle T, \begin{pmatrix} z & 0 \\ 0 & it \end{pmatrix} \rangle) = 0$$

one concludes

$$\Phi(f)(z) = \sum_{t \geq 0} a\left(\begin{pmatrix} t & 0 \\ 0 & 0 \end{pmatrix} ; f \right) e(tz).$$

Applying this fact to $f|_k M$ for all $M \in \mathrm{Sp}_4(\mathbb{Q})$ one proves the following.

Proposition 2.11. *Let f be a paramodular form. Then f is a cusp form if and only if its Fourier expansion reads*

$$f(Z) = \sum_{T>0} a(T; f) e(\langle T, Z \rangle),$$

this is, $T > 0$ whenever $a(T; f) \neq 0$.

We end this section by mentioning certain weights and levels for which all paramodular forms are cuspidal, we are interested in the particular case of weight $k = 2$. Consider the map

$$\begin{aligned} \iota : \mathcal{H} \times \mathcal{H} &\to \mathcal{H}_2 \\ (\tau, \omega) &\mapsto \begin{pmatrix} \tau & 0 \\ 0 & \omega \end{pmatrix}, \end{aligned}$$

which takes any form $f \in M_k(K(N))$ to $\iota^* f \in M_k(\mathrm{SL}_2(\mathbb{Z})) \otimes M_k(\mathrm{SL}_2(\mathbb{Z}))|_k \begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}$ by precomposition. For $k = 2$ or k odd the space $M_k(\mathrm{SL}_2(\mathbb{Z}))$ is zero, so $\iota^*(M_k(K(N)) = 0$. Hence the Siegel map Φ is zero on all of $M_k(K(N))$. By extending this idea to consider all the cusps, [PSY17] prove the following.

Proposition 2.12. *Let N be a squarefree positive integer, and let k be a positive integer. If $k = 2$ or k is odd then $M_2(K(N)) = S_2(K(N))$. If $k = 4, 6, 8, 10, 14$ then for all $f \in M_k(K(N)), f \in S_k(K(N))$ if and only if $a(0; f) = 0$.*

2.2 Hecke operators

To simplify the notation we let $\Gamma = K(N)$. For each matrix $M \in \mathrm{GSp}_4^+(\mathbb{Q})$ we have a corresponding double coset

$$\Gamma M \Gamma = \{G_1 M G_2 \mid G_1, G_2 \in \Gamma\}$$

with which we define a Hecke operator

$$T(\Gamma M \Gamma) : M_k(\Gamma) \to M_k(\Gamma)$$

as follows. The group Γ has a left action on $\Gamma M \Gamma$, so we can take representatives M_j for the left cosets of $\Gamma \backslash \Gamma M \Gamma$ so that $\Gamma M \Gamma = \bigsqcup_j \Gamma M_j$. Provided that this disjoint union is finite, we define

$$f|_k T(\Gamma M \Gamma) = \sum_j f|_k M_j.$$

This action is well-defined and it depends only on the dobule coset. Moreover, $T(\Gamma M \Gamma)$ preserves cusp forms.

For each prime $p \nmid N$, we define a Hecke operator

$$T(p) := T(\Gamma \operatorname{diag}(1, 1, p, p) \Gamma).$$

Its double coset decomposes as

$$\begin{aligned}
&\Gamma \operatorname{diag}(1,1,p,p)\Gamma \qquad (2.1)\\
&= \Gamma \begin{pmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ & & 1 & 0 \\ & & 0 & 1 \end{pmatrix} + \sum_{i \bmod p} \Gamma \begin{pmatrix} 1 & 0 & i & 0 \\ 0 & p & 0 & 0 \\ & & p & 0 \\ & & 0 & 1 \end{pmatrix} \qquad (2.2)\\
&+ \sum_{i,j \bmod p} \Gamma \begin{pmatrix} p & 0 & 0 & 0 \\ i & 1 & 0 & j \\ & & 1 & -i \\ & & 0 & p \end{pmatrix} + \sum_{i,j,k \bmod p} \Gamma \begin{pmatrix} 1 & 0 & i & j \\ 0 & 1 & j & k \\ & & p & 0 \\ & & 0 & p \end{pmatrix}. \qquad (2.3)
\end{aligned}$$

The action of $T(p)$ on the Fourier coefficients $a(T;f)$ is seen to be

$$\begin{aligned}
a(T; f|_k T(p)) &= a(pT; f) + p^{k-2} \sum_{j \bmod p} a\left(\frac{1}{p} T \begin{bmatrix} 1 & 0 \\ j & p \end{bmatrix}; f\right) \qquad (2.4)\\
&+ p^{k-2} a\left(\frac{1}{p} T \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}; f\right) + p^{2k-3} a\left(\frac{1}{p} T; f\right). \qquad (2.5)
\end{aligned}$$

We define another Hecke operator, also for $p \nmid N$, by

$$T_1(p^2) := T(\Gamma \operatorname{diag}(1,p,p^2,p)\Gamma).$$

Its coset decomposition and action on Fourier coefficients is described in [Bru+19]. We define two additional operators

$$\begin{aligned}
T_2(p^2) &:= T(\Gamma \operatorname{diag}(p,p,p,p)\Gamma) = p^{2k-6} id.\\
B(p^2) &:= p(T_1(p^2) + (1+p^2)T_2(p^2)).
\end{aligned}$$

If $f \in M_k(\Gamma)$ is an eigenform with

$$\begin{cases} f|_k T(p) & = a_p(f) f, \\ f|_k T_1(p^2) & = a_{1,p^2}(f) f, \end{cases}$$

then f is also an eigenform for $B(p^2)$ with eigenvalue $b_{p^2}(f) = p a_{1,p^2}(f) + p^{2k-5}(1+p^2)$. Roberts and Schmidt [RS06; RS07] assign to f the *spinor Euler factor* (also called the *spinor Hecke polynomial*) at $p \nmid N$

$$Q_p(f,T) := 1 - a_p(f)T + b_{p^2}(f)T^2 - p^{2k-3}a_p(f)T^3 + p^{4k-6}T^4. \qquad (2.6)$$

If f has integral Fourier coefficients, then $Q_p(f,T) \in 1 + T\mathbb{Z}[T]$. The coefficients of $Q_p(f,T)$ justify the choice of notation for the Euler factors L_p in equation (1.4). These factors come from associating a system of compatible Galois representations $\rho_{f,\ell} : G_{\mathbb{Q}} \to \mathrm{GSp}_4(\bar{\mathbb{Q}}_\ell)$ to f, see for example [Bru+19, Section 4.3].

As in the classical modular case, paramodular forms have a strong multiplicity one theorem. This means that an eigenform $f \in S_k(K(N))$ is determined by all but a finite number of its Hecke eigenvalues, as is proven in [Sch18, Theorem 2.6].

However, it is unclear how to recover the Fourier coefficients of f from its Hecke eigenvalues, something that would be immediate for classical modular forms (see Theorem 1.24). Using equation (2.4) to build a linear system seems futile at first, since it should lead to an ever growing amount of variables. Nonetheless, we can restrict to the case where most terms in the expression vanish to obtain some simple relations between infinitely many coefficients.

Proposition 2.13. *Let $f \in S_k(K(N))$ be a Hecke eigenform with Fourier expansion*

$$f(Z) = \sum_{T>0} a(T;f)e(\langle T, Z\rangle).$$

Fix $T = \begin{pmatrix} n & r/2 \\ r/2 & Nm \end{pmatrix}$ with determinant Δ, and let p be a prime not dividing Nm. Let $K = \mathbb{Q}(\sqrt{-\Delta})$.

(i) If p is inert in K, then

$$a(pT;f) = a_p a(T;f),$$

where a_p is the eigenvalue of f for $T(p)$.

(ii) If p is ramified in K then there is a single integer $0 \leq a < p$ such that

$$a(pT;f) = a_p a(T;f) - p^{k-2} a\left(\frac{1}{p}T\begin{bmatrix} 1 & 0 \\ a & p \end{bmatrix}; f\right).$$

(iii) If p is split in K then there are two distinct integers $0 \leq a < b < p$ such that

$$a(pT;f) = a_p a(T;f) - p^{k-2}\left(a\left(\frac{1}{p}T\begin{bmatrix} 1 & 0 \\ a & p \end{bmatrix}; f\right) + a\left(\frac{1}{p}T\begin{bmatrix} 1 & 0 \\ b & p \end{bmatrix}; f\right)\right).$$

In particular $a(T;f)$ determines infinitely many Fourier coefficients of f.

