Computational aspects of modular parametrizations of elliptic curves

Hao Chen

A dissertation submitted in partial fulfillment of the requirements for the degree of

Doctor of Philosophy

University of Washington

2011-2016

Reading Committee:

William Arthur Stein, Chair

First committee member

Next committee member

etc

Program Authorized to Offer Degree:
UW Mathematics

University of Washington

Abstract

Computational aspects of modular parametrizations
of elliptic curves

Hao Chen

Chair of the Supervisory Committee:
Professor William Arthur Stein
Department of Mathematics

We investigate computational problems related to modular parametrizations of elliptic curves defined over $\mathbb{Q}$. Chapter 1 covers the background materials. In Chapter 2, we develop algorithms to compute the Mazur Swinnerton-Dyer critical subgroup of elliptic curves, and verify that for all elliptic curves of rank two and conductor < 1000, the critical subgroup is torsion. In Chapter 3, we develop algorithms to compute Fourier expansions of $\Gamma_0(N)$ newforms at cusps other than the cusp at infinity. In Chapter 4 we study properties of Chow-Heegner points. We proved the index of Chow-Heegner points are always divisible by two when the conductor N has many prime divisors, and we develop algebraic algorithms to compute them.

TABLE OF CONTENTS

Page

Chapter 1

BACKGROUND

1.0.1 Algebraic curves

Let k be a field. A *nonsingular projective curve* X/k is an algebraic variety $X \subset \mathbb{P}^n$ such that $\dim(X) = 1$, X is smooth, and it has defining equations with coefficients in k. We'll abbreviate it with 'curve'.

For every curve X there is a nonnegative integer $g(X)$ called its *genus*, and a field $k(X)$ of transcendence degree 1 over k, called the *function field* of X. We have the following

Fact 1.0.1. *If x is a non constant rational function, then* $[k(X) : k(x)] = \deg x$.

We let $K^1(X)$ denote the group of meromorphic differentials on X.

Let $\varphi : X \to Y$ be a finite morphism between curves, then there exists a positive integer $d = \deg(\varphi)$ such that for all but finitely many points $y \in Y, \varphi^{-1}(y)$ consists of d distinct points.

Definition 1.0.2. A point $x \in X$ is *ramified* under φ if $|\varphi^{-1}(\varphi(x))| < d$.

Fix the morphism φ. For each $x \in X$ there is a positive integer $e_\varphi(x)$ called the *ramification index of φ at x*, and x is ramified under φ if and only if $e_\varphi(x) > 1$.

Let $\bar{k}$ be a fixed algebraic closure of k. A *divisor* on a curve X is a formal sum $D = \sum_{z\in X(\bar{k})} n_z[z]$ where $n_z = 0$ for all but finitely many $z \in X$. The set of divisors on X form a free abelian group, which we denoe by $\mathrm{div}(X)$.

The Galois group $G_k := \mathrm{Gal}(\bar{k}/k)$ acts on the group $\mathrm{div}(X)$ of divisors by $\sigma(\sum n_z[z]) = \sum n_z[\sigma(z)]$. We say a divisor $D \in \mathrm{div}(X)$ is *defined over k* if it is invariant under this action. The subgroup of G_k-invariant divisors is denoted by $\mathrm{div}_k(X)$.

Definition 1.0.3. The *ramification divisor* of φ is $R_\varphi = \sum_{p \in X}(e_\varphi(p) - 1)[p]$.

If the map φ is defined over k, then the ramification divisor R_φ is defined over k.

Theorem 1.0.4. *(Riemann-Hurwitz formula). For any nonzero differential* $\omega \in K^1(X)$

$$\operatorname{div}(\varphi^*(\omega)) = \varphi^*(\operatorname{div}(\omega)) + R_\varphi.$$

Taking degrees on both sides, we obtain the following formula on the degree of the ramification divisor R_φ, which is sometimes also referred to as the Riemann-Hurwitz formula.

Corollary 1.0.5. $2g(X) - 2 = \deg(\varphi) \cdot (2g(Y) - 2) + \deg R_\varphi$.

1.1 Elliptic curves

Let k be a field. An *elliptic curve* defined over k is the projective closure in $\mathbb{P}^2$ of an affine curve given by the Weierstrass equation $y^2 = x^3 + Ax + B$ with $A, B \in k$ and $4A^3 + 27B^2 \neq 0$. Alternatively, an elliptic curve over k is a nonsingular projective over k of genus one with a distinguished k-rational point $\mathcal{O} \in E(k)$.

Let E be an elliptic curve defined over a field k. It turns out that E also has the structure of an algebraic group. When $k = \mathbb{R}$, the group addition can be described as follows: suppose $P, Q \in E(\mathbb{R})$, and let R be the third point of intersection of the line PQ with E. Then one declares $P + Q = -R$. It turns out that this group law is algebraic, commutative and associative. Therefore, an elliptic curve over k is also an abelian variety over k of dimension 1. In particular, for any extension k'/k, the set $E(k')$ is an abelian group, with the identity element being $\mathcal{O}$.

Pinning down the structure of $E(k)$ is one of the central questions in 20th century algebraic number theory. We recall the famous Mordell-Weil theorem:

Theorem 1.1.1 (Mordell-Weil)**.** *If K is a number field and E is an elliptic curve over K. Then*

$$E(K) \cong \mathbb{Z}^r \times T$$

for some integer $r \geq 0$ and some finite abelian group T.

The integer r in the above theorem is called the (algebraic) *rank* of $E(K)$. It is not known whether the rank of elliptic curves over $\mathbb{Q}$ are bounded from above.

1.1.1 Elliptic curves as complex torus

Every elliptic curve over $\mathbb{C}$ is isomorphic to a complex torus $\mathbb{C}/\Lambda$, where Λ is a lattice in $\mathbb{C}$. Two lattices give rise to isomorphic elliptic curves if and only if they are homothetic, i.e., there exists a complex number α s.t. $\alpha\Lambda_1 = \Lambda_2$. The addition law on $\mathbb{C}/\Lambda$ is simply induced by the addition on $\mathbb{C}$. If $E = \mathbb{C}/\Lambda$, then one possible algebraic model of E is

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$$

where

$$g_2(\Lambda) = 60 \sum_{x\in\Lambda, x\neq 0} \frac{1}{|x|^4}$$

and

$$g_3(\Lambda) = 140 \sum_{x\in\Lambda, x\neq 0} \frac{1}{|x|^6}.$$

1.1.2 Reduction

For ease of exposition, we restrict our attention to the case $k = \mathbb{Q}$. Let E be an elliptic curve defined over $\mathbb{Q}$. For each prime p, there exists a reduced curve $\tilde{E}$ defined over the finite field $\mathbb{F}_p$, which is either an elliptic curve or a curve of genus zero. If $\tilde{E}$ is an elliptic curve, then we say that p is a prime of *good reduction*, otherwise, we say p is of *bad reduction*. Suppose p is a prime of good reduction, then we have a reduction map $\rho_p : E \to \tilde{E}$. Also, let N_p denote the cardinarlity of the finite group $\tilde{E}(\mathbb{F}_p)$, and let

$$a_p = p + 1 - N_p.$$

The theorem of Hasse gives an upper bound for the absolute value of a_p.

Theorem 1.1.2 (Hasse). *Let $E/\mathbb{Q}$ be an elliptic curve, and p be a prime of good reduction. Then $|a_p| \leq 2\sqrt{p}$.*

For a prime p of good reduction, consider the polynomial $f_p(x) = x^2 - a_p x + p$. Hasse's theorem implies that $f_p(x) = (x - \alpha_p)(x - \beta_p)$, where α_p, β_p is a pair of complex conjugates with absolute value $\sqrt{p}$. It is a fact that for any finite extension $\mathbb{F}_{p^r}$ of $\mathbb{F}_p$, we have the following formula

$$\#\tilde{E}(\mathbb{F}_{p^r}) = p^r + 1 - \alpha_p^r - \beta_p^r.$$

1.1.3 Conductor

Let $E/\mathbb{Q}$ be an elliptic curve. Then there is a positive integer N, called the conductor of E, with the property that N is divisible by the primes of bad reduction. When p is a prime of bad reduction, there is a procedure to determine the highest power of p dividing N, which we omit here. We only mention that when $p \geq 5$, we have $\mathrm{ord}_p(N) \leq 2$; when $p = 3, \mathrm{ord}_p(N) \leq 5$; when $p = 2, \mathrm{ord}_p(N) \leq 8$.

1.1.4 L-function and analytic rank

Suppose E is an elliptic curve over $\mathbb{Q}$. For each prime number p, we define $a_p(E)$ via the following formula:

$$a_p(E) = \begin{cases} p + 1 - |\tilde{E}(\mathbb{F}_p| & \text{good reduction} \\ 1 & \text{split multiplicative reduction} \\ -1 & \text{nonsplit multiplicative reduction} \\ 0 & \text{otherwise} \end{cases}$$

The local L-factor of E at p is $L_p(E,T) = 1 - a_p T + pT^2$ if p is of good reduction and $1 - a_p T$ otherwise. Finally, the L-function attached to E is defined as the following Euler product

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

We can also write $L(E,s)$ as a Dirichlet series

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

The series defining $L(E,s)$ converges for $\Re(s) > \frac{3}{2}$. It turns out (as a consequence of the celebrated modularity theorem) that $L(E,s)$ can be analytically continued to an entire function on the complex plane. The order of vanishing of $L(E,s)$ at $s=1$ is called the analytic rank of E. The rank part of the famous Birch and Swinnerton-Dyer (BSD) conjecture states that the analytic rank is equal to the algebraic rank, i.e.,

$$\operatorname{rank}(E(\mathbb{Q})) = \operatorname{ord}_{s=1} L(E,s).$$

As of now this conjecture is still open for $\operatorname{ord}_{s=1} L(E,s) > 1$.

1.2 Modular curves

The *modular group* $SL_2(\mathbb{Z})$ is the group of integer matrices with determinant 1. For each integer $N > 1$, consider the subgroup

$$\Gamma_0(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : N \mid c \right\}$$

The *modular curve* $X_0(N)$ is defined by $X_0(N) = \Gamma_0(N)\backslash(H \cup \mathbb{P}^1(\mathbb{Q}))$. The open modular curve is $Y_0(N) = \Gamma_0(N)\backslash H$. The complex points on $Y_0(N)$ "parametrizes" pairs (E,C), where $E/\mathbb{C}$ is an elliptic curve and $C \subseteq E(\mathbb{C})$ is a cyclic subgroup of order N. The equivalence classes of $\mathbb{P}^1(\mathbb{Q})$ under $\Gamma_0(N)$ are called *cusps*. The set of cusps is finite.

Similarly, we can define

$$\Gamma_1(N) = \left\{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z}) : a \equiv d \equiv 1 \mod N, c \equiv 0 \mod N \right\}$$

The corresponding modular curve is called $X_1(N)$. It is easy to verify that $\Gamma_1(N)$ is a normal subgroup of $\Gamma_0(N)$ with the quotient isomorphic to $(\mathbb{Z}/N\mathbb{Z})^*$. Hence there is a canonical projection $\pi : X_1(N) \to X_0(N)$

It turns out that $X_0(N)$ has the structure of a nonsingular projective algebraic curve. The genus of $X_0(N)$ is given by the following genus formula (see, for example, DS05).

$$g(X_0(N)) = 1 + \frac{d}{12} - \frac{\epsilon_2}{3} - \frac{\epsilon_3}{4} - \frac{\epsilon_\infty}{2}.$$

Here d is the index of $\Gamma_0(N)$ in $SL_2(\mathbb{Z})$, and ϵ_2 and ϵ_3 denote the number of elliptic points of period 2 and 3 in $X_0(N)$, and ϵ_∞ is the number of cusps. All these values can be explicitly computed. For example, we have

$$d = |SL_2(\mathbb{Z})/\Gamma_0(N)| = N \prod_{p|N} (1 + 1/p).$$

1.2.1 Function fields of modular curves

The j-invariant

$$j(q) = q^{-1} + 744 + 196884q + \cdots$$

(where $q = e^{2\pi i z}$) is a rational function on $X_0(1) \cong \mathbb{P}^1$. In fact, the function fields of $X_0(1)$ is generated by j: i.e., we have $\mathbb{Q}(X_0(1)) = \mathbb{Q}(j)$. Via pulling back, we can view j as a rational function on $X_0(N)$.

Let $j_N(z) := j(Nz)$. Then it turns out that j_N is a rational function on $X_0(N)$. Moreover, we have

$$\mathbb{Q}(X_0(N)) = \mathbb{Q}(j, j_N).$$

1.3 Modular forms

Recall that $\mathcal{H} = \{z \in \mathbb{C} : \Im(z) > 0\}$ is the complex upper half plane. For each integer k, the weight-k action of $SL_2(\mathbb{Z})$ on functions $f : H \to \mathbb{C}$ is defined as follows: suppose $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(\mathbb{Q})$, define

$$f|[g]_k(z) = \det(g)^{k/2}(cz + d)^{-k} f(gz).$$

We will omit the k in the subscript when the value of k is clear from the context.

Definition 1.3.1. Let $N \geq 1$ and k be integers. A *modular form* of weight k and level N is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ satisfying

(1) $f|[g]_k = f$ for all $g \in \Gamma_0(N)$.

(2) f can be holomorphically extended to $\mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$.

A modular form f is a *cusp form* if f vanishes at all cusps. For the precise definition of vanishing at cusps, see [DS06, I.2]. By definition, if f is a modular form, then f is 1-periodic: $f(z+1) = f(z)$. It has a q-expansion

$$f(q) = \sum_{n\geq 0} a_n q^n$$

where $q = e^{2\pi i z}$.

The vector space $S_k(\Gamma_0(N))$ of cusp forms of weight k and level N is finite dimensional. In particular, when $k = 2$, we have an isomorphism

$$S_2(\Gamma_0(N)) \cong \Omega^1(X_0(N)(\mathbb{C})),$$

which sends a cusp form f to the differential $\omega_f = f(z)dz$. As a consequence, $\dim_{\mathbb{C}} S_2(\Gamma_0(N)) = g(X_0(N))$.

We are going to be interested in a subset of cusp forms on $\Gamma_0(N)$ called *newforms*In particular, all cusp forms attached to elliptic curves defined over $\mathbb{Q}$ are newforms.

For each positive integer N, we have an elementary abelian 2-group $W \subseteq Aut_{\mathbb{Q}}(X_0(N))$, which we call the *Atkin-Lehner Group*, with generators $\{w_p\}_{p|N}$. The non-trivial elements of W are called *Atkin-Lehner* involutions. They act on $S_k(\Gamma_0(N))$ by invertible linear transformations. Any newform f is an eigenvector of every $w \in W$ with eigenvalue ± 1, i.e., $f|w = \pm f$. In particular, if $E/\mathbb{Q}$ is an elliptic curve and f is the modular form attached to E, then we have $f|w_N = (-1)^{r_{an}(E)} f$ where $w_N = \prod_{p|N} w_p$ is also called the Fricke involution, and $r_{an}(E)$ is the analytic rank of E we will define later.

1.3.1 Hecke operators

Let p be a prime, the Hecke operator T_p acts on $S_k(\Gamma_1(N))$ as follows. Write the double coset $\Gamma_1(N) \left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right) \Gamma_1(N)$ as $\sum_{i=1}^n \Gamma_1(N)\beta_i$. Then we define

$$T_p f = \sum_{i=1}^n f|[\beta_i]_k.$$

For $d \in (\mathbb{Z}/N\mathbb{Z})^*$, the diamond operators $\langle d \rangle$ is defined as follows. Choose any matrix $\gamma_d \in \Gamma_0(N)$ with lower entry d and

$$\langle d \rangle f := f|[\gamma_d]_k.$$

We have the following decomposition

$$S_k(\Gamma_1(N) = \oplus_{\chi:(\mathbb{Z}/N\mathbb{Z})^* \to \mathbb{C}^*} S_k(\Gamma_1(N), \chi)$$

where $S_k(\Gamma_1(N), \chi)$ is the subspace of $S_k(\Gamma_1(N))$ on which the diamond operators acts via the character χ. In particular, we have $S_k(\Gamma_0(N)) = S_k(\Gamma_1(N), \chi_0)$. Note that the T_p operators commute with the diamond operators. Hence $S_k(\Gamma_0(N))$ is stable under the T_p.

Moreover, $\{T_p : p \nmid N\}$ form a commuting family of normal operators. Hence they can be simultaneously diagonalized. So $S_k(\Gamma_1(N))$ has a basis consisting of simultaneous eigenforms.

1.3.2 Newforms

The Petersson inner product on two cusp forms on some congruence group Γ is

$$\langle f, g \rangle = \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(z) g(\bar{z}) \Im(z)^k d\mu(z)$$

where μ is the hyperbolic measure on the upper half plane.

Suppose we have two levels $M \mid N$. Then for any divisor d of N/M, there is a degeneracy map

$$\alpha_d : S_k(M) \to S_k(N) : f \mapsto f|[\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)]_k.$$

Definition 1.3.2. The old subspace of $S_k(N)$ is the span of $\alpha_d(S_k(M))$ where M, d range over all divisors of N s.t. $Md \mid N$. The new subspace of $S_k(N)$ is the ortogonal complement of the old subspace under the Petersson inner product.

The new subspace of $S_k(N)$ has a basis consisting of simultaneous eigenforms under T_p for all primes p. Given such an eigenform $f = \sum a_n q^n$, we could scale it so that $a_1 = 1$. The result is called a *newform*.

1.3.3 The modularity theorem

The famous modularity theorem, first proved for semi-stable elliptic curves over $\mathbb{Q}$ by Andrew Wiles and Richard Taylor in 1995, and proved for all elliptic curves over $\mathbb{Q}$ in 2001 by Breuil, Conrad, Diamond, and Taylor [BCDT01]), is a crucial achievement in number theory, which leads to the proof of Fermat's last theorem.

The modularity theorem has many equivalent forms. Here we state one form of the theorem.

Theorem 1.3.3 ([BCDT01])**.** *For every elliptic curve $E/\mathbb{Q}$ with conductor N there exists a surjective morphism*

$$\varphi : X_0(N) \to E$$

defined over $\mathbb{Q}$. Moreover, $\varphi^*(\omega_E) = c \cdot 2\pi i f_E(z)dz$ where f_E is a newform of weight 2 and level N, called the modular form attached to E*, and $c \in \mathbb{C}^\times$.*

Let ω_f denote the differential $f(z)dz \in S_2(\Gamma_0(N))$. Let Λ be the period lattice of E, with an isomorphism $\iota : E \cong \mathbb{C}/\Lambda$. The composition $\iota \circ \varphi : X_0(N) \to \mathbb{C}/\Lambda$ can be written as an integral:

$$[z] \mapsto \int_z^\infty \omega_f \pmod{\Lambda}.$$

1.4 Automorphic representation attached to newforms

Let f be a cuspidal newform for $\Gamma_1(N)$ with weight $k \geq 2$ and character ϵ. Let $\mathbb{A}_\mathbb{Q}$ be group the ad e les over $\mathbb{Q}$. Then f corresponds to an automorphic representation of $GL_2(\mathbb{A}_\mathbb{Q})$, denoted by π_f. It turns out that π_f decomposes as a restricted tensor product over places v of $\mathbb{Q}$:

$$\pi_f = \prod_v \pi_{f,v},$$

where each $\pi_{f,v}$ is an irreducible admissible representation of $GL_2(\mathbb{Q}_v)$. The component $\pi_{f,\infty}$ is determined by the weight k; when $p \nmid N$, the p-component $\pi_{f,p}$ is determined by k, ϵ, and $a_p(f)$. The problem of determining the isomorphism class of $\pi_{f,p}$ when $p \mid N$

is more subtle and is solved by Loeffler and Weinstein in [fixme]. Their algorithm uses modular symbols and is now implemented in Sage. In section (fixme) of this thesis, we will take a numerical perspective and demonstrate how the pseudo-eigenvalues of Atkin-Lehner operators on newforms give information on the local components $\pi_{f,p}$ when $p \mid N$.

