Explicit approaches to modular abelian varieties

by

William Arthur Stein

B.S. (Northern Arizona University) 1994

A dissertation submitted in partial satisfaction of the
requirements for the degree of
Doctor of Philosophy

in

Mathematics

in the

Graduate Division
of the
University of California at Berkeley

Committee in charge:

Professor Hendrik Lenstra, Chair
Professor Bjorn Poonen
Professor Bin Yu

Spring 2000

The dissertation of William Arthur Stein is approved:

Chair Date

Date

Date

University of California at Berkeley

Spring 2000

Explicit approaches to modular abelian varieties

Abstract

Explicit approaches to modular abelian varieties

by

William Arthur Stein

Doctor of Philosophy in Mathematics

University of California at Berkeley

Professor Hendrik Lenstra, Chair

I investigate the Birch and Swinnerton-Dyer conjecture, which ties together the constellation of invariants attached to an abelian variety. I attempt to verify this conjecture for certain specific modular abelian varieties of dimension greater than one. The key idea is to use Barry Mazur's notion of visibility, coupled with explicit computations, to produce lower bounds on the Shafarevich-Tate group. I have not finished the proof of the conjecture in these examples; this would require computing explicit upper bounds on the order of this group.

I next describe how to compute in spaces of modular forms of weight at least two. I give an integrated package for computing, in many cases, the following invariants of a modular abelian variety: the modular degree, the rational part of the special value of the L-function, the order of the component group at primes of multiplicative reduction, the period lattice, upper and lower bounds on the torsion subgroup, and the real volume. Taken together, these algorithms are frequently sufficient to compute the odd part of the conjectural order of the Shafarevich-Tate group of an analytic rank 0 optimal quotient of $J_0(N)$, with N square-free. I have not determined the exact structure of the component group, the order of the component group at primes whose square divides the level, or the exact order of the torsion subgroup in all cases. However, I do provide generalizations of some of the above algorithms to higher weight forms with nontrivial character.

Professor Hendrik Lenstra
Dissertation Committee Chair

To my parents and my grandmother, Annette Maurer.

Contents

List of Figures

List of Tables

List of Symbols

Symbol	**Definition**	**Page**
$A^\vee$	dual to A	33
$\boldsymbol{\mathcal{B}}_k(N,\varepsilon)$	module of boundary modular symbols	21
c_A	Manin constant of A	57
m_A	modular degree	50
$\mathbf{e}_i$	ith winding element $X^{i-1}Y^{k-2-(i-1)}\{0,\infty\}$	52
$\boldsymbol{\mathcal{M}}_k(N,\varepsilon)$	module of modular symbols	20
$\overline{\boldsymbol{\mathcal{M}}}_k(N,\varepsilon)$	module of extended modular symbols	59
$M[I]$	$\cap_{a\in I}\ker(a)$	
$P(X,Y)\{\alpha,\beta\}$	higher weight modular symbol	20
$[P(X,Y),(u,v)]$	higher weight Manin symbol	27
$\boldsymbol{\mathcal{S}}_k(N,\varepsilon)$	module of cuspidal modular symbols	21
T_n	nth Hecke operator	29
V_k	module of homogeneous polynomials of degree k	20
W_d	dth Atkin-Lehner involution	23
α_t, β_t	degeneracy maps	24
Θ_f	rational period mapping	47
σ, τ	$\sigma=\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$, $\tau=\left(\begin{smallmatrix}0&-1\\1&-1\end{smallmatrix}\right)$	27
Φ_f	analytic period mapping	59
$\Phi_{A,p}$	component group of A at p	71
Ω_A	real volume	66
$\langle\ ,\ \rangle$	integration pairing	22
$*$	star involution	23

Acknowledgements

It is a pleasure to thank my thesis adviser, Hendrik Lenstra, for patiently guiding my intellectual development in innumerable ways. In addition, Robert Coleman, Barry Mazur, and Ken Ribet generously shared their countless ideas and unbounded enthusiasm with me. Robert helped me to understand p-adics, Barry taught me to visualize Shafarevich-Tate groups, and Ken explained congruences, component groups, and tutored me in the elusive art of mathematical exposition.

This thesis would not have been possible without the questions that arose out of exhilarating collaborations with Amod Agashe, Kevin Buzzard, Loïc Merel, David Moulton, Ed Schaefer, Helena Verrill, and Joe Wetherell. I would like to thank Ahmed Abbes, Matt Baker, Brian Conrad, János Csirik, Jordan Ellenberg, Edray Goins, David Jones, Ezra Miller, Bjorn Poonen, and Mak Trifkovic for asking and answering many stimulating questions.

I wish to thank Hendrik Lenstra and Ken Ribet for providing me with financial support during part of the writing of this thesis, Sarah M. Hallam for providing further support, the `Cal@SiliconValley` university fellowship for supporting me throughout my final year, and the Magma group for their computational support.

Finally, I would like to thank Bjorn Poonen for thoroughly reading this thesis and pointing out many ways in which it could be improved.

Preface

The object of numerical computation is theoretical advance.
–A. O. L. Atkin, see [5]

The definition of the spaces of modular forms as functions on the upper half plane satisfying a certain equation is very abstract. The definition of the Hecke operators even more so. Nevertheless, one wishes to carry out explicit investigations into these objects.

We are fortunate that we now have methods available that allow us to transform the vector space of cusp forms of given weight and level into a concrete object, which can be explicitly computed. We have the work of Atkin-Lehner, Birch, Swinnerton-Dyer, Manin, Merel, and many others to thank for this (see [6, 16, 45]). For example, the Eichler-Selberg trace formula, as extended in [30], can be used to compute characteristic polynomials of Hecke operators. One can compute Hecke operators using Brandt matrices and quaternion algebras [32, 52]; another closely related method involves the module of enhanced supersingular elliptic curves [47]. In the course of computing large tables of invariants of elliptic curves in [16], Cremona demonstrated the power of systematic computation using modular symbols.

Various methods often must be used in concert to obtain information about the package of invariants attached to a modular form. For example, computing orders of component groups of optimal quotients of $J_0(N)$ involves computations on the module of supersingular elliptic curves combined with modular symbols techniques (see Chapter 4).

Chapter 1 is an attempt to systematically prove the Birch and Swinnerton-Dyer conjecture for a certain finite list of rank-0 quotients of $J_0(N)$ that have nontrivial Shafarevich-Tate groups. The key idea is to use Barry Mazur's notion of visibility, coupled with explicit computations, to produce lower bounds on the Shafarevich-Tate group. I have not finished the proof of the conjecture in these examples; this would require computing explicit upper bounds on the order of this group. However, I obtain explicit formulas and data that will be helpful in further investigations.

The following three chapters describe the algorithms used in Chapter 1, along with generalizations to eigenforms on $\Gamma_1(N)$ of integral weight greater than two. I have used these algorithms to investigate the Artin Conjecture [12], Serre's conjecture, and many other problems not described in this thesis. I have implemented most of the algorithms that are described in Chapters 2–4 in both MAGMA and C++; this implementation should be available in the standard release of MAGMA in versions 2.7 and greater.

William A. Stein
University of California, Berkeley

Chapter 1

The Birch and Swinnerton-Dyer conjecture

Now that the Shimura-Taniyama conjecture has been proved, many experts consider the Birch and Swinnerton-Dyer conjecture (BSD conjecture) to be one of the main outstanding problems in the field (see [19, pg. 549] and [68, Intro.]). This conjecture ties together many of the arithmetic and analytic invariants of an elliptic curve. At present, there is no general class of elliptic curves for which the full BSD conjecture is known, though a slightly weakened form is known for a fairly broad class of complex multiplication elliptic curves of analytic rank 0 (see [55]), and several deep partial results have been obtained during the last twenty years (see, e.g., [27] and [33]).

Approaches to the BSD conjecture that rely on congruences between modular forms are likely to require a deeper understanding of the analogue of the BSD conjecture for higher-dimensional abelian varieties. As a first step, this chapter presents theorems and explicit computations of some of the arithmetic invariants of modular abelian varieties.

The reader is urged to also read A. Agashe's 2000 Berkeley Ph.D. thesis which cover similar themes. The paper of Cremona and Mazur's [18] paints a detailed experimental picture of the way in which congruences link Mordell-Weil and Shafarevich-Tate groups of elliptic curves.

1.1 The BSD conjecture

By [10] we now know that every elliptic curve over $\mathbf{Q}$ is a quotient of the curve $X_0(N)$, whose complex points are the isomorphism classes of pairs consisting of a (generalized) elliptic curve and a cyclic subgroup of order N. Let $J_0(N)$ denote the Jacobian of $X_0(N)$; this is an abelian variety of dimension equal to the genus of $X_0(N)$ whose points correspond to the degree 0 divisor classes on $X_0(N)$. The survey article [21] is a good guide to the facts and literature about the family of abelian varieties $J_0(N)$.

Following Mazur [41], we make the following definition.

Definition 1.1 (Optimal quotient). An *optimal quotient* of $J_0(N)$ is a quotient A of $J_0(N)$ by an abelian subvariety.

Consider an optimal quotient A such that $L(A,1) \neq 0$. By [35], $A(\mathbf{Q})$ and $Ш(A)$ are both finite. The BSD conjectureasserts that

$$\frac{L(A,1)}{\Omega_A} = \frac{\#Ш(A) \cdot \prod_{p|N} c_p}{\#A(\mathbf{Q}) \cdot \#A^\vee(\mathbf{Q})}.$$

Here the Shafarevich-Tate group

$$Ш(A) := \ker\left(H^1(\mathbf{Q}, A) \to \prod_v H^1(\mathbf{Q}_v, A)\right)$$

is a measure of the failure of the local-to-global principle; the Tamagawa numbers c_p are the orders of the groups of rational points of the component groups of A (see Chapter 4); the real number Ω_A is the measure of $A(\mathbf{R})$ with respect to a basis of differentials having everywhere nonzero good reduction (see Section 3.12.6); and $A^\vee$ is the abelian variety dual to A (see [50, §9]). This chapter makes a small contribution to the long-term goal of verifying the above conjecture for many specific abelian varieties on a case-by-case basis. In a large list of examples, we compute the conjectured order of $Ш(A)$, up to a power of 2, and then show that $Ш(A)$ is at least as big as conjectured. We also discuss methods to obtain upper bounds on $\#Ш(A)$, but do not carry out any computations in this direction. This is the first step in a program to verify the above conjecture for an infinite family of quotients of $J_0(N)$.

1.1.1 The ratio $L(A,1)/\Omega_A$

Extending classical work on elliptic curves, A. Agashe and the author proved the following theorem.

Theorem 1.2. *Let m be the largest square dividing N. The ratio $L(A,1)/\Omega_A$ is a rational number that can be explicitly computed, up to a unit (conjecturally 1) in $\mathbf{Z}[1/(2m)]$.*

Proof. The proof uses modular symbols combined with an extension of the argument used by Mazur in [41] to bound the Manin constant. The modular symbols part of the proof for L-functions attached to newforms of weight $k \geq 2$ is given in Section 3.10; it involves expressing the ratio $L(A,1)/\Omega_A$ as the lattice index of two modules over the Hecke algebra. The bound on the Manin constant is given in Section 3.11. □

The author has computed $L(A,1)/\Omega_A$ for all simple optimal quotients of level $N \leq 1500$; this table can be obtained from the author's web page.

Remark 1.3. The method of proof should also give similar results for special values of twists of $L(A,s)$, just as it does in the case $\dim A = 1$ (see [16, Prop. 2.11.2]).

1.1.2 Torsion subgroup

We can compute upper and lower bounds on $\#A(\mathbf{Q})_{\mathrm{tor}}$, see Section 3.8; these frequently determine $\#A(\mathbf{Q})_{\mathrm{tor}}$.

These methods, combined with the method used to obtain Theorem 1.2, yield the following corollary, which supports the expected cancellation between torsion and c_p coming from the reduction map sending rational points to their image in the component group of A. The corollary also generalizes to higher weight forms, thus suggesting a geometric way to think about reducibility of modular Galois representations.

Corollary 1.4. *Let n be the order of the image of $(0)-(\infty)$ in $A(\mathbf{Q})$, and let m be the largest square dividing N. Then $n \cdot L(A,1)/\Omega_A \in \mathbf{Z}[1/(2m)]$.*

For the proof, see Corollary 3.48 in Chapter 3.

1.1.3 Tamagawa numbers

We prove the following theorem in Chapter 4.

Theorem 1.5. *When $p^2 \nmid N$, the number c_p can be explicitly computed (up to a power of 2).*

We can compute the order c_p of the group of rational points of the component group, but not its structure as a group. When $p^2 \mid N$ it may be possible to compute c_p using the Drinfeld-Katz-Mazur model of $X_0(N)$, but we have not yet done this. There are also good bounds on the primes that can divide c_p when $p^2 \mid N$.

Systematic computations (see Section 4.7.1) using this formula suggest the following conjectural refinement of a result of Mazur [40].

Conjecture 1.6. *Suppose N is prime and A is an optimal quotient of $J_0(N)$ corresponding to a newform f. Then $A(\mathbf{Q})_{\mathrm{tor}}$ is generated by the image of $(0)-(\infty)$ and $c_p = \#A(\mathbf{Q})_{\mathrm{tor}}$. Furthermore, the product of the c_p over all simple optimal quotients corresponding to newforms equals the numerator of $(N-1)/12$.*

I have checked this conjecture for all $N \leq 997$ and, up to a power of 2, for all $N \leq 2113$. The first part is known when A is an elliptic curve (see [48]). Upon hearing of this conjecture, Mazur reportedly proved it when all "q-Eisenstein quotients" are simple. There are three promising approaches to finding a complete proof. One involves the explicit formula of Theorem 1.5; another is based on Ribet's level lowering theorem (see [53]), and a third makes use of a simplicity result of Merel (see [46]).

The formula that lies behind Theorem 1.5 probably has a natural analogue in weight greater than 2. One could then guess that it produces Tamagawa numbers of motifs attached to eigenforms of higher weight; however, we have no idea if this is really the case. These numbers appear in the conjectures of Bloch and Kato, which generalize the BSD conjecture to motifs (see [7]). Anyone wishing to try to compute them should be aware of Neil Dummigan's paper [22], which gives some information about the Tamagawa numbers of motifs attached by Scholl in [57] to modular eigenforms.

1.1.4 Upper bounds on $\#Ш(A)$

V. Kolyvagin (see [34]) and K. Kato (see, e.g., [58]) constructed Euler systems that were used to prove that $Ш(A)$ is *finite* when $L(A,1) \neq 0$. To verify the full BSD conjecture for certain abelian varieties, we must make the Kolyvagin-Kato finiteness bound explicit. Kolyvagin's bounds involve computations with Heegner points, and Kato's involve a study of the Galois representations associated to A.

Kolyvagin's bounds

In [33], Kolyvagin obtains explicit upper bounds for $\#Ш(A)$ for a certain (finite) list of elliptic curves A by computing the index in $A(K)$ of the subgroup generated by the Heegner point, where K is a suitable imaginary quadratic extension. In [35], Kolyvagin and Logachev generalize Kolyvagin's earlier results; in Section 1.6, "Unsolved problems", they say that: "If one were to compute the height of a Heegner point y [...] considered in the present paper, then one would have succeeded in obtaining an upper bound for $\#Ш$ for this curve." (By "curve" they mean abelian variety.) This suggests that explicit computations should yield upper bounds on the order of $Ш(A)$, but that they had not yet figured out how to carry out such computations.

Kato's bounds

Kato has constructed Euler systems coming from K_2-groups of modular curves. These can be used to prove the following theorem (see, e.g., [56, Cor. 3.5.19]).

Theorem 1.7 (Kato). *Suppose E is an elliptic curve over $\mathbf{Q}$ without complex multiplication that E has conductor N, that E has good reduction at p, that p does not divide $2r_E \prod_{q|N} L_q(q^{-1})\#E(\mathbf{Q}_q)_{\mathrm{tor}}$, and the Galois representation $\rho_{E,p} : G_{\mathbf{Q}} \to \mathrm{Aut}(E[p])$ is surjective. Then*

$$\#Ш(E)_{p^\infty} \text{ divides } \frac{L(E,1)}{\Omega_E}.$$

Here $L_q(x)$ is the local Euler factor at q and the constant r_E arises in the construction of Kato's Euler system. Rubin suggests that computing r_E is not very difficult (private communication). Appropriate variants of Kato's arguments give similar results for quotients of $J_0(N)$ of arbitrary dimension, though these have not been written down.

1.1.5 Lower bounds on $\#Ш(A)$

One approach to showing that $Ш(A)$ is as *at least* as large as predicted by the BSD conjecture is suggested by Mazur's notion of the visible part $Ш(A)^\circ$ of $Ш(A)$ (see [18, 43]). Let $A^\vee \subset J_0(N)$ be the dual to A. The *visible part* of $Ш(A^\vee)$ is the kernel of the natural map $Ш(A^\vee) \to Ш(J_0(N))$. Mazur observed that if an element of order p in $Ш(A^\vee)$ is visible, then it is explained by a "jump in the rank of Mordell-Weil" in the sense that there is another abelian subvariety $B \subset J_0(N)$ such that $p \mid \#(A^\vee \cap B)$ and the rank of B is positive.

Mazur's observation can be turned around: if there is another abelian variety B of positive rank such that $p \mid \#(A^\vee \cap B)$, then, under mild hypotheses (see Theorem 1.8), there is an element of $Ш(A^\vee)$ of order p. From a computational point of view it is easy to understand the intersections $A^\vee \cap B$; see Section 3.6. From a theoretical point of view, nontrivial intersections "correspond" to congruences between modular forms. Thus the well-developed theory of congruences between modular forms can be used to obtain a lower bound on $\#Ш(A^\vee)$.

Invisible elements of $\#Ш(A^\vee)$

Numerical experiments suggest that as $A^\vee$ varies, $Ш(A^\vee)$ is often *not* visible inside of $J_0(N)$. For example (see Table 1.2), the BSD conjecture predicts the existence of invisible elements of odd order in $Ш(A^\vee)$ for almost half of the 37 optimal quotients of prime level ≤ 2113.

Visibility at higher level

For every integer M (Ribet [54] tells us which M to choose), we can ask whether $Ш(A^\vee)$ maps to 0 under one of the natural maps $A^\vee \to J_0(NM)$; that is, we can ask whether $Ш(A^\vee)$ "becomes visible at level NM." We have been unable to prove in any particular case that $Ш(A^\vee)$ is not visible at level N, but becomes visible at some level NM. See Section 1.4.1 for some computations which strongly indicate that such examples exist.

Visibility in some Jacobian

Johan de Jong proved that if E is an elliptic curve over a number field K and $c \in H^1(K, E)$ then there is a Jacobian J and an imbedding $E \hookrightarrow J$ such that c maps to 0 under the natural map $H^1(K, E) \to H^1(K, J)$ (see Remark 3 in [18]); de Jong's proof appears to generalize when E is replaced by an abelian variety, but time does not permit going into the details here.

1.1.6 Motivation for considering abelian varieties

If A is an elliptic curve, then explaining $Ш(A)$ using only congruences between elliptic curves will probably fail. This is because pairs of non-isogenous elliptic curves with isomorphic p-torsion for large p are, according to E. Kani's conjecture, extremely rare. It is crucial to understand what happens in all dimensions.

Within the range accessible by computer, abelian varieties exhibit more richly textured structure than elliptic curves. For example, there is a visible element of prime order 83341 in the Shafarevich-Tate group of an abelian variety of prime conductor 2333; in contrast, over all optimal elliptic curves of conductor up to 5500, it appears that the largest order of an element of a Shafarevich-Tate group is 7 (see the discussion in [18]).

1.2 Existence of nontrivial visible elements of $Ш(A)$

The reader who wants to see tables of Shafarevich-Tate groups can safely skip to the next section.

Without relying on any unverified conjectures, we will use the following theorem to exhibit abelian varieties A such that the visible part of $Ш(A)$ is nonzero. In the following theorem we do *not* assume that J is the Jacobian of a curve.

Theorem 1.8. *Let A and B be abelian subvarieties of an abelian variety J such that $A \cap B$ is finite and $A(\mathbf{Q})$ is finite. Assume that B has purely toric reduction at each prime at which J has bad reduction. Let p be an odd prime at which J has good reduction, and assume that p does not divide the orders of any of the (geometric) component groups of A and B, or the orders of the torsion subgroups of $(J/B)(\mathbf{Q})$ and $B(\mathbf{Q})$. Suppose further that $B[p] \subset A \cap B$. Then there exists an injection*

$$B(\mathbf{Q})/pB(\mathbf{Q}) \hookrightarrow Ш(A)^{\circ}$$

of $B(\mathbf{Q})/pB(\mathbf{Q})$ into the visible part of Ш(A).

Proof. Let $C = J/A$. The long exact sequence of Galois cohomology associated to the short exact sequence

$$0 \to A \to J \to C \to 0$$

begins

$$0 \to A(\mathbf{Q}) \to J(\mathbf{Q}) \to C(\mathbf{Q}) \xrightarrow{\delta} H^1(\mathbf{Q}, A) \to \cdots .$$

Because $B[p] \subset A$, the map $B \to C$, obtained by composing the inclusion $B \hookrightarrow J$ with $J \to C$, factors through multiplication-by-p, giving the following commutative diagram:

$$\begin{tikzcd}
 & B \arrow[r, "p"] \arrow[d] & B \arrow[d] \\
A \arrow[r] & J \arrow[r] & C.
\end{tikzcd}$$

Because $B(\mathbf{Q})[p] = 0$ and $B(\mathbf{Q}) \cap A(\mathbf{Q}) = 0$, we deduce the following commutative diagram with exact rows:

$$\begin{tikzcd}
 & 0 \arrow[d] & K_1 \arrow[d] & K_2 \arrow[d] & \\
0 \arrow[r] & B(\mathbf{Q}) \arrow[r, "p"] \arrow[d] & B(\mathbf{Q}) \arrow[r] \arrow[d] \arrow[dr, "\pi"] & B(\mathbf{Q})/pB(\mathbf{Q}) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & J(\mathbf{Q})/A(\mathbf{Q}) \arrow[r] \arrow[d] & C(\mathbf{Q}) \arrow[r] & \delta(C(\mathbf{Q})) \arrow[r] & 0 \\
 & K_3, & & &
\end{tikzcd}$$

where K_1 and K_2 are the indicated kernels and K_3 is the cokernel. We have the snake lemma exact sequence

$$0 \to K_1 \to K_2 \to K_3.$$

Because $B(\mathbf{Q})[p] = 0$ and K_2 is a p-torsion group, we have $K_1 = 0$. The quotient $J(\mathbf{Q})/B(\mathbf{Q})$ has no p-torsion because it is a subgroup of $(J/B)(\mathbf{Q})$; also, $A(\mathbf{Q})$ is a finite group of order coprime to p, so $K_3 = J(\mathbf{Q})/(A(\mathbf{Q}) + B(\mathbf{Q}))$ has no p-torsion. Thus $K_2 = 0$.

The above argument shows that $B(\mathbf{Q})/pB(\mathbf{Q})$ is a subgroup of $H^1(\mathbf{Q}, A)$. However, $H^1(\mathbf{Q}, A)$ contains infinitely many elements of order p (see [59]), whereas $Ш(A)[p]$ is a finite group, so we must work harder to deduce that $B(\mathbf{Q})/pB(\mathbf{Q})$ lies in $Ш(A)[p]$. Fix $x \in B(\mathbf{Q})$. We must show that $\pi(x)$ lies in $Ш(A)[p]$; equivalently, that $\mathrm{res}_v(\pi(x)) = 0$ for all places v of $\mathbf{Q}$.

At the archimedean place $v = \infty$, the restriction $\mathrm{res}_v(\pi(x))$ is killed by 2 and the odd prime p, hence $\mathrm{res}_v(\pi(x)) = 0$.

Suppose that v is a place at which J has bad reduction. By hypothesis, B has purely toric reduction, so over the maximal unramified extension $\mathbf{Q}_v^{\mathrm{ur}}$ of $\mathbf{Q}_v$ there is an isomorphism $B \cong \mathbf{G}_m^d/\Gamma$ of $\mathrm{Gal}(\overline{\mathbf{Q}}_v/\mathbf{Q}_v^{\mathrm{ur}})$-modules, for some "lattice" Γ. For example, when $\dim B = 1$, this is the Tate curve representation of B. Let n be the order of the component group of B at v; thus n equals the order of the cokernel of the valuation map $\Gamma \to \mathbf{Z}^d$. Choose a representative $P = (x_1, \ldots, x_d) \in \mathbf{G}_m^d$ for the point x. Then nP can be adjusted by elements of Γ so that each of its components $x_i \in \mathbf{G}_m$ has valuation 0. By assumption, p is a prime at which J has good reduction, so $p \neq v$; it follows that there is a point $Q \in \mathbf{G}_m^d(\mathbf{Q}_v^{\mathrm{ur}})$ such that $pQ = nP$. Thus the cohomology class $\mathrm{res}_v(\pi(nx))$ is unramified at v. By [51, Prop. I.3.8],

$$H^1(\mathbf{Q}_v^{\mathrm{ur}}/\mathbf{Q}_v, A(\mathbf{Q}_v^{\mathrm{ur}})) = H^1(\mathbf{Q}_v^{\mathrm{ur}}/\mathbf{Q}_v, \Phi_{A,v}(\overline{\mathbf{F}}_v)),$$

where $\Phi_{A,v}$ is the component group of A at v. Since the component group $\Phi_{A,v}(\overline{\mathbf{F}}_v)$ has order n, it follows that

$$\mathrm{res}_v(\pi(nx)) = n\,\mathrm{res}_v(\pi(x)) = 0.$$

Since the order p of $\mathrm{res}_v(\pi(x))$ is coprime to n, we conclude that $\mathrm{res}_v(\pi(x)) = 0$.

Next suppose that J has good reduction at v and that v is *odd*, in the sense that the residue characteristic of v is odd. To simplify notation in this paragraph, since v is a non-archimedean place of $\mathbf{Q}$, we will also let v denote the odd prime number which is the residue characteristic of v. Let $\mathcal{A}$, $\mathcal{J}$, $\mathcal{C}$, be the Néron models of A, J, and C, respectively (for more on Néron models, see Chapter 4). Let A, J, C, also denote the sheaves on the étale-site over $\mathrm{Spec}(\mathbf{Z}_v)$ determined by the group schemes $\mathcal{A}$, $\mathcal{J}$, and $\mathcal{C}$, respectively. Since v is odd, $1 = e < v - 1$, so we may apply [8, Thm. 7.5.4] to conclude that the sequence of group schemes

$$0 \to \mathcal{A} \to \mathcal{J} \to \mathcal{C} \to 0$$

is exact; in particular, it is exact as a sequence of sheaves on the étale site (see the proof of [8, Thm. 7.5.4]). Thus it is exact on the stalks, so by [49, 2.9(d)] the sequence

$$0 \to \mathcal{A}(\mathbf{Z}_v^{\mathrm{ur}}) \to \mathcal{J}(\mathbf{Z}_v^{\mathrm{ur}}) \to \mathcal{C}(\mathbf{Z}_v^{\mathrm{ur}}) \to 0$$

is exact; by the Néron mapping property the sequence

$$0 \to A(\mathbf{Q}_v^{\mathrm{ur}}) \to J(\mathbf{Q}_v^{\mathrm{ur}}) \to C(\mathbf{Q}_v^{\mathrm{ur}}) \to 0$$

is also exact. Thus $\mathrm{res}_v(\pi(x))$ in unramified, so it arises by inflation from an element of $H^1(\mathbf{Q}_v^{\mathrm{ur}}/\mathbf{Q}_v, A)$. By [51, Prop. I.3.8],

$$H^1(\mathbf{Q}_v^{\mathrm{ur}}/\mathbf{Q}_v, A) \cong H^1(\mathbf{Q}_v^{\mathrm{ur}}/\mathbf{Q}_v, \Phi_{A,v}),$$

where $\Phi_{A,v}$ is the component group of A at v. Since A has good reduction, $\Phi_{A,v} = 0$, hence $\mathrm{res}_v(\pi(x)) = 0$.

If J has bad reduction at $v = 2$, then we already dealt with 2 above. Consider the case when J has good reduction at 2. Because the absolute ramification index e of $\mathbf{Z}_2$ is 1, which is *not* less than $v - 1 = 1$, we can not apply [8, Thm. 7.5.4]. However, we can modify our situation by an isogeny of degree a power of 2, then apply a different theorem as follows. The 2-primary subgroup Ψ of $A \cap B$ is rational as a subgroup over $\mathbf{Q}$, in the sense that the conjugates of any point in Ψ are also contained in Ψ. The abelian varieties $\tilde{J} = J/\Psi$, $\tilde{A} = A/\Psi$, and $\tilde{B} = B/\Psi$ also satisfy the hypothesis of the theorem we are proving. By [8, Prop. 7.5.3(a)], the corresponding sequence of Néron models

$$0 \to \tilde{\mathcal{A}} \to \tilde{\mathcal{J}} \to \tilde{\mathcal{C}} \to 0$$

is exact, so the sequence

$$0 \to \tilde{A}(\mathbf{Q}_v^{\mathrm{ur}}) \to \tilde{J}(\mathbf{Q}_v^{\mathrm{ur}}) \to \tilde{C}(\mathbf{Q}_v^{\mathrm{ur}}) \to 0$$

is exact. Thus the image of $\mathrm{res}_v(\pi(x))$ in $H^1(\mathbf{Q}_v, \tilde{A})$ is unramified. It equals 0, again by [51, Prop. 3.8], since the component group of $\tilde{A}$ at v has order a power of 2 (in fact it is trivial, since $\tilde{A}$ has good reduction at 2), whereas $\pi(x)$ has odd prime order p. Thus $\mathrm{res}_v(\pi(x)) = 0$, since the kernel of $H^1(\mathbf{Q}_v, A) \to H^1(\mathbf{Q}_v, \tilde{A})$ is a finite group of 2-power order. $\square$

1.3 Description of tables

In this section we describe our tables of optimal quotients of $J_0(N)$, which have nontrivial Shafarevich-Tate group. The tables, which can be found on pages 15–18, were computed using a combination of HECKE [64], LIDIA, NTL, PARI, and most successfully MAGMA [9]. The component group computations at non-prime level rely on Kohel's quaternion algebra package, which was also written in MAGMA.

We compute the conjectural order of the Shafarevich-Tate group of an abelian variety A, and then make assertions about the Shafarevich-Tate group of $A^\vee$. This is justified because the order of $Ш(A^\vee)$ equal the order of $Ш(A)$, since both are finite and the Cassells-Tate pairing sets up a nondegenerate duality between them.

1.3.1 Notation

Each optimal quotient A of $J_0(N)$ is denoted by a label, such as **389E**, which consists of a level N and a letter indicating the isogeny class. In the labeling, N is a positive integer and the isogeny class is given by a letter: the first isogeny class is labeled **A**, the second is labeled **B**, the third labeled **C**, and so on. Thus **389E** is the fifth isogeny class of optimal quotient of $J_0(389)$, corresponding to a Galois-conjugacy class of newforms. The isogeny classes that we consider are in bijection with the Galois-conjugacy classes of newforms in $S_2(\Gamma_0(N))$. The classes of newforms are ordered as described in Section 3.5.5.

WARNING: The *odd part* of a rational number x is $x/2^v$, where $v = \mathrm{ord}_2(x)$. In the tables, only the **odd parts** of the arithmetic invariants of A are given.

1.3.2 Table 1.2: Shafarevich-Tate groups at prime level

Table 1.2 was constructed as follows. Using the results of Section 3.10, we computed the odd part of the conjectural order $\#\text{Ш}_{\text{an}}(A)$ of the Shafarevich-Tate group of every optimal quotient of $J_0(p)$ that corresponds to a single Galois conjugacy-class of eigenforms and has analytic rank 0, for p a prime with $p \leq 2161$. We also computed a few sporadic examples of prime level p with $p > 2161$. The sporadic examples appear at the bottom of the table below a horizontal line.

Notation

The columns of the table contain the following information. The abelian varieties A for which $\#\text{Ш}_{\text{an}}(A)$ is greater than 1 are laid out in the first column of Table 1.2. The second column contains the dimensions of the abelian varieties in the first column. The third column contains the *odd part* (i.e., largest odd divisor) of the order of the Shafarevich-Tate group, as predicted by the BSD conjecture. Column four contains the odd parts of the modular degrees of the abelian varieties in the first column.

The fifth column contains an optimal quotient B of $J_0(p)$ of positive analytic rank, such that the ℓ-torsion of $B^\vee$ is contained in $A^\vee$, when one exists, where ℓ is a divisor of $\#\text{Ш}_{\text{an}}(A)$. We computed this intersection using the algorithm described in Section 3.6. Such a B is called an *explanatory factor*. When no such abelian varieties exists, we write "NONE" in the fifth column. The sixth column contains the dimensions of the abelian varieties in the fifth column, and the seventh column contains the odd parts of the modular degrees of the abelian varieties in the fifth column.

Ranks of the explanatory factors

That the explanatory factors have positive analytic rank follows from our modular symbols computation of $L(B,1)/\Omega_B$. This is supported by the table in [11], except in the case **2333A**, where there is a mistake in [11] (see below).

The explanatory factor **389A** is the first elliptic curve of rank 2. The table in [11] suggests that the explanatory factor **1061B** is the first 2-dimensional abelian variety (attached to a newform) whose Mordell-Weil group when tensored with the field of fractions F of the corresponding ring of Fourier coefficients, is of dimension 2 over F. Similarly **1567B** appears to be the first 3-dimensional one of rank 2, and **2333A** is the first 4-dimensional one of rank 2. It thus seems very likely that the ranks of each explanatory factor is exactly 2, though we have not proved this.

Discussion of the data

There are 23 examples in which $\text{Ш}(A)$ is visible and 18 in which $\text{Ш}(A)$ is invisible. The largest visible $\text{Ш}(A)$ found occurs at level 2333 and has order at least 83341^2 (83341 is prime). The largest invisible $\text{Ш}(A)$ occurs in a 112-dimensional abelian variety at level 2111 and has order at least 211^2.

The example **1283C** demonstrates that $\#\text{Ш}_{\text{an}}(A)$ can divide the modular degree, yet be *invisible*. In this case 5 divides $\#\text{Ш}_{\text{an}}(A)$. Since 5 divides the modular degree, it follows that there must be other non-isogenous subvarieties of $J_0(1283)$ that intersect **1283C** in a subgroup of order divisible by 5. In this case, the only such subvariety is **1283A**, which has dimension 2 and whose 5-torsion is contained in **1283C**. However **1283A** has analytic (hence algebraic) rank 0, so $\#\text{Ш}_{\text{an}}(A)$ cannot be visible.

The cases **1483D**, **1567D**, **2029C**, and **2593B** are interesting because *all* of Ш, even though it has two nontrivial p-primary components in each of these cases, is made visible in a single B. In the case **1913E** only the 5-primary component of Ш is visible in **1913A**, but still *both* the 5-primary and 61-primary components of Ш are visible in **1913C**.

Examples **1091C** and **1429B** were first found in [1] and **1913B** in [18].

Errata to Brumer's paper

Contrary to our computations, [11] suggests that **2333A** has rank 0. However, the author pointed the discrepancy out to Brumer who replied:

> I looked in vain for information about θ-relations on 2333 and have concluded that I never ran the interval from 2300 to 2500 or else had lost all info by the time I wrote up the paper. The punchline: 4 relations for 2333 and 2 relations for 2381 (also missing from the table).

1.3.3 Tables 1.3–1.6: New visible Shafarevich-Tate groups

Let n denote the largest odd square dividing the numerator of $L(A,1)/\Omega_A$. Table 1.3 lists those A such that for some $p \mid n$ there exists a quotient B of $J_0(N)$, corresponding to a *newform* and having positive analytic rank, such that $(A^\vee \cap B^\vee)[p] \neq 0$. Our search was systematic up to level 1001, but there might be omitted examples between levels 1001 and 1028. Table 1.4 contains further arithmetic information about each explanatory factor. Table 1.6 gives the quantities involved in the formula of Chapter 4 for Tamagawa numbers, for each of the abelian varieties A in Table 1.3.

Notation

Most of the notation is the same as in Table 1.2. However the additional columns w_q and c_p contain the signs of the Atkin-Lehner involutions and the Tamagawa numbers, respectively. These are given in order, from smallest to largest prime divisor of N.

In each case B has dimension 1. When $4 \mid N$, we write "a" for c_2 to remind us that we did not compute c_2 because the reduction at 2 is additive. Again only *odd parts* of the invariants are given. Section 4.7.2 contains a discussion of the notation used in the headings of Table 1.6.

Remarks on the data

The explanatory factors B of level ≤ 1028 are *exactly* the set of rank 2 elliptic curves of level ≤ 1028.

Table 1.1: Odd invisible $|Ш_E| > 1$, all $N \leq 5500$ (from Table 1 of [18])

E	$\sqrt{\lvert Ш_E\rvert}$	m_E	**F**	m_F	Remarks
2849A	3	$2^5 \cdot 5 \cdot 61$	**NONE**	–	
3364C	7	$2^6 \cdot 3^2 \cdot 5^2 \cdot 7$	**none**	–	
4229A	3	$2^3 \cdot 3 \cdot 7 \cdot 13$	**none**	–	
4343B	3	$2^4 \cdot 1583$	**NONE**	–	
4914N	3	$2^4 \cdot 3^5$	**none**	–	**E** has rational 3-torsion
5054C	3	$2^3 \cdot 3^3 \cdot 11$	**none**	–	
5073D	3	$2^5 \cdot 3 \cdot 5 \cdot 7 \cdot 23$	**none**	–	
5389A	3	$2^2 \cdot 2333$	**NONE**	–	

1.4 Further visibility computations

1.4.1 Does Ш become visible at higher level?

This section is concerned with whether or not the examples of invisible elements of Shafarevich-Tate groups of elliptic curves of level N that are given in [18] become visible in abelian surfaces inside appropriate $J_0(Np)$. We analyze each of the cases in Table 1 of [18]. For the reader's convenience, the part of this table which concerns us is reproduced as Table 1.1. The most interesting examples we give are **2849A** and **5389A**. As in [18], the assertions below assume the truth of the BSD conjecture.