Proof. We consider equation (2.4), which also equals $a_p a(T;f)$. The last two terms are forced to be zero, because $p \nmid Nm$. For any j,

$$T\begin{bmatrix} 1 & 0 \\ j & p \end{bmatrix} = \begin{pmatrix} n + jr + j^2Nm & p\frac{r}{2} + jpNm \\ p\frac{r}{2} + jpNm & p^2Nm \end{pmatrix},$$

so $a\left(\frac{1}{p}T\begin{bmatrix} 1 & 0 \\ j & p \end{bmatrix}; f\right)$ can only be nonzero if p divides $n + jr + j^2Nm$. Again since $p \nmid Nm$, this will happen exactly when j is a root mod p of the polynomial $P_T(X) = NmX^2 + rX + n$. This polynomial has 0, 1 or 2 roots mod p when p is inert, ramified or split in $\mathbb{Q}[X]/P_T(X)$. This is precisely the field K, because $P_T(X)$ has discriminant $r^2 - 4Nmn = -\det(2T) = -4\Delta$. □

We conclude the section with a comment on level-raising and newforms. Given any integer $N > 1$, the matrix

$$\begin{pmatrix} 1 & & & \\ & & & 1/N \\ & & -1 & \\ & N & & \end{pmatrix}$$

lies in $K(N)$ and no other paramodular group. This means that, even if $N|M$, there is no inclusion between the groups $K(N)$ and $K(M)$, and hence a paramodular form of level N is not necessarily a paramodular form of level M. Roberts and Schmidt [RS06] give level-raising operators

$$\begin{aligned} \eta_p :& M_k(K(N)) \to M_k(K(Np^2)), \\ \theta'_p :& M_k(K(N)) \longrightarrow M_k(K(Np)), \\ \theta_p :& M_k(K(N)) \longrightarrow M_k(K(Np)), \end{aligned}$$

which are defined in terms of matrix actions and preserve cusp forms. One can define a Petersson scalar product, which allows for a definition of old and new subspaces in terms of the product and the images of η_p, θ'_p and θ_p for all primes p. A newform is then defined as a cusp form in the new subspace which is an eigenform with respect to all Hecke operators.

Thanks to the fact that there are no Siegel modular forms of level 1 [Fre83, Satz 3.15], all forms in prime level are new. This will be enough when we give the example in level 277 for its later usage with paramodularity.

2.3 Construction of paramodular forms

The Fourier expansion of a paramodular cusp form $f \in S_k(K(N))$,

$$f\begin{pmatrix} \tau & z \\ z & \omega \end{pmatrix} = \sum_{T \in \mathcal{X}_2(N), T>0} a(T; f) e\left(\langle T, \begin{pmatrix} \tau & z \\ z & \omega \end{pmatrix} \rangle\right)$$

can be rearranged as a Fourier-Jacobi expansion, by setting $q = e(\tau), \zeta = e(z)$,

$$\begin{aligned} f\begin{pmatrix} \tau & z \\ z & \omega \end{pmatrix} &= \sum_{m=1}^{\infty} f_m(\tau, z) e(Nm\omega), \\ f_m(\tau, z) &= \sum_{n,r \in \mathbb{Z}, 4Nnm > r^2} a\left(\begin{pmatrix} n & r/2 \\ r/2 & Nm \end{pmatrix}; f\right) q^n \zeta^r. \end{aligned}$$

For fixed τ each f_m is a Jacobi function giving a projective embedding of the elliptic curve $\mathbb{C}/\langle 1, \tau \rangle$. For fixed z, they are modular forms of weight k for certain congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$. These observations motivate the definition of Jacobi forms.

Define the parabolic subgroup Γ_∞ of $\mathrm{Sp}_4(\mathbb{Z})$ as

$$\Gamma_\infty = \mathrm{Sp}_4(\mathbb{Z}) \cap \begin{pmatrix} * & 0 & * & * \\ * & * & * & * \\ * & 0 & * & * \\ 0 & 0 & 0 & * \end{pmatrix}, \; * \in \mathbb{Z}.$$

Definition 2.14. *A level one Jacobi form of weight $k \in \frac{1}{2}\mathbb{Z}$, index $m \in \mathbb{Q}$ and character $\chi : \Gamma_\infty \to \mathbb{C}$, denoted $\phi \in J_{k,m}(\chi)$, is a holomorphic map*

$$\begin{aligned} \phi : \mathcal{H}_1 \times \mathbb{C} &\to \mathbb{C} \\ (\tau, z) &\mapsto \phi(\tau, z) \end{aligned}$$

such that, if $\tilde{\phi} : \mathcal{H}_2 \to \mathbb{C}$ is defined by $\tilde{\phi}(\Omega) = \phi(\tau, z)e(m\omega)$ for $\Omega = \begin{pmatrix} \tau & z \\ z & \omega \end{pmatrix}$, we then have:

1. *For each $\gamma \in \Gamma_\infty$, $\tilde{\phi}|_k\gamma = \chi(\gamma)\tilde{\phi}$, and*
2. *$\phi(\tau, z) = \sum_{n \geq 0,\ r \in \mathbb{Z}} c(n, r)q^n\zeta^r$, where $c(n, r) = 0$ unless $4mn - r^2 \geq 0$.*

If $c(n, r) = 0$ unless $4mn - r^2 > 0$ then $\phi \in J^{cusp}_{k,m}(\chi)$ is a cusp form.

Jacobi forms are the main tool to build Siegel paramodular forms. We will now see how to find them using theta blocks. We will then enunciate Gritsenko's lift to show that any Jacobi form can be the first coefficient of a Siegel paramodular form.

The Jacobi theta function $\vartheta : \mathcal{H} \times \mathbb{C} \to \mathbb{C}$ is defined either as a theta series

$$\vartheta(\tau, z) = \sum_{n=-\infty}^{\infty} \left(\frac{-4}{n}\right) q^{n^2/8}\zeta^{n/2} = \sum_{n=-\infty}^{\infty} (-1)^n q^{\frac{(2n+1)^2}{8}} \zeta^{\frac{2n+1}{2}}$$

or as the triple product

$$\vartheta(\tau, z) = q^{1/8}\zeta^{1/2} \prod_{n=1}^{\infty} (1 - q^n)(1 - q^n\zeta)(1 - q^{n-1}\zeta^{-1}).$$

It is a holomorphic Jacobi form with non-trivial character of weight 1/2 and index 1/2. For positive $a \in \mathbb{Z}$, we denote by ϑ_a the Jacobi form

$$\vartheta_a(\tau, z) := \vartheta(\tau, az),$$

which is of weight 1/2 and index $a^2/2$.

The Dedekind eta function is defined in the upper half-plane by the equation

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

If $\tau \in \mathcal{H}$ then $|q| < 1$, so the product converges absolutely and is nonzero, and moreover $\eta(\tau)$ is analytic on $\mathcal{H}$. We have $\eta(\tau + 1) = e^{\pi i/12}\eta(\tau)$, so $\eta^{24}(\tau)$ is periodic with period 1. Choosing the appropriate branch of $z^{1/2}$, one shows that $\eta(-1/\tau) = (-i\tau)^{1/2}\eta(\tau)$. This function is used to describe several classical modular forms, for instance, the unique normalized eigenform $f \in S_2(\Gamma_0(11))$ can be written as

$$f(\tau) = (\eta(\tau)\eta(11\tau))^2.$$

Gritsenko, Skoruppa and Zagier [GSZ19] note that for positive integers a and b, the quotient

$$Q_{a,b}(\tau, z) = \frac{\vartheta_a(\tau, z)\vartheta_b(\tau, z)\vartheta_{a+b}(\tau, z)}{\eta(\tau)}$$

is a holomorphic Jacobi form of weight 1 and index $a^2 + ab + b^2$. In addition, setting $g = \gcd(a, b)$, $Q_{a,b}$ is a cusp form if $3g^3 \mid ab(a + b)$. To generalize this fact, they introduce the notion of theta blocks.

Definition 2.15. *A theta block of length r is a function of the form*

$$\vartheta_{a_1}\vartheta_{a_2}\cdots\vartheta_{a_r}\eta^n,$$

where n is an integer and each a_j is a nonzero integer. A generalized theta block is a holomorphic function on $\mathcal{H} \times \mathbb{C}$ of the form

$$\frac{\vartheta_{a_1}\vartheta_{a_2}\cdots\vartheta_{a_r}}{\vartheta_{b_1}\vartheta_{b_2}\cdots\vartheta_{b_s}}\eta^n$$

where n is an integer and the a_j, b_j are nonzero integers. A (generalized) theta block is called holomorphic if it is holomorphic at infinity, i.e., if it is a Jacobi form. If we drop the holomorphy requirement, such a function is called a theta function.

Gritsenko, Skoruppa, and Zagier also give a useful criterion to find Jacobi forms of a given weight and index, which is what we need to generate Siegel paramodular forms of our target weight and level.