Chapter 2

COMPUTING THE MAZUR SWINNERTON-DYER CRITICAL SUBGROUP OF ELLIPTIC CURVES

2.1 Introduction

Let E be an elliptic curve over $\mathbb{Q}$ and let $L(E,s)$ be the L-function of E. The rank part of the Birch and Swinnerton-Dyer (BSD) conjecture states that

$$\operatorname{rank}(E(\mathbb{Q})) = \operatorname{ord}_{s=1} L(E,s).$$

The right hand side is called the *analytic rank of* E, and is denoted by $r_{\text{an}}(E)$. The left hand side is called the *algebraic rank of* E. The rank part of the BSD conjecture is still open when $r_{\text{an}}(E) > 1$, and its proof for the case $r_{\text{an}}(E) = 1$ uses the *Gross-Zagier formula*, which relates the value of certain L-functions to heights of Heegner points.

Let N denote the conductor of E. The modular curve $X_0(N)$ is a nonsingular projective curve defined over $\mathbb{Q}$. Since E is modular(Breuil, Conrad, Diamond, and Taylor [BCDT01]), there is a surjective morphism $\varphi : X_0(N) \to E$ defined over $\mathbb{Q}$. Let ω_E be the invariant differential on E and let $\omega = \varphi^*(\omega_E)$. Then ω is a holomorphic differential on $X_0(N)$ and we have $\omega = cf(z)dz$, where f is the normalized newform attached to E and c is a nonzero constant. In the rest of the paper, we fix the following notations: the elliptic curve E, the conductor N, the morphism φ, and the differential ω. Let R_φ be the ramification divisor of φ.

Definition 2.1.1 (Mazur and Swinnerton-Dyer [MSD74])**.** The *critical subgroup* of E is

$$E_{\text{crit}}(\mathbb{Q}) = \langle \operatorname{tr}(\varphi([z])) : [z] \in \operatorname{supp} R_\varphi \rangle,$$

where $\operatorname{tr}(P) = \sum_{\sigma:\mathbb{Q}(P)\to\bar{\mathbb{Q}}} P^\sigma$.

Since the divisor R_φ is defined over $\mathbb{Q}$, every point $[z]$ in its support is in $X_0(N)(\overline{\mathbb{Q}})$, hence $\varphi([z]) \in E(\overline{\mathbb{Q}})$, justifying the trace operation. The group $E_{\mathrm{crit}}(\mathbb{Q})$ is a subgroup of $E(\mathbb{Q})$. Observe that $R_\varphi = \mathrm{div}(\omega)$, thus $\deg R_\varphi = 2g(X_0(N))-2$. In the rest of the paper, we use the notation $\mathrm{div}(\omega)$ in place of the ramification divisor R_φ. In addition, we will assume E is an optimal elliptic curve, so φ is unique up to sign. This justifies the absence of φ in the notation $E_{\mathrm{crit}}(\mathbb{Q})$.

Recall the construction of *Heegner points*: for an imaginary quadratic order $\mathcal{O} = \mathcal{O}_d$ of discriminant $d < 0$, let $H_d(x)$ denote its *Hilbert class polynomial.*

Definition 2.1.2. A point $[z] \in X_0(N)$ is a *"generalized Heegner point"* if there exists a negative discriminant d s.t. $H_d(j(z)) = H_d(j(Nz)) = 0$. If in addition we have $(d, 2N) = 1$, then $[z]$ is a *Heegner point.*

For any discriminant d, let E_d denote the quadratic twist of E by d. Then the Gross-Zagier formula in [GZ86] together with a non-vanishing theorem for $L(E_d, 1)$ (see, for example, Bump, Friedberg, and Hoffstein [BFH90]) implies the following

Theorem 2.1.3. *(1) If* $r_{\mathrm{an}}(E) = 1$*, then there exists a Heegner point* $[z]$ *on* $X_0(N)$ *such that* $\mathrm{tr}(\varphi([z]))$ *has infinite order in* $E(\mathbb{Q})$*.*
(2) If $r_{\mathrm{an}}(E) \geq 2$*, then* $\mathrm{tr}(\varphi([z])) \in E(\mathbb{Q})_{\mathrm{tors}}$ *for every "generalized Heegner point"* $[z]$ *on* $X_0(N)$*.*

The first case in the above theorem is essential to the proof of rank BSD conjecture for $r_{\mathrm{an}}(E) = 1$. We observe that the defining generators of the critical subgroup also take the form $\mathrm{tr}(\varphi([z]))$. Then a natural question is:

Question 2.1.4. *Does there exist an elliptic curve* E *defined over* $\mathbb{Q}$ *such that* $r_{\mathrm{an}}(E) \geq 2$ *and* $\mathrm{rank}(E_{\mathrm{crit}}(\mathbb{Q})) > 0$*?*

We will show that the answer is negative for all elliptic curves with conductor $N < 1000$, using *critical polynomials* attached to elliptic curves.

2.1.1 Main results

Let E, N, φ, and ω be as defined previously, and write $\operatorname{div}(\omega) = \sum_{[z]\in X_0(N)} n_z[z]$. Let j denote the j-invariant function.

Definition 2.1.5. The *critical j-polynomial* of E is

$$F_{E,j}(x) = \prod_{z\in \operatorname{supp}\operatorname{div}(\omega), j(z)\neq\infty} (x - j(z))^{n_z}.$$

Because $\operatorname{div}(\omega)$ is defined over $\mathbb{Q}$ and has degree $2g(X_0(N)) - 2$, we have $F_{E,j}(x) \in \mathbb{Q}[x]$ and $\deg F_{E,j} \leq 2g(X_0(N)) - 2$, where equality holds if $\operatorname{div}(\omega)$ does not contain cusps. For any non-constant modular function $h \in \mathbb{Q}(X_0(N))$, the *critical h-polynomial* of E is defined similarly, by replacing j with h.

In this paper we give two algorithms *Poly Relation* and *Poly Relation-YP* to compute critical polynomials. The algorithm *Poly Relation* computes the critical j-polynomial $F_{E,j}$, and the algorithm *Poly Relation* computes the critical h-polynomial $F_{E,h}$ for some modular function h chosen within the algorithm. We then relate the critical polynomials to the critical subgroup via the following theorem. Recall that $H_d(x)$ denotes the Hilbert class polynomial associated to a negative discriminant d. We prove the following theorem.

Theorem 2.1.6. *Suppose $r_{\mathrm{an}}(E) \geq 2$, and assume at least one of the following holds:*
(1) $F_{E,h}$ is irreducible for some non-constant function $h \in \mathbb{Q}(X_0(N))$.
(2) There exist negative discriminants D_k and positive integers s_k for $1 \leq k \leq m$ with $\mathbb{Q}(\sqrt{D_k}) \neq \mathbb{Q}(\sqrt{D_{k'}})$ for all $k \neq k'$, and an irreducible polynomial $F_0 \in \mathbb{Q}[x]$, such that

$$F_{E,j} = \prod_{k=1}^{m} H_{D_k}^{s_k} \cdot F_0.$$

Then $\operatorname{rank}(E_{\mathrm{crit}}(\mathbb{Q})) = 0$.

Combining Theorem 2.1.6 with our computation of critical polynomials, we verified the main result of this chapter stated in the following corollary.

Corollary 2.1.7. *For all elliptic curves E of analytic rank 2 and conductor N smaller than 1000, the rank of $E_{\mathrm{crit}}(\mathbb{Q})$ is zero.*

2.2 The norm method

Let E be an elliptic curve over $\mathbb{Q}$ with square free conductor N, and let f be the associated newform. Taking $A_1, \cdots, A_n$ to be a set of representatives for $\Gamma_0(N)\backslash SL_2(\mathbb{Z})$, we define

Definition 2.2.1. The *norm* of f is the product

$$\mathrm{Norm}_N(f) = \prod_{i=1}^{n} f|[A_i]_2$$

By construction, we know that $\mathrm{Norm}_N(f)$ is a modular form of weight $2n$ on $SL_2(\mathbb{Z})$.

Remark 2.2.2. In practice we normalise $\mathrm{Norm}_N(f)$ so that its q-expansion has leading coefficient 1.

We recall from [DS06, III.7] the formulae for the number of *elliptic points* on $\Gamma_0(N)$ of order 2 and 3:

$$\epsilon_2(N) = \prod_{p|N}\left(1 + \left(\frac{1}{p}\right)\right), \ \epsilon_3(N) = \prod_{p|N}\left(1 + \left(\frac{-3}{p}\right)\right).$$

Let E_4, E_6 be the *Eisenstein series* of level 1 weight 4 and 6, respectively. Let Δ be the *discriminant modular form*, which is a cusp form of level 1 and weight 12.

Theorem 2.2.3. *If*

$$F_f(q) = \frac{\mathrm{Norm}_N(f)(q)}{\Delta^A E_4^B E_6^C}$$

where

$$B = \epsilon_3(N)k, \quad C = \frac{\epsilon_2(N)k}{2}, \quad \textit{and } A = \frac{k[SL_2(\mathbb{Z}) : \Gamma_0(N)] - 4B - 6C}{12}.$$

Then $F_{E,j}(j(q)) = F_f(q)$.

If we can compute $\mathrm{Norm}_N(f)$, we will have an algorithm to compute $F_{E,j}(x)$ by 'cancelling the poles' as done in [AO03]. We are going to compute the q-expansion of $\mathrm{Norm}_N(f)$ when N is square free. First, we deal with the case when $N = p$ is prime. Following [AO03], we define

Definition 2.2.4. For any holomorphic function $f : H \to \mathbb{C}$

$$\mathfrak{N}_p(f) = f \cdot \prod_{i=0}^{p-1} f\left(\frac{z+i}{p}\right).$$

Lemma 2.2.5. *[AO03] Let f be a newform of prime level p, then* $\mathrm{Norm}_p(f) = \mathfrak{N}_p(f)$.

This lemma allows us to compute the q-expansion of $\mathfrak{N}_p(f)$ from the q-expansion of f. A slight generalization of Lemma 2.2.5 yields

Lemma 2.2.6. *(C.) If N is square free with prime factorization $N = p_1 \cdots p_n$ then*

$$\mathrm{Norm}_N(f) = \mathfrak{N}_{p_1} \circ \mathfrak{N}_{p_2} \circ \cdots \mathfrak{N}_{p_n}(f).$$

The key idea of the proof is that when N is square free, the coset representatives of $\Gamma_0(N)\backslash SL_2(\mathbb{Z})$ have a simple description. To be precise, we state a lemma.

Lemma 2.2.7. *Let p, M be positive integers with p prime,$(p, M) = 1$. Consider the matrices*

$$\alpha_i = \left(\begin{smallmatrix} 1 & 0 \\ iM & 1 \end{smallmatrix}\right),\ 0 \le i \le p-1, \alpha_p = \left(\begin{smallmatrix} 1 & (mp-1)/M \\ M & mp \end{smallmatrix}\right),$$

where m is any integer such that $mp \equiv 1 \pmod{M}$. Then

$$\Gamma_0(pM)\backslash\Gamma_0(M) = \bigcup_{i=0}^{p-1} \Gamma_0(pM)\alpha_i.$$

The proof of Lemma 2.2.7 is omitted. Note that it is a special case of [DS06, III, Ex 3.7.7]).

Proof of Lemma 2.2.6: We use induction on the number of prime divisors $\sigma(N)$ of N. The case $\sigma(N) = 1$ is covered by Lemma 2.2.5. For the inductive step, choose any prime $p \mid N$ and write $N = pM$. Let $\{\beta_j\}$ be a set of coset representatives for $\Gamma_0(M)\backslash SL_2(\mathbb{Z})$. By Lemma 2.2.7, if $\alpha_i = \left(\begin{smallmatrix} 1 & 0 \\ iM & 1 \end{smallmatrix}\right)$, then

$$\mathrm{Norm}_N(f) = \sum_{i,j} f|[\beta_j][\alpha_i] = \sum_i \mathrm{Norm}_M(f)|[\alpha_i].$$

We are going to show $SL_2(\mathbb{Z}) = \cup\Gamma_0(p)\alpha_i$. This can be seen by direct calculation: first, $\left(\begin{smallmatrix} 1 & 0 \\ iM & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ jM & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} * & * \\ (i-j)M & 1 \end{smallmatrix}\right)$; second, $\left(\begin{smallmatrix} 1 & (mp-1)/M \\ M & mp \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ iM & 1 \end{smallmatrix}\right)^{-1} = \left(\begin{smallmatrix} * & * \\ M(1-mpi) & * \end{smallmatrix}\right)$. Therefore we have

$$\mathrm{Norm}_N(f) = \mathrm{Norm}_p(\mathrm{Norm}_M(f)).$$

Using the inductive hypothesis $\mathrm{Norm}_M(f) = \prod_{p|M} \mathfrak{N}_p(f)$, we conclude that $\mathrm{Norm}_N(f) = \prod_{p|N} \mathfrak{N}_p(f)$. The proof is complete.

Now we can describe our algorithm to compute $F_{E,j}$ when the conductor of E is square free.

Algorithm 1 Norm method to compute $F_{E,j}$ when N_E is square free.

Input: E = Elliptic curve over $\mathbb{Q}$ with conductor N.

Output: The critical j-polynomial $F_{E,j}(x)$.

1: Use Lemma?, compute the q-expansion of $\mathrm{Norm}_N(f)$.
2: Use Theorem? to compute $F_f(q)$. Normalize $F_f(q)$ so that it has leading coefficient 1.
3: Set $n \Leftarrow -\mathrm{ord}_q F_f(q)$. Compute q-expansion of j to precision $2n$.
4: **while** $n >= 0$ **do**
5: $\quad a_n \Leftarrow q^{-n}$ coefficient $of F_f$.
6: $\quad F_f \Leftarrow F_f - a_n j^n$.
7: $\quad n \Leftarrow n - 1$.
8: **end while**
9: Output $F_{E,j}(x) = \sum_{i=0}^{n} a_i x^i$.

2.3 The algorithm Poly relation

Let $C/\mathbb{Q}$ be a curve. For a rational function $r \in \mathbb{Q}(C)$, let $\mathrm{div}_0(r)$ denote its divisor of zeros, and define $\deg r = \deg(\mathrm{div}_0(r))$.

Definition 2.3.1. Let r, u be two non-constant rational functions on C. A *minimal polynomial relation between* r *and* u is an irreducible polynomial $P(x, y) \in \mathbb{Q}[x, y]$ such that

$P(r,u)=0$ and $deg_x(P)\le \deg u, \deg_y(P)\le \deg r$.

Minimal polynomial relation always exists and is unique up to scalar multiplication. Write $\operatorname{div}(r)=\sum_{[z]\in X_0(N)} n_z[z]$ and $P(x,y)=f_n(y)x^n+\cdots+f_1(y)x+f_0(y)$. We will prove that

Proposition 2.3.2. *If $\mathbb{Q}(C)=\mathbb{Q}(r,u)$ and $\gcd(f_0(y),f_n(y))=1$, then there is a constant $c\neq 0$ s.t.*

$$f_0(y)=c\prod_{z\in\operatorname{div}_0(r)\setminus\operatorname{div}_\infty(u)}(y-u(z))^{n_z}.$$

Proof. Dividing $P(x,y)$ by $f_n(y)$, we get $x^n+\cdots+\frac{f_0(x)}{f_n(y)}$, which is a minimal polynomial of r over $\mathbb{Q}(u)$. So $\operatorname{Norm}_{\mathbb{Q}(r,u)/\mathbb{Q}(u)}(r)=\frac{f_0(u)}{f_n(u)}$. The rest of the proof uses a fact on extensions of valuations(see, for example, [Stea, Theorem 17.2.2]), which we now quote.

Lemma 2.3.3. *Suppose v is a nontrivial valuation on a field K and let L be a finite extension of K. Then for any $a\in L$,*

$$\sum_{1\le j\le J} w_j(a)=v(\operatorname{Norm}_{L/K}(a)),$$

where the w_j are normalized valuations equivalent to extensions of v to L.

We continue with the proof. For any $z_0\in C$ such that $u(z_0)\neq\infty$, consider the valuation $v=\operatorname{ord}_{(u-u(z_0))}$ on $\mathbb{Q}(u)$. The set of extensions of v to $\mathbb{Q}(C)=\mathbb{Q}(r,u)$ is in bijection with $\{z\in C: u(z)=u(z_0)\}$. Take $a=r$ and apply Lemma 2.3.3, we obtain

$$\sum_{z:u(z)=u(z_0)}\operatorname{ord}_z(r)=\operatorname{ord}_{u-u(z_0)}\frac{f_0(u)}{f_n(u)}.$$

Combining the identities for all $z_0\in C\setminus\operatorname{div}_\infty(u)$, we have for some constant c,

$$\prod_{z\in\operatorname{div}(r):u(z)\neq\infty}(y-u(z))^{n_z}=c\cdot\frac{f_0(y)}{f_n(y)}.$$

If $r(z)=0$, then the condition $\gcd(f_0(y),f_n(y))=1$ implies that $f_0(u(z))=0$ and $f_n(u(z))\neq 0$. Therefore, since $\gcd(f_0,f_n)=1$, we must have

$$f_0(y)=c\prod_{z\in\operatorname{div}_0(r)\setminus\operatorname{div}_\infty(u)}(y-u(z))^{n_z}.$$

This completes the proof. $\square$

For completeness we also deal with the case where $u(z) = \infty$, which was left out in the above proof. The corresponding valuation on $\mathbb{Q}(u)$ is ord_∞ defined by $\mathrm{ord}_\infty(g/h) = \deg g - \deg h$ for $0 \neq g, h \in \mathbb{Q}[u]$. We derive that

$$\sum_{z:u(z)=\infty} \mathrm{ord}_z(r) = \deg f_n - \deg f_0.$$

Next we apply Proposition 2.3.2 to the computation of $F_{E,j}$. In the rest of the paper, $\mathrm{d}j = j'(z)dz$ is viewed as a differential on $X_0(N)$. Fix the following two modular functions on $X_0(N)$:

$$r = j(j-1728)\frac{\omega}{\mathrm{d}j},\ u = \frac{1}{j}. \tag{2.3.1}$$

First we compute the divisor of r. Let $\mathcal{E}_2(N)$ and $\mathcal{E}_3(N)$ denote the set of elliptic points of order 2 and 3 on $X_0(N)$, respectively. Then

$$\mathrm{div}(\mathrm{d}j) = -j^*(\infty) - \sum_{c=cusp} c + \frac{1}{2}\left(j^*(1728) - \sum_{z\in\mathcal{E}_2(N)} z\right) + \frac{2}{3}\left(j^*(0) - \sum_{z\in\mathcal{E}_3(N)} z\right). \tag{2.3.2}$$

Writing $j^*(\infty) = \sum_{c=cusp} e_c[c]$, we obtain

$$\mathrm{div}(r) = \mathrm{div}(\omega) + \frac{1}{2}\left(j^*(1728) + \sum_{z\in\mathcal{E}_2(N)} z\right) + \frac{1}{3}\left(j^*(0) + 2\sum_{z\in\mathcal{E}_3(N)} z\right) - \sum_{c=cusp}(e_c - 1)[c]. \tag{2.3.3}$$

Note that (2.3.3) may not be the simplified form of $\mathrm{div}(r)$, due to possible cancellations when $\mathrm{supp}\,\mathrm{div}(\omega)$ contains cusps. But since the definition of $F_{E,j}$ only involves critical points that are not cusps, the form of $\mathrm{div}(r)$ in (2.3.3) works fine for our purpose.

