

©Copyright 2011-2016

Hao Chen

# 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

Abstract goes here.

# TABLE OF CONTENTS

|   | Page |
|---|------|
| Glossary . . . . .  | ii   |
| Chapter 1: Introduction . . . . .   | 1    |
| Chapter 2: Computing the Mazur Swinnerton-Dyer critical subgroup of elliptic curves | 2    |
| Chapter 3: Chow-Heegner points computations . . . . .                               | 3    |
| Chapter 4: Fourier expansions of modular forms forms at all cusps . . . . .         | 4    |
| 4.1 Preliminaries . . . . .   | 4    |
| 4.2 Reducing to the case of newforms . . . . .                                      | 6    |
| 4.3 Twists of newforms . . . . .  | 7    |
| 4.4 Pseudo-eigenvalues . . . . .  | 10   |
| 4.5 Formula for the Fourier expansion of $f$ at width one cusps: Part 1 . . . . .   | 13   |
| 4.6 Formula for the Fourier expansion of $f$ at width one cusps: Part 2 . . . . .   | 14   |
| 4.7 A Converse Theorem . . . . .  | 18   |
| 4.8 Fields of definitions . . . . .   | 20   |
| 4.9 Denominators . . . . .  | 21   |
| 4.10 Examples . . . . .   | 21   |
| 4.11 Applications . . . . .   | 21   |
| 4.12 Automorphic representations; norm of first terms . . . . .                     | 22   |
| Chapter 5: Things I tried to do but did not end up giving a nice result . . . . .   | 25   |
| Bibliography . . . . .  | 26   |

## **GLOSSARY**

ARGUMENT: replacement text which customizes a  $\text{\LaTeX}$  macro for each particular usage.

## **DEDICATION**

to all of you

## Chapter 1

# **INTRODUCTION**

## Chapter 2

# COMPUTING THE MAZUR SWINNERTON-DYER CRITICAL SUBGROUP OF ELLIPTIC CURVES



## Chapter 3

# CHOW-HEEGNER POINTS COMPUTATIONS

## Chapter 4

# FOURIER EXPANSIONS OF MODULAR 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:

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

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 [Edixhoven], 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 [Ed], 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 4.6.7 and Algorithm 3. 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 contains some examples.

### 4.1 Preliminaries

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

**Definition 4.1.1.** 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  $\infty$  means taking the isotropy subgroup of  $\infty$  in the corresponding group.

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

**Lemma 4.1.2.** *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  $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ . For  $N' \in \mathbb{Z}$  we compute

$$\alpha \begin{pmatrix} 1 & N' \\ 0 & 1 \end{pmatrix} \alpha^{-1} = \begin{pmatrix} * & * \\ -c^2 N' & * \end{pmatrix}.$$

Hence  $\begin{pmatrix} 1 & N' \\ 0 & 1 \end{pmatrix} \in (\alpha^{-1}\{\pm I\}\Gamma_0(N)\alpha)_\infty \iff N \mid c^2 N' \iff \frac{N}{\gcd(d_z^2, N)} \mid N'$ . 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

$$f|_\alpha(z) = (\det(\alpha))^{k/2} (cz + d)^{-k} f(\alpha z), \quad \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

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  $\alpha$ . Nonetheless, when the cusp  $z$  has width one, the expansion is indeed well-defined as a power series in  $q$ .

**Lemma 4.1.3.** *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  $\alpha$ .*

*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  $\alpha = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}$ , 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 4.1.4.** *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  $w_Q\alpha = \alpha'u$ , where  $\alpha' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in SL_2(\mathbb{Z})$  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  $\alpha''$  is of form  $\begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}$ . Note that for an upper triangular matrix  $u = \begin{pmatrix} u_0 & u_1 \\ 0 & u_2 \end{pmatrix}$ , we have  $f|u|(q) = f(q^{u_0/u_2}e^{2\pi i u_1/u_2})$ .

## 4.2 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  $g(q^d) = d^{-k/2}g|(\begin{smallmatrix} d & 0 \\ 0 & 1 \end{smallmatrix})$ . 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  $\begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}\alpha = \alpha'u$ . 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 4.2.1.** 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  $f_z$ .

### 4.3 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  $\chi$  a Dirichlet character, the *twist*  $f_\chi$  is a modular form with expansion  $f_\chi(q) = \sum a_n(f)\chi(n)q^n$ .