Theorem 2.16 (Gritsenko, Skoruppa, Zagier)**.** *Let $\ell \in \mathbb{N}$, $t \in \mathbb{Z}$, $\mathbf{n} = (n_1, \ldots, n_\ell) \in \mathbb{Z}^\ell$, $\mathbf{d} = (d_1, \ldots, d_\ell) \in \mathbb{N}^\ell$. Let also $n = \sum_{i=1}^{\ell} n_i$. Define a meromorphic function $\mathrm{TB}[t, \mathbf{n}, \mathbf{d}] : \mathcal{H}_1 \times \mathbb{C} \to \mathbb{C}$ by*

$$\mathrm{TB}[t, \mathbf{n}, \mathbf{d}](\tau, z) = \eta(\tau)^t \prod_{i=1}^{\ell} \vartheta_{d_i}(\tau, z)^{n_i}.$$

The function $\mathrm{TB}[t, \mathbf{n}, \mathbf{d}]$ is a Jacobi cusp form of weight k and index m if and only if

1. *$2k = t + n$,*
2. *$2m = \sum_{i=1}^{\ell} n_i d_i^2$,*

3. $t + 3n \equiv 0 \bmod 24$,

4. *For all* $d \in \mathbb{N}$, $\sum_{i:d|d_i} n_i \geq 0$,

5. *The function* $\frac{k}{12} + \sum_{i=1}^{\ell} n_i \bar{B}_2(d_i x)$ *has a positive minimum on* $[0, 1]$. *Here* $B_2 = \frac{1}{2}x^2 - \frac{1}{2}x + \frac{1}{12}$ *and* $\bar{B}_2(x) = B_2(x - [x])$ *is the periodic extension of its restriction to* $[0, 1]$.

We consider a special case of theta blocks to ensure conditions 1, 3 and 4 are always satisfied. As before, take $\ell \in \mathbb{N}$, $k \in \mathbb{Z}$, $[d_1, \dots, d_\ell] \in \mathbb{Z}^\ell$. We define a theta block of weight k and index $m = \frac{1}{2}\sum_{i=1}^{\ell} d_i^2$ by

$$\mathrm{TB}_k[d_1, \dots, d_\ell](\tau, z) = \eta(\tau)^{2k} \prod_{i=1}^{\ell} \frac{\vartheta_{d_i}(\tau, z)}{\eta(\tau)}.$$

For this to be a Jacobi cusp form it is sufficient that $12 \mid k + \ell$ and that $\frac{k}{12} + \sum_{i=1}^{\ell} \bar{B}_2(d_i x) > 0$.

Formally, the q-expansion of η can be seen inside the Puiseux series ring of any ring R of zero characteristic,

$$R[[q^{1/\infty}]] = \left\{ \sum_{n \geq n_0} a_n q^n \mid a_n \in R, n_0 \in \mathbb{Q} \right\}.$$

Similarly, we can see the q-ζ-expansion of ϑ inside the ring $R[[q^{1/\infty}, \zeta^{1/\infty}]]$. This situation is not ideal for computation, since multiplication in $R[[q^{1/\infty}, \zeta^{1/\infty}]]$ is relatively slow. To improve on this, we rewrite the Jacobi theta function as

$$\vartheta(\tau, z) = q^{1/8}(\zeta^{1/2} - \zeta^{-1/2}) \sum_{n \geq 1} (-1)^{n+1} q^{\binom{n}{2}} \sum_{j=1-n}^{n-1} \zeta^j.$$

Then, we note that the fractionary power of q in $\mathrm{TB}_k[d_1, \dots, d_\ell]$ is $q^{\frac{2k-\ell}{24} + \frac{\ell}{8}} = q^{\frac{2k-\ell+3\ell}{24}} = q^{\frac{2k+2\ell}{24}}$. By the condition $12 \mid k + \ell$, this is actually an integer power. Now we only need to compute the so-called *baby block*

$$\prod_{i=1}^{\ell} (\zeta^{d_i/2} - \zeta^{-d_i/2})$$

in the Puiseux series ring $\mathbb{Z}[[\zeta^{1/\infty}]]$, a finite computation, and the remaining infinite series can be computed in the Laurent series ring $\mathbb{Z}((q, \zeta))$. In order to compute series up to a certain precision, we can work in the polynomial ring $\mathbb{Z}[q, \zeta]$, which has efficient multiplication by the use of 2-dimensional discrete Fourier transforms.

Example 2.17. *The Fourier expansion of the theta block* $\mathrm{TB}_2[2,4,4,4,5,6,8,9,10,14]$ *is*

$$\begin{aligned}\Big(&\frac{1}{z^{33}}+\frac{-1}{z^{31}}+\frac{-3}{z^{29}}+\frac{-1}{z^{28}}+\frac{2}{z^{27}}+\frac{1}{z^{26}}+\frac{3}{z^{25}}+\frac{2}{z^{24}}+\frac{-1}{z^{22}}+\frac{-1}{z^{19}}+\frac{-2}{z^{18}}+\frac{-3}{z^{17}}\\ &+\frac{-3}{z^{16}}+\frac{-2}{z^{15}}+\frac{2}{z^{14}}+\frac{2}{z^{13}}+\frac{2}{z^{12}}+\frac{3}{z^{11}}+\frac{1}{z^{10}}+\frac{1}{z^{9}}+\frac{2}{z^{8}}+\frac{-1}{z^{6}}+\frac{-1}{z^{5}}\\ &+\frac{-1}{z^{4}}+\frac{-2}{z^{3}}+\frac{1}{z}-2+z-2z^3-z^4-z^5-z^6+2z^8+z^9+z^{10}+3z^{11}\\ &+2z^{12}+2z^{13}+2z^{14}-2z^{15}-3z^{16}-3z^{17}-2z^{18}-z^{19}-z^{22}+2z^{24}\\ &+3z^{25}+z^{26}+2z^{27}-z^{28}-3z^{29}-z^{31}+z^{33}\Big)q+O(q^2).\end{aligned}$$

Having constructed Jacobi forms via theta blocks, it remains to lift them to Siegel paramodular forms. This is the purpose of the Gritsenko lift. A single Jacobi form gives us a coefficient in the Fourier-Siegel expansion of a form in $S_k(K(N))$. To get further coefficients, we define the level raising operator $V_m : J_{k,N}^{cusp} \to J_{k,mN}^{cusp}$ (compare the notation with (1.7)) by

$$\phi|V_m = \sum_{n>0, r\in\mathbb{Z}} \left(\sum_{\delta|\gcd(m,n,r)} \delta^{k-1} c\left(\frac{mn}{\delta^2}, \frac{r}{\delta}; \phi\right)\right) q^n \zeta^r.$$

Theorem 2.18 (Gritsenko). *Let* $\phi \in J_{k,N}^{cusp}$ *with Fourier series*

$$\phi(\tau, z) = \sum_{n>0, r\in\mathbb{Z}} c(n,r;\phi) q^n \zeta^r.$$

There is a form $\mathrm{Grit}(\phi) \in S_k(K(N))$ *given by*

$$\mathrm{Grit}(\phi)\begin{pmatrix}\tau & z\\ z & \omega\end{pmatrix} = \sum_{4mnN-r^2>0} (\phi|V_m) e(mN\omega).$$

The proof can be found in [Gri95]. The Fourier coefficients of ϕ and $\mathrm{Grit}(\phi)$ are related by the equality

$$a\left(\begin{pmatrix} n & r/2\\ r/2 & Nm\end{pmatrix}; \mathrm{Grit}(\phi)\right) = c\left(n, r; \phi \mid V_m\right) = \sum_{\delta|\gcd(m,n,r)} \delta^{k-1} c\left(\frac{mn}{\delta^2}, \frac{r}{\delta}; \phi\right).$$

2.3.1 Example: the nonlift in level 277

As we will see in the next chapter, we are interested in paramodular forms of weight 2 which are not Gritsenko lifts, which are also called nonlifts. By working in $S_4(K(N))$ and $S_8(K(N))$, Poor and Yuen [PY15] prove that there are no nonlifts of weight 2 and level $N < 277$, and the first nonlift is found in level $N = 277$.

One of its expression is as follows. One defines ten theta blocks,

$$\begin{array}{ll}
\Xi_1 := \mathrm{TB}_2[2,4,4,4,5,6,8,9,10,14] & \Xi_6 := \mathrm{TB}_2[2,3,3,5,5,7,8,10,10,13] \\
\Xi_2 := \mathrm{TB}_2[2,3,4,5,5,7,7,9,10,14] & \Xi_7 := \mathrm{TB}_2[2,3,3,4,5,6,7,9,10,15] \\
\Xi_3 := \mathrm{TB}_2[2,3,4,4,5,7,8,9,11,13] & \Xi_8 := \mathrm{TB}_2[2,2,4,5,6,7,7,9,11,13] \\
\Xi_4 := \mathrm{TB}_2[2,3,3,5,6,6,8,9,11,13] & \Xi_9 := \mathrm{TB}_2[2,2,4,4,6,7,8,10,11,12] \\
\Xi_5 := \mathrm{TB}_2[2,3,3,5,5,8,8,8,11,13] & \Xi_{10} := \mathrm{TB}_2[2,2,3,5,6,7,9,9,11,12].
\end{array} \tag{2.7}$$