How we found the explanatory curves

We use a naive heuristic observation to find possible explanatory curves of higher level, even though their conductors are out of the range of Cremona's tables. Note that we have not proved that these factors are actually explanatory in any cases, and expect that in some cases they are not.

First we recall some of the notation from Table 1 of [18], which is partially reproduced below. The "NONE" label in the row corresponding to an elliptic curve E indicates that there are elements in $Ш(E)$ whose order does not divide the modular degree of E, and hence they must be invisible. The label "none" indicates only that no suitable explanatory elliptic curves could be found, so $Ш(E)$ is not visible in an *abelian surface* inside $J_0(N)$; it could, however, be visible in the full abelian variety $J_0(N)$.

Studying the Weierstrass equations corresponding to the curves in [18] reveals that the elliptic curves labeled "NONE" have unusually large height, as compared to their conductors. However, the explanatory factors often have unusually small height. Motivated by this purely heuristic observation, we make a table of all elliptic curves of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_1, a_2, a_3 \in \{-1, 0, 1\}$, $|a_4|, |a_6| < 1000$, and conductor bounded by 50000. The bound on the conductor is required only so that the table will fit within computer storage. This table took a few days to generate.

2849A

Barry Mazur and Adam Logan found the first known example of an *invisible* Shafarevich-Tate group. This was $\text{Ш}(E)$, where E is the elliptic curve **2849A**, which has minimal Weierstrass equation

$$E: \quad y^2 + xy + y = x^3 + x^2 - 53484x - 4843180.$$

Consulting our table of curves of small height, we find an elliptic curve F of conductor $8547 = 2849 \cdot 3$ such that $f_E \equiv f_F \pmod 3$, where f_E and f_F are the newforms attached to E and F, respectively. This is a congruence for *all* eigenvalues a_p attached to E and F. The elliptic curve F is defined by the equation

$$F: \quad y^2 + xy + y = x^3 + x^2 - 154x - 478.$$

Cremona's program `mwrank` reveals that the Mordell-Weil group of F has rank 2. Thus maybe $\text{Ш}(E)$ becomes visible at level 8547. Unfortunately, visibility of $\text{Ш}(E)$ is not implied by Theorem 1.8 because the geometric component group of F at 3 has order divisible by 3.

4343B

Consider the elliptic curve E labeled **4343B**. According to Table 1 of [18], $\text{Ш}(E)$ has order 9, but the modular degree prevents $\text{Ш}(E)$ from being visible in $J_0(4343)$. At level $21715 = 5 \cdot 4343$ there is an elliptic curve F of rank 1 that is congruent to E. Its equation is

$$F: \quad y^2 - xy - y = x^3 - x^2 + 78x - 256.$$

5389A

The last curve labeled "NONE" in the table is curve **5389A**, which has minimal Weierstrass equation

$$y^2 + xy + y = x^3 - 35590x - 2587197.$$

The main theorem of [54] implies that there exists a newform that is congruent modulo 3 to the newform corresponding to **5389A** and of level $3 \cdot 5389$. This is because $(-2)^2 = (3+1)^2 \pmod 3$. However, our table of curves of small height does not contain any curve of conductor $3 \cdot 5389$. Next we observe that $(-2)^2 \equiv (7+1)^2 \pmod 3$, so using Ribet's theorem we can instead augment the level by 7. Our table of small-height curves contains just one (up to isogeny) elliptic curve of conductor 37723, and *luckily* the corresponding newform is congruent modulo 3 to the newform corresponding to **5389A** (away from primes dividing the level)! The Weierstrass equation of this curve is

$$F: \quad y^2 - y = x^3 + x^2 + 34x - 248.$$

According to Cremona's program `mwrank`, the rank of F is 2.

3364C, 4229A, 5073D

Perhaps $\text{Ш}(E)$ is already visible in some of the cases in which the curve is labeled "none", because the method fails in most of these cases. Each of the curves **3364C**, **4229A**, and **5073D** is labeled "none". In none of these 3 cases are we able to find an explanatory factor at higher level, within the range of our table of elliptic curves of small height.

4194N, 5054C

The curve **4914N** is labeled "none" and we find the remark "E has rational 3-torsion". There is a congruent curve F of conductor 24570 given by the equation

$$F: \quad y^2 - xy = x^3 - x^2 - 15x - 75,$$

and $F(\mathbf{Q}) = \{0\}$. The curve **5054C** is labeled "none" and its Shafarevich-Tate group contains invisible elements of order 3. We find a congruent curve of level 25270 and rank 1. The equation of the congruent curve is

$$F: y^2 - xy = x^3 + x^2 - 178x + 882.$$

1.4.2 Positive rank example

The abelian varieties with nontrivial $\text{Ш}(A)$ that one finds in both ours and Cremona's tables all have rank 0. In this section we outline a computation which sugggests, but does not prove, that there is a positive-rank abelian subvariety A of $J_0(5077)$ such that $\text{Ш}(A)$ possesses a nontrivial visible element of order 31.

According to [16], the smallest conductor elliptic curve E of rank 3 is found in $J = J_0(5077)$. The number 5077 is prime, and the isogeny decomposition of J is[1]

$$J \sim A \times B \times E,$$

where each of A, B, and E are abelian subvarieties of J associated to newforms, which have dimensions 205, 216, and 1, respectively. Using Remark 3.38 or [69], we find that the modular degree of E is $1984 = 2^6 \cdot 31$. The sign of the Atkin-Lehner involution on E is the same as its sign on A, so $E[31] \subset A$. We have $E(\mathbf{Q}) \cong \mathbf{Z} \times \mathbf{Z} \times \mathbf{Z}$, and the component group of E is trivial. The numerator of $(5077-1)/12$ is $3^2 \cdot 47$, so [40] implies that none of the abelian varieties above have 31-torsion. It might be possible to find an analogue of Theorem 1.8 that applies when A has positive rank, and deduce in this case that $\text{Ш}(A)$ contains visible elements of order 31.

[1]This decomposition was found in about one minute using the Mestre-Oesterlé method of graphs (see [47]).

Table 1.2: Shafarevich-Tate groups at prime level. (The entries in the columns "mod deg" and "$\#Ш_{\mathrm{an}}$" are only really the odd parts of "mod deg" and "$\#Ш_{\mathrm{an}}$".)

A	dim	$\#Ш_{\mathrm{an}}(A)$	mod deg(A)	**B**	dim	mod deg(B)
389E	20	5^2	5	**389A**	1	5
433D	16	7^2	$3\cdot7\cdot37$	**433A**	1	7
563E	31	13^2	13	**563A**	1	13
571D	2	3^2	$3^2\cdot127$	**571B**	1	3
709C	30	11^2	11	**709A**	1	11
997H	42	3^4	3^2	**997B**	1	3
1061D	46	151^2	$61\cdot151\cdot179$	**1061B**	2	151
1091C	62	7^2	1	NONE		
1171D	53	11^2	$3^4\cdot11$	**1171A**	1	11
1283C	62	5^2	$5\cdot41\cdot59$	NONE		
1429B	64	5^2	1	NONE		
1481C	71	13^2	$5^2\cdot2833$	NONE		
1483D	67	$3^2\cdot5^2$	$3\cdot5$	**1483A**	1	$3\cdot5$
1531D	73	3^2	3	**1531A**	1	3
1559B	90	11^2	1	NONE		
1567D	69	$7^2\cdot41^2$	$7\cdot41$	**1567B**	3	$7\cdot41$
1613D	75	5^2	$5\cdot19$	**1613A**	1	5
1621C	70	17^2	17	**1621A**	1	17
1627C	73	3^4	3^2	**1627A**	1	3^2
1693C	72	1301^2	1301	**1693A**	3	1301
1811D	98	31^2	1	NONE		
1847B	98	3^6	1	NONE		
1871C	98	19^2	14699	NONE		
1877B	86	7^2	1	NONE		
1907D	90	7^2	$3\cdot5\cdot7\cdot11$	**1907A**	1	7
1913B	1	3^2	$3\cdot103$	**1913A**	1	$3\cdot5^2$
1913E	84	$5^4\cdot61^2$	$5^2\cdot61\cdot103$	**1913A,C**	$1,2$	$3\cdot5^2, 5^2\cdot61$
1933C	83	$3^2\cdot7^2$	$3\cdot7$	**1933A**	1	$3\cdot7$
1997C	93	17^2	1	NONE		
2027C	94	29^2	29	**2027A**	1	29
2029C	90	$5^2\cdot269^2$	$5\cdot269$	**2029A**	2	$5\cdot269$
2039F	99	$3^4\cdot5^2$	$19\cdot29\cdot7759\cdot3214201$	NONE		
2063C	106	13^2	$61\cdot139$	NONE		
2089J	91	11^2	$3\cdot5\cdot11\cdot19\cdot73\cdot139$	**2089B**	1	11
2099B	106	3^2	1	NONE		
2111B	112	211^2	1	NONE		
2113B	91	7^2	1	NONE		
2161C	98	23^2	1	NONE		
2333C	101	83341^2	83341	**2333A**	4	83341
2339C	114	3^8	6791	NONE		
2411B	123	11^2	1	NONE		
2593B	109	$67^2\cdot2213^2$	$67\cdot2213$	**2593A**	4	$67\cdot2213$

Table 1.3: New visible Shafarevich-Tate groups

A	dim	$\#Ш_{\mathrm{an}}$	w_q	c_p	$\#A(\mathbf{Q})$	$\frac{\#A(\mathbf{Q})\cdot L(A,1)}{\Omega_A}$	mod deg(A)	**B**
389E	20	5^2	$-$	97	97	5^2	5	**389A**
433D	16	7^2	$-$	3^2	3^2	7^2	$3\cdot 7\cdot 37$	**433A**
446F	8	11^2	$+-$	$1,3$	3	11^2	$11\cdot 359353$	**446B**
563E	31	13^2	$-$	281	281	13^2	13	**563A**
571D	2	3^2	$-$	1	1	3^2	$3^2\cdot 127$	**571B**
655D	13	3^4	$+-$	$1,1$	1	3^4	$3^2\cdot 19\cdot 515741$	**655A**
664F	8	5^2	$-+$	$a,1$	1	5^2	5	**664A**
681B	1	3^2	$+-$	$1,1$	1	3^2	$3\cdot 5^3$	**681C**
707G	15	13^2	$+-$	$1,1$	1	13^2	$13\cdot 800077$	**707A**
709C	30	11^2	$-$	59	59	11^2	11	**709A**
718F	7	7^2	$+-$	$1,1$	1	7^2	$7\cdot 151\cdot 35573$	**718B**
794G	14	11^2	$+-$	$3,1$	3	11^2	$3\cdot 7\cdot 11\cdot 47\cdot 35447$	**794A**
817E	15	7^2	$+-$	$1,5$	5	7^2	$7\cdot 79$	**817A**
916G	9	11^2	$-+$	$a,1$	1	11^2	$3^9\cdot 11\cdot 17\cdot 239$	**916C**
944O	6	7^2	$+-$	$a,1$	1	7^2	7	**944E**
997H	42	3^4	$-$	83	83	3^4	3^2	**997BC**
1001L	7	7^2	$+-+$	$1,1,1$	1	7^2	$7\cdot 19\cdot 47\cdot 2273$	**1001C**
1028E	14	11^2	$-+$	$a,1$	3	$3^4\cdot 11^2$	$3^{13}\cdot 11$	**1028A**

Table 1.4: Explanatory factors

B	rank	w_q	c_p	$\#A(\mathbf{Q})$	mod deg(A)	Comments
389A	2	$-$	1	1	5	first curve of rank 2
433A	2	$-$	1	1	7	
446B	2	$+-$	$1,1$	1	11	called **446D** in [16]
563A	2	$-$	1	1	13	
571B	2	$-$	1	1	3	
655A	2	$+-$	$1,1$	1	3^2	
664A	2	$-+$	$1,1$	1	5	
681C	2	$+-$	$1,1$	1	3	
707A	2	$+-$	$1,1$	1	13	
709A	2	$-$	1	1	11	
718B	2	$+-$	$1,1$	1	7	
794A	2	$+-$	$1,1$	1	11	
817A	2	$+-$	$1,1$	1	7	
916C	2	$-+$	$3,1$	1	$3\cdot 11$	
944E	2	$+-$	$1,1$	1	7	
997B	2	$-$	1	1	3	
997C	2	$-$	1	1	3	
1001C	2	$+-+$	$1,3,1$	1	$3^2\cdot 7$	
1028A	2	$-+$	$3,1$	1	$3\cdot 11$	intersects **1028E** mod 11

Table 1.5: Factorizations

$\mathbf{446} = 2\cdot 223$	$\mathbf{655} = 5\cdot 131$	$\mathbf{664} = 2^3\cdot 83$	$\mathbf{681} = 3\cdot 227$
$\mathbf{707} = 7\cdot 101$	$\mathbf{718} = 2\cdot 359$	$\mathbf{794} = 2\cdot 397$	$\mathbf{817} = 19\cdot 43$
$\mathbf{916} = 2^2\cdot 229$	$\mathbf{944} = 2^4\cdot 59$	$\mathbf{1001} = 7\cdot 11\cdot 13$	$\mathbf{1028} = 2^2\cdot 257$

Table 1.6: Component groups

A	dim	p	w_q	$\#\Phi_{X,p}$	$m_{X,p}$	$\#\Phi_{A,p}(\overline{\mathbf{F}}_p)$
389E	20	389	$-$	97	$5\cdot 97$	97
433D	16	433	$-$	3^2	$3^3\cdot 7\cdot 37$	3^2
446F	8	223	$-$	3	$3\cdot 11\cdot 359353$	3
		2	$+$	3	$3\cdot 11$	$3\cdot 359353$
563E	31	563	$-$	281	$13\cdot 281$	281
571D	2	571	$-$	1	$3^2\cdot 127$	1
655D	13	131	$-$	1	$3^2\cdot 19\cdot 515741$	1
		5	$+$	1	3^2	$19\cdot 515741$
664F	8	83	$+$	1	5	1
681B	1	227	$-$	1	$3\cdot 5^3$	1
		3	$+$	1	$3\cdot 5^2$	5
707G	15	101	$-$	1	$13\cdot 800077$	1
		7	$+$	1	13	800077
709C	30	709	$-$	59	$11\cdot 59$	59
718F	7	359	$-$	1	$7\cdot 151\cdot 35573$	1
		2	$+$	1	7	$151\cdot 35573$
794G	14	397	$-$	3	$3^2\cdot 7\cdot 11\cdot 47\cdot 35447$	3
		2	$+$	3	$3\cdot 11$	$3^2\cdot 7\cdot 47\cdot 35447$
817E	15	43	$-$	5	$5\cdot 7\cdot 79$	5
		19	$+$	1	7	79
916G	9	229	$+$	1	$3^9\cdot 11\cdot 17\cdot 239$	1
944O	6	59	$-$	1	7	1
997H	42	997	$-$	83	$3^2\cdot 83$	83
1001L	7	13	$+$	1	$7\cdot 19\cdot 47\cdot 2273$	1
		11	$-$	1	$7\cdot 19\cdot 47\cdot 2273$	1
		7	$+$	1	$7\cdot 19\cdot 47$	2273
1028E	14	257	$+$	1	$3^{13}\cdot 11$	1

Chapter 2

Modular symbols

Modular symbols permeate this thesis. In their simplest incarnation, modular symbols provide a finite presentation for the homology group $H_1(X_0(N), \mathbf{Z})$ of the Riemann surface $X_0(N)$. This presentation is equipped with such a rich structure that from it we can deduce the action of the Hecke operators; this is already sufficient information for us to compute a basis for the space $S_2(\Gamma_0(N), \mathbf{C})$ of cusp forms.

We recall the definition of spaces of modular symbols in Sections 2.1–2.2. Then in Section 2.3, we review the duality between modular symbols and modular forms. In Section 2.4, we see that modular symbols are furnished with analogues of each of the standard operators that one finds on spaces of modular forms, and in Section 2.5 we see that the same is true of the degeneracy maps. Section 2.6 describes Manin symbols, which supply a convenient finite presentation for the space of modular symbols. Finally, Section 2.7 introduces the complex torus attached to a newform, which appears in various guises throughout this thesis.

Before continuing, we offer an apology. We will only consider modular symbols that are already equipped with a fixed Dirichlet character. Though fixing a character complicates the formulas, the resulting increase in efficiency is of extreme value in computational applications. Fixing a character allows us to compute in just the part of the space of modular symbols for $\Gamma_1(N)$ that interests us. We apologize for any inconvenience this may cause the less efficiency minded reader.

Acknowledgment. This chapter and the next were greatly influenced by the publications of Cremona [15, 16] and Merel [45], along with the foundational contributions of Manin [38], Mazur [42, 39], and Shokurov [63]. Cremona's book [16] provides a motivated roadmap that guides the reader who wishes to compute with modular symbols in the familiar context of elliptic curves, and Merel's article provides an accessible overview of the action of Hecke operators on higher weight modular symbols, and the connection between modular symbols and related cohomology theories.

2.1 The definition of modular symbols

Fix a positive integer N, an integer $k \geq 2$, and a continuous homomorphism

$$\varepsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$$

such that $\varepsilon(-1) = (-1)^k$. We call N the *level*, k the *weight*, and ε the *Dirichlet character*.

Consider the quotient of the abelian group generated by all formal symbols $\{\alpha, \beta\}$, with $\alpha, \beta \in \mathbf{P}^1(\mathbf{Q}) = \mathbf{Q} \cup \{\infty\}$, by the following relations:

$$\{\alpha, \beta\} + \{\beta, \gamma\} + \{\gamma, \alpha\} = 0,$$

for all $\alpha, \beta, \gamma \in \mathbf{P}^1(\mathbf{Q})$. Let $\boldsymbol{\mathcal{M}}$ be the torsion-free quotient of this group by its torsion subgroup. Because $\boldsymbol{\mathcal{M}}$ is torsion free, $\{\alpha, \alpha\} = 0$ and $\{\alpha, \beta\} = -\{\beta, \alpha\}$.

Remark 2.1. One is motivated to consider these relations by viewing $\{\alpha, \beta\}$ as the homology class of an appropriate path from α to β in the upper half plane.

Let V_{k-2} be the $\mathbf{Z}$-submodule of $\mathbf{Z}[X, Y]$ made up of all homogeneous polynomials of degree $k-2$, and set $\boldsymbol{\mathcal{M}}_k := V_{k-2} \otimes \boldsymbol{\mathcal{M}}$. For $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbf{Q})$ and $P \in V_{k-2}$, let

$$\begin{aligned} gP(X,Y) &= P\left(\det(g) g^{-1} \begin{pmatrix} X \\ Y \end{pmatrix}\right) = P\left(\begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}\right) \\ &= P(dX - bY, -cX + aY). \end{aligned}$$

This defines a left action of $\mathrm{GL}_2(\mathbf{Q})$ on V_{k-2}; it is a left action because

$$\begin{aligned} (gh)P(v) &= P(\det(gh)(gh)^{-1} v) = P(\det(h) h^{-1} \det(g) g^{-1} v) \\ &= gP(\det(h) h^{-1} v) = g(hP(v)). \end{aligned}$$

Combining this action with the action of $\mathrm{GL}_2(\mathbf{Q})$ on $\mathbf{P}^1(\mathbf{Q})$ by linear fractional transformations gives a left action of $\mathrm{GL}_2(\mathbf{Q})$ on $\boldsymbol{\mathcal{M}}_k$:

$$g(P \otimes \{\alpha, \beta\}) = g(P) \otimes \{g(\alpha), g(\beta)\}.$$

Finally, for $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, let $\varepsilon(g) := \varepsilon(\overline{a})$, where $\overline{a} \in \mathbf{Z}/N\mathbf{Z}$ is the reduction modulo N of a.

Let

$$\mathbf{Z}[\varepsilon] := \mathbf{Z}[\varepsilon(a) : a \in \mathbf{Z}/N\mathbf{Z}]$$

be the subring of $\mathbf{C}$ generated by the values of the character ε.

Definition 2.2 (Modular symbols). The space of *modular symbols* $\boldsymbol{\mathcal{M}}_k(N, \varepsilon)$ of level N, weight k and character ε is the largest torsion-free quotient of $\boldsymbol{\mathcal{M}}_k \otimes \mathbf{Z}[\varepsilon]$ by the $\mathbf{Z}[\varepsilon]$-submodule generated by the relations $gx - \varepsilon(g)x$ for all $x \in \boldsymbol{\mathcal{M}}_k$ and all $g \in \Gamma_0(N)$.

Denote by $P\{\alpha, \beta\}$ the image of $P \otimes \{\alpha, \beta\}$ in $\boldsymbol{\mathcal{M}}_k(N, \varepsilon)$. For any $\mathbf{Z}[\varepsilon]$-algebra R, let

$$\boldsymbol{\mathcal{M}}_k(N, \varepsilon; R) := \boldsymbol{\mathcal{M}}_k(N, \varepsilon) \otimes_{Z[\varepsilon]} R.$$

See Section 3.1 for an algorithm which can be used to compute $\boldsymbol{\mathcal{M}}_k(N, \varepsilon; \mathbf{Q}(\varepsilon))$.

2.2 Cuspidal modular symbols

Let $\boldsymbol{\mathcal{B}}$ be the free abelian group generated by the symbols $\{\alpha\}$ for all $\alpha \in \mathbf{P}^1(\mathbf{Q})$. There is a left action of $\mathrm{GL}_2(\mathbf{Q})$ on $\boldsymbol{\mathcal{B}}$ given by $g\{\alpha\} = \{g(\alpha)\}$. Let $\boldsymbol{\mathcal{B}}_k := V_{k-2} \otimes \boldsymbol{\mathcal{B}}$, and let $\mathrm{GL}_2(\mathbf{Q})$ act on $\boldsymbol{\mathcal{B}}_k$ by $g(P\{\alpha\}) = (gP)\{g(\alpha)\}$.

Definition 2.3 (Boundary modular symbols). The space $\boldsymbol{\mathcal{B}}_k(N,\varepsilon)$ of *boundary modular symbols* is the largest torsion-free quotient of $\boldsymbol{\mathcal{B}}_k \otimes \mathbf{Z}[\varepsilon]$ by the relations $gx = \varepsilon(g)x$ for all $g \in \Gamma_0(N)$ and $x \in \boldsymbol{\mathcal{B}}_k$.

Denote by $P\{\alpha\}$ the image of $P \otimes \{\alpha\}$ in $\boldsymbol{\mathcal{B}}_k(N,\varepsilon)$. The *boundary map*

$$\delta : \boldsymbol{\mathcal{M}}_k(N,\varepsilon) \to \boldsymbol{\mathcal{B}}_k(N,\varepsilon)$$

is defined by

$$\delta(P\{\alpha,\beta\}) = P\{\beta\} - P\{\alpha\}.$$

Definition 2.4 (Cuspidal modular symbols). The space $\boldsymbol{\mathcal{S}}_k(N,\varepsilon)$ of *cuspidal modular symbols* is the kernel of δ.

The three spaces defined above fit together in the following exact sequence:

$$0 \to \boldsymbol{\mathcal{S}}_k(N,\varepsilon) \to \boldsymbol{\mathcal{M}}_k(N,\varepsilon) \xrightarrow{\delta} \boldsymbol{\mathcal{B}}_k(N,\varepsilon).$$

2.3 Duality between modular symbols and modular forms

For any positive integer k, any $\mathbf{C}$-valued function f on the complex upper half plane

$$\mathfrak{h} := \{z \in \mathbf{C} : \mathrm{im}(z) > 0\},$$

and any matrix $\gamma \in \mathrm{GL}_2(\mathbf{Q})$, define a function $f|[\gamma]_k$ on $\mathfrak{h}$ by

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

Definition 2.5 (Cusp forms). Let $S_k(N,\varepsilon)$ be the complex vector space of holomorphic functions $f(z)$ on $\mathfrak{h}$ that satisfy the equation

$$f|[\gamma]_k = \varepsilon(\gamma)f$$

for all $\gamma \in \Gamma_0(N)$, and such that f is holomorphic and vanishes at all cusps, in the sense of [21, pg. 42].

Definition 2.6 (Antiholomorphic cusp forms). Let $\overline{S}_k(N,\varepsilon)$ be the space of *antiholomorphic cusp forms*; the definition is as above, except

$$\frac{f(\gamma z)}{(c\overline{z}+d)^k} = \overline{\varepsilon}(\gamma)f(z)$$

for all $\gamma \in \Gamma_0(N)$.

There is a canonical isomorphism of real vector spaces between $S_k(N,\varepsilon)$ and $\overline{S}_k(N,\varepsilon)$ that associates to f the antiholomorphic cusp form defined by the function $z \mapsto \overline{f(z)}$.

Theorem 2.7 (Merel). *There is a pairing*

$$\langle\ ,\ \rangle : (S_k(N,\varepsilon) \oplus \overline{S}_k(N,\varepsilon)) \times \boldsymbol{\mathcal{M}}_k(N,\varepsilon;\mathbf{C}) \to \mathbf{C}$$

given by

$$\langle f \oplus g, P\{\alpha,\beta\}\rangle = \int_\alpha^\beta f(z)P(z,1)dz + \int_\alpha^\beta g(z)P(\overline{z},1)d\overline{z},$$

where the path from α to β is, except for the endpoints, contained in $\mathfrak{h}$. The pairing is perfect when restricted to $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;\mathbf{C})$.

Proof. Take the ε part of each side of [45, Thm. 3]. □

2.4 Linear operators

2.4.1 Hecke operators

For each positive integer n and each space V of modular symbols or modular forms, there is a *Hecke operator* T_n, which acts as a linear endomorphism of V. For the definition of T_n on modular symbols, see [45, §2]. Alternatively, because we consider only modular symbols with character, the following recipe completely determines the Hecke operators. First, when $n = p$ is prime, we have

$$T_p(x) = \left[\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} + \sum_{r \bmod p} \begin{pmatrix} 1 & r \\ 0 & p \end{pmatrix}\right] x,$$

where the first matrix is omitted if $p \mid N$. If m and n are coprime, then $T_{mn} = T_m T_n$. Finally, if p is a prime, $r \geq 2$ is an integer, ε is the Dirichlet character of associated to V, and k is the weight of V, then

$$T_{p^r} = T_p T_{p^{r-1}} - \varepsilon(p)p^{k-1}T_{p^{r-2}}.$$

Definition 2.8. The *Hecke algebra associated to V* is the subring

$$\mathbf{T} = \mathbf{T}_V = \mathbf{Z}[\ldots T_n \ldots]$$

of $\mathrm{End}(V)$ generated by all Hecke operators T_n, with $n = 1, 2, 3, \ldots$.

Proposition 2.9. *The pairing of Theorem 2.7 respects the action of the Hecke operators, in the sense that $\langle fT, x\rangle = \langle f, Tx\rangle$ for all $T \in \mathbf{T}$, $x \in \boldsymbol{\mathcal{M}}_k(N,\varepsilon)$, and $f \in S_k(N,\varepsilon) \oplus \overline{S}_k(N,\varepsilon)$.*

Proof. See [45, Prop. 10]. □

2.4.2 The $*$-involution

The matrix $j = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$ defines an involution $*$ of $\boldsymbol{\mathcal{M}}_k(N,\varepsilon)$ given by $x \mapsto x^* = j(x)$. Explicitly,

$$(P(X,Y)\{\alpha,\beta\})^* = P(X,-Y)\{-\alpha,-\beta\}.$$

Because the space of modular symbols is constructed as a quotient, it is not obvious that the $*$-involution is well defined.

Proposition 2.10. *The $*$-involution is well defined.*

Proof. Recall that $\boldsymbol{\mathcal{M}}_k(N,\varepsilon)$ is the largest torsion-free quotient of the free $\mathbf{Z}[\varepsilon]$-module generated by symbols $x = P\{\alpha,\beta\}$ by the submodule generated by relations $\gamma x - \varepsilon(\gamma)x$ for all $\gamma \in \Gamma_0(N)$. In order to check that the operator $*$ is well defined, it suffices to check, for any $x \in \boldsymbol{\mathcal{M}}_k$, that $*(\gamma x - \varepsilon(\gamma)x)$ is of the form $\gamma' y - \varepsilon(\gamma')y$, for some y in $\boldsymbol{\mathcal{M}}_k$. Note that if $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, then $j\gamma j^{-1} = \left(\begin{smallmatrix} a & -b \\ -c & d \end{smallmatrix}\right)$ is also in $\Gamma_0(N)$ and $\varepsilon(j\gamma j^{-1}) = \varepsilon(\gamma)$. We have

$$\begin{aligned} j(\gamma x - \varepsilon(\gamma)x) &= j\gamma x - j\varepsilon(\gamma)x \\ &= j\gamma j^{-1} jx - \varepsilon(\gamma)jx \\ &= (j\gamma j^{-1})(jx) - \varepsilon(j\gamma j^{-1})(jx). \end{aligned}$$

□

If f is a modular form, let f^* be the holomorphic function $\overline{f(-\overline{z})}$, where the bar denotes complex conjugation. The Fourier coefficients of f^* are the complex conjugates of those of f; though f^* is again a holomorphic modular form, its character is $\overline{\varepsilon}$ instead of ε. The pairing of Theorem 2.7 is the restriction of a pairing on the full spaces without character, and we have the following proposition.

Proposition 2.11. *We have*

$$\langle f^*, x^* \rangle = \overline{\langle f, x \rangle}.$$

Definition 2.12 (Plus-one quotient). The *plus-one quotient* $\boldsymbol{\mathcal{M}}_k(N,\varepsilon)_+$ is the largest torsion-free quotient of $\boldsymbol{\mathcal{M}}_k(N,\varepsilon)$ by the relations $x^* - x = 0$ for all $x \in \boldsymbol{\mathcal{M}}_k(N,\varepsilon)$. Similarly, the *minus-one quotient* is the quotient of $\boldsymbol{\mathcal{M}}_k(N,\varepsilon)$ by all relations $x^* + x = 0$, for $x \in \boldsymbol{\mathcal{M}}_k(N,\varepsilon)$.

WARNING 2.13. We were forced to make a choice in our definition of the operator $*$. Fortunately, it agrees with that of [16, §2.1.3], but *not* with the choice made in [45, §1.6].

2.4.3 The Atkin-Lehner involutions

In this section we assume that k is even and $\varepsilon^2 = 1$. The assumption on ε is necessary only so that the involution we are about to define preserves $\boldsymbol{\mathcal{M}}_k(N,\varepsilon)$. More generally, it is possible to define a map which sends $\boldsymbol{\mathcal{M}}_k(N,\varepsilon)$ to $\boldsymbol{\mathcal{M}}_k(N,\overline{\varepsilon})$.

To each divisor d of N such that $(d, N/d) = 1$ there is an *Atkin-Lehner involution* W_d of $\boldsymbol{\mathcal{M}}_k(N, \varepsilon)$, which is defined as follows. Using the Euclidean algorithm, choose integers x, y, z, w such that

$$dxw - (N/d)yz = 1.$$

Next let $g = \left(\begin{smallmatrix} dx & y \\ Nz & dw \end{smallmatrix}\right)$ and define

$$W_d(x) := \frac{1}{d^{\frac{k-2}{2}}} \cdot g(x).$$

For example, when $d = N$ we have $g = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$. The factor of $d^{\frac{k-2}{2}}$ is necessary to normalize W_d so that it is an involution.

On modular forms there is an Atkin-Lehner involution, also denoted W_d, which acts by $W_d(f) = f|[W_d]_k$. These two like-named involutions are compatible with the integration pairing:

$$\langle W_d(f), x\rangle = \langle f, W_d(x)\rangle.$$

2.5 Degeneracy maps

In this section, we describe natural maps between spaces of modular symbols of different levels.

Fix a positive integer N and a Dirichlet character $\varepsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$. Let M be a positive divisor of N that is divisible by the conductor of ε, in the sense that ε factors through $(\mathbf{Z}/M\mathbf{Z})^*$ via the natural map $(\mathbf{Z}/N\mathbf{Z})^* \to (\mathbf{Z}/M\mathbf{Z})^*$ composed with some uniquely defined character $\varepsilon' : (\mathbf{Z}/M\mathbf{Z})^* \to \mathbf{C}^*$. For any positive divisor t of N/M, let $T = \left(\begin{smallmatrix} 1 & 0 \\ 0 & t \end{smallmatrix}\right)$ and fix a choice $D_t = \{T\gamma_i : i = 1, \ldots, n\}$ of coset representatives for $\Gamma_0(N)\backslash T\Gamma_0(M)$.

WARNING 2.14. There is a mistake in [45, §2.6]: The quotient "$\Gamma_1(N)\backslash\Gamma_1(M)T$" should be replaced by "$\Gamma_1(N)\backslash T\Gamma_1(M)$".

Proposition 2.15. *For each divisor t of N/M there are well-defined linear maps*

$$\alpha_t : \boldsymbol{\mathcal{M}}_k(N, \varepsilon) \to \boldsymbol{\mathcal{M}}_k(M, \varepsilon'), \qquad \alpha_t(x) = (tT^{-1})x = \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} x$$

$$\beta_t : \boldsymbol{\mathcal{M}}_k(M, \varepsilon') \to \boldsymbol{\mathcal{M}}_k(N, \varepsilon), \qquad \beta_t(x) = \sum_{T\gamma_i \in D_t} \varepsilon'(\gamma_i)^{-1} T\gamma_i x.$$

Furthermore, $\alpha_t \circ \beta_t$ is multiplication by $t^{k-2} \cdot [\Gamma_0(M) : \Gamma_0(N)]$.

Proof. To show that α_t is well defined, we must show that for each $x \in \boldsymbol{\mathcal{M}}_k(N, \varepsilon)$ and $\gamma = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$, that we have

$$\alpha_t(\gamma x - \varepsilon(\gamma)x) = 0 \in \boldsymbol{\mathcal{M}}_k(M, \varepsilon').$$

We have

$$\alpha_t(\gamma x) = \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} \gamma x = \begin{pmatrix} a & tb \\ c/t & d \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} x = \varepsilon'(a) \begin{pmatrix} t & 0 \\ 0 & 1 \end{pmatrix} x,$$

so

$$\alpha_t(\gamma x - \varepsilon(\gamma)x) = \varepsilon'(a)\alpha_t(x) - \varepsilon(\gamma)\alpha_t(x) = 0.$$

We next verify that β_t is well defined. Suppose that $x \in \boldsymbol{\mathcal{M}}_k(M, \varepsilon')$ and $\gamma \in \Gamma_0(M)$; then $\varepsilon'(\gamma)^{-1}\gamma x = x$, so

$$\begin{aligned}\beta_t(x) &= \sum_{T\gamma_i \in D_t} \varepsilon'(\gamma_i)^{-1} T\gamma_i \varepsilon'(\gamma)^{-1}\gamma x \\ &= \sum_{T\gamma_i\gamma \in D_t} \varepsilon'(\gamma_i\gamma)^{-1} T\gamma_i\gamma x.\end{aligned}$$

This computation shows that the definition of β_t does not depend on the choice D_t of coset representatives. To finish the proof that β_t is well defined we must show that, for $\gamma \in \Gamma_0(M)$, we have $\beta_t(\gamma x) = \varepsilon'(\gamma)\beta_t(x)$ so that β_t respects the relations that define $\boldsymbol{\mathcal{M}}_k(M, \varepsilon)$. Using that β_t does not depend on the choice of coset representative, we find that for $\gamma \in \Gamma_0(M)$,

$$\begin{aligned}\beta_t(\gamma x) &= \sum_{T\gamma_i \in D_t} \varepsilon'(\gamma_i)^{-1} T\gamma_i\gamma x \\ &= \sum_{T\gamma_i\gamma^{-1} \in D_t} \varepsilon'(\gamma_i\gamma^{-1})^{-1} T\gamma_i\gamma^{-1}\gamma x \\ &= \varepsilon'(\gamma)\beta_t(x).\end{aligned}$$

To compute $\alpha_t \circ \beta_t$, we use that $\#D_t = [\Gamma_0(N) : \Gamma_0(M)]$:

$$\begin{aligned}\alpha_t(\beta_t(x)) &= \alpha_t\left(\sum_{T\gamma_i} \varepsilon'(\gamma_i)^{-1} T\gamma_i x\right) \\ &= \sum_{T\gamma_i} \varepsilon'(\gamma_i)^{-1}(tT^{-1})T\gamma_i x \\ &= t^{k-2}\sum_{T\gamma_i} \varepsilon'(\gamma_i)^{-1}\gamma_i x \\ &= t^{k-2}\sum_{T\gamma_i} x \\ &= t^{k-2} \cdot [\Gamma_0(N) : \Gamma_0(M)] \cdot x.\end{aligned}$$

The scalar factor of t^{k-2} appears instead of t, because t is acting on x as an element of $\mathrm{GL}_2(\mathbf{Q})$ *not* as an an element of $\mathbf{Q}$. $\square$

Definition 2.16 (New and old modular symbols). The subspace $\boldsymbol{\mathcal{M}}_k(N, \varepsilon)^{\mathrm{new}}$ of *new modular symbols* is the intersection of the kernels of the α_t as t runs through all positive divisors of N/M and M runs through positive divisors of M strictly less than N and divisible by the conductor of ε. The subspace $\boldsymbol{\mathcal{M}}_k(N, \varepsilon)^{\mathrm{old}}$ of *old modular symbols* is the subspace generated by the images of the β_t where t runs through all positive divisors of N/M and M runs through positive divisors of M strictly less than N and divisible by the conductor of ε.