Next we show $\mathbb{Q}(r,u) = \mathbb{Q}(X_0(N))$ for the functions r, u in (2.3.1). First we prove a lemma.

Lemma 2.3.4. *Let $N > 1$ be an integer and $f \in S_2(\Gamma_0(N))$ be a normalized newform. Suppose $\alpha \in SL_2(\mathbb{Z})$ and $f|[\alpha] = f$, then $\alpha \in \Gamma_0(N)$.*

Proof. Write $\alpha = \left(\begin{smallmatrix} a & b \\ M & d \end{smallmatrix}\right)$. First we show that it suffices to consider the case where $d = 1$. Since $(M, d) = 1$, there exists $y, w \in \mathbb{Z}$ such that $My + dw = 1$. By replacing (y, w) with $(y + kd, w - kM)$ if necessary, we may assume $(y, N) = 1$. Now we can find $x, z \in \mathbb{Z}$ such that $\gamma = \left(\begin{smallmatrix} x & y \\ Nz & w \end{smallmatrix}\right) \in \Gamma_0(N)$, and $\alpha\gamma = \left(\begin{smallmatrix} * & * \\ M & 1 \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ with $f|[\alpha\gamma] = f[\gamma] = f$. We then further reduce to the case where $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ M & 1 \end{smallmatrix}\right)$, by noticing that $\left(\begin{smallmatrix} 1 & -b \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_0(N)$ and

$$\left(\begin{smallmatrix} 1 & -b \\ 0 & 1 \end{smallmatrix}\right) \cdot \left(\begin{smallmatrix} a & b \\ M & 1 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ M & 1 \end{smallmatrix}\right).$$

Let $w_N = \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right)$ be the Fricke involution on $X_0(N)$. Then $f|[w_N] = \pm f$, hence $f|[w_N\alpha w_N] = f$. We compute that $w_N\alpha w_N = \left(\begin{smallmatrix} -N & M \\ 0 & -N \end{smallmatrix}\right)$, thus $f(q) = f|[\left(\begin{smallmatrix} -N & M \\ 0 & -N \end{smallmatrix}\right)](q) = f(q\zeta_N^{-M})$, where $\zeta_N = e^{2\pi i/N}$. The leading term of $f(q)$ is q, while the leading term of $f(q\zeta_N^{-M})$ is $\zeta_N^{-M}q$. So we must have $\zeta_N^{-M} = 1$, i.e., $N \mid M$. Hence $\alpha \in \Gamma_0(N)$ and the proof is complete. $\square$

Proposition 2.3.5. *Let r, u be the two functions on $X_0(N)$ defined in (2.3.1), then $\mathbb{Q}(r, u) = \mathbb{Q}(X_0(N))$.*

Lemma 2.3.6. *Let g be the genus of $X_0(N)$. If $T \geq 2g - 2$ is a positive integer, then rj^T and u satisfy the second condition of Proposition 2.3.2.*

Proof. Let $r_1 = rj^T$. When $T \geq 2g - 2$, the support of $\mathrm{div}_\infty(r_1)$ is the set of all cusps. Suppose $\gcd(f_n, f_0) > 1$. Let $p(y)$ be an irreducible factor of $\gcd(f_0, f_n)$. Consider the valuation ord_p on the field $K(y)$. Since $P(x, y)$ is irreducible, there exists an integer i with $0 < i < n$ such that $p(y) \nmid f_i$. Thus the Newton polygon of P with respect to the valuation ord_p has at least one edge with negative slope and one edge with positive slope. Therefore, for any Galois extension of L of $K(u)$ containing $K(r, u)$ and a valuation $\mathrm{ord}_\mathfrak{p}$ on L extending ord_p, where $\mathfrak{p}$ is an irreducible polynomial in $L[y]$ dividing $p(y)$, there exists two conjugates r', r'' of r such that $\mathrm{ord}_\mathfrak{p}(r') < 0$ and $\mathrm{ord}_\mathfrak{p}(r'') > 0$. This implies that $\mathrm{div}_0(r') \cap \mathrm{div}_\infty(r'') \neq \emptyset$. Fix $L = K(X(N))$, then all conjugates of r_1 in $K(X(N))/K(u)$ are of the form $r_1(\alpha z)$ for some $\alpha \in \mathrm{SL}_2(\mathbb{Z})$, Hence the set of poles of any conjugate of r_1 is the set of all cusps on $X(N)$, a contradiction. $\square$

Note that for any $T \in \mathbb{Z}$, we have $\mathbb{Q}(rj^T, u) = \mathbb{Q}(r, u) = \mathbb{Q}(X_0(N))$. Hence when $T \geq 2g-2$, the pair (rj^T, u) satisfies both assumptions of Proposition 2.3.2. We thus obtain

Theorem 2.3.7. *Let $T \geq 2g-2$ be a positive integer and let*

$$P(x, y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$$

be a minimal polynomial relation of rj^T and u. Then there exist integers A, B and a nonzero constant c such that

$$F_{E,j}(y) = cf_0(1/y) \cdot y^A (y-1728)^B.$$

The integers A and B are defined as follows. Let $\epsilon_i(N) = |\mathcal{E}_i(N)|$ for $i = 2$ or 3 and let $d_N = [SL_2(\mathbb{Z}) : \Gamma_0(N)]$, then $A = \deg f_n - T \cdot d_N - \frac{1}{3}(d_N + 2\epsilon_3(N))$ and $B = -\frac{1}{2}(d_N + \epsilon_2(N))$.

Proof. Write $\mathrm{div}(\omega) = \sum_{[z]\in X_0(N)} n_z[z]$. Applying Proposition 2.3.2 to rj^T and u, we get

$$\prod_{z:u(z)\neq 0,\infty} (y - u(z))^{n_z} \cdot (y - 1/1728)^{\frac{1}{2}(d_N+\epsilon_2(N))} = cf_0(y) \tag{a}$$

and

$$\sum_{z:u(z)=\infty} \mathrm{ord}_z(\omega) + T \cdot d_N + \frac{1}{3}(d_N + 2\epsilon_3(N)) = \deg f_n - \deg f_0. \tag{b}$$

To change from $u = \frac{1}{j}$ to j, we replace y by $1/y$ in (a) and multiply both sides by $y^{\deg f_0}$ to obtain

$$\prod_{z:j(z)\neq 0,\infty} (y - j(z))^{n_z} \cdot (y - 1728)^{\frac{1}{2}(d_N+\epsilon_2(N))} = cf_0(1/y)y^{\deg f_0}.$$

The contribution of $\{z \in \mathrm{div}(\omega) : j(z) = 0\}$ to $F_{E,j}$ can be computed from (b), so

$$\begin{aligned} F_{E,j}(y) &= c \cdot y^{\deg f_n - \deg f_0 - T\cdot d_N - \frac{1}{3}(d_N+2\epsilon_3(N))} y^{\deg f_0} \cdot (y-1728)^{-\frac{1}{2}(d_N+\epsilon_2(N))} f_0(1/y) \\ &= c \cdot y^{\deg f_n - T\cdot d_N - \frac{1}{3}(d_N+2\epsilon_3(N))} (y-1728)^{-\frac{1}{2}(d_N+\epsilon_2(N))} f_0(1/y). \end{aligned}$$

□

Now we describe the algorithm *Poly Relation*.

Algorithm 2 *Poly relation*

Input: E = Elliptic Curve over $\mathbb{Q}$; N = conductor of E; f = the newform attached to E. Values of $g = g(X_0(N))$, $d_N, \epsilon_2(N)$, $\epsilon_3(N)$, and c_N = number of cusps of $X_0(N)$.

Output: The critical j-polynomial $F_{E,j}(x)$.

1: Fix a large integer M. $T := 2g - 2$.
2: $r_1 := j^{2g-1}(j - 1728)\frac{f}{j'}$, $u := \frac{1}{j}$.
3: $\deg r_1 := (2g - 1)d_N - c_N, \deg u := d_N$.
4: Compute the q-expansions of r_1 and u to q^M.
5: Let $\{c_{a,b}\}_{0\leq a\leq \deg u, 0\leq b\leq \deg r_1}$ be unknowns, compute a vector that spans the one-dimensional vector space
6: $K = \{(c_{a,b}) : \sum c_{a,b} r(q)^a u(q)^b \equiv 0 \pmod{q^M}\}$.
7: $P(x, y) := \sum c_{a,b} x^a y^b$. Write $P(x, y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$.
8: $A := \deg f_n - T \cdot d_N - \frac{1}{3}(d_N + 2\epsilon_3(N))$, $B := -\frac{1}{2}(d_N + \epsilon_2(N))$.
9: Output $F_{E,j}(x) = cf_0(1/x) \cdot x^A(x - 1728)^B$.

Note that an upper bound on the number of terms M in the above algorithm can be taken to be $2 \deg r \deg u + 1$, by the following lemma.

Lemma 2.3.8. *Let $r, u \in \mathbb{Q}(X_0(N))$ be non-constant functions. If there is a polynomial $P \in \mathbb{Q}[x, y]$ such that $\deg_x P \leq \deg u$, $\deg_y P \leq \deg r$, and*

$$P(r, u) \equiv 0 \pmod{q^M}$$

for some $M > 2 \deg u \deg r$, then $P(r, u) = 0$.

Proof. Suppose $P(r, u)$ is non-constant as a rational function on $X_0(N)$, then $\deg P(r, u) \leq \deg r^{\deg u} u^{\deg r} = 2 \deg u \deg r$. It follows from $P(r, u) \equiv 0 \pmod{q^M}$ that $\mathrm{ord}_{[\infty]} P(r, u) \geq M$. Since $M > 2 \deg u \deg r$, the number of zeros of $P(r, u)$ is greater than its number of poles, a contradiction. Thus $P(r, u)$ is a constant function. But then $P(r, u)$ must be 0 since it has a zero at $[\infty]$. This completes the proof. ∎

Remark 2.3.9. When N is square free, there is a faster method that computes $F_{E,j}$ by computing the *Norm* of the modular form f, defined as $\mathrm{Norm}(f) = \prod f|[A_i]$, where $\{A_i\}$ is a set of right coset representatives of $\Gamma_0(N)$ in $\mathrm{SL}_2(\mathbb{Z})$. This approach is inspired by Ahrlgen and Ono [AO03], where j-polynomials of Weierstrass points on $X_0(p)$ are computed for p a prime.

Remark 2.3.10. In practice, in order to make the algorithm faster, we make different choices of r to make $\deg r$ small. Let η denote the Dedekind η-function and let $\Delta = \eta^{24}$ denote the discriminant modular form of level 1 and weight 12. When $4 \mid N$ we may take $r_4 = \frac{\omega j h_2}{\mathrm{d}j(32+h_4)}$, where $h_2 = \frac{\Delta(z)-512\Delta(2z)}{\Delta(z)+256\Delta(2z)}$ and $h_4 = (\eta(z)/\eta(4z))^8$. Then $\mathrm{div}(r_4) = \mathrm{div}(\omega) + D - D'$, where D and D' are supported on the cusps of $X_0(N)$, and $\deg D = c_N - \delta$, where δ is the number of cusps on $X_0(N)$ that are equivalent to $[\infty]$ modulo $\Gamma_0(4)$. Hence r_4 has a relatively small degree and is better suited for computation.

Remark 2.3.11. In order to speed up the computation, instead of taking $T = 2g - 2$ in the algorithm, we may take $T = 0$. First, if $\mathrm{div}(\omega)$ does not contain cusps(for example, this happens if N is square free), then the functions r and u already satisfies the assumptions of Proposition 2.3.2. Second, if $\mathrm{div}(\omega)$ does contain cusps, then $\deg(r)$ will be smaller than its set value in the algorithm, due to cancellation between zeros and poles. As a result, the vector space K will have dimension greater than 1. Nonetheless, using a basis of K, we could construct a set of polynomials $P_i(x, y)$ with $P_i(r, u) = 0$. Now $P(x, y)$ is the greatest common divisor of the $P_i(x, y)$.

We show a table of critical j-polynomials. Recall that $H_d(x)$ denotes the Hilbert class polynomial associated to a negative discriminant d. We use Cremona's labels [Cre] for elliptic curves in Table 2.3.1.

---

[1] In this case $\mathrm{div}(\omega) = [1/4] + [3/4] + [1/12] + [7/12]$ in supported on cusps.

Table 2.3.1: Critical polynomials for some elliptic curves with conductor smaller than 100

E	$g(X_0(N))$	Factorization of $F_{E,j}(x)$
37a	2	$H_{-148}(x)$
37b	2	$H_{-16}(x)^2$
44a	4	$H_{-44}(x)^2$
48a	3	1 [1]
67a	5	$x^8 + 1467499520383590415545083053760x^7 + \cdots$
89a	7	$H_{-356}(x)$

2.4 *Yang pairs and the algorithm* Poly Relation-YP

The main issue with the algorithm *Poly Relation* is efficiency. The matrix we used to solve for $\{c_{a,b}\}$ has size roughly of the same magnitude as conductor N. As N gets around 1000, computing the matrix kernel quickly becomes impractical. So a new method is needed.

We introduce an algorithm *Poly Relation-YP* to compute critical polynomials attached to elliptic curves. The algorithm is inspired by an idea of Yifan Yang in [Yan06]. The algorithm *Poly Relation-YP* does not compute the critical j-polynomial. Instead, it computes a critical h-polynomial, where h is some non-constant modular function on $X_0(N)$ chosen within the algorithm. First we restate a lemma of Yang.

Lemma 2.4.1 (Yang [Yan06])**.** *Suppose g, h are modular functions on $X_0(N)$ with a unique pole of order m, n at the cusp $[\infty]$, respectively, such that* $\gcd(m,n) = 1$*. Then*
(1) $\mathbb{Q}(g,h) = \mathbb{Q}(X_0(N))$.
(2) If the leading Fourier coefficients of g and h are both 1, then there is a minimal polynomial relation between g and h of form

$$y^m - x^n + \sum_{a,b\geq 0, am+bn<mn} c_{a,b}x^a y^b. \tag{2.4.1}$$

Definition 2.4.2. A pair of two non-constant modular functions on $X_0(N)$ is said to be a *Yang pair* if they satisfy the assumptions of Lemma 2.4.1.

Following [Yan06], we remark that in order to find a minimal polynomial relation of a Yang pair, we can compute the Fourier expansion of $y^m - x^n$ and use products of form $x^a y^b$ to cancel the pole at $[\infty]$ until we reach zero. This approach is significantly faster than the method we used in *Poly Relation*, which finds a minimal polynomial relation of two arbitrary modular functions. This gain in speed is the main motivation of introducing *Poly Relation-YP*.

Let

$$\eta = q^{\frac{1}{24}} \prod_{n \geq 1} (1 - q^n)$$

be the Dedekind η function. For any positive integer d, define the function η_d as $\eta_d(z) = \eta(dz)$.

Let N be a positive integer. An *η-product of level N* is a function of the form

$$h(z) = \prod_{d|N} \eta_d(z)^{r_d}$$

where $r_d \in \mathbb{Z}$ for all $d \mid N$.

The next theorem of Ligozat gives sufficient conditions for a η-product to be a modular function on $X_0(N)$.

Lemma 2.4.3 (Ligozat's Criterion [Lig75])**.** *Let $h = \prod_{d|N} \eta_d(z)^{r_d}$ be an η-product of level N. Assume the following:*
(1) $\sum_d r_d \frac{N}{d} \equiv 0 \pmod{24}$; (2) $\sum_d r_d d \equiv 0 \pmod{24}$; (3) $\sum_d r_d = 0$;
(4) $\prod_{d|N} (\frac{N}{d})^{r_d} \in \mathbb{Q}^2$.
Then h is a modular function on $X_0(N)$.

If $h \in \mathbb{Q}(X_0(N))$ is an η-product, then the divisor $\mathrm{div}(h)$ is supported on the cusps of $X_0(N)$. The next theorem allows us to construct η-products with prescribed divisors.

Lemma 2.4.4 (Ligozat [Lig75]). *Let $N > 1$ be an integer. For every positive divisor d of N, let (P_d) denote the sum of all cusps on $X_0(N)$ of denominator d. Let ϕ denote the Euler's totient function. Then there exists an explicitly computable η-product $h \in \mathbb{Q}(X_0(N))$ such that*

$$\operatorname{div}(h) = m_d(\,(P_d) - \phi(\gcd(d, N/d))[\infty]\,)$$

for some positive integer m_d.

Remark 2.4.5. By 'explicitly computable' in Lemma 2.4.4, we mean that one can compute a set of integers $\{r_d : d \mid N\}$ that defines the η-product h with desired property. It is a fact that the order of vanishing of an η product at any cusp of $X_0(N)$ is an linear combination of the integers r_d. So prescribing the divisor of an η-product is equivalent to giving a linear system on the variables r_d. Thus we can solve for the r_d's and obtain the q-expansion of h from the q-expansion of η.

The next proposition is a direct consequence of Lemma 2.4.4.

Proposition 2.4.6. *Let $D \geq 0$ be a divisor on $X_0(N)$ such that D is supported on the cusps. Then there exists an explicitly computable η-product $h \in \mathbb{Q}(X_0(N))$ such that* $\operatorname{div}(h)$ *is of the form $D' - m[\infty]$, where m is a positive integer and $D' \geq D$.*

Recall our notation from section 2.3 that $r = j(j-1728)\frac{\omega}{\mathrm{d}j}$.

Proposition 2.4.7. *There exists an explicitly computable function $h \in \mathbb{Q}(X_0(N))$ such that*
(1) The functions rh and $j(j-1728)h$ form a Yang pair;
(2) $j(j-1728)h$ is zero at all cusps of $X_0(N)$ except the cusp $[\infty]$.

Proof. Let $T = \operatorname{div}_\infty(j)$. Note that the support of T is the set of all cusps. From (2.3.3) we have $\operatorname{div}_\infty(r) \leq T$, $\operatorname{div}(j(j-1728)) = 2T$, $\operatorname{ord}_{[\infty]}(T) = 1$, and $\operatorname{ord}_{[\infty]}(r) = 0$. Applying Proposition 2.4.6 to the divisor $D = 4(T - [\infty])$, we obtain an η-product $h \in \mathbb{Q}(X_0(N))$ such that $\operatorname{div}(h) = D' - m[\infty]$, where $D' \geq D$ and $m \geq 0$. Then $\operatorname{div}_\infty(rh) = m[\infty]$ and $\operatorname{div}_\infty(j(j-1728)h) = (m+2)[\infty]$. If m is odd, then $(m, m+2) = 1$ and (1) follows.

Otherwise, we can replace h by jh. Then a similar argument shows that rh and $j(j-1728)h$ have a unique pole at $[\infty]$ and have degree $m+1$ and $m+3$, respectively. Since m is even in this case, we have $(m+1, m+3) = 1$ and (1) holds.

What we just showed is the existence of an η-product $h \in \mathbb{Q}(X_0(N))$ s.t. either h or jh satisfies (1). Now (2) follows from the fact that $\operatorname{div}_0(j(j-1728)h) > 2(T - [\infty])$ and $\operatorname{div}_0(j^2(j-1728)h) > (T - [\infty])$. □

Let h be a modular function that satisfies the conditions of Proposition 2.4.7. The next theorem allows us to compute $F_{E,j(j-1728)h}(x)$. For ease of notation, let $\tilde{r} = rh$ and $\tilde{h} = j(j-1728)h$.