**Lemma 4.3.1.** [AWL78, Proposition 3.1] *Let  $F \in S_k(\Gamma_1(N), \epsilon)$ , where  $\epsilon$  is a character of conductor  $N'$ . Let  $\chi$  be a character modulo  $M$ . Put  $\tilde{N} = \text{lcm}(N, N'M, M^2)$ . Then  $f_\chi \in S_k(\Gamma_1(\tilde{N}), \epsilon\chi^2)$ .*

In particular, when  $\epsilon$  is the trivial character and the conductor  $M$  of  $\chi$  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  $\chi$* .

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

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

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

**Lemma 4.3.2.** [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  $\text{cond}(\epsilon_Q) = q^\alpha, \alpha \geq 0$ . Let  $\chi$  be a character with conductor  $q^\beta, \beta \geq 1$ . 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  $F_\chi$  is  $Q'M$  provided (a)  $\max\{q^{\alpha+\beta}, q^{2\beta}\} < Q$  if  $Q' = Q$ , or (b)  $\text{cond}(\epsilon_Q \chi) = \max\{q^\alpha, q^\beta\}$  if  $Q' > Q$ .*

**Lemma 4.3.3.** [AWL78, Theorem 3.2] *Let  $q \mid N$  and  $Q$  be the  $q$ -primary part of  $N$ . Write  $N = QM$ . Let  $\chi$  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  $\text{cond}(\chi)^2 \mid N$ .

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 4.3.4.** *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 4.3.5.** *Let  $g_1, g_2$  be two normalised newforms of levels  $N_1 \mid N_2$  and the same nebentypus character  $\epsilon$ . Assume  $\epsilon$  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  $1 \leq n \leq B$ . 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 1** Identifying  $f \otimes \chi$

---

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

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

```

1: if  $Q = 1$  then
2:   return  $N$ .
3: end if
4:  $Q' := \text{cond}(\chi^2)$ ;  $N_0 := \frac{N}{q^{v_q(N)}}$ ;  $M_0 := Q'N_0$ ;  $t := \frac{N}{M_0} \in \mathbb{Z}$ .
5: for each positive divisor  $d$  of  $t$  do
6:   Set  $V_d := S_k(M_0d, \chi^2)$ .
7:   Compute a basis of newforms  $\{g_1^{(d)}, \dots, g_{s_d}^{(d)}\}$  of  $V_d$ .
8:   Set  $B_d :=$  the Sturm bound for  $\Gamma_1(M_0dq^2)$ .
9:   for  $1 \leq j \leq s_d$  do
10:    if  $a_n(g_j^{(d)}) = a_n(f)\chi(n)$  for all  $1 \leq n \leq B_d, \gcd(n, q) = 1$  then
11:      return  $M_0d$ .
12:    end if
13:   end for
14: end for
```

---

We give some sample computations applying the above algorithm.

**Example 4.3.6.** 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  $\chi$  with modulus 5. In other words,  $f$  is 5-minimal.

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

**Example 4.3.7.** 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  $\chi$  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

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

#### 4.4 Pseudo-eigenvalues

Let  $\epsilon$  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 4.4.1.** 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 4.4.2.** *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 4.4.3.** *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

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

□

Suppose  $\alpha, \beta$  are distinct points on the arc  $\{z \in \mathbb{C} | \text{Im}(z) > 0, |z| = 1/\sqrt{N}\}$ . 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 2** 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  $w(f)$ .

- 1:  $n_0 := 10, z_0 := \frac{i}{\sqrt{N}}, \delta = 10^{-3}$ .
  - 2: Randomly generate  $n_0$  points  $\{z_1, \dots, z_{N_0}\} \subseteq \{z | 0 < \text{Im}(z) < \frac{1}{2\sqrt{N}}, |z| = \frac{1}{\sqrt{N}}\}$ .
  - 3: **for**  $1 \leq i \leq n_0$  **do**
  - 4:     compute the period integral  $c_i = \int_{z_0}^{z_i} 2\pi i f(z) z^{\frac{k-2}{2}} dz$ .
  - 5:      $w_i \leftarrow c_i / \bar{c}_i$ .
  - 6: **end for**
  - 7: **if** the standard deviation of  $w_1, \dots, w_{n_0}$  is less than  $\delta$  **then**
  - 8:      $w \leftarrow \frac{1}{n_0}(\sum_i w_i)$ .
  - 9:     **return**  $w$ .
  - 10: **else**
  - 11:     **return** FAIL.
  - 12: **end if**
-

#### 4.5 Formula for the Fourier expansion of $f$ at width one cusps: Part 1

First we recall some notations from [AWL78].