WARNING: The new and old subspaces need not be disjoint, as the following example illustrates! This is contrary to the statement on page 80 of [45].

Example 2.17. We justify the above warning. Consider, for example, the case $N = 6$, $k = 2$, and trivial character. The spaces $\boldsymbol{\mathcal{M}}_2(2)$ and $\boldsymbol{\mathcal{M}}_2(3)$ are each of dimension 1, and each is generated by the modular symbol $\{\infty, 0\}$. The space $\boldsymbol{\mathcal{M}}_2(6)$ is of dimension 3, and is generated by the 3 modular symbols $\{\infty, 0\}$, $\{-1/4, 0\}$, and $\{-1/2, -1/3\}$. The space generated by the 2 images of $\boldsymbol{\mathcal{M}}_2(2)$ under the 2 degeneracy maps has dimension 2, and likewise for $\boldsymbol{\mathcal{M}}_2(3)$. Together these images generate $\boldsymbol{\mathcal{M}}_2(6)$, so $\boldsymbol{\mathcal{M}}_2(6)$ is equal to its old subspace. However, the new subspace is nontrivial because the two degeneracy maps $\boldsymbol{\mathcal{M}}_2(6) \to \boldsymbol{\mathcal{M}}_2(2)$ are equal, as are the two degeneracy maps $\boldsymbol{\mathcal{M}}_2(6) \to \boldsymbol{\mathcal{M}}_2(3)$. In particular, the intersection of the kernels of the degeneracy maps has dimension at least 1 (in fact, it equals 1).

Computationally, it appears that something similar to this happens if and only if the weight is 2, the character is trivial, and the level is composite. This behavior is probably related to the nonexistence of a characteristic 0 Eisenstein series of weight 2 and level 1.

The following tempting argument is incorrect; the error lies in the fact that an element of the old subspace is a *linear combination* of $\beta_t(y)$'s for various y's and t's: "If x is in both the new and old subspace, then $x = \beta_t(y)$ for some modular symbol y of lower level. This implies $x = 0$ because

$$0 = \alpha_t(x) = \alpha_t(\beta_t(y)) = t^{k-2} \cdot [\Gamma_0(N) : \Gamma_0(M)] \cdot y.\text{"}$$

Remark 2.18. The map $\beta_t \circ \alpha_t$ cannot in general be multiplication by a scalar since $\boldsymbol{\mathcal{M}}_k(M, \varepsilon')$ usually has smaller dimension than $\boldsymbol{\mathcal{M}}_k(N, \varepsilon)$.

2.5.1 Computing coset representatives

Definition 2.19 (Projective line mod N). Let N be a positive integer. Then the *projective line* $\mathbf{P}^1(N)$ is the set of pairs (a, b), with $a, b \in \mathbf{Z}/N\mathbf{Z}$ and $\gcd(a, b, N) = 1$, modulo the eqivalence relation which identifies (a, b) and (a', b') if and only if $ab' \equiv ba' \pmod{N}$.

Let M be a positive divisor of N and t a divisor of N/M. The following *random* algorithm computes a set D_t of representatives for the orbit space $\Gamma_0(M)\backslash T\Gamma_0(N)$. There are deterministic algorithms for computing D_t, but all of the ones the author has found are *vastly* less efficient than the following random algorithm.

Algorithm 2.20. Let $\Gamma_0(N/t, t)$ denote the subgroup of $\mathrm{SL}_2(\mathbf{Z})$ consisting of matrices that are upper triangular modulo N/t and lower triangular modulo t. Observe that two right cosets of $\Gamma_0(N/t, t)$ in $\mathrm{SL}_2(\mathbf{Z})$, represented by $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} a' & b' \\ c' & d' \end{smallmatrix}\right)$, are equivalent if and only if $(a, b) = (a', b')$ as points of $\mathbf{P}^1(t)$ and $(c, d) = (c', d')$ as points of $\mathbf{P}^1(N/t)$. Using the following algorithm, we compute right coset representatives for $\Gamma_0(N/t, t)$ inside $\Gamma_0(M)$.

1. Compute the number $[\Gamma_0(M) : \Gamma_0(N)]$ of cosets.

2. Compute a random element $x \in \Gamma_0(M)$.

3. If x is not equivalent to anything generated so far, add it to the list.

4. Repeat steps (2) and (3) until the list is as long as the bound of step (1).

There is a natural bijection between $\Gamma_0(N)\backslash T\Gamma_0(M)$ and $\Gamma_0(N/t,t)\backslash\Gamma_0(M)$, under which $T\gamma$ corresponds to γ. Thus we obtain coset representatives for $\Gamma_0(N)\backslash T\Gamma_0(M)$ by left multiplying each coset representative of $\Gamma_0(N/t,t)\backslash\Gamma_0(M)$ by T.

2.5.2 Compatibility with modular forms

The degeneracy maps defined above are compatible with the corresponding degeneracy maps $\tilde{\alpha}_t$ and $\tilde{\beta}_t$ on modular forms. This is because the degeneracy maps on modular forms are defined by summing over the same coset representatives D_t. Thus we have the following compatibilities.

$$\langle\tilde{\alpha}_t(f), x\rangle = \langle f, \alpha_t(x)\rangle,$$
$$\langle\tilde{\beta}_t(f), x\rangle = \langle f, \beta_t(x)\rangle.$$

If p is prime to N, then $T_p\alpha_t = \alpha_t T_p$ and $T_p\beta_t = \beta_t T_p$.

2.6 Manin symbols

From the definition given in Section 2.1, it is not obvious that $\boldsymbol{\mathcal{M}}_k(N,\varepsilon)$ is of finite rank. The Manin symbols provide a finite presentation of $\boldsymbol{\mathcal{M}}_k(N,\varepsilon)$ that is vastly more useful from a computational point of view.

Definition 2.21 (Manin symbols). The *Manin symbols* are the set of pairs

$$[P(X,Y),(u,v)]$$

where $P(X,Y)\in V_{k-2}$ and $0\le u,v<N$ with $\gcd(u,v,N)=1$.

Define a *right* action of $\mathrm{GL}_2(\mathbf{Q})$ on the free $\mathbf{Z}[\varepsilon]$-module M generated by the Manin symbols as follows. The element $g=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)$ acts by

$$[P,(u,v)]g = [g^{-1}P(X,Y),(u,v)g] = [P(aX+bY,cX+dY),(au+cv,bu+dv)].$$

Let $\sigma=\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)$ and $\tau=\left(\begin{smallmatrix}0&-1\\1&-1\end{smallmatrix}\right)$. Let $\boldsymbol{\mathcal{M}}_k(N,\varepsilon)'$ be the largest torsion-free quotient of M by the relations

$$\begin{aligned} x+x\sigma&=0,\\ x+x\tau+x\tau^2&=0,\\ \varepsilon(\lambda)[P,(u,v)]-[P,(\lambda u,\lambda v)]&=0.\end{aligned}$$

Theorem 2.22. *There is a natural isomorphism $\varphi:\boldsymbol{\mathcal{M}}_k(N,\varepsilon)'\longrightarrow\boldsymbol{\mathcal{M}}_k(N,\varepsilon)$ given by*

$$[X^iY^{2-k-i},(u,v)]\mapsto g(X^iY^{k-2-i}\{0,\infty\})$$

where $g=\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\mathrm{SL}_2(\mathbf{Z})$ is any matrix such that $(u,v)\equiv(c,d) \pmod N$.

Proof. In [45, §1.2, §1.7] it is proved that $\varphi\otimes_{\mathbf{Z}[\varepsilon]}\mathbf{C}$ is an isomorphism, so φ is injective and well defined. The discussion in Section 2.6.1 below ("Manin's trick") shows that every element in $\boldsymbol{\mathcal{M}}_k(N,\varepsilon)$ is a $\mathbf{Z}[\varepsilon]$-linear combination of elements in the image, so φ is surjective as well. □

2.6.1 Conversion between modular and Manin symbols

For some purposes it is better to work with modular symbols, and for others it is better to work with Manin symbols. For example, there are descriptions of the Atkin-Lehner involution in terms of both Manin and modular symbols; it appears more efficient to compute this involution using modular symbols. On the other hand, practically Hecke operators can be computed more efficiently using Manin symbols. It is thus essential to be able to convert between these two representations. The conversion from Manin to modular symbols is straightforward, and follows immediately from Theorem 2.22. The conversion back is accomplished using the method used to prove Theorem 2.22; it is known as "Manin's trick", and involves continued fractions.

Given a Manin symbol $[X^iY^{k-2-i},(u,v)]$, we write down a corresponding modular symbol as follows. Choose $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$ such that $(c,d) \equiv (u,v) \pmod{N}$. This is possible by Lemma 1.38 of [62, pg. 20]; in practice, finding $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is not completely trivial, but can be accomplished using the extended Euclidean algorithm. Then

$$\begin{aligned}
[X^iY^{k-2-i},(u,v)] \quad \longleftrightarrow \quad & \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)(X^iY^{k-2-i}\{0,\infty\}) \\
&= (dX-bY)^i(-cX+aY)^{2-k-i}\left\{\frac{b}{d},\frac{a}{c}\right\}.
\end{aligned}$$

In the other direction, suppose that we are given a modular symbol $P(X,Y)\{\alpha,\beta\}$ and wish to represent it as a sum of Manin symbols. Because

$$P\{a/b,c/d\} = P\{a/b,0\} + P\{0,c/d\},$$

it suffices to write $P\{0,a/b\}$ in terms of Manin symbols. Let

$$0 = \frac{p_{-2}}{q_{-2}} = \frac{0}{1},\ \frac{p_{-1}}{q_{-1}} = \frac{1}{0},\ \frac{p_0}{1} = \frac{p_0}{q_0},\ \frac{p_1}{q_1},\ \frac{p_2}{q_2},\ \ldots,\ \frac{p_r}{q_r} = \frac{a}{b}$$

denote the continued fraction convergents of the rational number a/b. Then

$$p_jq_{j-1} - p_{j-1}q_j = (-1)^{j-1} \qquad \text{for } -1 \le j \le r.$$

If we let $g_j = \begin{pmatrix} (-1)^{j-1}p_j & p_{j-1} \\ (-1)^{j-1}q_j & q_{j-1} \end{pmatrix}$, then $g_j \in \mathrm{SL}_2(\mathbf{Z})$ and

$$\begin{aligned}
P(X,Y)\{0,a/b\} &= P(X,Y)\sum_{j=-1}^{r}\left\{\frac{p_{j-1}}{q_{j-1}},\frac{p_j}{q_j}\right\} \\
&= \sum_{j=-1}^{r} g_j((g_j^{-1}P(X,Y))\{0,\infty\}) \\
&= \sum_{j=-1}^{r} [g_j^{-1}P(X,Y),((-1)^{j-1}q_j,q_{j-1})].
\end{aligned}$$

Note that in the jth summand, $g_j^{-1}P(X,Y)$, replaces $P(X,Y)$. Since $g_j \in \mathrm{SL}_2(\mathbf{Z})$ and $P(X,Y)$ has integer coefficients, the polynomial $g_j^{-1}P(X,Y)$ also has integer coefficients, so no denominators are introduced.

The continued fraction expansion $[c_1, c_2, \ldots, c_n]$ of the rational number a/b can be computed using the Euclidean algorithm. The first term, c_1, is the "quotient": $a = bc_1 + r$, with $0 \leq r < b$. Let $a' = b$, $b' = r$ and compute c_2 as $a' = b'c_2 + r'$, etc., terminating when the remainder is 0. For example, the expansion of $5/13$ is $[0, 2, 1, 1, 2]$. The numbers

$$d_i = c_1 + \cfrac{1}{c_2 + \frac{1}{c_3 + \cdots}}$$

will then be the (finite) convergents. For example if $a/b = 5/13$, then the convergents are

$$0/1,\ 1/0,\ d_1 = 0,\ d_2 = \frac{1}{2},\ d_3 = \frac{1}{3},\ d_4 = \frac{2}{5},\ d_5 = \frac{5}{13}.$$

2.6.2 Hecke operators on Manin symbols

Thoerem 2 of [45] gives a description of the Hecke operators T_n directly on the space of Manin symbols. This avoids the expense of first converting a Manin symbol to a modular symbol, computing T_n on the modular symbol, and then converting back. For the reader's convenience, we very briefly recall Merel's theorem here, along with an enhancement due to Cremona.

As in [16, §2.4], define R_p as follows. When $p = 2$,

$$R_2 := \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix} \right\}.$$

When p is odd, R_p is the set of 2×2 integer matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ with determinant p, and either

1. $a > |b| > 0$, $d > |c| > 0$, and $bc < 0$; or
2. $b = 0$, and $|c| < d/2$; or
3. $c = 0$, and $|b| < a/2$.

Proposition 2.23. *For* $[P(X,Y),(u,v)] \in \boldsymbol{\mathcal{M}}_k(N,\varepsilon)$ *and* p *a prime, we have*

$$\begin{aligned} T_p([P(X,Y),(u,v)]) &= \sum_{g \in R_p} [P(X,Y),(u,v)].g \\ &= \sum_{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in R_p} [P(aX+bY, cX+dY), (au+cv, bu+dv)], \end{aligned}$$

where the sum is restricted to matrices $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ *such that* $\gcd(au+cv, bu+dv, N) = 1$.

Proof. For the case $k = 2$ and an algorithm to compute R_p, see [16, §2.4]. The general case follows from [45, Theorem 2] applied to the set $\boldsymbol{\mathcal{S}}$ of [45, §3] by observing that when p is an odd *prime* $\boldsymbol{\mathcal{S}}'_p$ is empty. $\square$

2.6.3 The cuspidal and boundary spaces in terms of Manin symbols

This section is a review of Merel's explicit description of the boundary map in terms of Manin symbols for $\Gamma = \Gamma_1(N)$ (see [45, §1.4]). In the next section, we describe a very efficient way to compute the boundary map.

Let $\mathcal{R}$ be the equivalence relation on $\Gamma\backslash\mathbf{Q}^2$ which identifies the element $[\Gamma\left(\begin{smallmatrix}\lambda u\\ \lambda v\end{smallmatrix}\right)]$ with $\mathrm{sign}(\lambda)^k[\Gamma\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)]$, for any $\lambda \in \mathbf{Q}^*$. Denote by $B_k(\Gamma)$ the finite dimensional $\mathbf{Q}$-vector space with basis the equivalence classes $(\Gamma\backslash\mathbf{Q}^2)/\mathcal{R}$. The dimension of this space is $\#(\Gamma\backslash\mathbf{P}^1(\mathbf{Q}))$.

Proposition 2.24. *The map*

$$\mu : \boldsymbol{\mathcal{B}}_k(\Gamma) \to B_k(\Gamma), \qquad P\left\{\frac{u}{v}\right\} \mapsto P(u,v)\left[\Gamma\begin{pmatrix}u\\ v\end{pmatrix}\right]$$

is well defined and injective. Here u and v are assumed coprime.

Thus the kernel of $\delta : \boldsymbol{\mathcal{S}}_k(\Gamma) \to \boldsymbol{\mathcal{B}}_k(\Gamma)$ is the same as the kernel of $\mu \circ \delta$.

Proposition 2.25. *Let $P \in V_{k-2}$ and $g = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$. We have*

$$\mu \circ \delta([P,(c,d)]) = P(1,0)[\Gamma\left(\begin{smallmatrix}a\\ c\end{smallmatrix}\right)] - P(0,1)[\Gamma\left(\begin{smallmatrix}b\\ d\end{smallmatrix}\right)].$$

2.6.4 Computing the boundary map

In this section we describe how to compute the map $\delta : \boldsymbol{\mathcal{M}}_k(N,\varepsilon) \to B_k(N,\varepsilon)$ given in the previous section. The algorithm presented here generalizes the one in [16, §2.2]. To compute the image of $[P,(c,d)]$, with $g = \left(\begin{smallmatrix}a & b\\ c & d\end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z})$, we must compute the class of $[\left(\begin{smallmatrix}a\\ c\end{smallmatrix}\right)]$ and of $[\left(\begin{smallmatrix}b\\ d\end{smallmatrix}\right)]$. Instead of finding a canonical form for cusps, we use a quick test for equivalence modulo scalars. In the following algorithm, by the ith standard cusp we mean the ith basis vector for a basis of $B_k(N,\varepsilon)$. The basis is constructed as the algorithm is called successively. We first give the algorithm, then prove the facts used by the algorithm in testing equivalence.

Algorithm 2.26. Given a cusp $[\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)]$ this algorithm computes an integer i and a scalar α such that $[\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)]$ is equivalent to α times the ith standard cusp. First, using Proposition 2.27 and Algorithm 2.28, check whether or not $[\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)]$ is equivalent, modulo scalars, to any cusp found so far. If so, return the index of the representative and the scalar. If not, record $\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)$ in the representative list. Then, using Proposition 2.30, check whether or not $\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)$ is forced to equal zero by the relations. If it does not equal zero, return its position in the list and the scalar 1. If it equals zero, return the scalar 0 and the position 1; keep $\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)$ in the list, and record that it is zero.

In the case considered in Cremona's book [16], the relations between cusps involve only the trivial character, so they do not force any cusp classes to vanish. Cremona gives the following two criteria for equivalence.

Proposition 2.27 (Cremona). *Let $\left(\begin{smallmatrix}u_i\\ v_i\end{smallmatrix}\right)$, $i = 1,2$ be written so that* $\gcd(u_i,v_i) = 1$.

1. *There exists $g \in \Gamma_0(N)$ such that $g\left(\begin{smallmatrix} u_1 \\ v_1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} u_2 \\ v_2 \end{smallmatrix}\right)$ if and only if*

$$s_1 v_2 \equiv s_2 v_1 \pmod{\gcd(v_1 v_2, N)}, \quad \textit{where } s_j \textit{ satisfies } u_j s_j \equiv 1 \pmod{v_j}.$$

2. *There exists $g \in \Gamma_1(N)$ such that $g\left(\begin{smallmatrix} u_1 \\ v_1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} u_2 \\ v_2 \end{smallmatrix}\right)$ if and only if*

$$v_2 \equiv v_1 \pmod{N} \textit{ and } u_2 \equiv u_1 \pmod{\gcd(v_1, N)}.$$

Proof. The first is Proposition 2.2.3 of [16], and the second is Lemma 3.2 of [15]. □

Algorithm 2.28. Suppose $\left(\begin{smallmatrix} u_1 \\ v_1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} u_2 \\ v_2 \end{smallmatrix}\right)$ are equivalent modulo $\Gamma_0(N)$. This algorithm computes a matrix $g \in \Gamma_0(N)$ such that $g\left(\begin{smallmatrix} u_1 \\ v_1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} u_2 \\ v_2 \end{smallmatrix}\right)$. Let s_1, s_2, r_1, r_2 be solutions to $s_1 u_1 - r_1 v_1 = 1$ and $s_2 u_2 - r_2 v_2 = 1$. Find integers x_0 and y_0 such that $x_0 v_1 v_2 + y_0 N = 1$. Let $x = -x_0(s_1 v_2 - s_2 v_1)/(v_1 v_2, N)$ and $s_1' = s_1 + x v_1$. Then $g = \begin{pmatrix} u_2 & r_2 \\ v_2 & s_2 \end{pmatrix} \cdot \begin{pmatrix} u_1 & r_1 \\ v_1 & s_1' \end{pmatrix}^{-1}$ sends $\left(\begin{smallmatrix} u_1 \\ v_1 \end{smallmatrix}\right)$ to $\left(\begin{smallmatrix} u_2 \\ v_2 \end{smallmatrix}\right)$.

Proof. This follows from the proof of Proposition 2.27 in [16]. □

To see how the ε relations, for nontrivial ε, make the situation more complicated, observe that it is possible that $\varepsilon(\alpha) \neq \varepsilon(\beta)$ but

$$\varepsilon(\alpha)\left[\begin{pmatrix} u \\ v \end{pmatrix}\right] = \left[\gamma_\alpha \begin{pmatrix} u \\ v \end{pmatrix}\right] = \left[\gamma_\beta \begin{pmatrix} u \\ v \end{pmatrix}\right] = \varepsilon(\beta)\left[\begin{pmatrix} u \\ v \end{pmatrix}\right];$$

One way out of this difficulty is to construct the cusp classes for $\Gamma_1(N)$, then quotient out by the additional ε relations using Gaussian elimination. This is far too inefficient to be useful in practice because the number of $\Gamma_1(N)$ cusp classes can be unreasonably large. Instead, we give a quick test to determine whether or not a cusp vanishes modulo the ε-relations.

Lemma 2.29. *Suppose α and α' are integers such that* $\gcd(\alpha, \alpha', N) = 1$. *Then there exist integers β and β', congruent to α and α' modulo N, respectively, such that* $\gcd(\beta, \beta') = 1$.

Proof. By [62, 1.38] the map $\mathrm{SL}_2(\mathbf{Z}) \to \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ is surjective. By the Euclidean algorithm, there exist integers x, y and z such that $x\alpha + y\alpha' + zN = 1$. Consider the matrix $\left(\begin{smallmatrix} y & -x \\ \alpha & \alpha' \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbf{Z}/N\mathbf{Z})$ and take β, β' to be the bottom row of a lift of this matrix to $\mathrm{SL}_2(\mathbf{Z})$. □

Proposition 2.30. *Let N be a positive integer and ε a Dirichlet character of modulus N. Suppose $\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)$ is a cusp with u and v coprime. Then $\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)$ vanishes modulo the relations*

$$\left[\gamma\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)\right] = \varepsilon(\gamma)\left[\left(\begin{smallmatrix} u \\ v \end{smallmatrix}\right)\right], \qquad \textit{all } \gamma \in \Gamma_0(N)$$

if and only if there exists $\alpha \in (\mathbf{Z}/N\mathbf{Z})^*$, with $\varepsilon(\alpha) \neq 1$, such that

$$\begin{aligned} v &\equiv \alpha v \pmod{N}, \\ u &\equiv \alpha u \pmod{\gcd(v, N)}. \end{aligned}$$

Proof. First suppose such an α exists. By Lemma 2.29 there exists $\beta, \beta' \in \mathbf{Z}$ lifting α, α^{-1} such that $\gcd(\beta, \beta') = 1$. The cusp $\left(\begin{smallmatrix}\beta u\\ \beta' v\end{smallmatrix}\right)$ has coprime coordinates so, by Proposition 2.27 and our congruence conditions on α, the cusps $\left(\begin{smallmatrix}\beta u\\ \beta' v\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)$ are equivalent by an element of $\Gamma_1(N)$. This implies that $\left[\left(\begin{smallmatrix}\beta u\\ \beta' v\end{smallmatrix}\right)\right] = \left[\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)\right]$. Since $\left[\left(\begin{smallmatrix}\beta u\\ \beta' v\end{smallmatrix}\right)\right] = \varepsilon(\alpha)\left[\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)\right]$, our assumption that $\varepsilon(\alpha) \neq 1$ forces $\left[\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)\right] = 0$.

Conversely, suppose $\left[\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)\right] = 0$. Because all relations are two-term relations, and the $\Gamma_1(N)$-relations identify $\Gamma_1(N)$-orbits, there must exists α and β with

$$\left[\gamma_\alpha \begin{pmatrix}u\\ v\end{pmatrix}\right] = \left[\gamma_\beta \begin{pmatrix}u\\ v\end{pmatrix}\right] \qquad \text{and } \varepsilon(\alpha) \neq \varepsilon(\beta).$$

Indeed, if this did not occur, then we could mod out by the ε relations by writing each $\left[\gamma_\alpha \left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)\right]$ in terms of $\left[\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)\right]$, and there would be no further relations left to kill $\left[\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)\right]$. Next observe that

$$\left[\gamma_{\beta^{-1}\alpha} \begin{pmatrix}u\\ v\end{pmatrix}\right] = \left[\gamma_{\beta^{-1}}\gamma_\alpha \begin{pmatrix}u\\ v\end{pmatrix}\right] = \varepsilon(\beta^{-1})\left[\gamma_\alpha \begin{pmatrix}u\\ v\end{pmatrix}\right] = \varepsilon(\beta^{-1})\left[\gamma_\beta \begin{pmatrix}u\\ v\end{pmatrix}\right] = \left[\begin{pmatrix}u\\ v\end{pmatrix}\right].$$

Applying Proposition 2.27 and noting that $\varepsilon(\beta^{-1}\alpha) \neq 1$ shows that $\beta^{-1}\alpha$ satisfies the properties of the "α" in the statement of the proposition we are proving. $\square$

We enumerate the possible α appearing in Proposition 2.30 as follows. Let $g = (v, N)$ and list the $\alpha = v \cdot \frac{N}{g} \cdot a + 1$, for $a = 0, \dots, g-1$, such that $\varepsilon(\alpha) \neq 0$.

Working in the plus one or minus one quotient. Let s be a sign, either $+1$ or -1. To compute $\boldsymbol{\mathcal{S}}_k(N, \varepsilon)_s$ it is necessary to replace $B_k(N, \varepsilon)$ by its quotient modulo the additional relations $\left[\left(\begin{smallmatrix}-u\\ v\end{smallmatrix}\right)\right] = s\left[\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)\right]$ for all cusps $\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)$. Algorithm 2.26 can be modified to deal with this situation as follows. Given a cusp $x = \left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)$, proceed as in Algorithm 2.26 and check if either $\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)$ or $\left(\begin{smallmatrix}-u\\ v\end{smallmatrix}\right)$ is equivalent (modulo scalars) to any cusp seen so far. If not, use the following trick to determine whether the ε and s-relations kill the class of $\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)$: use the unmodified Algorithm 2.26 to compute the scalars α_1, α_2 and standard indices i_1, i_2 associated to $\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}-u\\ v\end{smallmatrix}\right)$, respectively. The s-relation kills the class of $\left(\begin{smallmatrix}u\\ v\end{smallmatrix}\right)$ if and only if $i_1 = i_2$ but $\alpha_1 \neq s\alpha_2$.

2.7 The complex torus attached to a modular form

Fix integers $N \geq 1$, $k \geq 2$, and let ε be a mod N Dirichlet character. For the rest of this section assume that $\varepsilon^2 = 1$.

We construct a lattice in $\mathrm{Hom}(S_k(N, \varepsilon), \mathbf{C})$ that is invariant under complex conjugation and under the action of the Hecke operators. The quotient of $\mathrm{Hom}(S_k(N, \varepsilon), \mathbf{C})$ by this lattice is a complex torus $J_k(N, \varepsilon)$, which is equipped with an action of the Hecke operators and of complex conjugation.

The reader may wish to compare our construction with a closely related construction of Shimura [60]. Shimura observes that the Petersson pairing gives his torus the structure of an abelian variety over $\mathbf{C}$. Note that his torus is, a priori, different than our torus. We do not know if our torus has the structure of abelian variety over $\mathbf{C}$.

When $k = 2$, the torus $J_2(N, \varepsilon)$ is the set of complex points of an abelian variety, which is actually defined over $\mathbf{Q}$; when $k > 2$, the study of these complex tori is of interest in trying to understand the conjectures of Bloch and Kato (see [7]) on motifs attached to modular forms.

Let $\boldsymbol{\mathcal{S}} = \boldsymbol{\mathcal{S}}_k(N, \varepsilon)$ (respectively, $S = S_k(N, \varepsilon)$) be the space of cuspidal modular symbols (respectively, cusp forms) of weight k, level N, and character ε. The Hecke algebra $\mathbf{T}$ acts in a way compatible with the integration pairing $\langle\, , \rangle : S \times \boldsymbol{\mathcal{S}} \to \mathbf{C}$. This pairing induces a $\mathbf{T}$-module homomorphism $\Phi : \boldsymbol{\mathcal{S}} \to S^* = \mathrm{Hom}_{\mathbf{C}}(S, \mathbf{C})$, called the *period mapping*. Because $\varepsilon^2 = 1$, the $*$-involution preserves S.

Proposition 2.31. *The period mapping Φ is injective and $\Phi(\boldsymbol{\mathcal{S}})$ is a lattice in S^*.*

Proof. By Theorem 2.7,
$$\boldsymbol{\mathcal{S}} \otimes_{\mathbf{R}} \mathbf{C} \cong \mathrm{Hom}_{\mathbf{C}}(S \oplus \overline{S}, \mathbf{C}).$$
Because $\varepsilon^2 = 1$, we have $S = S_k(N, \varepsilon; \mathbf{R}) \otimes_{\mathbf{R}} \mathbf{C}$. Set $S_{\mathbf{R}} := S_k(N, \varepsilon; \mathbf{R})$ and likewise define $\overline{S}_{\mathbf{R}}$. We have
$$\mathrm{Hom}_{\mathbf{C}}(S \oplus \overline{S}, \mathbf{C}) = \mathrm{Hom}_{\mathbf{R}}(S_{\mathbf{R}} \oplus \overline{S}_{\mathbf{R}}, \mathbf{R}) \otimes_{\mathbf{R}} \mathbf{C}.$$
Let $\boldsymbol{\mathcal{S}}_{\mathbf{R}} = \boldsymbol{\mathcal{S}}_k(N, \varepsilon; \mathbf{R})$ and $\boldsymbol{\mathcal{S}}_{\mathbf{R}}^+$ be the subspace fixed under $*$. By Proposition 2.11 we have maps
$$\boldsymbol{\mathcal{S}}_{\mathbf{R}}^+ \to \mathrm{Hom}_{\mathbf{R}}(S_{\mathbf{R}} \oplus \overline{S}_{\mathbf{R}}, \mathbf{R}) \to \mathrm{Hom}_{\mathbf{R}}(S_{\mathbf{R}}, \mathbf{R})$$
and
$$\boldsymbol{\mathcal{S}}_{\mathbf{R}}^- \to \mathrm{Hom}_{\mathbf{R}}(S_{\mathbf{R}} \oplus \overline{S}_{\mathbf{R}}, i\mathbf{R}) \to \mathrm{Hom}_{\mathbf{R}}(S_{\mathbf{R}}, i\mathbf{R}).$$
The map $\boldsymbol{\mathcal{S}}_{\mathbf{R}}^+ \to \mathrm{Hom}_{\mathbf{R}}(S_{\mathbf{R}}, \mathbf{R})$ is an isomorphism: the point is that if $\langle \bullet, x\rangle$, for $x \in \boldsymbol{\mathcal{S}}_{\mathbf{R}}^+$, vanishes on $S_{\mathbf{R}}$ then it vanishes on the whole of $S \oplus \overline{S}$. Likewise, the map $\boldsymbol{\mathcal{S}}_{\mathbf{R}}^- \to \mathrm{Hom}_{\mathbf{R}}(S_{\mathbf{R}}, i\mathbf{R})$ is an isomorphism. Thus
$$\boldsymbol{\mathcal{S}} \otimes \mathbf{R} = \boldsymbol{\mathcal{S}}_{\mathbf{R}} \cong \mathrm{Hom}_{\mathbf{R}}(S_{\mathbf{R}}, \mathbf{R}) \oplus \mathrm{Hom}_{\mathbf{R}}(S_{\mathbf{R}}, i\mathbf{R}) \cong \mathrm{Hom}_{\mathbf{C}}(S, \mathbf{C}).$$
Finally, we observe that $\boldsymbol{\mathcal{S}}$ is by definition torsion free, which completes the proof. □

The torus $J_k(N, \varepsilon)$ fits into an exact sequence
$$0 \longrightarrow \boldsymbol{\mathcal{S}} \xrightarrow{\ \Phi\ } \mathrm{Hom}_{\mathbf{C}}(S, \mathbf{C}) \longrightarrow J_k(N, \varepsilon) \longrightarrow 0.$$
Let $f \in S$ be a newform and S_f the complex vector space spanned by the Galois conjugates of f. The period map Φ_f associated to f is the map $\boldsymbol{\mathcal{S}} \to \mathrm{Hom}_{\mathbf{C}}(S_f, \mathbf{C})$ obtained by composing Φ with restriction to S_f. Set
$$A_f := \mathrm{Hom}_{\mathbf{C}}(S_f, \mathbf{C})/\Phi_f(\boldsymbol{\mathcal{S}}).$$

We associate to f a subtorus of J as follows. Let $I_f = \mathrm{Ann}_{\mathbf{T}}(f)$ be the annihilator of f in the Hecke algebra, and set
$$A_f^\vee := \mathrm{Hom}_{\mathbf{C}}(S, \mathbf{C})[I_f]/\Phi(\boldsymbol{\mathcal{S}}[I_f])$$

where $\mathrm{Hom}_{\mathbf{C}}(S, \mathbf{C})[I_f] = \cap_{t \in I_f} \ker(t)$.

The following diagram summarizes the tori just defined; its columns are exact but its rows need not be.

$$\begin{array}{ccccc} 0 & & 0 & & 0 \\ \downarrow & & \downarrow & & \downarrow \\ \boldsymbol{\mathcal{S}}[I_f] & \longrightarrow & \boldsymbol{\mathcal{S}} & \longrightarrow & \Phi_f(\boldsymbol{\mathcal{S}}) \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Hom}_{\mathbf{C}}(S, \mathbf{C})[I_f] & \longrightarrow & \mathrm{Hom}_{\mathbf{C}}(S, \mathbf{C}) & \longrightarrow & \mathrm{Hom}_{\mathbf{C}}(S[I_f], \mathbf{C}) \\ \downarrow & & \downarrow & & \downarrow \\ A_f^{\vee} & \longrightarrow & J_k(N, \varepsilon) & \longrightarrow & A_f \\ \downarrow & & \downarrow & & \downarrow \\ 0 & & 0 & & 0 \end{array} \tag{2.1}$$

2.7.1 The case when the weight is 2

When $k = 2$ and $\varepsilon = 1$ the above is just Shimura's classical association of an abelian variety to a modular form; see [62, Thm. 7.14] and [61]. In this case A_f and $A_f^{\vee}$ are abelian varieties that are defined over $\mathbf{Q}$. Furthermore A_f is an *optimal quotient* of J, in the sense that the kernel of the map $J \to A_f$ is connected. For a summary of the main results in this situation, see Section 4.6.

Chapter 3

Applications of modular symbols

In the previous chapter we introduced several spaces of modular symbols, and observations such as "Manin's trick" suggested that we could compute with them. The duality between modular symbols and modular forms hints that modular symbols might be useful in computing information about modular forms. In the present chapter, we gather together the fruits of our investigation into this connection.

Sections 3.1–3.5 of this chapter give a method to compute the irreducible components of the spaces $\boldsymbol{\mathcal{M}}_k(N,\varepsilon)$ of modular symbols. In Section 3.6 we observe that computing intersections of certain abelian varieties can be reduced to linear algebra over $\mathbf{Z}$ by viewing the abelian varieties as complex tori and considering the appropriate diagrams. In Sections 3.7, we continue this trend by pointing out that many invariants of the complex torus attached to a modular form can be computed without computing any approximate period lattices. In Section 3.8, we discuss well-known methods for computing both an upper and lower bound on the order of the torsion subgroup of certain abelian varieties. Section 3.9 presents an algorithm for computing the modular degree of the complex torus associated to a newform.

In Section 3.10 we aim squarely at the problem of gathering data related to the Birch and Swinnerton-Dyer conjecture and its generalizations, where we give a formula for the rational numbers $|L(A_f,j)/\Omega_j|$ attached to a newform. In Section 3.11 we compare the ratio computed in the previous section to the one considered in the Birch and Swinnerton-Dyer conjecture; the two numbers differ by a Manin constant, which we bound. Finally, in Section 3.12 we give algorithms for approximating the period lattice and related numerical quantities associated to a newform of arbitrary weight.

3.1 Computing the space of modular symbols

Definition 3.1. Let W be a subspace of a finite-dimensional vector space V. To *compute* the quotient V/W means to give a matrix representing the projection $V \to V/W$, with respect to some basis for V and some basis B for V/W, along with a lift to V of each element of B.

In other words, to compute V/W means to create a reduction function that assigns to each element of V its canonical representative on the "free basis" B.

Let N be a positive integer, fix a mod N Dirichlet character ε, let $K := \mathbf{Q}[\varepsilon]$ be the smallest extension containing the values of ε, and let $\mathcal{O} := \mathbf{Z}[\varepsilon]$.

Algorithm 3.2. Given a positive integer N, a Dirichlet character ε, and an integer $k \geq 2$ this algorithm computes $\boldsymbol{\mathcal{M}}_k(N, \varepsilon; K)$. We compute the quotient presentation given in Theorem 2.22 in three steps.

1. Let V_1 be the finite-dimensional K-vector space generated by the Manin symbols $[X^iY^{k-2-i}, (u,v)]$ for $i = 0, \dots, k-2$ and $0 \leq u, v < N$ with $\gcd(u,v,N) = 1$. Let W_1 be the subspace of V_1 generated by all differences
$$[X^iY^{k-2-i}, (\lambda u, \lambda v)] - \varepsilon(\lambda)[X^iY^{k-2-i}, (u,v)].$$
Because all relations are two-term, it is easy to compute $V_2 := V_1/W_1$. In computing this quotient, we do not have to explicitly compute the *large* matrix representing the linear map $V_1 \to V_2$, as it can be replaced by a suitable "reduction procedure" involving arithmetic in $\mathbf{Z}/N\mathbf{Z}$.