Theorem 2.4.8. *Suppose h is a modular function on $X_0(N)$ that satisfies the conditions in Proposition 2.4.7. Let $P(x,y)$ be a minimal polynomial relation of $\tilde{r}$ and $\tilde{h}$ of form (2.4.1). Write $P(x,y) = f_n(y)x^n + \cdots + f_1(y)x + f_0(y)$, and let g be the genus of $X_0(N)$, then*

$$F_{E,\tilde{h}}(x) = x^{2g-2-\deg h} f_0(x).$$

Proof. The idea is to apply Proposition 2.3.2 to the Yang pair $(\tilde{r}, \tilde{h})$. By Lemma 2.4.1, every Yang pair satisfies its first assumption. To see the second assumption holds, observe that $f_n(y) = -1$ in (2.4.1), so $\gcd(f_n(y), f_0(y)) = 1$. Hence we can apply Proposition 2.3.2 and obtain

$$f_0(y) = \prod_{z \in \operatorname{div}_0(\tilde{r}) \setminus \operatorname{div}_\infty(\tilde{h})} (y - \tilde{h}(z))^{n_z}.$$

By construction of h, there is a divisor $D \geq 0$ on $X_0(N)$ supported on the finite set $j^{-1}(\{0, 1728\}) \cup h^{-1}(0)$, such that $\operatorname{div}(rh) = \operatorname{div}(\omega) + D - (\deg h)[\infty]$. Taking degrees on both sides shows $\deg D = \deg h - (2g-2)$. Since $\tilde{h}(z) = 0$ for all $z \in \operatorname{supp} D$, we obtain

$$f_0(x) = F_{E,\tilde{h}}(x) \cdot x^{\deg h - 2g + 2}.$$

This completes the proof. □

Next we describe the algorithm *Poly Relation-YP*.

Algorithm 3 *Poly Relation-YP*

Input: E = Elliptic Curve over $\mathbb{Q}$, f = the newform attached to E.

Output: a non-constant modular function h on $X_0(N)$ and the critical $\tilde{h}$-polynomial $F_{E,\tilde{h}}$, where $\tilde{h} = j(j-1728)h$.

Find an η product h that satisfies Proposition 2.4.7.
$\tilde{r} := j(j-1728)h\frac{f}{j'}$, $\quad \tilde{h} := j(j-1728)h$.
$M := (\deg \tilde{r} + 1)(\deg \tilde{h} + 1)$.
Compute q-expansions of $\tilde{r}$, $\tilde{h}$ to q^M.
Compute a minimal polynomial relation $P(x,y)$ of form (2.4.1)
using the method mentioned after Lemma 2.4.1.
Output $F_{E,\tilde{h}}(x) = x^{2g-2-\deg h}P(0,x)$.

Remark 2.4.9. The functions $\tilde{r}$ and $\tilde{h}$ in the above algorithm are constructed in order that Theorem 2.4.8 has a nice and short statement. However, their degrees are large, which is not optimal for computational purposes. In practice, one can make different choices of two modular functions with smaller degrees to speed up the computation. This idea is illustrated in the following example.

Example 2.4.10. Let E be the elliptic curve

$$E : y^2 = x^3 - 7x + 10$$

labeled as **664a1** in Cremona's table. Then $r_{\mathrm{an}}(E) = 2$, and $X_0(664)$ has genus 81. Let $r = r_4$ be as defined in Remark 2.3.10. Using the method described in Remark 2.4.5, we found two η-products

$$h_1 = (\eta_2)^{-4}(\eta_4)^6(\eta_8)^4(\eta_{332})^6(\eta_{664})^{-12},\ h_2 = (\eta_2)^{-1}(\eta_4)(\eta_{166})^{-1}(\eta_8)^2(\eta_{332})^5(\eta_{664})^{-6}$$

with the following properties: $h_1, h_2 \in \mathbb{Q}(X_0(N))$, $\mathrm{div}(rh_1) = \mathrm{div}(\omega) + D - 247[\infty]$, where $D \geq 0$ is supported on cusps, and $\mathrm{div}(h_2) = 21[1/332] + 61[1/8] + 21[1/4] - 103[\infty]$. Since

(247,103) =1, the functions rh_1 and h_2 form a Yang pair. We then computed

$$F_{E,h_2}(x) = x^{160} - 1443491497715558443975973096765345920086503212026560026755519644 4x^{158} + \cdots.$$

The polynomial F_{E,h_2} is irreducible in $\mathbb{Q}[x]$.

2.5 *The critical subgroup* $E_{crit}(\mathbb{Q})$

Recall the definition of the critical subgroup for an elliptic curve $E/\mathbb{Q}$:

$$E_{\mathrm{crit}}(\mathbb{Q}) = \langle \mathrm{tr}(\varphi(e)) : e \in \operatorname{supp} \operatorname{div}(\omega) \rangle.$$

Observe that to generate $E_{\mathrm{crit}}(\mathbb{Q})$, it suffices to take one representative from each Galois orbit of $\operatorname{supp} \operatorname{div}(\omega)$. Therefore, if we let n_ω denote the number of Galois orbits in $\operatorname{div}(\omega)$, then

$$\mathrm{rank}(E_{\mathrm{crit}}(\mathbb{Q})) \leq n_\omega.$$

For any rational divisor $D = \sum_{[z] \in X_0(N)} n_z[z]$ on $X_0(N)$, let $p_D = \sum_{z \in \operatorname{supp} D} n_z \varphi([z])$, then $p_D \in E(\mathbb{Q})$. Note that $p_D = 0$ if D is a principal divisor. The point $p_{\operatorname{div}(\omega)}$ is a linear combination of the defining generators of $E_{\mathrm{crit}}(\mathbb{Q})$.

Lemma 2.5.1. $6\, p_{\operatorname{div}(\omega)} \equiv -3 \sum_{c \in \mathcal{E}_2(N)} \varphi(c) - 4 \sum_{d \in \mathcal{E}_3(N)} \varphi(d) \pmod{E(\mathbb{Q})_{\mathrm{tors}}}$.

Proof. Let $r_0 = \omega / \mathrm{d}j$, then $r_0 \in \mathbb{Q}(X_0(N))$, hence $p_{\operatorname{div}(r_0)} = 0$. From $\operatorname{div}(r_0) = \operatorname{div}(\omega) - \operatorname{div}(\mathrm{d}j)$, we deduce that $p_{\operatorname{div}(\omega)} = p_{\operatorname{div}(\mathrm{d}j)}$. The lemma then follows from the formula of $\operatorname{div}(\mathrm{d}j)$ given in (2.3.2) and the fact that the image of any cusp under φ is torsion. □

Proposition 2.5.2. *Assume at least one of the following holds:*

(1) $r_{\mathrm{an}}(E) \geq 2$*;*

(2) $X_0(N)$ *has no elliptic point.*

Then $\mathrm{rank}(E_{\mathrm{crit}}(\mathbb{Q})) \leq n_\omega - 1$.

Proof. By Lemma 2.5.1 and Theorem 2.1.3, either assumption implies that $p_{\operatorname{div}(\omega)}$ is torsion. But $p_{\operatorname{div}(\omega)}$ is a linear combination of the n_ω generators of $E_{\mathrm{crit}}(\mathbb{Q})$, so these generators are linearly dependent in $E_{\mathrm{crit}}(\mathbb{Q}) \otimes \mathbb{Q}$. Hence the rank of $E_{\mathrm{crit}}(\mathbb{Q})$ is smaller than n_ω. □

Now we are ready to prove Theorem 2.1.6.

Proof of Theorem 2.1.6. First, note that the definition of $F_{E,j}$ only involves critical points that are not cusps. However, since images of cusps under φ are torsion, we can replace $\operatorname{div}(\omega)$ by $\operatorname{div}(\omega) \setminus \{$ cusps of $X_0(N)\}$ if necessary and assume that $\operatorname{div}(\omega)$ does not contain cusps. (1) Let $d = \deg F_0$, then there exists a Galois orbit in $\operatorname{div}(\omega)$ of size d, and the other $(2g-2-d)$ points in $\operatorname{div}(\omega)$ are CM points. Let z be any one of the $(2g-2-d)$ points, then $j(z)$ is a root of $H_{D_k}(x)$ and $z \in \mathbb{Q}(\sqrt{D_k})$. Since $\operatorname{div}(\omega)$ is invariant under the Fricke involution w_N, one sees that $j(Nz)$ is also a root of $F_{E,j}$. Therefore, $j(Nz)$ is the root of $H_{D_{k'}}(x)$ for some $1 \leq k' \leq m$. Since z and Nz define the same quadratic field, we must have $\mathbb{Q}(\sqrt{D_k}) = \mathbb{Q}(\sqrt{D_{k'}})$, which implies $k = k'$ by our assumption. It follows that $[z]$ is a "generalized Heegner point"(as defined in Definition 2.1.2) and $\operatorname{tr}(\varphi([z]))$ is torsion. By the form of $F_{E,j}$, there exists a point $[z_0] \in \operatorname{supp}\operatorname{div}(\omega)$ such that $j(z_0)$ is a root of F_0. Then we have $\operatorname{rank}(E_{\text{crit}}(\mathbb{Q})) = \operatorname{rank}(\langle \operatorname{tr}(\varphi([z_0])\rangle) = \operatorname{rank}(\langle p_{\operatorname{div}(\omega)}\rangle)$. Finally, Lemma 2.5.1 implies $\langle p_{\operatorname{div}(\omega)}\rangle = 0$, and it follows that $\operatorname{rank}(E_{\text{crit}}(\mathbb{Q})) = 0$.

(2) If $F_{E,h}$ is irreducible, then we necessarily have $n_\omega = 1$, and the claim follows from Proposition 2.5.2.

Remark 2.5.3. Christophe Delaunay has an algorithm to compute $\operatorname{div}(\omega)$ numerically as equivalence classes of points in the upper half plane(see [Del02] and [Del05]). A table of critical points for the elliptic curve

$$E : y^2 + y = x^3 + x^2 - 2x$$

with rank 2 and Cremona label **389a** is presented in [Del02, Appendix B.1]. The results suggested that $\operatorname{div}(\omega)$ contains two Heegner points of discriminant 19, and the critical subgroup $E_{\text{crit}}(\mathbb{Q})$ is torsion. Using the critical j-polynomial for **389a** in Table 2.6.1, we can confirm the numerical results of Delaunay.

2.6 Data: critical polynomials for rank two elliptic curves

The columns of Table 2.6.1 are as follows. The column labeled E contains labels of elliptic curves, and those labeled g contains the genus of $X_0(N)$, where N is the conductor of E. The column labeled h contains a modular function on $X_0(N)$: either the j invariant or some η-product. The last column contains the factorization of the critical h-polynomial of E defined in Section 2.1.1. The factors of $F_{E,j}$ that are Hilbert class polynomials are written out explicitly. Table 2.6.1 contains *all* elliptic curves with conductor $N \leq 1000$ and rank 2. By observing that all the critical polynomials in the table satisfy one of the assumptions of Theorem 2.1.6, we obtain Corollary 2.1.7.

From our computation, it seems hard to find an elliptic curve $E/\mathbb{Q}$ with $r_{\mathrm{an}}(E) \geq 2$ and $\mathrm{rank}(E_{\mathrm{crit}}(\mathbb{Q})) > 0$. Nonetheless, some interesting questions can be raised.

Question 2.6.1. *For all elliptic curves $E/\mathbb{Q}$, does $F_{E,j}$ always factor in $\mathbb{Q}[x]$ as a product of Hilbert class polynomials and one irreducible polynomial?*

If the answer to Question 2.6.1 is positive, then we would know $E_{\mathrm{crit}}(\mathbb{Q})$ is torsion wheneve $r_{an}(E) \geq 2$.

Another way to construct rational points on E is to take any cusp form $g \in S_2(\Gamma_0(N), \mathbb{Z})$ and define $E_g(\mathbb{Q}) = \langle \mathrm{tr}(\varphi([z]) : [z] \in \mathrm{supp}\,\mathrm{div}(g(z)dz) \rangle$.

Question 2.6.2. *Does there exist $g \in S_2(\Gamma_0(N), \mathbb{Z})$ such that $E_g(\mathbb{Q})$ is non-torsion?*

Remark 2.6.3. Consider the irreducible factors of $F_{E,j}$ that are *not* Hilbert class polynomials. It turns out that their constant terms has many small primes factors, a property also enjoyed by Hilbert class polynomials. For example, consider the polynomial $F_{67a,j}$. It is irreducible and not equal to any Hilbert class polynomial, while its constant term has factorization

$$2^{68} \cdot 3^2 \cdot 5^3 \cdot 23^6 \cdot 443^3 \cdot 186145963^3.$$

It is interesting to investigate the properties of these polynomials.

Table 2.6.1: Critical polynomials for elliptic curves of rank 2 and conductor < 1000

E	$g(X_0(N))$	h	Factorization of $F_{E,h}(x)$
389a	32	j	$H_{-19}(x)^2(x^{60}+\cdots)$
433a	35	j	$x^{68}+\cdots$
446d	55	j	$x^{108}+\cdots$
563a	47	j	$H_{-43}(x)^2(x^{90}-\cdots)$
571b	47	j	$H_{-67}(x)^2(x^{90}-\cdots)$
643a	53	j	$H_{-19}(x)^2(x^{102}-\cdots)$
664a	81	$\frac{\eta_4\eta_8^2\eta_{332}^5}{\eta_{166}\eta_{664}^6\eta_2}$	$x^{160}-\cdots$
655a	65	j	$x^{128}-\cdots$
681c	75	j	$x^{148}-\cdots$
707a	67	j	$x^{132}-\cdots$
709a	58	j	$x^{114}-\cdots$
718b	89	j	$H_{-52}(x)^2(x^{172}-\cdots)$
794a	98	j	$H_{-4}(x)^2(x^{192}-\cdots)$
817a	71	j	$x^{140}-\cdots$
916c	113	j	$H_{-12}(x)^8(x^{216}+\cdots)$
944e	115	$\frac{\eta_{16}^4\eta_4^2}{\eta_8^6}$	$x^{224}-\cdots$
997b	82	j	$H_{-27}(x)^2(x^{160}-\cdots)$
997c	82	j	$x^{162}-\cdots$

Chapter 3

FOURIER EXPANSIONS OF MODULAR FORMS FORMS AT ALL CUSPS

Let k be a positive even integer and let $f \in S_k(\Gamma_0(N))$ be a nonzero cusp form. Then f has a Fourier expansion at the cusp infinity:

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

where a_n are complex numbers and $q = e^{2\pi i \tau}$. We are concerned with the problem of computing the Fourier expansion of f at other cusps. When N is square-free, this problem is solved by Asai [Asa76]. The problem is studied in the Ph.D. thesis of Christophe Delaunay and in [CE11], where a numerical algorithm is proposed. We will give a numerical algorithm to compute such expansions. Our approach is different from the one proposed in [CE11], for they require working at a higher level: to compute expansions at cusps of denominator Q, one needs to compute period matrices for forms of level NR^2, where $R = \gcd(Q, \frac{N}{Q})$. As a contrast, our algorithm works at levels dividing N.

The main results of this chapter are Theorem 3.6.7 and Algorithm 6. The former gives a formula for the Fourier expansion of a newform $f \in S_k(\Gamma_0(N))$ at any cusp z of width one, and the latter describes how to use the formula to explicitly compute such expansion. Along the way, we will develop algorithms to compute the twists $f \otimes \chi$ and the pseudo-eigenvalue of newforms under the Fricke involution.

Section [fixme] contains some examples.

3.1 Preliminaries

Let $N \geq 1$ be an integer and let $X_0(N)$ be the modular curve of level N.

Definition 3.1.1. Let z be a cusp on $X_0(N)$. If $z \neq \infty$, write $z = [a/c]$ with $\gcd(a,c) = 1$. The *denominator* of z is

$$d_z = \gcd(c, N).$$

If $z = \infty$, we set $d_\infty = N$. Choose $\alpha \in SL_2(\mathbb{Z})$ such that $\alpha(\infty) = z$. The *width* of z is

$$h_z = \left| \frac{SL_2(\mathbb{Z})_\infty}{(\alpha^{-1}\{\pm I\}\Gamma_0(N)\alpha)_\infty} \right|$$

where the subscript ∞ means taking the isotropy subgroup of ∞ in the corresponding group.

The width of a cusp can be computed in terms of its denominator. In fact, we have

Lemma 3.1.2. *If z is a cusp on $X_0(N)$, then*

$$h_z = \frac{N}{\gcd(d_z^2, N)}.$$

Proof. When $z = [\infty]$, we have $d_\infty = N$ and $h_\infty = 1$, so the formula holds trivially. Otherwise, write $z = [\frac{a}{c}]$ and find $\alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. For $N' \in \mathbb{Z}$ we compute

$$\alpha \left(\begin{smallmatrix} 1 & N' \\ 0 & 1 \end{smallmatrix}\right) \alpha^{-1} = \left(\begin{smallmatrix} * & * \\ -c^2 N' & * \end{smallmatrix}\right).$$

Hence $\left(\begin{smallmatrix} 1 & N' \\ 0 & 1 \end{smallmatrix}\right) \in (\alpha^{-1}\{\pm I\}\Gamma_0(N)\alpha)_\infty \iff N \mid c^2 N' \iff \frac{N}{\gcd(d_z^2, N)} \mid N'$. This completes the proof. $\square$

In particular, the width of a cusp z is one if and only if $N \mid d_z^2$.

Suppose f is a modular form on $\Gamma_0(N)$ of positive even weight k and $\alpha \in GL_2(\mathbb{Q})$. Recall the weight-$k$ action is defined as

$$f|\alpha(\tau) = (\det(\alpha))^{k/2}(cz + d)^{-k} f(\alpha\tau),\ \alpha = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right).$$

In particular, if $\alpha \in SL_2(\mathbb{Z})$, then $f|\alpha$ is a modular form on $\Gamma(N)$. So $f|\alpha$ has a q-expansion, which is a power series in $q^{\frac{1}{N}}$. A natural thing to do is to define the expansion of f at the cusp z as the expansion of $f|\alpha$. However, note that this may not be well-defined: in general the expansion depends on the choice of α. Nonetheless, when the cusp z has width one, the expansion is indeed well-defined as a power series in q.

Lemma 3.1.3. *Let z be a cusp on $X_0(N)$ with $h_z = 1$. Choose $\alpha \in SL_2(\mathbb{Z})$ such that $\alpha(\infty) = z$. Then $f|\alpha$ is a cusp form on $\Gamma_1(N)$. Moreover, the function $f|\alpha$ is independent of the choice of α.*

Proof. It is easy to verify that $\Gamma_1(N) \subseteq \alpha^{-1}\Gamma_0(N)\alpha$, hence the first claim holds. Now suppose $\beta \in SL_2(\mathbb{Z})$ is such that $\beta(\infty) = z$. Then $\alpha^{-1}\beta \in SL_2(\mathbb{Z})_\infty$. Since z has width one, we have $\alpha^{-1}\beta \in \alpha^{-1}\Gamma_0(N)\alpha$. Hence $\beta \in \Gamma_0(N)\alpha$, and it follows that $f|[\beta] = f|[\alpha]$. $\square$

In light of the lemma above, we define the *q-expansion of f at a width one cusp z* to be the q-expansion of $f|[\alpha]$, and denote it by f_z.