**Definition 4.5.1.** For a positive integer  $c'$ , let  $S'_c = \begin{pmatrix} 1 & \frac{1}{c'} \\ 0 & 1 \end{pmatrix}$ . If  $\chi$  is a character modulo  $c'$ , we define the operator on modular forms

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

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

$$\phi(c')S_{c'}^u = \sum_{\chi: \text{cond}(\chi)|c'} \chi(u) R_\chi(c'). \quad (4.5.1)$$

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

**Fact 4.5.2.**  $-N \cdot A_{N/c'}^{-1} = W_N S_{c'} W_N$ .

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

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

Since  $W_N^2 = id$  as operators, we have

$$A_c^{-u} = W_N S_{c'}^u W_N, \forall u \in \mathbb{Z}.$$

Parallel to the notion of  $R_\chi(c')$ , let  $\Phi_\chi(c) = \sum_{u=0}^{c'-1} \bar{\chi}(u) A_c^{-u}$ . Then  $\Phi_\chi(c) = W_N R_\chi(c') W_N$ . Similar to Formula 4.5.1, we have

$$\varphi(c') A_c^{-a} = \sum_{\text{cond}(\chi)|c'} \chi(a) \Phi_\chi(c) = \sum_{\text{cond}(\chi)|c'} \chi(a) W_N R_\chi(c') W_N. \quad (4.5.2)$$

Applying Formula 4.5.2 to  $f$ , we arrive at

$$f|_{[\frac{a}{c}]}(q) = \frac{1}{\varphi(c')} \sum_{\text{cond}(\chi)|c'} \chi(-a) f|W_N R_\chi(c') W_N. \quad (4.5.3)$$

$$= \frac{w(f)}{\varphi(c')} \sum_{\text{cond}(\chi)|c'} \chi(-a) f|R_\chi(c') W_N. \quad (4.5.4)$$

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

#### 4.6 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 4.6.1.** [Del02, Definition III.2.4] For a Dirichlet character  $\chi$  modulo  $b = \prod_{j \in J} p_j^{\alpha_j}$ . Let  $r = |J|$ . Decompose  $\chi$  uniquely as  $\chi = \chi_1 \cdots \chi_r$ , where  $\chi_i$  is a character modulo  $p_j^{\alpha_j}$ . We define  $\text{cond}'(\chi)$  multiplicatively, by putting

$$\text{cond}'(\chi_j) = \begin{cases} \text{cond}(\chi_j) & \text{if } \text{cond}(\chi_j) > 1 \\ p_j & \text{else} \end{cases} \quad (4.6.1)$$

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

$$g'(\chi) = (-1)^{|I|} \chi_{nt}(tr) g(\chi_{nt}). \quad (4.6.2)$$

Here  $g(\chi)$  is the usual Gauss sum of  $\chi$ : if  $\chi$  is a character modulo  $d$ , then  $g(\chi) = \sum_{a=1}^d e^{\frac{2\pi ia}{d}} \chi(a)$ .

**Lemma 4.6.2.** [Del02, Prop 2.6] Let  $c'$  be an integer such that  $c'^2 \mid N$ . For a Dirichlet character  $\chi$  mod  $c'$ , we have

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

Using this lemma, we can simplify formula 4.5.3 to

$$f|_{[\frac{a}{c}]} = \frac{w(f)}{\varphi(c')} \sum_{\text{cond}'(\chi)=c'} \chi(-a) g'(\bar{\chi}) f_{\chi_{nt}}|W_N. \quad (4.6.3)$$

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

$$f_{\chi_{nt}} = g| \prod_{i=1}^r K_{p_i}. \quad (4.6.4)$$

Moreover, we have

$$K_p = 1 - U_p B_p = \begin{cases} 1 - (T_p - \chi_{nt}^2(p) p^{\frac{k}{2}} B_p) | B_p & p \nmid M \\ 1 - T_p | B_p & p \mid M \end{cases}. \quad (4.6.5)$$

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  $\chi$  of conductor  $d$ , let  $S_\chi$  be the set of prime divisors of  $d$ . For any positive integer  $M$  and any finite set of integers  $S$ , define

$$\mathcal{B}_{S,M} = \{(S_1, S_2) \in (2^{\mathbb{Z}})^2 \mid S_1, S_2 \subseteq S, S_1 \cap S_2 = \emptyset, \gcd(M, \pi(S_2)) = 1\} \quad (4.6.6)$$

**Proposition 4.6.3.** *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  $g_\chi$  and  $\mathcal{B}_{S_\chi, M}$  is as in 4.6.6.

