UNIVERSITY OF CALIFORNIA SAN DIEGO

Algorithmic modular curve Chabauty-Coleman without equations

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

in

Mathematics

by

Chris Xu

Committee in charge:

Professor Kiran Kedlaya, Chair
Professor Jennifer Balakrishnan
Professor Shachar Lovett
Professor Aaron Pollack
Professor Cristian Popescu

2026

The Dissertation of Chris Xu is approved, and it is acceptable in quality and form for publication on microfilm and electronically.

University of California San Diego

2026

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

First and foremost, the author thanks his advisors Kiran Kedlaya and Aaron Pollack for their persistent encouragement and for countlessly many psychologically useful conversations over the years. The author thanks Jennifer Balakrishnan for pushing for the project, for her enthusiasm, and for her many helpful ideas. The author gives a special shoutout to Yongyuan Huang and Isabel Rendell for their contributions in the early stages of this project, and to Mingjie Chen and Jun Bo Lau for their initial code that suggested such a "model-free" algorithm was feasible. Additionally, the author thanks Brian Conrad and Maarten Derickx for several clarifying conversations about modular curves, and Tonghai Yang for remarking on the connections to restriction problems in the theory of automorphic forms.

This dissertation is currently being prepared for submission for publication of the material. The dissertation author was the primary investigator and author of this material.

VITA

2017–2021 Bachelor of Science, Massachusetts Institute of Technology

2021–2026 Teaching Assistant, Department of Mathematics
University of California, San Diego

2026 Doctor of Philosophy, University of California, San Diego

2026–2028/2029 Postdoctoral Researcher, Tsinghua University

FIELDS OF STUDY

Major Field: Mathematics

Studies in Pure Mathematics
Professors Kiran Kedlaya and Aaron Pollack

ABSTRACT OF THE DISSERTATION

Algorithmic modular curve Chabauty-Coleman without equations

by

Chris Xu

Doctor of Philosophy in Mathematics

University of California San Diego, 2026

Professor Kiran Kedlaya, Chair

On a modular curve of arbitrary congruence level, we introduce the notion of a "Makdisi symbol", a device that simultaneously gives a moduli-friendly coordinate system while also having an elegant Hecke theory. Concretely, these are cuspidal projections of products of two weight 1 Eisenstein series, and their study was originally pioneered by the work of Kamal Khuri-Makdisi. We show that a certain subclass of symbols, the "invertible Makdisi symbols", yield precisely the eigenforms of rank zero; combining this with the moduli interpretation, we obtain a systematic and relatively efficient algorithm to determine the rational points on a modular curve, so long as the curve has a rank zero eigenform. The algorithm is p-adic in nature, based on the method of

Chabauty-Coleman, and does not require finding any equations for the curve.

Introduction

Let $X/\mathbf{Q}$ be a curve of genus at least 2. By Faltings' theorem, $X(\mathbf{Q})$ is finite. However, the question of provably determining $X(\mathbf{Q})$ remains highly open in the general case. Despite this, a large class of curves can be tackled via *the method of Chabauty and Coleman*, which will be briefly described in the sequel.

Definition 0.0.1. We say that X satisfies the *Chabauty-Coleman condition* if there exists a quotient $\mathrm{Jac}(X) \twoheadrightarrow A_{/\mathbf{Q}}$ of the Jacobian of X, such that the Mordell-Weil rank r of $A(\mathbf{Q})$ is less than the dimension d of A.

If the Chabauty-Coleman condition holds for X, then in theory the method of Chabauty and Coleman will produce a finite set $X(\mathbf{Q}_p)_1$ containing $X(\mathbf{Q})$. In slightly more detail, p is a prime of good reduction, and $X(\mathbf{Q}_p)_1 \subset X(\mathbf{Q}_p)$ comes from zeroes of p-adic path integrals of certain *annihilating differentials* $V \leq H^0(X, \Omega^1)$.

In practice, it is hard to systematize the method to handle any sort of model thrown at it. This is the reason why most implementations of Chabauty-Coleman stick to hyperelliptic curves.

The goal of this paper is to show that if $X/\mathbf{Q}$ is a classical modular curve, then surprisingly, such a systematization is possible.

The GitHub repository that implements all of the algorithms below (minus the root-finding) can be found at [75]

Chapter 1

Preliminaries on elliptic curves and their moduli

In this section, we will introduce everything we need about elliptic curves, modular curves and modular forms. Because different authors set up different conventions for modular curves, we will give a thorough treatment of modular curves. To this end, we mostly follow [38].

1.1 Notation

Let $\widehat{\mathbf{Z}}$ denote the inverse limit $\varprojlim_n \mathbf{Z}/n\mathbf{Z}$, where the transition maps are precisely the reduction maps $\mathbf{Z}/mn\mathbf{Z} \twoheadrightarrow \mathbf{Z}/n\mathbf{Z}$. There is an isomorphism $\widehat{\mathbf{Z}} \xrightarrow{\sim} \prod_{p<\infty} \mathbf{Z}_p$. Let $\widehat{\mathbf{Q}} := \mathbf{A}_f$ denote the finite adele ring $\widehat{\mathbf{Z}} \otimes_{\mathbf{Z}} \mathbf{Q} = \prod_{p<\infty}(\mathbf{Q}_p, \mathbf{Z}_p)$. Let $\mathbf{A} := \mathbf{A}_{\mathbf{Q}}$ denote the adele ring $\mathbf{A} := \widehat{\mathbf{Q}} \times \mathbf{R}$.

Notation 1.1.1. If $\mathscr{G}_{/\mathbf{Z}}$ is an algebraic group, then we will denote elements of $\mathscr{G}(\mathbf{A})$ by the following:

- If $g \in \mathscr{G}(\mathbf{Q}) \hookrightarrow \mathscr{G}(\mathbf{A})$, we will just denote this as g.
- If p is a prime (finite or infinite), and $g \in \mathscr{G}(\mathbf{Q}_p)$, then we will denote $g_{(p)} \in \mathscr{G}(\mathbf{A})$ to be image of g under the inclusion $\mathscr{G}(\mathbf{Q}_p) \hookrightarrow \mathscr{G}(\mathbf{A})$.
- If M is an integer and $g \in \mathscr{G}(\mathbf{Z}/M\mathbf{Z})$, then we will let $g_M \in \mathscr{G}(\widehat{\mathbf{Z}})$ denote any lift of g under the surjection $\mathscr{G}(\widehat{\mathbf{Z}}) \to \mathscr{G}(\mathbf{Z}/M\mathbf{Z})$.

Fix an integer $N \geq 3$.

1.2 Elliptic curves with full level structure

By an *elliptic curve* $E \to S$, we mean a relative curve of genus 1 with smooth and geometrically connected fibers, with a marked point $0\colon S \to E$; then the space E becomes a group scheme via the usual slogan "three collinear points sum to zero" (the slogan holds at least affine-locally on S). By a *framing* of $E \to S$, we mean an fppf cover $T \to S$ and a homomorphism $\beta_0\colon \mathbf{Z}(N)^2 \to E[N](T)$ such that the set of images $\{\beta_0(a,b)\colon (a,b) \in \mathbf{Z}(N)^2\}$ form a "full set of sections" in the sense of [38]. (If N is invertible in $\mathscr{O}_S$, then we can take $T \to S$ to be étale, and β_0 to be an isomorphism.) Elements of $\mathbf{Z}(N)^2$ can be identified as row vectors (a,b) with entries in $\mathbf{Z}(N)$, and as such, framings can be identified as column vectors $\left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right]$ with entries A, B in $E[N](T)$. We will call the pair $(E_{/S}, \beta_0)$ a *framed elliptic curve*, and often we will omit the β_0.

By a *level N structure* on a framed elliptic curve $(E_{/S}, \beta_0)$, we mean a matrix $g := \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}_2(N)$, or more precisely, the homomorphism $\beta := \beta_0 \circ g\colon \mathbf{Z}(N)^2 \to E[N](T)$. If $\beta_0 := \left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right]$ is the framing of E, then β can be identified with $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]\left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right] = \left[\begin{smallmatrix} aA+bB \\ cA+dB \end{smallmatrix}\right]$. In this way, there is a natural left action of $\mathrm{GL}_2(N)$ on the level N structures of E, given by left multiplication of matrices. So the data of a framed elliptic curve with level structure is the tuple $((E_{/S}, \beta_0), g)$. We also say that the level structure is *defined over* T. If g is the identity matrix, then we may sometimes simply write $(E_{/S}, \beta_0)$.

Because $H^0(E, \Omega^1)$ is 1-dimensional (this is the definition of "genus 1"), there is an ambiguity in choice of $\omega \in H^0(E, \Omega^1)$, up to scaling by $\mathbf{G}_m$. Sometimes we will rigidify $((E_{/S}, \beta_0), g)$ further by making such a choice of ω. So the data of a framed elliptic curve with level structure and invariant differential is the tuple $((E_{/S}, \beta_0), \omega, g)$.

Now, suppose T is an étale cover of S for which the framing β_0 is defined. If N is invertible in $\mathscr{O}_S$, then there is a natural action of $\pi_1^{\acute{e}t}(S)$ on $E[N](T)$; the framing β_0 then yields the *mod N Galois representation* $\rho_{E,N}\colon \pi_1^{\acute{e}t}(S) \to \mathrm{GL}_2(N)$. Concretely, for $\sigma \in \pi_1^{\acute{e}t}(S)$, we get an automorphism $\sigma|_T\colon T \to T$, and then $\rho_{E,N}(\sigma) \in \mathrm{GL}_2(N)$ is defined as the unique matrix satisfying $\rho_{E,N}(\sigma) \cdot \beta_0 =$

$(\sigma|_T)_* \circ \beta_0$, the composition of β_0 with $(\sigma|_T)_*\colon E[N](T) \to E[N](T)$.

We recall the *Weil pairing*: it is a bilinear map of group schemes $e_N\colon E[N] \times E[N] \to \mu_N$. If $E_{/\mathbf{C}}$ is a complex elliptic curve given by the quotient $\mathbf{C}/(\tau\mathbf{Z}+\mathbf{Z})$, $\mathrm{Im}(\tau) > 0$, then we have

$$e_N\left(\frac{a\tau+b}{N}, \frac{c\tau+d}{N}\right) = \exp(2\pi i(ad-bc)/N).$$

1.3 Modular curves of full level

Fix a positive integer N. The scheme $Y(N)_{/\mathbf{Z}}$ parametrizes elliptic curves with full level N structure, and there is a canonical compactification $X(N)_{/\mathbf{Z}}$ obtained by "normalizing at the cusps". If $N \geq 3$ then these schemes are fine moduli spaces. In addition, we may identify $Y(N)(\mathbf{C})$ (resp. $X(N)(\mathbf{C})$) with a disjoint union of copies of the "classical" curve $\Gamma(N)\backslash\mathbf{H}$ (resp. $\Gamma(N)\backslash\mathbf{H}^*$), or even an adelic double quotient. Let us go into detail below.

We define $Y(N)_{/\mathbf{Z}}$ to be the moduli functor sending a scheme S to the set

$$Y(N)(S) := \{(E,\beta)\colon E/S,\ \beta \text{ level } N \text{ structure}\}/\sim,$$

where we define the equivalence relation $\sim$ by letting $(E,\beta) \sim (E',\beta')$ if there is an S-isomorphism $f\colon E \xrightarrow{\sim} E'$ such that $\beta' = f \circ \beta$. By [38, Corollary 4.7.1], the functor $Y(N)$ is representable by an affine scheme over $\mathbf{Z}$, whose geometric fibers are smooth everywhere except for the supersingular locus for primes p dividing N. In particular, $Y(N)$ is normal.

We compactify $Y(N)$ into $X(N)$ by "completing" along the cusps, described as follows. Recall that the coarse moduli functor $Y(1)_{/\mathbf{Z}}$ classifies elliptic curves and is isomorphic to $\mathrm{Spec}(\mathbf{Z}[j])$, where j is the *j-invariant*; we may embed $Y(1)$ inside of $X(1) \cong \mathbf{P}^1_{\mathbf{Z}}$ by gluing with $\mathrm{Spec}(\mathbf{Z}[1/j])$. Then, $X(N)_{/\mathbf{Z}[1/N]}$ is defined as the normalization of $X(1) \leftarrow Y(1)$ inside of $Y(N)$ along the map $Y(N) \to Y(1)$; it follows that $X(N)$ is proper as well.

The local ring around $j = \infty$ in $X(1)$ is isomorphic to $\mathbf{Z}[[q]]$; there is a distinguished elliptic

curve $\mathrm{Tate}(q)_{/\mathbf{Z}((q))}$ called the *Tate curve*, such that the structure morphism $\mathrm{Spec}(\mathbf{Z}((q))) \to X(1)$ factors through the above $\mathrm{Spec}(\mathbf{Z}[[q]])$. The Tate curve is isomorphic to the algebraic group $\mathbf{G}_m/q^{\mathbf{Z}}$, and as a result, after adjoining ζ_N and $q_N := q^{1/N}$ to the base, we may identify the level N structures on $\mathrm{Tate}(q)$ with the left $\mathrm{GL}_2(N)$-translates of the level structure $\begin{bmatrix} q_N \\ \zeta_N \end{bmatrix}$. Because $Y(1) \to X(1)$ is a compactification witnessed in the valuative criterion for properness by the inclusion $\mathrm{Spec}(\mathbf{Z}((q))) \to \mathrm{Spec}(\mathbf{Z}[[q]])$, we may represent points of the cuspidal subscheme $X(N)^\infty := X(N) - Y(N)$ by specifying a suitable level N structure on $\mathrm{Tate}(q)$; the actual "point" will correspond to the evaluation at $q = 0$. This perspective will be useful when we come to modular forms.

Let us give a detailed description of the complex points of $Y(N)$ and $X(N)$. Let $\mathbf{H}^* := \mathbf{H} \cup \mathbf{P}^1(\mathbf{Q})$ denote the extended upper half plane, endowed with the holomorphic structure as per [28, Section 2]. There is a natural action of $\mathrm{GL}_2^+(\mathbf{R})$ on $\mathbf{H}$ and a natural action of $\mathrm{SL}_2(\mathbf{Z})$ on $\mathbf{P}^1(\mathbf{Q})$. Their respective actions are given by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot \tau := \frac{a\tau + b}{c\tau + d}$$

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot [x : y] := [ax + by : cx + dy].$$

If $\Gamma(N)$ denotes the subgroup of $\mathrm{SL}_2(\mathbf{Z})$ consisting of matrices reducing to the identity modulo N, then the complex analytification $Y(N)(\mathbf{C})^{an}$ (resp. $X(N)(\mathbf{C})^{an}$) of $Y(N)$ (resp. $X(N)$) is biholomorphic to

$$\bigsqcup_{d \in \mathbf{Z}(N)^*} \Gamma(N) \backslash \mathbf{H} \text{ resp. } \bigsqcup_{d \in \mathbf{Z}(N)^*} \Gamma(N) \backslash \mathbf{H}^*.$$

This is a disconnected space whose components are distinguished by the value of the Weil pairing e_N considered as a global section of the structure sheaf: on the component $d \in \mathbf{Z}(N)^*$, the Weil pairing is the constant function $\exp(2\pi i d/N)$. Moreover, the identification of $X(N)(\mathbf{C})$ with the

extended upper half-plane quotient respects the natural left action of $\mathrm{GL}_2(N)$: letting (d,τ) denote the element $\tau \in \mathbf{H}^*$ on the component $d \in \mathbf{Z}(N)^*$, the identification is given by

$$\left(\mathbf{C}/(\mathbf{Z}\tau+\mathbf{Z}), \begin{bmatrix}\tau/N \\ d/N\end{bmatrix}\right) \mapsto (d,\tau)$$
$$\left(\mathrm{Tate}(q), \begin{bmatrix}q_N \\ \zeta_N^d\end{bmatrix}\right) \mapsto (d,[1:0]),$$

and the left action of $\mathrm{GL}_2(N)$ on the upper half-plane quotient is given simply by transporting over the left multiplication on the level structure. In particular, the cusps of $X(N)$ are given by pairs $(d,[a:b]) \in \mathbf{Z}(N)^* \times \mathbf{P}^1(\mathbf{Z}/N\mathbf{Z})$, as we may verify that $\Gamma(N)\backslash\mathbf{P}^1(\mathbf{Q}) \xrightarrow{\sim} \mathbf{P}^1(\mathbf{Z}/N\mathbf{Z})$: for a point in $\mathbf{P}^1(\mathbf{Q})$, take a representative $[a:b]$ such that $\gcd(a,b)=1$, and then reduce the coordinates modulo N.

Finally, let us mention the adelic perspective on the complex points of $Y(N)$ and $X(N)$. Let $K(N) \leq \mathrm{GL}_2(\widehat{\mathbf{Z}})$ denote the subgroup of matrices in $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ congruent to 1 modulo N.

Notation 1.3.1. Suppose B is an object that acts on the right on object A, and on the left on object C. We may form the fiber product $A \times_B C$ given by elements $(a,c) \in A \times C$, modulo the equivalence relations $(a,bc) \sim (ab,c)$ for any $b \in B$.

For any compact open subgroup $K^\infty \leq \mathrm{GL}_2(\widehat{\mathbf{Z}})$, define the double coset spaces

$$\mathrm{Sh}(K^\infty) := \mathrm{GL}_2(\mathbf{Q})\backslash \mathrm{GL}_2(\mathbf{A})/K^\infty$$
$$\mathrm{Sh}_X(K^\infty) := \mathbf{R}^\times_{>0}\mathrm{GL}_2(\mathbf{Q})\backslash \mathrm{GL}_2(\mathbf{A})/O(2)K^\infty.$$

(Note that $\mathrm{GL}_2(\mathbf{A}) = \mathrm{GL}_2(\widehat{\mathbf{Q}}) \times \mathrm{GL}_2(\mathbf{R})$. In these definitions, $\mathrm{GL}_2(\mathbf{Q})$ acts on the left via the diagonal embedding $\mathbf{Q} \hookrightarrow \mathbf{A}$, while K^∞ acts only the finite component $\mathrm{GL}_2(\widehat{\mathbf{Q}})$, while $O(2)$ acts only on $\mathrm{GL}_2(\mathbf{R})$.) We will represent elements of $\mathrm{Sh}(K^\infty)$ as tuples $(g_f, g_\infty) \in \mathrm{GL}_2(\widehat{\mathbf{Q}}) \times \mathrm{GL}_2^+(\mathbf{R})$ (note that $\mathrm{GL}_2^+(\mathbf{R})$ is OK, because the action of $\mathrm{GL}_2(\mathbf{Q})$ allows us to transfer the matrix $\left[\begin{smallmatrix}1 & 0 \\ 0 & -1\end{smallmatrix}\right]$ from the infinite to the finite places). We will represent elements of $\mathrm{Sh}_X(K^\infty)$ either as tuples (g_f, g_∞)

as before, or as tuples $(g_f, \tau) \in \mathrm{GL}_2(\widehat{\mathbf{Q}}) \times \mathbf{H}$; the matrix $g_\infty := \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}_2^+(\mathbf{R})$ will correspond to the element $\tau := \frac{ai+b}{ci+d}$. (Note that $\mathbf{R}^\times_{>0}\mathrm{SO}(2)$ preserves $i \in \mathbf{H}$ when acting on the left.)

Proposition 1.3.2. *The following hold:*

1. *The double quotient* $\mathrm{Sh}(K(N))$ *parametrizes isomorphism classes of triples* $(E_{/\mathbf{C}}, \omega, \beta)$ *where* E *is an elliptic curve over* $\mathbf{C}$*,* ω *is a holomorphic differential on* E*, and* β *is a level* N *structure on* E*.*

2. *The double quotient* $\mathrm{Sh}_X(K(N))$ *parametrizes isomorphism classes of pairs* $(E_{/\mathbf{C}}, \beta)$*, where* E *and* β *are as above. In particular* $\mathrm{Sh}_X(K(N))$ *is precisely* $Y(N)(\mathbf{C})$*.*

3. *The left action of* $\mathrm{GL}_2(N)$ *on the level structure* β *corresponds to the left action of* $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ *on the finite component of* $\mathrm{Sh}(K(N))$ *or* $\mathrm{Sh}_X(K(N))$*.*

Proof. First, we note the isomoprhisms

$$\mathrm{Sh}(K^\infty) = \mathrm{GL}_2(\mathbf{Q}) \backslash \mathrm{GL}_2(\mathbf{A}) / K^\infty \xrightarrow{\sim} K^\infty \backslash \mathrm{GL}_2(\widehat{\mathbf{Q}}) \times_{\mathrm{GL}_2^+(\mathbf{Q})} \mathrm{GL}_2^+(\mathbf{R})$$
$$\mathrm{Sh}_X(K^\infty) = \mathbf{R}^\times_{>0}\mathrm{GL}_2(\mathbf{Q}) \backslash \mathrm{GL}_2(\mathbf{A}) / O(2)K^\infty \xrightarrow{\sim} K^\infty \backslash \mathrm{GL}_2(\widehat{\mathbf{Q}}) \times_{\mathrm{GL}_2^+(\mathbf{Q})} \mathbf{H},$$

The first isomorphism identifies the class of $(g_f, g_\infty) \in \mathrm{GL}_2(\widehat{\mathbf{Q}}) \times \mathrm{GL}_2(\mathbf{R})$ with $(g_f^{-1}, g_\infty) \in \mathrm{GL}_2(\widehat{\mathbf{Q}}) \times \mathrm{GL}_2^+(\mathbf{R})$, again possibly after moving $\left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$ from the infinite to the finite place; the second isomorphism is similar, but identifying $g_\infty = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{GL}_2^+(\mathbf{R})$ with $\left[\begin{smallmatrix} ai+b \\ ci+d \end{smallmatrix}\right] \in \mathbf{H}$.

Let $\sigma_d := \left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right]_N$ for short. By strong approximation, we have the decompositions

$$\mathrm{GL}_2(\widehat{\mathbf{Q}}) = \bigsqcup_{d \in \mathbf{Z}(N)^*} K(N)\sigma_d \mathrm{GL}_2^+(\mathbf{Q})$$
$$\mathrm{GL}_2^+(\mathbf{Q}) = \bigsqcup_{\substack{d_1, d_2 \in \mathbf{Q} \\ d_1 | d_2}} \mathrm{SL}_2(\mathbf{Z})\mathrm{diag}(d_1, d_2)\,\mathrm{SL}_2(\mathbf{Z}).$$

For any element in $x \in \mathrm{Sh}(K(N))$ represented by $(g_f, g_\infty) \in \mathrm{GL}_2(\widehat{\mathbf{Q}}) \times \mathrm{GL}_2^+(\mathbf{R})$, we may use these decompositions to find a different representative of x of the form (σ_n, g'_∞), where $g'_\infty \in \mathrm{GL}_2^+(\mathbf{R})$ and $n \in \mathbf{Z}(N)^*$. There is a biholomorphism $\mathrm{GL}_2^+(\mathbf{R}) \xrightarrow{\sim} \mathbf{C}^\times \times \mathbf{H}$ given by sending $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ to $(j(g,i), \tau) := \left(ci+d, \frac{ai+b}{ci+d}\right)$. The data associated to x is therefore the tuple $(E, \omega, \beta) = \left(\mathbf{C}/(\tau\mathbf{Z}+\mathbf{Z}), j(g,i)\,dz, \left[\begin{smallmatrix} \tau/N \\ [n^{-1}]_N/N \end{smallmatrix}\right]\right)$. For the case of $\mathrm{Sh}_X(K(N))$, it is similar, except that ω is omitted.

The left action of $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ factors through $\mathrm{GL}_2(N)$, because $\mathrm{Sh}_X(K(N))$ and $\mathrm{Sh}(K(N))$ are right $K(N)$-orbits, and because $K(N)$ is normal in $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ (it is the kernel of the reduction mod N map). □

1.4 Modular curves of arbitrary level

For a subgroup G of $\mathrm{GL}_2(N)$, we may form coarse quotients $Y_G := G\backslash Y(N)$ and $X_G := G\backslash X(N)$. The scheme X_G can also be characterized by the normalization of $X(1)$ in Y_G:

$$\begin{array}{ccc} & & Y_G \\ & & \downarrow \\ X(1) & \longleftarrow & Y(1) \end{array}$$

Concretely, we may describe Y_G as follows.

Proposition 1.4.1. *Suppose $S_{/\mathbf{Z}[1/N]}$ is a scheme where at least one of the following holds:*

- *The integer 6 is invertible on S.*
- *S is the spectrum of a finite field.*
- *For $p | \gcd(6,N)$, the base change $S_{\mathbf{Z}_{(p)}}$ is flat over $\mathrm{Spec}(\mathbf{Z}_{(p)})$.*

Then, the set $Y_G(S)$ is in bijection with with the subset of

$$\{(j(E), [Gg\mu_E]) \in \mathscr{O}_S \times G\backslash \mathrm{GL}_2(N)/\mu_E : E_{/S} \text{ framed elliptic curve}\}$$

such that for all $\sigma \in \pi_1^{et}(S)$, we have $Gg\mu_E = Gg\rho_{E,N}(\sigma)\mu_E$. In other words, $\mathrm{im}(\rho_{E,N}) \subseteq g^{-1}Gg\mu_E$. *Here, μ_E is the group of automorphisms of E that are defined on some étale cover $T \to S$, the "geometric" automorphism group of E.*

Proof. By [38, Prop 8.1.6(3)], the following is valid for schemes $S_{/\mathbf{Z}[1/N]}$ on which either 6 is invertible, or which is flat after base change to $S_{\mathbf{Z}_{(p)}}$ for $p|\gcd(6,N)$: giving an S-point of X_G is the same as giving a diagram

$$\begin{array}{ccc} S' & \xrightarrow{\beta} & X(N) \\ \downarrow & & \\ S & & \end{array}$$

where S' is a G-torsor, and where $\beta\colon S' \to X(N)$ is G-equivariant. (Also, this characterization is valid when S is the spectrum of a finite field, because the coarse base change map is a universal homeomorphism on the special fibers.) Let us spell out this characterization in detail. By a G-torsor $S' \to S$, we mean an identification $\rho\colon \mathrm{Gal}(S'/S) \xrightarrow{\sim} G$; by a G-equivariant map $g := ((E_{/S'}, \beta_0), g)\colon S' \to X(N)$, we mean that for all $\gamma \in G$, the diagram

$$\begin{array}{ccc} S' & \xrightarrow{\rho(\gamma)} & S' \\ \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle g} \\ X(N) & \xrightarrow{\gamma} & X(N) \end{array}$$

commutes. Comparing the bottom and top transversals of the diagram, we obtain the following: for all $\gamma \in G$, there exists an automorphism of $E_{S'}$, whose restriction to $E[N]$ is represented by $a_\gamma \in \mathrm{GL}_2(N)$, such that $\gamma \cdot g = g \cdot \rho(\gamma) \cdot a_\gamma$. This is seen to be equivalent to the condition of the equality of double cosets $Gg\mu_E = Gg\rho_{E,N}(\sigma)\mu_E$ for all $\sigma \in \pi_1^{\acute{e}t}(S)$. □

Let us use this definition to describe the cusps of X_G. Let ∞ be the $\mathbf{Z}[1/N, \zeta_N]$-valued section of

$$X(N)^\infty := X(N) - Y(N)$$

represented by the framed elliptic curve

$$E := \left(\mathrm{Tate}(q), \begin{bmatrix} q_N \\ \zeta_N \end{bmatrix}\right).$$

The group μ_E is isomorphic to $U(N) := \pm\left\langle \left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right] \right\rangle$: the matrix $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ simply replaces q_N with a different choice of N-th root of q, and $\pm I$ is always in the automorphism group. The mod N Galois representation $\rho_{E,N}$ has image $\left\{ \left[\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right] \right\}$, because the Galois action factors through the action on the N-th roots of unity. Hence, rational points on $X_G^\infty := X_G - Y_G$ are in bijection with the subset of double cosets $GgU(N)$ such that for all $d \in \mathbf{Z}(N)^*$, we have $GgU(N) = Gg\sigma_d U(N)$.