Assume further that f is an eigenform under the Atkin-Lehner operators. We will show that in order to compute the expansion of $f|[\alpha]$ for any $\alpha \in SL_2(\mathbb{Z})$, it suffices to do so for $\alpha = \left(\begin{smallmatrix} 1 & 0 \\ m & 1 \end{smallmatrix}\right)$, where $0 \leq m < N$ and $N \mid \gcd(m, N)^2$. In particular, it suffices to compute the expansions of f at a some cusps of width one.

Lemma 3.1.4. *For any $\alpha \in SL_2(\mathbb{Z})$, there exists a matrix $w_Q \in W_N$ and an upper triangular matrix $u \in GL_2(\mathbb{Q})$ such that $w\alpha = \alpha' u$, where $\alpha' = \left(\begin{smallmatrix} a' & b \\ c' & d' \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$ satisfies $N \mid \gcd(N, c')^2$.*

Indeed, one may find Q using Lemma. Now $f|[\alpha] = f|[w_Q][w_Q\alpha] = f|[w_Q][\alpha'][u] = \lambda_Q(f)f[\alpha'][u] = \lambda_Q(f)f[\alpha''][u]$, where α'' is of form $\left(\begin{smallmatrix} 1 & 0 \\ m & 1 \end{smallmatrix}\right)$. Note that for an upper triangular matrix $u = \left(\begin{smallmatrix} u_0 & u_1 \\ 0 & u_2 \end{smallmatrix}\right)$, we have $f[u](q) = f(q^{u_0/u_2}e^{2\pi i u_1/u_2})$.

3.2 Reducing to the case of newforms

The space $S_k(\Gamma_0(N))$ is spanned by elements of form $g(q^d)$, where g is newform of level $M \mid N$ and d is a divisor of $\frac{N}{M}$. Note that $g(q^d) = d^{-k/2}g|\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)$. For any $\alpha \in SL_2(\mathbb{Z})$, we can find $\alpha' \in SL_2(\mathbb{Z})$ and $u \in GL_2(\mathbb{Q})$ such that $\left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right)\alpha = \alpha' u$. Hence to compute all expansions $f|[\alpha]$, it suffices to give an algorithm for newforms.

In the rest of this chapter, we will restrict ourselves to solving the following problem:

Problem 3.2.1. Let f be a normalized newform in $S_k(\Gamma_0(N))$ and z be a cusp on $X_0(N)$ of width one. Compute the q-expansion of f_z.

3.3 Twists of newforms

For $f \in S_k(\Gamma_1(N), \epsilon)$ a newform with expansion $f = \sum_n a_n(f)q^n$ and χ a Dirichlet character, the *twist* f_χ is a modular form with expansion $f_\chi(q) = \sum a_n(f)\chi(n)q^n$.

Lemma 3.3.1. *[AWL78, Proposition 3.1] Let $F \in S_k(\Gamma_1(N), \epsilon)$, where ϵ is a character of conductor N'. Let χ be a character modulo M. Put $\tilde{N} = lcm(N, N'M, M^2)$. Then $f_\chi \in S_k(\Gamma_1(\tilde{N}), \epsilon\chi^2)$.*

In particular, when ϵ is the trivial character and the conductor M of χ satisfies $M^2 \mid N$, we have $F_\chi \in S_k(\Gamma_1(N), \chi^2))$.

We write $f \otimes \chi$ for the unique newform such that $a_p(f \otimes \chi) = a_p(f_\chi)$ for all but finitely many primes p. From now, we refer to $f \otimes \chi$ as *the twist of f by χ*.

We quote two more results from [AWL78], which we will use extensively. First, we recall the definitions of U_d and B_d operators. For a modular form $f = \sum a_n q^n$ and a positive integer d, we put

$$f|U_d = \sum a_{nd}q^n, \; f|B_d = \sum a_n q^{nd}.$$

It is easy to see that for any positive integers d, d', we have U_d commutes with $B_{d'}$.

Lemma 3.3.2. *[AWL78, Theorem 3.1] Let $q \mid N$ and Q be the q-primary part of N. Write $N = QM$. Let F be a newform in $S_k(\Gamma_1(N), \epsilon)$ with $\mathrm{cond}(\epsilon_Q) = q^\alpha, \alpha \geq 0$. Let χ be a character with conductor q^β, $\beta \geq 1$. Put $Q' = \max\{Q, q^{\alpha+\beta}, q^{2\beta}\}$. Then*
(1) For each prime $q' \mid M, F_\chi$ is not of level $Q'M/q$.
(2) The exact level of F_χ is $Q'M$ provided (a) $\max\{q^{\alpha+\beta}, q^{2\beta}\} < Q$ if $Q' = Q$, or (b) $\mathrm{cond}(\epsilon_Q\chi) = \max\{q^\alpha, q^\beta\}$ if $Q' > Q$.

Lemma 3.3.3. *[AWL78, Theorem 3.2] Let $q \mid N$ and Q be the q-primary part of N. Write $N = QM$. Let χ be a character whose conductor equals a power of q. Let f be a newform in $S_k(\Gamma_1(N), \epsilon)$. Then $f \otimes \chi$ is a newform in $S_k(\Gamma_1(Q'M, \epsilon\chi^2)$, where Q' is a power of q. Moreover, we have*

$$f_\chi = f \otimes \chi - (f \otimes \chi)|U_q|B_q.$$

Since our goal is to compute expansions of newforms on $\Gamma_0(N)$, we will make the following assumptions: from now, unless otherwise noted, we assume f has trivial character, and that $\mathrm{cond}(\chi)^2 \mid N$.

Next, we consider the problem of identifying the newform $f \otimes \chi$. This includes finding its level and its q-expansion to arbitrarily many terms. We will assume that we have an oracle which, given weight k and level N, computes the expansions of all newforms in $S_k(\Gamma_1(N))$ to arbitrarily many terms (for example, use the algorithm in [Steb]).

Now we proceed on how to recognise the level of $f \otimes \chi$ from the coefficients of f. One potential obstacle is that we do not know all Fourier coefficients of $f \otimes \chi$: we only know that $a_n(f \otimes \chi) = a_n(f)\chi(n)$ when $\gcd(n, N) = 1$. This can be overcome using a variant of Sturm's argument. First we prove a lemma.

Lemma 3.3.4. *Let $f \in S_k(N, \epsilon)$ be a normalized newform and q be any positive integer. Then $f|U_q|B_q \in S_k(Nq^2, \epsilon)$.*

Proof. It is a standard fact that for any integer $d \geq 1$, the map $f \mapsto f|B_d$ takes $S_k(N, \epsilon)$ to $S_k(Nd, \epsilon)$. To prove the lemma, we consider two separate cases. First, assume $q \nmid N$, then we have $T_q = U_q + q^{k-1}\epsilon(q)B_q$. By our assumption, we have $f|T_q = a_q(f)f$. Therefore, we have $f|U_q|B_q = f|(T_q - q^{k-1}\epsilon(q)B_q)|B_q = a_q(f)f|B_q - q^{k-1}\epsilon(q)f|B_q^2$. Hence $f|U_q|B_q \in S_k(Nq^2, \epsilon)$. Now assume $q \mid N$, so $U_q = T_q$. Hence $f|U_q|B_q = a_q(f)f|B_q \in S_k(Nq, \epsilon) \subseteq S_k(Nq^2, \epsilon)$. $\square$

The next proposition generalised the usual Sturm bound argument for modular forms.

Proposition 3.3.5. *Let g_1, g_2 be two normalised newforms of levels $N_1 \mid N_2$ and the same nybentypus character ϵ. Assume ϵ has prime power conductor $Q = q^\beta$ such that $Q^2 \mid N_1$. Let B be the Sturm bound for the congruence subgroup $\Gamma_1(Nq^2)$. Suppose*

$$a_n(g_1) = a_n(g_2), \text{ for all } 1 \leq n \leq B \text{ such that } \gcd(n, q) = 1.$$

Then $g_1 = g_2$.

Proof. Following [AWL78], we define the operator K_q on the space of modular forms by

$$g|K_q = g - g|U_q|B_q.$$

Then the assumption is equivalent to the statement that $\delta = (g_1 - g_2)|K_q$ has $a_n(\delta) = 0$ for all $1 \le n \le B$. Since $\delta \in S_k(Nq^2, \epsilon)$, Sturm's theorem implies $\delta = 0$. We then know from [DS06, Theorem 5.7.1] that $g_1 - g_2 \in S_k(N_2, \epsilon)^{old}$. Suppose $N_1 < N_2$, then g_1 is in the old subspace, hence so is g_2, a contradiction. Therefore we must have $N_1 = N_2$. It follows that $g_1 - g_2 \in S_k(N_2, \epsilon)^{new}$, since g_1, g_2 are newforms. Since the new subspace and the old subspace intersect trivially, we must have $g_1 - g_2 = 0$. $\square$

Now we are ready to describe the algorithm.

Algorithm 4 Identifying $f \otimes \chi$

Input: k – a positive even integer; $f \in S_k(\Gamma_0(N))$ a normalized newform; χ a Dirichlet character of prime power conductor $Q = q^\beta$; $Q^2 \mid N$; B – a positive integer

Output: The level M_χ of $f \otimes \chi$ and the Fourier expansion of $f \otimes \chi$ up to q^B.

```
if Q = 1 then
    return N.
end if
Q' := cond(χ²); N_0 := N / q^{v_q(N)}; M_0 := Q'N_0; t := N / M_0 ∈ ℤ.
for each positive divisor d of t do
    Set V_d := S_k(M_0 d, χ²).
    Compute a basis of newforms {g_1^(d), ··· g_{s_d}^(d)} of V_d.
    Set B_d := the Sturm bound for Γ_1(M_0 d q²).
    for 1 ≤ j ≤ s_d do
        if a_n(g_i^(d)) = a_n(f)χ(n) for all 1 ≤ n ≤ B_d, gcd(n, q) = 1 then
            return M_0 d.
        end if
    end for
end for
```

We give some sample computations applying the above algorithm.

Example 3.3.6. Let f be the normalised newform attached to the elliptic curve

$$E : y^2 + xy + y = x^3 - x - 2$$

of Cremona label **50a**. Then $f \otimes \chi$ is new of level 50 for all Dirichlet characters χ with modulus 5. In other words, f is 5-minimal.

As another example, we demonstrate a newform which is not p-minimal.

Example 3.3.7. Let f be the normalised newform attached to the elliptic curve

$$E : y^2 + xy = x^3 + x^2 - 25x - 111$$

of label **98a**. Let χ be the Dirichlet character modulo 7 defined by $\chi(3 \pmod 7) = -1$. We found that $f \otimes \chi$ is a newform of level 14, with q-expansion

$$(f \otimes \chi)(q) = q - q^2 - 2q^3 + q^4 + 2q^6 + q^7 - q^8 + q^9 - 2q^{12} - 4q^{13} - q^{14} + O(q^{15}).$$

3.4 Pseudo-eigenvalues

Let ϵ be a Dirichlet character modulo N and let f be a newform in $S_k(N, \epsilon)$. For any divisor Q of N with $\gcd(Q, \frac{N}{Q}) = 1$, there is an algebraic number $w_Q(f)$ of absolute value one and a newform g in $S_k(N, \overline{\epsilon_Q}\epsilon_{N/Q})$ such that

$$W_Q(f) = w_Q(f)g,$$

Definition 3.4.1. The number $w_Q(f)$ is called the *pseudo-eigenvalue* of W_Q on f.

For ease of notations, we write $w(f) = w_N(f)$.

For a power series $f = \sum_{n \geq 0} a_n q^n$, its complex conjugate, denoted by f^*, is

$$f^*(q) = \sum \overline{a_n} q^n.$$

From [AWL78] we have $W_N(f) = w(f)f^*$. In the rest of this section, we describe an algorithm to efficiently compute $w(f)$ numerically. For a positive even integer k, let $\mathbb{M}(k)$ denote the space of weight-k modular symbols defined in [Steb]. The space $\mathbb{M}(k)$ is a quotient of $\mathbb{Z}[X,Y]_{k-2} \otimes \mathbb{P}^1(\mathbb{Q})^2$, and $GL_2(\mathbb{Q})$ acts on $\mathbb{M}(k)$ via the following rule

$$g(P(X,Y) \otimes \{\alpha, \beta\}) = P(g^{-1}(X,Y)^T)\{g(\alpha), g(\beta)\}.$$

Most importantly, there is a pairing between $\mathbb{M}(k)$ and the space of modular forms of weight k, defined as

$$\langle f, P(X,Y) \otimes \{\alpha, \beta\}\rangle_k = \int_\alpha^\beta f(z)P(z,1)dz.$$

We will suppress the subscript k if its value is clear from context.

Lemma 3.4.2. *Let $M \in \mathbb{M}(k)$ and $f \in S_k(\Gamma_1(N))$. Then*

$$N^{\frac{k}{2}-1}\langle f|W_N, M\rangle = \langle f, W_N M\rangle.$$

Proof. See proof of [Steb, Proposition 8.17]. Note that the extra factor $N^{\frac{k}{2}-1}$ is due to the different constants involved in the definition of the weight-k action of $GL_2(\mathbb{Q})$ on modular forms. $\square$

The map

$$* : P(x,y)\{\alpha, \beta\} \mapsto P(-x,y)\{-\bar{\alpha}, -\bar{\beta}\}$$

defines the *star involution* on the space $\mathbb{M}(k)$. We have $\langle f^*, M\rangle = \overline{\langle f, M^*\rangle}$.

Lemma 3.4.3. *Let f be a normalised newform on $\Gamma_1(N)$ with positive even weight k and let $M \in \mathbb{M}(k)$ be such that $W_N(M) = N^{k/2-1}M^*$. Assume $\langle f, M\rangle \neq 0$. Then*

$$w(f) = \frac{\langle f, M\rangle}{\overline{\langle f, M\rangle}}.$$

Proof. Since $W_N^2(M) = N^{k-2}M$ for all $M \in \mathbb{M}(k)$, the assumption implies $W_N(M^*) = N^{k/2-1}M$. Now

$$
\begin{aligned}
& N^{k/2-1}\langle f|W_N, M^*\rangle = \langle f, W_N(M^*)\rangle \\
\Longrightarrow\ & N^{k/2-1}w(f)\langle f^*, M^*\rangle = N^{k/2-1}\langle f, M\rangle \\
\Longrightarrow\ & w(f) = \frac{\langle f, M\rangle}{\langle f^*, M^*\rangle} \\
\Longrightarrow\ & w(f) = \frac{\langle f, M\rangle}{\overline{\langle f, M\rangle}}.
\end{aligned}
$$

□

Suppose α, β are distinct points on the arc $\{z \in \mathbb{C}|Im(z) > 0, |z| = 1/\sqrt{N}\}$. Then it is easy to verify that $M = (xy)^{k/2-1} \otimes \{\alpha, \beta\}$ satisfies $W_N(M) = M^*$. Finally, we arrive at the algorithm to compute $w(f)$.

Algorithm 5 Computing the pseudo-eigenvalue of newforms.

Input: k – a positive even integer. $f \in S_k(\Gamma_1(N))$ a normalized newform.

Output: a numerical approximation of $w(f)$.

```
n_0 := 10, z_0 := i/√N. δ = 10^{-3}.
Randomly generate n_0 points {z_1, ···, z_{N_0}} ⊆ {z | 0 < Im(z) < 1/(2√N), |z| = 1/√N}.
for 1 ≤ i ≤ n_0 do
    compute the period integral c_i = ∫_{z_0}^{z_i} 2πi f(z) z^{(k-2)/2} dz.
    w_i ← c_i / c̄_i.
end for
if the standard deviation of w_1, ···, w_{n_0} is less than δ then
    w ← (1/n_0)(∑_i w_i).
    return w.
else
    return FAIL.
end if
```

3.5 Formula for the Fourier expansion of f at width one cusps: Part 1

First we recall some notations from [AWL78].

Definition 3.5.1. For a positive integer c', let $S'_c = \left(\begin{smallmatrix} 1 & \frac{1}{c'} \\ 0 & 1 \end{smallmatrix}\right)$. If χ is a character modulo c', we define the operator on modular forms

$$f|R_\chi(c') = \sum_{u=0}^{c'-1} \bar{\chi}(u) f|S^u_{c'}.$$

Write R_χ in short for $R_\chi(\mathrm{cond}(\chi))$. Note that $f|R_\chi = g(\bar{\chi})f_\chi$. Conversely, if $(a, M) = 1$, we have

$$\phi(c')S^u_{c'} = \sum_{\chi:cond(\chi)|c'} \chi(u)R_\chi(c'). \tag{3.5.1}$$

For our convenience, we define some operators, which are essentially the conjugates of S'_c and $R_\chi(c')$ by W_N. Let $A'_c = \left(\begin{smallmatrix} 1 & 0 \\ c' & 1 \end{smallmatrix}\right)$. Then it is easy to verify the following matrix identity.

Fact 3.5.2. $-N \cdot A^{-1}_{N/c'} = W_N S_{c'} W_N$.

From now on, we assume c is a divisor of N and $c' = \frac{N}{c}$. Then as operators on modular forms,

$$A^{-1}_c = W_N S_{c'} W_N.$$

Since $W^2_N = id$ as operators, we have

$$A^{-u}_c = W_N S^u_{c'} W_N, \ \forall u \in \mathbb{Z}.$$

Parallel to the notion of $R_\chi(c')$, let $\Phi_\chi(c) = \sum_{u=0}^{c'-1} \bar{\chi}(u) A^{-u}_c$.Then $\Phi_\chi(c) = W_N R_\chi(c') W_N$. Similar to Formula 3.5.1, we have

$$\varphi(c')A^{-a}_c = \sum_{\mathrm{cond}(\chi)|c'} \chi(a)\Phi_\chi(c) = \sum_{\mathrm{cond}(\chi)|c'} \chi(a) W_N R_\chi(c') W_N. \tag{3.5.2}$$

Applying Formula 3.5.2 to f, we arrive at

$$f_{[\frac{a}{c}]}(q) = \tfrac{1}{\varphi(c')} \textstyle\sum_{\mathrm{cond}(\chi)|c'} \chi(-a) f|W_N R_\chi(c') W_N. \tag{3.5.3}$$

$$= \tfrac{w(f)}{\varphi(c')} \textstyle\sum_{\mathrm{cond}(\chi)|c'} \chi(-a) f|R_\chi(c') W_N. \tag{3.5.4}$$

Now it left to compute the expansions of each $f|R_\chi(c')W_N$ in the sum.

3.6 Formula for the Fourier expansion of f at width one cusps: Part 2

In this section, we describe how to compute the expansion of $f|R_\chi(c')W_N$. First note that $T_p = U_p + \epsilon(p)p^{\frac{k}{2}}B_p$ as operators on $S_k(\Gamma_1(N), \epsilon)$. It follows that T_p commutes with B_d for any positive integer d.

We recall some notations and a result from [Del02].