*Proof.* This is a direct consequence of multiplying out 4.6.4 using 4.6.5, using the fact that  $T_p$  commutes with  $B_d$ , and noting that  $T_p$  acts as multiplication by  $a_p(g_\chi)$  on  $g_\chi$ .  $\square$

Theorem 4.6.3 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 4.6.4.** *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.

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

□

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

**Lemma 4.6.5.** [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  $\epsilon$  is a character modulo  $N/p$  and  $p^2 \mid N$ , then  $a_p(f) = 0$ .*
- (2) *If  $\epsilon$  is a character modulo  $N/p$  and  $p^2 \nmid N$ , then  $a_p(f)^2 = \epsilon(p)p^{k-2}$ .*
- (3) *If  $\epsilon$  is not a character modulo  $N/p$ , then  $|a_p(f)| = p^{\frac{k-1}{2}}$ .*

**Lemma 4.6.6.** *Keep the notations in Proposition 4.6.3. 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  $\text{ord}_p(N') \leq \text{ord}_p(\text{cond}(\chi)^2) \leq \text{ord}_p(N)$ . 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  $\text{ord}_p(M) < \text{ord}_p(N)$ . Suppose not, then  $\text{ord}_p(M) = \text{ord}_p(N) \geq 2\text{ord}_p(\text{cond}(\chi))$ . Since  $\text{cond}(\chi^2) \leq \text{cond}(\chi)$ , we know  $\chi^2$  is a character modulo  $M/p$ . Applying case (1) of Lemma 4.6.5 to the newform  $g_\chi$ , 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 4.6.7.** *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  $z = [\frac{a}{d}]$  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*

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

Here

- $w(f)$  and  $w(f \otimes \chi)$  are the pseudo-eigenvalues.
- $g'(\chi)$  is the modified Gauss sum defined in 4.6.2 .
- $\text{cond}'$  is the modified conductor of a Dirichlet character in 4.6.1.
- $f_\chi^!$  is as follows: let  $M_\chi$  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 4.6.3.

*Proof.* We start from formula 4.6.3:

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

From 4.6.3, we have

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

To simplify notations, let  $c(f, \chi, S_1, S_2) = (-1)^{|S_1|} a_{\pi(S_1)}(f \otimes \chi) \pi(S_2)^{k/2} \chi_{nt}^2(\pi(S_2))$ . 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 4.6.4 to obtain the penultimate equality, and we could do that because of Lemma 4.6.6. Now the result follows.  $\square$

Theorem 4.6.7 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  $\chi$ , we then need to determine the level  $M_\chi$  and  $q$ -expansion of the newform  $f \otimes \chi$ , the latter boils down to knowing  $a_p(f \otimes \chi)$  for all primes  $p \mid \text{cond}(\chi)$ . Then we need to compute the pseudo-eigenvalues of  $f \otimes \chi$ . Finally, we combine these information together and apply Throem 4.6.7 to compute  $f_z$ .

---

**Algorithm 3** 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  $f_{[\frac{a}{c}]}(q)$ .

- 1:  $c' \leftarrow N/c$ .  $X \leftarrow$  The set of all Dirichlet characters  $\chi$  such that  $\text{cond}'(\chi) = c'$ .
  - 2: compute  $w(f)$  using Algorithm 2.
  - 3: **for**  $\chi$  in  $X$  **do**
  - 4:   Using Algorithm 1, compute the level  $M_\chi$  and the  $q$ -expansion of  $g_\chi := f \otimes \chi$  to  $B$  terms.
  - 5:   Compute  $w(g_\chi)$  using Algorithm 2.
  - 6: **end for**
  - 7: Apply Theorem 4.6.7 to compute  $f_z$  to  $B$  terms.
- 

#### 4.7 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 4.7.1.** *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  $\chi$  of such that  $\text{cond}'(\chi) = c'$ , the level  $M_\chi$ , the pseudo-eigenvalue  $w_{M_\chi}$  and the  $q$ -expansion of the newform  $f \otimes \chi$ .*

*Proof.* By plug in different  $a$ 's. We can solve for  $t_\chi$ . Consider the first nonzero term of  $t_\chi$ . Suppose

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

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

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

Proof of claim: the first and third case are easy to verify using Theorem 4.6.7. Now assume  $p \mid M$  and  $a_p(g_\chi) \neq 0$ . By Lemma 4.6.5, 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  $p \parallel M_\chi$  and  $\chi^2$  is a character modulo  $M_\chi/p$ . This means  $\chi^2$  is the trivial character. By Lemma 4.3.2, 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.,  $\text{ord}_p(N) = \beta$ . This is impossible since we have  $p^{2\beta} = \text{cond}(\chi)^2 \mid N$ .