Definition 1.4.2. The *width* of a cusp $g \cdot \infty$ is the smallest positive integer w such that the right coset Gg is stabilized by the right action of $\left[\begin{smallmatrix} 1 & w \\ 0 & 1 \end{smallmatrix}\right]$. The *cusp orbit* of $g \cdot \infty$ is the set of cusps associated to the double cosets $\{Gg\sigma_d U(N)\}_{d \in \mathbf{Z}(N)^*}$.

Let us now briefly describe the classical and adelic perspectives. Adelically, we may take the inverse image $K_G \leq \mathrm{GL}_2(\widehat{\mathbf{Z}})$ of $G \leq \mathrm{GL}_2(N)$ under the mod N reduction map, and then $Y_G(\mathbf{C})$ is identified with $\mathrm{Sh}_X(K_G)$; classically, the complex points of Y_G are given by

$$Y_G(\mathbf{C}) = G\backslash \left(\bigsqcup_{d \in \mathbf{Z}(N)^*} \Gamma(N)\backslash \mathbf{H} \right);$$

the compactified quotient X_G is given similarly, by replacing $\mathbf{H}$ with $\mathbf{H}^*$.

1.5 Generalities on modular forms

Modular forms are defined to be global sections of tensor powers of the tautological line bundle over the (compactified) modular curve. If the curve X_G is not a fine moduli scheme, then we may still recover a satisfactory definition by considering G-invariant sections on $X(N)$, although passing to G-invariants does not always commute with base change.

On $Y(N)$, there is the universal elliptic curve $\pi\colon \mathscr{E}(N) \to Y(N)$. As such, the relative sheaf of Kahler differentials $\pi_*\Omega^1_{\mathscr{E}(N)/Y(N)}$ is a line bundle, and we can extend this to a line bundle $\underline{\omega}$ on $X(N)$ by stipulating that, for a section f on a neighborhood of a cusp, with the cusp represented by $(\mathrm{Tate}(q),\beta)$, the evaluation $f(\mathrm{Tate}(q),\beta)$ is a power series in q with no negative exponents of q. A weight k modular form on $X(N)$ defined over a ring R is then an element of $H^0(X(N)_R,\underline{\omega}^{\otimes k})$. Letting C denote the cuspidal divisor, a weight k cusp form on $X(N)$ over R is an element of $H^0(X(N)_R,\underline{\omega}^{\otimes k}(-C))$, the modular forms that vanish on all cusps.

Remark 1.5.1. There is the following well-known characterization due to Katz. For a weight k modular form f on $X(N)$, then on a point $(E_{/R},\beta)\in X(N)(R)$, we may fix a holomorphic differential $\omega\in H^0(E,\Omega^1)$ and write f as $f(E,\omega,\beta)\,\omega^k$. There is a $\mathbf{G}_m$'s worth of ambiguity in our choice of ω, so if we want $f(E,\omega,\beta)\,\omega^k = f(E,\lambda\omega,\beta)(\lambda\omega)^k$ for all $\lambda\in R^\times$, we had better have $f(E,\omega,\beta)$ satisfy the property

$$f(E,\lambda\omega,\beta) = \lambda^{-k} f(E,\omega,\beta)$$

for all $\lambda\in R^\times$. Namely, we recover the definition of a modular form found in [37].

There is a natural right action of $\mathrm{GL}_2(N)$ on the space of modular forms, defined in the natural way: for a weight k modular form on $X(N)$, we define $f\mid_k g$ by $(f\mid_k g)(E,\omega,\beta) := f(E,\omega,g\cdot\beta)$. Then, a weight k modular form on X_G is defined to be a weight k modular form f on $X(N)$ that is invariant under the right action of $G\leq \mathrm{GL}_2(N)$. We denoted the space of weight k modular forms on X_G defined over the ring R as $M_k(X_G,R)$, and the subspace of cusp forms as $S_k(X_G,R)$.

Sometimes, we may access a modular form via its *q-expansion*.

Definition 1.5.2. Let f be a weight k modular form on $X(N)$, and let $g\in\mathrm{GL}_2(N)$. The *q-expansion of f* at the cusp $g\cdot\infty$ is the value of f on the tuple $\left(\mathrm{Tate}(q),dt/t,g\cdot\begin{bmatrix}q_N\\ \zeta_N\end{bmatrix}\right)$. Here, t is the local parameter induced by the canonical isomorphism $\mathbf{G}_m\xrightarrow{\sim}\mathrm{Spec}(\mathbf{Z}[t,t^{-1}])$, when $\mathrm{Tate}(q)$ is identified with $\mathbf{G}_m/q^{\mathbf{Z}}$. The definition of q-expansion is similar if $X(N)$ is replaced by X_G.

Remark 1.5.3. Let us be slightly more precise. If $w > 0$ is the width of a cusp $c := g \cdot \infty$ of X_G, then a modular form f on X_G will enjoy w different q-expansions "at" the cusp c, as

$$(f \mid_k g)(q) = \sum_{n=0}^{\infty} a_n q_w^n \quad \text{implies} \quad (f \mid_k g \left[\begin{smallmatrix} 1 & x \\ 0 & 1 \end{smallmatrix}\right])(q) = \sum_{n=0}^{\infty} a_n \zeta_w^{xn} q_w^n.$$

This same computation also shows that the q-expansion of f at a cusp with width w will have a power series expansion in terms of q_w.

We have the following theorem, known as the q-expansion principle.

Theorem 1.5.4. *Let R be a ring containing all N-th roots of unity, and let R' be a flat R-algebra. Suppose f is a modular form on X_G defined over R' such that for all $g \in \mathrm{GL}_2(N)$, the q-expansion of f at $g \cdot \infty$ lies in $R[\zeta_N][[q_N]]$. Then f descends to a modular form on $X(N)_R$, and for all $g \in \mathrm{GL}_2(N)$, the q-expansion of f at g lies in $\mathbf{Z}[\zeta_N][[q_N]] \otimes R$.*

Let us now describe the classical and adelic perspectives on modular forms. Classically, if $f\colon \mathbf{H}^* \to \mathbf{C}$ is a function, then, for k a nonnegative integer, there is a right "weight k" action of $\mathrm{GL}_2^+(\mathbf{R})$ on f, given by

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

where

$$j\left(\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right], \tau\right) := c\tau + d.$$

A weight k modular form with respect to a subgroup $\Gamma \leq \mathrm{SL}_2(\mathbf{Z})$ is then defined to be a holomorphic function $f\colon \mathbf{H}^* \to \mathbf{C}$, of moderate growth at the cusps (i.e. polynomial growth with respect to the parameter q^{-1} as q approaches 0), such that for all $\gamma \in \Gamma$, we have $f|_k\gamma = f$. (The exponent $k-1$ in $\det(\gamma)^{k-1}$ does not affect the definition; it is there to ensure that, for eigenfunctions of the Hecke algebra, the eigenvalue of the T_p operator matches with the p-th Fourier coefficient.) The q-expansion of f at ∞ can be obtained by expanding out f as a power series with respect to the

variable $q_N = \exp(2\pi i\tau/N)$. On the other hand, evaluation on the upper half-plane can be descrbed as evaluating on the corresponding elliptic curve: for $\tau \in \mathbf{H}$, we have

$$f(\tau) = f\left(\mathbf{C}/(\mathbf{Z}+\tau\mathbf{Z}), dz, \begin{bmatrix}\tau/N \\ 1/N\end{bmatrix}\right).$$

We may use the uniformization of $X(N)(\mathbf{C})$ by $\mathbf{H}^*$ to characterize a weight k modular form on $X(N)$ over $\mathbf{C}$ to be a tuple of functions $f := (f_d)_{d\in\mathbf{Z}(N)^*}$, each of which are weight k modular forms with respect to $\Gamma(N)$. Transferring over the action of $\mathrm{GL}_2(N)$ from the moduli description, we see that the right action of $\mathrm{SL}_2(N)$ is given by acting on each f_d by $\mathrm{SL}_2(\mathbf{Z})$, while for $n \in \mathbf{Z}(N)^*$ and $\sigma_n := \left[\begin{smallmatrix}1 & 0\\ 0 & n\end{smallmatrix}\right]_N$, we see that $f\mid_k \sigma_n = (f_{dn})_{d\in\mathbf{Z}(N)^*}$.

Let us describe the $\mathbf{Q}$-structure on $M_k(X(N),\mathbf{C})$. By the q-expansion principle, the space of modular forms $M_k(X(N),\mathbf{Q}(\zeta_N))$ can be characterized as tuples of functions $(f_d)_{d\in\mathbf{Z}(N)^*}$ such that each f_d has q-expansion lying in $\mathbf{Q}(\zeta_N)[[q_N]]$. The Weil pairing then gives a choice of ζ_N: simply let ζ_N be the value of the Weil pairing on the $d = 1$ component of $X(N)(\mathbf{C})$. The Galois action on the base, $\mathrm{Spec}(\mathbf{Q}(\zeta_N))$, yields via pullback an action of $\mathrm{Gal}(\mathbf{Q}(\zeta_N)/\mathbf{Q})$ on $M_k(X(N),\mathbf{Q}(\zeta_N))$ given by sending the element $\zeta_N \mapsto \zeta_N^d$ to the element $\sigma_d \in \mathrm{GL}_2(N)$. It follows that elements of $M_k(X(N),\mathbf{Q})$ can be described as modular forms for $\Gamma(N)$ whose q-expansion coefficients all lie in $\mathbf{Q}(\zeta_N)$; such an element $f = \sum_{n\geq 0} a_n q_N^n$ then yields a modular form for $X(N)$ given by $\left(\sum_{n\geq 0}\sigma_d(a_n)q_N^n\right)_{d\in\mathbf{Z}(N)^*}$. This description, combined with the q-expansion principle, allows us to describe the notion of a modular form defined over an arbitrary ring, in terms of its q-expansion coefficients.

There is a relationship between modular forms of weight 2 on $X(N)$ and holomorphic differentials on $X(N)$. To be precise, we have the following result:

Proposition 1.5.5 (Kodaira-Spencer isomorphism)**.** *Let D denote the cuspidal divisor of $X(N)$. Over $\mathbf{Z}[1/N]$, we have an isomorphism of line bundles* $\mathrm{KS}\colon \underline{\omega}^{\otimes 2} \xrightarrow{\sim} \Omega^1_{X(N)}(D)$*, given on global sections as follows: for f a weight 2 modular form, we have* $\mathrm{KS}(f) = f(q)\frac{dq}{q} = 2\pi i f(z)\,dz$.

Finally, let us briefly note the adelic perspective on modular forms. To a classical mod-

ular form $f := (f_d)_{d \in \mathbf{Z}(N)^*} \in M_k(X(N), \mathbf{C})$, we define its *adelization* $\phi_f \colon \mathrm{Sh}(K(N)) \to \mathbf{C}$ by the following: for each $\sigma_d := \left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right]_N$ and for each $g_\infty \in \mathrm{GL}_2^+(\mathbf{R})$, the function ϕ_f is characterized by the formula

$$\phi_f(\sigma_d, g_\infty) := (f_{d^{-1}} \mid_k g_\infty)(i) \cdot \det(g_\infty)^{2-k}.$$

(Similarly to before, the exponent $2-k$ of the determinant can be replaced by an arbitrary nonzero complex number, but is chosen simply so that the Hecke eigenvalues match up with the Hecke eigenvalues of the classical modular form.)

1.6 Hecke and diamond operators

If p is a prime not dividing the level N of $X(N)$, then the Hecke operator T_p can be defined on any quotient X_G of $X(N)$, and Hecke operators will commute with $X(N) \to X_G$. We will in fact see that because $X(N)$ is geometrically disconnected over $\mathbf{Q}$, the true definition does *not* always agree with operator one gets by naively extrapolating from the cases $X_0(N)$ or $X_1(N)$ (although in those cases the true and "naive" definitions will agree). We will define various diamond operators as well.

We recall the Hecke correspondence.

Notation 1.6.1. For N a positive integer, let $K_0(N) \leq \mathrm{GL}_2(N)$ denote the subgroup of upper triangular matrices; then it is well known that the corresponding modular curve $X_0(N)$ is the coarse moduli space parametrizing pairs (E, C), where E is an elliptic curve and $C \leq E[N]$ is a cyclic subgroup scheme (flat over the base) of order N.

The Hecke correspondence is defined to be the diagram

$$X(N) \xleftarrow[\mathrm{pr}_1]{} X(N) \times_{X(1)} X_0(p) \xrightarrow{\pi} X(N)$$

where pr_1 is projection onto $X(N)$, and where π is given on points by $\pi(E, \beta, C) = (E/C, \pi_C \circ \beta)$

(here $\pi_C \colon E \to E/C$ is the "mod C" isogeny). The Hecke operator T_p is then defined on points as $(T_p)_* := \pi_* \circ (\mathrm{pr}_1)^*$, and on sections as $T_p^* := (\mathrm{pr}_1)_* \circ \pi^*$.

We also recall various diamond operators.

Notation 1.6.2. For integers d coprime to N:

- Define $\sigma_d := \left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right]_N$.
- Define $\langle d \rangle := \left[\begin{smallmatrix} d^{-1} & 0 \\ 0 & d \end{smallmatrix}\right]_N$.
- Define $[d] := \left[\begin{smallmatrix} d & 0 \\ 0 & d \end{smallmatrix}\right]_N$.

The first goal is to re-express the Hecke operator T_p in more concrete terms.

Notation 1.6.3. Define $\Delta_p := \Delta_{p,1}$ to be the formal sum of representatives for the right coset space $\Gamma(N)\backslash\Gamma(N)\left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]\Gamma(N)$. Define $\Delta_{p,2}$ to be the formal sum of representatives for the right coset space $\Gamma(N)\backslash\Gamma(N)\left[\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right]\Gamma(N)$. So, for instance, if f is a weight k modular form on $X(N)$, then notate $f \mid_k \Delta_p$ for $\sum_{\alpha \in \Gamma(N)\backslash\Gamma(N)\left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]\Gamma(N)} f \mid_k \alpha$.

Proposition 1.6.4. *Let f be a modular form on $X(N)$, and let ϕ_f be its adelization. Let $\alpha \in \mathrm{Mat}_{2\times 2}(\mathbf{Z})$ be any integer matrix of determinant p, and recall that $\alpha_{(p)}$ denotes the element of $\mathrm{GL}_2(\widehat{\mathbf{Q}})$ that is α at the component p and trivial everywhere else.*

- *The adelization of $T_p f$ is precisely*

$$(\phi_f \mid [K(N)\alpha_{(p)}K(N)])(g_f, g_\infty) := \sum_{\gamma \in K(N)\backslash K(N)\alpha_{(p)}K(N)} \phi_f(g_f \cdot \gamma, g_\infty).$$

- *We have $T_p f = f \mid_k \Delta_p \mid_k \sigma_p = f \mid_k \Delta_{p,2} \mid_k \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]_N$.*

We observe that the choice of α does not matter, because $\mathrm{GL}_2(\mathbf{Z}_p)\alpha_{(p)}\mathrm{GL}_2(\mathbf{Z}_p)$ yields precisely the p-adically integral matrices of determinant p by the Cartan decomposition for p-adic groups.

Proof. Let us prove the second item first. Suppose f lies in $M_k(X(N), \mathbf{C})$, so that f is represented by modular forms $\{f_d\}_{d \in \mathbf{Z}(N)^*}$ on $\Gamma(N)\backslash\mathbf{H}$. Let ϕ_f be the adelization of f:

$$\phi_f\left(\left[\begin{smallmatrix} 1 & 0 \\ 0 & d^{-1} \end{smallmatrix}\right]_N, g_\infty\right) = (f_d \mid_k g_\infty)(i) \cdot \det(g_\infty)^{2-k}.$$

Then, take $\alpha = \left[\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right]$, so that $K(N)\alpha_{(p)}K(N) = \sqcup_i (\gamma_i \alpha)_p K^\infty$, where the γ_i are left coset representatives for the space $\mathrm{SL}_2(\mathbf{Z})/\Gamma_0(p)$; for example, one can take the γ_i to be the $p+1$ elements (with entries in $\mathbf{F}_p$)

$$\left\{ \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right], \ldots, \left[\begin{smallmatrix} 1 & 0 \\ p-1 & 1 \end{smallmatrix}\right], \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \right\}.$$

Since $p \nmid N$, we may take lifts of these elements to $\mathrm{SL}_2(\mathbf{Z})$ such that, they all reduce to the identity modulo N. Thus, we have

$$\begin{aligned}
\phi_f(\left[\begin{smallmatrix} 1 & 0 \\ 0 & d^{-1} \end{smallmatrix}\right]_N, g_\infty) \cdot T_p &= \sum_{i=0}^{p} \phi_f(\left[\begin{smallmatrix} 1 & 0 \\ 0 & d^{-1} \end{smallmatrix}\right]_N (\gamma_i \alpha)_{(p)}, g_\infty) \\
&= \sum_{i=0}^{p} \phi_f((\gamma_i \alpha)_{(p)} \left[\begin{smallmatrix} 1 & 0 \\ 0 & d^{-1} \end{smallmatrix}\right]_N, g_\infty) \\
&= \sum_{i=0}^{p} \phi_f(\alpha_N^{-1} (\gamma_i)_N^{-1} \left[\begin{smallmatrix} 1 & 0 \\ 0 & d^{-1} \end{smallmatrix}\right]_N, \alpha^{-1}\gamma_i^{-1} g_\infty) \\
&= \sum_{i=0}^{p} \phi_f(\left[\begin{smallmatrix} 1 & 0 \\ 0 & p^{-1}d^{-1} \end{smallmatrix}\right]_N, \left[\begin{smallmatrix} 1 & 0 \\ 0 & p^{-1} \end{smallmatrix}\right] \gamma_i^{-1} g_\infty) \\
&= \sum_{i=0}^{p} (f_{dp} \mid_k \left[\begin{smallmatrix} 1 & 0 \\ 0 & p^{-1} \end{smallmatrix}\right] \gamma_i^{-1} \mid_k g_\infty) \left(\sqrt{-1}\right) \det(p^{-1} g_\infty)^{2-k} \\
&= \sum_{i=0}^{p} (f_{dp} \mid_k \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right] \gamma_i^{-1} \mid_k g_\infty) \left(\sqrt{-1}\right) (p^{-1})^{k-2} \det(p^{-1} g_\infty)^{2-k}
\end{aligned}$$

which is precisely the adelization of the modular form $\tilde{f} := (\tilde{f}_d)_{d \in \mathbf{Z}(N)^*}$, where

$$\tilde{f}_d := \mathrm{Tr}^{\Gamma(N)}_{\Gamma(N)\cap\Gamma_0(p)} (f_{dp} \mid_k \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right])$$

taking note of the fact that the γ_i^{-1} now form right coset representatives for $(\Gamma(N) \cap \Gamma_0(p))\backslash\Gamma(N)$.

But now this is just

$$\tilde{f}_d = f_d \mid_k \sigma_p \mid_k [\Gamma(N) \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right] \Gamma(N)];$$

thus $T_p f = \tilde{f} = f \mid_k \sigma_p \mid_k \Delta_p$. Also, Δ_p and σ_p commute with each other because the former is supported on the archimedean place while the latter is supported at the mod N place. The equality of $T_p f$ with $f \mid_k \Delta_{p,2} \mid_k \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]_N$ proceeds in a completely similar fashion. This completes the proof of the second item.

For the first item, observe that during the computation, we saw that $\left(\left[\begin{smallmatrix} 1 & 0 \\ 0 & d^{-1} \end{smallmatrix}\right]_N, g_\infty\right)$ gets mapped to the set $\left\{\left(\left[\begin{smallmatrix} 1 & 0 \\ 0 & p^{-1}d^{-1} \end{smallmatrix}\right]_N, \left[\begin{smallmatrix} 1 & 0 \\ 0 & p^{-1} \end{smallmatrix}\right] \gamma_i^{-1} g_\infty\right)\right\}_{0 \le i \le p}$. If $\gamma_i^{-1} g_\infty$ corresponds to the complex elliptic curve $\mathbf{C}/(\omega_1 \mathbf{Z} + \omega_2 \mathbf{Z})$, then this mapping is taking $\left(\mathbf{C}/(\omega_1 \mathbf{Z} + \omega_2 \mathbf{Z}), \left[\begin{smallmatrix} \omega_1/N \\ \omega_2 \cdot d/N \end{smallmatrix}\right]\right)$ to

$$\left(\mathbf{C}/((\gamma_i^{-1} \cdot \omega)_1 \mathbf{Z} + (\gamma_i^{-1} \cdot \omega)_2 p^{-1} \mathbf{Z}), \left[\begin{smallmatrix} (\gamma_i^{-1} \cdot \omega)_1/N \\ (\gamma_i^{-1} \cdot \omega)_2 \cdot d/N \end{smallmatrix}\right]\right),$$

which corresponds precisely to the operation of taking an isogeny of degree p, for each cyclic subgroup of order p. Therefore, pullback by T_p corresponds to the double coset $K(N)\alpha_{(p)}K(N)$, and the first item follows. □

As a result of the computation above, we learn that the operator T_p satisfies some other very nice properties.

Corollary 1.6.5. *We have the following:*

- *For an inclusion of open subgroups $\pi\colon K_1 \hookrightarrow K_2$ of $\mathrm{GL}_2(\widehat{\mathbf{Z}})$, where the levels of the K_i are both coprime to p, we have $T_p \circ \pi = \pi \circ T_p$, where by abuse of notation we also let $\pi\colon X_{K_1} \to X_{K_2}$ be the corresponding map on modular curves.*
- *For different primes p_1 and p_2, we have $T_{p_1} T_{p_2} = T_{p_2} T_{p_1}$.*
- *On $\mathrm{Sh}_X(K(N))$, the operator T_p commutes with the natural right action of $\mathrm{GL}_2(N)$.*

Proof. It suffices to prove each equality on a dense open subset of the modular curve, so we may as well work with the complex points. Then, the equalities are all true for the reason that, in the computations in the above proposition, matrices at different components of $\widehat{\mathbf{Q}}$ can be "moved past" each other; for example, the first and third items are true because the component at p does not interact with the component at N, and the second item is true because the component at p_1 does not interact with the component at p_2. □

1.7 The Petersson inner product

Definition 1.7.1. There is a bilinear pairing on modular forms $\langle , \rangle_{X_G} : S_k(X_G) \times M_k(X_G) \to \mathbf{C}$, the *Petersson inner product*, given by

$$\langle f, g \rangle_{X_G} := \frac{1}{[\mathrm{GL}_2(N) : G]} \int_{X_G(\mathbf{C})} f(z)\overline{g(z)} y^{k-2}\, dx\, dy,$$

where we identify $X_G(\mathbf{C})$ with $G\backslash \left(\sqcup_{d \in \mathbf{Z}(N)^*} \Gamma(N) \backslash \mathbf{H}^* \right)$ as before.

The $\frac{1}{[\mathrm{GL}_2(N):G]}$ term ensures that the Petersson inner product is independent of replacing X_G with a cover $X_{G'}$ for $G' \leq G$.

Proposition 1.7.2. *Under the Petersson inner product, the adjoint of T_p is $T_p \langle p \rangle$; since this visibly commutes with T_p, it follows that T_p is diagonalizable, and the space $S_k(X(N), \mathbf{C})$ decomposes as a direct sum of "Hecke eigensystems" $S_k(X(N), \mathbf{C})[\mathfrak{m}]$, orthogonal to each other under the Petersson inner product. (Concretely, a Hecke eigensystem is a maximal ideal $\mathfrak{m}$ of the subring $\mathbf{T} := \mathbf{C}[\{T_p\}_{p \nmid N}]$ of $\mathbf{C}$-linear endomorphisms of $S_k(X(N), \mathbf{C})$.) Each Hecke eigensystem is also stable by the right action of* $\mathrm{GL}_2(N)$.

Proof. Let $f \in S_k$ and $g \in M_k$ be modular forms represented by $(f_d)_d$ and $(g_d)_d$. Then

$$\begin{aligned}\left\langle T_p f, g \right\rangle_{X(N)} &= \sum_{d \in \mathbf{Z}(N)^*} \int_{\Gamma(N)\backslash \mathbf{H}} \mathrm{Tr}^{\Gamma(N)}_{\Gamma(N)\cap\Gamma_0(p)} \left(f_{dp} \mid_k \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right] \right)(\tau) \overline{g_d(\tau)} y^{k-2}\, dx\, dy \\ &= \sum_{d \in \mathbf{Z}(N)^*} \int_{(\Gamma(N)\cap\Gamma_0(p))\backslash \mathbf{H}} p^{k-1} f_{dp}(p\tau) \overline{g_d(\tau)} y^{k-2}\, dx\, dy.\end{aligned}$$

Making the substitutions $d \mapsto dp^{-1}$ and $\tau \mapsto \tau/p$, we obtain that this integral equals

$$\sum_{d \in \mathbf{Z}(N)^*} \int_{(\Gamma(N)\cap\Gamma^0(p))\backslash \mathbf{H}} p^{-1} f_d(\tau) \overline{g_{dp^{-1}}(\tau/p)} y^{k-2}\, dx\, dy$$

which further simplifies to

$$\sum_{d \in \mathbf{Z}(N)^*} \int_{\Gamma(N)\backslash \mathbf{H}} f_d(\tau) \overline{\mathrm{Tr}^{\Gamma(N)}_{\Gamma(N)\cap\Gamma^0(p)} (g_{dp^{-1}} \mid_k \left[\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right])(\tau)} y^{k-2}\, dx\, dy,$$

but this is precisely $\left\langle f, g \mid_k \sigma_p \mid_k \Delta_{p,2} \right\rangle_{X(N)}$. Since $\Delta_{p,2} = T_p \left[\begin{smallmatrix} p^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right]_N$, it follows that $\sigma_p \Delta_{p,2}$ equals $T_p \langle p \rangle$. Thus we get

$$\left\langle T_p f, g \right\rangle_{X(N)} = \left\langle f, T_p \langle p \rangle g \right\rangle_{X(N)},$$

completing the proof. □

Chapter 2

Eichler-Shimura for geometrically disconnected modular curves

The purpose of this section is to verify that for a Hecke eigensystem $\mathfrak{m}$, the isogeny quotient associated to the $\mathfrak{m}$-isotypic component $H^0(X_G, \Omega^1)[\mathfrak{m}]$ is the "expected" abelian variety (recall that Proposition 1.5.5 allows us to identify holomorphic differentials with weight 2 cusp forms.) The appendix [27] does this for $\Gamma_1(N)$, and [65] or [66] work only with geometrically connected modular curves. Since [65] is hard to translate into today's language, I figured I would give a proof myself. We prove the following:

Theorem 2.0.1. *Let $\mathfrak{m}$ be a Hecke eigensystem such that $H^0(X_G, \Omega^1)[\mathfrak{m}] \neq 0$, and suppose that $\mathfrak{m}$ is associated to a newform orbit $[f] \in S_2(\Gamma_1(M))^{new}$, with corresponding abelian variety A_f. Then the quotient abelian variety $J_G/\mathfrak{m}J_G$ is a product of copies of A_f. Moreover, M must divide N^2.*

The section is organized as follows. First, we will review the Lie group-Lie algebra correspondence for Jacobians of curves, as well as classical Hecke theory. Next, we will give the initial reductions. Afterwards, we will use an Eichler-Shimura relation to finish off.