Definition 3.6.1. [Del02, Definition III.2.4] For a Dirichlet character χ modulo $b = \prod_{j \in J} p_j^{\alpha_j}$. Let $r = |J|$. Decompose χ uniquely as $\chi = \chi_1 \cdots \chi_r$, where χ_i is a character modulo $p_j^{\alpha_j}$. We define $\mathrm{cond}'(\chi)$ multiplicatively, by putting

$$\mathrm{cond}'(\chi_j) = \begin{cases} \mathrm{cond}(\chi_j) & if\, \mathrm{cond}(\chi_j) > 1 \\ p_j & else \end{cases} \tag{3.6.1}$$

Also, if $I = \{j \in J : \chi_j \text{ is trivial character modulo } p_j^{\alpha_j}\}$, we put $tr = \prod_{j \in I} p_j^{\alpha_j}$ $nt = b/tr$, $\chi_{tr} = \prod_{j \in I} \chi_j$, and $\chi_{nt} = \chi/\chi_{tr}$. Then we set

$$g'(\chi) = (-1)^{|I|}\chi_{nt}(tr)g(\chi_{nt}). \tag{3.6.2}$$

Here $g(\chi)$ is the usual Gauss sum of χ: if χ is a character modulo d, then $g(\chi) = \sum_{a=1}^{d} e^{\frac{2\pi i a}{d}}\chi(a)$. If $\chi = \chi_0$ is the trivial character, we set $g(\chi_0) = 0$.

Lemma 3.6.2. *[Del02, Prop 2.6] Let c' be an integer such that $c'^2 \mid N$. For a Dirichlet character χ mod c', we have*

$$f|R_\chi(c') = \begin{cases} g'(\bar{\chi})f_{\chi_{nt}} & if\, \mathrm{cond}'(\chi) = c' \\ 0 & else. \end{cases}$$

Using this lemma, we can simplify formula 3.5.3 to

$$f_{[\frac{a}{c}]} = \frac{w(f)}{\varphi(c')} \sum_{\mathrm{cond}'(\chi) = c'} \chi(-a)g'(\bar{\chi})f_{\chi_{nt}}|W_N. \tag{3.6.3}$$

Next, we compute $f_{\chi_{nt}}$ by the following: suppose $g = f \otimes \chi_{nt}$. Then

$$f_{\chi_{nt}} = g| \prod_{i=1}^{r} K_{p_i}. \tag{3.6.4}$$

Moreover, we have

$$K_p = 1 - U_p B_p = \begin{cases} 1 - (T_p - \chi_{nt}^2(p) p^{\frac{k}{2}} B_p)|B_p & p \nmid M \\ 1 - T_p|B_p & p \mid M \end{cases}. \tag{3.6.5}$$

Using the commutativity of T_* and B_*, we can write $f_{\chi_{nt}}$ in the form $\sum c_i (f \otimes \chi)(q^{d_i})$, where c_i and d_i are constants. To give a precise formula, we use the following notation. For a finite set S of integers, let $\pi(S) = \prod_{s \in S} s$ denote the product of all elements in S. For a Dirichlet character χ of conductor d, let S_χ be the set of prime divisors of d. For any positive integer M and any finite set of integers S, define

$$\mathcal{B}_{S,M} = \{(S_1, S_2) \in (2^{\mathbb{Z}})^2 | S_1, S_2 \subseteq S, S_1 \cap S_2 = \emptyset, \gcd(M, \pi(S_2)) = 1\} \tag{3.6.6}$$

Proposition 3.6.3. *Let $k \geq 2$ be an even integer and let f be a newform in $S_k(\Gamma_0(N))$. Then*

$$f_{\chi_{nt}} = \sum_{(S_1,S_2) \in \mathcal{B}_{S_\chi,M}} (-1)^{|S_1|} a_{\pi(S_1)}(g_\chi) \pi(S_2)^{k/2} \chi_{nt}^2(\pi(S_2)) g_\chi | B_{\pi(S_1)\pi(S_2)^2}.$$

Here $g_\chi = f \otimes \chi$, M is the level of g_χ and $\mathcal{B}_{S_\chi,M}$ is as in 3.6.6.

Proof. This is a direct consequence of multiplying out 3.6.4 using 3.6.5, using the fact that T_p commutes with B_d, and noting that T_p acts as multiplication by $a_p(g_\chi)$ on g_χ. $\square$

Theorem 3.6.3 will be our starting point of computing the expansion of f at width one cusps. We will use it to compute $f_{\chi_{nt}}|W_N$. First we prove two lemmas.

Lemma 3.6.4. *Let f be a newform of even weight k on $\Gamma_1(M)$ and suppose d, N are positive integers such that $Md \mid N$. Then*

$$f|B_d|W_N = \left(\frac{N}{Md^2}\right)^{k/2} w(f) (f|B_{\frac{N}{Md}})^*.$$

Proof. Straightforward computation.

$$\begin{aligned}
f|B_d|W_N &= d^{-k/2} f| \left(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} 0 & -1 \\ N & 0 \end{smallmatrix}\right) \\
&= d^{-k/2} f| \left(\begin{smallmatrix} 0 & -1 \\ M & 0 \end{smallmatrix}\right) \left(\begin{smallmatrix} N/md & 0 \\ 0 & 1 \end{smallmatrix}\right) \left(\begin{smallmatrix} d & 0 \\ 0 & d \end{smallmatrix}\right) \\
&= \left(\frac{N}{Md^2}\right)^{k/2} f|W_M|B_{N/Md} \\
&= \left(\frac{N}{Md^2}\right)^{k/2} w(f) f^*|B_{N/Md} \\
&= \left(\frac{N}{Md^2}\right)^{k/2} w(f)(f|B_{N/Md})^*.
\end{aligned}$$

□

Before stating the second lemma, we quote another result in [Li75] on the coefficients of a newform at primes dividing the level.

Lemma 3.6.5. *[Li75, Theorem 3 (iii)] Let* $f = \sum_{n\geq 1} a_n(f)q^n$ *be a normalized newform in* $S_k(\Gamma_1(N), \epsilon)$ *and let* p *be a prime dividing* N*. Then*
(1) If ϵ *is a character modulo* N/p *and* $p^2 \mid N$*, then* $a_p(f) = 0$*.*
(2) If ϵ *is a character modulo* N/p *and* $p^2 \nmid N$*, then* $a_p(f)^2 = \epsilon(p)p^{k-2}$*.*
(3) If ϵ *is not a character modulo* N/p*, then* $|a_p(f)| = p^{\frac{k-1}{2}}$*.*

Lemma 3.6.6. *Keep the notations in Proposition 3.6.3. If* $(S_1, S_2) \in \mathcal{B}_{S_\chi, M_\chi}$ *is such that* $a_{\pi(S_1)}(g_\chi) \neq 0$*. Then* $M\pi(S_1)\pi(S_2)^2 \mid N$*.*

Proof. Let p be a prime divisor of $N' := M\pi(S_1)\pi(S_2)^2$. If $p \nmid M$, then $\mathrm{ord}_p(N') \leq \mathrm{ord}_p(\mathrm{cond}(\chi)^2) \leq \mathrm{ord}_p(N)$. So we assume $p \mid M$, hence $p \nmid p(S_2)$. If $p \nmid p(S_1)$, then there's nothing to prove; if $p \mid \pi(S_1)$, we want to show that $\mathrm{ord}_p(M) < \mathrm{ord}_p(N)$. Suppose not, then $\mathrm{ord}_p(M) = \mathrm{ord}_p(N) \geq 2\,\mathrm{ord}_p(\mathrm{cond}(\chi))$. Since $\mathrm{cond}(\chi^2) \leq \mathrm{cond}(\chi)$, we know χ^2 is a character modulo M/p. Applying case (1) of Lemma 3.6.5 to the newform g_χ, we see that $a_p(g_\chi) = 0$, hence $a_{\pi(S_1)}(g_\chi) = 0$ by multiplicativity. □

Now we can state our main theorem from this chapter.

Theorem 3.6.7. *Let $k \geq 2$ be an even integer and let f be a normalized newform in $S_k(\Gamma_0(N))$. Let z be a cusp on $X_0(N)$ of width one. Write $z = \left[\frac{a}{d}\right]$ such that* $\gcd(a,d) = 1$, *$d \mid N$ and $N \mid d^2$. Let $d' = \frac{N}{d}$. Then the Fourier expansion of f at the cusp z is*

$$f_z(q) = \frac{w(f)}{\varphi(d')} \sum_{\chi:\mathrm{cond}'(\chi)=d'} \chi(-a)g'(\bar{\chi})w(f \otimes \chi)f^!_\chi(q).$$

Here

- *$w(f)$ and $w(f \otimes \chi)$ are the pseudo-eigenvalues.*
- *$g'(\chi)$ is the modified Gauss sum defined in 3.6.2 .*
- cond' *is the modified conductor of a Dirichlet character in 3.6.1.*
- *$f^!_\chi$ is as follows: let M_χ denote the level of $f \otimes \chi$. Then*

  $$f^!_\chi = \sum_{(S_1,S_2)\in\mathcal{B}_{S_{\chi_{nt}},M_\chi}} (-1)^{|S_1|}a_{\pi(S_1)}(f\otimes\chi)\left(\frac{N}{M_\chi\pi(S_1)^2\pi(S_2)^3}\right)^{k/2}\chi^2(\pi(S_2))(f\otimes\chi|B_{\frac{N}{M_\chi\pi(S_1)\pi(S_2)^2}})^*$$

  where the notations follow 3.6.3.

Proof. We start from formula 3.6.3:

$$f_{[\frac{a}{c}]} = \frac{w(f)}{\varphi(c')} \sum_{\mathrm{cond}'(\chi)=c'} \chi(-a)g'(\bar{\chi})f_{\chi_{nt}}|W_N.$$

From 3.6.3, we have

$$f_{\chi_{nt}} = \sum_{(S_1,S_2)\in\mathcal{B}_{S_\chi,M_\chi}} (-1)^{|S_1|}a_{\pi(S_1)}(f\otimes\chi)\pi(S_2)^{k/2}\chi^2_{nt}(\pi(S_2))f\otimes\chi|B_{\pi(S_1)\pi(S_2)^2}.$$

To simplify notations, let $c(f,\chi,S_1,S_2) = (-1)^{|S_1|}a_{\pi(S_1)}(f\otimes\chi)\pi(S_2)^{k/2}\chi^2_{nt}(\pi(S_2))$. Then

$$\begin{aligned} f_{\chi_{nt}}|W_N &= \sum_{(S_1,S_2)\in\mathcal{B}_{S_\chi,M_\chi}} c(f,\chi,S_1,S_2)f\otimes\chi|B_{\pi(S_1)\pi(S_2)^2}W_N \\ &= \sum_{(S_1,S_2)\in\mathcal{B}_{S_\chi,M_\chi}} c(f,\chi,S_1,S_2)\left(\frac{N}{M_\chi(\pi(S_1)\pi(S_2)^2)^2}\right)^{k/2} w(f\otimes\chi)(f\otimes\chi|B_{\frac{N}{M_\chi\pi(S_1)\pi(S_2)^2}})^* \\ &= w(f\otimes\chi)f^!_\chi. \end{aligned}$$

Note that we applied Lemma 3.6.4 to obtain the penultimate equality, and we could do that because of Lemma 3.6.6. Now the result follows. $\square$

Theorem 3.6.7 gives us an algorithm to compute the expansion of f_z, which we will describe below. But first, we take a closer look at what ingredients goes into the expansion. Given a newform $f \in S_k(\Gamma_0(N))$ and a width one cusp z of denominator c. We need to consider the twist of f by all Dirichlet characters of conductor dividing c. For each such character χ, we then need to determine the level M_χ and q-expansion of the newform $f \otimes \chi$, the latter boils down to knowing $a_p(f \otimes \chi)$ for all primes $p \mid \mathrm{cond}(\chi)$. Then we need to compute the pseudo-eigenvalues of $f \otimes \chi$. Finally, we combine these information together and apply Throem 3.6.7 to compute f_z.

Algorithm 6 Computing Fourier coefficients of f at width one cusps

Input: $f \in S_k(\Gamma_0(N))$ a newform; a, c – coprime integers such that $N \mid c^2$; B – a positive integer.

Output: The first B Fourier coefficients of $f_{\left[\frac{a}{c}\right]}(q)$.

1: $c' \leftarrow N/c$. $X \leftarrow$ The set of all Dirichlet characters χ such that $\mathrm{cond}'(\chi) = c'$.
2: compute $w(f)$ using Algorithm 5.
3: **for** χ in X **do**
4: Using Algorithm 4, compute the level M_χ and the q-expansion of $g_\chi := f \otimes \chi$ to B terms.
5: Compute $w(g_\chi)$ using Algorithm 5.
6: **end for**
7: Apply Theorem 3.6.7 to compute f_z to B terms.

3.7 A Converse Theorem

Given the work in previous sections, it is a natural question then to ask whether the information on twists of f is uniquely determined by the expansion of f at width one cusps. The answer is yes, and the precise statement is in the following theorem.

Theorem 3.7.1. *Let f be a normalized newform in $S_k(\Gamma_0(N))$. Assume the eigenvalue $w_N(f)$ is known. Suppose c is a positive divisor of N such that $N \mid c^2$. Then the expansions of f_z, where z runs through all cusps of denominator c, uniquely determines the following: for each Dirichlet character χ of such that* $\mathrm{cond}'(\chi) = c'$, *the level M_χ, the pseudo-eigenvalue w_{M_χ} and the q-expansion of the newform $f \otimes \chi$.*

Proof. By plug in different a's. We can solve for t_χ. Consider the first nonzero term of t_χ. Suppose

$$t_\chi = u_\chi q^{v_\chi} + O(q^{v_\chi+1}),\ u_\chi \neq 0.$$

Assuming that χ has prime power conductor $p^\beta > 1$, we claim that

$$\left|\frac{v^{k/2}}{u}\right| = \begin{cases} p^{k/2} & if p \nmid M_\chi \\ p^{1/2} & if p \mid M_\chi \text{ and } a_p(g) \neq 0 \\ 1 & else \end{cases} \cdot$$

Proof of claim: the first and third case are easy to verify using Theorem 3.6.7. Now assume $p \mid M$ and $a_p(g_\chi) \neq 0$. By Lemma 3.6.5, we have $|a_p(g_\chi)| = p^{k/2-1/2}$ or $p^{k/2-1}$. However, $|a_p(g_\chi)| = p^{k/2-1}$ only if $p \mid\mid M_\chi$ and χ^2 is a character modulo M_χ/p. This means χ^2 is the trivial character. By Lemma 3.3.2, we compute the p-level of $f = g_\chi \otimes \bar{\chi}$: note that $\max p, p^{\alpha+\beta}, p^{2\beta} > p$, so (ii) applies and the p-level of f is equal to $\max(p^\alpha, p^\beta) = p^\beta$, i.e., $\mathrm{ord}_p(N) = \beta$. This is impossible since we have $p^{2\beta} = \mathrm{cond}(\chi)^2 \mid N$.

Therefore, we have $|a_p(g_\chi)| = p^{k/2-1/2}$ and the claim follows.

Since $k \geq 2$, we could determine which case we are in. Then we can read off M_χ and $w_M(g_\chi)$. For example, if we are in the second case, then the level can be computed via $M_\chi = \frac{N}{v_\chi p}$. Now the N/M_χ's coefficient of t_χ is

$$\begin{aligned} a_{\frac{N}{M}}(t_\chi) &= w(g_\chi)(\tfrac{N}{M})^{k/2}(1 - |a_p(g_\chi)|^2 \chi^2(p) p^{-k/2}) \\ &= w(g_\chi)(\tfrac{N}{M})^{k/2}(1 - p^{k/2-1}\chi^2(p)). \end{aligned}$$

This allows us to solve $w(g_\chi)$. Finally, we compute $a_p(g_\chi)$ by $a_p(g) = \frac{-u_\chi}{w(g_\chi)\chi^2(p)(\frac{N}{Mp})^{k/2}}$. The value $a_p(g)$ determines the expansion of g_χ. Recursively, we could solve for all pn-coefficients of g_χ, from which we deduce it complete q-expansion.

In the general case, we consider the following subsets of S_χ. Let $S_1^* = \{p \in S_\chi : p \mid M\}$, $S_2^* = S_\chi \setminus S_1^*$, and $\widetilde{S_1^*} = \{p \in S_1^* : a_p(g_\chi) \neq 0\}$.

It follows that the leading term of t_χ belongs to the summand corresponding to $(\widetilde{S_1^*}, S_2^*)$ in Theorem 3.6.7. Still writing the leading term as $u_\chi q^{v_\chi}$, we have

$$u_\chi = w(g_\chi)\chi^2(p(S_2))a_{p(\widetilde{S_1^*})}(g_\chi)p(\widetilde{S_1^*})^{-k}(p(S_2^*)^{-3k/2}\left(\frac{N}{M_\chi}\right)^{k/2}, v_\chi = \frac{N}{M_\chi p(\widetilde{S_1^*})p(S_2^*)^2}.$$

Similar to the prime power conductor case above, we have $|a_{p(\widetilde{S_1^*})}(g_\chi)| = p(\widetilde{S_1^*})^{k/2-1/2}$. So

$$|v_\chi^k u_\chi^{-2}| = p(\widetilde{S_1^*})p(S_2^*)^2. \tag{3.7.1}$$

Hence we can factor $|v_\chi^k u_\chi^{-2}|$ and obtain $p(\widetilde{S_1^*})$ and $p(S_2^*)$. Then M_χ can be solved using v_χ. Plug it back into u_χ, we obtain $a_{p(\widetilde{S_1^*})}w(g_\chi)$. Finally, for each $p \in \widetilde{S_1^*}$, the $v_\chi p$'s coefficient of t_χ allows us to compute $a_{p(\widetilde{S_1^*})/p}(g_\chi)w(g_\chi)$. These together determines $w(g_\chi)$ and $a_{p(\widetilde{S_1^*})}$. The other Fourier coefficients of g_χ can then be computed recursively. □

3.8 *Field of definition*

In the previous sections, we have described an algorithm to compute the Fourier coefficients of f_z as complex numbers. In fact, the Fourier coefficients are algebraic numbers. More precisely, if d is the denominator of z and $d' = N/d$, then $f_z(q) \in K_f(\zeta_{d'})[[q]]$. Here K_f is the number field generated by the Fourier coefficients of f (at the cusp ∞). In this section, we provide a proof of this fact.

Lemma 3.8.1 ([Ste12b]). *(1) The cusps of $X_0(N)$ are rational over the field $\mathbb{Q}(\zeta_N)$.*
(2) For $s \in (\mathbb{Z}/N\mathbb{Z})^*$, let $\tau_s \in Gal(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ be defined by $\tau_s(\zeta_N) = \zeta_N^s$. Then

$$\tau_s\left(\left[\frac{a}{y}\right]\right) = \left[\frac{a}{ys'}\right],$$

where $s' \in \mathbb{Z}$ is chosen so that $ss' \equiv 1 \mod N$.

Using the lemma above, we can obtain a precise description of cusps of the same denominator d. We summarize the facts in the following proposition.

Proposition 3.8.2. *Let d be a positive divisor of N and let $d' = N/d$. Then*
(1) The cusps of denominator d on $X_0(N)$ are defined over the field $\mathbb{Q}(\zeta_{d'})$.

(2) Let $\tau_s \in Gal(\mathbb{Q}(\zeta_{d'}/\mathbb{Q}))$ be the map $\tau_s : \zeta_{d'} \to \zeta_{d'}^s$. Then

$$\tau_s\left([\frac{a}{d}]\right) = \left[\frac{a}{ds'}\right],$$

where $s' \in \mathbb{Z}$ is chosen so that $ss' \equiv 1 \mod d'$.