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  $M_\chi$  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  $N/M_\chi$ 's coefficient of  $t_\chi$  is

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

This allows us to solve  $w(g_\chi)$ . Finally, we compute  $a_p(g_\chi)$  by  $a_p(g) = \frac{-u_\chi}{w(g_\chi) \chi^2(p) \left(\frac{N}{Mp}\right)^{k/2}}$ . The

value  $a_p(g)$  determines the expansion of  $g_\chi$ . Recursively, we could solve for all  $pn$ -coefficients of  $g_\chi$ , from which we deduce its complete  $q$ -expansion.

In the general case, we consider the following subsets of  $S_\chi$ . 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  $t_\chi$  belongs to the summand corresponding to  $(\widetilde{S}_1^*, S_2^*)$  in Theorem 4.6.7. Still writing the leading term as  $u_\chi q^{v_\chi}$ , we have

$$u_\chi = w(g_\chi) \chi^2(p(S_2)) a_{p(\widetilde{S}_1^*)}(g_\chi) p(\widetilde{S}_1^*)^{-k} (p(S_2^*))^{-3k/2} \left( \frac{N}{M_\chi} \right)^{k/2}, \quad v_\chi = \frac{N}{M_\chi p(\widetilde{S}_1^*) p(S_2^*)^2}.$$

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

$$|v_\chi^k u_\chi^{-2}| = p(\widetilde{S}_1^*) p(S_2^*)^2. \quad (4.7.1)$$

Hence we can factor  $|v_\chi^k u_\chi^{-2}|$  and obtain  $p(\widetilde{S}_1^*)$  and  $p(S_2^*)$ . Then  $M_\chi$  can be solved using  $v_\chi$ . Plug it back into  $u_\chi$ , 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  $t_\chi$  allows us to compute  $a_{p(\widetilde{S}_1^*)/p}(g_\chi) w(g_\chi)$ . These together determine  $w(g_\chi)$  and  $a_{p(\widetilde{S}_1^*)}$ . The other Fourier coefficients of  $g_\chi$  can then be computed recursively.  $\square$

#### 4.8 Fields of definitions

In the previous sections, we have described an algorithm to compute the Fourier coefficients of  $f_z$ . In fact, the Fourier coefficients are algebraic numbers. More precisely, if  $c$  is the denominator of  $z$  and  $c' = N/c$ , then  $f_z(q) \in K_f(\zeta_{c'})[[q]]$ . Here  $K_f$  is the number field generated by the Fourier coefficients of  $f$  (at the cusp  $\infty$ ). Although this result is well-known, we include a proof for the reader's convenience.

**Lemma 4.8.1.** *Let  $c$  be a cusp of denominator  $d$  and let  $d' = N/d$ . Then*

$$\mathbb{Q}(\{a_n(f, c)\}) \subseteq \mathbb{Q}(\{a_n(f)\}, \zeta_{d'}).$$

(fixme: add proof)

## 4.9 Denominators

(fixme)

## 4.10 Examples

Let  $E = \mathbf{50a}$  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  $E = \mathbf{98a}$  and  $z = [\frac{1}{14}]$ . We computed numerically that

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

## 4.11 Applications

One applications of the computation done in this chapter is the norm method to the computation of  $j$ -polynomials introduced in Chapter . Recall that the issue with the norm method for non-square free level is computing the expansions of form  $f|\gamma$ , where  $\gamma$  runs over the set of right coset representatives of  $\Gamma_0(N)$  in  $SL_2(\mathbb{Z})$ . As we have seen, it suffices to compute the expansions of  $f$  at all width one cusps.

### 4.12 Automorphic representations; norm of first terms

In this section, we will restrict ourselves to the case when the Fourier coefficients of  $f$  are rational numbers. Then  $f$  induces an admissible representation  $\pi_f$  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  $\pi_f$  is the smallest among all twists  $\pi_{f \otimes \chi}$ .

We will follow the notations of David Loeffler and use the formula of Francois Brunault. Also, I will use Jacquet-Langlands, Gelbart, and Bushnell-Henniart.

Okay, what is my heuristics for general  $k$ ? What is it for  $\Gamma_1(N)$ ? What happens on the automorphic side?