2.1 Setup and definitions

2.1.1 Review of Jacobians

Let $X/\mathbf{Q}$ be a smooth projective curve of positive genus g. The *Jacobian* $J := \mathrm{Pic}^0(X)$ of X, is the abelian variety over $\mathbf{Q}$ parametrizing precisely the degree 0 line bundles on X. If $D \subset X$ is an effective divisor of degree d, defined over $\mathbf{Q}$, then we may define an *Abel-Jacobi map* $\mathrm{AJ}_D \colon X \to J$ given on points by $x \mapsto [d \cdot x - D]$. The cotangent space $\mathrm{Lie}(J)^\vee$ can be identified with $H^0(X, \Omega^1)$ by pulling back an invariant differential on J along AJ_D. The ring $\mathrm{End}_{\mathbf{Q}}(J)$ of endomorphisms of J (defined over $\mathbf{Q}$) acts on both J and $H^0(X, \Omega^1)$, and if $\mathfrak{m}$ is a two-sided ideal of $\mathrm{End}_{\mathbf{Q}}(J)$, then we may identify $H^0(X, \Omega^1)[\mathfrak{m}]$ as the cotangent space of $J/\mathfrak{m}J$. This gives a correspondence between $\mathfrak{m}$-isotypic components of $H^0(X, \Omega^1)$ and $\mathfrak{m}$-isotypic components of J (up to isogeny). We will call $J/\mathfrak{m}J$ the *isogeny quotient associated to* $H^0(X, \Omega^1)[\mathfrak{m}]$.

The Abel-Jacobi map induces an isomorphism $J^\vee \cong J$, where $J^\vee$ is the dual abelian variety parametrizing line bundles on J. For any correspondence r on X, there are pushforward and pullback endomorphisms r_* and r^* of J. They are dual to each other: if d is the degree of r, then $r_* \circ r^* = r^* \circ r_* = [d]$ (multiplication by d), as elements of $\mathrm{End}_{\mathbf{Q}}(J)$.

2.1.2 Hecke theory

Let $\mathbf{T}_G$ denote the subring of $\mathrm{End}_{\mathbf{Q}}(J_G)$ generated by T_p, for all $p \nmid N$. By a *Hecke eigensystem* $\mathfrak{m}$, we mean the intersection of a maximal ideal $\mathfrak{m}_{\mathbf{C}} \leq \mathbf{T}_G \otimes \mathbf{C}$ with $\mathbf{T}_G$. It is known that, for $G = K_1(N)$, each Hecke eigensystem $\mathfrak{m}$ of $\mathbf{T}_1(N)$ can be uniquely associated to a Galois orbit of weight 2 newforms $[f] \in S_2(\Gamma_1(M))^{new}$, for some M dividing N. Moreover, the $\mathfrak{m}$-isotypic component of $J_1(N)$ decomposes into a product of copies of $A_f := J_1(M)/\mathfrak{m}J_1(M)$. The number of copies is precisely the number of divisors of N/M, and the copies appear precisely due to "degeneracy maps" $f(\tau) \mapsto f(e\tau)$ for each divisor e of N/M.

2.2 The conjugation trick

Let us now proceed to prove Theorem 2.0.1 in earnest. Because the action of Hecke commutes with modular maps, we may replace X_G with $X(N)$. Then $X(N)$ enjoys not only an action of $\mathbf{T}(N)$, but also an action of $\mathrm{GL}_2(N)$ that commutes with $\mathbf{T}(N)$. We recall some diamond operators which were defined in Notation 1.6.2; we spell them out here for convenience.

Notation 2.2.1. For integers d coprime to N:

- Define $\sigma_d := \left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right]_N$.
- Define $\langle d \rangle := \left[\begin{smallmatrix} d^{-1} & 0 \\ 0 & d \end{smallmatrix}\right]_N$.
- Define $[d] := \left[\begin{smallmatrix} d & 0 \\ 0 & d \end{smallmatrix}\right]_N$.

Let $\mathbf{T}(N)^0$ be the ring extension of $\mathbf{T}(N)$ given by adjoining the endomorphisms σ_d and $\langle d \rangle$.

Notation 2.2.2. Define the following:

- Let $X(N)'$ denote $\left\{\left[\begin{smallmatrix} 1 & 0 \\ 0 & * \end{smallmatrix}\right]\right\} \backslash X(N)$. Elements are parametrized by triples (E, P, C), where E is an elliptic curve, P is an N-torsion point, and C is a cyclic subgroup of order N disjoint from the group generated by P.
- Let $K_1(M)$ and $K_0(M)$ denote the respective subgroups of $\mathrm{GL}_2(\widehat{\mathbf{Z}})$ given by the inverse image of the mod M reduction map of matrices of the form

$$\begin{bmatrix} 1 & * \\ 0 & * \end{bmatrix} \quad \text{resp.} \quad \begin{bmatrix} * & * \\ 0 & * \end{bmatrix}.$$

- Let $X_H(N^2)$ denote the quotient of $X(N^2)$ by $K_1(N) \cap K_0(N^2)$. Elements are parametrized by tuples

$$(\pi \colon E \to E', \pi' \colon E' \to E'', P),$$

where π and π' are cyclic of order N, where $\pi' \circ \pi$ is cyclic of order N^2, and where P is a generator of the kernel of the dual isogeny $\pi^\vee : E' \to E$.

We first observe that, as $\mathbf{Z}[1/N]$-schemes, $X(N)' \times_{\mathbf{Z}[1/N]} \mathbf{Z}[1/N, \zeta_N]$ is isomorphic to $X(N)$. Indeed, given a point $\left(E, \left[\begin{smallmatrix} P \\ Q \end{smallmatrix}\right]\right)$ of $X(N)$, we may associate the tuple $((E, P, \langle Q \rangle), e_N(P,Q))$. As a consequence, we have that, up to isogeny, $J(N) = \mathrm{Res}_{\mathbf{Z}[1/N,\zeta_N]/\mathbf{Z}[1/N]} J(N)'_{\mathbf{Z}[1/N,\zeta_N]}$.

We next observe that, as $\mathbf{Z}[1/N]$-schemes, $X_H(N^2)$ is isomorphic to $X(N)'$. Indeed, the tuple

$$(\pi : E \to E', \pi' : E' \to E'', P)$$

can be identified with $(E', P, \ker(\pi'))$. Since, on the level of groups, this is given by conjugation by the matrix $\left[\begin{smallmatrix} N & 0 \\ 0 & 1 \end{smallmatrix}\right]$, the isomorphism we just exhibited is known as the *conjugation trick*.

2.3 Some descent

The idea behind our proof of Theorem 2.0.1 is to prove it for manageable pieces of $J(N)$. By the theory of degeneracy operators, it suffices to prove the theorem for $A := \mathrm{Res}_{\mathbf{Q}(\zeta_N)/\mathbf{Q}} A_f$, where $[f]$ is a newform orbit of level M and nebentypus $[\psi]$. By the definition of $X_H(N^2)$, the level M must divide N^2, and the nebentypus ψ must have conductor dividing $\gcd(M,N)$. If V_f is the $\mathbf{Q}$-vector space of holomorphic differentials associated to A_f, then the abelian variety A is associated to $V_A := V_f \otimes_{\mathbf{Q}} \mathbf{Q}(\zeta_N)$, considered as a $\mathbf{Q}$-vector space.

The abelian variety A has a further action of the $\{\sigma_d\}_{d \in \mathbf{Z}(N)^*}$, and as such we obtain a decomposition $A \cong \prod_\chi A_{[f,\chi]}^{e_{[f,\chi]}}$ for suitable integers $e_{[f,\chi]}$. The abelian variety $A_{[f,\chi]}$ is associated to the subspace $V_{f,\chi}$ of V_A spanned by the Galois orbits of the element $f_\chi := \sum_{d \in \mathbf{Z}(M)^*} \overline{\chi}(d) \zeta_M^d f$ in $V_A \otimes_{\mathbf{Q}} \mathbf{C}$. Indeed, we see that $\sigma_{d'}$ acts on f_χ by multiplication by $\chi(d')$, since $\sigma_{d'}$ sends ζ_M^d to $\zeta_M^{dd'}$. Moreover, $A_{[f,\chi]}$ has Hecke eigenvalues agreeing with those on $A_{f \otimes \chi}$, where $f \otimes \chi$ is the twist of f by χ. Indeed, Δ_p acts on f_χ by multiplication by a_p, therefore $T_p = \Delta_p \sigma_p$ acts by $a_p \chi(p)$, which is precisely the T_p-eigenvalue of $f \otimes \chi$.

What remains to be seen is that $A_{[f,\chi]}$ is isomorphic to $A_{f\otimes\chi}$.

2.4 Eichler-Shimura

Let p be a prime not dividing N. The absolute Frobenius Fr_p acts on the modular curve $X(N)_{\mathbf{F}_p}$. On the universal elliptic curve $\mathscr{E} \to X(N)$, there is an associated *relative Frobenius*

$$\pi_{\mathrm{Fr}} \colon \mathscr{E}_{\mathbf{F}_p} \to \mathscr{E}_{\mathbf{F}_p}^{(p)}$$

over $X(N)_{\mathbf{F}_p}$. On functor of points, the map Fr_p sends (E,β) to $(E^{(p)}, \pi_{\mathrm{Fr}}(\beta))$.

The goal of this section is to prove the following.

Proposition 2.4.1. *The characteristic polynomial of* Fr_p *acting on* $H^1_{et}(X(N), \mathbf{Q}_\ell)$ *is given by*

$$X^2 - (\Delta_p)_* X + p[p]_* \in \mathbf{T}(N)^0[X],$$

a quadratic polynomial over the commutative subring of endomorphisms $\mathbf{T}(N)^0$.

First, we prove:

Proposition 2.4.2. *Let* $p \nmid N$. *As elements of* $\mathrm{End}_{\mathbf{F}_p}(J(N))$, *we have the equalities*

$$(T_p)_* = (\mathrm{Fr}_p)_* + [p]_* (\mathrm{Fr}_p)^*$$
$$(\mathrm{Fr}_p)_* \begin{bmatrix} p^{-1} & 0 \\ 0 & 1 \end{bmatrix}_* = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}_* (\mathrm{Fr}_p \, \sigma_p^{-1})_* \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}_*$$

Proof. Let us deal with the first item. We will compute the image of T_p on a Zariski dense subset of $X(N)_{\mathbf{F}_p}$. We can compute T_p on the ordinary locus. Let $E/W(\bar{\mathbf{F}}_p)$ be an elliptic curve over the Witt vectors of $\bar{\mathbf{F}}_p$, with special fiber $\overline{E}$ and generic fiber E_η. Of the $p+1$ order p subgroups of $E_\eta[p]$, exactly one of them is the kernel of mod p reduction (giving one copy of $(\mathrm{Fr}_p)_*$), and the other p subgroups will reduce mod p to the etale subgroup scheme $\overline{E}[p]^{red}$ (giving one copy of $[p]_* \mathrm{Fr}_p^*$;

note that Fr_p has degree p). Because $(T_p)_*$ has degree $p+1$, it follows that $(T_p)_*$ must necessarily be $(\mathrm{Fr}_p)_* + [p]_*(\mathrm{Fr}_p)^*$ (which we had verified equals $(T_p)_*$ on a Zariski dense subset).

Let us now deal with the second item. We have

$$\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \mathrm{Fr}_p \, \sigma_p^{-1} \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]^{-1} = \mathrm{Fr}_p \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right] \sigma_p^{-1} \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]^{-1}$$

which simplifies to $\mathrm{Fr}_p \left[\begin{smallmatrix} p^{-1} & 0 \\ 0 & 1 \end{smallmatrix}\right]$, since $\sigma_p = \left[\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right]$. (The reason we can move the Fr_p term to the left is because it is acting on the $E[N]$ side of the level structure, while the matrices are acting on the $\mathbf{Z}(N)^2$ side.)

This completes the proof. □

Now, we will prove Proposition 2.4.1.

Proof of Proposition 2.4.1. Fix an isomorphism $\overline{\mathbf{Q}}_\ell \cong \mathbf{C}$. For any smooth projective curve X over $\mathbf{Q}$, we have functorial isomorphisms between the system of realizations of motives associated to X:

$$V := H^1_{et}(X, \overline{\mathbf{Q}}_\ell) \cong H^1_B(X, \mathbf{Z}) \otimes_{\mathbf{Z}} \mathbf{C} \cong H^1_{dR}(X) \otimes_{\mathbf{Q}} \mathbf{C}.$$

The Hodge decomposition allows us to write

$$H^1_{dR}(X) \otimes \mathbf{C} \cong H^0(X, \Omega^1) \oplus \overline{H^0(X, \Omega^1)}.$$

Specializing to the case when $X = X(N)$, we learn from the Hodge decomposition that V is a free $\mathbf{T}(N)^0$-module of rank 2; indeed, given an eigenform $f \in H^0(X, \Omega^1)$, the conjugate $\bar{f}$ will have T_p-eigenvalue the complex conjugate of that of f, so on the level of Galois orbits, the actions of T_p agree.

Next, we see that we may multiply the first Eichler-Shimura relation by σ_p^{-1} to obtain

$$(\Delta_p)_* = (\mathrm{Fr}_p\,\sigma_p^{-1})_* + \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]_* (\mathrm{Fr}_p)^*.$$

On one hand, if we let X denote $\mathrm{Fr}_p\,\sigma_p^{-1}$, we can multiply both sides of the equation by X_* and rearrange, noting that $X_* X^* = p$, to obtain

$$X_*^2 - (\Delta_p)_* X_* + p\,\langle p\rangle_* = 0.$$

On the other hand,

$$\mathrm{Tr}((\Delta_p)_*|V) = \mathrm{Tr}((\mathrm{Fr}_p\,\sigma_p^{-1})_*|V) + \mathrm{Tr}(\left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]_* (\mathrm{Fr}_p)^*|V).$$

Under the (dual of the) Weil pairing $e_{\ell^\infty}^\vee : V \times V \to \mathbf{Q}_\ell$, an endomorphism is adjoint to its dual: for $\phi \in \mathrm{End}(J)$, we have

$$e_{\ell^\infty}^\vee(P, \phi_*(Q)) = e_{\ell^\infty}^\vee(\phi^* P, Q).$$

It follows that the trace of an endomorphism acting on etale cohomology agrees with the trace of the dual endomorphism. We note that the dual of $(\mathrm{Fr}_p\,\sigma_p^{-1})_*$ is precisely $\left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]_* (\mathrm{Fr}_p)^*$, and thus

$$\mathrm{Tr}((\Delta_p)_*|V) = 2\,\mathrm{Tr}((\mathrm{Fr}_p\,\sigma_p^{-1})_*|V).$$

Recalling that V is simply two copies of $S_2(X(N))$, we learn that $\mathrm{Tr}(\Delta_p|S_2) = \mathrm{Tr}((\mathrm{Fr}_p\,\sigma_p^{-1})_*|V)$.

Combining with the equation of X_*, we learn that the characteristic polynomial of $X = \mathrm{Fr}_p\,\sigma_p^{-1}$ acting on V, as a $\mathbf{T}(N)^0$-module, is given by $X^2 - \Delta_p X + p\,\langle p\rangle = 0$. Thus, since σ_p lies in $\mathbf{T}(N)^0$, the characteristic polynomial of $\mathrm{Fr}_p = X\sigma_p$ acting on V is given by

$$X^2 - \Delta_p \sigma_p X + p\,\langle p\rangle\,\sigma_p^2,$$

which simplifies to $X^2 - T_p X + p[p]$ as expected. □

2.5 End of proof

In this subsection, we complete the proof of Theorem 2.0.1.

Proof of Theorem 2.0.1. As we saw in Section 2.3, the abelian variety $A_{[f,\chi]}$ has the same Hecke eigenvalues as $A_{f\otimes\chi}$. On $A_{[f,\chi]}$, we have $\Delta_p = a_p(f)$, $\langle d\rangle = \psi(d)$ and $\sigma_d = \chi(d)$. Thus, $[d] = \langle d\rangle\, \sigma_d^2 = (\psi\chi^2)(d)$. Applying Proposition 2.4.1, we learn that the characteristic polynomial of Fr_p acting on $H^1_{et}(A_{[f,\chi]}, \mathbf{Q}_\ell)$ is given by

$$X^2 - a_p(f)\chi(p)X + p\cdot(\psi\chi^2)(p),$$

which is precisely the characteristic polynomial for $A_{f\otimes\chi}$. By Falting's isogeny theorem (even a special case for GL_2-type abelian varieties works, as given by [59]), we learn that $A_{[f,\chi]} = A_{f\otimes\chi}$. In other words, on a piece of $J(N)$ where T_p acts like it acts on $f\otimes\chi$, the abelian variety is actually $A_{f\otimes\chi}$. This completes the proof. □

By [43], we obtain the following crucial corollary:

Theorem 2.5.1. *Consider the abelian variety A corresponding to $S_2(X_G)_{rk=0}$, the $\mathbf{Q}$-span of weight 2 cusp eigenforms f on X_G corresponding to Hecke eigensystems whose corresponding newforms $\tilde{f} \in S_2(\Gamma_1(M))^{new}$ are of analytic rank zero (i.e. $L(\tilde{f},1) \neq 0$). Then $A(\mathbf{Q})$ is finite.*

Chapter 3

The method of Chabauty and Coleman, for modular curves

In this section we will recall Coleman integrals and the method of Chabauty and Coleman. This is an algorithm that outputs a finite set $X(\mathbf{Q}_p)_1$, contained in $X(\mathbf{Q}_p)$, and containing $X(\mathbf{Q})$. For the case of $X = X_G$ a modular curve, we will describe $X_G(\mathbf{Q}_p)_1$ explicitly in terms the vanishing locus of certain effectively computable Coleman integrals; we defer algorithms on how to compute these integrals to later sections. In particular, we prove the following theorem in this section:

Theorem 3.0.1. *Suppose that $X := X_G$ has a nontrivial rank zero isogeny quotient. Then $X(\mathbf{Q}_p)_1$ is a finite set containing $X(\mathbf{Q})$, and, on a residue disk $]U[$ of a point $U \in X(\mathbf{F}_p)$, the intersection $X(\mathbf{Q}_p)_{1,]U[}$ of $X(\mathbf{Q}_p)_1$ and $]U[$ can be given explicitly as follows.*

Let t be a uniformizing parameter on U, so that $]U[(\mathbf{Q}_p)$ gets identified with $p\mathbf{Z}_p$. Suppose that applying the Hecke operator T_p to $t = 0$ gives the points $t = \alpha_0, \ldots, \alpha_{(p)}$. Then $X(\mathbf{Q}_p)_{1,]U[}$ can be identified (under the parameter t) with the finite set

$$\left\{ x \in p\mathbf{Z}_p : \int_0^x \mathrm{KS}(f)(t)\,dt = \sum_{i=0}^{p} \int_0^{\alpha_i} \mathrm{KS}((p+1-T_p)^{-1} f)(t)\,dt \text{ for all } f \in S_2(X_G)_{rk=0} \right\}.$$

3.1 Coleman integration

Let $X/\mathscr{O}_{\mathbf{C}_p}$ be a curve over the ring of integers $\mathscr{O}_{\mathbf{C}_p}$ of $\mathbf{C}_p$, the completion of the algebraic closure $\bar{\mathbf{Q}}_p$ of $\mathbf{Q}_p$. A *wide open subspace* of X is defined to be any rigid analytic subspace W of X^{rig} that is the complement of a finite number of disjoint closed disks of radius < 1. The theory of Coleman integration then posits the existence of a well-defined bilinear pairing $\mathrm{Col}\colon \mathrm{Div}^0(W) \times H^0(W,\Omega^1) \to \mathbf{C}_p$, with notation $\int_D \omega := \mathrm{Col}(D,\omega)$, characterized by the following properties:

- If $\varphi\colon X \to X'$ is a morphism, then $\int_{\varphi_* D} \omega = \int_D \varphi^* \omega$.
- If $D = \sum_i [x_i] \in \mathrm{Div}^0(W)$ is supported on a single residue disk $]x[$, then we may choose a local uniformizer t on $]x[$, write $\omega =: f(t)\,dt \in \mathscr{O}_{\mathbf{C}_p}[\![t]\!]$, find a primitive $F \in \mathbf{C}_p[\![t]\!]$ such that $F'(t) = f(t)$, and compute $\int_D \omega = \sum_i F(t(x_i))$. Concretely, if $D = [Q] - [P]$ for $P, Q \in]x[$, and if $\omega = \sum_{i=0}^{\infty} a_i t^i\,dt$, then we may compute $\int_D \omega$ as

$$\begin{aligned}\int_{t(P)}^{t(Q)} f(t)\,dt &= \left[\sum_{i=1}^{\infty} a_{i-1}\frac{t^i}{i}\right]_{t(P)}^{t(Q)} \\ &= \sum_{i=1}^{\infty} \frac{a_{i-1}}{i}(t(Q)^i - t(P)^i).\end{aligned}$$

We will call notation such as $\int_D \omega$ a *Coleman integral*, and we will refer to the pairing as *Coleman integration*.

3.2 A crash course on Chabauty-Coleman

Here is a brief rundown of Chabauty-Coleman. Recall $X/\mathbf{Q}$ is a smooth projective curve of genus $g \geq 2$ with good reduction at prime p. Let J be the Jacobian of X. Choose a divisor D on X defined over $\mathbf{Q}$ of degree d, and define the morphism $\mathrm{AJ}_D\colon X \to J$ given by the rule $x \mapsto [d \cdot x - D]$; since D is defined over $\mathbf{Q}$, the map AJ_D is also defined over $\mathbf{Q}$. Let $\pi_{/\mathbf{Q}}\colon J \twoheadrightarrow A$ witness $A/\mathbf{Q}$ as an

abelian variety quotient of J, and consider the diagram

$$\begin{array}{ccc} X(\mathbf{Q}) & \longrightarrow & X(\mathbf{Q}_p) \\ \downarrow & & \downarrow \\ A(\mathbf{Q}) & \longrightarrow & A(\mathbf{Q}_p) \end{array}$$

where the horizontal arrows are inclusions and the vertical arrows are $\pi \circ \mathrm{AJ}_D$. Let $\overline{A(\mathbf{Q})}^{(p)}$ denote the p-adic closure of $A(\mathbf{Q})$ in the p-adic analytic group $A(\mathbf{Q}_p)$. Chabauty's idea was the following:

Theorem 3.2.1. *If* $\mathrm{rk}_{\mathbf{Z}}(A(\mathbf{Q})) < g$, *then* $\overline{A(\mathbf{Q})}^{(p)} \cap X(\mathbf{Q}_p)$ *is a finite subset of* $X(\mathbf{Q}_p)$ *containing* $X(\mathbf{Q})$.

Forty years later, Coleman was able to turn Chabauty's ideas into an algorithm. He did this by imposing a coordinate system on $A(\mathbf{Q}_p)$ given by a basis of holomorphic differentials.

Theorem 3.2.2. *Let* $V \leq H^0(A_{\mathbf{Q}_p}, \Omega^1) \leq H^0(X_{\mathbf{Q}_p}, \Omega^1)$ *denote the sub-*$\mathbf{Q}_p$*-vector space of holomorphic differentials* ω *on* $A_{\mathbf{Q}_p}$ *such that* $\omega|_{\overline{A(\mathbf{Q})}^{(p)}} = 0$. *Assume* $\mathrm{rk}_{\mathbf{Z}}(A(\mathbf{Q})) < g$. *Then the set*

$$X(\mathbf{Q}_p)_1 := \left\{ x \in X(\mathbf{Q}_p) \colon \int_D^{d \cdot x} \omega = 0 \text{ for all } \omega \in V \right\}$$

is a finite set containing $X(\mathbf{Q})$.

3.3 Application to modular curves

Now we specialize to the case when $X := X_G$ is a modular curve. We will assume from now on that $G \leq \mathrm{GL}_2(N)$ has surjective determinant and contains all scalar matrices, and we choose a prime $p \geq 5$ not dividing N. Let J_G be the Jacobian of X, and recall that for all abelian variety quotients A of J_G defined over $\mathbf{Q}$, the rank $\mathrm{rk}_{\mathbf{Z}}(A(\mathbf{Q}))$ will necessarily be a multiple of the dimension $\dim(A)$. This means that the maximal quotient of J_G for which we can hope to apply Chabauty-Coleman is precisely the maximal rank zero quotient of J_G. Call this quotient A.

Let D be the cuspidal divisor of X_G; it is clearly defined over $\mathbf{Q}$, and say it has degree d. Let $\mathrm{AJ}_D\colon X_G \to A$ be the Abel-Jacobi map $x \mapsto [d\cdot x - D]$ as before. Because $A(\mathbf{Q})$ is finite, we may further quotient A out by the subgroup scheme determined by $A(\mathbf{Q})$ to assume that the image of $X_G(\mathbf{Q})$ is 0 under AJ_D. We have the commutative diagram

$$\begin{array}{ccccc} X(\mathbf{Q}) & \longrightarrow & X(\mathbf{Q}_p) & & \\ \downarrow & & \downarrow & \searrow & \\ 0 & \longrightarrow & A(\mathbf{Q}_p) & \longrightarrow & \mathrm{Lie}(A) \end{array}$$

where the map $A(\mathbf{Q}_p) \to \mathrm{Lie}(A)$ is coming from the Coleman integration pairing. We get the following description of $X(\mathbf{Q}_p)_1$ by exploiting the Kodaira-Spencer isomorphism:

$$X(\mathbf{Q}_p)_1 = \left\{ x \in X(\mathbf{Q}_p)\colon \int_D^{d\cdot x} \mathrm{KS}(f) = 0 \text{ for all } f \in S_2(X_G)_{rk=0} \right\} \tag{3.1}$$

Now let us prove Theorem 3.0.1.