If we let $G_i = \mathrm{Grit}(\Xi_i)$ for $i = 1, \dots, 10$, the nonlift in $S_2(K(277))$ is given by the rational function

$$\begin{aligned}
f_{277} := (&-14G_1^2 - 20G_8G_2 + 11G_9G_2 + 6G_2^2 - 30G_7G_{10} + 15G_9G_{10} \\
&+ 15G_{10}G_1 - 30G_{10}G_2 - 30G_{10}G_3 + 5G_4G_5 + 6G_4G_6 + 17G_4G_7 \\
&- 3G_4G_8 - 5G_4G_9 - 5G_5G_6 + 20G_5G_7 - 5G_5G_8 - 10G_5G_9 - 3G_6^2 \\
&+ 13G_6G_7 + 3G_6G_8 - 10G_6G_9 - 22G_7^2 + G_7G_8 + 15G_7G_9 + 6G_8^2 \\
&- 4G_8G_9 - 2G_9^2 + 20G_1G_2 - 28G_3G_2 + 23G_4G_2 + 7G_6G_2 \\
&- 31G_7G_2 + 15G_5G_2 + 45G_1G_3 - 10G_1G_5 - 2G_1G_4 - 13G_1G_6 \\
&- 7G_1G_8 + 39G_1G_7 - 16G_1G_9 - 34G_3^2 + 8G_3G_4 + 20G_3G_5 \\
&+22G_3G_6 + 10G_3G_8 + 21G_3G_9 - 56G_3G_7 - 3G_4^2) \,/ \\
&(-G_4 + G_6 + 2G_7 + G_8 - G_9 + 2G_3 - 3G_2 - G_1)\,.
\end{aligned} \tag{2.8}$$

Poor and Yuen show the following result.

Theorem 2.19. *The subspace of Gritsenko lifts of $S_2(K(277))$ has dimension 10, whereas $\dim S_2(K(277)) = 11$. The form f_{277} is a Hecke eigenform with rational eigenvalues which is not a Gritsenko lift.*

2.4 Specialization

The expression (2.8) for f_{277} as a rational function of Gritsenko lifts creates an important problem: in order to compute enough coefficients to be able to find the Hecke eigenvalues, one needs to expand each theta block to very large exponents, to a point which is hardly tractable with a reasonable amount of computer resources.

To circumvent this problem, one can specialize the Siegel form to a modular curve, obtaining a classical modular form. The specialization is done with a ring homomorphism, allowing us to specialize each individual Gritsenko lift and reducing the amount of coefficients needed for each q-ζ-series.

Let $s \in \mathrm{GL}_2(\mathbb{R})$ be a symmetric positive definite matrix. The map

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto M^s = \begin{pmatrix} aI_2 & b \cdot s \\ c \cdot s^{-1} & dI_2 \end{pmatrix}$$

defines an injective homomorphism $\mathrm{SL}_2(\mathbb{R}) = \mathrm{Sp}_2(\mathbb{R}) \to \mathrm{Sp}_4(\mathbb{R})$. Moreover, multiplying s by $\tau \in \mathcal{H}_1$, we obtain a map $\phi_s : \mathcal{H}_1 \to \mathcal{H}_2$. This yields the specialization morphism $\phi_s^* : \mathcal{O}(\mathcal{H}_2) \to \mathcal{O}(\mathcal{H}_1)$, defined by $\phi_s^*(f)(\tau) = f(s\tau)$. This is trivially a ring homomorphism.

Lemma 2.20. *Let $f \in \mathcal{O}(\mathcal{H}_2)$ be a holomorphic function, let $M \in \mathrm{SL}_2(\mathbb{R})$, and let s be a symmetric positive definite matrix. Then*

$$\phi_s^*(f)|_{2k}M = \phi_s^*(f|_k M^s).$$

Proof. A short computation shows $j(M^s\langle s\tau\rangle) = j(M\langle\tau\rangle)^2$. Moreover, it is easy to show that $s \cdot M\langle\tau\rangle = M^s\langle s\tau\rangle$. Therefore for all $\tau \in \mathcal{H}_1$ we have

$$\begin{aligned}(\phi_s^*(f)|_{2k}M)(\tau) &= j(M\langle\tau\rangle)^{-2k}\phi_s^*(f)(M\langle\tau\rangle) = j(M\langle\tau\rangle)^{-2k}f(s \cdot M\langle\tau\rangle)\\ &= j(M^s\langle s\tau\rangle))^{-k}f(M^s\langle s\tau\rangle) = \phi_s^*(f|_kM^s)(\tau).\end{aligned}$$

□

Proposition 2.21. *Let $s = \begin{pmatrix} a & b \\ b & c/N \end{pmatrix}$ be a symmetric positive definite matrix with $a, b, c \in \mathbb{Z}$. The map ϕ_s^* defines a ring homomorphism*

$$\phi_s^* : M(K(N)) \to M(\Gamma_0(\det(s)N))$$

from the graded ring $M(K(N)) = \bigoplus_{k=0}^{\infty} M_k(K(N))$ of Siegel paramodular forms of level N, to the graded ring of classical modular forms of level $\det(s)N$. The map multiplies weights by two and maps cusp forms to cusp forms.

Proof. Let $f \in M_k(K(N))$ be a paramodular form of weight k. For $M = \begin{pmatrix} \alpha & \beta \\ \gamma\det(s)N & \delta \end{pmatrix} \in \Gamma_0(\det(s)N)$, we have

$$M^s = \begin{pmatrix} \alpha & 0\cdot N & a\beta & b\beta \\ 0 & \alpha & b\beta & c\beta/N \\ c\gamma & -b\gamma N & \delta & 0 \\ -b\gamma N & a\gamma N & 0 \cdot N & \delta \end{pmatrix},$$

so clearly $M^s \in K(N)$. Hence $\phi_s^*(f)|_{2k}M = \phi_s^*(f|_kM^s) = \phi_s^*(f)$, and $\phi_s^*(f)$ is a modular form for $\Gamma_0(\det(s)N)$ of weight $2k$. If f is a cusp form, then by definition $\Phi(f|_kM^s) = 0$. Now for all $M \in \mathrm{SL}_2(\mathbb{Z})$, $M^s \in \mathrm{Sp}_4(\mathbb{Q})$, and $\Phi(\phi_s^*(f)|_{2k}M) = \Phi(\phi_s^*(f|_kM^s))$ is the constant term of the q-expansion of $f|_kM^s$ which is zero when f is a cusp form. Hence $\phi_s^*(f)$ is also a cusp form. □

The resulting Fourier expansion of the classical modular form $\phi_s^*(f)$ will be

$$(\phi_s^*f)(\tau) = \sum_{n\geq 0}\left(\sum_{T:\ \langle T,s\rangle = n} a(T;f)\right)q^n. \tag{2.9}$$

We can generalise the specialization morphism a bit, by taking a 2-by-2 matrix ζ and setting $(\phi_{s,\zeta}^*f)(\tau) := f(s\tau+\zeta)$. If we let $f(Z) = \sum_{T>0} a(T;f)e(\langle T,Z\rangle) \in$

$S_k(K(N))$ be a cusp form and set $\chi_\zeta(T) = e(\langle \zeta, T\rangle$, we have

$$(\phi^*_{s,\zeta} f)(\tau) = \sum_{n \in \mathbb{Q}_{\geq 0}} \left(\sum_{T\colon \langle T, s\rangle} \chi_\zeta(T) a(T; f) \right) q^n.$$

Note that this lives in a Puiseux series ring. We may use this expression to compute the slash of f with a block upper-triangular matrix $\begin{pmatrix} A & B \\ 0 & D \end{pmatrix} \in \mathrm{GSp}_4^+(\mathbb{Q})$ with similitude $\mu = \det(AD)^{1/2}$,

$$\begin{aligned}
\phi^*_s(f|_k \begin{pmatrix} A & B \\ 0 & D \end{pmatrix})(\tau) &= (f|_k \begin{pmatrix} A & B \\ 0 & D \end{pmatrix})(s\tau) \\
&= \det(AD)^{k-3/2} \det(D)^{-k} f(AsD^{-1}\tau + BD^{-1}) \\
&= \det(A)^k \det(AD)^{-3/2} \sum_{n \in \mathbb{Q}_{\geq 0}} \left(\sum_{T\colon \langle T, AsD^{-1}\rangle = n} \chi_{BD^{-1}}(T) a(T; f) \right) q^n.
\end{aligned}$$

Using $s = \begin{pmatrix} a & b \\ b & c/N \end{pmatrix}$ as in the previous proposition, one can combine this action formula with the double coset decomposition (2.1) to yield the following expression for $f|_k T(p)$:

$$\phi^*_s\left(f|_k T(p)\right)(\tau) = p^{2k-3} f(ps\tau) \tag{2.10}$$

$$+ p^{k-3} \sum_{i \bmod p} f\left(\begin{pmatrix} a/p & b \\ b & pc/N \end{pmatrix} \tau + \begin{pmatrix} i/p & 0 \\ 0 & 0 \end{pmatrix} \right) \tag{2.11}$$

$$+ p^{k-3} \sum_{i \bmod p} \left(\sum_{j \bmod p} f\left(\begin{pmatrix} pa & b + ia \\ b + ia & (c/N + 2ib + i^2 a)/p \end{pmatrix} \tau + \begin{pmatrix} 0 & 0 \\ 0 & j/p \end{pmatrix} \right) \right) \tag{2.12}$$

$$+ p^{-3} \sum_{i,j,k \bmod p} f\left(s\tau/p + \begin{pmatrix} i/p & j/p \\ j/p & k/p \end{pmatrix} \right). \tag{2.13}$$

One can find several cancellations among the terms of these sums [Bru+19, Proposition 6.3.8], which yields a significant improvement in the complexity of computing this specialization.

