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

1985-2014

Reading Committee:

Name of Chairperson, Chair

First committee member

Next committee member

etc

Program Authorized to Offer Degree:
UW Information Technology

[†]an egocentric imitation, actually

University of Washington

Abstract

Computational aspects of modular parametrizations
of elliptic curves

Hao Chen

Chair of the Supervisory Committee:
Title of Chair Name of Chairperson
Department of Chair

Abstract goes here.

TABLE OF CONTENTS

GLOSSARY

ARGUMENT: replacement text which customizes a LaTeX macro for each particular usage.

DEDICATION

to all of you

Chapter 1

FOURIER EXPANSIONS OF CUSPIDAL MODULAR FORMS FORMS AT CUSPS

Let k be a positive even integer and let $f \in S_k(\Gamma_0(N))$ be a nonzero cusp form. We are concerned with the problem of computing the Fourier expansion of f at cusps of width one other than the cusp $[\infty]$. Note that such cusps exist if and only if N is not square-free. We will give two algorithms, one numerical and the other exact, to compute such expansions. The question is studied in the Ph.D. thesis of Christophe Delaunay. We draw insight from another preprint by F.Brunault. The question is also studied in [Edixhoven], where numerical algorithm is given. The algorithm in [Ed] for computing expansions requires 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 result of this chapter is Theorem 1.6.7 and Algorithm 3, which computes the Fourier expansion of a newform $f \in S_k(\Gamma_0(N))$ at any width one cusp z. Along the way, we have developed algorithms to compute the twists $f \otimes \chi$ and the pseudo-eigenvalue of newforms under the Fricke involution. Section contains some examples.

1.1 Preliminaries

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

Definition 1.1.1. 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 1.1.2. *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

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

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 1.1.3. *Let z be a cusp on $X_0(N)$ with width one. 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 $0 \le m < N$ 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 1.1.4. *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 $f[u](q) = f(q^{u_0/u_2}e^{2\pi i u_1/u_2})$.

1.2 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 1.2.1. Let f be a normalized newform in $S_2(\Gamma_0(N))$ and z be a cusp on $X_0(N)$ of width one. Compute the q-expansion of f_z.

1.3 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 1.3.1. *[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 $\tilde{N} = lcmN, N'M, M^2$. 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

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

Lemma 1.3.2. *[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 1.3.3. *[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 with conductor equal 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, such that*

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

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, which we denote by M_χ, 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 1.3.4. *Let $f \in S_k(N, \epsilon)$ be a normalized newform. Then $f|U_q|B_q \in S_k(Nq^2, \epsilon)$.*

Proof. We use 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 1.3.5. *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 $Q^2 \mid N$. 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 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. This forces $g_1 - g_2 = 0$. $\square$

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; 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(χ^2); 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, χ^2).
    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 q^2).
    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 1.3.6. 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 1.3.7. 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

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

1.4 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 1.4.1. The number $w_Q(f)$ is called the *pseudo-eigenvalue* of W_Q on f. 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 1.4.2. *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. □

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

Now we are ready to prove the main theorem of this section.

Theorem 1.4.3. *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 $\alpha, \beta \in \{z \in \mathbb{C} | Im(z) > 0, |z| = 1/\sqrt{N}\}$. 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 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 $w(f)$.

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

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

First we recall some notations from [AWL78].

Definition 1.5.1. For a positive integer c', let $S'_c = \begin{pmatrix} 1 & \frac{1}{c'} \\ 0 & 1 \end{pmatrix}$. If χ is a character modulo c', we define the operator on modular forms

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

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

$$\phi(c')S_{c'}^u = \sum_{\chi:cond(\chi)|c'} \chi(u)R_\chi(c'). \tag{1.5.1}$$

For our convenience, we define a new set of operators, which are basically the conjugates of S'_c and $R_\chi(c')$ by W_N. Let $A'_c = \begin{pmatrix} 1 & 0 \\ c' & 1 \end{pmatrix}$. Then we have

Fact 1.5.2. $-N \cdot A_{N/c'}^{-1} = W_N S_{c'} W_N$

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

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

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 1.5.1, we have

$$\varphi(c')A_c^{-a} = \sum_{\mathrm{cond}(\chi)|c'} \chi(a)\Phi_\chi(c) = \sum_{\mathrm{cond}(\chi)|c'} \chi(a) W_N R_\chi(c') W_N. \tag{1.5.2}$$

Finally, applying Formula 1.5.2 to f, we arrive at

$$f_{[\frac{a}{c}]}(q) = \tfrac{1}{\varphi(c')} \textstyle\sum_{\mathrm{cond}(\chi)|c'} \chi(-a) f|W_N R_\chi(c') W_N. \tag{1.5.3}$$

$$= \tfrac{w(f)}{\varphi(c')} \textstyle\sum_{\mathrm{cond}(\chi)|c'} \chi(-a) f|R_\chi(c') W_N. \tag{1.5.4}$$

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

1.6 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 the following identity between operators on $S_k(\Gamma_1(N),\epsilon)$:

$$T_p = U_p + \epsilon(p)p^{\frac{k}{2}}B_p.$$

We recall some notations and a result from [Del02], which states that $f|R_\chi(c')$ is a constant multiple of some twist $f_{\chi_{nt}}$.