Lemma 3.3.1. *Let $]U[$ be a residue disk of $U \in X(\mathbf{F}_p)$. Then, for $x \in]U[(\mathbf{Q}_p)$, we have that $(T_p)_* x$ is a divisor supported on $]U[$.*

Proof. Let $\pi\colon X(N) \to X_G = X$ be the modular map. By Proposition 2.4.2, $(T_p)_* = (\mathrm{Fr}_p)_* + [p]_*(\mathrm{Fr}_p)^*$ on $X(N)_{\mathbf{F}_p}$; applying this to the divisor $[\pi^{-1}(U)]$, we learn that $(T_p)_*[\pi^{-1}(U)]$ has the same support as $[\pi^{-1}(U)]$. (This is because the Frobenius is a universal homeomorphism, and also because G contains all scalar matrices, so $[p] = \left[\begin{smallmatrix} p & 0 \\ 0 & p \end{smallmatrix}\right]$ stabilizes $\pi^{-1}(U)$.) Because T_p commutes with π, it follows that, on X_G, we have that $(T_p)_*(U)$ is supported on U. □

Proof of Theorem 3.0.1. Chose a point $b \in]U[(\mathbf{Q}_p)$. We begin with $\int_D^{db} T_p^* \omega = \int_{(T_p)_* D}^{(T_p)_*(db)} \omega$. There-

fore,

$$\int_D^{db} (p+1-T_p)^*\omega = (p+1)\int_D^{db}\omega - \int_{(T_p)_*D}^{(T_p)_*(db)}\omega$$
$$= d\int_{(T_p)_*b}^{(p+1)b}\omega - d\int_{(T_p)_*D}^{(p+1)D}.$$

By Lemma 3.3.1 and the fact that $(T_p)_*$ takes cusps to cusps, as well as the fact that $p \nmid N$, it follows that for a cusp c, we have $(T_p)_*([c]) = (p+1)[c]$. Therefore, the second term in the right hand side vanishes, and we are left with

$$\int_D^{db} (p+1-T_p)^*\omega = d\int_{(T_p)_*b}^{(p+1)b}\omega.$$

Note that $(p+1-T_p)^*$ acting on $S_2(X_G)$ is invertible because, by the Deligne bounds, the eigenvalues of of T_p have complex absolute value bounded above by $2\sqrt{p}$ no matter the complex embedding. Thus, we can multiply both sides by $(p+1-T_p)^{-1}$. We can also write $(T_p)_*b$ as $b_0+\cdots+b_p$ for points $b_0,\ldots,b_p \in]U[(\mathbf{C}_p)$. In all, we thus have

$$\int_D^{db}\omega = d\sum_{i=0}^{p}\int_{b_i}^{b}(p+1-T_p)^{-1}\omega.$$

Now choose a uniformizer t on $]U[$ such that $t(b)=0$. Write $t(b_i)$ as α_i. Also write ω as $\mathrm{KS}(f)(t)\,dt$. We see that for $P \in]U[(\mathbf{Q}_p)$ such that $t(P)=x$, we have

$$\int_D^{dP}\omega = d\int_0^x \mathrm{KS}(f)(t)\,dt - d\sum_{i=0}^{p}\int_0^{\alpha_i}(p+1-T_p)^{-1}\mathrm{KS}(f)(t).$$

Comparing this with the description of $X(\mathbf{Q}_p)_1$ given in (3.1), we complete the proof. □

Chapter 4

Makdisi symbols

In this section, we will introduce the notion of a *Makdisi symbol*. Formally, they are simply given by cuspidal projections of products of two weight 1 Eisenstein series, but they have the nice property of also behaving like modular symbols. In addition, we will see that a certain subclass of Makdisi symbols, the *invertible Makdisi symbols*, will span precisely the space of holomorphic differentials relevant to Chabauty-Coleman, namely the rank zero weight 2 eigenforms.

4.1 Recollection of cusps and Eisenstein series

Let $N \geq 3$ be an integer. Following [63], define the sets

$$\begin{aligned}
\mathscr{C}_N &:= \{(x,y) \in \mathbf{Z}(N)^2 \colon \gcd(x,y,N) = 1\} \\
\mathscr{C}_N^{\pm} &:= \mathscr{C}_N / \{(x,y) \sim (-x,-y)\} \\
\mathbf{P}^1(N) &:= \mathscr{C}_N / \{(x,y) \sim (\lambda x, \lambda y) \colon \lambda \in \mathbf{Z}(N)^*\}
\end{aligned}$$

and recall that the cusps of $\Gamma(N)\backslash\mathbf{H}$ are parametrized precisely by $\mathscr{C}_N^{\pm}$.

Proposition 4.1.1. *Give the above sets a right action of* $\mathrm{SL}_2(\mathbf{Z})$ *via*

$$(x,y) \cdot \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] := (ax+cy, bx+dy).$$

Then there are identifications

$$\mathscr{C}_N = \Gamma_1(N)\backslash \mathrm{SL}_2(\mathbf{Z}), \quad \mathscr{C}_N^{\pm} = \pm\Gamma_1(N)\backslash \mathrm{SL}_2(\mathbf{Z}), \quad \mathbf{P}^1(N) = \Gamma_0(N)\backslash \mathrm{SL}_2(\mathbf{Z})$$

that all associate to $\Gamma\gamma = \Gamma\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbf{Z})$ *the element* $(c,d) = (0,1)\Gamma\gamma$*, for*

$$\Gamma = \Gamma_1(N), \pm\Gamma_1(N), \Gamma_0(N).$$

Proof. This is a matter of verifying that the stabilizer of $(0,1)$ is $\Gamma_1(N)$, the stabilizer of $\{(0,\pm 1)\}$ is $\pm\Gamma_1(N)$, and that the stabilizer of $[0:1]$ is $\Gamma_0(N)$. □

We next recall the notion of Eisenstein series on $X(N)$.

Definition 4.1.2. Let $k \geq 1$ be an integer, and let (x,y) be an element of $\mathscr{C}_N$. The *weight k Eisenstein series associated to* (x,y), denoted $E_k((x,y)_{/N};\tau,s)$, is defined as

$$E_k((x,y)_{/N};\tau,s) := \sum_{\alpha \in \mathbf{C}/(\tau\mathbf{Z}+\mathbf{Z})} \left(\frac{x\tau+y}{N}+\alpha\right)^{-k} \left|\frac{x\tau+y}{N}+\alpha\right|^{-2s}$$

whenever the sum is absolutely convergent, and otherwise via analytic continuation with respect to the complex variable s. Often, we will write $E_k((x,y)_{/N})$ or $E_k((x,y)_{/N};\tau)$ as shorthand for $E_k((x,y)_{/N};\tau,0)$.

The following formulas can be found in [28, Section 4].

Proposition 4.1.3. *The q-expansion of* $E_k((x,y)_{/N};\tau)$ *at* ∞ *is given by*

$$E_k((x,y)_{/N}) = c_k(x,y) + \frac{(-2\pi i)^k}{(k-1)!}\sum_{n=1}^{\infty} \sigma_{k-1}^{(x,y)}(n) q_N^n,$$

for some $c_k(x,y) \in \mathbf{C}$, where we are denoting

$$\sigma_k^{(x,y)}(n) := \sum_{\substack{mm'=n \\ m' \equiv x(N)}} \mathrm{sgn}(m) m^k \zeta_N^{ym}.$$

Proposition 4.1.4. *Let $c_k(x,y)$ be the constant term of the q-expansion of $E_k((x,y)_{/N})$ at ∞ as before. We have the following formulas for $k = 1$ and 2, valid when $0 \leq x,y < N$:*

$$c_1(x,y) = 2\pi i \cdot \begin{cases} \frac{1}{2}\frac{\zeta_N^y+1}{\zeta_N^y-1} & x = 0 \\ x/N - 1/2 & x \neq 0 \end{cases}$$

$$c_2(x,y) = (2\pi i)^2 \cdot \begin{cases} (\zeta_N^b + \zeta_N^{-b} - 2)^{-1} & x = 0 \\ 0 & x \neq 0. \end{cases}$$

The right action of $\mathrm{GL}_2(N)$ on modular forms is given on Eisenstein series by

$$E_k((x,y)_{/N}) \mid_k \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right] = E_k((ax+cy, bx+dy)_{/N}).$$

There is an associated space $\mathscr{E}_k(\Gamma(N)) \leq M_k(\Gamma(N))$ of Eisenstein series; there is a natural decomposition $S_k(\Gamma(N)) \oplus \mathscr{E}_k(\Gamma(N)) = M_k(\Gamma(N))$. If $k \geq 3$, then $\mathscr{E}_k(\Gamma(N))$ has dimension $\#\mathscr{C}_N^{\pm}$ and is spanned by $E_k((x,y)_{/N})$, with no relations between these elements. If $k = 2$, then $\mathscr{E}_2(\Gamma(N))$ has dimension $\#\mathscr{C}_N^{\pm} - 1$ and is spanned by elements of the form $E_2((x,y)_{/N}) - E_2((x',y')_{/N})$. If $k = 1$, then $\mathscr{E}_1(\Gamma(N))$ has dimension $\#\mathscr{C}_N^{\pm}/2$ and is spanned by $E_1((x,y)_{/N})$; there are additional relations coming from the fact that the $E_1((x,y)_{/N})$ are self-dual with respect to a certain Fourier transform on $\mathbf{Z}(N)^2$.

If $X \in \mathrm{Mat}_{2\times 2}(\mathbf{Z}/N\mathbf{Z})$ is a matrix $X = \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$, then define $E_{1,1}(X_{/N})$ to be the product

$$E_{1,1}(X_{/N}) := \frac{1}{(2\pi i)^2} E_1((a,b)_{/N}) E_1((c,d)_{/N}).$$

The expression $E_{1,1}(X_{/N})$ is a modular form of weight 2, but it is usually not a cusp form or Eisenstein series. The factor $1/(2\pi i)^2$ is there to ensure that the q-expansion coefficients lie in $\mathbf{Q}(\zeta_N)$.

If G is a subgroup of $\mathrm{GL}_2(N)$ containing $\pm I$, and if Γ_G is the intersection of G with $\mathrm{SL}_2(N)$, then define $E_{1,1}^G(X)$ to be the sum $\sum_{\gamma \in G/\{\pm 1\}} E_{1,1}((X\gamma)_{/N})$, and define $E_{1,1}^{\Gamma_G}(X)$ similarly (by replacing G with Γ_G). Finally, for a cusp $(x,y) \in \mathscr{C}_N^{\pm}$ corresponding to the coset $\pm\Gamma_1(N)g_0$, define $E_2^{\Gamma_G}(g_0)$ to be

$$E_2^{\Gamma_G}(g_0) := \frac{1}{(2\pi i)^2} \sum_{g \in \pm(\Gamma_G \cap g_0^{-1}\Gamma_1(N)g_0)\backslash\Gamma_G} E_2((x,y)g_{/N}).$$

4.2 Definition of Makdisi symbol

For a matrix $X \in \mathrm{Mat}_{2\times 2}(\mathbf{Z}/N\mathbf{Z})$, define the *Makdisi symbol associated to* X, notated $\mathrm{Mak}_N(X)$, to be the weight 2 cusp form given precisely by the cuspidal projection of $E_{1,1}(X_{/N})$. The right action of $\mathrm{GL}_2(N)$ is given by $\mathrm{Mak}_N(X).\gamma = \mathrm{Mak}_N(X \cdot \gamma)$. We say that a Makdisi symbol is *invertible* if X lies in $\mathrm{GL}_2(N)$.

Similarly to the Eisenstein series, define, for a subgroup G of $\mathrm{GL}_2(N)$ containing $\pm I$, the *G-Makdisi symbol* $\mathrm{Mak}_G(X)$ as the sum $\sum_{\gamma \in G/\{\pm 1\}} \mathrm{Mak}_N(X\gamma)$; define $\mathrm{Mak}_{\Gamma_G}(X)$ similarly.

We list some properties of Makdisi symbols that should remind the reader of the 2- and 3-term Manin relations enjoyed by modular symbols. To wit, temporarily let σ, τ and J denote the matrices

$$\sigma := \left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right], \quad \tau := \left[\begin{smallmatrix} 1 & 1 \\ -1 & 0 \end{smallmatrix}\right], \quad J := \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right].$$

Then, we have the following identities:

$$\begin{aligned}&\mathrm{Mak}_G(X)+\mathrm{Mak}_G(\sigma X)=\mathrm{Mak}_G(X)+\mathrm{Mak}_G(\tau X)+\mathrm{Mak}_G(\tau^2 X)\\&=\mathrm{Mak}_G(X)+\mathrm{Mak}_G(JX)=\mathrm{Mak}_G(X)-\mathrm{Mak}_G(-X)=0.\end{aligned}$$

Proof. All but the second identity are consequences from the definition of a Makdisi symbol as well as the fact that $E_1((-x,-y)_{/N})=-E_1((x,y)_{/N})$. The second identity is an expression of the fact that for $P,Q,R\in\mathbf{Z}(N)^2$ summing to the zero element, we have

$$E_1(P_{/N})E_1(Q_{/N})+E_1(Q_{/N})E_1(R_{/N})+E_1(R_{/N})E_1(P_{/N})\in\mathscr{E}_2(X(N));$$

see [40, Eq. 4.10]. □

4.3 The Hecke action

In this subsection, we will exhibit the Hecke action on a Makdisi symbol. We will use important calculations of Khuri-Makdisi in [40, Section 4] to prove the existence of "universal matrices", akin to the universal matrices in [54], that will yield an expression of the action of T_p on $\mathrm{Mak}_N(X)$ in approximately $p\log(p)$ Makdisi symbols. Such an action further supports the parallelism between Makdisi symbols and Manin symbols, and it is probably true that there is a Hecke equivariant map from the space of Manin symbols to the space of Makdisi symbols, although we do not need that result.

Let p be a prime number not dividing N. Recall that T_p denotes the Hecke operator at p, and that we have $T_p=\Delta_p\sigma_p$, where Δ_p is the "conventional Hecke operator"

$$\Delta_p:=\Gamma(N)\left[\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right]\Gamma(N)$$

and σ_p denotes acting by $\left[\begin{smallmatrix}1&0\\0&d\end{smallmatrix}\right]$ in $\mathrm{GL}_2(N)$. Let us compute this action for an arbitrary Makdisi

symbol $\mathrm{Mak}_N(X)$, $X \in \mathrm{Mat}_2(\mathbf{Z}/N)$. The operator Δ_p can be thought of as acting by $\left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]$, and then taking the trace from $\Gamma(Np)$ to $\Gamma(N)$, noting that we should divide by $\#\mathrm{SL}_2(p)/(p+1) = p(p-1)$ also.

We first compute

$$\begin{aligned} E_1((a,b)_{/N}; p\tau) &= \sum_{\alpha \in \mathbf{Z}p\tau + \mathbf{Z}} \left(\frac{ap\tau + b}{N} + \alpha\right)^{-1} \\ &= \sum_{k \in \mathbf{F}_p} \sum_{\alpha \in \mathbf{Z}p\tau + \mathbf{Z}p} \left(\frac{ap\tau + b}{N} + k + \alpha\right)^{-1} \\ &= p^{-1} \sum_{k \in \mathbf{F}_p} \sum_{\alpha \in \mathbf{Z}\tau + \mathbf{Z}} \left(\frac{ap\tau + (b+kN)}{Np} + \alpha\right)^{-1} \\ &= p^{-1} \sum_{k \in \mathbf{F}_p} E_1((ap, b+kN)_{/Np}). \end{aligned}$$

Let us recall some facts from [40]. For rings R_1 and R_2, let $R_1[\mathrm{Mat}_2(R_2)]$ denote the free R_1-module on the set of 2×2 matrices with coefficients in R_2.

Definition 4.3.1. Define the function $\mathrm{Mer}\colon \mathbf{Z}_{>0} \times \mathbf{Z} \to \mathbf{Q}[\mathrm{Mat}_2(\mathbf{Q})]$ characterized by

$$\begin{aligned} &\mathrm{Mer}(n,s) = \mathrm{Mer}(n, n+s) \\ &\mathrm{Mer}(n,s) = \begin{cases} n \cdot \left[\begin{smallmatrix} n & 0 \\ 0 & 1 \end{smallmatrix}\right] & s = 0 \\ n \cdot \left[\begin{smallmatrix} n & 0 \\ s & 1 \end{smallmatrix}\right] - \frac{n}{s} \cdot \mathrm{Mer}(s,n) \cdot \left[\begin{smallmatrix} 1 & 1/s \\ 0 & -n/s \end{smallmatrix}\right] & 1 \le s < n. \end{cases} \end{aligned}$$

Lemma 4.3.2. *The following hold.*

- *The function* $\mathrm{Mer}(n,s)$ *takes values in* $\mathbf{Q}[\mathrm{Mat}_2(\mathbf{Z})]$.
- *If we write*

$$\mathrm{Mer}(n,s) = \sum_{i \in I} r_i \left[\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right],$$

then for each $i \in I$ we have

$$\det \left[\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right] = \pm n, \quad a_i - s b_i \equiv c_i - s d_i \equiv 0 \bmod n.$$

Proposition 4.3.3. *Suppose that we have written*

$$\mathrm{Mer}(n,s) = \sum_{i \in I} r_i \left[\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right].$$

Then, for $A, B \in (\mathbf{Q}/\mathbf{Z})(Nn)$, and for $s \in \mathbf{Z}$, we have

$$\sum_{T \in (\mathbf{Q}/\mathbf{Z})[n]} \mathrm{Mak}\left(\left[\begin{smallmatrix} A+T \\ B-sT \end{smallmatrix}\right]\right) = \sum_{i \in I} r_i \, \mathrm{Mak}\left(\left[\begin{smallmatrix} a_i & b_i \\ c_i & d_i \end{smallmatrix}\right] \left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right]\right).$$

Proof of Proposition 4.3.3 and Lemma 4.3.2. This is essentially a reframing of [40, Prop. 4.6]. □

Lemma 4.3.4 (Chinese remainder theorem)**.** *Let* $\gcd(m,n) = 1$. *Then, in $\mathbf{Q}/\mathbf{Z}$, we have $a/(mn) = (a[n^{-1}]_m)/m + (a[m^{-1}]_n)/n$, where $[n^{-1}]_m$ denotes the multiplicative inverse of n modulo m.*

Proof. Let a_1 be a lift of an^{-1} mod m to $\mathbf{Z}$, and let a_2 be a lift of am^{-1} mod n to $\mathbf{Z}$. Then $a_1/m + a_2/n = (na_1 + ma_2)/(mn)$. We have $na_1 + ma_2$ is congruent to $n(an^{-1}) + 0 = a$ mod m and $0 + m(am^{-1}) = a$ mod n. By the Chinese remainder theorem, we win. □

Now, for $X := \left[\begin{smallmatrix} a & b \\ a' & b' \end{smallmatrix}\right] \in \mathrm{Mat}_{2\times 2}(\mathbf{Z}/N\mathbf{Z})$, we have

$$
\begin{aligned}
&E_{1,1}(X_{/N};\tau) \mid_2 \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right] \\
&= \det \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right] \cdot p^{-2} \cdot \sum_{(k,k')\in \mathbf{F}_p\times\mathbf{F}_p} E_1((ap,b)_{/Np} + (0,k)_{/p}) E_1((a'p,b')_{/Np} + (0,k')_{/p}) \\
&= p^{-1} \sum_{(k,k')\in \mathbf{F}_p\times\mathbf{F}_p} E_1((a,bp^{-1})_{/N} + (0,k)_{/p}) E_1((a',b'p^{-1})_{/N} + (0,k')_{/p}) \\
&= p^{-1}(E_1((a,bp^{-1})_{/N}) E_1((a',b'p^{-1})_{/N}) + \\
&\sum_{k'\in \mathbf{F}_p^*} E_1((a,bp^{-1})_{/N}) E_1((a',b'p^{-1})_{/N} + (0,k')_{/p}) \\
&+ \sum_{(k,s)\in \mathbf{F}_p^*\times\mathbf{F}_p} E_1((a,bp^{-1})_{/N} + (0,k)_{/p}) E_1((a',b'p^{-1})_{/N} + s(0,k)_{/p})).
\end{aligned}
$$

Now we are to take the trace of this expression from $\Gamma(Np)$ to $\Gamma(N)$, remembering to divide by $p(p-1)$ afterwards. To do this, we note that there is a transitive right action of $\mathrm{SL}_2(p)$ on the set

$\{(a,b)_{/p}\colon (a,b)\neq(0,0)\}$, with stabilizer size $\#SL_2(p)/(p^2-1)=p$. Thus,

$$\begin{aligned}
A_1 &:= \mathrm{Tr}^{\Gamma(N)}_{\Gamma(Np)} E_1((a,bp^{-1})_{/N})E_1((a',b'p^{-1})_{/N}) \\
&= p(p-1)(p+1)E_1((a,bp^{-1})_{/N})E_1((a',b'p^{-1})_{/N}) \\
A_2 &:= \mathrm{Tr}^{\Gamma(N)}_{\Gamma(Np)} \sum_{k'\in\mathbf{F}_p^*} E_1((a,bp^{-1})_{/N})E_1((a',b'p^{-1})_{/N}+(0,k')_{/p}) \\
&= p(p-1)\sum_{T\in\mathscr{E}[p]-0} E_1((a,bp^{-1})_{/N})E_1((a',b'p^{-1})_{/N}+T) \\
&= p^2(p-1)E_1((a,bp^{-1})_{/N})E_1((pa',b')_{/N}) - p(p-1)E_1((a,bp^{-1})_{/N})E_1((a',b'p^{-1})_{/N}) \\
A_3 &:= \mathrm{Tr}^{\Gamma(N)}_{\Gamma(Np)} \sum_{(k,s)\in\mathbf{F}_p^*\times\mathbf{F}_p} E_1((a,bp^{-1})_{/N}+(0,k)_{/p})E_1((a',b'p^{-1})_{/N}+s(0,k)_{/p}) \\
&= p(p-1)\sum_{s\in\mathbf{F}_p}\sum_{T\in\mathscr{E}[p]-0} E_1((a,bp^{-1})_{/N}+T)E_1((a',b'p^{-1})_{/N}+sT) \\
&= p(p-1)\left(\sum_{s\in\mathbf{F}_p}\mathrm{Mak}_N\left(\mathrm{Mer}(n,s)\cdot X\cdot\left[\begin{smallmatrix}1&0\\0&p^{-1}\end{smallmatrix}\right]\right)\right) \\
&- p^2(p-1)E_1((a,bp^{-1})_{/N})E_1((a',b'p^{-1})_{/N}).
\end{aligned}$$

Finally, we have

$$\begin{aligned}
E_{1,1}(X_{/N};\tau)\mid_2\Delta_p &= \frac{1}{p(p-1)}\mathrm{Tr}_{\Gamma(Np)/\Gamma(N)}E_{1,1}(X_{/N};\tau)\mid_2\left[\begin{smallmatrix}p&0\\0&1\end{smallmatrix}\right] \\
&= \frac{1}{p^2(p-1)}(A_1+A_2+A_3) \\
&= \frac{p+1}{p}\mathrm{Mak}_N(X\cdot\left[\begin{smallmatrix}1&0\\0&p^{-1}\end{smallmatrix}\right]) \\
&+ \left(\mathrm{Mak}_N(\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]X\left[\begin{smallmatrix}1&0\\0&p^{-1}\end{smallmatrix}\right]) - \frac{1}{p}\mathrm{Mak}_N(X\cdot\left[\begin{smallmatrix}1&0\\0&p^{-1}\end{smallmatrix}\right])\right) \\
&+ \left(\frac{1}{p}\left(\sum_{s\in\mathbf{F}_p}\mathrm{Mak}_N(\mathrm{Mer}(p,s)\cdot X\cdot\left[\begin{smallmatrix}1&0\\0&p^{-1}\end{smallmatrix}\right])\right) - \mathrm{Mak}_N(X\cdot\left[\begin{smallmatrix}1&0\\0&p^{-1}\end{smallmatrix}\right])\right) \\
&= \mathrm{Mak}_N(\left[\begin{smallmatrix}1&0\\0&p\end{smallmatrix}\right]X\left[\begin{smallmatrix}1&0\\0&p^{-1}\end{smallmatrix}\right]) + \frac{1}{p}\left(\sum_{s\in\mathbf{F}_p}\mathrm{Mak}_N(\mathrm{Mer}(p,s)\cdot X\cdot\left[\begin{smallmatrix}1&0\\0&p^{-1}\end{smallmatrix}\right])\right).
\end{aligned}$$

Thus, because $T_p = \Delta_p \cdot \left[\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right]_N$, we have

$$\mathrm{Mak}_N(X) \mid_2 T_p = \mathrm{Mak}_N(\left[\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right] X) + \frac{1}{p}\left(\sum_{s \in \mathbf{F}_p} \mathrm{Mak}_N(\mathrm{Mer}(p,s) \cdot X)\right).$$

Because acting by T_p commutes with passing to smaller congruence subgroups of level coprime to p, it follows that

$$\mathrm{Mak}_G(X) \mid_2 T_p = \mathrm{Mak}_G(\left[\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right] X) + \frac{1}{p}\left(\sum_{s \in \mathbf{F}_p} \mathrm{Mak}_G(\mathrm{Mer}(p,s) \cdot X)\right).$$

Corollary 4.3.5. *The span of the invertible Makdisi symbols is stable under Hecke operators.*

Proof. By Lemma 4.3.2 and the formula just above, we see that acting by T_p has the effect of multiplying X on the left by various matrices of determinant p. Since $p \nmid N$, it follows that $\mathrm{Mak}_G(X) \mid_2 T_p$ is also in the span of invertible Makdisi symbols. □

4.4 The rank zero quotient comes from invertible symbols

In this subsection, we will exhibit the rank zero quotient of X_G as precisely the span of the invertible Makdisi symbols. Such a result should be thought of as similar in spirit to the result of [13], although we will prove it using a Rankin-Selberg unfolding result of Khuri-Makdisi and Raji, rather than work with q-expansions. Recall that in [40], Khuri-Makdisi proves the following important theorem:

Theorem 4.4.1. *The* $\mathbf{Q}$*-vector space* $S_2(X(N))$ *of weight* 2 *cusp forms is spanned by the Makdisi symbols* $\{\mathrm{Mak}_N(X) \colon X \in \mathrm{Mat}_{2\times 2}(\mathbf{Z}/N\mathbf{Z})\}$.

The goal of this subsection is to prove the following analogous statement:

Theorem 4.4.2. *The* $\mathbf{Q}$*-vector space spanned by the rank zero Hecke eigenforms in* $S_2(X(N))$ *is precisely the span of the invertible Makdisi symbols* $\{\mathrm{Mak}_N(X) \colon X \in \mathrm{GL}_2(N)\}$.

Notation 4.4.3. If f_1 and f_2 are functions of some fixed set of variables valued in $\mathbf{C}$, write $f_1 \sim f_2$ if $f_1 = f_0 \cdot f_2$ for some nowhere vanishing function f_0.

Now let us begin the proof. By Corollary 4.3.5, we see that it suffices to show that the orthocomplement of the span of invertible Makdisi symbols are precisely the span of the positive rank weight 2 eigenforms. To this end, suppose f is a weight 2 eigenform on $X(N)$ (not necessarily new), represented by $(f_d)_{d\in\mathbf{Z}(N)^*}$. Without loss of generality, we may assume that the diamond operators also act by characters: namely, let $\{\langle d\rangle\}_{d\in\mathbf{Z}(N)^*}$ act with character ψ, and let $\{\sigma_d\}_{d\in\mathbf{Z}(N)^*}$ act with character χ. We break up $X(N)(\mathbf{C})$ into a disjoint union of $\phi(N)$ copies of $X(N)'(\mathbf{C}) = \Gamma(N)\backslash\mathbf{H}^*$ and obtain that for $\gamma \in \mathrm{GL}_2(N)$, we have

$$\left\langle f, E_{1,1}(\gamma, s)\right\rangle_{X(N)} \sim \sum_{d\in\mathbf{Z}(N)^*} \left\langle f_d, E_{1,1}(\gamma\sigma_d, s)\right\rangle_{X(N)'}.$$

Note that f_d can be considered as $f\mid_2 \sigma_d$, but restricted to the "canonical" connected component of $\Gamma(N)\backslash\mathbf{H}$ where ζ_N is identified with $\exp(2\pi i/N)$.