Two steps remain before we can perform the specialization. The first one is to decide which matrices T will be involved in the computation, which will obviously depend on the number of desired terms of the classical modular form to be computed. The second one is to fix the matrix s, which we will do according to the possible smallest coefficients of a given cusp form.

To solve the first issue we borrow again from [Bru+19]. We define, for a level N, a real symmetric matrix G, a maximum trace $u \in \mathbb{R}$ and minimum determinant $\delta \in \mathbb{R}$, the set

$$\mathcal{S}(N,G,u,\delta) = \left\{ T = \begin{pmatrix} n & r/2 \\ r/2 & Nm \end{pmatrix} \in \mathcal{X}_2(N) \;\middle|\; \langle T, G\rangle \leq u, \det(2T) \geq \delta, \right.$$
$$\left. \text{if } m = 0 \text{ then } n \geq 0, \text{ and if } m = n = 0 \text{ then } r < 0 \right\}.$$

Proposition 2.22. *Let $G = \begin{pmatrix} \alpha & \beta \\ \beta & \gamma \end{pmatrix} \in M_2(\mathbb{R})$ be positive definite with determinant $\Delta = \alpha\gamma - \beta^2 > 0$. Let*

$$X = 4\alpha u m N - \alpha^2 \delta - 4\Delta (mN)^2.$$

Then the matrices $\begin{pmatrix} n & r/2 \\ r/2 & Nm \end{pmatrix} \in \mathcal{S}(N,G,u,\delta)$ satisfy the following bounds.

(a) If $m \geq 1$, then

$$\begin{aligned} 1 \leq m &\leq \frac{\alpha(u + \sqrt{u^2 - \delta\Delta})}{2\Delta N}, \\ \frac{-2\beta m N - \sqrt{X}}{\alpha} \leq r &\leq \frac{-2\beta m N + \sqrt{X}}{\alpha}, \\ \frac{r^2 + \delta}{4mN} \leq n &\leq \frac{u - \beta r - \gamma m N}{\alpha}. \end{aligned}$$

(b) If $m = 0$ and $n > 0$, then

$$r^2 \leq -\delta \text{ and } 1 \leq n \leq \frac{u - \beta r}{\alpha}.$$

(c) If $m = n = 0$, then

$$r^2 \leq -\delta \text{ and } r < 0.$$

The proof is elementary and follows from the inequalities in the definition of $\mathcal{S}(N,G,u,\delta)$. One usually needs to interpret the resulting matrices as explained in Lemma 2.6; given $T \in \mathcal{S}(N,G,u,\delta)$, it is important to keep in mind that we might not know the coefficient $a(T;f)$ directly, but we may have it stored as $a(T[U];f)$ for some $U \in \Gamma^0_{\pm}(N)$.

Now, let $f \in S_k(K(N))$ be a cusp form, and let d be the smallest positive integer such that there is some $T \in \mathcal{X}_2(N)$ with $\det(2T) = d$ and $a(T;f)$ is nonzero, let T_0 be such a matrix. Note that there is a lower bound on the determinant d.

Lemma 2.23. *For prime level N, the lowest possible determinant d is*

$$\det(2T_0) = \begin{cases} 3, & N \equiv 1 \bmod 12, \\ 4, & N \equiv 5 \bmod 12, \\ 3, & N \equiv 7 \bmod 12, \\ 8, & N \equiv 11 \bmod 12. \end{cases}$$

Proof. If $T_0 = \begin{pmatrix} n & r/2 \\ r/2 & Nm \end{pmatrix}$ then $\det(2T_0) = 4Nnm - r^2 = d$ precisely when $-d$ is a square mod $4N$. The result follows from considering the smallest positive d for which this is possible, we show the cases $N \equiv 1, 7 \bmod 12$ (corresponding to $N \equiv 1 \bmod 3$).

We can rule out $d = 1$ and 2, since -1 and -2 are not squares mod 4. The next possibility is $d = 3$, and since $-3 \equiv 1 \bmod 4$ is a square we only need to compute the symbol $\left(\frac{-3}{N}\right)$. Now

$$\left(\frac{-3}{N}\right) = (-1)^{\frac{N-1}{2}} \left(\frac{3}{N}\right) = (-1)(-1)^{\frac{N-1}{2}} \left(\frac{N}{3}\right) = 1,$$

so $d = 3$ is the smallest possible determinant. The other cases are done similarly. □

We can now choose the appropriate matrix s. If we set $s = (2T_0)^*$, the adjoint of $2T_0$, we will have $\langle T_0, s\rangle = \mathrm{Tr}(2T_0(T_0)^*) = 4\det(T_0) = \det(2T_0) = d$. Because d was minimal, we already know the first term of the q-expansion of $\phi_s^*(f)$.

Lemma 2.24. *With the current setting for f, d, T_0 and s,*

$$\phi_s^*(f) = a(T_0; f)q^d + O(q^{d+1}).$$

Proof. Let $T_0 = \begin{pmatrix} n & r/2 \\ r/2 & Nm \end{pmatrix}$ so that

$$s = (2T_0)^* = \begin{pmatrix} 2n_0 & r_0 \\ r_0 & 2Nm_0 \end{pmatrix}^* = \begin{pmatrix} 2Nm_0 & -r_0 \\ -r_0 & 2n_0 \end{pmatrix}.$$

Because d is minimal, we have to compute the matrices in $\mathcal{S}(N, s, d, d)$. By Proposition 2.22, given $\begin{pmatrix} n & r/2 \\ r/2 & Nm \end{pmatrix} \in \mathcal{S}(N, s, d, d)$ we will have

$$1 \le m \le \frac{2Nm_0(d + \sqrt{d^2 - d^2}}{2dN} = m_0.$$

We also need to have $X = 4(2Nm_0)dmN - (2Nm_0)^2 d - 4d(mN)^2 = -4dN^2(m - m_0)^2 \ge 0$, but this can only happen if $m = m_0$ and $X = 0$. The second inequality is

$$\frac{2r_0 mN}{2Nm_0} \le r \le \frac{2r_0 mN}{2Nm_0},$$

so $r = r_0 \frac{m}{m_0} = r_0$. Finally, the third inequality

$$\frac{r^2 + d}{4mN} \le n \le \frac{d - (-r_0)r - 2n_0 mN}{2Nm_0} = n_0$$

yields $n = n_0$. Therefore $\mathcal{S}(N, s, d, d) = \{T_0\}$ and the result follows from (2.9). □

Example 2.25. *Let f be the nonlift of level $N = 277$ described in 2.3.1. The minimal determinant for $277 \equiv 1 \bmod 12$ is $d = 3$, and indeed for*

$$T_0 = \begin{pmatrix} 1 & 233/2 \\ 233/2 & 49 \cdot 277 \end{pmatrix}$$

we have $a(T; f) = -3 \neq 0$. Taking $s = (2T_0)^*$ and using the data in [LMFDB, Siegel modular form Kp.2_PY2_277], we can compute up to 89 coefficients in the q-expansion of $\phi_s^*(f) \in S_2(\Gamma_0(3 \cdot 277))$, which starts by

$$\phi_s^*(f) = -3q^3 + 6q^6 + 6q^9 + 3q^{12} + 3q^{15} - 12q^{18} + O(q^{21}).$$

The first few exponents might suggest that this is an old form coming from $g \in S_2(\Gamma_0(277))$, so that $\phi_s^*(f)(\tau) = g(3\tau)$. However $a_{34}(\phi_s^*(f)) \neq 0$, so this is not the case. Likewise, one sees that $\phi_s^*(f)$ is not an eigenform.

Appendix B contains other examples of q-expansions which we have computed by specialization of some nonlifts available in [LMFDB, Siegel modular forms for $K(p)$].

2.4.1 Implementation

During the realization of this project, we have implemented the method of specialization, which is capable of computing Hecke eigenvalues for the nonlift in level 277 from Example 2.3.1, and should be applicable to other eigenforms. This is, to our knowledge, the first public implementation of the algorithm described in [Bru+19], and the first one to use Sagemath [Sag21] (the original code was written in C++). The code can be found on Github [Flo21].

The implementation of the method poses a few challenges, which we outline here. As this chapter has shown, there are two ways of computing Hecke eigenvalues of a Siegel paramodular form. The first one needs having lots of coefficients of the form explicitly, and uses either the formula in (2.4) or a suitable specialization ϕ_s^*. In both cases, the algorithm described in Lemma 2.6 is needed to compare equivalent symmetric matrices.