2. Let σ act on the set of Manin symbols as in Section 2.6; thus
$$[X^iY^{k-2-i}, (u,v)]\sigma = (-1)^i[Y^iX^{k-2-i}, (v,-u)].$$
Let W_2 be the subspace of V_2 generated by the sums $x + x\sigma$ for $x \in V_2$. Because all relations are two-term relations, it is easy to compute $V_3 := V_2/W_2$.

3. Let τ act on Manin symbols as in Section 2.6; thus
$$[X^iY^{k-2-i}, (u,v)]\tau = [(-Y)^i(X-Y)^{k-2-i}, (v, -u-v)].$$
Note that the symbol on the right can be written as a sum of generating Manin symbols. Let W_3 be the subspace of V_3 generated by the sums $x + x\tau + x\tau^2$ where x varies over the images of a basis of V_2 (*not* just a basis for V_3!). Using some form of Gaussian elimination, we compute V_3/W_3. Finally, $\boldsymbol{\mathcal{M}}_k(N, \varepsilon; K) \approx V_3/W_3$.

Proof. For $\lambda \in (\mathbf{Z}/N\mathbf{Z})^*$, denote by $\langle\lambda\rangle$ the right action of λ on Manin symbols; thus
$$[X^iY^{k-2-i}, (u,v)]\langle\lambda\rangle = [X^iY^{k-2-i}, (\lambda u, \lambda v)].$$
By Theorem 2.22 the space $\boldsymbol{\mathcal{M}}_k(N, \varepsilon; K)$ is isomorphic to the quotient of the vector spaces V_1 of Step 1 modulo the relations $x + x\sigma = 0$, $x + x\tau + x\tau^2 = 0$, and $x\langle\lambda\rangle = \lambda x$ as x varies over all Manin symbols and λ varies over $(\mathbf{Z}/N\mathbf{Z})^*$.

As motivation, we note that a naive computation of V_1 modulo the σ, τ, and $\langle\lambda\rangle$ relations using Gaussian elimination is far too inefficient. This is why we compute the quotient in three steps. The complexity of Steps 1 and Steps 2 are negligible. The difficulty occurs in Step 3; at least the relations of this step occur in a space of dimension much smaller than that of V_1.

To see that the algorithm is correct, it is necessary only to observe that σ and τ both commute with all diamond-bracket operators $\langle\lambda\rangle$; this is an immediate consequence of the above formulas. We remark that in Step 3 it is in general *necessary* to compute the quotient by all relations $x + x\tau + x\tau^2$ with x the image of a basis vector for V_2 instead of just x in V_3 because σ and τ do not commute. $\square$

Remark 3.3. In implementing the above algorithm, one should take special care in Steps 1 and 2 because the relations can together force certain of the Manin symbols to equal 0. For example, there might be relations of the form $x_1 + x_2 = 0$ and $x_1 - x_2 = 0$ which together force $x_1 = x_2 = 0$.

Remark 3.4. To compute the plus-one quotient $\boldsymbol{\mathcal{M}}_k(N, \varepsilon; K)_+$, it is necessary to modify Step 2 of Algorithm 3.2 by including in W_2 the differences $x - xI$ where $I = \left(\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, and

$$[X^i Y^{k-2-i}, (u, v)]I = (-1)^i [X^i Y^{k-2-i}, (-u, v)].$$

Likewise, to compute the minus-one quotient we include the sums $x + xI$. Note, as in the remarks in the proof of Algorithm 3.2, we can not add in the I relations in Step 1 because I and σ do not commute.

Algorithm 3.5. Given a positive integer N, a Dirichlet character ε, and an integer $k \geq 2$, this algorithm computes the $\mathcal{O}$-modules $\boldsymbol{\mathcal{M}}_k(N, \varepsilon)$ and $\boldsymbol{\mathcal{S}}_k(N, \varepsilon)$. (We assume as given algorithms for performing standard operations on $\mathcal{O}$-modules.)

1. Using Algorithm 3.2 compute the K-vector space $V := \boldsymbol{\mathcal{M}}_k(N, \varepsilon; K)$.
2. Compute the $\mathcal{O}$-lattice L in V generated by the classes of the finitely many symbols $[X^i Y^{k-2-i}, (u, v)]$ for $i = 0, \ldots, k-2$ and $0 \leq u, v < N$ with $\gcd(u, v, N) = 1$. It is only necessary to take one symbol in each ε-equivalence class, so there are $(k - 2 + 1) \cdot \#\mathbf{P}^1(\mathbf{Z}/N\mathbf{Z})$ generating symbols. This computes $\boldsymbol{\mathcal{M}}_k(N, \varepsilon)$.
3. To compute the submodule $\boldsymbol{\mathcal{S}}_k(N, \varepsilon)$ of L, we use the algorithm of Section 2.6.4 to compute the boundary map $\delta : \boldsymbol{\mathcal{M}}_k(N, \varepsilon; K) \to B_k(N, \varepsilon; K)$. Then $\boldsymbol{\mathcal{S}}_k(N, \varepsilon)$ is the kernel of δ restricted to the lattice L.

As a check, using the formulas of Section 3.4, we compute the dimension of the space $S_k(N, \varepsilon)$ of cusp forms and compare with the dimension of $\boldsymbol{\mathcal{S}}_k(N, \varepsilon; K)$ computed in Algorithm 3.5. The latter dimension must equal twice the former one.

3.2 Computing the Hecke algebra

In this section we give an upper bound on the number of Hecke operators needed to generate the Hecke algebra as a $\mathbf{Z}$-module. The bound on Hecke operators is an application of [66], which was described to the author by Ribet and Agashe when $k = 2$ and the level is prime. There are much better bounds on the number of Hecke operators needed to generate the Hecke algebra as a *ring*, but we do not investigate them here.

Let Γ be a subgroup of $\mathrm{SL}_2(\mathbf{Z})$ that contains $\Gamma_1(N)$ for some N. Let $S_k(\Gamma; \mathbf{C})$ be the space of weight-k cuspforms for Γ, and let $\mathbf{T} \subset \mathrm{End}(S_k(\Gamma; \mathbf{C}))$ be the corresponding Hecke algebra. We now give a bound r such that the Hecke operators T_n, with $n \leq r$, generate $\mathbf{T}$ as a $\mathbf{Z}$-module.

For any ring $R \subset \mathbf{C}$, let $S_k(\Gamma; R)$ denotes the space of cuspforms for Γ with Fourier coefficients in R. Since $S_k(\Gamma; \mathbf{C}) = S_k(\Gamma; \mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{C}$, it makes sense to define

$$S_k(\Gamma; R) := S_k(\Gamma; \mathbf{Z}) \otimes_{\mathbf{Z}} R$$

for *any* ring R. The following proposition is well known.

Proposition 3.6. *For any ring R, the pairing*

$$\mathbf{T}_R \otimes_R S_k(N;R) \to R$$

that sends (T,f) to $a_1(Tf)$ is a perfect pairing, where $\mathbf{T}_R = \mathbf{T} \otimes_{\mathbf{Z}} R$. Furthermore, we have $(T_n, f) = a_n(f)$, where T_n is the nth Hecke operator.

Let

$$\mu = [\mathrm{SL}_2(\mathbf{Z}) : \Gamma],$$

and denote by $\lceil x \rceil$ the smallest integer $\geq x$.

Theorem 3.7 (Sturm). *Let λ be a prime ideal in the ring $\mathcal{O}$ of integers in some number field. If $f \in S_k(\Gamma;\mathcal{O})$ satisfies $a_n(f) \equiv 0 \pmod{\lambda}$ for $n \leq \lceil \frac{k}{12}\mu \rceil$, then $f \equiv 0 \pmod{\lambda}$.*

Proof. Theorem 1 of [66]. $\square$

Proposition 3.8. *If $f \in S_k(\Gamma)$ satisfies $a_n(f) = 0$ for $n \leq r = \lceil \frac{k}{12}\mu \rceil$, then $f = 0$.*

Proof. We must show that the composite map $S_k(\Gamma) \hookrightarrow \mathbf{C}[[q]] \to \mathbf{C}[[q]]/(q^{r+1})$ is injective. Because $\mathbf{C}$ is a flat $\mathbf{Z}$-module and $S_k(\Gamma;\mathbf{Z}) \otimes \mathbf{C} = S_k(\Gamma)$, it suffices to show that the map $F : S_k(\Gamma;\mathbf{Z}) \to \mathbf{Z}[[q]]/(q^{r+1})$ is injective. Suppose $F(f) = 0$, and let p be a prime number. Then $a_n(f) = 0$ for $n \leq r$, hence plainly $a_n(f) \equiv 0 \pmod{p}$ for any such n. Theorem 3.7 implies that $f \equiv 0 \pmod{p}$. Duplicating this argument shows that the coefficients of f are divisible by all primes p, so they are 0. $\square$

Theorem 3.9. *As a $\mathbf{Z}$-module, $\mathbf{T}$ is generated by $T_1, \ldots, T_r$, where $r = \lceil \frac{k}{12}\mu \rceil$.*

Proof. Let Z be the submodule of $\mathbf{T}$ generated by $T_1, T_2, \ldots, T_r$. Consider the exact sequence of additive abelian groups $0 \to Z \xrightarrow{i} \mathbf{T} \to \mathbf{T}/Z \to 0$. Let p be a prime and tensor this sequence with $\mathbf{F}_p$ to obtain the exact sequence

$$Z \otimes \mathbf{F}_p \xrightarrow{\bar{i}} \mathbf{T} \otimes \mathbf{F}_p \to (\mathbf{T}/Z) \otimes \mathbf{F}_p \to 0.$$

Put $R = \mathbf{F}_p$ in Proposition 3.6, and suppose that $f \in S_k(N, \mathbf{F}_p)$ pairs to 0 with each of $T_1, \ldots, T_r$. Then by Proposition 3.6, $a_m(f) = a_1(T_m f) = 0$ in $\mathbf{F}_p$ for each m, $1 \leq m \leq r$. Theorem 3.7 then asserts that $f = 0$. Thus the pairing, when restricted to the image of $Z \otimes \mathbf{F}_p$ in $\mathbf{T} \otimes \mathbf{F}_p$, is also perfect. Thus $\dim_{\mathbf{F}_p} \bar{i}(Z \otimes \mathbf{F}_p) = \dim_{\mathbf{F}_p} S_k(N, \mathbf{F}_p) = \dim_{\mathbf{F}_p} \mathbf{T} \otimes \mathbf{F}_p$, so $(\mathbf{T}/Z) \otimes \mathbf{F}_p = 0$; repeating this argument for all p shows that $\mathbf{T}/Z = 0$. $\square$

3.3 Representing and enumerating Dirichlet characters

Recall that a *Dirichlet character* is a homomorphism $\varepsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$.

The following lemma is well known.

Lemma 3.10. *If p is an odd prime, then $(\mathbf{Z}/p^n\mathbf{Z})^*$ is a cyclic group. The group $(\mathbf{Z}/2^n\mathbf{Z})^*$ is generated by -1 and 5.*

We use the following representation of Dirichlet characters. Factor N as a product of prime powers: $N = \prod_{i=1}^{r} p_i^{e_i}$ with $p_i < p_{i+1}$ and each $e_i > 0$; then $(\mathbf{Z}/N\mathbf{Z})^* \cong \prod_{i=1}^{r}(\mathbf{Z}/p_i^{e_i}\mathbf{Z})^*$. If p_i is odd then the lemma implies that $(\mathbf{Z}/p_i^{e_i}\mathbf{Z})^*$ is cyclic. If $p_1 = 2$, then $(\mathbf{Z}/p_1^{e_1}\mathbf{Z})^*$ is a product $\langle -1\rangle \times \langle 5\rangle$ of two cyclic groups, both possibly trivial. For each i, we let $a_i \in (\mathbf{Z}/p_i^{e_i}\mathbf{Z})^*$ be the smallest generator of the ith factor $(\mathbf{Z}/p_i^{e_i}\mathbf{Z})^*$. If $p_1 = 2$, let a_1 and a_2 correspond to the two factors $\langle -1\rangle$ and $\langle 5\rangle$, respectively; then a_3 corresponds to p_2, etc. Here a_i is smallest in the sense that the minimal lift $\tilde{a}_i \in \mathbf{Z}_{>0}$ is smallest. Let n be the exponent of $(\mathbf{Z}/N\mathbf{Z})^*$, and let $\zeta = e^{2\pi i/n} \in \mathbf{C}^*$. To give ε is the same as giving the images of each generator of a_i as a power of ζ. We thus represent ε as a vector of elements of $\mathbf{C}^*$ with respect to a canonically chosen, but unnatural, basis.

Alternatively, the vector representing a character ε can be equivalently viewed as a vector in $(\mathbf{Z}/n\mathbf{Z})^r$, where again n is the exponent of $(\mathbf{Z}/N\mathbf{Z})^*$. Such a vector represents a character if and only if the ith component of the vector has additive order dividing $\varphi(p_i^{e_i})$. If $p_1 = 2$, then there are $r+1$ entries instead of r entries, and the condition is suitably modified. If a vector $v = [d_1, \ldots, d_r]$ represents a character ε, then each of the Galois conjugate characters is represented by $[md_1, \ldots, md_r]$ where m varies over elements of $(\mathbf{Z}/n\mathbf{Z})^*$.

When performing actual machine computations, we work in the smallest field that contains all of the values of ε. Thus if $d = \gcd(d_1, \ldots, d_r, n)$, then we work in the subfield $\mathbf{Q}(\zeta^d)$, which is cheaper than working in $\mathbf{Q}(\zeta)$.

It is sometimes important to work in characteristic ℓ. Then the notation is as above, except ζ is replaced by a primitive mth root of unity, where m is the prime-to-ℓ part of n. Note that the primitive nth roots of unity in characteristic ℓ need not be conjugate; for example, both 2 and 3 are square roots of -1 in $\mathbf{F}_5$, but they are not conjugate. Thus we must specify ζ as part of the notation when giving a mod ℓ Dirichlet character.

Example 3.11. Suppose $N = p$ is an odd prime. The group of mod p Dirichlet characters (in characteristic 0) is isomorphic to $\mathbf{Z}/(p-1)\mathbf{Z}$, and two characters a and b are Galois conjugate if and only if there is an element $x \in (\mathbf{Z}/(p-1)\mathbf{Z})^*$ such that $xa = b$. A character is determined up to Galois conjugacy by its order, so the set of classes of mod p Dirichlet characters are in bijection with the set of divisors d of $p - 1 = \#(\mathbf{Z}/p\mathbf{Z})^*$.

Let p be an odd prime. The quadratic mod p character is denoted $[(p-1)/2]$. The quadratic mod $2p$ character is denoted by $[0, 0, (p-1)/2]$; the quadratic mod $4p$ character is denoted $[(p-1)/2, 0, (p-1)/2]$. If $n \geq 3$, then the exponent of $(\mathbf{Z}/2^n\mathbf{Z})^*$ is 2^{n-2}, so the nontrivial mod 2^n character that factors through $(\mathbf{Z}/4\mathbf{Z})^*$ is denoted $[2^{n-3}, 0]$.

Definition 3.12. The *conductor* of a character $\varepsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$ is the smallest divisor M of N such that ε factors through the natural reduction map $(\mathbf{Z}/N\mathbf{Z})^* \to (\mathbf{Z}/M\mathbf{Z})^*$.

For simplicity, we assume that N is odd. To compute the conductor of ε, let v be the vector in $(\mathbf{Z}/n\mathbf{Z})^r$ that represents ε, as above. Since both $(\mathbf{Z}/p_i^{e_i}\mathbf{Z})^*$ and $(\mathbf{Z}/p_i^{d}\mathbf{Z})^*$ are cyclic and the reduction map is surjective, we find that p_i^d, with $d \leq e_i$, divides the conductor of ε if and only if the ith component of v has additive order dividing $\varphi(p_i^d)$. We can thus compute the power of p_i dividing the conductor of ε by computing the smallest d such that $p_i^d \equiv p_i^{d-1}$ modulo the order of the ith component of v.

3.4 The dimension of $S_k(N, \varepsilon)$

An explicit formula for the dimension of $S_k(N, \varepsilon)$ is given in [13], without proof. For the reader's convenience, we reproduce it here.

Theorem 3.13 (Cohen-Oesterlé). *Let $k \geq 2$ be an integer and $\varepsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$ be a Dirichlet character such that $\varepsilon(-1) = (-1)^k$. Then*

$$\begin{aligned}\dim S_k(N,\varepsilon) = \delta + \frac{k-1}{12} \cdot N \cdot \prod_{p \mid N} \left(1 + \frac{1}{p}\right) \quad &- \quad \frac{1}{2} \cdot \prod_{p \mid N} \lambda(r_p, s_p, p) \\ + \gamma_k \sum_{\{x \in (\mathbf{Z}/N\mathbf{Z})^* \,:\, x^2+1=0\}} \varepsilon(x) \quad &+ \quad \mu_k \sum_{\{x \in (\mathbf{Z}/N\mathbf{Z})^* \,:\, x^2+x+1=0\}} \varepsilon(x).\end{aligned}$$

Let f be the conductor of ε, i.e., the smallest M such that ε factors through $(\mathbf{Z}/M\mathbf{Z})^*$. If $p \mid N$, then r_p (resp. s_p) denotes the exponent of p in the prime factorization of N (resp. f). Furthermore,

$$\lambda(r_p, s_p, p) := \begin{cases} p^{r'} + p^{r'-1} & \text{if } 2s_p \leq r_p = 2r' \\ 2p^{r'} & \text{if } 2s_p \leq r_p = 2r' + 1 \\ 2p^{r_p - s_p} & \text{if } 2s_p > r_p \end{cases}$$

$$\gamma_k := \begin{cases} 0 & \text{if } k \text{ is odd} \\ -\frac{1}{4} & \text{if } k \equiv 2 \pmod 4 \\ \frac{1}{4} & \text{if } k \equiv 0 \pmod 4 \end{cases}$$

$$\mu_k := \begin{cases} 0 & \text{if } k \equiv 1 \pmod 3 \\ -\frac{1}{3} & \text{if } k \equiv 2 \pmod 3 \\ \frac{1}{3} & \text{if } k \equiv 0 \pmod 3 \end{cases}$$

$$\delta := \begin{cases} 1 & \text{if } k = 2 \text{ and } \varepsilon \text{ is trivial} \\ 0 & \text{otherwise} \end{cases}$$

3.5 Decomposing the space of modular symbols

Consider the space $\boldsymbol{\mathcal{S}}_k(N, \varepsilon)$ of cuspidal modular symbols of level N and character ε over $K = \mathbf{Q}(\varepsilon)$. In this section we describe how to decompose the new part of $\boldsymbol{\mathcal{S}}_k(N, \varepsilon)$ as a direct sum of $\mathbf{T}$-modules corresponding to the Galois conjugacy classes of newforms with character ε. As an application, we can compute the q-expansions of the normalized cuspidal newforms of level N and character ε. Using the theory of Atkin-Lehner [4] as extended by Li [37], it is then possible to construct a basis for the space $S_k(N, \varepsilon; \mathbf{C})$ of cusp forms.

The algorithm is, for the most part, a straightforward generalization of the method used by Cremona [16] to enumerate the $\mathbf{Q}$-rational weight-two newforms corresponding to modular elliptic curves. Nevertheless, we present several tricks learned in the course of doing computations, which speed up the algorithm. One useful trick that Cremona also made use of is to work in the space dual to modular symbols as described in the next section.

3.5.1 Duality

Let $K = \mathbf{Q}[\varepsilon]$, and let $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^\perp$ denote $\mathrm{Hom}_K(\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K),K)$ equipped with its natural right $\mathbf{T}$-action: for $\varphi \in \boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^\perp$,

$$(\varphi T)(x) = \varphi(Tx).$$

The natural pairing

$$\langle\ ,\ \rangle : \boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^\perp \times \boldsymbol{\mathcal{S}}_k(N,\varepsilon;K) \to K \tag{3.1}$$

given by $\langle \varphi, x\rangle = \varphi(x)$ satisfies $\langle \varphi T, x\rangle = \langle \varphi, Tx\rangle$.

Viewing the elements $T \in \mathbf{T}$ as sitting inside $\mathrm{End}(\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K))$, the transpose map $T \mapsto T^t$ allows us to view $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^\perp$ as a left $\mathbf{T}$-module.

Proposition 3.14. *Let $V \subset \boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^{\mathrm{new}}$ be an irreducible new $\mathbf{T}$-submodule and set $I = \mathrm{Ann}_{\mathbf{T}}\, V$. Then the characteristic polynomial of each T_p on $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^\perp[I]$ is the same as the characteristic polynomial of T_p on V.*

Proof. We may assume for the purposes of proving the proposition that $K = \overline{\mathbf{Q}}$. There is a basis of simultaneous $\mathbf{T}$-eigenvectors for $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^{\mathrm{new}}$. With respect to this basis, $\mathbf{T}$ acts via diagonal matrices. The systems of eigenvalues coming from the old subspace are distinct from the systems of eigenvalues on the new space. Thus the dimension of $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^\perp[I]$ is the same as the dimension of V, instead of being too large. The proposition now follows by noting that the characteristic polynomial of a matrix is the same as the characteristic polynomial of its transpose. □

The degeneracy maps α_t and β_t of Section 2.5 give rise to maps $\alpha_t^\perp$ and $\beta_t^\perp$ between the dual spaces and having the dual properties to those of α_t and β_t. In particular, they commute with the Hecke operators T_p for p prime to N. The new and old subspace of $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^\perp$ are defined as in Definition 2.16.

Algorithm 3.15. This algorithm computes a decomposition of $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^{\perp\,\mathrm{new}}$ into irreducible submodules V.

Using Algorithm 3.2 compute $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)$. Then compute the maps β_t using Algorithm 2.20 and intersect the transposes of their kernels in order to obtain $\boldsymbol{\mathcal{S}}_k(N,\varepsilon)^{\perp\,\mathrm{new}}$. Compute the boundary map $\delta : \boldsymbol{\mathcal{S}}_k(N,\varepsilon;K) \to B_k(N,\varepsilon;K)$ using Algorithm 2.26. We cut out the cuspidal submodule $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^{\perp\,\mathrm{new}}$ using the Hecke operators, Algorithm 3.17, and Proposition 3.14. Set $p = 2$ and perform the following steps.

1. Using Algorithm 3.17, compute a matrix A representing the Hecke operator T_p on $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^{\perp\,\mathrm{new}}$.

2. Compute and factor the characteristic polynomial F of A.

3. For each irreducible factor f of F compute $V_f = \ker(f(A))$. Then, compute the $+1$ and -1 eigen-subspaces V_f^+ and V_f^- for the star involution. Let W denote one of these two eigen-subspaces, and use the following criteria to determine whether or not W is irreducible:

(a) If p is greater than the Sturm bound (see Theorem 3.9) then W must be irreducible.

(b) If the characteristic polynomial of some element $T \in \mathbf{T}$ acting on W is irreducible, then W is irreducible.

4. If W is irreducible, record W and consider the next factor of the characteristic polynomial in step 3. Otherwise, replace p by the next prime larger than p and replace $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^{\perp\,\mathrm{new}}$ by W, then repeat the above sequence of steps, beginning with step 1.

3.5.2 Efficient computation of Hecke operators on the dual space

In this section we give a method for computing the action of the Hecke operators $T_p \in \mathbf{T}$ on an invariant subspace $V \subset \boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^{\perp}$. A naive way to compute the right action of T_p on V is to compute a matrix representing T_p on $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)$, transpose to obtain T_p on $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^{\perp}$, and then restrict to V using Gaussian elimination. To compute T_p on $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)$, observe that $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)$ has a basis $e_1,\ldots,e_n$, where each e_i is a Manin symbol $[P,(c,d)]$, and that the action of T_p on $[P,(c,d)]$ can be computed using Section 2.6.2.

In practice, $d = \dim V$ will often be much less than n; we now describe how to compute T_p on V in d/n of the time it takes using the above naive method. This is a substantial savings when d is small. Transposing the injection $V \hookrightarrow \boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^{\perp}$, we obtain a surjection $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K) \to V^{\perp}$. There exists a subset $e_{i_1},\ldots,e_{i_d}$ of the e_i whose image forms a basis for $V^{\perp}$. With some care, it is then possible to compute T_p on $V^{\perp}$ by computing T_p on each of $e_{i_1},\ldots,e_{i_d}$.

In the rest of this section, we describe in terms of matrices a definite way to carry out this computation. Let V be an $n \times m$ matrix whose rows generate an n-dimensional subspace of an m-dimensional space of row vectors. Let T be an $m \times m$-matrix and suppose that V has rank n and that VT is contained in the row space of V. Let E be an $m \times n$ matrix with the property that the $n \times n$ matrix VE is invertible, with inverse D.

Proposition 3.16. *$VT = VTEDV$.*

Proof. Observe that
$$V(EDV) = (VED)V = IV = V.$$
Thus right multiplication by EDV
$$v \mapsto vEDV$$
induces the *identity map* on the row space of V. Since VT is contained in the row space of V, we have
$$(VT)EDV = VT,$$
as claimed. $\square$

We have not computed T, but we can compute T on each basis element $e_1,\ldots,e_d$ of the ambient space–unfortunately, d is extremely large. Our problem: quickly compute the action of T^t on the invariant subspace spanned by the rows of V. Can this be done without having to compute T on all e_i? Yes, the following algorithm shows how using a subset of only $n = \dim V$ of the e_i.

Algorithm 3.17. Let T be any linear transformation which leaves V invariant and for which we can compute $T(e_i)$ for $i = 1, \ldots, d$. This algorithm computes the matrix representing the action of T on V while computing $T(e_i)$ for only $\dim V$ of the i.

Choose any $m \times n$ matrix E whose columns are sparse linear combinations of the e_i and such that VE is invertible. For this we find a set of positions so that elements of the space spanned by the columns of V are determined by the entries in these spots. This is accomplished by row reducing, and setting E equal to the pivot columns. Using Gaussian elimination, compute the inverse D of the $n \times n$ matrix VE. The matrix representing the action of T with respect to V is then

$$V(TE)D = V(TE)(VE)^{-1}.$$

Proof. Let A be any matrix so that VA is the $n \times n$ identity matrix. By the proposition we have

$$VTA = (VTEDV)A = VTED(VA) = VTED = V(TE)D.$$

To see that VTA represents T, observe that by the proposition,

$$\begin{aligned} VTAV &= (VTEDV)AV = (VTEDVA)V \\ &= (VTED)(VA)V = (VTED)V = VT \end{aligned}$$

so that VTA gives the correct linear combination of the rows of V. □

3.5.3 Eigenvectors

Once a $\mathbf{T}$-simple subspace of $\boldsymbol{\mathcal{S}}^*$ has been identified, the following algorithm, which was suggested to the author by H. Lenstra, produces an eigenvector defined over an extension of the base field.

Algorithm 3.18. Let A be an $n \times n$ matrix over an arbitrary field K and suppose that the characteristic polynomial $f(x) = x^n + \cdots + a_1 x + a_0$ of A is irreducible. Let α be a root of $f(x)$ in an algebraic closure $\overline{K}$ of K. Factor $f(x)$ over $K(\alpha)$ as $f(x) = (x - \alpha)g(x)$. Then for any element $v \in K^n$ the vector $g(A)v$ is either 0 or it is an eigenvector of A with eigenvalue α. The vector $g(A)v$ can be computed by finding Av, $A(Av)$, $A(A(Av))$, and then using that

$$g(x) = x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_1 x + c_0,$$

where the coefficients c_i are determined by the recurrence

$$c_0 = -a_0/\alpha, \qquad c_i = (c_{i-1} - a_i)/\alpha.$$

We will prove below that $g(A)v \neq 0$ for all vectors v not in a proper subspace of K^n. Thus with high probability, a "randomly chosen" v will have the property that $g(A)v \neq 0$. Alternatively, if $v_1, \ldots v_n$ form a basis for K^n, then $g(A)v_i$ must be nonzero for some i.

Proof. By the Cayley-Hamilton theorem [36, XIV.3] we have that $f(A) = 0$. Consequently, for any $v \in K^n$, we have $(A - \alpha)g(A)v = 0$ so that $Ag(A)v = \alpha v$. Since f is irreducible it is the polynomial of least degree satisfied by A and so $g(A) \neq 0$. Therefore $g(A)v \neq 0$ for all v not in the proper closed subset $\ker(g(A))$. □

3.5.4 Eigenvalues

In this section we give an algorithm for computing the q-expansion of one of the newforms corresponding to a factor of $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^{\mathrm{new}}$. This is a generalization of the algorithm described in [16, §2.9].

Algorithm 3.19. Given a factor $V \subset \boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)^{\perp\,\mathrm{new}}$ as computed by Algorithm 3.15 this algorithm computes the q-expansion of one of the corresponding Galois conjugate newforms.

1. Using Algorithm 3.17 compute the action of the $*$-involution (Section 2.4) on V. Then compute the $+1$ eigenspace $V^+ \subset V$.

2. Find an element $T \in \mathbf{T}$ such that the characteristic polynomial of the matrix A of T acting on V^+ is irreducible. Such a T must exist by the primitive element theorem [36, V.4]. (Note: It is *not* always the case that T can be taken to equal some Hecke operator T_n. The first example with $k=2$ and $\varepsilon=1$ occurs at level $N=512$.)

3. Using Algorithm 3.5.3 compute an eigenvector e for A over an extension of K.

4. Because e is an eigenvector and the pairing given in Equation 3.1 respects the Hecke action, we have that for any Hecke operator T_n and element $w \in \boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)$, that

$$a_n\langle e,w\rangle = \langle eT_n, w\rangle = \langle e, T_n w\rangle.$$

Choose w so that $\langle e,w\rangle \neq 0$. Then

$$a_n = \frac{\langle e, T_n w\rangle}{\langle e,w\rangle}.$$

The a_n can now be computed by computing $\langle e,w\rangle$ once and for all, and then computing $\langle e, T_n w\rangle$ for each n. It is best to choose w in such a way that $T_n w$ can be computed quickly.

The beauty of this algorithm is that when w is a Manin symbol $[P(X,Y),(c,d)]$ the computation of $T_p w = \sum_{x\in R_p} wx$ is very quick, requiring us to only sum over the Heilbronn matrices of determinant p once.

In practice we compute only the eigenvalues a_p using the above algorithm, then use the following recurrences to obtain the a_n:

$$\begin{aligned} a_{nm} &= a_n a_m \qquad \text{if } (n,m)=1, \text{ and} \\ a_{p^r} &= a_{p^{r-1}} a_p - \varepsilon(p) p^{k-2} a_{p^{r-2}}. \end{aligned}$$

3.5.5 Sorting and labeling eigenforms

Systematically ordering the factors is essential, so that we can later refer to them. In Section 3.5.4 we saw how to associate to each new factor a sequence a_n of Hecke eigenvalues. These can be used to sort the factors.

Except in the case of weight 2 and trivial character, we use the following ordering. To each eigenvector associate the following sequence of integers

$$\mathrm{tr}(a_1), \mathrm{tr}(a_2), \mathrm{tr}(a_3), \mathrm{tr}(a_4), \mathrm{tr}(a_5), \mathrm{tr}(a_6), \ldots$$

where the trace is from $K_f = \mathbf{Q}(\ldots a_n \ldots)$ down to $\mathbf{Q}$. Sort the eigenforms by ordering the sequences in dictionary order with minus coming before plus. Since we included $\mathrm{tr}(a_1)$, this ordering gathers together factors of the same dimension. Furthermore, the sequence of traces determines the Galois conjugacy class of f, because the $g = \sum_{n\geq 1} \mathrm{tr}(a_n)q^n$ is the trace of f, hence g lies in the $\mathbf{C}$-vector space spanned by the Galois conjugates of f.

When $k = 2$ and the character is trivial we use a different and somewhat complicated ordering because it extends the notation for elliptic curves that was introduced in the second edition of [16] and has since become standard. Sort the factors of $\boldsymbol{\mathcal{S}}_k(N,\varepsilon)^{\mathrm{new}}$ as follows. First by dimension, with smallest dimension first. Within each dimension, sort in binary order, by the signs of the Atkin-Lehner involutions with $-$ corresponding to 0 and $+$ to 1. For example, if there are three Atkin-Lehner involutions then the sign patterns are sorted as follows:

$$+++,-++,+-+,--+,++-,-+-,+--,---.$$

Finally, let p be the smallest prime not dividing N. Within each of the Atkin-Lehner classes, sort by the magnitudes of the $K_f/\mathbf{Q}$-trace of a_p breaking ties by letting the positive trace be first. If there are still any ties, repeat the final step with the next smallest prime not dividing N, etc. (Note: It's not clear to the author that ties will always eventually be broken, though in his computation they always have been.)

3.6 Intersections and congruences

Consider a complex torus $J = V/\Lambda$, and let $A = V_A/\Lambda_A$ and $B = V_B/\Lambda_B$ be subtori whose intersection $A \cap B$ is finite.

Proposition 3.20. *There is a natural isomorphism of groups*

$$A \cap B \cong \left(\frac{\Lambda}{\Lambda_A + \Lambda_B}\right)_{\mathrm{tor}}.$$

Proof. There is an exact sequence

$$0 \to A \cap B \to A \oplus B \to J.$$

Consider the diagram

$$\begin{array}{ccccccc}
 & & \Lambda_A \oplus \Lambda_B & \longrightarrow & \Lambda & \longrightarrow & \Lambda/(\Lambda_A + \Lambda_B) \\
 & & \downarrow & & \downarrow & & \downarrow \\
 & & V_A \oplus V_B & \longrightarrow & V & \longrightarrow & V/(V_A + V_B) \\
 & & \downarrow & & \downarrow & & \downarrow \\
A \cap B & \longrightarrow & A \oplus B & \longrightarrow & J & \longrightarrow & J/(A+B).
\end{array}$$

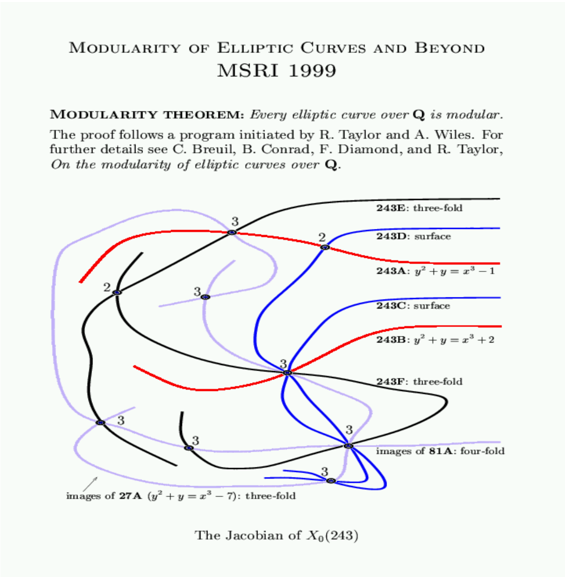

Figure 3.1: T-shirt design

The snake lemma gives an exact sequence

$$0 \to A \cap B \to \Lambda/(\Lambda_A + \Lambda_B) \to V/(V_A + V_B).$$

Since $V/(V_A + V_B)$ is a $\mathbf{C}$-vector space, the torsion part of $\Lambda/(\Lambda_A + \Lambda_B)$ must map to 0. No non-torsion in $\Lambda/(\Lambda_A + \Lambda_B)$ could map to 0, because if it did then $A \cap B$ would not be finite. The lemma follows. $\square$

The following formula for the intersection of n subtori is obtained in a similar way.

Proposition 3.21. *For $i = 1, \ldots, n$ let $A_i = V_i/\Lambda_i$ be a subtorus of $J = V/\Lambda$, and assume that each pairwise intersection $A_i \cap A_j$ is finite. Then*

$$A_1 \cap \cdots \cap A_n \cong \left(\frac{\Lambda \oplus \cdots \oplus \Lambda}{f(\Lambda_1 \oplus \cdots \oplus \Lambda_n)} \right),$$

where $f(x_1, \ldots, x_n) = (x_1 - x_2, x_2 - x_3, x_3 - x_4, \ldots, x_{n-1} - x_n)$.

Remark 3.22. Using this proposition the author constructed the T-shirt design in Figure 3.1.

Example 3.23. L. Kilford of London, England has recently discovered an example at prime level 503 in which "multiplicity one" fails. One verification of his example uses the above proposition. Let E_1, E_2, and E_3 be the three elliptic curves of conductor 503, and for each $i = 1, 2, 3$, let $\mathfrak{m}_i$ be the maximal ideal of $\mathbf{T} \subset \mathrm{End}(J_0(503))$ generated by 2 and all $T_p - a_p(E_i)$, with p prime. Each of the Galois representations $E_i[2]$ is irreducible, and one can check that $\mathfrak{m}_1 = \mathfrak{m}_2 = \mathfrak{m}_3$. If multiplicity one holds, then $E_1[2] = E_2[2] = E_3[2]$ inside of $J_0(503)$. However, this is not the case, as a modular symbols computation in the integral homology $H_1(X_0(N), \mathbf{Z})$ reveals that $E_1 \cap E_2 = \{0\}$.

3.6.1 A strategy for computing congruences

Let N be a positive integer, $k \geq 2$ an integer, and ε a mod N Dirichlet character. Suppose f and g are newforms in $S_k(N, \varepsilon; \overline{\mathbf{Q}})$. The following proposition gives rise to an algorithm for computing most congruences between infinite Fourier expansions.