Definition 4.4.4. Let $A \in \mathrm{Mat}_{2\times 2}(\mathbf{Z}/N\mathbf{Z})$ be a 2×2 matrix.

- Define X_A^+ to be the set of 2×2 matrices M with integer coefficients of positive determinant such that $M \equiv A \bmod N$.
- There is a right action of $\Gamma(N)$ on X_A^+ given by $M \mapsto M\gamma$. Define Y_A^+ to be the quotient $Y_A^+ := X_A^+/\Gamma(N)$.

We have the following important result found by applying [41, Prop. 2.5] to the case $\ell' = m' = 0$.

Theorem 4.4.5 (Khuri-Makdisi, Raji)**.** *Let $A \in \mathrm{Mat}_{2\times 2}(\mathbf{Z}/N\mathbf{Z})$ be a matrix, and let f be a weight 2 cusp form on $\Gamma(N)$. Then, for all $s \in \mathbf{C}$ of sufficiently large real part, the Petersson inner product*

$\left\langle f, E_{1,1}(A,s)\right\rangle$ *is a nonzero multiple of the following infinite sum:*

$$\sum_{M \in Y_A^+ \cup Y^+_{\left[\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right]_A}} \det(M)^{-s-1} \int_0^\infty (f \mid_2 M^{-1})(z)\, dz.$$

Thus, by 4.4.5, we have

$$\left\langle f, E_{1,1}(\gamma,s)\right\rangle_{X(N)} \sim \sum_{d \in \mathbf{Z}(N)^*} \sum_{M \in Y^+_{\gamma\sigma_d} \cup Y^+_{\left[\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right]\gamma\sigma_d}} \det(M)^{-s-1} \int_0^\infty (f_d \mid_2 M^{-1})(z)\, dz.$$

Notation 4.4.6. For $\gamma \in \mathrm{GL}_2(N)$, denote γ^c by $\sigma_{-1}\gamma\sigma_{-1}$.

We have

$$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \gamma\sigma_d = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \gamma^c \sigma_{-d}$$

and thus the Petersson inner product becomes

$$\sum_{d \in \mathbf{Z}(N)^*} \sum_{M \in Y^+_{\gamma\sigma_d} \cup Y^+_{\left[\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right]\gamma^c\sigma_d}} \det(M)^{-s-1} \int_0^\infty (f_d \mid_2 M^{-1})(z)\, dz.$$

We now present a crucial double coset lemma.

Lemma 4.4.7. *Let $X \in \mathrm{Mat}_{2\times 2}(\mathbf{Z})$ be an integral matrix such that $\gcd(\det(X), N) = 1$, and let $d_1, d_2 \in \mathbf{Z}$ be positive integers such that $d_1 \mid d_2$, and such that $d_1 d_2 \equiv \det(X) \bmod N$. Then the intersection of sets of integral matrices*

$$(X + N \cdot \mathrm{Mat}_{2\times 2}(\mathbf{Z})) \cap \left(\Gamma(1) \begin{bmatrix} d_1 & 0 \\ 0 & d_2 \end{bmatrix} \Gamma(1)\right)$$

is precisely one double coset $\Gamma(N)\beta\Gamma(N)$, for some $\beta \in \mathrm{Mat}_{2\times 2}(\mathbf{Z})$.

Proof. Let α denote the matrix element $\left[\begin{smallmatrix} d_1 & 0 \\ 0 & d_2 \end{smallmatrix}\right]$. Say that $\gamma_1, \gamma_2 \in \mathrm{SL}_2(N)$ are matrix elements such that $\gamma_1 \alpha \gamma_2^{-1} \equiv \alpha \bmod N$. We claim that there exist lifts $\tilde{\gamma}_1, \tilde{\gamma}_1 \in \mathrm{SL}_2(\mathbf{Z})$ of γ_1, γ_2 such that $\tilde{\gamma}_1 \alpha \tilde{\gamma}_2^{-1} = \alpha$. (A priori $\tilde{\gamma}_1$ and $\tilde{\gamma}_2$ may only lie in $\mathrm{Mat}_2(\mathbf{Z})$.) Indeed, we know that $\gamma_1 \equiv \alpha \gamma_2 \alpha^{-1} \bmod N$, and we want our lifts to satisfy $\tilde{\gamma}_1 = \alpha \tilde{\gamma}_2 \alpha^{-1}$. So, letting $r := d_2/d_1$, this is just asking if we can lift γ_2 to a $\tilde{\gamma}_2$ such that $\tilde{\gamma}_2 =: \left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ lies in the subgroup $\Gamma^0(r) \leq \mathrm{SL}_2(\mathbf{Z})$; for if this is the case, then $\alpha \tilde{\gamma}_2 \alpha^{-1} = \left[\begin{smallmatrix} a & b/r \\ rc & d \end{smallmatrix}\right]$ is determinant 1 with integer entries. But this answer is clearly true, by approximation. Thus the claim is proven.

As a consequence of the claim, we find that if two elements in $\Gamma(1)\alpha\Gamma(1)$ reduce modulo N to X, say notated as $x_1 := \gamma_{1,1}\alpha\gamma_{1,2}^{-1}$ and $x_2 := \gamma_{2,1}\alpha\gamma_{2,2}^{-1}$, we then have $(\gamma_{2,1}^{-1}\gamma_{1,1})\alpha(\gamma_{2,2}^{-1}\gamma_{1,2})^{-1} \equiv \alpha \bmod N$. We find lifts g_1 of $\gamma_{2,1}^{-1}\gamma_{1,1}$ and g_2 of $\gamma_{2,2}^{-1}\gamma_{1,2}$ such that $g_1 \alpha g_2^{-1} = \alpha$. Then the elements $h_1 := \gamma_{2,1} g_1 \gamma_{1,1}^{-1}$ and $h_2 := \gamma_{1,2} g_2^{-1} \gamma_{2,2}^{-1}$ both lie in $\Gamma(N)$, and satisfy $h_1 \cdot x_1 \cdot h_2 = x_2$. Hence, x_1 and x_2 lie in the same double coset. This proves the lemma. □

Back to the inner product. We are to enumerate lifts of $\gamma \left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right]$ for a given $d \in \mathbf{Z}(N)^*$ and $\gamma \in \mathrm{SL}_2(N)$. We have

$$(\gamma \left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right] + N \cdot \mathrm{Mat}_2(\mathbf{Z})) = \gamma(\left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right] + N \cdot \mathrm{Mat}_2(\mathbf{Z}))$$

and for a fixed $n > 0$ congruent to d mod N, that

$$\begin{aligned}
(\left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right] + N \cdot \mathrm{Mat}_2(\mathbf{Z}))^{\det = n} &= \bigcup_{\substack{d_1 d_2 = n \\ d_1 | d_2}} \left((\left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right] + N \cdot \mathrm{Mat}_2(\mathbf{Z})) \cap \Gamma(1) \left[\begin{smallmatrix} d_1 & 0 \\ 0 & d_2 \end{smallmatrix}\right] \Gamma(1) \right) \\
&= \bigcup_{\substack{d_1 d_2 = n \\ d_1 | d_2}} \Gamma(N) \langle d_1 \rangle^{-1} \left[\begin{smallmatrix} d_1 & 0 \\ 0 & d_2 \end{smallmatrix}\right] \Gamma(N) \\
&= \bigcup_{\substack{d_1 d_2 = n \\ d_1 | d_2}} d_1 \langle d_1 \rangle^{-1} \Gamma(N) \left[\begin{smallmatrix} 1 & 0 \\ 0 & d_2/d_1 \end{smallmatrix}\right] \Gamma(N).
\end{aligned}$$

As a consequence, $X^+_{\gamma\sigma_d}$ decomposes as double cosets

$$X^+_{\gamma\sigma_d} = \bigcup_{n\equiv d(N)} \bigcup_{\substack{d_1 d_2 = n \\ d_1 | d_2}} d_1 \gamma \langle d_1 \rangle^{-1} \Gamma(N) \left[\begin{smallmatrix} 1 & 0 \\ 0 & d_2/d_1 \end{smallmatrix}\right] \Gamma(N)$$

and thus the set $\{M^{-1} : M \in X^+_{\gamma\sigma_d}\}$ decomposes as

$$\bigcup_{n\equiv d(N)} \bigcup_{\substack{d_1 d_2 = n \\ d_1 | d_2}} \Gamma(N) \left[\begin{smallmatrix} d_2/d_1 & 0 \\ 0 & 1 \end{smallmatrix}\right] \Gamma(N) d_2^{-1} \langle d_1 \rangle \gamma^{-1}$$

and thus $\{M^{-1} : M \in Y^+_{\gamma\sigma_d}\}$ decomposes as

$$\bigcup_{n\equiv d(N)} \bigcup_{\substack{d_1 d_2 = n \\ d_1 | d_2}} d_2^{-1} \Delta_{d_2/d_1} \langle d_1 \rangle \gamma^{-1}.$$

Similarly, $\{M^{-1} : M \in Y^+_{\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]\gamma\sigma_d}\}$ decomposes as

$$\bigcup_{n\equiv d(N)} \bigcup_{\substack{d_1 d_2 = n \\ d_1 | d_2}} d_2^{-1} \Delta_{d_2/d_1} \langle d_1 \rangle \gamma^{-1,c} \left[\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right].$$

Noting that in weight 2, slashing by a scalar matrix does nothing, our Petersson inner product

becomes

$$\begin{aligned}
&\sum_{d\in\mathbf{Z}(N)^*}\sum_{M\in Y_{\gamma\sigma_d}^+\cup Y_{\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right]\gamma^c\sigma_d}^+} \det(M)^{-s-1}\int_0^\infty (f_d\mid_2 M^{-1})(z)\,dz\\
&=\sum_{\substack{n\geq 1\\(n,N)=1}}\sum_{\substack{d_1d_2=n\\d_1\mid d_2}} n^{-s-1}\int_0^\infty (f_n\mid_2\Delta_{d_2/d_1}\mid_2\langle d_1\rangle)\mid_2(\gamma^{-1}+\gamma^{-1,c}\left[\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right])(z)\,dz\\
&=\sum_{\substack{n\geq 1\\(n,N)=1}}\sum_{\substack{d_1d_2=n\\d_1\mid d_2}} n^{-s-1}\int_0^\infty (f\mid_2\sigma_{d_1}^2\mid_2 T_{d_2/d_1}\mid_2\langle d_1\rangle)\mid_2(\gamma^{-1}+\gamma^{-1,c}\left[\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right])(z)\,dz\\
&=\sum_{\substack{n\geq 1\\(n,N)=1}}\sum_{\substack{d_1d_2=n\\d_1\mid d_2}} n^{-s-1}\int_0^\infty a_{d_2/d_1}(\psi\chi^2)(d_1)(f\mid_2(\gamma^{-1}+\gamma^{-1,c}\left[\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right]))(z)\,dz\\
&=\left(\int_0^\infty f\mid_2(\gamma^{-1}+\gamma^{-1,c}\left[\begin{smallmatrix}0&1\\-1&0\end{smallmatrix}\right])\right)\cdot\sum_{n\geq 1}\sum_{\substack{d_1d_2=n\\d_1\mid d_2}}\frac{a_{d_2/d_1}(\psi\chi^2)(d_1)}{n^{s+1}}.
\end{aligned}$$

Noting that $f\mid_2(\gamma^{-1}+\gamma^{-1}\left[\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right])$ integrates to 0 along $\{0,\infty\}$, as well as distributing out the second term, we see that the sum becomes

$$\left(\int_0^\infty f\mid_2(\gamma^{-1}-\gamma^{-1,c})\right)\cdot L^{(N)}(f,s+1)L^{(N)}(\psi\chi^2,2s+2),$$

where the last two terms are L-values but with the terms in the Euler product corresponding to primes dividing N taken out. By [54, Prop. 8], the integral in the parentheses never vanishes unless f is zero, since $\gamma^{-1}-\gamma^{-1,c}$ lies in the -1 eigenspace for the star involution. Moreover, the expression $L^{(N)}(\psi,2s+2)$ never vanishes at $s=0$, and the terms omitted in the Euler product for $L^{(N)}(f,1)$ are never zero either. Thus, the expression above is zero at $s=0$ for all $\gamma\in\mathrm{SL}_2(N)$ if and only if $L(f,1)=0$. This completes the proof.

Chapter 5

Computing invertible Makdisi symbols in terms of Eisenstein series

In this section, we will compute expressions for invertible Makdisi symbols on G, for any subgroup G of $\mathrm{GL}_2(N)$ containing $\{\pm 1\}$. By the definition of Makdisi symbol, such a task boils down to finding the right weight 2 Eisenstein series to add to an expression $E_{1,1}(X_{/N})$ in order to get a cusp form. Strictly speaking, we can get by with linear algebra and q-expansions, but we find the prospect of an explicit formula much more exciting. To that end, we also hope that this section can be used in the future to prove various integrality properties.

5.1 Makdisi symbols of full level

Our first task is to compute the cuspidal projection $\mathrm{Mak}_N(\gamma)$, for $\gamma \in \mathrm{GL}_2(N)$. After translating by γ^{-1}, the problem reduces to finding a formula for $\mathrm{Mak}_N(\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right])$. We may write $\mathrm{Mak}_N(\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right])$ as

$$\mathrm{Mak}_N(\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]) = E_{1,1}(\left[\begin{smallmatrix}1 & 0\\ 0 & 1\end{smallmatrix}\right]_{/N}) - \frac{1}{(2\pi i)^2} \sum_{(x,y)\in \mathscr{C}_N^{\pm}} r_{(x,y)} E_2((x,y)_{/N})$$

for unknown terms $r_{(x,y)} \in \mathbf{Q}(\zeta_N)$. In this section, we will give an explicit formula for the $r_{(x,y)}$.

To explain the formula, we need some notation. Define the multiplicative groups

$$A := \mathbf{Z}(N)^*/\{\pm 1\}, \qquad A^\vee := \mathrm{Hom}(A, \mathbf{C}^*).$$

Define the function

$$\overline{B}_1(u) := \begin{cases} \{u\} - 1/2 & u \neq 0 \\ 0 & u = 0 \end{cases}$$

(here, $\{u\} := u - \lfloor u \rfloor$) and define the *generalized Bernoulli numbers* $B_{2,\chi}$ and $\mathscr{B}_{2,\chi}$ as given in [36, Section 2]. For a cusp $(x,y) \in \mathscr{C}_N^{pm}$, letting $0 \leq x, y < N$, define the functions

$$P_{int}, P_1, P_2 \colon A \to \mathbf{C}, \qquad P \colon A^\vee \to \mathbf{C}$$

by

$$\begin{aligned} P_{int}^{(x,y)}(u) &:= \overline{B}_1\left(\frac{ux}{N}\right)\overline{B}_1\left(\frac{uy}{N}\right) \\ P_1(b) &:= (\zeta_N^{b^{-1}} - 1)^{-1}\overline{B}_1\left(-\frac{b}{N}\right) \\ P_2(b) &:= (\zeta_N^{b^{-1}} - 1)^{-1}\overline{B}_1\left(\frac{b}{N}\right) \\ P(\chi) &:= -\frac{1}{4}\mathscr{B}_{2,\overline{\chi}}. \end{aligned}$$

Lastly, for any complex-valued function F whose domain is a finite abelian group B, we may define the Fourier transform $\mathscr{F}(F)$, which is a complex-valued function whose domain is the character group $B^\vee := \mathrm{Hom}(B, \mathbf{C}^*)$. We are now ready to state our theorem.

Theorem 5.1.1. *Let $r_{(x,y)}$ be as above. We have the following formulas for $r_{(x,y)}$:*

$$r_{(ua',-ua)} = \mathscr{F}^{-1}[\mathscr{F}[P_{int}^{(a,a')}]/P](u)$$
$$r_{(b,0)} = \mathscr{F}^{-1}[\mathscr{F}[P_1]/P](b)$$
$$r_{(0,b)} = \mathscr{F}^{-1}[\mathscr{F}[P_2]/P](b).$$

Proof. Recall that a modular form is a cusp form if and only if it vanishes at all cusps. Let $\left[\begin{smallmatrix} a & b \\ a' & b' \end{smallmatrix}\right] \in \mathrm{SL}_2(\mathbf{Z})$ be a matrix. Then, the constant term of $E_{1,1}(\left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]_{/N})$ at the cusp $\left[\begin{smallmatrix} a & b \\ a' & b' \end{smallmatrix}\right]$ is the constant term of $E_{1,1}(\left[\begin{smallmatrix} a & b \\ a' & b' \end{smallmatrix}\right]_{/N})$ at ∞, which is

$$\left(\delta(a)\frac{1}{2}\frac{\zeta_N^b+1}{\zeta_N^b-1}+\frac{a}{N}-\frac{1}{2}\right)\left(\delta(a')\frac{1}{2}\frac{\zeta_N^{b'}+1}{\zeta_N^{b'}-1}+\frac{a'}{N}-\frac{1}{2}\right)$$

while the constant term of $(2\pi i)^{-2}\sum_{(x,y)\in\mathscr{C}_N^{\pm}} r_{(x,y)}E_2((x,y)_{/N})$ at $\left[\begin{smallmatrix} a & b \\ a' & b' \end{smallmatrix}\right]$ is the constant term at ∞ of $(2\pi i)^{-2}\sum_{(x,y)\in\mathscr{C}_N^{\pm}} r_{(x,y)}E_2((ax+a'y,bx+b'y)_{/N})$, which is

$$\sum_{(x,y)\in\mathscr{C}_N^{\pm}} r_{(x,y)}\left(\delta(ax+a'y)\left(\zeta_N^{bx+b'y}+\zeta_N^{-(bx+b'y)}-2\right)^{-1}\right).$$

Equating these two expressions, we find two classes of equations:

- For all $[a:a'] \in \mathbf{P}^1(N)$ such that $a,a' \neq 0$, and all $u \in \mathbf{Z}(N)^*/\{\pm 1\}$, we have

$$\left(\frac{ua}{N}-\frac{1}{2}\right)\left(\frac{ua'}{N}-\frac{1}{2}\right) = \sum_{\lambda\in\mathbf{Z}(N)^*/\{\pm1\}} r_{\lambda a',-\lambda a}\left(\zeta_N^{-\lambda u^{-1}}+\zeta_N^{\lambda u^{-1}}-2\right)^{-1}.$$

These equations can be thought as to be associated to lines in the "interior" of $\mathbf{Z}(N)^2$.

- For all $b \in \mathbf{Z}(N)^*$, we have the two equations

$$(\zeta_N^{b^{-1}} - 1)^{-1} \left(\frac{N-b}{N} - \frac{1}{2} \right) = \sum_{\lambda \in \mathbf{Z}(N)^*/\{\pm 1\}} r_{(\lambda b, 0)} \left(\zeta_N^{\lambda} + \zeta_N^{-\lambda} - 2 \right)^{-1}$$
$$(\zeta_N^{b^{-1}} - 1)^{-1} \left(\frac{b}{N} - \frac{1}{2} \right) = \sum_{\lambda \in \mathbf{Z}(N)^*/\{\pm 1\}} r_{(0, \lambda b)} \left(\zeta_N^{\lambda} + \zeta_N^{-\lambda} - 2 \right)^{-1}.$$

  These equations can be thought as to be associated to the two "exterior" lines $[1:0]$ and $[0:1]$ of $\mathbf{Z}(N)^2$, respectively.

We will now take the Fourier transform of each of these equations, noting that the Fourier transform of a convolution of two functions is the pointwise product of the Fourier transforms of the respective functions. When we do this, the three equations become

$$\mathscr{F}\left[P_{int}^{(a,a')}(u) \right] = \mathscr{F}[r_{(ua', -ua)}] \mathscr{F}\left[\left(\zeta_N^{u^{-1}} + \zeta_N^{-u^{-1}} - 2 \right)^{-1} \right]$$
$$\mathscr{F}[P_1(b)] = \mathscr{F}[r_{(b,0)}] \mathscr{F}\left[\left(\zeta_N^{u^{-1}} + \zeta_N^{-u^{-1}} - 2 \right)^{-1} \right]$$
$$\mathscr{F}[P_2(b)] = \mathscr{F}[r_{(0,b)}] \mathscr{F}\left[\left(\zeta_N^{u^{-1}} + \zeta_N^{-u^{-1}} - 2 \right)^{-1} \right].$$

We briefly digress to observe that

$$\left(\zeta_N^{u^{-1}} + \zeta_N^{-u^{-1}} - 2 \right)^{-1} = -\frac{1}{4} \csc^2 \left(\frac{u^{-1}\pi}{N} \right).$$

By [36, Corollary 4.4], applied to the case $a = 2$, we find that

$$\mathscr{F}\left[\left(\zeta_N^{u^{-1}} + \zeta_N^{-u^{-1}} - 2 \right)^{-1} \right] (\chi) = -\frac{1}{4} \mathscr{B}_{2,\bar{\chi}} = P(\chi).$$

After substituting this expression into the three equations, dividing both sides of each equation by $L(\chi)$, and then taking the inverse Fourier transform, the proof is obtained. □

5.2 Makdisi symbols for quotients

We will now proceed to obtain a formula for $\mathrm{Mak}_{\Gamma_G}(\gamma)$ in terms of the expressions $E_{1,1}^{\Gamma_G}$, $E_2^{\Gamma_G}$ and $r_{(x,y)}$. In fact, we will obtain a formula for $\mathrm{Mak}_{\Gamma_G}(\gamma)$ at each cusp h, and we will then use this to obtain a formula for $\mathrm{Mak}_G(\gamma)$ at each cusp h, also in terms of $E_{1,1}^G$, $(2\pi i)^{-2}E_2^{\Gamma_G}$ and $r_{(x,y)}$. Of course, we recall that $E_{1,1}^{\Gamma_G}$, $E_{1,1}^G$ and E_2^G were defined in Section 4.1, and that $r_{(x,y)}$ was defined in Section 5.1 as elements of $\mathbf{Q}(\zeta_N)$ such that

$$\mathrm{Mak}_N(\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]) = E_{1,1}(\left[\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right]_{/N}) - \sum_{(x,y)\in\mathscr{C}_N^{\pm}} r_{(x,y)}E_2((x,y)_{/N}).$$

Then, for $\gamma\in\mathrm{SL}_2(\mathbf{Z})$, we have

$$\begin{aligned}
\mathrm{Mak}_N(\gamma\Gamma_G) &= \sum_{g\in\Gamma_G/\pm}\mathrm{Mak}_N(\gamma g)\\
&= \sum_{g\in\Gamma_G/\pm} E_{1,1}(\gamma g_{/N}) - \frac{1}{(2\pi i)^2}\sum_{\substack{(x,y)\in\pm\Gamma_1(N)\backslash\mathrm{SL}_2(\mathbf{Z})\\ g\in\Gamma_G/\pm}} r_{(x,y)}E_2((x,y)\gamma g_{/N})\\
&= E_{1,1}^{\Gamma_G}(\gamma) - \sum_{g_0:=(x,y)\in\pm\Gamma_1(N)\backslash\mathrm{SL}_2(\mathbf{Z})} r_{(x,y)}\cdot\#(\Gamma_G\cap(g_0\gamma)^{-1}\Gamma_1(N)g_0\gamma)E_2^{\Gamma_G}((x,y)\gamma)\\
&= E_{1,1}^{\Gamma_G}(\gamma) - \sum_{g_0:=(x,y)\in\pm\Gamma_1(N)\backslash\mathrm{SL}_2(\mathbf{Z})} r_{(x,y)\gamma^{-1}}\cdot\#(\Gamma_G\cap g_0^{-1}\Gamma_1(N)g_0)E_2^{\Gamma_G}((x,y))\\
&= E_{1,1}^{\Gamma_G}(\gamma) - \sum_{\substack{g_0:=(x,y)\in\Gamma_1(N)\backslash\mathrm{SL}_2(\mathbf{Z})/\Gamma_G\\ g\in\pm(\Gamma_G\cap g_0^{-1}\Gamma_1(N)g_0)\backslash\Gamma_G}} r_{(x,y)g\gamma^{-1}}\cdot\#(\Gamma_G\cap g_0^{-1}\Gamma_1(N)g_0)E_2^{\Gamma_G}(x,y)
\end{aligned}$$

so thus we arrive at the following.

Theorem 5.2.1. *If we define* $r_{(x,y)}^{\Gamma_G}(\gamma)$ *to be the expression*

$$\#(\Gamma_G\cap g_0^{-1}\Gamma_1(N)g_0)\cdot\sum_{g\in\pm(\Gamma_G\cap g_0^{-1}\Gamma_1(N)g_0)\backslash\Gamma_G} r_{(x,y)gh^{-1}},$$

then the expression $\mathrm{Mak}_{\Gamma_G}(\gamma)$ *equals*

$$E_{1,1}^{\Gamma_G}(\gamma) - \sum_{g_0:=(x,y)\in\Gamma_1(N)\backslash \mathrm{SL}_2(\mathbf{Z})/\Gamma_G} r_{(x,y)}^{\Gamma_G}(\gamma) E_2^{\Gamma_G}(x,y).$$

There is an evident analogue for $\mathrm{Mak}_G(\gamma)$. To wit: if we choose, for each $d \in \mathbf{Z}(N)^*$, a matrix $g_{(d)} \in G$ of determinant d, then we have

$$\begin{aligned}\mathrm{Mak}_G(\gamma) &= \sum_{d\in\mathbf{Z}(N)^*} \mathrm{Mak}_N(\gamma\Gamma_G g_{(d)}) \\ &= E_{1,1}^G(\gamma) - \sum_{\substack{d\in\mathbf{Z}(N)^* \\ g_0:=(x,y)\in\Gamma_1(N)\backslash \mathrm{SL}_2(\mathbf{Z})/\Gamma_G}} r_{(x,y)}^{\Gamma_G}(\gamma) E_2^{\Gamma_G}(x,y) \mid_2 g_{(d)};\end{aligned}$$

we can now simplify this sum, by making a substitution. For each $d \in \mathbf{Z}(N)^*$, we may replace (x,y) with $(x,y)\cdot g_{(d)}$, and obtain the following:

Theorem 5.2.2. *For each* $(x,y) \in \mathscr{C}_N^{\pm}$*, let* $r_{(x,y)}^{\Gamma_G}(\gamma)$ *be as in Theorem 5.2.1. If we define* $r_{(x,y)}^G(\gamma)$ *to be the expression*

$$r_{(x,y)}^G(\gamma) := \sum_{d\in\mathbf{Z}(N)^*} r_{(x,y)\cdot g_{(d)}}^{\Gamma_G}(\gamma),$$

where each $g_{(d)}$ *is any matrix in* G *of determinant* d*, then the expression* $\mathrm{Mak}_G(\gamma)$ *equals*

$$E_{1,1}^G(\gamma) - \sum_{g_0:=(x,y)\in\Gamma_1(N)\backslash \mathrm{SL}_2(\mathbf{Z})/\Gamma_G} r_{(x,y)}^G(\gamma) E_2^{\Gamma_G}(x,y).$$

Chapter 6

Computing a basis of holomorphic differentials from Makdisi symbols

In this section, we will describe how to compute a basis of the space $S_2(X_G)_{rk=0}$ in terms of Makdisi symbols. Although the basis will be as a $\mathbf{Q}$-vector space, we will be working with q-expansions whose coefficients are in $\mathbf{Q}(\zeta_N)$; recall that this is occurring because X_G is coming from a quotient of $X(N)$, which is the base change $X(N)' \times_{\mathbf{Q}} \mathbf{Q}(\zeta_N)$ considered as a scheme over $\mathbf{Q}$. We will first describe a sort of Sturm bound that works uniformly at all cusps of X_G. Then we will describe a process that can be best described as first computing the "Manin" relations, and then computing the rest of the relations via q-expansion coefficients and the Sturm bound.