With the approach of using the explicit form f_{277} as given in the LMFDB, we are able to compute Hecke eigenvalues $a_p(f_{277})$ for primes p up to 23. To go further, we need to use expression (2.8). We first compute each theta block, and then the corresponding Gritsenko lifts. We can then specialize each Gritsenko lift with the formula in (2.10) and combine all the Puiseux series to obtain the specialized form $\phi_s^*(f_{277})$. Since $f_{277} = Q(G_1, \dots, G_{10})$ is a rational function of Gritsenko lifts and ϕ_s^* is a ring homomorphism, the specialized form is

$$\phi_s^*(f_{277}) = Q(\phi_s^*(G_1), \dots, \phi_s^*(G_{10})).$$

The corresponding series for $f_{277}|_2 T(p)$ is then

$$\phi_s^*(f_{277}|_2 T(p)) = Q(\phi_s^*(G_1|_2 T(p)), \dots, \phi_s^*(G_{10}|_2 T(p))),$$

and we only need to compute the first nonzero coefficient of each classical modular form to divide and obtain the desired eigenvalue. The matrix s is decided with the discussion so far, taking into account that we do know the first nonzero coefficient of f_{277}.

To compute the theta blocks, we can multiply the factors for each of them up to a finite precision in the variable q. By shifting the possibly negative exponent in ζ (and keeping track of the shift each time we multiply), we may treat theta blocks and their factors as polynomials in q and ζ and multiply them via two-dimensional discrete Fourier transforms.

We do that with `numpy`'s Fast Fourier transform package[1]. Unfortunately, the complex-precision of the package limits the scope of our computation, and we are only capable of computing $a_2(f)$, $a_3(f)$ and $a_5(f)$ correctly. To compute from $a_7(f_{277})$ onward, we would need to raise the precision of the floating-point complex numbers, which rapidly multiplies the required execution memory. With sufficient computing resources, the method should be able to compute $a_p(f)$ for primes p up to at least 200, according to Yuen [Yue21].

[1] numpy.fft.fft

Chapter 3

Paramodularity

In Chapter 1 we have reviewed the elements of the Modularity Theorem over $\mathbb{Q}$. We have also seen how the result extends to incorporate modularity for certain kinds of higher dimensional abelian varieties. As we already mentioned, after modularity of GL_2-type varieties we have run out of classical newforms, so we have to turn to Siegel modular forms to try and relate them to some remaining classes of abelian varieties.

The simplest case still to be treated are abelian surfaces A over $\mathbb{Q}$ which have $\mathrm{End}(A) = \mathbb{Z}$ as its ring of endomorphisms defined over $\mathbb{Q}$. We say they have *trivial endomorphisms.*[1]

3.1 The paramodularity conjecture

We recall some relevant facts from the previous two chapters. If ℓ is a prime number and $A_{/\mathbb{Q}}$ is an abelian surface, we associate to it an ℓ-adic representation

$$\rho_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{GL}_4(\mathbb{Q}_\ell).$$

If p is another prime and $\mathrm{Frob}_{\mathfrak{p}}$ is an absolute Frobenius element over p, then the polynomial

$$L_p(A,T) = \det(1 - T\,\mathrm{Frob}_{\mathfrak{p}} \mid \mathrm{T}_\ell(A)^{I_{\mathfrak{p}}})$$

is well-defined, and in fact the action of inertia is trivial if $p \nmid \ell N_A$, where N_A is the conductor of A. We use the collection of all these polynomials to define the L-function of A,

$$L(A,s) := \prod_p L_p(A, p^{-s})^{-1}.$$

Recall that a Siegel paramodular form f of weight 2 and level N is called a non-lift if it lies outside the image of the Gritsenko lift

$$\mathrm{Grit} : J_{2,N}^{cusp} \to S_2(K(N)).$$

[1] N.B. [Bru+19] use the alternative name *typical surface* to refer to an abelian surface with $\mathrm{End}(A_{\bar{\mathbb{Q}}}) = \mathbb{Z}$. For most of the proven cases, these are equivalent because of [Bru+19, Lemma 4.1.1].

The L-function of an eigenform $f \in S_2(K(N))$ with respect to all Hecke operators is also given as a product of spinor Hecke polynomials

$$Q_p(f,T) = \det(1 - T\rho_{f,\ell}(\mathrm{Frob}_\mathfrak{p})|\,\mathrm{T}_\ell(f)^{I_\mathfrak{p}}),$$

with the suitable restriction so that the action of inertia is trivial, where

$$\rho_{f,\ell} : G_\mathbb{Q} \to \mathrm{GL}_4(\mathbb{Q}_\ell)$$

is the 4-dimensional ℓ-adic Galois representation associated to f [Bru+19, Section 4.3]. This takes the form described in (2.6),

$$Q_p(f,T) = 1 - a_p(f)T + b_{p^2}(f)T^2 - pa_p(f)T^3 + p^2T^4,$$

which we conveniently used to set the notation for the local Euler factor of an abelian surface. As explained in Chapter 2, $a_p(f)$ and $b_{p^2}(f)$ correspond to the Hecke eigenvalues of f with respect to the operators $T(p)$ and $B(p^2)$. The L-function of f is then

$$L(f,s) := \prod_p Q_p(f,p^{-s})^{-1},$$

and it can be seen to extend meromorphically to the whole complex plane. By the Čebotarev density theorem (Theorem 1.15), the equality of L-functions is equivalent to the representations $\rho_{A,\ell}$ and $\rho_{f,\ell}$ being equivalent.

A first version of the Paramodularity Conjecture is as follows.

Conjecture 3.1. *Given an abelian surface $A_{/\mathbb{Q}}$ of conductor N with $\mathrm{End}(A) = \mathbb{Z}$, there is a weight-2 nonlift Siegel paramodular newform $f_A \in S_2(K(N))$ with rational eigenvalues such that there is an equality of L-functions*

$$L(A,s) = L(f_A,s).$$

Brumer and Kramer [BK14] originally gave this statement, along with the converse one (each cusp form with rational eigenvalues has a corresponding abelian surface). It was later pointed out that the conjecture was incomplete, and one should not only consider typical abelian surfaces. A 4-dimensional abelian variety (also called an abelian fourfold) is said to have quaternion multiplication, or QM, if its ring of endomorphisms is an order in a quaternion algebra over $\mathbb{Q}$. Calegari [Cal18] explained the Paramodular Conjecture should also include them, proposing the following form of the statement.

Conjecture 3.2 (Brumer–Kramer–Calegari)**.** *Let $\mathcal{A}_N$ be the set of isogeny classes of abelian surfaces $A_{/\mathbb{Q}}$ of conductor N with $\mathrm{End}(A) = \mathbb{Z}$, let $\mathcal{B}_N$ be the set of isogeny classes of QM abelian fourfolds $B_{/\mathbb{Q}}$ of conductor N^2, and let $\mathcal{P}_N$ be the set of weight-2 nonlift Siegel paramodular newforms of level N with rational eigenvalues, up to nonzero scaling. There is a bijection $\mathcal{P}_N \leftrightarrow \mathcal{A}_N \cup \mathcal{B}_N$ such that*

$$L(X,s) = \begin{cases} L(f,s), & \text{if } X \in \mathcal{A}_N, \\ L(f,s)^2, & \text{if } X \in \mathcal{B}_N. \end{cases}$$

```
sage: R.<x> = QQ[]
sage: C = HyperellipticCurve(-x^2-x,x^3+x^2+x+1)
sage: C.change_ring(GF(2)).frobenius_polynomial()
x^4 + 2*x^3 + 4*x^2 + 4*x + 4
sage: C.change_ring(GF(3)).frobenius_polynomial()
x^4 + x^3 + x^2 + 3*x + 9
sage: C.change_ring(GF(5)).frobenius_polynomial()
x^4 + x^3 - 2*x^2 + 5*x + 25
sage: C.change_ring(GF(7)).frobenius_polynomial()
x^4 - x^3 + 3*x^2 - 7*x + 49
```

Figure 3.1: Example of computing local zeta functions for the hyperelliptic curve $C : y^2 + (x^3 + x^2 + x + 1)y = -x^2 - x$. Note that the characteristic polynomial given is $\det(X - \mathrm{Frob}_p)$, which corresponds to $X^4 L_p(A, 1/X)$ in our notation.

We should mention that such abelian fourfolds have yet to be found, and to that effect extensive computational searches have been performed with little success so far.

3.2 Known cases

The first step before conjecturing paramodularity was to gather evidence on both sides. Perhaps surprisingly, the first pieces of such evidence were results of nonexistence. On the one hand, Brumer and Kramer [BK14] showed which odd conductors $N < 500$ were not possible for a typical abelian surface. On the other hand, Poor and Yuen [PY15] proved the following result, compatible with the results of Brumer and Kramer.

Theorem 3.3. *For primes $p < 600$ not in the set $\{277, 349, 353, 389, 461, 523, 587\}$, $S_2(K(p))$ is spanned by Gritsenko lifts.*

After ruling out surface conductors and paramodular levels spanned completely by Gritsenko lifts, the next step is to produce candidate surfaces and nonlifts. For small levels, [LMFDB] contains tables of isogeny classes of abelian surfaces over $\mathbb{Q}$ which are the Jacobian of a genus-2 hyperelliptic curve. We hinted a way to find nonlifts in Section 2.3.1, and there is a large body of literature on trying to find them, see for example [PY07], [PY15], [PSY17].