Proof. From part (2) of Lemma 3.8.1, we see that if c is a cusp of denominator d and $s \equiv 1 \mod d'$, then $\tau_s(c) = c$. The claims now follow directly from this observation. □

Proposition 3.8.3. *We have*
(1) $\mathbb{Q}(\{a_n(f_c)\}) \subseteq \mathbb{Q}(\{a_n(f)\}, \zeta_{d'})$.
(2) Let $\sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ be such that $\sigma|_{\mathbb{Q}(\zeta_N)} = \tau_s$. Then

$$(f_c)^\sigma = (f^\sigma)_{\tau_s(c)}.$$

Proof. First, (1) follows from (2), for if σ fixes $\mathbb{Q}(\{a_n(f)\}, \zeta_{d'})$, then $f^\sigma = \sigma$ and $\tau_s(z) = z$. To prove (2), let g be a meromorphic modular form of weight k, level 1, and rational Fourier coefficients (for example, one can choose $g = (\mathrm{d}j)^{k/2}$). Then it suffices to prove the claim for f/g, since $g|_k\gamma = g$ for all $\gamma \in SL_2(\mathbb{Z})$. Now f/g is a rational function on $X_0(N)$. Since the function field of $X_0(N)$ is generated by j and j_N, So we may write write $f/g = P(j, j_N)/Q(j, j_N)$, where $P, Q \in K_f[x, y]$. Now fix$\gamma_c \in SL_2(\mathbb{Z})$ such that $\gamma_c(\infty) = c$. Since $j|\gamma_c = j$, it suffices to prove the claim for j_N. WLOG, we can assume $\gamma_c = \left(\begin{smallmatrix} 1 & ld \\ 0 & 1 \end{smallmatrix}\right)$, where $d = d_z$ and $\gcd(l, N) = 1$. Then $j_N|\gamma_c = j(N\gamma_c(z)) = j(\frac{dz+l'}{d'}) = \sum a_n(j)e^{2\pi i\frac{l'}{d'}}q^{nd/d'}$, where l' is an integer such that $l'l \equiv 1 \mod d'$. Hence for σ in (2), we have $(j_N|\gamma_c)^\sigma = \sum a_n(j)e^{2\pi i\frac{l's}{d'}}q^{nd/d'}$. On the other hand, we compute $(j_N^\sigma)_{\tau_s(c)} = (j_N)_{\tau_s(c)} = j_N|\left(\begin{smallmatrix} 1 & lds' \\ 0 & 1 \end{smallmatrix}\right) = \sum a_n(j)e^{2\pi i\frac{l'}{d'}}q^{nd/d'}$. So $(j_N|\gamma_c)^\sigma = (j_N^\sigma)_{\tau_s(c)}$. Hence the same claim for f holds. □

3.9 Examples

Let $E =$ **50a** and consider the 4 cusps of denominator 10 on $X_0(50)$. The corresponding first terms of q-expansions at these cusps are

$$\begin{aligned} a_1(f, \frac{1}{10}) &= \frac{1}{5}\zeta_5^3 - \frac{3}{5}\zeta_5^2 + \frac{3}{5}\zeta_5 - \frac{1}{5} \\ a_1(f, \frac{3}{10}) &= \frac{3}{5}\zeta_5^3 + \frac{6}{5}\zeta_5^2 + \frac{4}{5}\zeta_5 + \frac{2}{5} \\ a_1(f, \frac{7}{10}) &= \frac{2}{5}\zeta_5^3 - \frac{1}{5}\zeta_5^2 - \frac{4}{5}\zeta_5 - \frac{2}{5} \\ a_1(f, \frac{9}{10}) &= -\frac{6}{5}\zeta_5^3 - \frac{2}{5}\zeta_5^2 - \frac{3}{5}\zeta_5 - \frac{4}{5}. \end{aligned}$$

As another examples, let $E =$ **98a** and $z = [\frac{1}{14}]$. We computed numerically that

$$\begin{aligned} f_c(q) = {} & (-0.755001687308946 - 0.172324208281817i)\, q + (0.441471704846525 - 0.916725441095080i)\, q^2 \\ & + (1.39294678431094 + 1.11083799261729i)\, q^3 + (0.696473392155471 - 0.555418996308649i)\, q^4 \\ & + (1.51000337461789 - 0.344648416563641i)\, q^6 + \left(-3.80647894157196 \times 10^{-16} - 3.02371578407382i\right) q^7 \\ & + (0.755001687308946 + 0.172324208281817i)\, q^8 + (-0.441471704846525 + 0.916725441095080i)\, q^9 + \\ & (-0.882943409693050 - 1.83345088219016i)\, q^{12} + (-3.02000674923578 + 0.689296833127282i)\, q^{13} \\ & + \left(3.80647894157196 \times 10^{-16} + 3.02371578407382i\right) q^{14} + O(q^{15}) \end{aligned}$$

3.10 Automorphic representations; norm of first terms

References: [BH06], [LW10]. [Bru12]. [Kra90]. [JL72].

In this section, we will restrict ourselves to the case when the Fourier coefficients of f are rational numbers. Then f induces an admissible reprensetation π_f of $GL_2(\mathbb{A}_{\mathbb{Q}})$. We will see that the expansion of f at all cusps can also be computed from the local component $\pi_{f,p}$. Loeffler and Weinstein gave an algorithm to compute such local components.

We will restrict ourselves to the simplest case when f is twist-minimal, which means that the conductor of π_f is the smallest among all twists $\pi_{f\otimes\chi}$.

We will follow the notations of David Loeffler and use the formula of [Bru12].

Let z be a width one cusp of denominator c. Then the first coefficient $a_1(f_z)$ is an element in $K_f(\zeta_{c'})$. For simplicity, we assume that $c' = p^\alpha$ is a prime power. It can be proved using automorphic representations + local langlands correspondence that there exists β such that $p^\beta a_1(f_z) \in \bar{\mathbb{Z}}$. One question is: what prime ideals appears in the prime factorisation of $(a_1(f,z))$? It seems from our numerical data, that

$$\mathrm{ord}_{\mathfrak{q}}(a_1(f_z)) > 0 \implies \mathfrak{q} \cap \mathbb{Z} \equiv \pm 1 \pmod{p}.$$

The following is a table of data.

3.10.1 Cuspidal local constants

We keep the assumptions that f is a newform attached to an elliptic curve $E/\mathbb{Q}$ and f is twist-minimal. Assume p is a prime dividing the conductor N of E such that $v_p(N) = 2$. Then there exists a character $\varphi : \mathbb{F}_{p^2}^\times \to \mathbb{C}^\times$ which determines $\pi_{f,p}$. We will prove

Lemma 3.10.1. *Let $\psi : \mathbb{Q}_p \to \mathbb{C}^\times$ be a character of level one (e.g. $\psi(x) = e(\{\frac{x}{p}\}_p)$). Then*

$$\epsilon(\pi_{f,p}, 1/2, \psi) = \frac{-1}{p} \sum_{x \in \mathbb{F}_{p^2}^\times} \psi(x + x^p)\varphi(x).$$

If χ is a Dirichlet character such that the $f \otimes \chi$ has the same level as f. Then

$$\epsilon(\pi_{f\otimes\chi,p}, 1/2, \psi) = \frac{-1}{p} \sum_{x \in \mathbb{F}_{p^2}^\times} \psi(x + x^p)\varphi(x)\bar{\chi}(x^{p+1}).$$

Proof. By [BH06], taking $n = r = 1$, we have

$$p^2 \epsilon(\pi_{f,p}, 1/2, \psi) \cdot \mathrm{id} = \sum_{x \in GL_2(\mathbb{F}_p)} \psi(tr(x))\pi_{f,p}^\vee(x). \tag{3.10.1}$$

where $\pi_{f,p}^\vee$ denotes the contragredient representation. The representation $\pi_{f,p}$ has dimension $(p-1)$. Taking traces, we obtain

$$p^2(p-1)\epsilon(\pi_{f,p}, 1/2, \psi) \cdot \mathrm{id} = \sum_{x \in GL_2(\mathbb{F}_p)} \psi(tr(x))Tr(\pi_{f,p}^\vee(x)). \tag{3.10.2}$$

By assumption, $\pi_{f,p}$ arises from a cupsidal representation of the finite group $GL_2(\mathbb{F}_p)$, which is in turn induced from φ. (See Fulton-Harris), we have formulae for $Tr(\pi^\vee_{f,p}(x))$. Splitting the sum corresponding to four types of conjugacy classes, we computed $S_1 = (p-1)\sum_{x\in\mathbb{F}_p^\times}\psi(2x)$, $S_2 = (p^2-1)\sum_{x\in\mathbb{F}_p^\times}\psi(2x)(-1)$, $S_3 = 0$, and $S_4 = (p^2-p)/2\sum_{x\in\mathbb{F}_{p^2}\setminus\mathbb{F}_p}\psi(tr(x))(\overline{\varphi(x)+\varphi(x^p)})$. So the sum on the right hand side of 3.10.2 equals $(p-p^2)\sum_{x\in\mathbb{F}_{p^2}^\times}\psi(tr(x))\overline{\varphi(x)}$. Dividing by $p^2(p-1)$ gives the formula.

□

Moreover, since E is defined over $\mathbb{Q}$, the character of $\pi_{f,p}$ takes rational values. Hence the order of φ is 3,4 or 6. The local Langlands correspondence claims that the order of φ is equal to the order of the inertia subgroup of $Gal(L/\mathbb{Q})$, where L is the smallest number field over which E acquires good reduction (to-do: check this). The case $p \geq 5$ is easy, as we have the following lemma:

Lemma 3.10.2. *[Kra90, Proposition 1] Let Δ denote the minimal discriminant of E. Then for $p \geq 5$, the order of φ is equal to $\frac{12}{\gcd(12, v_p(\Delta))}$.*

We remark that for $p = 2$ or 3, the order of φ can be determined using results of [Kra90].

We remark that for elliptic curves, $v_2(N)$ is at most 8 and $v_3(N)$ is at most 5. For the sake of simplicity, we do not treat the case when $v_p(N) > 2$ here, but we point out the local constants can be also computed from formula in [BH06], once the local component is determined using [LW10].

Example 3.10.3. An example with trivial central character. Let f be the newform attached to $E =$ **121a**. Using Sage, we computed $w(f) = -1$. Since the weight of f is 2, we know $\epsilon_\infty = -1$ (since the central character of π_f is trivial, the level of the additive character ψ_∞ does not matter). The discriminant of E is $\Delta = -121$, so φ has order 6. Using Lemma 3.10.1, we computed that $\epsilon_{11}(\pi_{f,11}, 1/2) = -1$. This verifies $w(f) = -\prod_{p\leq\infty}\epsilon_p$.

Example 3.10.4. We give an example with nontrivial central character. Let f be as in the previous example, and let χ be the Dirichlet character of $\mathbb{F}_{11}^\times$ defined by $\chi(2) = e^{2\pi i/10}$.

Lemma 3.10.1 gives

$$\epsilon_{11}(\pi_{f\otimes\chi,11}, 1/2) = 0.64.. + 0.76..i$$

an algebraic number with miminal polynomial $x^{20}+109/121x^15+2861/1331x^10+109/121x^5+1$. So $w = -\epsilon_{11}\epsilon_\infty = \epsilon_{11}$. Using the numerical Algorithm 5, we compute $w(f \otimes \chi) = 0.642573377564283 + 0.766224154177894i$. This confirms the computation.

3.11 Norm of first terms computations

We keep the assumptions from the previous section, that f is a newform in $S_2(\Gamma_0(N))$, attached to an elliptic curve $E/\mathbb{Q}$. We assume f is twist-minimal and $p \geq 5$ is a prime dividing the conductor N such that $v_p(N) = 2$. In this case, the cusp $z_p = \left[\frac{-p}{N}\right]$ is of width one, and the q-expansion of f at z_p takes an especially simple form. We summarize this in the lemma below.

Lemma 3.11.1. *With the assumptions above, there exists a Galois-invariant set of numbers* $\{b_1, \ldots, b_{p-1}\} \subseteq \mathbb{Q}(\zeta_p)$*, such that*

$$f_{z_p}(q) = \sum_{n\geq 1} a_n(f) b_{n \mod p} q^n.$$

More precisely, the b_j *are given by*

$$b_j = w(f) \sum_{\chi:\mathrm{cond}(\chi)=p} g(\bar{\chi}) w(f \otimes \chi)\chi(n)$$

Proof. First, the assumptions imply that $a_n(f) = 0$ if $p \mid n$. So the right hand side of the formula is well-defined. The formulae then follow directly from Theorem 3.6.7. We have $b_j \in \mathbb{Q}(\zeta_p)$ since the cusp z_p is defined over $\mathbb{Q}(\zeta_p)$, by Proposition 3.8.3. Moreover, the cusps $\{z_p^{(j)} = \frac{-jp}{N} : 1 \leq j \leq p-1\}$ form a Galois orbit on $X_0(N)$, and one has

$$a_n(f_{z_p^{(j)}}) = a_{jn}(f_{z_p}), \forall n \geq 1, 1 \leq j \leq p-1.$$

In particular, we have $\{b_j\} = \{a_1(f_{z_p^{(j)}})\}$. Since the latter set is Galois-invariant, so is the former. $\square$

We remark that it is clear from the formula of b_j that they are algebraic number. However, the formula does not imply directly that they lie in $\mathbb{Q}(\zeta_p)$.

We give another formula of $a_1(f_{z_p})$ in light of the previous section.

Lemma 3.11.2. *Keeping the assumptions in the previous two sections, we have*

$$a_1(f_{z_p}) = \frac{\sum_{x\in\mathbb{F}_{p^2}^\times} \psi(x+x^p+x^{p+1})\varphi(x)}{\sum_{x\in\mathbb{F}_{p^2}^\times} \psi(x+x^p)\varphi(x)}.$$

Proof. In this special case, formula [] simplifies to

$$\begin{aligned} a_1(f_{z_p}) &= w(f) \sum_{\chi:\mathrm{cond}(\chi)=p} g(\bar{\chi}) w(f\otimes\chi) \\ &= \sum_{\chi:\mathrm{cond}(\chi)=p} g(\bar{\chi}) w(f\otimes\chi) w(f)^{-1} \,(\text{since } w(f)^2=1) \\ &= \sum_{\chi:\mathrm{cond}(\chi)=p} g(\bar{\chi}) \frac{\epsilon_p(\pi_{f\otimes\chi}, 1/2, \psi)}{\epsilon_p(\pi_f, 1/2, \psi)}. \end{aligned}$$

We explain the last equality: first we have $w(f) = \prod_{l\leq\infty} \epsilon_l(\pi_{f,l}, 1/2, \psi)$ and $w(f\otimes\chi) = \prod_{l\leq\infty} \epsilon_l(\pi_{f\otimes\chi,l}, 1/2, \psi)$. Since χ has conductor p, we know the epsilon factors are the same except for $l=p$. Hence $\frac{w(f\otimes\chi)}{w(f)} = \frac{\epsilon_p(\pi_{f\otimes\chi},1/2,\psi)}{\epsilon_p(\pi_f,1/2,\psi)}$.

Now by a formula in [Bru], we have

$$\sum_{\chi:\mathrm{cond}(\chi)=p} g(\bar{\chi})\epsilon_p(\pi_{f\otimes\chi}, 1/2, \psi) = \frac{-1}{p} \sum_{x\in\mathbb{F}_{p^2}^\times} \psi(x+x^p+x^{p+1})\varphi(x).$$

This combined with our Lemma 3.10.1 gives the result. □

Example 3.11.3. Let f be the newform attached to $E = \mathbf{49a}$. One checks that f is twist-minimal and φ has order 4. Using Lemma 3.11.2, we computed

$$a_1(f_{-1/7}) = -\frac{5}{7}\zeta_7^5 - \frac{3}{7}\zeta_7^4 - \frac{1}{7}\zeta_7^3 + \frac{1}{7}\zeta_7^2 + \frac{3}{7}\zeta_7 - \frac{2}{7} = 0.623489... + 1.29468...i.$$

The numerical algorithm gives $a_1(f_{-1/7}) = 0.623489801858733... + 1.29468991410431...i$. Hence our formulae are consistent for this example.

3.11.1 A result linking first term to critical polynomials

One motivation to study the factorization of $a_1(f_{z_p})$ as a principal fractional ideal in $\mathbb{Q}(\zeta_p)$ is that they relate to critical points of modular parametrizaiton of E in the following way:

Theorem 3.11.4. *Suppose there exists a prime ideal $\mathfrak{q}$ in $\mathbb{Q}(\zeta_p)$ lying above a prime $q \neq p$, such that $\mathfrak{q} \mid a_1(f_{z_p)}$ and $\mathrm{ord}_{\mathfrak{q}}(a_1(f_{z_p})) < \frac{p-1}{2}$. Then $F_{E,j}(x)$ is not integral at q.*

To prove the theorem, first we make some preparations in p-adic analysis. Let p be a prime, $\mathbb{C}_p$ be a completion of a choice of $\bar{\mathbb{Q}}_p$. Let q be a formal variable. Let ord_p denote the p-adic valuation on $\mathbb{C}_p$ and let $D(1)$ denote the open unit disk

$$D(1) = \{x \in \mathbb{C}_p : \mathrm{ord}_p(x) > 0\}.$$

Lemma 3.11.5. *Let $f = 1 + \sum a_n q^n \in \mathbb{C}_p[[q]]$ be such that f converges on $D(1)$. Then the following are equivalent:*
(1) there exists some i such that $\mathrm{ord}_p(a_i) < 0$.
(2) there exists $\alpha \in D(1)$ with $f(\alpha) = 0$.

Proof. Consider the first segment of the Newton polygon of f. Assume (1) then the segment is necesarily finite, since otherwise f does not . Hence by a theorem on Newton polygon, we have (2); now assume that (2) holds. Let $\lambda = -\mathrm{ord}_p(\alpha) < 0$. Assume towards contradiction that (1) is false. Let N be the total horizontal length of all segments of $N(f)$ with slope $\leq \lambda$. The assumption then implies $N = 0$. Hence by Weierstrass preparation theorem, we know f is nonzero on the closed disc $D(|\alpha|_p^+)$, a contradiction to (2). □

Proposition 3.11.6. *Suppose $K/\mathbb{Q}_p$ is a finite extension with uniformizer π. Let $f_j : 1 \leq j \leq n$ be power series with constant terms one and let $F = \prod_j f_j$. Suppose there exists i such that $\mathrm{ord}_\pi(a_i(f_1)) < 0$. Then there exists an index $i' \geq 1$ such that $\mathrm{ord}_\pi(a_{i'}(F)) < 0$.*

Proof. By Lemma 3.11.5, the condition implies that f_j converges on $D(1)$ for all j and f_1 has a root in $D(1)$. Since F is the product of the f_j's, we know that F has a root in $D(1)$. Hence the claim follows, again using Lemma 3.11.5. □

Fix a prime $\mathfrak{p}$ above p in $\bar{\mathbb{Q}}$. We say a laurent series $f \in \bar{\mathbb{Q}}((q))$ is called integral at p if $f = q^s(1 + \sum_{n\geq 1} a_n q^n)$ with $\mathrm{ord}_p(a_n) \geq 0$ for all n. One sees that if f is integral, then $\frac{1}{f}$ is also integral. Product of two integral power series is integral. We similarly define the notion for a monic polynomial $F[x] \in \mathbb{Q}[x]$ to be integral at p.

Let $K/\mathbb{Q}$ be a cyclic extension with Galois group G. Let $n = [K : \mathbb{Q}]$. Let l be a prime, unramified in K. Let $I \subseteq \mathcal{O}_K$ be an ideal whose norm is a power of l, and let $H = \{\sigma \in G : \sigma(I) = I\}$ be the stabilizer of I under the action of G.