6.1 Sturm bound

On X_G, let $\mathscr{I}$ be an index set for the cusps of X_G. (Recall that cusps are parametrized by the double coset space $G\backslash \mathrm{GL}_2(N)/U(N)$). For cusp $i \in \mathscr{I}$, let w_i be the width of i, let Q_i be the size of the Galois orbit of i, and suppose cusp i is given by the double coset $i = [Gh_iU(N)]$. (Recall that the action of Galois is given by $[Gh_iU(N)].\sigma_d = [Gh_i\sigma_dU(N)]$, where $\sigma_d = \left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right]$ as usual.) Let g denote the genus of X_G.

Proposition 6.1.1. *Suppose $C \in \mathbf{Z}_{>0}$ is such that the following inequalities hold:*

$$\left\lfloor \frac{C \cdot w_i}{N} \right\rfloor \geq 1 \quad \textit{for all } i \in \mathscr{I}$$
$$\sum_{i \in \mathscr{I}} Q_i \left(\left\lfloor \frac{C \cdot w_i}{N} \right\rfloor - 1 \right) \geq 2g - 2.$$

Then, if $f \in S_2(X_G)$ is a weight 2 cusp form such that, for all $i \in \mathscr{I}$, the first C terms of the q_N-expansion of $f \mid_2 \gamma_i$ vanish (including the coefficient of q_N^C), then $f = 0$.

Proof. Suppose f is such that the hypothesis holds. Then, under the Kodaira-Spencer isomorphism, $\mathrm{KS}(f)$ is a global section of the sheaf $\Omega^1(-D)$, where D is the effective divisor supported on the cusps, such that the multiplicity of the cusp $[Gh_iU(N)]$ (and all of its Galois conjugates) in D is $\left\lfloor \frac{C \cdot w_i}{N} \right\rfloor - 1$. However, under the hypothesis of the proposition, $\deg(D) > 2g-2$, implying that the degree of $\Omega^1(-D)$ is negative. This forces f to be 0. □

6.2 Computation

Let us now generate a basis of holomorphic differentials. We begin with the set $\{\mathrm{Mak}_G(\gamma) : \gamma \in \mathrm{SL}_2(\mathbf{Z})/\Gamma_G\}$, and we use the Manin relations above to compute a spanning set $\{\mathrm{Mak}_G(\gamma_i)\}_{i \in \mathscr{M}}$ for $S_2(X_G)_{rk=0}$, indexed by the set $\mathscr{M}$. Of course, there will be more relations, because the Makdisi symbols are only good enough to span the rank 0 part of $S_2(X_G)$. This is what we will resolve with q-expansions.

First, we compute in $X(N)$. For $k \in \{1,2\}$ we precompute the q-expansions of $E_k((x,1)_{/N})$ for all $0 \leq x \leq N/2$, up to precision $O(q_N^{C+1})$. Then it is not so hard to recover $E_k((x,i)_{/N})$, for if $(x,1) \cdot \left[\begin{smallmatrix} 1 & b \\ 0 & d \end{smallmatrix}\right] = (x,i)$ for some $b \in \mathbf{Z}(N)$ and $d \in \mathbf{Z}(N)^*$, we have

$$E_k((x,i)_{/N}) = E_k((x,1)_{/N}) \mid_k \left[\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right] \mid_k \left[\begin{smallmatrix} 1 & b \\ 0 & 1 \end{smallmatrix}\right].$$

Or, if $x > N/2$, then we have

$$E_k((x,1)_{/N}) = (-1)^k E_k((N-x,-1)_{/N}) = -E_k((N-x,1)_{/N}) \mid_k \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right].$$

We compute products of two weight 1 Eisenstein series. We choose coset representatives $\left[\begin{smallmatrix} a & * \\ b & * \end{smallmatrix}\right]$ for the right coset space $\mathrm{GL}_2(N)/\pm\left[\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right]$, and then compute $E_{1,1}(\left[\begin{smallmatrix} a & * \\ b & * \end{smallmatrix}\right]_{/N})$ using the computation of weight 1 Eisenstein series above. Then we can use the same trick that we used for computing $E_k((x,i)_{/N})$, to get $E_{1,1}(\gamma_{/N})$ for any $\gamma \in \mathrm{GL}_2(N)$.

Next up, we take G-orbits to obtain q-expansions on X_G. Let $\{h_j\}_{j\in\mathscr{J}}$ be representatives for the double coset space $\Gamma_G \backslash \mathrm{SL}_2(N)/U(N)$ parametrizing the cusps of X_G. For each pair $(i,j) \in \mathscr{M} \times \mathscr{J}$, we first compute, using the formula Theorem 5.2.1 the q-expansion of the Makdisi symbol

$$\mathrm{Mak}_{\Gamma_G}(\gamma_i) \mid_2 h_j.$$

Afterwards, for each pair $(i,j) \in \mathscr{M} \times \mathscr{I}$, we compute $\mathrm{Mak}_G(\gamma_i) \mid_2 h_j$ by noting that

$$\begin{aligned} \mathrm{Mak}_G(\gamma_i) \mid_2 h_j &= \sum_{d \in \mathbf{Z}(N)^*} \mathrm{Mak}_{\Gamma_G}(\gamma_i) \mid_2 g_{(d)} h_j \\ &= \sum_{d \in \mathbf{Z}(N)^*} \mathrm{Mak}_{\Gamma_G}(\gamma_i) \mid_2 h_{x(d,j)} \mid_2 \begin{bmatrix} 1 & b(d,j) \\ 0 & d \end{bmatrix} \end{aligned}$$

where $x(d,j) \in \mathscr{J}$ and $b(d,j) \in \mathbf{Z}(N)$ are suitable elements such that the relation

$$h_{x(d,j)} \begin{bmatrix} 1 & b(d,j) \\ 0 & d \end{bmatrix} h_j^{-1} \in G$$

holds. We pause to note that this can always be done, because such a relation is expressing the fact that the double coset $\Gamma_G h_j U(N)$ is mapped to the Galois orbit of the double coset $G h_{x(d,j)} U(N)$. In any case, we have thus computed, for each $(i,j) \in \mathscr{M} \times \mathscr{I}$, the q-expansion of $\mathrm{Mak}_G(h_i)$ at the

cusp γ_j. Applying the Sturm bound, we see that the q-expansions we have computed of

$$\mathrm{Mak}_G(h_i) \mid \gamma_1, \ldots, \mathrm{Mak}_G(h_i) \mid \gamma_j$$

determine $\mathrm{Mak}_G(h_i)$ uniquely. This allows us to find all the other relations between the $\{\mathrm{Mak}_G(h_i)\}_{i \in \mathscr{M}}$ that were not picked up by the Manin relations. We end up with:

- Elements $\{\gamma_i\}_{i \in \mathscr{M}.\mathscr{M}}$ in the coset space $\mathrm{SL}_2(\mathbf{Z})/\Gamma_G$, such that $\{\mathrm{Mak}_G(\gamma_i)\}_{i \in \mathscr{M}.\mathscr{M}}$ is a basis for $S_2(X_G)_{rk=0}$ over $\mathbf{Q}$.
- A row-echelon matrix that allows us to express, for any $g \in \mathrm{SL}_2(\mathbf{Z})/\Gamma_G$, the Makdisi symbol $\mathrm{Mak}_G(g)$ as a linear combination of $\mathrm{Mak}_G(\gamma_i)$.

6.2.1 Future work: faster computation of Fourier coefficients

For $\gamma, h \in \mathrm{SL}_2(\mathbf{Z})$, we have worked out how to obtain the q-expansion coefficients of $E_{1,1}^{\Gamma_G}(\gamma) \mid_2 h$ that is efficient even if the level N is large, but for time reasons, we have decided not to include the approach here. Morally, the reason that this speedup can be obtained is because the q-expansion coefficients of $E_{1,1}(\gamma_{/N})$ are relatively sparse, and so roughly speaking it is faster to work with double cosets involving Γ_G rather than sum up along Γ_G. (which becomes impractical when N is a three-digit number). When we release this dissertation as a preprint, we will have this part typed up.

6.3 Eliminating cuspidal residue disks via the formal immersion method

The Chabauty-Coleman algorithm will end up relying on the computation of zeroes of power series in each residue disk defined over $\mathbf{F}_p$. However, if the residue disk is cuspidal, then the width w may be quite small compared to N. This poses an issue, because it means that if we

want to compute C terms of precision, then we will have to compute at least $C \cdot N/w$ terms of the q_N-expansion.

The solution to this conundrum turns out to be rather simple. Namely, we will find a finite set of primes S, such that, for a prime p not in S, the Chabauty-Coleman locus $X(\mathbf{Q}_p)_1$ will contain no points in any cuspidal residue disk. We will accomplish this by invoking a lemma on formal immersions due to Parent and Raynaud.

Let us begin by describing how to compute a basis for the $\mathbf{Z}[1/N]$-module of weight 2 cusp forms defined over $\mathbf{Z}[1/N]$. We begin with the following proposition.

Proposition 6.3.1. *Let $f \in S_2(X_G)$ be a modular form such that for all cusps γ_j, the q-expansion coefficients of $f \mid \gamma_j$ up to $O(q_N^C)$ are $\mathbf{Z}[1/N]$-integral. Then f is $\mathbf{Z}[1/N]$-integral.*

Proof. First, we note that the Sturm bound holds for weight 2 cusp forms in all characteristics p prime to N. Indeed, because X_G is smooth over $\mathbf{Z}[1/N]$, the dimension $\dim_{\mathbf{F}_p} H^0((X_G)_{\mathbf{F}_p}, \Omega^1)$ remains constant as p varies.

Suppose that the hypothesis of the statement holds, but suppose f is not $\mathbf{Z}[1/N]$-integral. Let $D > 1$ be the smallest integer such that $D \cdot f$ has $\mathbf{Z}[1/N]$-integral coefficients. Then $D \cdot f$ is nonzero, but all coefficients up to $O(q_N^C)$ are 0 when f is reduced modulo p, for all primes p dividing D. By the Sturm bound in positive characteristic, it follows that $D/p \cdot f$ is $\mathbf{Z}[1/N]$-integral, which contradicts our assumption that D was the smallest integer. □

As a result, we have an efficient way to compute the $\mathbf{Z}[1/N]$-structure on weight 2 cusp forms.

Corollary 6.3.2. *Let M be the matrix whose rows are indexed by a basis $\{\mathrm{Mak}_G(\gamma_i)\}_{i \in \mathscr{M}\mathscr{M}}$ of $S_2(X_G)_{rk=0}$, and such that for each $i \in \mathscr{M}\mathscr{M}$, row i is indexed by the q-expansion coefficients $\{Mak_G(\gamma_i) \mid h_j\}_{j \in \mathscr{J}}$ of $\mathrm{Mak}_G(g_i)$ at all cusps. Then, the saturation of M from $\mathbf{Q}$ to $\mathbf{Z}$ gives q-expansion coefficients for a basis of precisely the weight 2 cusp forms in $S_2(X_G)_{rk=0}$ defined over $\mathbf{Z}[1/N]$.*

Next, we recall some notions surrounding the concept of a formal immersion; see [30, Section 2] for details. A morphism $f\colon X \to Y$ of (noetherian) schemes is a *formal immersion* at $x \in X$ if and only if the map of completed local rings $f^*\colon \widehat{\mathscr{O}}_{Y,f(x)} \to \widehat{\mathscr{O}}_{X,x}$ is a surjection. Equivalently, it suffices for the map on cotangent spaces to be a surjection. We recall the following important property:

Lemma 6.3.3. *Let R be a noetherian local ring with residue field k. Let $f\colon X \to Y$ be a map of noetherian schemes over R, that is a formal immersion at the point $x \in X(k)$. Then, if $P, Q \in X(R)$ are such that $f(P) = f(Q)$, and if both P and Q reduce to x on the special fiber, then we must necessarily have $P = Q$.*

Proof. See [30, Lemma 2.2]. □

Proposition 6.3.4. *Let $\{f_i\}$ be a basis for $S_2(X_G)_{rk=0}$ over $\mathbf{Z}[1/N]$. Let γ be a cusp of X_G, of width w, and suppose that the cusp γ is defined over $F := \mathbf{Q}(\zeta_N)^H$, for H a subgroup of $\mathbf{Z}(N)^*$. Let $a_1(f_i \mid \gamma)$ denote the coefficient of q_w^1 in the q-expansion of f_i and let $I \leq \mathscr{O}_F$ be the ideal*

$$I := (a_1(f_1 \mid \gamma), a_1(f_2 \mid \gamma), \dots)\mathscr{O}_F.$$

Then, for precisely the primes p in the set

$$S := \{p\colon\ p \text{ divides } \mathrm{Norm}_{F/\mathbf{Q}}(I)\} \cap \{p\colon\ p \bmod N \in H\},$$

the cusp γ corresponds to an $\mathbf{F}_p$-residue disk for which where the Abel-Jacobi map $\mathrm{AJ}_\gamma\colon X_G \to A$ into the maximal rank 0 quotient A of the jacobian of X fails to be a formal immersion.

Proof. The mod p residue disk of γ is defined over $\mathbf{F}_p$ (and not some extension) if and only if p splits in F, which is equivalent to $p(\bmod N)$ lying in the subgroup $H \leq \mathbf{Z}(N)^*$.

The ideal I as considered in the statement is divisible by precisely the primes p of $\mathscr{O}_F$ such that AJ_γ fails to be a formal immersion at the reduction of $\gamma \bmod p$. Indeed, if p divides I, then,

modulo p, the elements $a_1(f_i \mid \gamma)$ are all 0; we would need at least one non-zero element mod p in order to span the one-dimensional cotangent space at γ mod p. □

Theorem 6.3.5. *Let $\{\gamma_i\}_{i\in\mathscr{I}}$ be an enumeration of the Galois orbits of the cusps of X_G. For each $i \in \mathscr{I}$, let $F_i = \mathbf{Q}(\zeta_N)^{H_i}$ denote the field of definition of γ_i, and let I_{γ_i} denote the ideal associated to γ_i, as considered in Proposition 6.3.4. Let I_i be the ideal in $\mathbf{Z}$ defined by $\mathrm{Norm}_{F/\mathbf{Q}}(I_{\gamma_i})$. Let S denote the set of primes*

$$S := \bigcup_{i\in\mathscr{I}} \{p\colon \text{ } p \text{ divides } I_i \text{ and } p \bmod N \in H_i\}.$$

Then, for any prime $p \notin S$, the locus of rational points $X_G(\mathbf{Q})$ does not intersect any cuspidal residue disks.

Proof. Let A denote the maximal rank 0 quotient of the jacobian of X. If $p \notin S$, then for every cusp γ_i, the Abel-Jacobi map $\mathrm{AJ}_{\gamma_i}\colon X_G \to A$ is a formal immersion. Suppose $x \in X_G(\mathbf{Q})$ lies in the same mod p residue disk as $\gamma_i \in X_G(F_i)$ and is different from γ_i. Then Lemma 6.3.3 implies that the divisor class $[x-\gamma_i]$ is nontrivial in A. On the other hand, we claim that $[x-\gamma_i]$ is torsion in A. Indeed, if we let D denote the divisor given by summing the Galois orbit of γ_i, say of degree d, then $[d\cdot x - D]$ lies in $A(\mathbf{Q})$ and is thus torsion in A; thus, since $[d\cdot(x-\gamma_i)] = [d\cdot X - D] + [D - d\gamma_i]$ and since $[D-d\gamma_i]$, being supported at the cusps, is known to be torsion (in fact, it is torsion even in J), it follows that $[d\cdot(x-\gamma_i)]$ and thus $[x-\gamma_i]$ is torsion in A.

By [55, Prop. 2.3], it follows the class $[x-\gamma_i]$ in A has order p^n for some natural number n satisfying $p^n - p^{n-1} \leq 1$. However, we assumed that $p \geq 5$, so this forces $n = 0$, and thus $[x-\gamma_i]$ is trivial in A, contradicting what was said earlier. This completes the proof. □

Chapter 7

Setting up the residue disks

From now on, we will fix a prime $p \geq 5$, not dividing N, such that, for S as in Theorem 6.3.5, the prime p does not lie in S. For each of the finitely many $U \in X_G(\mathbf{F}_p)$, there is an associated *residue disk* $X_G(\mathbf{Q}_p)_{]U[}$, and the Chabauty-Coleman locus $X_G(\mathbf{Q}_p)_1$ partitions by residue disk into sets $X_G(\mathbf{Q}_p)_{1,]U[}$.

In this section, we will set up the necessary information for each residue disk $]U[$ in order to compute $X_G(\mathbf{Q}_p)_{1,]U[}$. Recall that we may identify $U \in X(\mathbf{F}_p)$ with a tuple $(E, [Gg\mu_E])$, where $E/\mathbf{F}_p$ is a framed elliptic curve, and where $[Gg\mu_E]$ is a double coset in $G\backslash \mathrm{GL}_2(N)/\mu_E$ such that $[Gg\mu_E] = [Gg\,\mathrm{Fr}_p\,\mu_E]$. We will find, for each $]U[$, a uniformizing parameter t such that the infinitesimal neighborhood of X_G at U is isomorphic to $\mathbf{Z}_p[[t]]$, along with a family of framed elliptic curves $E_t \to \mathrm{Spf}(\mathbf{Z}_p[[t]])$ such that $Gg = Gg\,\mathrm{Fr}_p$. We will then use the description of t and E_t to express the locus $X_G(\mathbf{Q}_p)_{1,]U[}$ as the common zero set of integrals of invertible Makdisi symbols. Also, by Theorem 6.3.5, we can skip over the "cuspidal" residue disks.

7.1 Enumerating residue disks

First, we find all j-invariants $\bar{j}_0 \in \mathbf{F}_p$ such that there exist $U \in X_G(\mathbf{F}_p)$ with j-invariant $\bar{j}_0$. This can be done using Andrew Sutherland's intrinsic

`GL2jInvariant(p)`.

(Note that this intrinsic will give the j-invariants for $G^T := \{(g^{-1})^t : g \in G\}$ rather than G, but this is fine because we assumed that G contains all scalar matrices, so G is conjugate to G^T via $\left[\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right]$.) For such $\bar{j}_0$, we construct the elliptic curve over $\mathbf{F}_p$ given by

$$E: \begin{cases} y^2 = x^3 - 27 \cdot 1728x & \bar{j}_0 \equiv 1728 (\bmod\ p) \\ y^2 = x^3 + 54 \cdot 1728^2 & \bar{j}_0 \equiv 0 (\bmod\ p) \\ y^2 = x^3 - 27\bar{j}_0(\bar{j}_0 - 1728)x + 54\bar{j}_0(\bar{j}_0 - 1728)^2 & \text{otherwise.} \end{cases}$$

In order to talk about level structures on E, we will construct a framing $\beta_0 \colon \mathbf{Z}(N)^2 \to E[N](\bar{\mathbf{F}}_p)$ of E following [49, Section 5]. In [49], Mascot constructs a β_0 as follows. For each ℓ dividing N with exponent e, factor the polynomial given by $\Psi_{\ell^e}(x)/\Psi_{\ell^{e-1}}(x)$. Choose two roots $x_{A,\ell}$ and $x_{B,\ell}$ randomly, and pick two points $P_{A,\ell}, P_{B,\ell}$ on $E[\ell^e]$ with those respective x-coordinates. Check if $e_{\ell^e}(P_{A,\ell}, P_{B,\ell}) \neq 1$; if it is 1, then repeat this process until it is not 1. At the end, output $A := \sum_{\ell | N} P_{A,\ell}$ and $B := \sum_{\ell | N} P_{B,\ell}$, and let β_0 be $\left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right]$.

We will also need to compute matrices for various endomorphisms of E with respect to the framing β_0. The answer can yet again be found in [49, Section 5], namely:

Proposition 7.1.1. *Let $\phi \in \mathrm{End}(E)$ be an endomorphism. Then, with respect to β_0, the action of ϕ on $E[N]$ is given by the matrix*

$$\begin{bmatrix} \log(e_N(\phi(A), B)) & -\log(e_N(\phi(A), A)) \\ \log(e_N(\phi(B), B)) & -\log(e_N(\phi(B), A)) \end{bmatrix},$$

where the logarithm is the discrete logarithm on Nth roots of unity, with base $e_N(A, B)$.

Proof. For indeterminates a, b, c, d, write $\phi(A) = aA + bB$ and $\phi(B) = cA + dB$. Then compute the Weil pairings of $\phi(A)$ and $\phi(B)$ with A and B, noting that the Weil pairing $e_N(\cdot, \cdot)$ is alternating. □

Using Proposition 7.1.1, we can compute the matrices attached to the Frobenius endomor-

phism Fr_p as well as the automorphism group μ_E of $E_{\bar{\mathbf{F}}_p}$; then, we simply enumerate the double coset space $G\backslash \mathrm{GL}_2(N)/\mu_E$ by representatives $\{g_i\}$, and then for each g_i, test if $\mathrm{Fr}_p \in g_i^{-1} G g_i \mu_E$.

The resulting set of residue disks is a list of tuples $((E,\beta_0),g)$, where $E := (E,\beta_0)$ denotes a framed elliptic curve over $\mathbf{F}_p$, and where $g \in \mathrm{GL}_2(N)$ constitutes a G-level structure of E as per the previous paragraph.

7.2 Universal families for each residue disk

With the enumeration in hand, we will now construct for each $U := ((E,\beta_0),g) \in X_G(\mathbf{F}_p)$, a uniformizing parameter t for the infinitesimal neighborhood $]U[$ of U and a family E_t of elliptic curves over $]U[$.

On the residue disk $]U[$, let $\bar{j}_0 \in \mathbf{F}_p$ denote the j-invariant of U. We choose a suitable lift of $\bar{j}_0$ to an element j_0 of characteristic zero as follows. If $\bar{j}_0 = 0$ (resp. 1728), then we set j_0 to be 0 (resp. 1728). Otherwise, $\bar{j}_0$ is a j-invariant that is not 0 or 1728, and we just choose any $j_0 \in \mathbf{Z}$ lifting $\bar{j}_0$.

We will now construct an open p-adic unit disk and a family of framed elliptic curves, and then show that this data constitutes precisely the infinitesimal neighborhood $]U[$ of U. Let us begin with the unit disk construction. For a suitably chosen $u \in \mathbf{Z}_p^\times$ depending on $[Gg\mu_E]$, to be chosen later, we construct a map

$$\mathrm{Spf}(\mathbf{Z}_p[[t]]) \to \mathrm{Spf}(\mathbf{Z}_p[[j-j_0]]) \subset X(1)$$

given by

$$j = \begin{cases} ut^2 + 1728 & j_0 = 1728 \\ ut^3 & j_0 = 0 \\ j_0 + t & \text{otherwise} \end{cases}.$$

Next, we describe a family $E_{t,u}$ of elliptic curves over $\mathrm{Spf}(\mathbf{Z}_p[[t]])$. To wit, we define $E_{t,u}$ by

$$E_{t,u}\colon \begin{cases} y^2 = x^3 - 27u(ut^2+1728)x + 54u^2t(ut^2+1728)) & j_0 = 1728 \\ y^2 = x^3 - 27ut(ut^3-1728)x + 54u(ut^3-1728)^2 & j_0 = 0 \\ y^2 = x^3 - 27(t+j_0)(t+j_0-1728)x + 54(t+j_0)(t+j_0-1728)^2 & \text{otherwise.} \end{cases}$$

In the next paragraph, we will describe a method to compute $u \in \mathbf{Z}_p^\times$, but let us first explain why it is necessary to choose certain $u \in \mathbf{Z}_p^\times$. Visibly, $E_{t,u}$ deforms E, at least up to "twisting by u", but simply letting u be 1 will not necessarily guarantee that Fr_p lies in the group $g^{-1}Gg$; rather, it only guarantees the existence of an automorphism $a \in \mu_E$ such that $\mathrm{Fr}_p \cdot a$ lies in $g^{-1}Gg$. This is an issue, because when E is deformed to a family $\mathscr{E}$ over $\mathrm{Spf}(\mathbf{Z}_p[[t]])$, the automorphism group may shrink, meaning that $\mathscr{E} \to \mathrm{Spf}(\mathbf{Z}_p[[t]])$ does not actually constitute a $\mathbf{Z}_p[[t]]$-rational point of X_G. As a result, we will have to take a suitable twist of $\mathscr{E}$ in order to remedy this, in particular so that Fr_p lies in $g^{-1}Gg$ on the nose. We also note that since G is assumed to contain $\pm I$, the above situation will only concern us when j_0 is either 0 or 1728; in those situations, we will be taking either a cubic or quartic twist.

We now describe a method to choose $u \in \mathbf{Z}_p^\times$. First, we check if $g\,\mathrm{Fr}_p\,g^{-1}$ lies in G if we consider $E_{t,u}$ when u is set to be just 1; if this is the case, then we do not do anything, and we just let u be 1. Otherwise, there are three cases.

- If $j_0 = 1728$, then take any quartic twist; any two quartic twists will differ by at most

a quadratic twist, and as said before, since $-I \in G$, quadratic twists do not concern us. Concretely, choose any $u \in \mathbf{Z}_p^\times / \mathbf{Z}_p^{\times 4}$, and then take $E_{t,u}$ to be our family.