The first few cases of Conjecture 3.1 were proven using a generalized Faltings-Serre method [Bru+19]. To put it briefly, the method works by comparing a finite number of traces of Frobenius elements through the representations of the surface $A_{/\mathbb{Q}}$ and the eigenform f.

If we have a surface $A_{/\mathbb{Q}}$ given as the Jacobian of a hyperelliptic curve, $A = \mathrm{Jac}(C)$, by the discussion of Section 1.1.3 it is enough to compute the local zeta function of C at the desired primes. This is implemented in widespread computer algebra packages; in Sagemath, it can be done via the commands in Figure 3.1.

Theorem 3.4. *Let C be the curve over $\mathbb{Q}$ defined by*

$$C : y^2 + (x^3 + x^2 + x + 1)y = -x^2 - x.$$

Let A be the Jacobian of C, which has $\operatorname{End}(A) = \mathbb{Z}$ and conductor 277. Let $f_{277} \in S_2(K(277))$ be the nonlift Siegel paramodular cusp form of weight 2 and level 277, unique up to scalar multiple. For all primes p, we have

$$L_p(A, s) = Q_p(f_{277}, s).$$

In particular $L(A, s) = L(f_{277}, s)$ and A is paramodular.

Proof. See [Bru+19, Section 7.1]. The final step in the proof is to compare the *traces of Frobenius* $a_p(A)$ and $a_p(f_{277})$ from the Euler factors and the spinor Hecke polynomials, respectively, for all primes $p \leq 43$. For the surface A, this can be done by counting points of the curve C: if $\tilde{C}_{/\mathbb{F}_p}$ is the reduction of C modulo p, it can be shown that

$$a_p(A) = p + 1 - \#\tilde{C}(\mathbb{F}_p).$$

The values $a_p(f_{277})$ correspond to the Hecke eigenvalues of f_{277} for $T(p)$, and they are computed as explained in Section 2.4. □

The paper [Bru+19] also establishes the paramodularity of two surfaces of conductors 353 and 587. Cris Poor and David S. Yuen [PY] keep a running list of paramodular candidates for levels up to 1000, as well as the cases that have already been proven.

3.3 Paramodularity of GL_4-type abelian varieties

We define a notion of abelian variety that generalizes the situation of surfaces $A_{/\mathbb{Q}}$ with $\operatorname{End}(A) = \mathbb{Z}$.

Definition 3.5. *We say an abelian variety $A_{/\mathbb{Q}}$ is of GL_4-type if $\operatorname{End}^0(A)$ contains a number field of degree $\frac{\dim A}{2}$.*

The terminology is motivated by the following proposition, which is proven in exactly the same way as Proposition 1.35.

Proposition 3.6. *If K is a number field of degree $\frac{\dim A}{2}$ contained in $\operatorname{End}^0(A)$, then the Tate modules $\mathrm{V}_\ell(A)$ associated with A are free of rank four over $K \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$. Accordingly, the action of $G_{\mathbb{Q}}$ on $\mathrm{V}_\ell(A)$ defines a representation with values in $\mathrm{GL}_4(K \otimes \mathbb{Q}_\ell)$, and every prime λ of $\mathcal{O}_K$ lying over ℓ gives a representation*

$$\rho_\lambda : G_{\mathbb{Q}} \to \mathrm{GL}_4(K_\lambda).$$

□

We would like to generalize Conjecture 3.1 to GL_4-type abelian varieties, hoping for an analogue of Ribet's Theorem 1.41, as was already proposed in [BK14, Conjecture 1.4]. We consider abelian varieties $A_{/\mathbb{Q}}$ with real multiplication, that is, such that their endomorphism ring contains an order $\mathcal{O}$ in a totally real number field K. In that case, we say A has RM by $\mathcal{O}$ (or sometimes, by K).

Given a Siegel paramodular eigenform $f \in S_2(K(N))$, we let $K_f = \mathbb{Q}(\{a_p\})$ be the number field generated by the Hecke eigenvalues of f. Compare this definition with that of K_g for a classical modular eigenform g: in that case, the Fourier coefficients and Hecke eigenvalues coincide whenever the form is normalized; on the other hand, the field generated by Fourier-Siegel coefficients of f (as long as they are algebraic) certainly contains the Hecke eigenvalues, and this definition avoids having to normalize the Fourier-Siegel expansion.

Conjecture 3.1 then generalizes naturally to say that there should be an abelian variety of GL_4-type with RM by $\mathcal{O}_{K_f}$ with

$$L(A_f, s) = \prod_{\sigma : K_f \hookrightarrow \mathbb{R}} L(f^\sigma, s).$$

Conversely, an abelian variety A of GL_4-type with RM by $\mathcal{O}_{K_f}$ should be isogenous to A_f for some weight-2 nonlift newform f for $K(N)$.

However, this generalization cannot be the proper one, since in the case $K_f = \mathbb{Q}$, the current statement of the paramodularity conjecture says we have to consider QM abelian fourfolds. Being speculative, one possibility could be to consider varieties of dimension $4[K_f : \mathbb{Q}]$ such that their endomorphism algebra is a quaternion algebra over K_f.

To consider the case where $\mathrm{End}^0(A)$ contains a CM field[2] of degree $\frac{\dim A}{2}$, and by mirroring [Rib04], one should also take into account Siegel paramodular forms with nontrivial character, see for example [JR17].

We need to stress the fact that we do not have an "Eichler-Shimura construction" to build an abelian variety from a form $f \in S_2(K(N))$. In the case of classical modular forms, a form $g \in S_2(\Gamma_0(N))$ corresponded to a differential on the modular curve $X_0(N)$, from which we had a way to build a quotient of the Jacobian $J_0(N)$. This situation is, unfortunately, unavailable to us.

[2] A CM field is an imaginary quadratic extension of a totally real field.

Bibliography

[AL70] A. O. L. Atkin and J. Lehner. "Hecke operators on $\Gamma_0(m)$". In: *Mathematische Annalen* 185.2 (June 1, 1970), pp. 134–160. ISSN: 1432-1807. DOI: `10.1007/BF01359701`.

[BK14] Armand Brumer and Kenneth Kramer. "Paramodular abelian varieties of odd conductor". In: *Transactions of the American Mathematical Society* 366.5 (May 2014), pp. 2463–2516. ISSN: 0002-9947, 1088-6850. DOI: `10.1090/S0002-9947-2013-05909-0`.

[Bru+19] Armand Brumer et al. "On the paramodularity of typical abelian surfaces (and reduction of G-covariant bilinear forms)". In: *Algebra & Number Theory* 13.5 (July 12, 2019), pp. 1145–1195. ISSN: 1944-7833, 1937-0652. DOI: `10.2140/ant.2019.13.1145`. arXiv: `1805.10873`.

[Cal18] Frank Calegari. *The paramodular conjecture is false for trivial reasons*. Jan. 15, 2018. URL: `https://www.galoisrepresentations.com/2018/01/15/the-paramodular-conjecture-is-false-for-trivial-reasons/` (visited on 06/25/2021).

[Cox89] David A. Cox. *Primes of the form x2 + ny2: Fermat, class field theory, and complex multiplication*. New York: Wiley, 1989. 351 pp.

[Dar04] Henri Darmon. *Rational points on modular elliptic curves*. Providence (R.I.): Published for the Conference Board of the Mathematical Sciences by the American Mathematical Society with support from the National Science Foundation, 2004. 129 pp. ISBN: 978-0-8218-2868-7.

[Die07] Luis Victor Dieulefait. "The level 1 weight 2 case of Serre's conjecture". In: *Revista Matemática Iberoamericana* 23.3 (Dec. 31, 2007), pp. 1115–1124. ISSN: 0213-2230. DOI: `10.4171/rmi/525`.

[DS05] Fred Diamond and Jerry Shurman. *A First course in modular forms*. Waltham, MA [etc.]: Springer, 2005. 436 pp.

[Flo21] Enric Florit. *Siegel paramodular forms: f277 and specialization*. June 25, 2021. URL: `https://github.com/3nr1c/siegel-paramodular-forms`.

[Fre83] E. Freitag. *Siegelsche Modulfunktionen.* Berlin [etc.]: Springer, 1983. 341 pp.

[Gri95] Valeri Gritsenko. “Arithmetical lifting and its applications”. In: *Number Theory: Paris 1992–3.* Ed. by Sinnou David. London Mathematical Society Lecture Note Series. Cambridge: Cambridge University Press, 1995, pp. 103–126. DOI: 10.1017/CBO9780511661990.008.

[GSZ19] Valery Gritsenko, Nils-Peter Skoruppa, and Don Zagier. “Theta Blocks”. In: *arXiv:1907.00188 [math]* (June 2019). arXiv: 1907.00188. (Visited on 05/27/2021).