Also there's the question about normalization, which was never specified.

Raw data?

Let  $z$  be a 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  $\beta$  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

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

The following is a table of data.

(fix: add table)

#### 4.12.1 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  $\varphi : \mathbb{F}_{p^2}^\times \rightarrow \mathbb{C}^\times$  which determines  $\pi_{f,p}$ . We will prove

**Lemma 4.12.1.** *Let  $\psi : \mathbb{Q}_p \rightarrow \mathbb{C}^\times$  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  $\chi$  is a Dirichlet character such that the  $f \otimes \chi$  has the same level as  $f$ . Then*

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

to-do: add formula for twists

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

$$p^2 \epsilon(\pi_{f,p}, 1/2, \psi) \cdot \text{id} = \sum_{x \in GL_2(\mathbb{F}_p)} \psi(\text{tr}(x)) \pi_{f,p}^\vee(x). \quad (4.12.1)$$

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

$$p^2(p-1) \epsilon(\pi_{f,p}, 1/2, \psi) \cdot \text{id} = \sum_{x \in GL_2(\mathbb{F}_p)} \psi(\text{tr}(x)) \text{Tr}(\pi_{f,p}^\vee(x)). \quad (4.12.2)$$

By assumption,  $\pi_{f,p}$  arises from a cuspidal representation of the finite group  $GL_2(\mathbb{F}_p)$ , which is in turn induced from  $\varphi$ . (See Fulton-Harris), we have formulae for  $\text{Tr}(\pi_{f,p}^\vee(x))$ . 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  $S_4 = (p^2-p)/2 \sum_{x \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p} \psi(\text{tr}(x)) (\overline{\varphi(x) + \varphi(x^p)})$ . So the sum on the right hand side of 4.12.2 equals  $(p-p^2) \sum_{x \in \mathbb{F}_{p^2}^\times} \psi(\text{tr}(x)) \overline{\varphi(x)}$ . 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  $\varphi$  is 3, 4 or 6.

**Lemma 4.12.2** (See Kraus?). *Let  $\Delta$  denote the minimal discriminant of  $E$ . Then for  $p \geq 5$ , the order of  $\varphi$  is equal to  $\frac{12}{\gcd(12, v_p(\Delta))}$ .*

The local Langlands correspondence claims that the order of  $\varphi$  is equal to the order of the inertia subgroup of  $\text{Gal}(L/\mathbb{Q})$ , where  $L$  is the smallest number field over which  $E$  acquires good reduction (to-do: check this).

For  $p = 2$  or  $3$ , the order of  $\varphi$  can be determined using Kraus's result <http://gdz.sub.uni-goettingen.de/dms/load/img/?PPN=GDZPPN002231468&IDDOC=219018>, or Dokchitser's paper Euler factors determine local Weil representations.

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 [BH], once the local component is determined using [DW].

**Example 4.12.3.** An example with trivial central character. Let  $f$  be the newform attached to  $E = \mathbf{121a}$ . Using Sage, we computed  $w(f) = -1$ . Since the weight of  $f$  is 2, we know  $\epsilon_\infty = -1$  (since the central character of  $\pi_f$  is trivial, the level of the additive character  $\psi_\infty$  does not matter). The discriminant of  $E$  is  $\Delta = -121$ , so  $\varphi$  has order 6. Using Lemma 4.12.1, we computed that  $\epsilon_{11}(\pi_{f,11}, 1/2) = -1$ . This verifies  $w(f) = -\prod_{p \leq \infty} \epsilon_p$ .

**Example 4.12.4.** We give an example with nontrivial central character. Let  $f$  be as in the previous example, and let  $\chi$  be the Dirichlet character of  $\mathbb{F}_{11}^\times$  defined by  $\chi(2) = e^{2\pi i/10}$ . Lemma 4.12.1 gives

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

an algebraic number with minimal 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 2, we compute  $w(f \otimes \chi) = 0.642573377564283 + 0.766224154177894i$ . This confirms the computation.

## Chapter 5

**THINGS I TRIED TO DO BUT DID NOT END UP GIVING A  
NICE RESULT**

generalizing the “congruence number” definition using other cusps.

Prove the “ $\pm 1 \bmod p$ ” guess.

Generalize another paper by William on computing order of component groups. (The original paper uses a trick which William fails to remember).

Prove even index for Chow-Heegner points.

Computing the critical subgroup for 5077a (multimodular is not practical).

Critical points of reduction of modular parametrization.

## 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.
- [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>.
- [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.
- [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.



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