- If $j_0 = 0$ and $p \equiv 1 \bmod 3$, we first find $a \in \mu_E$ such that $\mathrm{Fr}_p \cdot a$ lies in $g^{-1}Gg$. From a, we extract the unique third root of unity $\zeta_3 \in \mathbf{F}_p^\times$ such that the action of a on x-coordinates is given by multiplication by ζ_3. We find a primitive root $\bar{u}$ of $\mathbf{F}_p^\times$ such that $\bar{u}^{(p-1)/3}$ equals ζ_3, and we claim that any lift $u \in \mathbf{Z}_p^\times$ of $\bar{u}$ will do the trick. Indeed, twisting by u changes the model over $t = p = 0$ from

$$y^2 = x^3 + 54 \cdot 1728^2 \text{ to } y^2 = x^3 + 54 \cdot 1728^2 u,$$

meaning that, when the curves are identified by $(x,y) \mapsto (u^{1/3}x, u^{1/2}y)$, the Frobenius endomorphism changes from $(x,y) \mapsto (\mathrm{Fr}_p(x), \mathrm{Fr}_p(y))$ to

$$\begin{aligned}(u^{1/3}x, u^{1/2}y) &\mapsto \left(u^{1/3} \cdot \frac{\mathrm{Fr}_p(u^{1/3})}{u^{1/3}} \mathrm{Fr}_p(x), u^{1/2} \cdot \frac{\mathrm{Fr}_p(u^{1/2})}{u^{1/2}} \mathrm{Fr}_p(x) \right) \\ &= (u^{1/3} \cdot u^{(p-1)/3} \mathrm{Fr}_p(x), u^{1/2} \cdot u^{(p-1)/2} \mathrm{Fr}_p(y)).\end{aligned}$$

That is, on the x-coordinate, the Frobenius Fr_p changes into $[\zeta_3] \circ \mathrm{Fr}_p$, and on the y-coordinate, the Frobenius is multiplied by a factor of ± 1. But this is precisely the mapping $\mathrm{Fr}_p \cdot a$ (up to the automorphism ± 1), which we said lies inside $g^{-1}Gg$. Thus our claim is verified. (In fact, this extra "automorphism" is precisely the cocycle that defines the cubic twist in question.)

- If $j_0 = 0$ and $p \equiv 2 \bmod 3$, we claim that there exists an automorphism $a' \in \mu_E$ such that, if we define $\tilde{g} := g \cdot a'$, then we have $\mathrm{Fr}_p \in \tilde{g}^{-1}G\tilde{g}$. (Crucially, $\tilde{g}$ and g represent the same double coset $[Gg\mu_E]$, so we are free to change g to $\tilde{g}$ without restriction.) Indeed, if $\alpha \in \mu_E$ is the automorphism $(x,y) \mapsto (\zeta_3 x, -y)$, we compute that $\alpha \cdot \mathrm{Fr}_p$ equals $\mathrm{Fr}_p \cdot \alpha^{-1}$, since both compositions map (x,y) to $(\zeta_3 x^p, -y^p)$; here we are using the fact that $p \equiv 2 \bmod 3$ to deduce

that $(\zeta_3^{-1})^p = \zeta_3$ for $\mathrm{Fr}_p \cdot \alpha^{-1}$. Thus, if $k \in \mathbf{Z}/6\mathbf{Z}$ is such that $\mathrm{Fr}_p \cdot \alpha^k \in g^{-1}Gg$, then first we can assume that k is even, multiplying by the automorphism $[-1]$ if needed; then we may take a' to be $\alpha^{k/2}$, for then

$$\mathrm{Fr}_p = \alpha^{k/2}\,\mathrm{Fr}_p\,\alpha^{k/2} = (a')^{-1}(\mathrm{Fr}_p\,\alpha^k)(a') \in \tilde{g}^{-1}G\tilde{g}.$$

This verifies the claim.

We now claim the following.

Proposition 7.2.1. *Choose u as above. If $U \in X_G(\mathbf{F}_p)$ is not elliptic, then the family $E_{t,u} \to \mathrm{Spf}(\mathbf{Z}_p[[t]])$ along with its implicit framing β_0 and G-level structure $[Gg]$, identifies $\mathrm{Spf}(\mathbf{Z}_p[[t]])$ with the infinitesimal neighborhood $]U[$ of U. If $U \in X_G(\mathbf{F}_p)$ is elliptic, then $((E_{t,u}, \beta_0), g)$ identifies $\mathrm{Spf}(\mathbf{Z}_p[[t]])$ with a finite cover of $]U[$.*

Proof. On $]U[$, choose a local coordinate t_0; for example, t_0 can be taken to be $\mathbf{Z}[1/N]$-integral.

From the choice of u, the family $E_{t,u}$ gives a map $\mathrm{Spf}(\mathbf{Z}_p[[t]]) \to X_G$. At all finite quotients of $\mathbf{Z}_p[[t]]$, the map $\mathrm{Spec}(\mathbf{Z}_p[[t]]/(p,t)^n) \to X_G$ is an infinitesimal thickening of the map $U\colon\ \mathrm{Spec}(\mathbf{F}_p) \to X_G$, and thus factors through $]U[= \mathrm{Spf}(\mathbf{Z}_p[[t_0]])$. Taking the colimit, we obtain a map

$$\mathrm{Spf}(\mathbf{Z}_p[[t]]) \to \mathrm{Spf}(\mathbf{Z}_p[[t_0]]) =]U[,$$

and also note that this map sits over $\mathrm{Spf}(\mathbf{Z}_p[[j - j_0]])$, so that there are maps to there from both the source and the target. The map $]U[\to \mathrm{Spf}(\mathbf{Z}_p[[j - j_0]])$ is induced by the map $X_G \to X(1)$, and the map $\mathrm{Spf}(\mathbf{Z}_p[[t]]) \to \mathrm{Spf}(\mathbf{Z}_p[[j - j_0]])$ is induced by our choice of t. In what follows, let R denote $\mathbf{Z}_p[[t]]$ for convenience. We have four cases:

- If $j_0 \neq 0, 1728$, then $X_G \to X(1)$ is unramified under U, thus $(j - j_0)R = (t_0)R$. Since we also identified t with $j - j_0$, it follows that the map $\mathrm{Spf}(R) \to]U[$ is an isomorphism.

- If $j_0 = 0$ (resp. 1728), and $U \in X_G(\mathbf{F}_p)$ is elliptic, then the map $]U[\to \mathrm{Spf}(\mathbf{Z}_p[[j - j_0]])$ is still an isomorphism, and of which $\mathrm{Spf}(R)$ sits above a 3-fold (resp. 2-fold) cover.

- If $j_0 = 0$ and $U \in X_G(\mathbf{F}_p)$ is not elliptic, then we $(j)R = (t_0^3)R$, thus there exists $u' \in \mathbf{Z}_p^\times$ such that $j = u't_0^3 + O(pt_0^3, t_0^4)$. On the other hand, we also have $j = ut^3$, whence the equation

$$ut^3 = u't_0^3 + O(pt_0^3, t_0^4).$$

  Remembering the map $\mathrm{Spf}(R) \to]U[$, we see that t_0 can also be written as a power series in $\mathbf{Z}_p[[t]]$. Equating leading terms, this forces u/u' to lie in $\mathbf{Z}_p^{\times 3}$; from this, we get an expression of t as a power series in terms of t_0, and thus $\mathrm{Spf}(R) \to]U[$ is an isomorphism.

- The case when $j_0 = 1728$ and $U \in X_G(\mathbf{F}_p)$ is not elliptic plays similarly to the $j_0 = 0$ counterpart. In this case, we have

$$ut^2 = j - 1728 = u't_0^2 + O(pt_0^2, t_0^3)$$

  and, by similar considerations, we see that u/u' lies in $\mathbf{Z}_p^{\times 2}$, and then are able to write t as a power series in terms of t_0, thus confirming that $\mathrm{Spf}(R) \to]U[$ is an isomorphism here too.

□

7.3 Digression: modular polynomials

In this subsection we will recall some properties surrounding modular polynomials, in preparation for a more explicit description for $X(\mathbf{Q}_p)_1$ on each residue disk. We recall that the j-invariant identifies $X(1)$ with $\mathbf{P}^1$. Define γ_2 and γ_3 to be functions satisfying $\gamma_2^3 = j$ and $\gamma_3^2 = j - 1728$; then γ_2 identifies $X_{ns}^+(3)$ with $\mathbf{P}^1$ and γ_3 identifies $X_{ns}(2)$ with $\mathbf{P}^1$. The modular polynomials $\Phi_p(X,Y)$, $\Phi_p^{\gamma_2}(X,Y)$ and $\Phi_p^{\gamma_3}(X,Y)$ are given by the graphs of the Hecke correspondence T_p for the

respective groups $X(1)$, $X_{ns}^{+}(3)$ and $X_{ns}(2)$, with respect to the respective parameters j, γ_2 and γ_3, normalized so that the coefficient of X^{p+1} in each polynomial is 1. These modular polynomials are all symmetric in X and Y (so for instance $\Phi_p(X,Y) = \Phi_p(Y,X)$), and modulo p the modular polynomials all reduce to $(X-Y^p)(X^p-Y)$ (that this occurs is a consequence of the Eichler-Shimura relation). We briefly describe how to compute the modular polynomials in question.

- The modular polynomial Φ_p is taken from Andrew Sutherland's website; see [33] for more details.

- The modular polynomial $\Phi_p^{\gamma_2}(X,Y)$ is a factor of $\Phi_p(X^3,Y^3)$, and below we claim that it can be identified as the smaller of the two irreducible factors of $\Phi_p(X^3,Y^3)$. Indeed, if $\Phi_p^{\gamma_2}(X,Y)$ is a factor, then $\Phi_p^{\gamma_2}(X,\zeta_3 Y)$ and $\Phi_p^{\gamma_2}(X,\bar{\zeta}_3 Y)$ are also factors. These three factors are pairwise relatively prime to each other; this is because $\Phi_p(X^3,Y^3)$ permutes the fibers above the pair $(j(\tau), j(p\tau))$ (or at least generically so). Thus,

$$\Phi_p(X^3,Y^3) = \Phi_p^{\gamma_2}(X,Y)\Phi_p^{\gamma_2}(X,\zeta_3 Y)\Phi_p^{\gamma_2}(X,\zeta_3^2 Y),$$

  and the product of the latter two factors form an irreducible polynomial over $\mathbf{Z}[X,Y]$, of whose degree is obviously larger than that of $\Phi_p^{\gamma_2}(X,Y)$.

- The modular polynomial $\Phi_p^{\gamma_3}(X,Y)$ is a factor of $\Phi_p(X^2+1728, Y^2+1728)$; similar to the case of γ_2, it follows that we have a factorization

$$\Phi_p(X^2+1728,Y^2+1728) = \Phi_p^{\gamma_3}(X,Y)\Phi_p^{\gamma_3}(X,-Y).$$

  The factor $\Phi_p^{\gamma_3}(X,Y)$ can be identified as the unique factor such that the coefficient $a_{p,p}$ of X^pY^p reduces to -1 modulo p (by the Eichler-Shimura relation); for the other factor, its coefficient of X^pY^p is $-a_{p,p}$.

Lemma 7.3.1. *For any of the parameters $t = j - j_0, \gamma_2, \gamma_3$, the polynomial $\Phi_p^t(0,t)$ is a degree $p+1$ polynomial in t whose roots all have p-adic valuation bounded below by $1/(p+1)$.*

Proof. By Eichler-Shimura, the polynomial reduces mod p to t^{p+1}. Thus the Newton polygon of the polynomial has slope at least $1/(p+1)$; the claim follows. □

7.4 The Chabauty-Coleman locus on a residue disk

Recall that by Theorem 3.0.1 and by Theorem 4.4.2, the set $X(\mathbf{Q}_p)_1$ breaks up into a disjoint union of $X(\mathbf{Q}_p)_{1,]U[}$ for each $U \in X(\mathbf{F}_p)$, and that $X(\mathbf{Q}_p)_{1,]U[}$ is precisely the simultaneous vanishing loci of

$$\int_0^x \mathrm{KS}(f)(t)\,dt - \sum_{i=0}^{p} \int_0^{\alpha_i} \mathrm{KS}((p+1-T_p)^{-1} f)(t)\,dt$$

as f ranges through invertible Makdisi symbols on G, and where the α_i are the images of $t = 0$ under $(T_p)_*$.

Notation 7.4.1. If $P(X) = \sum_{k=0}^{d} c_k X^k$ is a degree d polynomial, let $e_k(P)$ denote the k-th symmetric sum of the roots of $P(X)$, and let $p_k(P)$ denote the k-th power sum of the roots of $P(X)$.

Combining Theorem 3.0.1 with our descriptions of residue disks $]U[$ and uniformizing parameters $t = t_U$, as well as Theorem 4.4.2, we obtain the following:

Theorem 7.4.2. *Let $U \in Y(\mathbf{F}_p)$ denote a residue disk $]U[$, and choose as uniformizing parameter t as per the rule above. Choose a basis $\{\mathrm{Mak}_G(h_i)\}_{i \in \mathscr{I}}$ of $S_2(X_G)_{rk=0}$, and let $\mathbf{B}_{U,t}$ be the matrix whose rows are indexed by $\mathscr{I}$, and such row i contains the infinite, 0-indexed list of coefficients for $\mathrm{KS}(\mathrm{Mak}_G(h_i))(t) \in \mathbf{Z}_p[[t]]$. By abuse of notation, let T_p denote the matrix of the Hecke operator acting on the basis $\{\mathrm{Mak}_G(h_i)\}_{i \in \mathscr{I}}$ of $S_2(X_G)_{rk=0}$. Let $\mathbf{M}_{antider}$ be the diagonal matrix $\mathrm{diag}(1, 1/2, 1/3, \dots)$, let $\mathbf{v}_{U,t}$ be the column vector whose transpose $\mathbf{v}^T$ is*

$$(p_1(\Phi_p^t(0,t)), p_2(\Phi_p^t(0,t)), p_3(\Phi_p^t(0,t)), \dots),$$

and let $\mathbf{x}$ *be the column vector whose transpose* $\mathbf{x}^T$ *is* $(x, x^2, x^3, \dots)$*. Then*

$$X(\mathbf{Q}_p)_{1,]U[} = \left\{ x \in p\mathbf{Z}_p \colon \mathbf{B}_{U,t} \cdot \mathbf{M}_{antider} \cdot \mathbf{x} - (p+1-T_p)^{-1} \cdot \mathbf{B}_{U,t} \cdot \mathbf{M}_{antider} \cdot \mathbf{v} = 0 \right\},$$

noting that the second term is a column vector of "constant terms", while the first term gives the rest of the terms of the power series.

We note that the quantities $p_k(\Phi_p^t(0,t))$, as k varies, can be computed efficiently by using Newton-Girard formulae:

Proposition 7.4.3 (Newton-Girard formulae)**.** *If* $P(X) = \sum_{k=0}^{d} c_k X^k$ *is a degree* d *polynomial, let* $e_j := e_j(P)$ *and* $p_j := p_j(P)$ *denote the same elementary symmetric and power sums as before. Then the following hold:*

- *We have* $e_k = (-1)^k \frac{c_{d-k}}{c_d}$ *for* $0 \leq k \leq d$.
- *We have*

$$p_k = \begin{cases} (-1)^{k-1} k e_k + \sum_{i=1}^{k-1} (-1)^{k-1+i} e_{k-1} p_i & 1 \leq k \leq d \\ \sum_{i=k-d}^{k-1} (-1)^{k-1+i} e_{k-1} p_i & k > d. \end{cases}$$

Chapter 8

Power series on every residue disk

In the previous section, we have set up tiny Coleman integrals for the Chabauty-Coleman locus on every relevant residue disk of consideration. In this section, we will explain how to compute the power series expansion of a holomorphic differential attached to an invertible Makdisi symbol with respect to a uniformizing parameter t. Specifically, our goal is to compute the power series expansion for $(\mathrm{KS} \circ \mathrm{Mak}_G)(\gamma)$ "at" a residue disk attached to the mod p point $((E, \beta_0), [Gh\mu_E])$. We will do this by evaluating $(\mathrm{KS} \circ \mathrm{Mak}_G)(\gamma)$ "at" suitable points $t^{p+1} = \alpha_1 p, \ldots, \alpha_C p$, where C is the desired p-adic precision, and then Lagrange interpolating to obtain a degree $C \cdot (p+1)$ polynomial in t that constitutes our approximation to the power series. (The reason why we use t^{p+1} instead of t will become apparent later on; in a nutshell, this is to compensate for the fact that the roots of the modular polynomial have small p-valuation. See Subsection 8.4 and Subsection 8.5 for more details on this.) In particular, we note the following:

8.1 The differential

Recall that the Kodaira-Spencer map gives

$$\mathrm{KS}(f) = f\frac{dq}{q} = f \cdot 2\pi i\, d\tau.$$

Our first aim is to express $2\pi i\, d\tau$ as a polynomial differential in terms of t, for whatever t is chosen. To prepare ourselves, here are some facts about differentials.

Proposition 8.1.1. *We have* $\frac{1}{2\pi i}\frac{dj}{d\tau} = -\frac{E_6 j}{E_4}$.

Proof. See [50]. □

Proposition 8.1.2. *Suppose* $(E,\omega) = (y^2 = x^3 + ax + b, dx/(2y))$. *Then we have*

$$\frac{E_4(E,\omega)}{E_6(E,\omega)} = \frac{2\pi^2}{9}\cdot\frac{a}{b}.$$

Proof. This follows from the theory of the Weierstrass $\wp$-function. □

Let t be the local uniformizing parameter, and let the equation for our universal elliptic curve over $]U[$ be given by $y^2 = x^3 + a(t)x + b(t)$. (A Weierstrass equation always comes equipped with the invariant differential $dx/(2y)$.) Then

$$\begin{aligned} 2\pi i\frac{d\tau}{dt} &= 2\pi i\frac{j'(t)}{j'(\tau)} = 2\pi i j'(t)\cdot\frac{-E_4}{2\pi i E_6\cdot j} \\ &= -\frac{E_4 j'(t)}{E_6 j} = -\frac{2\pi^2}{9}\frac{a(t)}{b(t)}\frac{j'(t)}{j(t)} \\ &= (2\pi i)^2\cdot\frac{a(t)j'(t)}{18b(t)j(t)}, \end{aligned}$$

thus

$$(KS)\left(\frac{f}{(2\pi i)^2}\right) = \frac{f(t)a(t)j'(t)}{18b(t)j(t)}\,dt.$$

In particular, recalling our definitions of t, $a(t)$ and $b(t)$:

$$j = \begin{cases} ut^2 + 1728 & j_0 = 1728 \\ ut^3 & j_0 = 0 \\ j_0 + t & \text{otherwise} \end{cases}$$

$$(a(t), b(t)) = \begin{cases} (-27u(ut^2+1728), 54u^2t(ut^2+1728)) & j_0 = 1728 \\ (-27ut(ut^3-1728), 54u(ut^3-1728)^2) & j_0 = 0 \\ (27(t+j_0)(t+j_0-1728), 54(t+j_0)(t+j_0-1728)^2) & \text{otherwise,} \end{cases}$$

we readily obtain:

$$(KS)\left(\frac{f}{(2\pi i)^2}\right) = \begin{cases} -\frac{f(t)\,dt}{18(ut^2+1728)} & j_0 = 1728 \\ -\frac{f(t)\,dt}{12(ut^3-1728)} & j_0 = 0 \\ -\frac{f(t)\,dt}{36(t+j_0)(t+j_0-1728)} & \text{otherwise.} \end{cases} \tag{8.1}$$

8.1.3 Elliptic points and changing uniformizers

Sometimes U will be an elliptic point, in which case $\mathrm{KS}(f)$ will enjoy a power series expansion in $\mathbf{Z}_p[[j-j_0]]\,dj$. We illustrate these cases as follows.

- If $j_0 = 1728$, then we had set $j = ut^2 + 1728$, thus

$$a_0 + a_1(j-1728) + a_2(j-1728)^2 + \cdots\, dj = 2u(a_0 t + a_1 ut^3 + a_2 u^2 t^5 + \cdots)\, dt.$$

- If $j_0 = 0$, then we had set $j = ut^3$, thus

$$a_0 + a_1 j + a_2 j^2 + \cdots\, dj = 3u(a_0 t^2 + a_1 ut^5 + a_2 u^2 t^8 + \cdots)\, dt.$$

8.2 Sampling elliptic curves in characteristic zero

Let C be our desired p-adic precision. We are to consider the universal elliptic curve $E_{t,u}$, evaluated at each of the points $t^{p+1} = \alpha_1 p, \alpha_2 p, \ldots, \alpha_C p$. From now on, fix such a t^{p+1}. (So t will live in a ramified extension of $\mathbf{Q}_p$ of degree $p+1$.) With our framing $\beta_0 = \left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right]$ of E, we choose random lifts $(\tilde{x}_A, \tilde{y}_A)$ of A and $(\tilde{x}_B, \tilde{y}_B)$ of B, both to characteristic zero, and then iterate for each of these lifts the process

$$(x,y) \mapsto (DF)(x,y)^{-1} \cdot F(x,y),$$

where DF denotes the matrix derivative of the vector-valued function F, and where F is given by

$$F(x,y) := \left[\begin{smallmatrix} y^2 - x^3 - a(t)x - b(t) \\ \Psi_N(x,y) \end{smallmatrix}\right].$$

(Here, Ψ_N is the N-division polynomial, to be introduced shortly.) Essentially, what we are doing here is performing a p-adic version of Newton or Hensel iteration; from the coordinates of the function F, and in particular because $E[N]$ is an etale group scheme in characteristic p for $p \nmid N$, the process will converge to the unique point on $y^2 = x^3 + a(t)x + b(t)$ that is an N-division point and that lifts the framing $\left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right]$. This process also explains why we were allowed to be vague about our choice of framing for deformations of our elliptic curve E; it turns out that the framing on the special fiber determines the framing everywhere on $]U[$.

Here are the equations for everything we need to compute here. We have

$$(DF)(x,y) = \left[\begin{smallmatrix} -3x^2 - A & 2y \\ (\Psi_N)_x & (\Psi_N)_y \end{smallmatrix}\right].$$

The division polynomials $\Psi_N(x,y)$ are given by the recurrence

$$\begin{aligned}
\Psi_0(x,y) &= 0 \\
\Psi_1(x,y) &= 1 \\
\Psi_2(x,y) &= 2y \\
\Psi_3(x,y) &= 3x^4 + 6Ax^2 + 12Bx - A^2 \\
\Psi_4(x,y) &= 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\
\Psi_{2m}(x,y) &= \frac{\Psi_m}{2y} \cdot (\Psi_{m+2}\Psi_{m-1}^2 - \Psi_{m-2}\Psi_{m+1}^2) \\
\Psi_{2m+1}(x,y) &= \Psi_{m+2}\Psi_m^3 - \Psi_{m-1}\Psi_{m+1}^3.
\end{aligned}$$

Hence, $(\nabla\Psi_N)(x,y) = ((\Psi_N)_x, (\Psi_N)_y)$ is given by

$$\begin{aligned}
\nabla\Psi_0 &= \nabla\Psi_1 = (0,0) \\
\nabla\Psi_2 &= (0,2) \\
\nabla\Psi_3 &= (12y^2, 0) \\
\nabla\Psi_4 &= (4y(12Ax^3 + 36Bx^2 - 4A^2x - 4Ay^2 + 2x\Psi_3), \Psi_4/y) \\
\nabla\Psi_{2m} &= (\nabla\Psi_m)\frac{\Psi_{2m}}{\Psi_m} + \frac{\Psi_m}{2y}((\nabla\Psi_{m+2})\Psi_{m-1}^2 + 2(\nabla\Psi_{m-1})\Psi_{m+2}\Psi_{m-1} - (\nabla\Psi_{m-2})\Psi_{m+1}^2 \\
&\quad - 2(\nabla\Psi_{m+1})\Psi_{m-2}\Psi_{m+1}) - \langle 0, \Phi_{2m}/y\rangle \\
\nabla\Psi_{2m+1} &= (\nabla\Psi_{m+2})\Psi_m^3 + 3\Psi_{m+2}\Psi_m^2(\nabla\Psi_m) - (\nabla\Psi_{m-1})\Psi_{m+1}^3 - 3\Psi_{m-1}\Psi_{m+1}^2(\nabla\Psi_{m+1}).
\end{aligned}$$

8.3 Computing "Eisenstein tables"

Now suppose we have an elliptic curve E, differential ω and framing $\beta_0 = \left[\begin{smallmatrix} A \\ B \end{smallmatrix}\right]$, with $\mathscr{W} = (E, \omega, \beta_0) = (y^2 = x^3 + Ax + B, dx/(2y), \left[\begin{smallmatrix} P \\ Q \end{smallmatrix}\right])$. We will now compute, for each $(a,b) \in \mathbf{Z}(N)^2$ of exact order N, the weights 1 and 2 Eisenstein series $E_1((a,b)_{/N}; \mathscr{W})$ and $E_2((a,b)_{/N}; \mathscr{W})$. We

have optimized this process to the best extent possible, using the Frobenius action as well as double-and-add sequences. We explain the process below.

First, we recall some formulas. If P and Q are points of E, then we have the *slope function*

$$\lambda(P,Q) := \begin{cases} \frac{y(Q)-y(P)}{x(Q)-x(P)} & P \neq Q \\ \frac{3x(P)^2+A}{2y(P)} & P = Q. \end{cases}$$

We recall the addition formula:

$$(x(P+Q), y(P+Q)) = (\lambda(P,Q)^2 - x(P) - x(Q), \lambda(P,Q) \cdot (x(P) - x(P+Q)) - y(P)).$$

Now we have the following moduli interpretation of E_1 and E_2, thanks to the work of Khuri-Makdisi in [40, Section 3] and further developed by Mascot in [49, Section 4]: for all row vectors $v, w \in \mathbf{Z}(N)^2$, we have

$$\begin{aligned} E_2(v_{/N}; \mathscr{W}) - E_2(0; \mathscr{W}) &= x(\beta_0(v)) \\ E_1(v_{/N}; \mathscr{W}) + E_1(w_{/N}; \mathscr{W}) &= E_1((v+w)_{/N}; \mathscr{W}) - \lambda(\beta_0(v), \beta_0(w)). \end{aligned}$$

We loop over representatives of the double coset space $K_0(N) \backslash \mathrm{GL}_2(N) / \langle \mathrm{Fr}_p \rangle$. If $\left[\begin{smallmatrix} * & * \\ a & b \end{smallmatrix}\right]$ is a representative for such a double coset, then start by computing $P := (a,b)\beta_0 = aA + bB$. Let $r \in \mathbf{Z}_{>0}$ be the smallest positive integer such that $(a,b)\,\mathrm{Fr}_p^r$ is a scalar multiple of (a,b) (i.e. Fr_p^r fixes the line generated by P), and let $\lambda \in \mathbf{Z}(N)^*$ be such that $(a,b)\,\mathrm{Fr}_p^r = (\lambda a, \lambda b)$. Choose representatives $\{a_1, \ldots, a_n\}$ for the quotient group $\mathbf{Z}(N)^* / \langle \lambda \rangle$, with the provision that λ must be used as the representative for the identity coset. As per [1, Algorithm 4.8, page 16], we may create an addition sequence $\mathscr{S}(a_1, \ldots, a_n)$ that contains all a_i.

We will now explain how to efficiently compute weight 1 Eisenstein series. Fix a row vector

$v \in \mathbf{Z}(N)^*$ of exact order N, and define quantities $c_1, \ldots, c_{N-1}$ by

$$c_m := E_1(mv_{/N}; \mathscr{W}) - m \cdot E_1(v_{/N}; \mathscr{W}).$$

Then, we have the following statements about c_1 in relation to computing Eisenstein series.