[HS00] Marc Hindry and Joseph H. Silverman. *Diophantine Geometry: An Introduction.* Graduate Texts in Mathematics. New York: Springer-Verlag, 2000. DOI: 10.1007/978-1-4612-1210-2.

[JR17] Jennifer Johnson-Leung and Brooks Roberts. “Twisting of Siegel paramodular forms”. In: *International Journal of Number Theory* 13.7 (Aug. 1, 2017), pp. 1755–1854. ISSN: 1793-0421. DOI: 10.1142/S1793042117501019.

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger. “Serre’s modularity conjecture (I)”. In: *Inventiones mathematicae* 178.3 (July 4, 2009), p. 485. ISSN: 1432-1297. DOI: 10.1007/s00222-009-0205-7.

[KW09b] Chandrashekhar Khare and Jean-Pierre Wintenberger. “Serre’s modularity conjecture (II)”. In: *Inventiones mathematicae* 178.3 (July 4, 2009), p. 505. ISSN: 1432-1297. DOI: 10.1007/s00222-009-0206-6.

[LMFDB] The LMFDB Collaboration. *The L-functions and Modular Forms Database.* http://beta.lmfdb.org. [Online; accessed 30 May 2021]. 2021.

[Poo19] Cris Poor. “Paramodularity”. In: Analytic and Arithmetic Theory of Automorphic Forms (Jan. 2019), pp. 187–201. ISSN: 1880-2818.

[PSY17] Cris Poor, Jerry Shurman, and David S. Yuen. “Siegel paramodular forms of weight 2 and squarefree level”. In: *International Journal of Number Theory* 13.10 (May 2017), pp. 2627–2652. ISSN: 1793-0421. DOI: 10.1142/S1793042117501469.

[PY] Cris Poor and David S. Yuen. *Degree 2 Siegel Paramodular Forms of Weight 2 and Levels up to 1000.* URL: http://www.siegelmodularforms.org/pages/degree2/paramodular-wt2-all/index.html (visited on 06/25/2021).

[PY07] Cris Poor and David S. Yuen. “Computations of spaces of Siegel modular cusp forms”. In: *Journal of the Mathematical Society of Japan* 59.1 (Jan. 2007), pp. 185–222. ISSN: 0025-5645, 1881-1167. DOI: 10.2969/jmsj/1180135507.

[PY15] Cris Poor and David Yuen. “Paramodular cusp forms”. In: *Mathematics of Computation* 84.293 (May 2015), pp. 1401–1438. ISSN: 0025-5718, 1088-6842. DOI: 10.1090/S0025-5718-2014-02870-6.

[Rib04] Kenneth A. Ribet. “Abelian Varieties over Q and Modular Forms”. In: *Modular Curves and Abelian Varieties*. Ed. by John E. Cremona et al. Progress in Mathematics. Basel: Birkhäuser, 2004, pp. 241–261. ISBN: 9783034879194. DOI: `10.1007/978-3-0348-7919-4_15`.

[RS06] Brooks Roberts and Ralf Schmidt. “On modular forms for the paramodular groups”. In: *Automorphic Forms and Zeta Functions*. WORLD SCIENTIFIC, Jan. 1, 2006, pp. 334–364. ISBN: 9789812566324. DOI: `10.1142/9789812774415_0015`.

[RS07] Brooks Roberts and Ralf Schmidt. *Local Newforms for GSp(4)*. Lecture Notes in Mathematics. Berlin Heidelberg: Springer-Verlag, 2007. ISBN: 9783540733232. DOI: `10.1007/978-3-540-73324-9`.

[Sag21] The Sage Developers. *SageMath, the Sage Mathematics Software System (Version 9.2)*. `https://www.sagemath.org`. 2021.

[Sch18] Ralf Schmidt. “Packet structure and paramodular forms”. In: *Transactions of the American Mathematical Society* 370.5 (May 2018), pp. 3085–3112. ISSN: 0002-9947, 1088-6850. DOI: `10.1090/tran/7028`.

[Sil09] Joseph H. Silverman. *The Arithmetic of elliptic curves*. 2nd ed. New York: Springer-Verlag, 2009. 513 pp.

[Yue21] David S. Yuen. *Personal communication*. 2021.

Appendix A

Legendre reduction

Algorithm 1: Legendre reduction.

```
Input: $T = \begin{pmatrix} n & r/2 \\ r/2 & m \end{pmatrix} \in \mathcal{X}_2(1)$
Output: $\tilde{T} \in \mathcal{X}_2(1)$, $U \in \mathrm{GL}_2(\mathbb{Z})$, $v \in \mathbb{P}(\mathbb{Z}/N\mathbb{Z})$ such that $\tilde{T}$ is
        Legendre reduced ($0 \leq r \leq n \leq m$), $T[U] = \tilde{T}$, and
        $Uv = (0,1)^t$.
Let $U \leftarrow \mathrm{Id}$, $v \leftarrow (0,1)^t$.
repeat
    if $m < n$ then
        Let $R = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$
        $v \leftarrow R^{-1}v$
        $U \leftarrow U \cdot R$
        $T \leftarrow T[R]$
    end
    if $n$ ¡ —$r$— then
        Let $\lambda = \left\lceil \frac{-r/2}{n} + \frac{1}{2} \right\rceil$, $R = \begin{pmatrix} 1 & \lambda \\ 0 & 1 \end{pmatrix}$
        $v \leftarrow R^{-1}v$
        $U \leftarrow U \cdot R$
        $T \leftarrow T[R]$
    end
until $|r| \leq n \leq m$;
if $r < 0$ then
    Let $R = \mathrm{diag}(1, -1)$
    $v \leftarrow R^{-1}v$
    $U \leftarrow U \cdot R$
    $T \leftarrow T[R]$
end
return $T$, $U$ and $v$.
```

Appendix B

Examples of specialization

- $N = 277$, $T_0 = \begin{pmatrix} 1 & 233/2 \\ 233/2 & 13573 \end{pmatrix}$, $a(T_0; f_{277}) = -3$.

  $\phi_s^*(f_{277}) = -3q^3+6q^6+6q^9+3q^{12}+3q^{15}-12q^{18}+3q^{21}-18q^{24}-3q^{27}-6q^{30}+6q^{33}+O(q^{34})$.

- $N = 349$, $T_0 = \begin{pmatrix} 1 & 245/2 \\ 245/2 & 15007 \end{pmatrix}$, $a(T_0; f_{349}) = 3$.

  $\phi_s^*(f_{349}) = 3q^3-6q^6-6q^9+3q^{12}-3q^{15}+12q^{18}-12q^{21}-6q^{24}+9q^{27}+6q^{30}+3q^{33}-6q^{36}+O(q^{38})$.

- $N = 353$, $T_0 = \begin{pmatrix} 1 & 42 \\ 42 & 1765 \end{pmatrix}$, $a(T_0; f_{353}) = 2$.

  $\phi_s^*(f_{353}) = 2q^4 - 4q^8 - 4q^{12} - 2q^{16} - 2q^{20} + 8q^{24} + 10q^{32} - 2q^{36} + O(q^{38})$.

- $N = 389$, $T_0 = \begin{pmatrix} 1 & 115 \\ 115 & 13226 \end{pmatrix}$, $a(T_0; f_{389}) = -2$.

  $\phi_s^*(f_{389}) = -2q^4 + 4q^8 + 4q^{12} + 2q^{20} - 8q^{24} + 6q^{28} - 4q^{32} - 2q^{36} + O(q^{40})$.

- $N = 461$, $T_0 = \begin{pmatrix} 1 & 48 \\ 48 & 2305 \end{pmatrix}$, $a(T_0; f_{461}) = 2$.

  $\phi_s^*(f_{461}) = 2q^4-2q^8-6q^{12}-4q^{16}-2q^{20}+6q^{24}+4q^{32}+4q^{36}+2q^{40}+O(q^{44})$.

- $N = 523$, $T_0 = \begin{pmatrix} 1 & 121/2 \\ 121/2 & 3661 \end{pmatrix}$, $a(T_0; f_{523}) = -3$.

  $\phi_s^*(f_{523}) = -3q^3+3q^6+3q^9+6q^{12}+12q^{15}-3q^{18}-6q^{24}-12q^{30}-6q^{33}-6q^{36}+3q^{39}+O(q^{42})$.

- $N = 587^+$, $T_0 = \begin{pmatrix} 2 & 380 \\ 380 & 72201 \end{pmatrix}$, $a(T_0; f_{587^+}) = 2$.

$$\phi_s^*(f_{587^+}) = 2q^8 - 4q^{16} - 4q^{24} - 2q^{32} + 8q^{48} + O(q^{50}).$$

- $N = 587^-$, $T_0 = \begin{pmatrix} 4 & 137/2 \\ 137/2 & 1174 \end{pmatrix}$, $a(T_0; f_{587^-}) = 1$.

$$\phi_s^*(f_{587^-}) = q^{15} - q^{30} - 3q^{45} - q^{60} + O(q^{71}).$$