The advantage of the algorithm is that it only involves finite exact computations and does not rely on the computation of q-expansions. A disadvantage is that congruences between q-expansions need not be reflected by the corresponding modular symbols, so the proposition need not give all congruences. This is illustrated in Example 3.23.

The author first learned about this strategy from the section entitled "First strategy: Computing m-congruences of period lattices" in [18].

Proposition 3.24. *Suppose f and g are newforms in $S_k(N, \varepsilon; \overline{\mathbf{Q}})$. Let I_f and I_g be the corresponding annihilators in the Hecke algebra $\mathbf{T}$. Let $\Lambda = \boldsymbol{\mathcal{S}}_k(N, \varepsilon; \mathcal{O})$, and set $\Lambda_f = \Lambda[I_f]$ and $\Lambda_g = \Lambda[I_g]$. If $p \mid \#\left(\frac{\Lambda}{\Lambda_f + \Lambda_g}\right)_{\mathrm{tor}}$ then there is a prime $\wp$ of residue characteristic p such that $f \equiv g \pmod{\wp}$.*

Proof. Consider the exact sequence

$$0 \to \Lambda_f \oplus \Lambda_g \to \Lambda \to \Lambda/(\Lambda_f + \Lambda_g) \to 0$$

where the first map is $(a, b) \mapsto a - b$. Upon tensoring this sequence with $\mathbf{F}_p$ we obtain:

$$Z \to (\Lambda_f \otimes \mathbf{F}_p) \oplus (\Lambda_g \otimes \mathbf{F}_p) \to \Lambda \otimes \mathbf{F}_p \to (\Lambda/(\Lambda_f + \Lambda_g)) \otimes \mathbf{F}_p \to 0,$$

where $Z = \mathrm{Tor}^1(\Lambda/(\Lambda_f + \Lambda_g), \mathbf{F}_p)$. Denote by $\mathrm{im}(\Lambda_f)$ the image of $\Lambda_f \otimes \mathbf{F}_p$ in $\Lambda \otimes \mathbf{F}_p$ and likewise for Λ_g. Our assumption that p divides the torsion part of $\Lambda/(\Lambda_f + \Lambda_g)$ implies that Z is nonzero, so $\mathrm{im}(\Lambda_f)$ and $\mathrm{im}(\Lambda_g)$ have nonzero intersection inside the $\mathbf{F}_p$-vector space $\Lambda \otimes \mathbf{F}_p$. The Hecke algebra $\mathbf{T}$ acts on $\mathrm{im}(\Lambda_f)$ through its action on f, that is, through the quotient $\mathbf{T}/I_f$; similarly, $\mathbf{T}$ acts on $\mathrm{im}(\Lambda_g)$ through $\mathbf{T}/I_g$. Thus $\mathbf{T}$ acts on the nonzero $\mathbf{T} \otimes \mathbf{F}_p$-module $\mathrm{im}(\Lambda_f) \cap \mathrm{im}(\Lambda_g)$ through $\mathbf{T}/(I_f + I_g + p)$. This implies that $I_f + I_g + p$ is not the unit ideal, which is equivalent to the assertion of the proposition. □

3.7 The rational period mapping

Consider a triple (N, k, ε), and let $K = \mathbf{Q}[\varepsilon]$. Let I be an ideal in the Hecke algebra $\mathbf{T}$ associated to (N, k, ε). The rational period mapping associated to I is a map from the space $\boldsymbol{\mathcal{M}}_k(N, \varepsilon; K)$ of modular symbols to a finite dimensional K-vector space. It is a computable analogue of the classical integration pairing, and is of great value in extracting the rational parts of analytic invariants; e.g., of special values of L-functions. In the next section we use it to compute the image of cuspidal points on $J(N, k, \varepsilon)$.

Definition 3.25. Let $D := \mathrm{Hom}_K(\boldsymbol{\mathcal{M}}_k(N, \varepsilon; K), K)[I]$; the *rational period mapping* is the natural quotient map

$$\Theta_I : \boldsymbol{\mathcal{M}}_k(N, \varepsilon; K) \to \frac{\boldsymbol{\mathcal{M}}_k(N, \varepsilon; K)}{\bigcap \{\ker(\varphi) : \varphi \in D\}}.$$

If $f \in S_k(N,\varepsilon)$ is a newform, set $\Theta_f := \Theta_{I_f}$ where I_f is the annihilator of f in the Hecke algebra.

Algorithm 3.26. This algorithm computes Θ_I. Choose a basis for $W = \boldsymbol{\mathcal{M}}_k(N,\varepsilon;K)$ and use it to view W as a space of column vectors equipped with a left action of $\mathbf{T}$. View $W^* = \mathrm{Hom}_K(\boldsymbol{\mathcal{M}}_k(N,\varepsilon;K),K)$ as the space of row vectors of length equal to $\dim \boldsymbol{\mathcal{M}}_k(N,\varepsilon;K)$; thus W^* is dual to W via the natural pairing between row and column vectors. The Hecke operators act on W^* on the right. Compute a basis $\varphi_1,\ldots,\varphi_n$ for the K-vector space $W^*[I]$. Then the rational period mapping with respect to this basis is $\varphi_1 \times \cdots \times \varphi_n$; it is given by the matrix whose rows are $\varphi_1,\ldots,\varphi_n$.

Proof. The kernels of $\varphi_1 \times \cdots \times \varphi_n$ and Θ_I are the same. □

Example 3.27. Let I be the annihilator of the newform $f = q - 2q^2 + \cdots \in M_2(37,1;\mathbf{Q})$ corresponding to the elliptic curve **37k2A**. There is a basis for $W = \boldsymbol{\mathcal{M}}_2(37,1;\mathbf{Q})$ such that

$$T_2 = \begin{pmatrix} -1 & 1 & 1 & -1 & 0 \\ 1 & -1 & 1 & 0 & 0 \\ 0 & 0 & -2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 3 \end{pmatrix}$$

The characteristic polynomial of T_2 is $x^2(x+2)^2(x-3)$. Thus $W[I] = \ker(T_2+2)$ is spanned by the column vectors $(1,-1,0,1/2,0)^t$ and $(0,0,1,-1/2,0)^t$, and $W^*[I] = \ker(T_2^t + 2)$ is spanned by the row vectors $(1,0,-1,0,0)$ and $(0,1,-1,0,0)$. The rational period mapping is $\Theta_I((a,b,c,d,e)^t) = (a-c, b-c)$.

Lemma 3.28.

$$\dim \boldsymbol{\mathcal{M}}_k(N,\varepsilon;K)[I] = \dim \mathrm{Hom}_K(\boldsymbol{\mathcal{M}}_k(N,\varepsilon;K),K)[I].$$

Proof. Let $W = \boldsymbol{\mathcal{M}}_k(N,\varepsilon;K)$ and W^* be its dual. Let $a_1,\ldots,a_n$ be a set of generators for I. Choose a basis for W that is compatible with the following filtration:

$$0 \subset (\ker(a_1) \cap \cdots \cap \ker(a_n)) \subset (\ker(a_1) \cap \cdots \cap \ker(a_{n-1})) \subset \cdots \subset \ker(a_1) \subset W.$$

The rank of a matrix equals the rank of its transpose, so the dimension of $\ker(a_1)$ is the same as the dimension of $\ker(a_1^t)$, that is, $\dim W[(a_1)] = \dim W^*[(a_1)]$. Since $\mathbf{T}$ is commutative, a_2 leaves $\ker(a_1)$ invariant; because of how we chose our basis for W, the transpose of $a_2|_{\ker(a_1)}$ is $a_2^t|_{\ker(a_1^t)}$. Thus again, $\dim(\ker(a_2|_{\ker(a_1)}))$ equals $\dim(\ker(a_2^t|_{\ker(a_1^t)}))$. Proceeding inductively, we prove the lemma. □

Corollary 3.29. *Suppose $\boldsymbol{\mathcal{M}}_k(N,\varepsilon;K)[I] \subset \boldsymbol{\mathcal{S}}_k(N,\varepsilon;K)$, and let $P : \boldsymbol{\mathcal{M}}_k(N,\varepsilon;K) \to \mathrm{Hom}_{\mathbf{C}}(S_k(N,\varepsilon;\mathbf{C})[I],\mathbf{C})$ be the classical period map induced by the integration pairing. Then $\ker(P) = \ker(\Theta_I)$.*

Proof. Since $P(\boldsymbol{\mathcal{M}}_k(N,\varepsilon;\mathcal{O}))$ is known to be a finite-covolume $\mathcal{O}$-lattice in the complex vector space $\mathrm{Hom}_{\mathbf{C}}(S_k(N,\varepsilon;\mathbf{C})[I],\mathbf{C})$, the K-dimension of $\mathrm{im}(P)$ equals $2\cdot\dim_{\mathbf{C}} S_k(N,\varepsilon;\mathbf{C})[I]$, which in turn equals $\dim_K \boldsymbol{\mathcal{M}}_k(N,\varepsilon;K)[I]$. Thus by Lemma 3.28 the images $\mathrm{im}(P)$ and $\mathrm{im}(\Theta_I)$ have the same dimension, hence $\ker(P)$ and $\ker(\Theta_I)$ also have the same dimension. It thus suffices to prove the inclusion $\ker(\Theta_I) \subset \ker(P)$. Suppose $\Theta_I(x) = 0$; then $\varphi(x) = 0$ for all $x \in W^*[I]$, where $W = \boldsymbol{\mathcal{M}}_k(N,\varepsilon;K)$. Thus $\varphi(x) = 0$ for all $\varphi \in (W \otimes \mathbf{C})^*[I]$. Since the integration pairing that defines P respects the action of $\mathbf{T}$, the composition of P with any linear functional lies in $(W \otimes \mathbf{C})^*[I]$. Thus $P(x) = 0$, as required. $\square$

3.8 The images of cuspidal points

Consider a triple (N, k, ε), and let $K = \mathbf{Q}[\varepsilon]$. Recall that integration defines a period mapping

$$P : \boldsymbol{\mathcal{M}}_k(N,\varepsilon;K) \to \mathrm{Hom}_{\mathbf{C}}(S_k(N,\varepsilon;\mathbf{C}),\mathbf{C}).$$

A *cuspidal point* of

$$J = J(N,k,\varepsilon) := \frac{\mathrm{Hom}_{\mathbf{C}}(S_k(N,\varepsilon;\mathbf{C}),\mathbf{C})}{P(\boldsymbol{\mathcal{S}}_k(N,\varepsilon;\mathcal{O}))}$$

is a point that is in the image under P of $\boldsymbol{\mathcal{M}}_k(N,\varepsilon;\mathcal{O})$. It is of great interest to compute the structure of the cuspidal subgroup of J and of the quotients of J. For example, when $k = 2$ and $\varepsilon = 1$, the torus J can be identified with $J_0(N)(\mathbf{C})$. In this case, Manin proved (see [38]) that the cuspidal point $\{0,\infty\}$ is a torsion point in $J_0(N)(\mathbf{Q})$, so its order gives a lower bound on $J_0(N)(\mathbf{Q})_{\mathrm{tor}}$.

Algorithm 3.30 (Cuspidal subgroup). Let I be an ideal in the Hecke algebra $\mathbf{T}$. This algorithm computes the cuspidal subgroup of the quotient A_I of J. Using Algorithm 3.5 compute $\boldsymbol{\mathcal{M}}_k(N,\varepsilon;\mathcal{O})$ and $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;\mathcal{O})$. Using Algorithm 3.26, compute the rational period mapping Θ_I. Then the cuspidal subgroup is the subgroup of $\Theta_I(\boldsymbol{\mathcal{S}}_k(N,\varepsilon;\mathcal{O}))$ generated by the elements $\Theta_I(x)$ for $x \in \boldsymbol{\mathcal{M}}_k(N,\varepsilon;\mathcal{O})$. In particular, the point of $A_I(\mathbf{C})$ corresponding to $X^iY^{k-2-i}\{\alpha,\beta\}$ is the image of $\Theta_I(X^iY^{k-2-i}\{\alpha,\beta\})$ in the quotient of $\Theta_I(\boldsymbol{\mathcal{M}}_k(N,\varepsilon;\mathcal{O}))$ by $\Theta_I(\boldsymbol{\mathcal{S}}_k(N,\varepsilon;\mathcal{O}))$.

Example 3.31. This example continues Example 3.27. The basis chosen is also a basis for $\boldsymbol{\mathcal{M}}_2(37,1;\mathbf{Z})$, so by computing the boundary map, or the integer kernel of $T_2(T_2+2)$, we find that $\boldsymbol{\mathcal{S}}_2(37,1;\mathbf{Z})$ is spanned by $(1,0,0,0,0)$, $(0,1,0,0,0)$, $(0,0,1,0,0)$, and $(0,0,0,1,0)$. Thus $\Theta_I(\boldsymbol{\mathcal{S}}_2(37,1;\mathbf{Z}))$ is generated by $(1,0)$ and $(0,1)$. The modular symbols $\{0,\infty\}$ is represented by $(0,0,0,0,-1)$, so the image of the cusp $(0)-(\infty) \in J_0(37)$ is 0 in **37k2A**.

The rational period mapping associated to **37k2B** (with respect to some basis) is

$$\Theta_I((a,b,c,d,e)^t) = (a - c - 2d + \frac{2}{3}e,\ b + c + 2d - \frac{2}{3}e).$$

Thus $\Theta_I(\boldsymbol{\mathcal{S}}_2(37,1;\mathbf{Z}))$ is generated by $(1,0)$ and $(0,1)$. The image of $\{0,\infty\}$ is is $\frac{2}{3}(1,-1)$, so the image of $(0)-(\infty)$ in **37k2B** has order 3.

3.8.1 Rational torsion

Let f be a newform of weight 2, and suppose $\varepsilon = 1$. Manin proved that $(0)-(\infty)$ defines an element of $J_0(N)(\mathbf{Q})_{\mathrm{tor}}$. Thus the order of the image of $(0)-(\infty)$ provides a lower bounds on $\#A_f(\mathbf{Q})_{\mathrm{tor}}$. In general, many other points in the cuspidal subgroup can be rational. Determining which would give a better lower bound on the rational subgroup; the author has not yet carried out such computations (see, however, [65]).

3.8.2 Upper bound on torsion: Counting points mod p

Let f be a newform of weight 2, and suppose $\varepsilon = 1$. The Hecke algebra $\mathbf{T}$ acts through a quotient $\overline{\mathbf{T}}$ on the subspace of $S_2(\Gamma_0(N))$ spanned by the Galois conjugates of f. Let $\chi_p(X)$ be the characteristic polynomial of the image of T_p in $\overline{\mathbf{T}}$. Suppose $p \nmid N$ and let $N_p = \#A_f(\mathbf{F}_p)$ be the number of points on the mod p reduction of the abelian variety A_f.

Proposition 3.32. *For each prime p not dividing N,*

$$N_p = \chi_p(p+1).$$

Proof. This is probably well-known, but we give a proof (which was suggested to the author by Matt Baker). It follows from the Eichler-Shimura theorem that the following relation holds in the endomorphism ring of $A_f/\mathbf{F}_p$:

$$T_p = \mathrm{Frob} + \mathrm{Ver} = \mathrm{Frob} + p/\mathrm{Frob}.$$

Let $\ell \neq p$ be a prime. If the characteristic polynomial of Frob on an ℓ-adic Tate module of $A_f/\mathbf{F}_p$ is $F(t)$, and the characteristic polynomial of T_p on differentials $H^0(A_f/\mathbf{F}_p, \Omega)$ is $f(t)$, then we have $f(t) = x^{-d}F(x)$, where $t = x + (p/x)$ and $d = \dim A_f$. In other words, the relation above gives an easy conversion between f and F. Since it's a general fact that $\#A_f(\mathbf{F}_p) = F(1)$, we have $\#A_f(\mathbf{F}_p) = f(p+1)$. □

The following theorem is proved using formal groups.

Theorem 3.33. *Let A be an abelian variety over $\mathbf{Q}$, with good reduction outside N. Suppose $p \nmid N$. Then the kernel of the reduction map $A(\mathbf{Q})_{\mathrm{tor}} \to A(\mathbf{F}_p)$ is killed by p. If $p > 2$ then the kernel is trivial.*

By taking gcd's we obtain an upper bound on $\#A(\mathbf{Q})_{\mathrm{tor}}$. This upper bound is not in general sharp; in fact, it is unchanged if A is replaced by any isogenous abelian variety. For example, $X_0(11)$ and $X_1(11)$ are isogenous, but have different torsion subgroups.

3.9 The modular degree

Let f be a newform of level N, weight $k \geq 2$ and character ε such that $\varepsilon^2 = 1$. In this section we define and give an algorithm to compute the modular degree of the torus A_f attached to f.

Definition 3.34. The *modular map* is the map $\theta_f : A_f^\vee \to A_f$ that is induced by the bottom row of Diagram 2.1 on page 34. The *modular degree* m_f of f (or of A_f) is the degree of this map. If f has weight two, then θ_f is a polarization so by [50, Thm. 13.3] its degree is a perfect square; in this case we *instead* define the modular degree m_f to be the positive square root of the degree of θ_f.

Remark 3.35. When $E/\mathbf{Q}$ be a modular elliptic curve of conductor N that is an optimal quotient of $J_0(N)$, then m_f is the usual modular degree, which is the least degree of a map $X_0(N) \to E$.

Remark 3.36. When $k \neq 2$, the degree of θ_f need not be a perfect square. For example, there is a one-dimensional quotient A_f associated to the unique rational newform

$$f = q + 2q^2 - 8q^3 + 4q^4 + 5q^5 - 16q^6 - 4q^7 + \cdots \in S_4(10)$$

such that the kernel of θ_f is isomorphic to $\mathbf{Z}/10\mathbf{Z}$.

Next, for a newform f let θ'_f be the part of $\#\ker(\theta_f)$ that is coprime to the level. There is a newform in $f \in S_4(\Gamma_0(77))$ such that θ'_f is not a perfect square at 2. For identification purposes, we remark that the field generated by the Fourier coefficients of f has discriminant $2^3 \cdot 3^3 \cdot 2417$.

Algorithm 3.37. Let I_f be the annihilator of f in the Hecke algebra. The modular kernel $\ker(\theta_f)$ is isomorphic to the cokernel of the natural map $\boldsymbol{\mathcal{S}}[I_f] \to \Phi_f(\boldsymbol{\mathcal{S}})$ of Diagram 2.1 on page 34. This cokernel can be computed by replacing Φ_f by the rational period map Θ_{I_f}.

Proof. For concreteness, we give the proof only in the case of weight-two and trivial character. The proof in the general case is similar. Let $S = S_2(\Gamma_0(N), \mathbf{C})$ be the complex vector space of weight-two modular forms of level N, and set $H = H_1(X_0(N), Z)$. The integration pairing $S \times H \to \mathbf{C}$ induces a natural map

$$\Phi_f : H \to \operatorname{Hom}(S[I_f], \mathbf{C}).$$

Using the classical Abel-Jacobi theorem, we deduce the following commutative diagram, which has exact columns, but whose rows are not exact.

$$\begin{tikzcd}
0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] \\
H[I_f] \arrow[r] \arrow[d] & H \arrow[r] \arrow[d] & \Phi_f(H) \arrow[d] \\
\operatorname{Hom}(S, \mathbf{C})[I_f] \arrow[r] \arrow[d] & \operatorname{Hom}(S, \mathbf{C}) \arrow[r] \arrow[d] & \operatorname{Hom}(S[I_f], \mathbf{C}) \arrow[d] \\
A_f^\vee(\mathbf{C}) \arrow[r] \arrow[d] \arrow[rr, bend right] & J_0(N)(\mathbf{C}) \arrow[r] \arrow[d] & A_f(\mathbf{C}) \arrow[d] \\
0 & 0 & 0
\end{tikzcd}$$

By the snake lemma, the kernel of $A_f^\vee(\mathbf{C}) \to A_f(\mathbf{C})$ is isomorphic to the cokernel of the map $H[I_f] \to \Phi_f(H)$, which proves the proposition. $\square$

Remark 3.38. Suppose E is an optimal quotient of $J_0(p)$, with p prime. The surjectivity result in [48] implies that it is possible to efficiently compute the modular degree using only the method of graphs. For more details, see Chapter 4.

3.10 The rational part of $L(A_f, j)$

Let $k \geq 2$ be an integer, and let $\varepsilon : (\mathbf{Z}/N\mathbf{Z})^* \to \mathbf{C}^*$ be a Dirichlet character such that $\varepsilon^2 = 1$. This assumption on ε is made only for simplicity; there is no fundamental obstruction to considering arbitrary characters. For the remainder of this section we fix a newform $f \in S_k(N, \varepsilon)$. We will compute certain rational numbers associated to f.

The author was motivated to prove the results of this section after seeing Agashe's results in the case $k = 2$ and $\varepsilon = 1$; see [2, Ch. 4].

3.10.1 L-functions

Definition 3.39. The L-series associated to f is the complex-analytic function

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

Hecke proved that $L(f, s)$ has an analytic continuation to the whole complex plane. In particular, it makes sense to consider the values $L(f, j)$ where $j \in \{1, 2, \ldots, k-1\}$ is an integer in the "critical strip." The general consesus is that these special values have deep arithmetic significance, in the sense that the quotients $L(f, j)/\omega_{f,j}$ should be algebraic numbers, where $\omega_{f,j}$ is an appropriate period of f, and that these algebraic numbers should encode deep arithmetic properties of the motive attached to f.

For simplicity, especially when doing explicit computations, it is desirable to work exclusively with ratios that are rational numbers instead of algebraic numbers. For this purpose, we consider instead the complex torus A_f attached to f, and introduce

$$L(A_f, s) := \prod_{i=1}^{d} L(f_i, s),$$

where $f_1, \ldots, f_d$ are the distinct Galois-conjugates of f. As we will see, $L(A_f, j)/\Omega_j \in \mathbf{Q}$, where Ω_j will be defined below.

Though the notation $L(A_f, s)$ suggests that there might be a way to attach an L-function to a general complex torus, this is definitely *not* what we have in mind. For our present purposes, the notation $L(A_f, s)$ is nothing more than a convenient shorthand for the product of the L-functions attached to the Galois conjugates of f. However, in the case when $k = 2$ and $\varepsilon = 1$, the L-function $L(A_f, s)$ is known to be the canonical L-series associated to the abelian variety $A_f/\mathbf{Q}$; see, e.g., the discussion in [20, Sec. 7].

3.10.2 Winding elements

Generalizing Mazur and Merel's terminology when $k = 2$, we define winding elements as follows.

Definition 3.40 (Winding element). For $1 \leq i \leq k-1$, the ith *winding element* is

$$\mathbf{e}_i := X^{i-1} Y^{k-2-(i-1)} \{0, \infty\} \in \boldsymbol{\mathcal{M}}_k(N, \varepsilon; \mathbf{Z}).$$

For example, when $k = 2$ there is one winding element $\mathbf{e} = \mathbf{e}_1 = \{0, \infty\}$. See [44, §2.2] for a topologically motivated discussion of the terminology "winding element."

3.10.3 Real and minus volumes

We briefly review the association of a complex torus to a Galois-conjugacy class of newforms. Consider the space $S_k(N, \varepsilon; \mathbf{Z})$ of cusp forms in $S_k(N, \varepsilon)$ whose q-expansion at infinity has Fourier coefficients which lie in $\mathbf{Z}$. Let V be the $\mathbf{C}$-vector space spanned by the Galois conjugates $f_1, \ldots, f_d$ of f, and choose a $\mathbf{Z}$-basis $g_1, \ldots, g_d$ for the intersection $V \cap S_k(N, \varepsilon; \mathbf{Z})$. Then integration via the pairing of Theorem 2.7 against $g_1, \ldots, g_d$ defines a map $\boldsymbol{\mathcal{S}}_k(N, \varepsilon; \mathbf{Z}) \to \mathbf{C}^d$ whose cokernel is $A_f(\mathbf{C})$. Viewing $A_f(\mathbf{C})$ in this way, the standard measure on $\mathbf{C}^d$ defines a measure on $A_f(\mathbf{C})$.

Because $\varepsilon^2 = 1$, the complex torus $A(\mathbf{C})$ is equipped with an action of complex conjugation. There are two distinguished additive subgroups of $A(\mathbf{C})$: the subgroup $A(\mathbf{R})$ of elements fixed under complex conjugation, and the subgroup $A(\mathbf{C})^-$ of elements sent to their additive inverse by complex conjugation. When j is odd, let Ω_j be the measure of the subgroup fixed under conjugation, and when j is even, let Ω_j be the measure of the subgroup sent to its inverse under conjugation, times i^d, where d is the dimension of A. When j is odd, we call Ω_j the *real volume*; otherwise, we call Ω_j the *minus volume* (see Definition 3.58).

3.10.4 The theorem

We are now prepared to state a theorem that gives a computable expression for the ratio $|L(A_f, j)/\Omega_j|$. This theorem grew out of joint work with Agashe. It generalizes Cremona's method for computation $L(E, 1)/\Omega_E$ when E is an elliptic curve (see [16, §2.8]).

As an immediate corollary of the formula, we see that $|L(A_f, j)/\Omega_j|$ is a rational number. This was already known when $f \in S_2(\Gamma_0(N))$ (see [28, §2]). The author remains ignorant as to whether or not the general corollary was known before, or even if the real numbers Ω_j, exactly as defined here, had been previously considered. However, rationality of certain related period ratios has been known for some time, due to work of Manin, Shimura, and Hatada. For a clear historical summary of these rationality results see Li's MathSciNet review of [29]. See also [42, 44].

We take the absolute value of $L(A_f, j)/\Omega_j$ for simplicity only because at present we do not wish to worry about powers of the 4th root of unity i.

Theorem 3.41. *Let $f \in S_k(N, \varepsilon)$ be a newform, where $k \geq 2$ and $\varepsilon^2 = 1$, and let $j \in \{1, 2, \ldots, k-1\}$ be an integer in the critical strip. Let $\sigma = (-1)^{j-1}$, and let Θ_f be the rational periopd mapping associated to f (see Definition 3.25). Then*

$$\left| \frac{L(A_f, j)}{\Omega_j} \right| = [\Theta_f(\boldsymbol{\mathcal{S}}_k(N, \varepsilon; \mathbf{Z})^\sigma) : \Theta_f(\mathbf{T}\mathbf{e}_j)],$$

where $\boldsymbol{\mathcal{S}}_k(N, \varepsilon; \mathbf{Z})^\sigma$ denotes the submodule of $\boldsymbol{\mathcal{S}}_k(N, \varepsilon; \mathbf{Z})$ on which the $*$-involution acts as σ, and Ω_j is the real or minus volume of A_f, as in Section 3.10.3. The right hand expression in the formula is a lattice index, whose definition is given below.

Remark 3.42. In the context of the BSD conjecture, $\Omega_{A_f} = \Omega_1 \cdot c_\infty$, where c_∞ is the number of connected components of $A_f(\mathbf{R})$.

The theorem involves lattice indexes, which we define as follows.

Definition 3.43. Let V be a finite-dimensional vector space over $\mathbf{R}$. A *lattice* $L \subset V$ is a free abelian group of rank equal to the dimension of V such that $\mathbf{R}L = V$. If $L, M \subset V$ are lattices, the *lattice index* $[L : M] \in \mathbf{R}$ is the absolute value of the determinant of an automorphism of V taking L isomorphically onto M. For convenience we set $[L : M] = 0$ for any lattice L and additive abelian group M contained in V and of rank strictly smaller than $\dim V$.

The following fact allows us to compute the lattice the index without using complex numbers.

Lemma 3.44. *Suppose $\tau_i : V \to W_i$, $i = 1, 2$, are surjective linear maps such that $\ker(\tau_1) = \ker(\tau_2)$. Let L and M be lattices in V such that $\tau_i(L)$ and $\tau_i(M)$ are both lattices for $i = 1, 2$. Then*

$$[\tau_1(L) : \tau_1(M)] = [\tau_2(L) : \tau_2(M)].$$

Proof. Surjectivity and equality of kernels insures that there is a unique isomorphism $\iota : W_1 \to W_2$ such that $\iota\tau_1 = \tau_2$. Let σ be an automorphism of W_1 such that $\sigma(\tau_1(L)) = \tau_1(M)$. Then

$$\iota\sigma\iota^{-1}(\tau_2(L)) = \iota\sigma\tau_1(L) = \iota\tau_1(M) = \tau_2(M).$$

Since conjugation does not change the determinant,

$$[\tau_2(L) : \tau_2(M)] = |\det(\iota\sigma\iota^{-1})| = |\det(\sigma)| = [\tau_1(L) : \tau_1(M)].$$

□

Proof of Theorem 3.41. Let $\Phi = \Phi_f$ be the period map $\boldsymbol{\mathcal{M}}_k(N, \varepsilon; \mathbf{Z}) \to \mathbf{C}^d$ defined by fixing a basis $f_1, f_2, \ldots, f_d$ of the conjugates of the *newform* f; thus

$$\Phi(x) = (\langle f_1, x\rangle, \langle f_2, x\rangle, \ldots \langle f_d, x\rangle) \in \mathbf{C}^d.$$

We view $\mathbf{C}^d$ as an algebra with unit element $\mathbf{1} = (1, \ldots, 1)$ equipped with an action of the Hecke operators. The operator T_p acts as $(a_p^{(1)}, \ldots, a_p^{(d)})$, where the components $a_p^{(j)}$ are the Galois conjugates of a_p. Let $\mathbf{Z}^d \subset \mathbf{R}^d \subset \mathbf{C}^d$ be the standard submodules.

For brevity, set $\boldsymbol{\mathcal{S}} = \boldsymbol{\mathcal{S}}_k(N, \varepsilon; \mathbf{Z})$. Let $\mu(\Phi(\boldsymbol{\mathcal{S}}^\sigma))$ be the measure of a fundamental domain for the lattice $\Phi(\boldsymbol{\mathcal{S}}^\sigma)$; equivalently, $\mu(\Phi(\boldsymbol{\mathcal{S}}^\sigma))$ is the absolute value of the determinant of a basis for $\Phi(\boldsymbol{\mathcal{S}}^\sigma)$. Observe that $\mu(\Phi(\boldsymbol{\mathcal{S}}^\sigma)) = [\mathbf{Z}^d : \Phi(\boldsymbol{\mathcal{S}}^\sigma)]$ and $|L(A_f, j)| = [\mathbf{Z}^d : \Phi(\mathbf{e}_j)\mathbf{Z}^d]$.

Let $W \subset \mathbf{C}^d$ be the $\mathbf{Z}$-module spanned by the "columns" of a basis for $S_k(N, \varepsilon; \mathbf{Z})[I_f]$. More precisely, if $g_1, \ldots, g_d$ is a basis, then the nth column is the vector $(a_n(g_1), \ldots, a_n(g_d))$, where $a_n(g_i)$ is the coefficient of q^n in the q-expansion of g_i at infinity. Because Ω_j is computed with respect to a basis for $S_k(N, \varepsilon; \mathbf{Z})[I_f]$,

$$\mu(\Phi(\boldsymbol{\mathcal{S}}^\sigma)) = [W : \mathbf{T}\mathbf{1}] \cdot \Omega_j.$$

Observe that $S_k(N,\varepsilon;\mathbf{Z})$ is saturated, in the sense that there are no nontrivial linear relations between the g_i when reduced modulo any prime p. To see this, note that if $\sum a_i g_i \equiv 0 \pmod{p}$, then $\frac{1}{p}\sum a_i g_i \in S_k(N,\varepsilon;\mathbf{Z})$ which, if the a_i are not all 0, is contrary to our assumption that $g_1,\ldots,g_d$ are a $\mathbf{Z}$-basis. Because "row rank = column rank", the same must be true for the "columns" defined in the previous paragraph, so $[\mathbf{Z}^d : W] = 1$. It follows that $[\mathbf{Z}^d : \mathbf{T1}] = [W : \mathbf{T1}]$.

The following calculation combines together the above observations using properties of the lattice index:

$$\begin{aligned}
[\Phi(\boldsymbol{\mathcal{S}}^\sigma):\Phi(\mathbf{T}\mathbf{e}_j)] &= [\Phi(\boldsymbol{\mathcal{S}}^\sigma):\mathbf{Z}^d]\cdot[\mathbf{Z}^d:\Phi(\mathbf{T}\mathbf{e}_j)]\\
&= \frac{1}{[\mathbf{Z}^d:\Phi(\boldsymbol{\mathcal{S}}^\sigma)]}\cdot[\mathbf{Z}^d:\Phi(\mathbf{T}\mathbf{e}_j)]\\
&= \frac{1}{\mu(\Phi(\boldsymbol{\mathcal{S}}^\sigma))}\cdot[\mathbf{Z}^d:\Phi(\mathbf{e}_j)\mathbf{Z}^d]\cdot[\Phi(\mathbf{e}_j)\mathbf{Z}^d:\Phi(\mathbf{T}\mathbf{e}_j)]\\
&= \frac{|L(A_f,j)|}{\mu(\Phi(\boldsymbol{\mathcal{S}}^\sigma))}\cdot[\Phi(\mathbf{e}_j)\mathbf{Z}^d:\Phi(\mathbf{T}\mathbf{e}_j)]\\
&= \frac{|L(A_f,j)|}{\mu(\Phi(\boldsymbol{\mathcal{S}}^\sigma))}\cdot[\Phi(\mathbf{e}_j)\mathbf{Z}^d:\Phi(\mathbf{e}_j)\mathbf{T1}]\\
&= \frac{|L(A_f,j)|}{|\Omega_j|\cdot[W:\mathbf{T1}]}\cdot[\mathbf{Z}^d:\mathbf{T1}]\\
&= \frac{|L(A_f,j)|}{|\Omega_j|}.
\end{aligned}$$

Theorem 3.41 now follows by using Lemma 3.44, to replace Φ by Θ_f. □

3.10.5 Bounding the denominator of the ratio

In this section we bound the denominators of the ratios appearing in the previous section. We begin with the following lemma, which follows easily from the alternative description of the boundary map given in Proposition 2.25.

Lemma 3.45. *For $j = 2,\ldots,k-2$ the winding element $\mathbf{e}_j$ lies in $\boldsymbol{\mathcal{S}}_k(N,\varepsilon;\mathbf{Z})$.*

Proof. Recall that $\mathbf{e}_j = P(X,Y)\{0,\infty\}$ where $P(X,Y) = X^{j-1}Y^{k-2-(j-1)}$. Since $2 \le j \le k-2$, it follows that $P(1,0) = P(0,1) = 0$, so Propositison 2.25 implies that $\mathbf{e}_j$ maps to 0 under the boundary map. □

Proposition 3.46. *For $j = 2,\ldots,k-2$,*

$$\frac{L(A_f,j)}{\Omega_j} \in \mathbf{Z}.$$

Proof. This follows from Theorem 3.41 because $\Theta_f(\mathbf{T}\mathbf{e}_j) \subset \Theta_f(\boldsymbol{\mathcal{S}}_k(N,\varepsilon;\mathbf{Z})^\sigma)$, so the lattice index is an integer. □

For the rest of this section, we assume for simplicity that $\varepsilon = 1$.

Lemma 3.47. *For $j = 1$ and $j = k-1$, we have for each $p \nmid N$ that*

$$(T_p - (1 + p^{k-1}))\mathbf{e}_j \in \boldsymbol{\mathcal{S}}_k(N, \varepsilon; \mathbf{Z}).$$

Proof. This is a standard calculation; see, e.g., [16, §2.8] for the case when $k = 2$. □

Proposition 3.48. *Let $j \in \{1, \ldots, k-1\}$, and let n be the order of the image in $A_f(\mathbf{C})$ of the modular symbol $\mathbf{e}_j$, so $n = 1$ if $j \notin \{1, k-1\}$. Then*

$$\frac{L(A_f, j)}{\Omega_j} \in \frac{1}{n}\mathbf{Z}.$$

Proof. Let x denote the image of $\mathbf{e}_j \in A_f(\mathbf{C})$, and set $I = \mathrm{Ann}(x) \subset \mathbf{T}$. Though we write $A_f(\mathbf{C})$ here and below, we will always work within the subgroup of $A_f(\mathbf{C})$ generated by the image of $\boldsymbol{\mathcal{M}}_k(N, \varepsilon; \mathbf{Z})$ under the period map.

First we check that the Hecke operators all act as scalars on x. Since f is a *newform*, the Hecke operators T_p, for $p \mid N$, act as 0 or $\pm p^{k/2-1}$ on f, and hence in the same way on $A_f(\mathbf{C})$ (see, e.g., the end of section 6 of [21]). If $p \nmid N$, Lemma 3.47 shows that $T_p(x) = (1+p^{k-1})x$.

Let $C = \mathbf{Z}x$ denote the cyclic subgroup of $A_f(\mathbf{C})$ generated by x, so n is the order of C. Since the Hecke operators act as scalars on C, we are pleased to find that there is an injection $\mathbf{T}/I \hookrightarrow C$ which sends T_p to $T_p(x)$.