Proposition 8.3.1. *The following identities hold:*

$$\begin{aligned} c_1 &= 0. \\ c_{m+n} &= c_m + c_n + \lambda(m\beta_0(v), n\beta_0(v)). \\ E_1(v_{/N}; \mathscr{W}) &= -\frac{c_{N-1}}{N}. \\ E_1(mv_{/N}; \mathscr{W}) &= c_m - \frac{m}{N} c_{N-1}. \\ c_{m \cdot u} &= \mathrm{Fr}_p^r(c_m) + m \cdot c_u. \end{aligned}$$

Proof. The first four statements can be derived from the characterization given earlier:

$$E_1(v_{/N}; \mathscr{W}) + E_1(w_{/N}; \mathscr{W}) = E_1((v+w)_{/N}; \mathscr{W}) - \lambda(\beta_0(v), \beta_0(w)).$$

For the last statement, we note that

$$c_{m \cdot u} - m \cdot c_u = E_1(muv_{/N}; \mathscr{W}) - mE_1(uv_{/N}; \mathscr{W}) = \mathrm{Fr}_p^r(c_m)$$

where the last equality holds because the automorphism Fr_p^r acts on all coordinates in sight by Frobenius, and hence acts on all slopes by Frobenius, and hence on the c_m. □

Now the algorithm to compute $E_1((a,b)_{/N}; \mathscr{W})$ and $E_2((a,b)_{/N}; \mathscr{W})$ for all $(a,b) \in \mathbf{Z}(N)^2$ of exact order N proceeds as follows.

- Loop over representatives $\left[\begin{smallmatrix} * & * \\ a & b \end{smallmatrix}\right]$ of $K_0(N) \backslash \mathrm{GL}_2(N) / \langle \mathrm{Fr}_p \rangle$.

- For such a representative, let $v := (a,b)$, let $P := \beta_0(v) = av_1 + bv_2$, and let $r,u \in \mathbf{Z}(N)^*$ be as above.

- Use the double-and-add sequence $\mathscr{S}(a_1,\ldots,a_n)$ to compute $E_2(a_i v_{/N};\mathscr{W}) = x(\beta_0(a_i v))$ for $i = 1,\ldots,n$. In the process of doing this, we are also computing slopes, and use that information to also compute $c_{a_1},\ldots,c_{a_n}$ along the way.

- Act via Fr_p^r to obtain $c_1,\ldots,c_{N-1}$ as well as $E_2(v_{/N};\mathscr{W}),\ldots,E_2((N-1)v_{/N};\mathscr{W})$.

- Act via $\mathrm{Fr}_p,\ldots,\mathrm{Fr}_p^{r-1}$ to obtain the values of E_1 and E_2 for all other points in the lines contained in the orbit of the Frobenius Fr_p acting on the line $\langle v\rangle$.

After we are done with this, we use Equation (8.1), Theorem 5.2.1, Theorem 5.2.2 and Theorem 5.1.1 to compute the holomorphic differential $\mathrm{KS}(\mathrm{Mak}_G(\gamma);\mathscr{W})$ as some scalar times dt, where $\mathscr{W}$ is the datum as the parameter t ranges along $t^{p+1} = \alpha_1,\ldots,\alpha_C p$. What to do after this will be covered in the next section.

8.4 Lagrange interpolation

We claim that a nice choice of sampling points is given by $t^{p+1} = a_{i,j}p$, for $a_{i,j}$ given by the formula

$$a_{i,j} := \zeta_{p-1}^i(1+pj)$$

and where the tuple (i,j) runs over $\mathbf{Z}/(p-1)\mathbf{Z} \times \{0,1,\ldots,C-1\}$; using these samples, we can run a combination of fast Fourier transform and Lagrange interpolation in order to recover the power series. We first recall the explicit form of the Chinese remainder theorem.

Proposition 8.4.1 (Chinese remainder theorem)**.** *Let R be a principal ideal domain, and let $(P_1),\ldots,(P_n)$ be pairwise coprime principal ideals of R with product $P := \prod_{i=1}^n P_i$. Suppose $f \in R$*

satisfies $f \equiv f_i \bmod P_i$ for each $1 \leq i \leq n$. Then we have

$$f \equiv \sum_{i=1}^{n} f_i \left(\prod_{j \neq i} P_j \right) \left[\prod_{j \neq i} P_j \right]_{P_i}^{-1} (\bmod P),$$

where the notation $[x]_{P_i}^{-1}$ means to take any lift of the multiplicative inverse of x modulo P_i.

Now recall our situation. We are computing a power series $F(t) \in \mathbf{Z}_p[[t]]$ by computing $F_{i,j} := F(\bmod t^{p+1} - a_{i,j}p)$ as the tuple (i,j) runs over $\mathbf{Z}/(p-1)\mathbf{Z} \times \{0,1,\ldots,C-1\}$, and where $a_{i,j} := \zeta_{p-1}^i(1+pj)$. For a fixed $j \in \{0,1,\ldots,C-1\}$, it then follows that $F(t)$ modulo $t^{p^2-1} - (1+pj)^{p-1}p^{p-1}$, which we will denote as $F_j(t)$, is given by

$$\begin{aligned}
F_j(t) &= \sum_{i=0}^{p-2} F_{i,j}(t) \left(\prod_{k \neq i} (t^{p+1} - \zeta_{p-1}^k(1+pj)p)/((\zeta_{p-1}^i - \zeta_{p-1}^k)(1+pj)p) \right) \\
&= \sum_{i=0}^{p-2} F_{i,j}(t) \frac{t^{p^2-1} - [(1+pj)p]^{p-1}}{t^{p+1} - \zeta_{p-1}^i(1+pj)p} [(1+pj)p]^{-(p-1)} \cdot \zeta_{p-1}^i \cdot (p-1)^{-1} \\
&= [p(p-1)(pj+1)]^{-1} \sum_{i=0}^{p-2} F_{i,j}(t) \left(1 + \frac{t^{p+1}}{\zeta_{p-1}^i(1+pj)p} + \cdots + \left[\frac{t^{p+1}}{\zeta_{p-1}^i(1+pj)p} \right]^{p-2} \right) \\
&= \sum_{k=0}^{p-2} \left((p-1)^{-1}[(1+pj)p]^{-(k+1)} \sum_{i=0}^{p-2} F_{i,j}(t) \zeta_{p-1}^{-ik} \right) t^{(p+1)k}.
\end{aligned}$$

Therefore, we learn that for each $j \in \{0,1,\ldots,C-1\}$, the polynomial $F_j(t)$ can be computed by using fast Fourier techniques on each of the $F_{i,j}$'s to compute the expressions above.

Now our situation is that for each $j \in \{0,1,\ldots,C-1\}$, we have $F(t) \equiv F_j(t) \bmod t^{p^2-1} - (1+pj)^{p-1}p^{p-1}$; this can be done by using Lagrange interpolation techniques.

8.5 Precision analysis of Lagrange interpolation

We now ascertain the precision of the polynomial obtained from Lagrange interpolation. Suppose $F(t) \equiv F_i(t)(\bmod t^{p+1} - \alpha_i p)$ for i ranging in an index set $\mathscr{I}$ of size $C \cdot (p-1)$, and

such that $\{\alpha_i\}_{i\in\mathscr{I}}$ is a subset of $\mathbf{Z}_p$ containing C elements congruent to e mod p for each $e \in \{1,\ldots,p-1\}$. The main theorem is 8.5.3, which gives the error of $F(t)$ versus the polynomial $\tilde{F}(t)$ obtained by Lagrange interpolation.

Lagrange interpolation gives $\tilde{F}(t)$, which is $F(t)$ modulo $\prod_{i\in\mathscr{I}}(t^{p+1}-\alpha_i p)$; namely, this will be

$$\sum_{i\in\mathscr{I}} \frac{F_i(t)\prod_{j\neq i}(t^{p+1}-\alpha_j p)}{p^{C(p-1)-1}\prod_{j\neq i}(\alpha_i-\alpha_j)} = \sum_{i\in\mathscr{I}} F_i(t)\left(\prod_{j\neq i}(\alpha_i-\alpha_j)\right)^{-1}\left(\prod_{j\neq i}\left(\frac{t^{p+1}}{p}-\alpha_j\right)\right).$$

Lemma 8.5.1. *We have* $v_p\left(\prod_{j\in I-\{i\}}(\alpha_i-\alpha_j)\right) \leq \left\lfloor C\left(1+\frac{1}{p-1}\right)-1\right\rfloor$.

Proof. Because the condition that $\{\alpha_i\}_{i\in\mathscr{I}}$ has C elements in each nonzero mod p residue class, we get an upper bound for the left hand side given by

$$(C-1)+\left(\left\lceil\frac{C}{p}\right\rceil-1\right)+\left(\left\lceil\frac{C}{p^2}\right\rceil-1\right)+\cdots$$

and now summing up by geometric series and using the fact that $v_p(\mathbf{Z}_p)\in\mathbf{Z}$, we obtain the result. □

Corollary 8.5.2. *Suppose each $F_i(t)$ has been computed to be a polynomial of degree at most p and such that each term has been computed to precision $O(p^{C(p-1)})$. Then, the precision of $[t^{i-1}]F(t)$ is at least $O(p^v)$, where*

$$v := \left\lceil C\left(p-2-\frac{1}{p-1}\right)\right\rceil+2-\left\lceil\frac{i}{p+1}\right\rceil.$$

Proof. We plug in the results of the lemma into the formula for $F(t)$; we also see that the terms of the form $x^{p+1}/p-\alpha_j$ force the precision to go down by one digit every $p+1$ terms. Combining this with the base precision of $F_i(t)$, we obtain the corollary. □

Theorem 8.5.3. *Suppose each $F_i(t)$ has been computed to be a polynomial of degree at most p and such that each term has been computed to precision $O(p^{C(p-1)})$. Then Lagrange interpolation gives*

an approximation $\tilde{F}(t)$ of $F(t)$ such that, for $t in p\mathbf{Z}_p$, the p-adic valuation of the error $(\tilde{F}-F)(t)$ is at least

$$\min\left(C(p-1)+\frac{1}{p+1}-\log_p(C(p^2-1)+1), \left\lceil C\left(p-2-\frac{1}{p-1}\right)\right\rceil+2-\left\lfloor\log_p(C(p^2-1))\right\rfloor\right).$$

Proof. By Theorem 7.4.2, the constant term for each power series cutting out $X(\mathbf{Q}_p)_1$ has constant term given by $\sum_{k=1}^{\infty}\frac{c_{k-1}}{k}p_k(\Phi_p^t(0,t))$. Lagrange interpolation will give $\sum_{k=1}^{(p+1)\cdot\#\mathscr{I}}\frac{c_{k-1}}{k}p_k(\Phi_p^t(0,t))$. By Corollary 8.5.2, the coefficient c_{k-1} is determined with precision

$$\left\lceil C\left(p-2-\frac{1}{p-1}\right)\right\rceil+2-\left\lceil\frac{k}{p+1}\right\rceil,$$

while by Lemma 7.3.1, the valuation of $k^{-1}p_k(\Phi_p^t(0,t))$ is at least

$$\left\lceil\frac{k}{p+1}\right\rceil-\left\lfloor\log_p(k)\right\rfloor.$$

Adding these two quantities gives that the roundoff error is given by the second term in the claimed valuation error.

Now let us turn to the truncation error; the valuation for each term after $(p+1)\cdot\#\mathscr{I}$-th term is at least

$$\frac{\#\mathscr{I}\cdot(p+1)+1}{p+1}-\log_p(\#\mathscr{I}\cdot(p+1)+1)$$

which is again true by Lemma 7.3.1. Since $\#\mathscr{I}=C(p-1)$, this means the truncation error is precisely the first term in the claimed valuation error.

This completes the proof. □

8.6 Root finding mod p^n

With the power series of the holomorphic differentials computed, we now apply Theorem 7.4.2 and Proposition 7.4.3 to find the suitable "constant term" of the power series given by antidifferentiation of the holomorphic differentials; it is then only a matter of finding the common zero locus of these power series to find $X(\mathbf{Q}_p)_1$. In this section we will detail an algorithm to obtain the roots of a polynomial $P(t) \in (\mathbf{Z}/p^n\mathbf{Z})[t]$. After this is done, we could apply the Magma command `PowerRelation(r,d)` for each root r to test for candidate minimal polynomials of small degree and height, if we believe that $X(\mathbf{Q}_p)_1$ ought to consist of *algebraic* p-adic points.

Please note that, although Corollary 8.5.2 tells us that the precision to which we know a power series $F(t)$ is decreasing to 0 after a finite number of terms, we are only interested in solutions to $F(t) = 0$ for $t \in p\mathbf{Z}_p$, and thus, we will instead compute the roots of $F(pt)$; then, Theorem 8.5.3 tells us that we have computed *all terms* of $F(pt)$ up to a certain precision.

Notation 8.6.1. For $P(t) = a_0 + a_1 t + \cdots + a_d t^d \in (\mathbf{Z}/p^n\mathbf{Z})[t]$, let $v_p(P) := \max_{0 \le i \le d} v_p(a_i)$. If $v_p(P) = m$, then let $P(t)^{norm} \in (\mathbf{Z}/p^{n-m}\mathbf{Z})[t]$ denote $P(t)/p^m$.

The algorithm goes as follows. We will loop through elements of a list S, making modifications until it is empty. Start with $S := [\langle 0, 0, P(t), n\rangle]$ and $\mathscr{R} = \{\}$. We will now loop over the following.

- In each transversal of this loop, we will iterate over S.
- First, create a new list $S' := []$. Now do the following for each element $\langle a, b, f(t), r\rangle$ of S.
- If $v_p(f) = m$, then replace $\langle a, b, f(t), r\rangle$ with $\langle a, b, f(t)/p^m, r - m\rangle$.
- If $r = 0$, then remove $\langle a, b, f(t), r\rangle$ from S and add $a + O(p^b)$ to the set $\mathscr{R}$.
- If $r = 1$, then for each root $\alpha \in \mathbf{F}_p$ of $f(t) \in \mathbf{F}_p[t]$, add $a + \alpha p^b + O(p^{b+1})$ to the set $\mathscr{R}$.

- If $r \geq 2$, then, for each root $\bar{\alpha} \in \mathbf{F}_p$ of the reduction $\bar{f}(t) \in \mathbf{F}_p[t]$, choose any lift $\alpha \in \mathbf{Z}/p^r\mathbf{Z}$ of $\bar{\alpha}$.

    1. If $f'(\alpha) \not\equiv 0 (\bmod p)$, then perform Newton iteration by applying to α the map $x \mapsto x - f(x)/f'(x)$ until a fixed point α_0 is reached. Add $a + \alpha_0 p^b + O(p^{b+r})$ to the set $\mathscr{R}$.
    2. If $f'(\alpha) \equiv 0 (\bmod p)$ but $f(\alpha) \not\equiv 0 (\bmod p^2)$, then discard α from consideration.
    3. If $f'(\alpha) \equiv 0 (\bmod p)$ and $f(\alpha) \equiv 0 (\bmod p^2)$, then for each $0 \leq k < p$, add the element $\langle a + \alpha p^b + k p^{b+1}, b+2, P(\alpha + kp + tp^2), r \rangle$ to the list S'.

- After all elements of S have been iterated over: replace S with S' if S' is not empty and loop again, or if S' is empty then output $\mathscr{R}$.

Bibliography

[1] M. J. Coster, *Some Algorithms on Addition Chains and Their Complexity*, Department of Computer Science Report CS-R9024, Centrum voor Wiskunde en Informatica (CWI), Amsterdam, 1990.

[2] Assaf, E., *Computing classical modular forms for arbitrary congruence subgroups*, Arithmetic Geometry, Number Theory, and Computation (2021), pp. 43–104.

[3] Atkin, A. & Li, W., *Twists of newforms and pseudo-eigenvalues of W-operators*, Invent. Math. **48** (1978), 221–243.

[4] Balakrishnan, J., Best, A., Bianchi, F., Lawrence, B., Müller, J., Triantafillou, N. & Vonk, J., *Two recent p-adic approaches towards the (effective) Mordell conjecture*, Arithmetic L-functions and Differential Geometric Methods **338** (2021), pp. 31–74.

[5] Jennifer S. Balakrishnan, L. Alexander Betts, Daniel R. Hast, Aashraya Jha & J. Steffen Müller, *Rational points on the non-split Cartan modular curve of level 27 and quadratic Chabauty over number fields*, arXiv:2501:07833, 2025.

[6] Balakrishnan, J. & Mazur, B., *Ogg's torsion conjecture: fifty years later (with an appendix by Netan Dogra)*, Bull. Amer. Math. Soc. (N.S.) **62**, 235–268 (2025).

[7] Jennifer S. Balakrishnan, *Coleman Integration for Hyperelliptic Curves: Algorithms and Applications*, Ph.D. thesis, Department of Mathematics, Massachusetts Institute of Technology, 2011.

[8] Jennifer S. Balakrishnan & J. Steffen Müller, *Computational tools for quadratic Chabauty*, 2020.

[9] Karim Belabas & Henri Cohen, *Modular forms in Pari/GP*, arXiv:1810.00547, 2018.

[10] Best, A., Bober, J., Booker, A., Costa, E., Cremona, J., Derickx, M., Lee, M., Lowry-Duda, D., Roe, D., Sutherland, A. & Voight, J., *Computing classical modular forms*, Arithmetic Geometry, Number Theory, and Computation (2021), pp. 131–213.

[11] Bilu, Y. & Parent, P., *Serre's uniformity problem in the split Cartan case*, Ann. Of Math. (2). **173** (2011), 569–584.

[12] Bilu, Y., Parent, P. & Rebolledo, M., *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier (Grenoble) **63** (2013), 957–984.

[13] Borisov, L. & Gunnells, P., *Toric modular forms and nonvanishing of L-functions*, J. Reine Angew. Math. **539** (2001), pp. 149–165.

[14] Box, J., *Computing models for quotients of modular curves*, Res. Number Theory **7** (2021), no. 51, 34.

[15] Bröker, R., Lauter, K. & Sutherland, A., *Modular polynomials via isogeny volcanoes*, Math. Comp. **81** (2012), 1201–1231.

[16] Brunault, F. & Neururer, M., *Fourier expansions at cusps*, Ramanujan J. **53** (2020), 423–437.

[17] Kevin Buzzard, *Automorphic forms for* GL_2 *over* $\mathbf{Q}$, preprint available at https://www.ma.imperial.ac.uk/~buzzard/maths/research/notes/automorphic_forms_for_gl2_over_Q.pdf, 2008.

[18] Česnavičius, K., *Coarse base change fails for some modular curves*, Algebr. Geom. **4** (2017), 444–451.

[19] Česnavičius, K., Neururer, M. & Saha, A., *The Manin constant and the modular degree*, J. Eur. Math. Soc. **26** (2024), 573–637.

[20] Chabauty, C., *Sur les points rationnels des courbes algébriques de genre supérieur à l'unité*, C. R. Acad. Sci. Paris **212** (1941), pp. 882–885.

[21] Mingjie Chen, Kiran Kedlaya & Jun Bo Lau, *Coleman integration on modular curves*, arXiv:2401.14513, 2024.

[22] Cohen, H., *Expansions at cusps and Petersson products in Pari/GP*, Elliptic Integrals, Elliptic Functions and Modular Forms in Quantum Field Theory (2019), pp. 161–181.

[23] Cohen, H. & Strömberg, F., *Modular Forms: A Classical Approach*, Graduate Studies in Mathematics, Volume 179, 2017.

[24] Coleman, R., *Effective Chabauty*, Duke Math. J. **52** (1985), 765–770.

[25] Coleman, R. & Gross, B., *p-adic heights on curves*, Algebraic Number Theory **17** (1989), pp. 73–81.

[26] Dan J. Collins, *Numerical computation of Petersson inner products and q-expansions*, arXiv:1802.09740, 2018.

[27] Conrad, Brian, *The Shimura Construction in Weight 2*, Appendix to Kenneth A. Ribet & William A. Stein, *Lectures on Serre's Conjecture*, Math 252: Modular Abelian Varieties, University of California, Berkeley, Fall 2003. Available at .

[28] Diamond, F. & Shurman, J., *A first course in modular forms*, Springer-Verlag, New York, 2005.

[29] Dickson, M. & Neururer, M., *Products of Eisenstein series and Fourier expansions of modular forms at cusps*, J. Number Theory **188** (2018), pp. 137–164.

[30] Derickx, M., S. Kamienny, W. Stein, & M. Stoll,*Torsion Points on Elliptic Curves over Number Fields of Small Degree*, arXiv:1707.00364v1, 2017.

[31] Dokchitser, T. & Dokchitser, V., *A remark on Tate's algorithm and Kodaira types*, Acta Arith. **160** (2013), 95–100.

[32] Dupont, R., *Fast evaluation of modular functions using Newton iterations and the AGM*, Math. Comp. **80** (2011), 1823–1847.

[33] Enge, A. & Sutherland, A., *Class invariants by the CRT method*, Algorithmic Number Theory **6197** (2010), pp. 142–156.

[34] Justine Gauthier, *Fast Multipoint Evaluation on n Arbitrary Points*, MSc thesis, Simon Fraser University, 2017.

[35] Gross, B. & Zagier, D., *On singular moduli*, J. Reine Angew. Math. **355** (1985), pp. 191–220.

[36] Isaacson, Brad, *Three Imprimitive Character Sums*, Integers: Electronic Journal of Combinatorial Number Theory **21** (2021), Article A103.

[37] Nicholas M. Katz, *p-adic Properties of Modular Schemes and Modular Forms*, Modular Functions of One Variable III, edited by W. Kuyk and J.-P. Serre, Lecture Notes in Mathematics, vol. **350**, pp. 69–190, Springer Berlin, 1973.

[38] Katz, N. & Mazur, B., *Arithmetic moduli of elliptic curves*, Princeton University Press, Princeton, NJ, 1985.

[39] Khuri-Makdisi, K., *Asymptotically fast group operations on Jacobians of general curves*, Math. Comp. **76** (2007), 2213–2239.

[40] Khuri-Makdisi, K., *Moduli interpretation of Eisenstein series*, Int. J. Number Theory **8** (2012), 715–748.

[41] Khuri-Makdisi, K. & W. Raji, *Periods of Modular Forms and Identities Between Eisenstein Series*, Math. Ann. **367** (2017), pp. 165–183.

[42] Kida, M., *Galois descent and twists of an abelian variety*, Acta Arith. **73** (1995), 51–57.

[43] Kolyvagin, V. & Logachëv, D., *Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties*, Algebra I Analiz **1** (1989), 171–196.

[44] LMFDB Collaboration, *The L-functions and modular forms database*, 2025.

[45] LMFDB Collaboration, *Home page of the newform orbit class 37.2.a.b*.

[46] LMFDB Collaboration, *Home page of the newform orbit class 43.2.a.b*.

[47] Loeffler, D. & Weinstein, J., *On the computation of local components of a newform*, Math. Comp. **81** (2012), 1179–1200.

[48] Lozano-Robledo, Á., *Galois representations attached to elliptic curves with complex multiplication*, Algebra & Number Theory **16** (2022), 777–837.

[49] Mascot, N., *Moduli-friendly Eisenstein series over the p-adics and the computation of modular Galois representations*, Research in Number Theory **8** (2022), no. 48.

[50] Jeffery (user "Jeffrey"). *Regarding the derivative of the j-invariant*, Mathematics Stack Exchange, 2015.

[51] Mazur, B., *Rational points on modular curves*, Modular Functions of one Variable V (1977), pp. 107–148.

[52] Mazur, B., *Modular curves and the Eisenstein ideal (with an appendix by Mazur and M. Rapoport)*, Inst. Hautes Études Sci. Publ. Math. (1977), 33–186.

[53] McCallum, W. & Poonen, B., *The Method of Chabauty and Coleman*, Panoramas et Synthèses, Société Mathématique de France, Paris **36** (2012), 99–117.

[54] Merel, L., *Universal Fourier Expansions of Modular Forms*, In *On Artin's Conjecture for Odd 2-dimensional Representations*, Lecture Notes in Mathematics 1994, Springer, 2009, pp. 41–60.

[55] Pierre Parent, *Torsion des courbes elliptiques sur les corps cubiques*, Annales de l'Institut Fourier **50** (2000), no. 3, pp. 723–749.

[56] Poonen, B., *Computing Torsion Points on Curves*, Experiment. Math. **10** (2001), no. 3, 449–466.

[57] Rabiner, L., Schafer, R. & Rader, C., *The chirp z-transform algorithm and its application*, Bell System Tech. J. **48** (1969), pp. 1249–1292.

[58] Raum, M. & Xia, J., *All modular forms of weight 2 can be expressed by Eisenstein series*, Res. Number Theory **6** (2020), no. 32.

[59] Ribet, K., *Twists of modular forms and endomorphisms of abelian varieties*, Math. Ann. **253** (1980), 43–62.

[60] Ribet, K. A., & W. A. Stein, *Lectures on Serre's Conjectures*, IAS/Park City Mathematics Series, vol. 9, American Mathematical Society, 2001. Available online at .

[61] Ritzmann, P., *A fast numerical algorithm for the composition of power series with complex coefficients*, Theoret. Comput. Sci. **44** (1986), 1–16.

[62] Rouse, J., Sutherland, A. & Zureick-Brown, D., *ℓ-adic images of Galois for elliptic curves over* **Q** *(and an appendix with John Voight)*, Forum Math. Sigma **10** (2022), no. e62.

[63] Soumyadip Sahu, *A note on the spaces of Eisenstein series on general congruence subgroups*, arXiv:2312.10627, 2024.

[64] Schertz, R., *Complex Multiplication*, Cambridge University Press, Cambridge, 2010.

[65] Shimura, G., *Introduction to the arithmetic theory of automorphic functions*, Princeton University Press, Princeton, NJ, 1994.

[66] Shimura, G., *On the factors of the jacobian variety of a modular function field*, J. Math. Soc. Japan **25** (1973), pp. 523–544.

[67] Shimura, G., *The special values of the zeta functions associated with cusp forms*, Comm. Pure Appl. Math. **29** (1976), 783–804.

[68] Shimura, G., *On the periods of modular forms*, Math. Ann. **229** (1977), 211–221.

[69] Siksek, S., *Chabauty and the Mordell-Weil sieve*, Advances on Superelliptic Curves and their Applications **41** (2015), pp. 194–224.

[70] Silverman, J., *The Arithmetic of Elliptic Curves*, Springer, Dordrecht, 2009.

[71] Silverman, J., *Advanced topics in the arithmetic of elliptic curves*, Springer-Verlag, New York, 1994.

[72] Andrew Sutherland, *Modular polynomials for the classpoly software package*, available at https://math.mit.edu/~drew/SmallModPolys.html.

[73] Westerholt-Raum, M., *Products of vector valued Eisenstein series*, Forum Math. **29** (2017), 157–186.

[74] Chris Xu, *Rigorous expansions of modular forms at CM points, I: Denominators*, preprint available at https://chrisxudoesmath.com/papers/powerseries1.pdf, 2025.

[75] Chris Xu, `model-free-chabauty` software package, available at https://github.com/chrisxu3/model-free-chabauty, 2024.

[76] David Zywina, *Computing actions on cusp forms*, arXiv:2001.07270, 2021.

[77] David Zywina, *Explicit open images for elliptic curves over* **Q**, arXiv:2001.07270, 2024.

[78] David Zywina, `OpenImageQ` software package, available at https://github.com/davidzywina/OpenImage, 2024.