Lemma 3.11.7. *Assume that H contains G^2, i.e., the subgroup of squares in G. Then $\mathrm{ord}_l(Norm(I)) \geq n/2$.*

Proof. Really we have two cases: $H = G$ and $H = G^2$. In the first case, I is necessarily a power of l. Hence $\mathrm{ord}_l(Norm(I)) \geq n$ indeed; in the second case, Let $\mathfrak{l}_1, \ldots, \mathfrak{l}_g$ denote the primes above l. Since G is abelian, we know $Stab(\mathfrak{l}_i) = Stab(\mathfrak{l}_1)$ for any i, so let H_0 denote that stabilizer. The action of G/H_0 on the set $\{\mathfrak{l}_1, \ldots, \mathfrak{l}_g\}$ provides an embedding it as a cyclic subgroup of S_g, generated by a g-cycle τ. If g is odd; then τ^2 is another g-cycle, so it does not fix any proper subset of $\{1, 2, \ldots, g\}$, so again I is divisible by l; suppose g is even, then τ^2 factors as a product of two $(g/2)$-cycles s_1 and s_2. WLOG $s_1 = (135 \cdots g-1)$. Then $I = (\mathfrak{l}_1\mathfrak{l}_3 \ldots \mathfrak{l}_{g-1})^t$ for some positive integer t. Hence $Norm(I) = l^{nt/2} \geq l^{n/2}$. This completes the proof. □

Lemma 3.11.8. *For any prime p, $F_{E,j}$ is integral at p if and only if* $\mathrm{Norm}(f)$ *is integral at p.*

Proof. Note that $\mathrm{Norm}(f)$ is integral at p if and only if $F_f(q)$ is . Now we use the fact that $F_{E,j}(j(q)) = F_f(q)$. Suppose $F_{E,j}$ is integral at p. Since $j(q)$ is integral at p, the coefficients of $F_f(q)$ have nonnegative valuations. Moreover, since $F_{E,j}(x)$ is monic, the leading coefficient of $F_f(q)$ is 1. Hence $F_f(q)$ is integral at p. Now assume that $F_f(q)$ is integral at p. By examining Algorithm 1, we see that the coefficients of $F_{E,j}$ lies in the ring generated over $\mathbb{Z}$ by the coefficients of F_f and coefficients of j. In particular, $F_{E,j}$ is integral at p. □

Proposition 3.11.9. *Let $b_1, \ldots, b_{p-1}$ be the "first terms" in our case. Assume for some prime l we have*

$$0 < \mathrm{ord}_l(Norm(b_1)) < \frac{p-1}{2}.$$

Then $Norm(f)$ is not integral at l.

Proof. Since $\prod_{cuspz} \tilde{f}_z$ divides $\mathrm{Norm}(f) = \prod \widetilde{f|A_i}$, by Lemma 3.11.5, the claim will follow if we can show there exists z and a prime ideal $\mathfrak{l}$ such that the normalized series $\tilde{f}_z(q) = \sum a_n b_n / b_1 q^n$ has a non-$\mathfrak{l}$-integral coefficient. So let us assume that this is not the case. Let I be the l-part of the principal ideal (b_1), and let $H \leq G = (\mathbb{Z}/p\mathbb{Z})^\times$ denote the stablizer of I. The assumption implies that H does not contain G^2. Hence there exists an integer m such that (1) m is a square modulo p; (2) $\sigma_m(I) \neq I$; (3) $j \mod p \notin H$. Pick such an integer m and set $c_m = b_m/b_1$. Then from (2) we see that there exists some prime ideal $\mathfrak{l}$ above l such that $\mathrm{ord}_{\mathfrak{l}}(c_m) < 0$. By Dirichlet's theorem on primes in arithmetic progressions, we can find a prime $r \neq l$ such that $l'^2 \equiv m \mod p$. Then $r \mod p \notin H$. Hence there exists some prime $\mathfrak{l}'$ above l such that $\mathrm{ord}_{\mathfrak{l}'}(c_r) < 0$. Recall that for any n we have $a_n(f_z) = a_n(f) c_{n \mod p}$. Suppose towards contradiction that $\tilde{f}_z(q)$ is l-integral. Then $a_r(f)$ and $a_{r^2}(f)$ must be both divisible by l. But $a_{r^2} = a_r^2 - r$, so $r = l$, a contradiction. □

Now we can see that Theorem 3.11.4 is a direct consequence of Proposition 3.11.9 and Lemma 3.11.8.

3.11.2 Data

From the above discussion, we see that there are at most three possibilities for each p, corresponding to the order of φ being 3,4 or 6.

Consider $N_{f,p} = Norm(a_1(f_{z_p})) \in \mathbb{Z}$. It is easy to show that we always have $p \mid N_{f,p}$. The following is a table of the prime divisors of the norm, when such primes exist.

As an observation, we found that the primes l in the third column of the above table all satisfy a congruence relation

$$l \equiv \pm 1 \mod p.$$

Table 3.11.1: table of prime divisors $l \neq p$ of $N_{f,p}$

p	order of φ	primes $l \neq p, l \mid N_{f,p}$
17	3	509
19	4	37
23	3	1103
23	4	47
29	3	173
31	4	557
41	3	1209, 9103
41	6	163
43	4	4129
47	3	13034039
47	4	2819
53	3	107, 317, 8161
53	6	107
59	3	1061, 537173407
59	4	827, 42953
67	4	2143, 10853
71	3	634532719903
71	4	6613947917
71	6	3407
79	4	157, 232181473
83	3	167, 1110041, 142761594097
83	4	701553683
83	6	228913
89	3	508367, 146277136013
89	6	1069, 6053

It would be interesting to prove or disprove this in general.

Chapter 4

INDEX OF CHOW-HEEGNER POINTS

We consider a special case of the Chow-Heegner points that has a simple description due to Shouwu Zhang. Let E, F be nonisogenous elliptic curves defined over $\mathbb{Q}$ of the same conductor N. The Chow-Heegner point $P_{E,F} \in E(\mathbb{Q})$ is constructed by the following procedure: take any point on $F(\mathbb{C})$, take its inverse image on $X_0(N)$, then map that image down to E and take the sum the resulting points. In [DDLR15], Darmon, Daub, Lichtenstein and Rotger developed an algorithm to compute Chow-Heegner points via iterated integrals. In [Ste12a], Stein developed a fast and conceptually easy algorithm to numerically compute Chow-Heegner points. The following theorem is proved by Yuan-Zhang-Zhang in [YZZ11]:

Theorem 4.0.1 (Yuan-Zhang-Zhang)**.** *Let $L(E, F, F, s) = L(E, s)L(E, Sym^2(F), s)$. Assume that the local root numbers of $L(E, F, F, s)$ at every prime of bad reduction is +1 and that the root number at infinity is -1. Then*

$$\hat{h}(P_{E,F}) = (\star) \cdot L'(E, F, F, \frac{1}{2}),$$

where $(\star)$ is nonzero.

In particular, when the analytic rank of E is at least two, the Chow-Heegner point $P_{E,F}$ is torsion. When the rank of $E(\mathbb{Q})$ is one, we consider the index $i_{E,F} = [E(\mathbb{Q})/tors : \mathbb{Z}P_{E,F}]$. Theorem 4.0.1 combined with the Bloch-Kato conjecture on critical values of motivic L-functions suggests that this index might be linked to interesting arithmetic invariants related to E and F.

Numerical evidence in [Ste12a] suggests that the index $i_{E,F}$ is always divisible by 2, when it is finite. I proved the following theorem.

Theorem 4.0.2. *Let $\sigma_0(N)$ denote the number of distinct prime factors of N. If*

$$\sigma_0(N) > \log_2(\#E[2](\mathbb{Q})) + \log_2(\#F[2](\mathbb{Q})) + 2,$$

then $P_{E,F} \in 2E(\mathbb{Q})$. Hence the index $i_{E,F}$ is divisible by 2, if it is finite.

I prove the theorem in Section 5.2. In Section 5.3, I develop an exact algorithm to compute the Chow-Heegner point, using the methods in Chapter 2.

4.1 Definitions

We recall the definition from [Ste12a]. Consider a pair E, F of nonisogenous optimal elliptic curves over $\mathbb{Q}$ of the same conductor N and fix modular parametrizations from $X_0(N)$ to both curves.

Let $(\varphi_E)_*$ and $(\varphi_F)^*$ denote the pushforward and pullback map on divisors. Let $Q \in F(\mathbb{C})$ be any point, we define

$$P_{E,F,Q} = \sum (\varphi_E)_*(\varphi_F)^*(Q),$$

where $\sum$ means the sum of the points in the divisor, using the group law on E. By [Ste12a, Proposition 1.1], $P_{E,F,Q}$ is independent of the choice of Q. Let $P_{E,F} = P_{E,F,Q}$ for any choice of Q. Since we may choose $Q = \mathcal{O} \in \mathbb{F}(\mathbb{Q})$, it follows that $P_{E,F} \in E(\mathbb{Q})$.

4.2 The index

In this section, we make the additional assumption $r_{an}(E) = 1$. Consider the index

$$i_{E,F} = [E(\mathbb{Q})/tors : \mathbb{Z}P_{E,F}].$$

We quote a lemma of Calegari and Emerton [CE09].

Lemma 4.2.1 ([CE09])**.** *Let E/k be an elliptic curve and let A be the group of automorphisms of E as a curve over k. Suppose W is a finite elementary abelian 2-subgroup of A. Then the order of W divides twice the order of $E[2](k)$.*

Theorem 4.2.2. *Let E, F be elliptic curves defined over $\mathbb{Q}$, with the same conductor N. Let $\sigma_0(N)$ denote the number of distinct prime factors of N. If*

$$\sigma_0(N) > \log_2(|E(\mathbb{Q})[2]|) + \log_2(|F(\mathbb{Q})[2]|) + 2,$$

then $P_{E,F} \in 2E(\mathbb{Q})$. In particular, if $\sigma_0(N) \geq 7$, then the condition holds automatically, and $P_{E,F} \in 2E(\mathbb{Q})$.

Proof. Consider the group $\mathcal{W}$ of Atkin-Lehner involutions on $X_0(N)$. This group is elementary 2-abelian, and it descends to automorphisms on F and automorphisms on E, as curves. So we have a map

$$\pi : \mathcal{W} \to Aut(E) \times Aut(F)$$

By the Lemma above, we have $im(p_1 \circ \pi) \leq 2|E[2](\mathbb{Q})|$ and $im(p_2 \circ \pi) \leq 2|F[2](\mathbb{Q})|$. Hence the size of the image of π is bounded above by $4|E(\mathbb{Q})[2]| \cdot |F(\mathbb{Q})[2]|$. But we also know that

$$|\mathcal{W}| = 2^{\sigma_0(N)}.$$

Hence our assumption implies that $\ker(\pi)$ is nontrivial. Equivalently, there exists $w \in \mathcal{W}$ that acts as identity on both E and F. Now we consider the following diagram:

$$\begin{tikzcd}
& X_0(N) \arrow[d] \arrow[ddl] \arrow[ddr] & \\
& X_0(N)/w \arrow[dl] \arrow[dr] & \\
E & & F
\end{tikzcd}$$

Let $\mathcal{O} \in F(\mathbb{Q})$ be the identity element. We have $P_{E,F} = P_{E,F,\mathcal{O}} = \sum(\varphi_E)_*(\varphi_F)^*(O) = \sum(\tilde{\varphi_E})_*\pi_*\pi^*\tilde{\varphi_F}^*(O) = 2\sum(\tilde{\varphi_E})_*\tilde{\varphi_F}^*(O) \in 2E(\mathbb{Q})$. □

4.3 Applying the idea of IPR to the computation of Chow-Heegner points

We develop an algorithm to compute the Chow-Heegner point $P_{E,F}$. Let x_E, y_E, x_F, y_F be the compositions of φ, ψ with the x and y coordinate functions on E and F, respectively. We will use the algorithm in PARI to compute the q-expansions of x_E, x_F, y_E and y_F.

Algorithm 7 Using polynomial relation to compute the Chow-Heegner point $P_{E,F}$

Input: E, F = non-isogeneous elliptic curves of conuductor N; q-expansions of x_E, y_E, x_F, y_F.

Output: the Chow-Heegner point $P_{E,F}$.

1: $u_E \Leftarrow (x_F)^{-1}$ and $u_F \Leftarrow (x_F)^{-1}$.
2: Mimicing steps 4-7 of Algorithm 2, compute an irreducible polynomial $F(x,y)$ such that $F_{E,F}(u_E, u_F) = 0$.
3: $f_{ch,x}(x) \Leftarrow F_{E,F}(x, 0)$.
4: Repeat steps 2-5 for $v_E = (y_E)^{-1}$ and u_F, get $f_{ch,y}(y)$.
5: $K \Leftarrow$ the splitting field of $f_{ch,x}$. Write $f_{ch,x}(x) = \prod(x - a_i), a_i \in K$.
6: **for** each a_i **do**
7:     Find a point $p_i = (a_i, b_i)$ on $E(\bar{\mathbb{Q}})$.
8:     **if** $f_{ch,y}(b_i) = 0$ **then**
9:         $P_i = p_i$.
10:     **else**
11:         $P_i = -p_i$.
12:     **end if**
13: **end for**
14: Output $P_{E,F} = \sum_i P_i$.

Example 4.3.1. Consider $E = \mathbf{89a}$ and $F = \mathbf{89b}$. Here $\deg(\varphi_E) = 2$ and $\deg(\varphi_F) = 5$. Let $D = \varphi(\psi^*(\infty)) \in \mathrm{div}(E)$. Define $G_1(x) = \prod_{P \in D}(x - x(P))$ and $G_2(y) = \prod_{P \in D}(y - y(P))$. Using the first steps in Algorithm 7, we computed

$$G_1(x) = x^4 + \frac{13}{4}x^3 + \frac{17}{4}x^2 + \frac{21}{4}x + \frac{9}{2},\ G_2(y) = y^4 + \frac{1}{8}y^3 + \frac{21}{4}y^2 + \frac{7}{2}y + 3.$$

It turns out that $G_1(x)$ is irreducible over $\mathbb{Q}$. Let K be its splitting field, and write $G_1(x) = \prod(x - a_i)$ with $a_i \in K$. For each a_i, we found that $b_i = -\frac{8}{9}a_i^3 - \frac{20}{9}a_i^2 - \frac{28}{9}a_i - \frac{10}{3}$ is the corresponding root of G_2 such that $(a_i, b_i) \in E$. Hence

$$P_{E,F} = \sum_{i=1}^{4} P_i, \quad \text{where } P_i = (a_i, b_i).$$

Carrying out the summation in Sage, we obtain $P_{E,F} = (\frac{3}{4}, -\frac{15}{8})$. This agrees with Stein's result for the pair (**89a**,**89b**) in [Ste12a].

BIBLIOGRAPHY

[AO03] Scott Ahlgren and Ken Ono. Weierstrass points on $X_0(p)$ and supersingular j-invariants. *Mathematische Annalen*, 325(2):355–368, 2003.

[Asa76] Tetsuya Asai. On the fourier coefficients of automorphic forms at various cusps and some applications to rankin's convolution. *Journal of the Mathematical Society of Japan*, 28(1):48–61, 1976.

[AWL78] AOL Atkin and Wein-Ch'ing Winnie Li. Twists of newforms and pseudo-eigenvalues of w-operators. *Inventiones mathematicae*, 48(3):221–243, 1978.

[BCDT01] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises. *Journal of the American Mathematical Society*, pages 843–939, 2001.

[BFH90] Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein. Nonvanishing theorems for L-functions of modular forms and their derivatives. *Inventiones mathematicae*, 102(1):543–618, 1990.

[BH06] Colin J Bushnell and Guy Henniart. *The local Langlands conjecture for GL (2)*, volume 335. Springer Science & Business Media, 2006.

[Bru] François Brunault. personal communication.

[Bru12] François Brunault. On the ramification of modular parametrizations at the cusps. *arXiv preprint arXiv:1206.2621*, 2012.

[CE09] Frank Calegari and Matthew Emerton. Elliptic curves of odd modular degree. *Israel Journal of Mathematics*, 169(1):417–444, 2009.

[CE11] Jean-Marc Couveignes and Bas Edixhoven. *Computational aspects of modular forms and Galois representations*. Princeton University Press, 2011.

[Che] Hao Chen. Computing Fourier expansion of $\Gamma_0(N)$ newforms at non-unitary cusps. In preparation.

[Cre] J.E Cremona. Elliptic curve data. `http://www.maths.nott.ac.uk/personal/jec/ftp/data/INDEX.html`.

[DDLR15] Henri Darmon, Michael Daub, Sam Lichtenstein, and Victor Rotger. Algorithms for chow-heegner points via iterated integrals. *Mathematics of Computation*, 2015.

[Del02] Christophe Delaunay. Formes modulaires et invariants de courbes elliptiques définies sur $\mathbb{Q}$. *Thèse de doctorat, Université Bordeaux 1*, décembre 2002.

[Del05] Christophe Delaunay. Critical and ramification points of the modular parametrization of an elliptic curve. *J. Théor. Nombres Bordeaux*, 17:109–124, 2005.

[DI95] Fred Diamond and John Im. Modular forms and modular curves. In *Seminar on Fermat?s Last Theorem, Providence, RI*, pages 39–133, 1995.

[DS06] Fred Diamond and Jerry Shurman. *A first course in modular forms*, volume 228. Springer Science & Business Media, 2006.

[GZ86] Benedict H Gross and Don B Zagier. Heegner points and derivatives of L-series. *Inventiones mathematicae*, 84(2):225–320, 1986.

[JL72] Hervé Jacquet and Robert P Langlands. *Automorphic forms on GL (2)*, volume 278. Citeseer, 1972.

[Kra90] Alain Kraus. Sur le défaut de semi-stabilité des courbes elliptiques à réduction additive. *Manuscripta mathematica*, 69(1):353–385, 1990.

[Li75] Wen-Ch'ing Winnie Li. Newforms and functional equations. *Mathematische Annalen*, 212(4):285–315, 1975.

[Lig75] Gérard Ligozat. Courbes modulaires de genre 1. *Mémoires de la Société Mathématique de France*, 43:5–80, 1975.

[LW10] David Loeffler and Jared Weinstein. On the computation of local components of a newform. *arXiv preprint arXiv:1008.2796*, 2010.

[Mah74] Kurt Mahler. On the coefficients of transformation polynomials for the modular function. *Bulletin of the Australian Mathematical Society*, 10(02):197–218, 1974.

[MS04] Thom Mulders and Arne Storjohann. Certified dense linear system solving. *Journal of Symbolic Computation*, 37(4):485–510, 2004.

[MSD74] B. Mazur and P. Swinnerton-Dyer. Arithmetic of Weil curves. *Invent. Math.*, 25:1–61, 1974.

[S+14] W. A. Stein et al. *Sage Mathematics Software (Version 6.4)*. The Sage Development Team, 2014. `http://www.sagemath.org`.

[Sil09] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106. Springer, 2009.

[Stea] William Stein. Algebraic number theory, a computational approach. `https://github.com/williamstein/ant`.

[Steb] William A Stein. *Modular forms, a computational approach*, volume 79.

[Ste12a] William Stein. Numerical computation of chow-heegner points associated to pairs of elliptic curves. 2012.

[Ste12b] Glenn Stevens. *Arithmetic on modular curves*, volume 20. Springer Science & Business Media, 2012.

[Yan06] Yifan Yang. Defining equations of modular curves. *Advances in Mathematics*, 204(2):481–508, 2006.

[YZZ11] X. Yuan, S. Zhang, and W. Zhang. Triple product L-series and Gross-Schoen cycles I: split case. Preprint, 2011.