Setting $\boldsymbol{\mathcal{S}} = \boldsymbol{\mathcal{S}}_k(N, \varepsilon; \mathbf{Z})$ and applying Theorem 3.41 we find that

$$\begin{aligned}
\pm\frac{L(A_f, j)}{\Omega_j} &= [\Theta_f(\boldsymbol{\mathcal{S}}^+) : \Theta_f(\mathbf{T}e)] \\
&= [\Theta_f(\boldsymbol{\mathcal{S}}^+) : \Theta_f(I\mathbf{e})] \cdot [\Theta_f(I\mathbf{e}) : \Theta_f(\mathbf{T}\mathbf{e})] \\
&= [\Theta_f(\boldsymbol{\mathcal{S}}^+) : I\Theta_f(\mathbf{e})] \cdot [I\Theta_f(\mathbf{e}) : \mathbf{T}\Theta_f(\mathbf{e})] \\
&= \frac{[\Theta_f(\boldsymbol{\mathcal{S}}^+) : I\Theta_f(\mathbf{e})]}{[\mathbf{T}\Theta_f(\mathbf{e}) : I\Theta_f(\mathbf{e})]}.
\end{aligned}$$

To conclude that

$$\frac{[\Theta_f(\boldsymbol{\mathcal{S}}^+) : I\Theta_f(\mathbf{e})]}{[\mathbf{T}\Theta_f(\mathbf{e}) : I\Theta_f(\mathbf{e})]} \in \frac{1}{n}\mathbf{Z}$$

we make two observations. By the construction of $A_f(\mathbf{C})$, the ideal I consists of those elements of $\mathbf{T}$ that send $\Theta_f(\mathbf{e})$ into $\Theta_f(\boldsymbol{\mathcal{S}}^+)$, so $[\Theta_f(\boldsymbol{\mathcal{S}}^+) : I\Theta_f(\mathbf{e})] \in \mathbf{Z}$. Second, there is a surjective map

$$\mathbf{T}/I \to \frac{\mathbf{T}\Theta_f(\mathbf{e})}{I\Theta_f(\mathbf{e})}$$

sending t to $t\Theta_f(\mathbf{e})$, so $[\mathbf{T}\Theta_f(\mathbf{e}) : I\Theta_f(\mathbf{e})]$ divides $n = \#C = \#(\mathbf{T}/I)$. □

Remark 3.49 (Historical notes). In the special case when $k = 2$, the modular symbol $\mathbf{e}_1$ corresponds to $(0)-(\infty) \in J_0(N)$. In this situation, Manin proves at the bottom of page 28 of [38] that $(0)-(\infty) \in J_0(N)(\mathbf{Q})$, and asserts in the footnote to [38, Cor. 3.6] that $(0)-(\infty)$ has finite order. Based on observations such as a special case of the above proposition, he declares: "These explicit formulas have the structure predicted by the Birch-Swinnerton-Dyer conjectures."

The main result of this section was inspired by a weaker result of Agashe, which can be found in Chapter 4 of [2]. Agashe considers only the case $k = 2$ and replaces n by the order of the subgroup of $J_0(N)(\overline{\mathbf{Q}})$ generated by *all* cusps.

3.11 The Manin constant

In this section $k = 2$ and $\varepsilon = 1$; we sometimes omit k and ε from the notation. The assumption that $k = 2$ will be essential, because we do not know how to define a Manin constant in other weights, let alone bound it.

Consider the optimal quotient A of $J_0(N)$ corresponding to a *newform* f on $\Gamma_0(N)$ of weight 2. Let I_A be the kernel of the natural map from the Hecke algebra to $\mathrm{End}(A)$. The *Manin constant* c_A of A is the lattice index

$$c_A := [S_2(\Gamma_0(N);\mathbf{Z})[I_A] : H^0(\mathcal{A}, \Omega_{\mathcal{A}/\mathbf{Z}})]$$

taken inside of $S_2(\Gamma_0(N);\mathbf{Q})$. Though, a priori, c_A is a rational number, the work of [31] implies that $c_A \in \mathbf{Z}$ (see, e.g., [3]).

Generalizing a theorem of Mazur, we prove that c_A is a unit in $\mathbf{Z}[\frac{1}{2m}]$, where m is the largest square dividing N. Essentially no new ideas beyond what Mazur used are involved. We then conjecture that $c_A = 1$, and give supporting numerical evidence.

For related results involving modular "building blocks" for $J_1(N)$, we refer the reader to [26, §4].

3.11.1 The primes that might divide c_A

In the special case $\dim A = 1$, the Manin constant is the classical Manin constant of A, and in [41] Mazur proved that c_A is a unit in $\mathbf{Z}[\frac{1}{2m}]$. We generalize his proof to obtain the analogous result in dimension greater than 1.

Theorem 3.50. *Let A be the new optimal quotient of $J_0(N)$ corresponding to a newform f. Then the Manin constant c_A is a unit in $\mathbf{Z}[\frac{1}{2m}]$, where m is the largest square dividing N.*

Proof. The reader is strongly recommended to keep the proof of Proposition 3.1 in [41] at hand while reading the following argument.

Let π denote the map $J_0(N) \to A$; let $\mathcal{A}$ denote the Néron model of A over $R := \mathbf{Z}[\frac{1}{2m}]$, and $\mathcal{J}$ the Néron model of $J_0(N)$ over R. Let $\mathcal{X}$ be the minimal proper regular model for $X_0(N)$ over R. As in Mazur's proof in [41], consider the diagram

$$H^0(\mathcal{A}, \Omega_{\mathcal{A}}) \xrightarrow{\pi^*} H^0(\mathcal{J}, \Omega_{\mathcal{J}}) \cong H^0(\mathcal{X}, \Omega^{\mathrm{reg}}_{\mathcal{X}}) \xrightarrow{q\text{-exp}} R[[q]]. \qquad (3.2)$$

(Note that "$\Omega^{\mathrm{reg}}_{\mathcal{X}}$" is not defined to be the usual sheaf of differentials; see, e.g., the discussion in [40, pg. 67].) The map π^* must be an inclusion, by [41, Cor. 1.1]. To show that the Manin constant is a unit in R, it suffices to check that the image of $H^0(\mathcal{A}, \Omega_{\mathcal{A}})$ in $R[[q]]$ is *saturated*, in the sense that the cokernel is torsion free; indeed, the image of $S_2(\Gamma_0(N);R)[I]$ is saturated and $S_2(\Gamma_0(N);R)[I] \otimes \mathbf{Q} = q\text{-exp}(\pi^*(H^0(\mathcal{A}, \Omega_{\mathcal{A}}))) \otimes \mathbf{Q}$.

For the image of $H^0(\mathcal{A},\Omega_{\mathcal{A}})$ in $R[[q]]$ to be saturated means that the quotient D is torsion free. Let ℓ be a prime not dividing $2m$; tensoring

$$0 \to H^0(\mathcal{A},\Omega_{\mathcal{A}}) \xrightarrow{q\text{-exp}} R[[q]] \to D \to 0$$

with $\mathbf{F}_\ell$ we obtain

$$0 \to D[\ell] \to H^0(\mathcal{A},\Omega_{\mathcal{A}}) \otimes \mathbf{F}_\ell \to \mathbf{F}_\ell[[q]] \to D \otimes \mathbf{F}_\ell \to 0.$$

Here we have used that $\mathrm{Tor}^1(D,\mathbf{F}_\ell)$ is the ℓ-torsion in D, and that $\mathrm{Tor}^1(-,\mathbf{F}_\ell)$ vanishes on the torsion-free group $R[[q]]$. (Alternatively, we could have used the snake lemma.) To show that $D[\ell]=0$, it suffices to prove that the map $\Psi : H^0(\mathcal{A},\Omega_{\mathcal{A}}) \otimes \mathbf{F}_\ell \to \mathbf{F}_\ell[[q]]$ is injective.

Since $\ell \neq 2$ and A is an optimal quotient, [41, Cor 1.1] gives an exact sequence

$$0 \to H^0(\mathcal{A}/\mathbf{Z}_\ell,\Omega_{\mathcal{A}/\mathbf{Z}_\ell}) \to H^0(\mathcal{J}/\mathbf{Z}_\ell,\Omega_{\mathcal{J}/\mathbf{Z}_\ell}) \to H^0(\mathcal{B}/\mathbf{Z}_\ell,\Omega_{\mathcal{B}/\mathbf{Z}_\ell}) \to 0$$

where $\mathcal{B}$ is the Néron model of $\ker(J \to A)$. In particular, $H^0(\mathcal{B}/\mathbf{Z}_\ell,\Omega_{\mathcal{B}/\mathbf{Z}_\ell})$ is torsion free, so

$$\begin{aligned} H^0(\mathcal{A}/\mathbf{Z}_\ell,\Omega_{\mathcal{A}/\mathbf{Z}_\ell}) \otimes \mathbf{F}_\ell \to H^0(\mathcal{J}/\mathbf{Z}_\ell,\Omega_{\mathcal{J}/\mathbf{Z}_\ell}) \otimes \mathbf{F}_\ell &\cong H^0(\mathcal{X}/\mathbf{Z}_\ell,\Omega^{\mathrm{reg}}_{\mathcal{X}/\mathbf{Z}_\ell}) \otimes \mathbf{F}_\ell \\ &\cong H^0(\mathcal{X}/\mathbf{F}_\ell,\Omega^{\mathrm{reg}}_{\mathcal{X}/\mathbf{F}_\ell}) \end{aligned}$$

is injective. (The last isomorphism is by [40, Prop. 3.3, pg. 68].) We also remark that

$$H^0(\mathcal{A},\Omega_{\mathcal{A}}) \otimes \mathbf{F}_\ell \cong H^0(\mathcal{A}/\mathbf{Z}_\ell,\Omega_{\mathcal{A}/\mathbf{Z}_\ell}) \otimes \mathbf{F}_\ell,$$

because $\mathbf{Z}_\ell$ is torsion free, hence flat over R. Thus the map

$$H^0(\mathcal{A},\Omega_{\mathcal{A}}) \otimes \mathbf{F}_\ell \to H^0(\mathcal{X}/\mathbf{F}_\ell,\Omega^{\mathrm{reg}}_{\mathcal{X}/\mathbf{F}_\ell})$$

is injective.

If $\ell \nmid N$, then injectivity of Ψ now follows from the q-expansion principle, which asserts that the q-expansion map $H^0(\mathcal{X}/\mathbf{F}_\ell,\Omega^{\mathrm{reg}}_{\mathcal{X}/\mathbf{F}_\ell}) \to \mathbf{F}_\ell[[q]]$ is injective.

Suppose ℓ does divide N, and let $\omega \in \ker(\Psi)$. Since $\ell \mid N$ and $\ell \nmid 2m$, we have that $\ell \,||\, N$; thus $\mathcal{X}/\mathbf{F}_\ell$ breaks up into a union of two irreducible components, and the q-expansion principle implies only that ω vanishes on the irreducible component containing the cusp ∞. However, since A is *new* and corresponds to a *single* eigenform, ω is an eigenvector for the involution W_N (since f and all of its conjugates are). Since W_N permutes the two components, ω must be 0 on all $\mathcal{X}/\mathbf{F}_\ell$. Therefore $\omega = 0$, and hence Ψ is injective. $\square$

3.11.2 Numerical evidence for the $c_A = 1$ conjecture

In the paper [24], the authors show that $c_A = 1$ for 28 two-dimensional optimal quotients of $J_0(N)$ (see Section 3.12.8). The non-square-free levels treated are:

$$N = 3^2\cdot 7,\quad 3^2\cdot 13,\quad 5^3,\quad 3^3\cdot 5,\quad 3\cdot 7^2,\quad 5^2\cdot 7,\quad 2^2\cdot 47,\quad 3^3\cdot 7.$$

In every case, $c_A = 1$.

Conjecture 3.51 (Agashe). *Let A be an optimal quotient of $J_0(N)$, and let c_A be the corresponding Manin constant. Then $c_A = 1$.*

3.12 Analytic invariants

Fix a newform

$$f = \sum_{n\geq 1} a_n q^n \in S_k(N, \varepsilon),$$

and assume that $\varepsilon^2 = 1$**.**

Remark 3.52. Our assumption that $\varepsilon^2 = 1$ does not imply that f has totally real Fourier coefficients. There is an eigenform in $S_2(24, \varepsilon)$ whose Fourier coefficients are not totally real, where ε is one of the characters of conductor 8.

Let $K_f = \mathbf{Q}(\ldots a_n \ldots)$ and let $f_1, \ldots, f_d$ be the Galois conjugates of f, where $d = [K_f : \mathbf{Q}]$. As in Section 2.7, we consider the complex torus A_f attached to f. In this section we describe how to compute the torus A_f and the special values at the critical integers $1, 2, \ldots, k-1$ of the L function $L(A_f, s)$ associated to A_f. (See 3.39 for the definition of $L(A_f, s)$.)

Let

$$f = \sum_{n\geq 1} a_n q^n \in M_k(N, \varepsilon)$$

be a modular form (we do not assume that f is an eigenform). We recall the integration pairing of Theorem 2.7:

$$\langle\, ,\, \rangle : M_k(N, \varepsilon) \times \boldsymbol{\mathcal{M}}_k(N, \varepsilon) \longrightarrow \mathbf{C}$$

$$\langle f, P\{\alpha, \beta\}\rangle = 2\pi i \int_\alpha^\beta f(z) P(z, 1) dz.$$

Let $I_f \subset \mathbf{T}$ be the kernel of the map $\mathbf{T} \to K_f$ sending T_n to a_n. The integration pairing gives rise to the period mapping

$$\Phi_f : \boldsymbol{\mathcal{M}}_k(N, \varepsilon) \to \mathrm{Hom}_{\mathbf{C}}(S_k(N, \varepsilon)[I_f], \mathbf{C}),$$

and $A_f = \mathrm{Hom}_{\mathbf{C}}(S_k(N, \varepsilon)[I_f], \mathbf{C})/\Phi_f(\boldsymbol{\mathcal{S}}_k(N, \varepsilon))$ is the cokernel.

3.12.1 Extended modular symbols

For the purposes of computing periods, it is advantageous to extend the notion of modular symbols to allows symbols of the form $P\{z, w\}$ where z and w are now arbitrary elements of $\mathfrak{h}^* = \mathfrak{h} \cup \mathbf{P}^1(\mathbf{Q})$. The free abelian group $\overline{\boldsymbol{\mathcal{M}}}_k$ of *extended modular symbols* is spanned by such symbols, and is of uncountable rank over $\mathbf{Z}$. However, it is still equipped with an action of $\Gamma_0(N)$ and we can form the largest torsion-free quotient $\overline{\boldsymbol{\mathcal{M}}}_k(N, \varepsilon)$ of $\overline{\boldsymbol{\mathcal{M}}}_k$ by the relations $\gamma x = \varepsilon(\gamma) x$ for $\gamma \in \Gamma_0(N)$.

The integration pairing extends to $\overline{\boldsymbol{\mathcal{M}}}_k(N, \varepsilon)$. There is a natural embedding $\iota : \boldsymbol{\mathcal{M}}_k(N, \varepsilon) \hookrightarrow \overline{\boldsymbol{\mathcal{M}}}_k(N, \varepsilon)$ which respects the pairing in the sense that $\langle f, \iota(x)\rangle = \langle f, x\rangle$. In many cases it is advantageous to replace $x \in \boldsymbol{\mathcal{M}}_k(N, \varepsilon)$ first by $\iota(x)$, and then by an equivalent sum $\sum y_i$ of symbols $y_i \in \overline{\boldsymbol{\mathcal{M}}}_k(N, \varepsilon)$. The period $\langle f, x\rangle$ is then replaced by the equivalent sum of periods $\sum \langle f, y_i\rangle$. The latter is frequently *much* easier to approximate numerically.

3.12.2 Numerically computing period integrals

Consider a point α in the upper half plane and any one of the (extended) modular symbols $X^mY^{k-2-m}\{\alpha,\infty\}$. Given a cusp form $g=\sum_{n\geq 1} b_nq^n \in S_k(N,\varepsilon)$ and an integer $m\in\{0,1,\dots,k-2\}$, we find that

$$\langle g,\, X^mY^{k-2-m}\{\alpha,\infty\}\rangle = 2\pi i\int_{\alpha}^{i\infty} g(z)z^m dz = 2\pi i \sum_{n=1}^{\infty} b_n \int_{\alpha}^{i\infty} e^{2\pi i n z} z^m dz. \tag{3.3}$$

The reversal of summation and integration is justified because the imaginary part of α is positive so that the sum converges absolutely. This is made explicit in the following lemma, which can be proved using repeated integration by parts.

Lemma 3.53.

$$\int_{\alpha}^{i\infty} e^{2\pi i n z} z^m dz \;=\; e^{2\pi i n\alpha} \sum_{s=0}^{m}\left(\frac{(-1)^s\alpha^{m-s}}{(2\pi i n)^{s+1}} \prod_{j=(m+1)-s}^{m} j\right). \tag{3.4}$$

The following proposition is the higher weight analogue of [16, Prop. 2.1.1(5)].

Proposition 3.54. *For any $\gamma\in\Gamma_0(N)$, $P\in V_{k-2}$ and $\alpha\in\mathfrak{h}^*$ the following holds:*

$$\begin{aligned} P\{\infty,\gamma(\infty)\} &= P\{\alpha,\gamma(\alpha)\} + (P-\varepsilon(\gamma)\gamma^{-1}P)\{\infty,\alpha\} && (3.5)\\ &= \varepsilon(\gamma)(\gamma^{-1}P)\{\alpha,\infty\} - P\{\gamma(\alpha),\infty\}. && (3.6)\end{aligned}$$

Proof. By definition, if $x\in\boldsymbol{\mathcal{M}}_k(N,\varepsilon)$ is a modular symbol and $\gamma\in\Gamma_0(N)$ then $\gamma x=\varepsilon(\gamma)x$; in particular, $\varepsilon(\gamma)\gamma^{-1}x = x$, so

$$\begin{aligned} P\{\infty,\gamma(\infty)\} &= P\{\infty,\alpha\} + P\{\alpha,\gamma(\alpha)\} + P\{\gamma(\alpha),\gamma(\infty)\}\\ &= P\{\infty,\alpha\} + P\{\alpha,\gamma(\alpha)\} + \varepsilon(\gamma)\gamma^{-1}(P\{\gamma(\alpha),\gamma(\infty)\})\\ &= P\{\infty,\alpha\} + P\{\alpha,\gamma(\alpha)\} + \varepsilon(\gamma)(\gamma^{-1}P)\{\alpha,\infty\}\\ &= P\{\alpha,\gamma(\alpha)\} + P\{\infty,\alpha\} - \varepsilon(\gamma)(\gamma^{-1}P)\{\infty,\alpha\}\\ &= P\{\alpha,\gamma(\alpha)\} + (P-\varepsilon(\gamma)\gamma^{-1}P)\{\infty,\alpha\}.\end{aligned}$$

The second equality in the statement of the proposition now follows easily. □

In the classical case of weight two and trivial character, the error term $(P-\varepsilon(\gamma)\gamma^{-1}P)\{\infty,\alpha\}$ vanishes. In general this term does not vanish, instead perturbing the analogues of the formulas found in [16, 2.10].

Algorithm 3.55. Given a triple $\gamma\in\Gamma_0(N)$, $P\in V_{k-2}$ and $g\in S_k(N,\varepsilon)$ (as a q-expansion to some precision) this algorithm computes the period integral $\langle g,\, P\{\infty,\gamma(\infty)\}\rangle$. Express γ as $\left(\begin{smallmatrix} a & b\\ cN & d\end{smallmatrix}\right)\in\Gamma_0(N)$ and take $\alpha=\frac{-d+i}{cN}$ in Proposition 3.54. Replacing γ by $-\gamma$ if necessary, we find that the imaginary parts of α and $\gamma(\alpha)=\frac{a+i}{cN}$ are both equal to $1/(cN)$ which is positive. Equation 3.3 and Lemma 3.53 can now be used to compute the period integrals of Proposition 3.54.

With the goal of computing period lattices in mind, it is reassuring to know that every element of $\boldsymbol{\mathcal{S}}_k(N,\varepsilon)$ can be written as a linear combination of symbols of the form $P\{\infty,\gamma(\infty)\}$. The author asked Helena Verrill if this is the case and she was eventually able to prove that it is; the proof is given below. In the special case of weight two and trivial character, this is the assertion, which was proved by Manin [38], that the group homomorphism $\Gamma_0(N) \to H_1(X_0(N),\mathbf{Z})$ sending γ to $\{0,\gamma(0)\}$ is surjective. When the weight is greater than two, we have not found any similar group-theoretic statement.

Proposition 3.56. *Any element of $\boldsymbol{\mathcal{S}}_k(N,\varepsilon)$ can be written in the form*

$$\sum_{i=1}^{n} P_i\{\infty,\gamma_i(\infty)\}$$

with $P_i \in V_{k-2}$ and $\gamma_i \in \Gamma_0(N)$. Moreover, P_i and γ_i can be chosen so that $\sum \varepsilon(\gamma_i)P_i = \sum \gamma_i^{-1}P_i$.

Proof.[1] First recall the definition of the spaces $\boldsymbol{\mathcal{M}}$, $\boldsymbol{\mathcal{M}}_k = V_{k-2}\otimes\boldsymbol{\mathcal{M}}$ and $\boldsymbol{\mathcal{M}}_k(N,\varepsilon) = \boldsymbol{\mathcal{M}}_k/I$ (see Section 2.1). Let $I = I_{N,\varepsilon}$ be the ideal in the group ring of $\Gamma_0(N)$ generated by all elements of the form $\varepsilon(\gamma)-\gamma$ for $\gamma\in\Gamma_0(N)$.

Suppose $v \in \boldsymbol{\mathcal{S}}_k(N,\varepsilon)$. Use the relation $\{\alpha,\beta\} = \{\infty,\beta\} - \{\infty,\alpha\} \in \boldsymbol{\mathcal{M}}$ to see that any v is the image of an element $\tilde{v} \in \boldsymbol{\mathcal{M}}_k$ of the form

$$\tilde{v} = \sum_{\beta\in\mathbf{Q}} P_\beta \otimes \{\infty,\beta\} \in \boldsymbol{\mathcal{M}}_k$$

with only finitely many P_β nonzero. The boundary map δ lifts in a natural way to $V_{k-2}\otimes\boldsymbol{\mathcal{M}}$, as illustrated.

$$\begin{tikzcd}
 & I(V_{k-2}\otimes\boldsymbol{\mathcal{M}}) \arrow[r] \arrow[d] & I(V_{k-2}\otimes\boldsymbol{\mathcal{B}}) \arrow[d] \\
 & V_{k-2}\otimes\boldsymbol{\mathcal{M}} \arrow[r, "\tilde{\delta}"] \arrow[d] & V_{k-2}\otimes\boldsymbol{\mathcal{B}} \arrow[d] \\
\boldsymbol{\mathcal{S}}_k(N,\varepsilon) \arrow[r, hook] & \boldsymbol{\mathcal{M}}_k(N,\varepsilon) \arrow[r, "\delta"] & \boldsymbol{\mathcal{B}}_k(N,\varepsilon)
\end{tikzcd}$$

Our assumption that $\delta(v)=0$ implies that $\tilde{\delta}(\tilde{v}) \in I(V_{k-2}\otimes\boldsymbol{\mathcal{B}})$. So there are $Q_{\gamma,\beta}\in V_{k-2}$, for $\gamma\in\Gamma_0(N)$ and $\beta\in\mathbf{P}^1(\mathbf{Q})$, only finitely many nonzero, such that

$$\tilde{\delta}(\tilde{v}) = \sum_{\gamma,\beta}(\varepsilon(\gamma)-\gamma)(Q_{\gamma,\beta}\otimes\{\beta\}).$$

[1] The author thanks Helena Verrill for permission to reproduce her proof here.

We now use a summation trick.

$$\begin{aligned}\sum_{\beta\in\mathbf{Q}}\tilde{\delta}(\tilde{v}) = P_\beta\otimes\{\beta\} - P_\beta\otimes\{\infty\} &= \sum_{\gamma,\beta}\varepsilon(\gamma)Q_{\gamma,\beta}\otimes\{\beta\} - (\gamma Q_{\gamma,\beta})\otimes\{\gamma\beta\}\\ &= \sum_{\gamma,\beta}\varepsilon(\gamma)Q_{\gamma,\beta}\otimes\{\beta\} - (\gamma Q_{\gamma,\gamma^{-1}\beta})\otimes\{\beta\}\\ &= \sum_{\gamma,\beta}\Big(\varepsilon(\gamma)Q_{\gamma,\beta} - \gamma Q_{\gamma,\gamma^{-1}\beta}\Big)\otimes\{\beta\}.\end{aligned}$$

Equating terms we deduce that for $\beta\neq\infty$,

$$P_\beta = \sum_\gamma \varepsilon(\gamma)Q_{\gamma,\beta} - \gamma Q_{\gamma,\gamma^{-1}\beta}.$$

Using this expression for P_β and that $\varepsilon(\gamma)\gamma^{-1}$ acts trivially on $\boldsymbol{\mathcal{M}}_k(N,\varepsilon)$ we find that

$$\begin{aligned}v = \sum_\beta P_\beta\{\infty,\beta\} &= \sum_{\gamma,\beta}\Big(\varepsilon(\gamma)Q_{\gamma,\beta} - \gamma Q_{\gamma,\gamma^{-1}\beta}\Big)\{\infty,\beta\}\\ &= \sum_{\gamma,\beta}\varepsilon(\gamma)Q_{\gamma,\beta} - \varepsilon(\gamma)\gamma^{-1}\Big(\gamma Q_{\gamma,\gamma^{-1}\beta}\Big)\{\infty,\beta\}\\ &= \sum_{\gamma,\beta}\varepsilon(\gamma)Q_{\gamma,\beta}\{\infty,\beta\} - \varepsilon(\gamma)Q_{\gamma,\gamma^{-1}\beta}\{\gamma^{-1}\infty,\gamma^{-1}\beta\}\\ &= \sum_{\gamma,\beta}\varepsilon(\gamma)Q_{\gamma,\beta}\{\infty,\beta\} - \varepsilon(\gamma)Q_{\gamma,\beta}\{\gamma^{-1}\infty,\beta\}\\ &= \sum_{\gamma,\beta}\varepsilon(\gamma)Q_{\gamma,\beta}\{\infty,\gamma^{-1}\infty\}.\end{aligned}$$

This is of the desired form. □

Unlike the case of weight two and trivial character, Proposition 3.56 does not give generators for $\boldsymbol{\mathcal{S}}_k(N,\varepsilon)$. This is because not every element of the form $P\{\infty,\gamma(\infty)\}$ must lie in $\boldsymbol{\mathcal{S}}_k(N,\varepsilon)$. However, if $\gamma P = P$ then $P\{\infty,\gamma(\infty)\}$ does lie in $\boldsymbol{\mathcal{S}}_k(N,\varepsilon)$. It would be interesting to know under what circumstances $\boldsymbol{\mathcal{S}}_k(N,\varepsilon)$ is generated by symbols of the form $P\{\infty,\gamma(\infty)\}$ with $\gamma P = P$. This sometimes fails for k odd; for example, when $k=3$ the condition $\gamma P = P$ implies that $\gamma\in\Gamma_0(N)$ has an eigenvector with eigenvalue 1, hence is of finite order. When k is even the author can see no obstruction to generating $\boldsymbol{\mathcal{S}}_k(N,\varepsilon)$ using such symbols.

3.12.3 The W_N-trick

In this section we assume that k is even. Consider the involution W_N defined in Section 2.4.3. This is an involution that acts on both modular symbols and modular forms. The follow proposition shows how to compute $\langle g, P\{\infty,\gamma(\infty)\}\rangle$ under certain restrictive assumptions. It generalizes the main result of [17] to higher weight. (Compare also [25].)

Proposition 3.57. *Let $g \in S_k(N,\varepsilon)$ be a cusp form which is an eigenform for the Atkin-Lehner involution W having eigenvalue $w \in \{\pm 1\}$. Then for any $\gamma \in \Gamma_0(N)$ and any $P \in V_{k-2}$, with the property that $\gamma P = \varepsilon(\gamma)P$, we have for any $\alpha \in \mathfrak{h}$ the following formula:*

$$\langle g, P\{\infty, \gamma(\infty)\}\rangle =$$

$$\langle g, w\frac{P(Y,-NX)}{N^{k/2-1}}\{W(\alpha),\infty\} + (P - w\frac{P(Y,-NX)}{N^{k/2-1}})\{i/\sqrt{N},\infty\} - P\{\gamma(\alpha),\infty\}\rangle.$$

Here $W(\alpha) = -1/(N\alpha)$.

Proof. By Proposition 3.54 our condition on P implies that $P\{\infty,\gamma(\infty)\} = P\{\alpha,\gamma(\alpha)\}$. The steps of the following computation are described below.

$$\begin{aligned}
&\langle g, P\{\alpha,\gamma(\alpha)\}\rangle\\
&\quad = \langle g, P\{\alpha, i/\sqrt{N}\} + P\{i/\sqrt{N}, W(\alpha)\} + P\{W(\alpha),\gamma(\alpha)\}\rangle\\
&\quad = \langle g, w\frac{W(P)}{N^{k/2-1}}\{W(\alpha), i/\sqrt{N}\} + P\{i/\sqrt{N}, W(\alpha)\} + P\{W(\alpha),\gamma(\alpha)\}\rangle\\
&\quad = \langle g, (w\frac{W(P)}{N^{k/2-1}} - P)\{W(\alpha), i/\sqrt{N}\} + P\{W(\alpha),\infty\} - P\{\gamma(\alpha),\infty\}\rangle\\
&\quad = \langle g, w\frac{W(P)}{N^{k/2-1}}\{W(\alpha),\infty\} + (P - w\frac{W(P)}{N^{k/2-1}})\{i/\sqrt{N},\infty\} - P\{\gamma(\alpha),\infty\}\rangle.
\end{aligned}$$

For the first step, we break the path into three paths. In the second step, we apply the W-involution to the first term, and use that the action of W is compatible with the pairing $\langle\,,\rangle$. The third step involves combining the first two terms and breaking up the third. In the final step, we replace $\{W(\alpha), i/\sqrt{N}\}$ by $\{W(\alpha),\infty\} + \{\infty, i/\sqrt{N}\}$ and regroup. $\square$

A good choice for α is $\alpha = \gamma^{-1}\left(\frac{b}{d} + \frac{i}{d\sqrt{N}}\right)$, so that $W(\alpha) = \frac{c}{d} + \frac{i}{d\sqrt{N}}$. This maximizes the minimum of the imaginary parts of α and $W(\alpha)$.

Let $\gamma = \left(\begin{smallmatrix} a & b \\ c & d\end{smallmatrix}\right) \in \Gamma_0(N)$. A polynomial P for which $\gamma(P) = P$ is given by

$$P(X,Y) = (cX^2 + (d-a)XY - bY^2)^{\frac{k-2}{2}}.$$

This formula was obtained by viewing V_{k-2} as the $(k-2)$th symmetric product of the two-dimensional space on which $\Gamma_0(N)$ acts naturally. For example, observe that since $\det(\gamma) = 1$ the symmetric product of two eigenvectors for γ is an eigenvector in V_2 having eigenvalue 1. For the same reason, if $\varepsilon(\gamma) \neq 1$, there is often no polynomial $P(X,Y)$ such that $\gamma(P) = \varepsilon(\gamma)P$. When this is the case, first choose γ so that $\varepsilon(\gamma) = 1$.

Since the imaginary parts of the terms $i/\sqrt{N}$, α and $W(\alpha)$ in the proposition are all relatively large, the sums appearing in Equation 3.3 converge quickly if d is small. Let us emphasize, that *it is* **extremely** *important to choose γ in Proposition 3.57 with d small, otherwise the series will converge* very *slowly.*

3.12.4 Computing the period mapping

Let $I \subset \mathbf{T}$ be the kernel of the map $\mathbf{T} \to K_f$ sending T_n to a_n. As in Section 3.7, let $\Theta_f = \Theta_I$ be the rational period mapping associated to f. We have a commutative diagram

$$\begin{tikzcd}[column sep=small]
\boldsymbol{\mathcal{M}}_k(N,\varepsilon) \arrow[rr, "\Phi_f"] \arrow[dr, "\Theta_f"'] & & \mathrm{Hom}_{\mathbf{C}}(S_k(N,\varepsilon)[I], \mathbf{C}) \\
& \dfrac{\boldsymbol{\mathcal{M}}_k(N,\varepsilon)}{\ker(\Phi_f)} \arrow[ur, "i_f"'] &
\end{tikzcd}$$

Using Algorithm 3.26, we can compute Θ_f so to compute Φ_f we need to compute i_f. Let $g_1, \ldots, g_d$ be a basis for the $\mathbf{Q}$-vector space $S_k(N, \varepsilon; \mathbf{Q})[I]$. We will compute the period mapping with respect to the basis of $\mathrm{Hom}_{\mathbf{Q}}(S_k(N, \varepsilon; \mathbf{Q})[I], \mathbf{C})$ dual to this basis. Choose elements $x_1, \ldots, x_d \in \boldsymbol{\mathcal{M}}_k(N, \varepsilon)$ with the following properties:

1. Using Proposition 3.54 or Proposition 3.57 it is possible to compute the period integrals $\langle g_i, x_j\rangle$, $i, j \in \{1, \ldots d\}$ efficiently.
2. The $2d$ elements $v + *v$ and $v - *v$ for $v = \Theta_f(x_1), \ldots, \Theta_f(x_d)$ span a space of dimension $2d$.

Given this data, we can compute

$$i_f(v + *v) = 2\mathrm{Re}(\langle g_1, x_i\rangle, \ldots, \langle g_d, x_i\rangle)$$

and

$$i_f(v - *v) = 2i\mathrm{Im}(\langle g_1, x_i\rangle, \ldots, \langle g_d, x_i\rangle).$$

We break the integrals into real and imaginary parts because this increases the precision of our answers. Since the vectors $v_n + *v_n$ and $v_n - *v_n$, $n = 1, \ldots, d$ span $\frac{\boldsymbol{\mathcal{M}}_k(N,\varepsilon)}{\ker(\Phi_f)}$ we have computed i_f.

It is advantageous when possible to find symbols x_i satisfying the conditions of Proposition 3.57. This is usually possible when d is very small, but in practice we have had problems doing this when d is large, for example with **131k2B**, in which case the dimension is 10.

3.12.5 Computing special values

For $s = 1, \ldots, k-1$ we have

$$L(f,s) = \frac{-2\pi^{s-1} i^{s-1}}{(s-1)!} \cdot \langle f, X^{s-1} Y^{k-1-s}\{0,\infty\}\rangle, \tag{3.7}$$

$$L(A_I, s) = \prod_{i=1}^{d} L(f_i, s). \tag{3.8}$$

Let

$$\mathbf{e}_i := X^{i-1}\{0, \infty\}$$

denote the ith *winding element*. In section 3.12.4 we computed the period map Φ_f with respect to a basis $g_1, \ldots, g_d$ for $S_k(N, \varepsilon; \mathbf{Q})[I]$. Upon writing f as a K_f-linear combination $\alpha_1 g_1 + \cdots + \alpha_d g_d$ we find that

$$\begin{aligned} \langle f, \mathbf{e}_i \rangle &= \langle \alpha_1 g_1 + \cdots + \alpha_d g_d, \mathbf{e}_i \rangle \\ &= \alpha_1 \langle g_1, \mathbf{e}_i \rangle + \cdots + \alpha_d \langle g_d, \mathbf{e}_i \rangle \\ &= \alpha_1 \Phi_f(\mathbf{e}_i)_1 + \cdots + \alpha_d \Phi_f(\mathbf{e}_i)_d \end{aligned}$$

Here $\Phi_f(\mathbf{e}_i)_j$ denotes the jth coordinate of $\Phi_f(\mathbf{e}_i)$. Finally using Equation 3.7 we compute the special value.

3.12.6 The real and minus volume associated to A_f

Fix a choice of basis $g_1, \ldots, g_d$ for the free $\mathbf{Z}$-module $S_k(N, \varepsilon; \mathbf{Z})[I]$, where I is the annihilator in the Hecke algebra of our fixed newform f.

For any $x \in \boldsymbol{\mathcal{S}}_k(N, \varepsilon)$ we have, by Proposition 2.11,

$$\begin{aligned} \overline{\Phi_f(x)} &= (\overline{\langle g_1, x \rangle}, \ldots, \overline{\langle g_d, x \rangle}) \\ &= (\langle g_1^*, x^* \rangle, \ldots, \langle g_d^*, x^* \rangle) \\ &= (\langle g_1, x^* \rangle, \ldots, \langle g_d, x^* \rangle) \in \Phi_f(\boldsymbol{\mathcal{S}}_k(N, \varepsilon)), \end{aligned}$$

so complex conjugation leaves invariant the period lattice

$$\Lambda_f = \Phi_f(\boldsymbol{\mathcal{S}}_k(N, \varepsilon)) \subset \mathrm{Hom}_{\mathbf{C}}(S_k(N, \varepsilon)[I], \mathbf{C}).$$

Fix a $\mathbf{Z}$-basis for $S_k(N, \varepsilon; \mathbf{Z})[I]$, thus making an identification $\mathrm{Hom}_{\mathbf{C}}(S_k(N, \varepsilon)[I], \mathbf{C}) \cong \mathbf{C}^d$. The above observation implies that $A_f(\mathbf{C}) \cong \mathbf{C}^d / \Lambda_f$ is equipped with an action of complex conjugation. Our choice of basis defines a real-valued measure μ on $A_f(\mathbf{C})$, coming from the standard measure on $\mathbf{C}^d$. The measure does not depend on the choice of $\mathbf{Z}$-basis.

Definition 3.58 (Real and minus volume). The *real measure* Ω_f^+ is the measure $\mu(A_f(\mathbf{R}))$. The *minus measure* Ω_f^- is the measure $\mu(A_f(\mathbf{C})^-)$ times i^d, where $A_f(\mathbf{C})^-$ is the set of points in $A_f(\mathbf{C})$ on which complex conjugation acts as -1.

Thus, in connection with Section 3.10.3, $|\Omega_f^+| = |\Omega_1|$ and $|\Omega_f^-| = |\Omega_2|$.

Algorithm 3.59. To compute Ω_f^+ and Ω_f^-, proceed as follows. Using Algorithm 3.26, compute $\boldsymbol{\mathcal{S}}_k(N, \varepsilon)/\mathrm{Ker}(\Phi_f)$. Next, compute a basis for the kernel $(\boldsymbol{\mathcal{S}}_k(N, \varepsilon)/\mathrm{Ker}(\Phi_f))^+$ of the map induced by the $*$-involution. Using Section 3.12.4 compute the image of this basis under i_f; this is a basis for Λ_f^+. The determinant of this latter basis then gives the measure $(\Omega_f^+)^0$ of the identity component $A_f(\mathbf{R})^0$ of $A_f(\mathbf{R})$. Finally $\Omega_f^+ = c_\infty^+ \cdot (\Omega_f^+)^0$, where the number c_∞^+ of real components can be computed using the algorithm in Section 3.12.7

Remark 3.60 (Alternative method). Suppose s is an integer in the set $\{1, \ldots, k-1\}$, and let $\sigma = +$ or $\sigma = -$, depending on whether s is odd or even, respectively. Section 3.10 contains a formula for the ratio $L(A_f, s)/\Omega_f^\sigma$. When this ratio is nonzero, Ω_f^σ can be determined by computing $L(A_f, s)/\Omega_f^\sigma$ and $L(A_f, s)$, using Section 3.12.5.

Remark 3.61. When $k = 2$ and ε is trivial, A_f has the structure of abelian variety over $\mathbf{Q}$. The quantity Ω_f^+ above is related to the quantity Ω_A appearing in the Birch and Swinnerton-Dyer conjecture [67] for A_f. The latter quantity is the measure of $A_f(\mathbf{R})$ with respect to a basis of integral differentials on the Néron model of A_f over $\mathrm{Spec}(\mathbf{Z})$. The two quantities are related by the Manin constant, which the author conjectures is always 1 (see Section 3.11).

3.12.7 The component groups c_∞^+ and c_∞^-

Assume in this section that f has *totally real* Fourier coefficients and continue to assume that $\varepsilon^2 = 1$.

Definition 3.62. Let c_∞^+ be the number of components of the topological space $A_f(\mathbf{R})$. Let c_∞^- be the number of components of $A_f(\mathbf{C})^-$, where $A_f(\mathbf{C})^-$ is the set of points $z \in A_f(\mathbf{C})$ such that $\overline{z} = -z$.

Proposition 3.63. *Let $\overline{C}$ be the map induced by complex conjugation on $\Lambda_f/2\Lambda_f = \Lambda_f \otimes \mathbf{F}_2$. Then*

$$c_\infty^+ = c_\infty^- = 2^{\dim(\ker(\overline{C}-1))-d},$$

where d is the dimension of A_f.

Proof. We must compute the order of the component group

$$\Psi = \frac{A_f(\mathbf{R})}{A_f(\mathbf{R})^0} = \frac{(\mathbf{C}^d/\Lambda_f)^+}{\mathbf{R}^d/\Lambda_f^+},$$

where $\mathbf{R}^d/\Lambda_f^+$ is the identity component because it is the continuous image of the connected set $\mathbf{R}^d$. For $v \in \mathbf{C}^d$ denote by $\overline{v}$ its complex conjugate and by $[v]$ its image in $\mathbf{C}^d/\Lambda_f$. Suppose $[v] \in (\mathbf{C}^d/\Lambda_f)^+$; this means that $[v] = [\overline{v}]$, so since $v + \overline{v} \in \mathbf{R}^d$ we have

$$2[v] = [v] + [\overline{v}] \in \mathbf{R}^d/\Lambda_f^+,$$

so Ψ is annihilated by 2. Thus there is $\lambda \in \Lambda_f$ so that $2v + \lambda \in \mathbf{R}^d$, and so $v + \frac{1}{2}\lambda \in \mathbf{R}^d$, i.e., v can be written as an element of $\frac{1}{2}\Lambda_f$ plus an element of $\mathbf{R}^d$. This means that Ψ is generated by the image of $(\frac{1}{2}\Lambda_f/\Lambda_f)^+$. Thus

$$\Psi \cong \frac{(\frac{1}{2}\Lambda_f/\Lambda_f)^+}{(\frac{1}{2}\Lambda_f \cap \mathbf{R}^d)/\Lambda_f^+} \cong \frac{(\Lambda_f/2\Lambda_f)^+}{\Lambda_f^+/2\Lambda_f^+}$$

Consequently

$$\dim_{\mathbf{F}_2} \Psi = \dim(\Lambda_f/2\Lambda_f)^+ - \dim \Lambda_f^+/2\Lambda_f^+ = \dim(\ker(\overline{C}-1)) - d.$$

Here $\Lambda_f^+/2\Lambda_f^+$ has dimension d because Λ_f^+ is a lattice in $\mathbf{R}^d$, hence a free $\mathbf{Z}$-module of rank d.

The argument for c_∞^- proceeds in the same way, and results in the same answer because

$$\dim(\ker(\overline{C}-1)) = \dim(\ker(\overline{C}+1)).$$

□

To compute C on Λ_f, use Algorithm 3.26 to compute the action of $*$ on

$$\boldsymbol{\mathcal{S}}_k(N,\varepsilon)/\operatorname{Ker}(\Phi_f) \cong \Lambda_f.$$

3.12.8 Examples

Jacobians of genus-two curves

The author is among the the six authors of [24], who gather empirical evidence for the BSD conjecture for Jacobian of genus two curves. Of the 32 Jacobians considered, all but four are optimal quotients of $J_0(N)$ for some N. The methods of this section can be used to compute Ω_f^+ for the Jacobians of these 28 curves. Using explicit models for the genus two curves, the authors of [24] computed the measure of A with respect to a basis for the Néron differentials of A. In all 28 cases our answers agreed to the precision computed. Thus in these cases we have numerically verified that the Manin constant equals 1.

The first example considered in [24] is the Jacobian $A = J_0(23)$ of the modular curve $X_0(23)$. This curve has as a model

$$y^2 + (x^3 + x + 1)y = -2x^5 - 3x^2 + 2x - 2$$

from which one can compute the BSD $\Omega_A = 2.7328....$ The following is an integral basis of cusp forms for $S_2(23)$.

$$\begin{aligned} g_1 &= q - q^3 - q^4 - 2q^6 + 2q^7 + \cdots \\ g_2 &= q^2 - 2q^3 - q^4 + 2q^5 + q^6 + 2q^7 + \cdots \end{aligned}$$

The space $\boldsymbol{\mathcal{M}}_2(23;\mathbf{Q})$ of modular symbols has dimension five and is spanned by $\{-1/19, 0\}$, $\{-1/17, 0\}$, $\{-1/15, 0\}$, $\{-1/11, 0\}$ and $\{\infty, 0\}$. The submodule $\boldsymbol{\mathcal{S}}_2(23;\mathbf{Z})$ has rank four and has as basis the first four of the above five symbols. Choose $\gamma_1 = \left(\begin{smallmatrix} 8 & 1 \\ 23 & 3 \end{smallmatrix}\right)$ and $\gamma_2 = \left(\begin{smallmatrix} 6 & 1 \\ 23 & 4 \end{smallmatrix}\right)$ and let $x_i = \{\infty, \gamma_i(\infty)\}$. Using the W_N-trick (see Section 3.12.3) we compute the period integrals $\langle g_i, x_j\rangle$ using 97 terms of the q-expansions of g_1 and g_2, and obtain

$$\begin{aligned} \langle g_1, x_1\rangle &\sim -1.3543 + 1.0838i, & \langle g_1, x_2\rangle &\sim -0.5915 + 1.6875i \\ \langle g_2, x_1\rangle &\sim -0.5915 - 0.4801i, & \langle g_2, x_2\rangle &\sim -0.7628 + 0.6037i \end{aligned}$$

Using 97 terms we already obtain about 14 decimal digits of accuracy, but we do not reproduce them all here. We next find that

$$\langle g_1, x_1 + x_1^*\rangle \sim 2\mathrm{Re}(-1.3543 + 1.0838i) = 2.7086,$$

and so on. Upon writing each generator of $\boldsymbol{\mathcal{S}}_2(23)$ in terms of $x_1 + x_1^*$, $x_1 - x_1^*$, $x_2 + x_2^*$ and $x_2 - x_2^*$ we discover that the period mapping with respect to the basis dual to g_1 and g_2 is (approximately)

$$\begin{aligned} \{-1/19, 0\} &\mapsto (\ \ 0.5915 - 1.6875i, & 0.7628 - 0.6037i) \\ \{-1/17, 0\} &\mapsto (-0.5915 - 1.6875i, & -0.7628 - 0.6037i) \\ \{-1/15, 0\} &\mapsto (-1.3543 - 1.0838i, & -0.5915 + 0.4801i) \\ \{-1/11, 0\} &\mapsto (-1.5256, & 0.3425) \end{aligned}$$

Working in $\boldsymbol{\mathcal{S}}_2(23)$ we find $\boldsymbol{\mathcal{S}}_2(23)^+$ is spanned by $\{-1/19, 0\} - \{-1/17, 0\}$ and $\{-1/11, 0\}$. Using the algorithm of Section 3.12.6, we find that there is only one real component so

$$\Omega_I^+ \sim \begin{vmatrix} 1.1831 & 1.5256 \\ -1.5256 & 0.3425 \end{vmatrix} = 2.7327...$$

To greater precision we find that $\Omega_f^+ \sim 2.7327505324965$. This agrees with the value in [24]; since the Manin constant is an integer, it must equal 1.

Table 3.1: Volumes associated to level one cusp forms.

k	Ω^+	Ω^-
12	0.002281474899	$0.000971088287i$
16	0.003927981492	$0.000566379403i$
18	0.000286607497	$0.023020042428i$
20	0.008297636952	$0.0005609325015i$
22	0.002589288079	$0.0020245743816i$
24	0.000000002968	$0.0000000054322i$
26	0.003377464512	$0.3910726132671i$
28	0.000000015627	$0.0000000029272i$

Level one cusp forms

In the following two sections we consider several specific examples of tori attached to modular forms of weight greater than two.

Let $k \geq 12$ be an even integer. Associated to each Galois conjugacy class of normalized eigenforms f, there is a torus A_f over $\mathbf{R}$. The real and minus volume of the first few of these tori are displayed in Table 3.1. For weights 24 and 28 we give Ω^-/i so that the columns will line up nicely. In each case, 97 terms of the q-expansion were used.

The volumes appear to be *much* smaller than the volumes of weight two abelian varieties. The dimension of each A_f is 1, except for weights 24 and 28 when the dimension is 2.

CM elliptic curves of weight greater than two

Let f be a rational newform with “complex multiplication”, in the sense that “half” of the Fourier coefficients of f are zero. For our purposes, it is not necessary to define complex multiplication any more precisely. Experimentally, it appears that the associated elliptic A_f has rational j-invariant. As evidence for this we present Table 3.2, which includes the analytic data about every rational CM form of weight four and level ≤ 197. The computations of Table 3.2 were done using at least 97 terms of the q-expansion of f. The rationality of j could probably be proved by observing that the CM forces A_f to have extra automorphisms.

In these examples, the invariants c_4 and c_6 are unrecognizable to the author; in contrast, in weight 2 these invariants are (expected to be) integers (see [16, 2.14]).

Some abelian varieties of large dimension

In Table 3.3, we give the volumes of five abelian varieties of dimension greater than 1. In each case, at least 200 terms of the q-expansions were used.

Table 3.2: CM elliptic curves of weight > 2.

E	j	Ω^+	Ω^-	c_4	c_6
9k4A	0	0.2095	$0.1210i$	0.0000	-56626421686.2951
32k4A	1728	0.2283	$0.2283i$	-3339814.8874	0.0000
64k4D	1728	0.1614	$0.1614i$	53437038.1988	0.0000
108k4A	0	0.0440	$0.0762i$	-14699.2655	24463608892439.7456
108k4C	0	0.0554	$0.0960i$	1608.7743	6115643810955.1724
121k4A	-2^{15}	0.0116	$0.0385i$	85659519816.8841	25723073306989527.1216
144k4E	0	0.0454	$0.0262i$	81.1130	-549788016394046.1396
27k6A	0	0.0110	$0.0191i$	0.0000	97856189971744203.7795
32k6A	1728	0.0199	$0.0199i$	-58095643136.7658	8.0094

Table 3.3: Volumes of higher dimensional abelian varieties.

A	dim	Ω^+	Ω^-
79k2B	5	10	$209i$
83k2B	6	22	41
131k2B	10	51	615
11k4A	2	0.0815	0.0212
17k4B	3	0.0047	$0.0007i$

Chapter 4

Component groups of optimal quotients

Let A be an abelian variety over the rational numbers $\mathbf{Q}$. The Birch and Swinnerton-Dyer conjecture supplies a formula for the order of the Shafarevich-Tate group of A. A key step in computing this order is to find each of the Tamagawa numbers c_p of A. The Tamagawa numbers are defined as follows, where the definition of Néron model and component group is given below.

Definition 4.1 (Tamagawa number). Let p be a prime, let $\mathcal{A}$ be a Néron model of A over the p-adic integers $\mathbf{Z}_p$, and let $\Phi_{A,p}$ be the component group of $\mathcal{A}$ at p. Then the *Tamagawa number* c_p of A is the order of the group $\Phi_{A,p}(\mathbf{F}_p)$ of $\mathbf{F}_p$-rational points of $\Phi_{A,p}(\overline{\mathbf{F}}_p)$.

Remark 4.2. We warn the reader that the Tamagawa number is defined in a different way in some other papers. The definitions are equivalent.

In this chapter we present a method for computing the Tamagawa numbers c_p, up to a power of 2, under the hypothesis that A has purely toric reduction at p. Such A are plentiful among the modular abelian varieties; for example, if A is a new optimal quotient of $J_0(N)$ and p exactly divides N, then A is purely toric at p.

In Sections 4.1–4.5 we state and prove an explicit formula involving component groups of fairly general abelian varieties. Then in Section 4.6 we turn to quotients of modular Jacobians $J_0(N)$. We give several tables and issue a conjecture and a question.

The results of this chapter were inspired by a letter that Ribet wrote to Mestre, in which he treats the case when A is an elliptic curve.

4.1 Main results

4.1.1 Néron models and component groups

Let A be an abelian variety over a finite extension K of the p-adic numbers $\mathbf{Q}_p$. Let $\mathcal{O}$ be the ring of integers of K, let $\mathfrak{m}$ be its maximal ideal, and let $k = \mathcal{O}/\mathfrak{m}$ be the residue class field.

Definition 4.3 (Néron model). A *Néron model* of A is a smooth commutative group scheme $\mathcal{A}$ over $\mathcal{O}$ such that A is its generic fiber and $\mathcal{A}$ satisfies the Néron mapping property: the restriction map

$$\mathrm{Hom}_{\mathcal{O}}(S, \mathcal{A}) \longrightarrow \mathrm{Hom}_K(S_K, A)$$

is bijective for all *smooth* schemes S over $\mathcal{O}$.

The Néron mapping property implies that $\mathcal{A}$ is unique up to a unique isomorphism, so we will refer without hesitation to "the" Néron model of A.

The closed fiber $\mathcal{A}_k$ of $\mathcal{A}$ is a group scheme over k, which need not be connected; denote by $\mathcal{A}_k^0$ the connected component containing the identity. There is an exact sequence

$$0 \longrightarrow \mathcal{A}_k^0 \longrightarrow \mathcal{A}_k \longrightarrow \Phi_A \longrightarrow 0,$$

where Φ_A a finite étale group scheme over k. Equivalently, Φ_A may be viewed as a finite abelian group equipped with an action of $\mathrm{Gal}(\overline{k}/k)$.

Definition 4.4 (Component group). The *component group* of an abelian variety $\mathcal{A}$ over a local field K is the group scheme $\Phi_A = A_k/A_k^0$ defined above.

4.1.2 Motivating problem

This chapter is motivated by the problem of computing the groups $\Phi_{A,p}$ attached to quotients A of Jacobians of modular curves $X_0(N)$. When A has semistable reduction, Grothendieck and Mumford described the component group in terms of a monodromy pairing on certain free abelian groups. When $A = J = J_0(N)$ is the Jacobian of $X_0(N)$, this pairing can be explicitly computed, hence the component group Φ_J can also be computed; this has been done in many cases in [40] and [23].

Suppose now that $A = A_f$ is an optimal quotient of $J_0(N)$ that is attached to a newform f, so that the kernel of the map $\pi : J \to A$ is connected. There is a natural map $\pi_* : \Phi_J \to \Phi_A$. We wish to compute the image and the order of the cokernel of π_*.

4.1.3 The main result

We now state our main result more precisely, necessarily supressing some of the definitions of the terms used until later. Suppose $\pi : J \to A$ is an optimal quotient, with J a Jacobian with semistable reduction and A having purely toric reduction. We express the component group of A in terms of the monodromy pairing associated to J.

Let $m_A = \sqrt{\deg(\theta_A)}$, where $\theta_A : A^\vee \to A$ is induced by the canonical principal polarization of J arising from the θ-divisor. Let X_J be the character group of the toric part of the closed fiber of the Néron model of J. Let $\mathcal{L}$ be the saturation of the image of X_A in X_J. The monodromy pairing induces a map $\alpha : X_J \to \mathrm{Hom}(\mathcal{L}, \mathbf{Z})$. Let Φ_X be the cokernel of α and $m_X = [\alpha(X_J) : \alpha(\mathcal{L})]$ be the order of the finite group $\alpha(X_J)/\alpha(\mathcal{L})$. We obtain the equality

$$\frac{\#\Phi_A}{m_A} = \frac{\#\Phi_X}{m_X}.$$

Using the snake lemma, one see that Φ_X is isomorphic to the image of the natural map $\Phi_J \to \Phi_A$, and the above formula implies that the cokernel of the map $\Phi_J \to \Phi_A$ has order m_A/m_X.

If the optimal quotient $J \to A$ arises from a modular form on $\Gamma_0(N)$, then the quantities m_A, m_X and Φ_X can be explicitly computed, hence we can compute $\#\Phi_A$.

4.2 Optimal quotients of Jacobians

Let J be a Jacobian, and let θ_J be the canonical principal polarization arising from the θ-divisor. Recall that an *optimal quotient* of J is an abelian variety A and a surjective map $\pi : J \to A$ whose kernel is an abelian subvariety B of J. Denote by $J^\vee$ and $A^\vee$ the abelian varieties dual to J and A, respectively. Upon composing the dual of π with $\theta_J^\vee = \theta_J$, we obtain a map

$$A^\vee \xrightarrow{\pi^\vee} J^\vee \xrightarrow{\theta_J} J.$$

Proposition 4.5. *The map $A^\vee \to J$ is injective.*

Proof. Since θ_J is an isomorphism it suffices to prove that $\pi^\vee$ is injective. Since the dual of $\pi^\vee$ is $(\pi^\vee)^\vee = \pi$ and π is surjective, the map $\pi^\vee$ must have finite kernel. Thus $A^\vee \to C = \mathrm{im}(\pi^\vee)$ is an isogeny. Let G denote the kernel of this isogeny, and dualize. By [50, §11] we have the following two commutative diagrams:

$$\begin{tikzcd} G \arrow[r] & A^\vee \arrow[r, two heads] \arrow[dr, "\pi^\vee"'] & C \arrow[d] \\ & & J^\vee \end{tikzcd} \quad \xrightarrow{\text{dualize}} \quad \begin{tikzcd} A & C^\vee \arrow[l] & G^\vee \arrow[l] \\ & J, \arrow[ul, "\pi"] \arrow[u, "\varphi"'] & \end{tikzcd}$$

where $G^\vee$ is the Cartier dual of G. Since $G^\vee$ is finite, $\ker(\varphi)$ is of finite index in $\ker(\pi)$. Since $\ker(\pi)$ is an abelian variety, as a group it is divisible. But a divisible group has no nontrivial finite-index subgroups (divisibility is a property inherited by quotients, and nonzero finite groups are not divisible). Thus $\ker(\varphi) = \ker(\pi)$, so $G^\vee = 0$. It follows that $G = 0$. ☐

Henceforth we will abuse notation and denote the injection $A^\vee \to J$ by $\pi^\vee$. The kernel of θ_A equals the intersection of $A^\vee$ and $B = \ker(\pi)$, as depicted in the following diagram:

$$\begin{tikzcd} A^\vee \cap B \arrow[r] \arrow[d] & B \arrow[d] \\ A^\vee \arrow[r, hook, "\pi^\vee"] \arrow[dr, "\theta_A"'] & J \arrow[d, "\pi"] \\ & A. \end{tikzcd}$$

Since θ_A is a polarization, the degree $\#\ker(\theta_A)$ of θ_A is a perfect square (see [50, Thm. 13.3]). Recall that the *modular degree* is the integer

$$m_A = \sqrt{\#\ker(\theta_A)}.$$

For an algorithm to compute m_A, see Section 3.9 and Corollary 4.23.

4.3 The closed fiber of the Néron model

Let K be a finite extension of $\mathbf{Q}_p$ with ring of integers $\mathcal{O}$ and residue class field k. Let A be an abelian variety over K and denote its Néron model by $\mathcal{A}$. Let Φ_A be the group of connected components of the closed fiber $\mathcal{A}_k$. This group is a finite étale group scheme over k; equivalently, it is a finite abelian group equipped with an action of $\mathrm{Gal}(\overline{k}/k)$. There is an exact sequence of group schemes

$$0 \to \mathcal{A}_k^0 \to \mathcal{A}_k \to \Phi_A \to 0.$$

The group scheme $\mathcal{A}_k^0$ is an extension of an abelian variety $\mathcal{B}$ of some dimension a by a group scheme $\mathcal{C}$; we have a diagram

$$\begin{array}{ccccccccc} & & 0 & & & & & & \\ & & \downarrow & & & & & & \\ & & \mathcal{T} & & & & & & \\ & & \downarrow & & & & & & \\ 0 & \to & \mathcal{C} & \to & \mathcal{A}_k^0 & \to & \mathcal{B} & \to & 0 \\ & & \downarrow & & & & & & \\ & & \mathcal{U} & & & & & & \\ & & \downarrow & & & & & & \\ & & 0 & & & & & & \end{array}$$

with $\mathcal{T}$ a torus of dimension t and $\mathcal{U}$ a unipotent group of dimension u. The abelian variety A is said to have *purely toric reduction* if $t = \dim A$, and have *semistable reduction* if $u = 0$.

Definition 4.6 (Character group of torus). The *character group*

$$X_A = \mathrm{Hom}_{\overline{k}}(\mathcal{T}_{/\overline{k}}, \mathbf{G}_{m/\overline{k}})$$

is a free abelian group of rank t contravariantly associated to A.

As discussed in, e.g., [53], if A is semistable there is a *monodromy pairing* $X_A \times X_{A^\vee} \to \mathbf{Z}$ and an exact sequence

$$0 \to X_{A^\vee} \to \mathrm{Hom}(X_A, \mathbf{Z}) \to \Phi_A \to 0.$$

4.4 Rigid uniformization

In this section we review the rigid analytic uniformization of a semistable abelian variety over a finite extension K of the maximal unramified extension $\mathbf{Q}_p^{\mathrm{ur}}$ of $\mathbf{Q}_p$. We use this uniformization to prove that if A has purely toric reduction, and $\phi : A^\vee \to A$ is a symmetric isogeny (as defined below), then

$$\deg(\phi) = (\#\,\mathrm{coker}(X_A \to X_{A^\vee}))^2.$$

We also prove some lemmas about character groups.

It is possible to prove the assertions we will need without recourse to rigid uniformization, as Ahmed Abbes has pointed out to the author.

4.4.1 Raynaud's uniformization

Theorem 4.7 (Raynaud). *If A is a semistable abelian variety, its universal covering (as defined in [14]) is isomorphic to an extension G of an abelian variety B with good reduction by a torus T. The covering map from G to A is a homomorphism, and its kernel is a twisted free abelian group Γ of finite rank.*

This may be summarized by the diagram

$$\begin{tikzcd} & \Gamma \arrow[d] & \\ T \arrow[r] & G \arrow[r] \arrow[d] & B \\ & A, & \end{tikzcd}$$

which we call the *uniformization cross* of A.

Remark 4.8. The group Γ can be identified with the character group $X_{A^\vee}$ of the previous and latter sections.

The uniformization cross of the dual abelian variety $A^\vee$ is

$$\begin{tikzcd} & \Gamma^\vee \arrow[d] & \\ T^\vee \arrow[r] & G^\vee \arrow[r] \arrow[d] & B^\vee \\ & A^\vee, & \end{tikzcd}$$

where $\Gamma^\vee = \mathrm{Hom}(T, \mathbf{G}_m)$, where $T^\vee = \mathrm{Hom}(\Gamma, \mathbf{G}_m)$, and the morphisms $\Gamma^\vee \to G^\vee$ and $T^\vee \to G^\vee$ are the one-motif duals of the morphisms $T \to G$ and $\Gamma \to G$, respectively. For more details see, e.g., [14].

To avoid confusion when considering the uniformization of more than one abelian variety, we will often denote the objects T, G, Γ, and B connected with A by T_A, G_A, Γ_A, and B_A, respectively.

Example 4.9 (Tate curve). If $E/\mathbf{Q}_p$ is an elliptic curve with split multiplicative reduction, then the uniformization is $E = \mathbf{G}_m/q^{\mathbf{Z}}$ where $q = q(j)$ is obtained by inverting the expression for j as a function of $q(z) = e^{2\pi i z}$.

4.4.2 Some lemmas

Let $\pi : J \to A$ be an optimal quotient, assume that J has semistable reduction, and that A has purely toric reduction.

Lemma 4.10. *The map $\Gamma_J \to \Gamma_A$ induced by π is surjective.*

Proof. Since G_J is simply connected, π induces a map $G_J \to T_A$ and a map $\Gamma_J \to \Gamma_A$. Because π is surjective and T_A is a torus, the map $G_J \to T_A$ is surjective. Upon applying the snake lemma to the following diagram, we obtain a surjective map from $B = \ker(\pi)$ to $M = \mathrm{coker}(\Gamma_J \to \Gamma_A)$:

$$\begin{tikzcd}
 & \Gamma_J \arrow[r] \arrow[d] & \Gamma_A \arrow[r] \arrow[d] & M \arrow[r] \arrow[d] & 0 \\
 & G_J \arrow[r] \arrow[d] & T_A \arrow[r] \arrow[d] & 0 & \\
B \arrow[r] & J \arrow[r, "\pi"] & A. & &
\end{tikzcd}$$

Since $\pi : J \to A$ is an optimal quotient, the kernel B is connected. Thus M must also be connected. Since M is discrete it follows that $M = 0$. □

Abelian varieties with purely toric reduction

Assume that A has purely toric reduction. Then $B = 0$, and the uniformization cross is simply

$$\begin{tikzcd}
\Gamma \arrow[d] \\
T \arrow[d] \\
A.
\end{tikzcd}$$

Definition 4.11 (Symmetric isogeny). A *symmetric isogeny* $\varphi : A^\vee \to A$ is an isogeny such that the map $\varphi^\vee : A^\vee \to (A^\vee)^\vee = A$ is equal to φ.

Let $\varphi : A^\vee \to A$ be a symmetric isogeny. Denote by $\varphi_t : T^\vee \to T$ and $\varphi_a : \Gamma^\vee \to \Gamma$ the maps induced by φ.

Proposition 4.12. *There is an exact sequence*

$$0 \to \ker(\varphi_t) \to \ker(\varphi) \to \mathrm{coker}(\varphi_a) \to 0,$$

and $\ker(\varphi_t)$ *is the Cartier dual of* $\mathrm{coker}(\varphi_a)$.

Proof. Since φ is an isogeny we obtain the following diagram:

$$\begin{tikzcd}
0 \arrow[r] \arrow[d] & \Gamma^\vee \arrow[r, "\varphi_a"] \arrow[d] & \Gamma \arrow[r] \arrow[d] & \mathrm{coker}(\varphi_a) \arrow[d] \\
\ker(\varphi_t) \arrow[r] \arrow[d] & T^\vee \arrow[r, "\varphi_t"] \arrow[d] & T \arrow[r] \arrow[d] & 0 \\
\ker(\varphi) \arrow[r] & A^\vee \arrow[r, "\varphi"] & A. &
\end{tikzcd}$$

The snake lemma then gives the claimed exact sequence.

For the second assertion, observe that if we take one-motif duals of every object in the diagram

$$\begin{tikzcd} & \Gamma^\vee \arrow[r, "\varphi_a"] \arrow[d] & \Gamma \arrow[r] \arrow[d] & \operatorname{coker}(\varphi_a) \\ \ker(\varphi_t) \arrow[r] & T^\vee \arrow[r, "\varphi_t"] & T & \end{tikzcd}$$

we obtain the following diagram:

$$\begin{tikzcd} & T & T^\vee \arrow[l, "\varphi_a^\vee"'] & \operatorname{coker}(\varphi_a)^\vee \arrow[l] \\ \ker(\varphi_t)^\vee & \Gamma \arrow[l] \arrow[u] & \Gamma^\vee. \arrow[l, "\varphi_t^\vee"] \arrow[u] & \end{tikzcd}$$

Since φ is symmetric, $\varphi_a^\vee = \varphi_t$, so

$$\ker(\varphi_t) = \operatorname{coker}(\varphi_a)^\vee.$$

□

Lemma 4.13. $\#\ker(\varphi) = \#\operatorname{coker}(\varphi_a)^2$

Proof. Use the exact sequence of Proposition 4.12 together with the observation that the order of a finite group scheme equals the order of its Cartier dual. □

4.5 The main theorem

Let $\pi : J \to A$ be an optimal quotient, with J a Jacobian having semistable reduction and A an abelian variety having purely toric reduction. Let X_A, $X_{A^\vee}$, and X_J denote the character groups of the toric parts of the closed fibers of the abelian varieties A, $A^\vee$, and J, respectively.

4.5.1 Description of the component group in terms of the monodromy pairing

Recall that there is a pairing $X_A \times X_{A^\vee} \to \mathbf{Z}$ called the monodromy pairing. We have an exact sequence

$$0 \to X_{A^\vee} \to \operatorname{Hom}(X_A, \mathbf{Z}) \to \Phi_A \to 0.$$

If J is a Jacobian then J is canonically self-dual via the θ-polarization, so the monodromy pairing on J can be viewed as a pairing $X_J \times X_J \to \mathbf{Z}$, and there is an exact sequence

$$0 \to X_J \to \operatorname{Hom}(X_J, \mathbf{Z}) \to \Phi_J \to 0.$$

Example 4.14 (Tate curve). Suppose $E = \mathbf{G}_m/q^{\mathbf{Z}}$ is a Tate curve over $\mathbf{Q}_p^{\mathrm{ur}}$. The monodromy pairing on $X_E = q^{\mathbf{Z}}$ is

$$\langle q, q\rangle = \mathrm{ord}_p(q) = -\,\mathrm{ord}_p(j).$$

Thus Φ_E is cyclic of order $-\,\mathrm{ord}_p(j)$.

Proof of the main theorem

We now prove the main theorem. Let $\pi : J \to A$ be an optimal quotient, and let $\theta : A^\vee \to A$ denote the induced polarization. Let π_*, π^*, θ_*, and θ^* be the maps induced on character groups by the various functorialities, as indicated in the following two key diagrams:

$$\begin{tikzcd} A^\vee \arrow[r, hook, "\pi^\vee"] \arrow[dr, "\theta"'] & J \arrow[d, two heads, "\pi"] \\ & A \end{tikzcd} \qquad\qquad \begin{tikzcd} X_A \arrow[r, hook, "\pi^*"] \arrow[dr, "\theta^*"] & X_J \arrow[d, two heads, "\pi_*"] \\ & X_{A^\vee}. \arrow[ul, bend left, "\theta_*"] \end{tikzcd}$$

The surjectivity of π_* was proved in Lemma 4.10. The injectivity of π^* follows because

$$\theta_*\pi_*\pi^* = \theta_*\theta^* = \deg(\theta) \neq 0,$$

and multiplication by a nonzero integer on a free abelian group is injective.

Let

$$\alpha : X_J \to \mathrm{Hom}(\pi^* X_A, \mathbf{Z})$$

be the map defined by the monodromy pairing restricted to $X_J \times \pi^* X_A$.

Lemma 4.15. $\ker(\pi_*) = \ker(\alpha)$

Proof. Suppose $x \in \ker(\pi_*)$, and let $y = \pi^* z$ with $z \in X_A$. Then

$$\langle x, y\rangle = \langle x, \pi^* z\rangle = \langle \pi_* x, z\rangle = 0,$$

so $x \in \ker(\alpha)$. Next let $x \in \ker(\alpha)$. Then for all $z \in X_A$,

$$0 = \langle x, \pi^* z\rangle = \langle \pi_* x, z\rangle,$$

so $\pi_* x$ is in the kernel of the monodromy map

$$X_{A^\vee} \to \mathrm{Hom}(X_A, \mathbf{Z}).$$

Since $X_{A^\vee}$ and $\mathrm{Hom}(X_A, \mathbf{Z})$ are free of the same finite rank and the cokernel is torsion, the monodromy map is injective. Thus $\pi_* x = 0$ and $x \in \ker(\pi_*)$. $\square$

Lemma 4.16. *There is an exact sequence*

$$X_J \to \mathrm{Hom}(\pi^* X_A, \mathbf{Z}) \to \Phi_A \to 0.$$

Proof. Lemma 4.15 gives the following commutative diagram with exact rows

$$\begin{tikzcd}
0 \arrow[r] & X_J/\ker(\alpha) \arrow[r] \arrow[d, "\cong"] & \mathrm{Hom}(\pi^* X_A, \mathbf{Z}) \arrow[r] \arrow[d, "\cong"] & \mathrm{coker}(\alpha) \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & X_{A^\vee} \arrow[r] & \mathrm{Hom}(X_A, \mathbf{Z}) \arrow[r] & \Phi_A \arrow[r] & 0.
\end{tikzcd}$$

By Lemma 4.15, the first vertical map is an isomorphism. The second is an isomorphism because it is induced by the isomorphism $\pi^* : X_A \to \pi^* X_A$. It follows that $\mathrm{coker}(\alpha) \cong \Phi_A$, as claimed. □

Let $\mathcal{L}$ be the *saturation* of $\pi^* X_A$ in X_J; thus $\pi^* X_A$ is a finite-index subgroup of $\mathcal{L}$ and the quotient $X_J/\mathcal{L}$ is torsion free. For L of finite index in $\mathcal{L}$, define the *modular degree* of L to be

$$m_L = [\alpha(X_J) : \alpha(L)],$$

and the *component group* of L to be

$$\Phi_L = \mathrm{coker}(X_J \to \mathrm{Hom}(L, \mathbf{Z})).$$

When $L = \mathcal{L}$ and A is fixed, we often slightly abuse notation and write $m_X = m_{\mathcal{L}}$ and $\Phi_X = \Phi_{\mathcal{L}}$. We think of m_X and Φ_X as the character group "modular degree and component group" of A.

Lemma 4.17. *Choose a subgroup L of finite index in $\mathcal{L}$. The rational number $\dfrac{\#\Phi_L}{m_L}$ is independent of the choice of L.*

Proof. Suppose L' is another finite index subgroup of $\mathcal{L}$, and let $n = [L : L']$. Here n is a rational number, the lattice index of L' in L. Since α is injective when restricted to $\mathcal{L}$, it follows that

$$m_{L'} = [\alpha(X_J) : \alpha(L')] = [\alpha(X_J) : \alpha(L)] \cdot [\alpha(L) : \alpha(L')] = m_L \cdot n.$$

Similarly, $\#\Phi_{L'} = \#\Phi_L \cdot n$. □

Recall that $m_A = \sqrt{\deg(\theta)}$ and

$$\Phi_A \cong \mathrm{coker}(X_{A^\vee} \to \mathrm{Hom}(X_A, \mathbf{Z})),$$

where m_A is the modular degree of A and Φ_A is the component group of A.

Theorem 4.18. *For any subgroup L of finite index in $\mathcal{L}$, the following relation holds:*

$$\frac{\#\Phi_A}{m_A} = \frac{\#\Phi_L}{m_L}.$$

Proof. By Lemma 4.17 we may assume that $L = \pi^* X_A$. With this choice of L, Lemma 4.16 asserts that $\Phi_L \cong \Phi_A$. By Lemma 4.15, properties of the index, and Lemma 4.13 we have

$$\begin{aligned} m_L &= [\alpha(X_J) : \alpha(L)] \\ &= [\pi_*(X_J) : \pi_*(L)] \\ &= [X_{A^\vee} : \pi_*(\pi^* X_A)] \\ &= [X_{A^\vee} : \theta^* X_A] \\ &= \#\operatorname{coker}(\theta^*) \\ &= \sqrt{\deg(\theta)} = m_A. \end{aligned}$$

□

Proposition 4.19.

$$\operatorname{image}(\Phi_J \to \Phi_A) \cong \Phi_{\mathcal{L}}.$$

Proof. Since $\pi^* X_A \subset \mathcal{L} \subset X_J$, an application of Lemma 4.16 gives the following commutative diagram with exact rows:

$$\begin{tikzcd} X_J \arrow[r] \arrow[d, equal] & \operatorname{Hom}(X_J, \mathbf{Z}) \arrow[r] \arrow[d] & \Phi_J \arrow[r] \arrow[d] & 0 \\ X_J \arrow[r] \arrow[d, equal] & \operatorname{Hom}(\mathcal{L}, \mathbf{Z}) \arrow[r] \arrow[d] & \Phi_{\mathcal{L}} \arrow[r] \arrow[d] & 0 \\ X_J \arrow[r] & \operatorname{Hom}(\pi^* X_A, \mathbf{Z}) \arrow[r] & \Phi_A \arrow[r] & 0. \end{tikzcd}$$

The map $\operatorname{Hom}(\mathcal{L}, \mathbf{Z}) \to \operatorname{Hom}(\pi^* X_A, \mathbf{Z})$ is an isomorphism, so the map $\Phi_{\mathcal{L}} \to \Phi_A$ is injective. Thus

$$\operatorname{image}(\Phi_J \to \Phi_A) \cong \operatorname{image}(\Phi_J \to \Phi_{\mathcal{L}}).$$

The cokernel of $\operatorname{Hom}(X_J, \mathbf{Z}) \to \operatorname{Hom}(\mathcal{L}, \mathbf{Z})$ surjects onto the cokernel of $\Phi_J \to \Phi_{\mathcal{L}}$. Using the exact sequence

$$0 \to \mathcal{L} \to X_J \to X_J/\mathcal{L} \to 0,$$

we find that

$$\operatorname{coker}(\operatorname{Hom}(X_J, \mathbf{Z}) \to \operatorname{Hom}(\mathcal{L}, \mathbf{Z})) \subset \operatorname{Ext}^1(X_J/\mathcal{L}, \mathbf{Z}).$$

Because $\mathcal{L}$ is saturated, the quotient $X_J/\mathcal{L}$ is torsion free, so the indicated Ext^1 group vanishes. Thus the map $\Phi_J \to \Phi_{\mathcal{L}}$ is surjective, from which the proposition follows. □

The following corollary follows from Theorem 4.18 and Proposition 4.19.

Corollary 4.20.

$$\#\operatorname{coker}(X_J \to X_A) = \frac{m_A}{m_{\mathcal{L}}}.$$

Remark 4.21. A non-obvious consequence of this corollary is that

$$m_{\mathcal{L}} \mid m_A.$$

4.6 Optimal quotients of $J_0(N)$

We now summarize some facts about $J_0(N)$ that will be used in our numerical computations. Some of these facts were discussed in greater generality in the previous chapters of this thesis.

4.6.1 Modular curves and semistability

Let $X_0(N)$ be the modular curve associated to the subgroup $\Gamma_0(N)$ of $\mathrm{SL}_2(\mathbf{Z})$ that consists of those matrices which are upper triangular modulo N. Initially, $X_0(N)$ is constructed as a Riemann surface as the quotient

$$\Gamma_0(N)\backslash(\{z : z \in \mathbf{C},\, \mathrm{Im}(z) > 0\} \cup \mathbf{P}^1(\mathbf{Q})).$$

With some work, we find that $X_0(N)$ has a canonical structure of algebraic curve over $\mathbf{Q}$.

Suppose that p is a prime divisor of N such that N/p is coprime to p. We write $p \,||\, N$. In this situation, it is well-known that the Jacobian $J_0(N)$ of $X_0(N)$ has semistable reduction at p.

4.6.2 Newforms and optimal quotients

The Hecke algebra

$$\mathbf{T} = \mathbf{Z}[\dots T_n \dots] \subset \mathrm{End}(J_0(N))$$

is a commutative ring of endomorphisms of $J_0(N)$ of $\mathbf{Z}$-rank equal to the dimension $J_0(N)$. The character group $X_{J_0(N)}$ of $J_0(N)$ at p is equipped with a functorial action of $\mathbf{T}$. The Hecke algebra $\mathbf{T}$ also acts on the complex vector space $S = S_2(\Gamma_0(N), \mathbf{C})$ of cusp forms.

A newform f is an eigenform normalized so that the coefficient of q in the Fourier expansion of f at the cusp ∞ is 1, and such that f is not a modular form of any level $N' \mid N$, with N' a proper divisor of N.

Let f be a newform, and associate to f the ideal I_f of the Hecke algebra $\mathbf{T}$ of elements which annihilate f. Then $\mathcal{O}_f = \mathbf{T}/I_f$ is an order in the ring of integers of the totally real number field K_f obtained by adjoining the Fourier coefficients of f to $\mathbf{Q}$. The quotient

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

is an optimal quotient of $J_0(N)$ of dimension equal to $[K_f : \mathbf{Q}]$. It is purely toric at p, since $p \,||\, N$.

4.6.3 Homology and the modular degree

Let $H = H_1(X_0(N), \mathbf{Z})$ be the integral homology of the complex algebraic curve $X_0(N)$. Integration defines a $\mathbf{T}$-equivariant nondegenerate pairing $S \times H \to \mathbf{C}$. This pairing induces a map $\alpha : H \to \mathrm{Hom}_{\mathbf{C}}(S, \mathbf{C})$.

Theorem 4.22. *We have the following commutative diagram of* $\mathbf{T}$*-modules:*

$$\begin{tikzcd}
H[I_f] \arrow[r, hook] \arrow[d, hook] & H \arrow[r, two heads] \arrow[d, hook] & \alpha(H) \arrow[d, hook] \\
\mathrm{Hom}_{\mathbf{C}}(S,\mathbf{C})[I_f] \arrow[r, hook] \arrow[d, two heads] & \mathrm{Hom}_{\mathbf{C}}(S,\mathbf{C}) \arrow[r, two heads] \arrow[d, two heads] & \mathrm{Hom}_{\mathbf{C}}(S[I_f],\mathbf{C}) \arrow[d, two heads] \\
A_f^{\vee}(\mathbf{C}) \arrow[r, hook] \arrow[rr, bend right, "\theta_A"'] & J(\mathbf{C}) \arrow[r, two heads] & A_f(\mathbf{C})
\end{tikzcd}$$

Proof. This can be deduced from [61]. See also Section 2.7. □

Corollary 4.23. $m_A^2 = [\alpha(H) : \alpha(H[I_f])]$.

Proof. Recall that m_A is by definition equal to $\sqrt{\deg(\theta_A)}$. The kernel of an isogeny between complex tori is isomorphic to the cokernel of the induced map on lattices. The corollary now follows from the diagram of Theorem 4.22, which indicates that the index $[\alpha(H) : \alpha(H[I_f])]$ is the cokernel of the map $H[I_f] \to \alpha(H)$.

For more details, see Section 3.9. □

4.6.4 Rational points of the component group (Tamagawa numbers)

Let $\mathrm{Frob}_p : X_J \to X_J$ denote the map induced by the Frobenius automorphism. We have $\mathrm{Frob}_p = -W_p$, where W_p is the map induced by the Atkin-Lehner involution on $J_0(p)$. Let f be a newform, $A = A_f$ the corresponding optimal quotient, and w_p the sign of the eigenvalue of W_p on f.

Proposition 4.24.

$$\Phi_A(\mathbf{F}_p) = \begin{cases} \Phi_A(\overline{\mathbf{F}}_p) & \textit{if } w_p = -1, \\ \Phi_A(\overline{\mathbf{F}}_p)[2] & \textit{if } w_p = 1. \end{cases}$$

Proof. If $w_p = -1$, then $\mathrm{Frob}_p = 1$ and the $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$-action of $\Phi_A(\overline{\mathbf{F}}_p)$ is trivial. In this case $\Phi(\mathbf{F}_p) = \Phi(\overline{\mathbf{F}}_p)$. Next suppose $w_p = 1$. Recall that we have an exact sequence

$$0 \to X_{A^\vee} \to \mathrm{Hom}(X_A, \mathbf{Z}) \to \Phi_A \to 0.$$

Since W_p acts as $+1$ on f, it also acts as $+1$ on each of the four modules A, X_A, $\mathrm{Hom}(X_A, \mathbf{Z})$, and Φ_A. Thus $\mathrm{Frob}_p = -W_p$ acts as -1 on Φ_A. Since the subgroup of 2-torsion elements of a finite abelian group equals the subgroup of elements fixed under -1, it follows that $\Phi_A(\mathbf{F}_p) = \Phi_A(\overline{\mathbf{F}}_p)[2]$. □

WARNING: When we extend this result to the whole of $J_0(N)$, it is necessary to be exceedingly careful! The action of $\mathrm{Frob}_p = T_p$ need not be by ± 1, even though it must be by an involution of order 2. For example, the component group of $J_0(65)$ at 5 is cyclic of order 42. The action of Frob_5 is by multiplication by -13. Note that $(-13)^2 = 1 \pmod{42}$. The fixed points of multiplication by -13 is the order 14 subgroup of $\mathbf{Z}/42\mathbf{Z}$.

4.7 Computations

Using the algorithms of Chapter 3, we can enumerate the optimal quotients A_f of $J_0(N)$ and compute the modular degree m_A. The method of graphs (see [47]) and quaternion algebras (see [32]) can be used to compute $X = X_{J_0(N)}$ with its $\mathbf{T}$-action and the monodromy pairing. We can then compute the following three modules: the saturated submodule $\mathcal{L} = \bigcap_{t\in I_f} \ker(t)$ of X, the character group modular degree $m_X = m_{\mathcal{L}}$, and $\Phi_X = \Phi_{\mathcal{L}}$. By Theorem 4.18 we obtain

$$\#\Phi_A = \#\Phi_X \cdot \frac{m_A}{m_X}.$$

Using this method, we have computed $\#\Phi_A$ in a number of cases. We give tables that report on some of these computations in Secton 4.7.2. In the next section we discuss a conjecture and a question, which were both suggested by our numerical computations.

4.7.1 Conjectures and questions

Suppose that $N = pM$ with $(p, M) = 1$. Let

$$H_{\mathrm{new}} = \ker\Big(H_1(X_0(N), \mathbf{Z}) \longrightarrow H_1(X_0(M), \mathbf{Z}) \oplus H_1(X_0(M), \mathbf{Z})\Big),$$

where the map is induced by the two natural degeneracy maps $X_0(N) \to X_0(M)$.

The Hecke algebra $\mathbf{T}$ acts on H_{new}, and also on the submodule $H_{\mathrm{new}}[I_f]$ of those elements that are annihilated by I_f. Integration defines a map $\alpha : H_{\mathrm{new}} \to \mathrm{Hom}(S[I_f], \mathbf{C})$. Define the p-new homology modular degree m_H by

$$m_H^2 = [\alpha(H_{\mathrm{new}}) : \alpha(H_{\mathrm{new}}[I_f])].$$

We expect that there is a very close relationship between m_X and m_H.

Question 4.25. Is m_X equal to m_H?

The following conjecture offers a refinement of some of the results of [40].

Conjecture 4.26 (Refined Eisenstein conjecture). *Let p be a prime and let $f_1, \dots, f_n$ be a set of representatives for the Galois-conjugacy classes of newforms in $S_2(\Gamma_0(p))$. Let $A_1, \dots, A_n$ be the optimal quotients associated to $f_1, \dots, f_n$, respectively. Then for each i, $i = 1, \dots, n$, we have*

$$\#A_i(\mathbf{Q})_{\mathrm{tor}} = \#\Phi_{A_i}(\overline{\mathbf{F}}_p) = \#\Phi_{A_i}(\mathbf{F}_p).$$

Furthermore,

$$\#\Phi_{J_0(p)}(\overline{\mathbf{F}}_p) = \prod_{i=1}^{d} \#\Phi_{A_i}(\overline{\mathbf{F}}_p).$$

We have verified Conjecture 4.26 for all $p \le 757$, and, up to a power of 2, for all $p < 2000$.

Remark 4.27. It is tempting to guess that, e.g., the natural map

$$\Phi_{J_0(113)}(\overline{\mathbf{F}}_p) \to \prod_{i=1}^{4} \Phi_{A_i}(\overline{\mathbf{F}}_p)$$

is an isomorphism. Two of the $\Phi_{A_i}(\overline{\mathbf{F}}_p)$ have order 2, so the product $\prod \Phi_{A_i}(\overline{\mathbf{F}}_p)$ can not be a cyclic group. However, the groups $\Phi_{J_0(p)}(\overline{\mathbf{F}}_p)$ are known to be cyclic for all primes p.

4.7.2 Tables

We have computed component groups of many optimal quotients A_f of $J_0(N)$. In this section we provide tables, which hint at the data we have gathered. Our notation for optimal quotients is described in Section 1.3.1. See also Table 1.6.

Table 4.1: Component groups at low level

Table 4.1 gives the component groups of the quotients A_f of $J_0(N)$ for $N \leq 106$. The column labeled d contains the dimensions of the A_f, and the column labeled $\#\Phi_{A,p}$ contains a list of the orders of the component groups of A_f, one for each divisor p of N, ordered by increasing p. An entry of "?" indicates that $p^2 \mid N$, so our algorithm does not apply. A component group order is starred if the $\mathrm{Gal}(\overline{\mathbf{F}}_p/\mathbf{F}_p)$-action is nontrivial.

Table 4.2–4.3: Big component groups

Using the algorithms described in Section 3.10, we computed the rational numbers $L(A,1)/\Omega_A$ for every optimal quotient A that is attached to a newform of level ≤ 1500. There are exactly 5 optimal quotients A such that the numerator of $L(A,1)/\Omega_A$ is nonzero and divisible by a prime $> 10^9$. The Birch and Swinnerton-Dyer conjecture predicts that these large prime divisors must divide either $\#\Phi_A$ or the Shafarevich-Tate group of A. This is the case, as Table 4.3 shows.

Table 4.4: Quotients of $J_0(N)$

Table 4.4 contains all of the invariants involved in the computation of component groups for each of the newform optimal quotients of levels 65, 66, 68, and 69.

Table 4.5: Quotients of $J_0(p)^-$

We computed the quantities m_A, m_X and Φ_X for each abelian variety $A = A_f$ associated to a newform of prime level p with $p \leq 757$. The results are as follows:

1. In all cases $m_A = m_X$, so the map $\Phi_J \to \Phi_A$ is surjective.
2. $\Phi_A = 1$ whenever the sign of the Atkin-Lehner involution w_p on A is 1.
3. $\prod \#\Phi_A(\overline{\mathbf{F}}_p) = \#\Phi_J(\overline{\mathbf{F}}_p)$

Table 4.5 lists those A of level ≤ 631 for which $w_p = -1$, along with the order of the corresponding component group.

Table 4.1: Component groups at low level

A	d	$\#\Phi_{A,p}$	A	d	$\#\Phi_{A,p}$	A	d	$\#\Phi_{A,p}$	A	d	$\#\Phi_{A,p}$
11A	1	5	**51A**	1	$3, 1^*$	**72A**	1	$?, ?$	**90C**	1	$4, ?, 1$
14A	1	$6^*, 3$	**51B**	2	$16^*, 4$	**73A**	1	2	**91A**	1	$1^*, 1^*$
15A	1	$4^*, 4$	**52A**	1	$?, 2^*$	**73B**	2	1^*	**91B**	1	$1, 1$
17A	1	4	**53A**	1	1^*	**73C**	2	3	**91C**	2	$7, 1^*$
19A	1	3	**53A**	1	1^*	**74A**	2	$9^*, 3$	**91D**	3	$4^*, 8$
20A	1	$?, 2^*$	**53B**	3	13	**74B**	2	$95, 1^*$	**92A**	1	$?, 1^*$
21A	1	$4, 2^*$	**54A**	1	$3^*, ?$	**75A**	1	$1^*, ?$	**92B**	1	$?, 1$
23A	2	11	**54B**	1	$3, ?$	**75B**	1	$1, ?$	**93A**	2	$4^*, 1^*$
24A	1	$?, 2^*$	**55A**	1	$2, 2^*$	**75C**	1	$5, ?$	**93B**	3	$64, 2^*$
26A	1	$3^*, 3$	**55B**	2	$14^*, 2$	**76A**	1	$?, 1^*$	**94A**	1	$2, 1^*$
26B	1	$7, 1^*$	**56A**	1	$?, 1$	**77A**	1	$2^*, 1^*$	**94B**	2	$94^*, 1$
27A	1	$?$	**56B**	1	$?, 1^*$	**77B**	1	$3^*, 2$	**95A**	3	$10, 2^*$
29A	2	7	**57A**	1	$2^*, 1^*$	**77C**	1	$6, 3^*$	**95B**	4	$54^*, 6$
30A	1	$4^*, 3, 1^*$	**57B**	1	$2, 2^*$	**77D**	2	$2, 2^*$	**96A**	1	$?, 2$
31A	2	5	**57C**	1	$10, 1^*$	**78A**	1	$16^*, 5^*, 1$	**96B**	1	$?, 2^*$
32A	1	$?$	**58A**	1	$2^*, 1^*$	**79A**	1	1^*	**97A**	3	1^*
33A	1	$6^*, 2$	**58B**	1	$10, 1^*$	**79B**	5	13	**97B**	4	8
34A	1	$6, 1^*$	**59A**	5	29	**80A**	1	$?, 2$	**98A**	1	$2^*, ?$
35A	1	$3^*, 3$	**61A**	1	1^*	**80B**	1	$?, 2^*$	**98B**	2	$14, ?$
35B	2	$8, 4^*$	**61B**	3	5	**81A**	2	$?$	**99A**	1	$?, 1^*$
36A	1	$?, ?$	**62A**	1	$4, 1^*$	**82A**	1	$2^*, 1^*$	**99B**	1	$?, 1$
37A	1	1^*	**62B**	2	$66^*, 3$	**82B**	2	$28, 1^*$	**99C**	1	$?, 1^*$
37B	1	3	**63A**	1	$?, 1^*$	**83A**	1	1^*	**99D**	1	$?, 1^*$
38A	1	$9^*, 3$	**63B**	2	$?, 3$	**83B**	6	41	**100A**	1	$?, ?$
38B	1	$5, 1^*$	**64A**	1	$?$	**84A**	1	$?, 1^*, 2^*$	**101A**	1	1^*
39A	1	$2^*, 2$	**65A**	1	$1^*, 1^*$	**84B**	1	$?, 3, 2$	**101B**	7	25
39B	2	$14, 2^*$	**65B**	2	$3^*, 3$	**85A**	1	$2^*, 1$	**102A**	1	$2^*, 2^*, 1^*$
40A	1	$?, 2$	**65C**	2	$7, 1^*$	**85B**	2	$2^*, 1^*$	**102B**	1	$6^*, 6, 1^*$
41A	3	10	**66A**	1	$2^*, 3, 1^*$	**85C**	2	$6, 1^*$	**102C**	1	$8, 4, 1$
42A	1	$8, 2^*, 1^*$	**66B**	1	$4, 1^*, 1^*$	**86A**	2	$21^*, 3$	**103A**	2	1^*
43A	1	1^*	**66C**	1	$10, 5, 1$	**86B**	2	$55, 1^*$	**103B**	6	17
43B	2	7	**67A**	1	1	**87A**	2	$5, 1^*$	**104A**	1	$?, 1^*$
44A	1	$?, 1^*$	**67B**	2	1^*	**87B**	3	$92^*, 4$	**104B**	2	$?, 2$
45A	1	$?, 1^*$	**67C**	2	11	**88A**	1	$?, 1^*$	**105A**	1	$1, 1, 1$
46A	1	$10^*, 1$	**68A**	2	$?, 2^*$	**88B**	2	$?, 2^*$	**105B**	2	$10^*, 2^*, 2$
47A	4	23	**69A**	1	$2, 1^*$	**89A**	1	1^*	**106A**	1	$4^*, 1^*$
48A	1	$?, 2$	**69B**	2	$22^*, 2$	**89B**	1	2	**106B**	1	$5^*, 1$
49A	1	$?$	**70A**	1	$4, 2^*, 1^*$	**89C**	5	11	**106C**	1	$24, 1^*$
50A	1	$1^*, ?$	**71A**	3	5	**90A**	1	$2^*, ?, 3$	**106D**	1	$3, 1^*$
50B	1	$5, ?$	**71B**	3	7	**90B**	1	$6, ?, 1^*$			

Table 4.2: Big $L(A,1)/\Omega_A$

A	dim	N	$L(A,1)/\Omega_A \cdot$ Manin constant
1154E	20	$2\cdot 577$	$2^? \cdot 85495047371/17^2$
1238G	19	$2\cdot 619$	$2^? \cdot 7553329019/5\cdot 31$
1322E	21	$2\cdot 661$	$2^? \cdot 57851840099/331$
1382D	20	$2\cdot 691$	$2^? \cdot 37\cdot 1864449649/173$
1478J	20	$2\cdot 739$	$2^? \cdot 7\cdot 29\cdot 1183045463/5\cdot 37$

Table 4.3: Big component groups

A	p	w	$\#\Phi_X$	m_X	$\#\Phi_A(\overline{\mathbf{F}}_p)$
1154E	2	$-$	17^2	2^{24}	$2^? \cdot 17^2 \cdot 85495047371$
	577	$+$	1	$2^{26}\cdot 85495047371$	$2^?$
1238G	2	$-$	$5\cdot 31$	2^{26}	$2^? \cdot 5\cdot 31\cdot 7553329019$
	619	$+$	1	$2^{28}\cdot 7553329019$	$2^?$
1322E	2	$-$	331	2^{28}	$2^? \cdot 331\cdot 57851840099$
	661	$+$	1	$2^{32}\cdot 57851840099$	$2^?$
1382D	2	$-$	173	2^{29}	$2^? \cdot 37\cdot 173\cdot 1864449649$
	691	$+$	1	$2^{31}\cdot 37\cdot 1864449649$	$2^?$
1478J	2	$-$	$5\cdot 37$	2^{31}	$2^? \cdot 5\cdot 7\cdot 29\cdot 37\cdot 1183045463$
	739	$+$	1	$2^{33}\cdot 7\cdot 29\cdot 1183045463$	$2^?$

Table 4.4: Component groups of quotients of $J_0(N)$

A	dim	p	w_p	$\#\Phi_X$	m_X	m_A	$\#\Phi_A$
65A	1	5	$+$	1	2	2	1
		13	$+$	1	2		1
65B	2	5	$+$	3	2^2	2^2	3
		13	$-$	3	2^2		3
65C	2	5	$-$	7	2^2	2^2	7
		13	$+$	1	2^2		1
66A	1	2	$+$	1	2	2^2	2
		3	$-$	3	2^2		3
		11	$+$	1	2^2		1
66B	1	2	$-$	2	2	2^2	2^2
		3	$+$	1	2^2		1
		11	$+$	1	2^2		1
66C	1	2	$-$	1	2	$2^2 \cdot 5$	$2 \cdot 5$
		3	$-$	1	2^2		5
		11	$-$	1	$2^2 \cdot 5$		1
68A	2	17	$+$	2	$2 \cdot 3$	$2 \cdot 3$	2
69A	1	3	$-$	2	2	2	2
		23	$+$	1	2		1
69B	2	3	$+$	2	2	$2 \cdot 11$	$2 \cdot 11$
		23	$-$	2	$2 \cdot 11$		2

Table 4.5: Component groups of quotients of $J_0(p)^-$

A	d	$\#\Phi_A$	A	d	$\#\Phi_A$	A	d	$\#\Phi_A$	A	d	$\#\Phi_A$
11A	1	5	**157B**	7	13	**313A**	2	1	**487B**	2	3
17A	1	2^2	**163C**	7	3^3	**313C**	12	$2\cdot 13$	**487C**	3	1
19A	1	3	**167B**	12	83	**317B**	15	79	**487D**	16	3^3
23A	2	11	**173B**	10	43	**331D**	16	$5\cdot 11$	**491C**	29	$5\cdot 7^2$
29A	2	7	**179A**	1	1	**337B**	15	$2^2\cdot 7$	**499C**	23	83
31A	2	5	**179C**	11	89	**347D**	19	173	**503B**	1	1
37B	1	3	**181B**	9	$3\cdot 5$	**349B**	17	29	**503C**	1	1
41A	3	$2\cdot 5$	**191B**	14	$5\cdot 19$	**353A**	1	2	**503D**	3	1
43B	2	7	**193C**	8	2^4	**353B**	3	2	**503F**	26	251
47A	4	23	**197C**	10	7^2	**353D**	14	$2\cdot 11$	**509B**	28	127
53B	3	13	**199A**	2	1	**359D**	24	179	**521B**	29	$2\cdot 5\cdot 13$
59A	5	29	**199C**	10	$3\cdot 11$	**367B**	19	61	**523C**	26	$3\cdot 29$
61B	3	5	**211A**	2	5	**373C**	17	31	**541B**	24	$3^2\cdot 5$
67A	1	1	**211D**	9	7	**379B**	18	$3^2\cdot 7$	**547C**	25	$7\cdot 13$
67C	2	11	**223C**	12	37	**383C**	24	191	**557B**	1	1
71A	3	5	**227B**	2	1	**389A**	1	1	**557D**	26	139
71B	3	7	**227C**	2	1	**389E**	20	97	**563A**	1	1
73A	1	2	**227E**	10	113	**397B**	2	1	**563E**	31	281
73C	2	3	**229C**	11	19	**397C**	5	11	**569B**	31	$2\cdot 71$
79B	5	13	**233A**	1	2	**397D**	10	3	**571A**	1	1
83B	6	41	**233C**	11	29	**401B**	21	$2^2\cdot 5^2$	**571B**	1	1
89B	1	2	**239B**	17	$7\cdot 17$	**409B**	20	$2\cdot 17$	**571C**	2	1
89C	5	11	**241B**	12	$2^2\cdot 5$	**419B**	26	$11\cdot 19$	**571D**	2	1
97B	4	2^3	**251B**	17	5^3	**421B**	19	$5\cdot 7$	**571F**	4	1
101B	7	5^2	**257B**	14	2^6	**431B**	1	1	**571I**	18	$5\cdot 19$
103B	6	17	**263B**	17	131	**431D**	3	1	**577A**	2	3
107B	7	53	**269C**	16	67	**431F**	24	$5\cdot 43$	**577B**	2	1
109A	1	1	**271B**	16	$3^2\cdot 5$	**433A**	1	1	**577C**	3	1
109C	4	3^2	**277B**	3	1	**433B**	3	1	**577D**	18	2^4
113A	1	2	**277D**	9	23	**433D**	16	$2^2\cdot 3^2$	**587C**	31	293
113B	2	2	**281B**	16	$2\cdot 5\cdot 7$	**439C**	25	73	**593B**	1	2
113D	3	7	**283B**	14	47	**443C**	1	1	**593C**	2	1
127B	7	$3\cdot 7$	**293B**	16	73	**443E**	22	$13\cdot 17$	**593E**	27	$2\cdot 37$
131B	10	$5\cdot 13$	**307A**	1	1	**449B**	23	$2^4\cdot 7$	**599C**	37	$13\cdot 23$
137B	7	$2\cdot 17$	**307B**	1	1	**457C**	20	$2\cdot 19$	**601B**	29	$2\cdot 5^2$
139A	1	1	**307C**	1	1	**461D**	26	$5\cdot 23$	**607D**	31	101
139C	7	23	**307D**	1	1	**463B**	22	$7\cdot 11$	**613C**	27	$3\cdot 17$
149B	9	37	**307E**	2	3	**467C**	26	233	**617B**	28	$2\cdot 7\cdot 11$
151B	3	1	**307F**	9	17	**479B**	32	239	**619B**	30	103
151C	6	5^2	**311B**	22	$5\cdot 31$	**487A**	2	1	**631B**	32	$3\cdot 5\cdot 7$

Bibliography

[1] A. Agashé, *On invisible elements of the Tate-Shafarevich group*, C. R. Acad. Sci. Paris Sér. I Math. **328** (1999), no. 5, 369–374.

[2] A. Agashe, *The Birch and Swinnerton-Dyer formula for modular abelian varieties of analytic rank* 0, U. C. Berkeley Ph.D. thesis (2000).

[3] A. Agashe and W. A. Stein, *On the generalized manin constant for quotients of* $J_0(N)$, in preparation.

[4] A. O. L. Atkin and J. Lehner, *Hecke operators on* $\Gamma_0(m)$, Math. Ann. **185** (1970), 134–160.

[5] B. Birch, *Atkin and the Atlas Lab*, Proceedings of the conference in honor of A. O. L. Atkin held at the University of Illinois, Chicago, IL, September 1995, Amer. Math. Soc., Providence, RI, 1998, pp. 13–20.

[6] B. J. Birch and W. Kuyk (eds.), *Modular functions of one variable. IV*, Springer-Verlag, Berlin, 1975, Lecture Notes in Mathematics, Vol. 476.

[7] S. Bloch and K. Kato, *L-functions and Tamagawa numbers of motives*, The Grothendieck Festschrift, Vol. I, Birkhäuser Boston, Boston, MA, 1990, pp. 333–400.

[8] S. Bosch, W. Lütkebohmert, and M. Raynaud, *Néron models*, Springer-Verlag, Berlin, 1990.

[9] W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symb. Comp. **24** (1997), no. 3-4, 235–265, http://www.maths.usyd.edu.au:8000/u/magma/.

[10] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*, or Wild* 3*-adic exercises*, (2000), http://www.math.harvard.edu/HTML/Individuals/Richard_Taylor.html.

[11] A. Brumer, *The rank of* $J_0(N)$, Astérisque (1995), no. 228, 3, 41–68, Columbia University Number Theory Seminar (New York, 1992).

[12] K. Buzzard and W. A. Stein, *Modularity of some icosahedral Galois representations*, in preparation.

[13] H. Cohen and J. Oesterlé, *Dimensions des espaces de formes modulaires*, (1977), 69–78. Lecture Notes in Math., Vol. 627.

[14] R. Coleman, *The monodromy pairing*, Asian Math. Journal (1999).

[15] J. E. Cremona, *Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction*, Math. Proc. Cambridge Philos. Soc. **111** (1992), no. 2, 199–218.

[16] ———, *Algorithms for modular elliptic curves*, second ed., Cambridge University Press, Cambridge, 1997.

[17] ———, *Computing periods of cusp forms and modular elliptic curves*, Experiment. Math. **6** (1997), no. 2, 97–107.

[18] J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, to appear in Experiment. Math.

[19] H. Darmon, *Wiles' theorem and the arithmetic of elliptic curves*, Modular forms and Fermat's last theorem (Boston, MA, 1995), Springer, New York, 1997, pp. 549–569.

[20] H. Darmon and L. Merel, *Winding quotients and some variants of Fermat's last theorem*, J. Reine Angew. Math. **490** (1997), 81–100.

[21] F. Diamond and J. Im, *Modular forms and modular curves*, Seminar on Fermat's Last Theorem, Providence, RI, 1995, pp. 39–133.

[22] N. Dummigan, *Period ratios of modular forms*, to appear in Math. Annalen.

[23] B. Edixhoven, *L'action de l'algèbre de Hecke sur les groupes de composantes des jacobiennes des courbes modulaires est "Eisenstein"*, Astérisque (1991), no. 196–197, 7–8, 159–170 (1992), Courbes modulaires et courbes de Shimura (Orsay, 1987/1988).

[24] E. V. Flynn, F. Leprévost, E. F. Schaefer, W. A. Stein, M. Stoll, and J. L. Wetherell, *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, Math. of Comp. (2000).

[25] D. Goldfeld, *On the computational complexity of modular symbols*, Math. Comp. **58** (1992), no. 198, 807–814.

[26] J. González and J-C. Lario, $\mathbf{Q}$*-curves and their Manin ideals*, preprint (2000).

[27] B. Gross and D. Zagier, *Heegner points and derivatives of L-series*, Invent. Math. **84** (1986), no. 2, 225–320.

[28] B. H. Gross, *L-functions at the central critical point*, Motives (Seattle, WA, 1991), Amer. Math. Soc., Providence, RI, 1994, pp. 527–535.

[29] K. Hatada, *Multiplicity one theorem and modular symbols*, J. Math. Soc. Japan **33** (1981), no. 3, 445–470.

[30] H. Hijikata, *Explicit formula of the traces of Hecke operators for* $\Gamma_0(N)$, J. Math. Soc. Japan **26** (1974), no. 1, 56–82.

[31] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Princeton University Press, Princeton, N.J., 1985.

[32] D. R. Kohel, *Hecke module structure of quaternions*, preprint (1998).

[33] V. A. Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*, Proceedings of the International Congress of Mathematicians, Vol. I, II (Kyoto, 1990) (Tokyo), Math. Soc. Japan, 1991, pp. 429–436.

[34] ______, *On the structure of Shafarevich-Tate groups*, Algebraic geometry (Chicago, IL, 1989), Springer, Berlin, 1991, pp. 94–121.

[35] V. A. Kolyvagin and D. Y. Logachev, *Finiteness of* Ш *over totally real fields*, Math. USSR Izvestiya **39** (1992), no. 1, 829–853.

[36] S. Lang, *Algebra*, third ed., Addison-Wesley Publishing Co., Reading, Mass., 1993.

[37] W-C. Li, *Newforms and functional equations*, Math. Ann. **212** (1975), 285–315.

[38] J. I. Manin, *Parabolic points and zeta functions of modular curves*, Izv. Akad. Nauk SSSR Ser. Mat. **36** (1972), 19–66.

[39] B. Mazur, *Courbes elliptiques et symboles modulaires*, Séminaire Bourbaki, 24ème année (1971/1972), Exp. No. 414, Springer, Berlin, 1973, pp. 277–294. Lecture Notes in Math., Vol. 317.

[40] ______, *Modular curves and the Eisenstein ideal*, Inst. Hautes Études Sci. Publ. Math. (1977), no. 47, 33–186 (1978).

[41] ______, *Rational isogenies of prime degree (with an appendix by D. Goldfeld)*, Invent. Math. **44** (1978), no. 2, 129–162.

[42] ______, *On the arithmetic of special values of L functions*, Invent. Math. **55** (1979), no. 3, 207–240.

[43] ______, *Visualizing elements of order three in the Shafarevich-Tate group*, preprint (1999).

[44] B. Mazur and P. Swinnerton-Dyer, *Arithmetic of Weil curves*, Invent. Math. **25** (1974), 1–61.

[45] L. Merel, *Universal Fourier expansions of modular forms*, On Artin's conjecture for odd 2-dimensional representations (Berlin), Springer, 1994, pp. 59–94.

[46] ______, *L'accouplement de Weil entre le sous-groupe de Shimura et le sous-groupe cuspidal de* $J_0(p)$, J. Reine Angew. Math. **477** (1996), 71–115.

[47] J.-F. Mestre, *La méthode des graphes. Exemples et applications*, Proceedings of the international conference on class numbers and fundamental units of algebraic number fields (Katata) (1986), 217–242.

[48] J.-F. Mestre and J. Oesterlé, *Courbes de Weil semi-stables de discriminant une puissance m-ième*, J. Reine Angew. Math. **400** (1989), 173–184.

[49] J. S. Milne, *Étale cohomology*, Princeton University Press, Princeton, N.J., 1980.

[50] ———, *Abelian varieties*, Arithmetic geometry (Storrs, Conn., 1984), Springer, New York, 1986, pp. 103–150.

[51] ———, *Arithmetic duality theorems*, Academic Press Inc., Boston, Mass., 1986.

[52] A. Pizer, *An algorithm for computing modular forms on* $\Gamma_0(N)$, J. Algebra **64** (1980), no. 2, 340–390.

[53] K. A. Ribet, *On modular representations of* $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ *arising from modular forms*, Invent. Math. **100** (1990), no. 2, 431–476.

[54] ———, *Raising the levels of modular representations*, Séminaire de Théorie des Nombres, Paris 1987–88, Birkhäuser Boston, Boston, MA, 1990, pp. 259–271.

[55] K. Rubin, *The "main conjectures" of Iwasawa theory for imaginary quadratic fields*, Invent. Math. **103** (1991), no. 1, 25–68.

[56] ———, *Euler Systems*, Princeton University Press, Spring 2000, Annals of Mathematics Studies **147**, http://math.Stanford.EDU/~rubin/weyl.html.

[57] A. J. Scholl, *Motives for modular forms*, Invent. Math. **100** (1990), no. 2, 419–430.

[58] ———, *An introduction to Kato's Euler systems*, Galois Representations in Arithmetic Algebraic Geometry, Cambridge University Press, 1998, pp. 379–460.

[59] I. R. Shafarevich, *Exponents of elliptic curves*, Dokl. Akad. Nauk SSSR (N.S.) **114** (1957), 714–716.

[60] G. Shimura, *Sur les intégrales attachées aux formes automorphes*, J. Math. Soc. Japan **11** (1959), 291–311.

[61] ———, *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan **25** (1973), no. 3, 523–544.

[62] ———, *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994, Reprint of the 1971 original, Kan Memorial Lectures, 1.

[63] V. V. Šokurov, *Modular symbols of arbitrary weight*, Funkcional. Anal. i Priložen. **10** (1976), no. 1, 95–96.

[64] W. A. Stein, HECKE*: The modular symbols calculator*, Software (available online) (1999).

[65] G. Stevens, *Arithmetic on modular curves*, Birkhäuser Boston Inc., Boston, Mass., 1982.

[66] J. Sturm, *On the congruence of modular forms*, Number theory (New York, 1984–1985), Springer, Berlin, 1987, pp. 275–280.

[67] J. Tate, *On the conjectures of Birch and Swinnerton-Dyer and a geometric analog*, Séminaire Bourbaki, Vol. 9, Soc. Math. France, Paris, 1995, pp. Exp. No. 306, 415–440.

[68] C. Viola, *Arithmetic theory of elliptic curves. Lectures given at the 3rd session of the Centro Internazionale Matematico Estivo (CIME).*, Springer-Verlag, Berlin, 1997 (English).

[69] D. Zagier, *Modular parametrizations of elliptic curves*, Canad. Math. Bull. **28** (1985), no. 3, 372–384.

Index