Definition 1.6.1. [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

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

Also, if $I = \{j \in J : \chi_j$ 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

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

Here $g(\chi)$ is the usual Gauss sum associated with χ.

Lemma 1.6.2. *[Del02, Prop 2.6] Let c' be such that $c'^2 \mid N$. For a Dirichlet character χ mod c', we have*

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

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

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

Moreover, we have

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

Using the commutativity of T and B, we can write $f_{\chi_{nt}}$ in the form $\sum c_i g(q_i^d)$, 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 $p(S) = \prod_{s \in S} s$ denote the product of all elements in S.

Theorem 1.6.3. *Let $S_\chi = \{p_1, \cdots, p_r\}$ be the set of prime divisors of* $\mathrm{cond}(\chi)$*.*
Let $\mathcal{B}_{\chi,M} = \{(S_1, S_2) | S_1, S_2 \subseteq S_\chi, S_1 \cap S_2 = \emptyset, \gcd(M, p(S_2)) = 1.\}$. Write $g_\chi = f \otimes \chi$. Then

$$f_{\chi_{nt}} = \sum_{(S_1,S_2) \in B_{S,M}} a_{p(S_1)}(g_\chi) p(S_2)^{k/2} \chi_{nt}^2(p(S_2)) g_\chi | B_{p(S_1)p(S_2)^2}.$$

Theorem 1.6.3 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 1.6.4. *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*

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

where $w_M(f)$ is the pseudo-eigenvalue of f defined in previous sections.

Proof. Straightforward computation.

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

$\square$

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

Lemma 1.6.5. *[Li75, Theorem 3 (iii)] Let $f = \sum_{n\geq 1} a_n(f)q^n$ be a normalized newform in $S_k(\Gamma_1(N), \epsilon)$, p 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 1.6.6. *Using notations in Theorem 1.6.3, and assume $(S_1, S_2) \in \mathcal{B}_{S,M}$ is such that $a_{p(S_1)}(g_\chi) \neq 0$. Then $Mp(S_1)p(S_2)^2 \mid N$.*

Proof. Let p be a prime divisor of $N' := Mp(S_1)p(S_2)^2$. 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 it follows from $M \mid N$; if $p \mid p(S_1)$, 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 Lemma 1.6.5 to the newform g_χ on level M, we see that $a_p(g_\chi) = 0$, hence $a_{p(S_1)}(g_\chi) = 0$ by multiplicativity. $\square$

Applying Lemma 1.6.4 to Theorem 1.6.3, we finally arrive at

Theorem 1.6.7. *Let f be a normalized newform in $S_2(\Gamma_0(N))$ and $z = [a/c]$ be a cusp on $X_0(N)$ of width one. Then f_z is*

$$f_z = \frac{w(f)}{\varphi(c')} \sum_{\chi:\mathrm{cond}'(\chi)=c'} \chi(-a)g'(\bar{\chi})w(g_\chi)t_\chi.$$

Here t_χ is as follows: let M_χ denote the level of $g_\chi := f \otimes \chi$. Then

$$t_\chi = \sum_{(S_1,S_2)\in B_{S_{\chi nt}, M_\chi}} (-1)^{|S_1|} a_{p(S_1)}(g_\chi) \left(\frac{N}{M_\chi p(S_1)^2 p(S_2)^3}\right)^{k/2} \chi(p(S_2))\overline{g_\chi | B_{\frac{N}{M_\chi p(S_1)p(S_2)^2}}}.$$

This theorem gives us an algorithm to compute the expansion of f_z, which we 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 $p \mid \mathrm{cond}(\chi)$. Then we need to compute the. Finally, we combine these information together and apply Throem 1.6.7 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 $f_z(q)$.

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 2.
3: **for** χ in X **do**
4: Compute M_χ and the expansion of $g_\chi := f \otimes \chi$ to B terms, using Algorithm 1
5: Compute $g'(\bar{\chi})$.
6: Compute $w(g_\chi)$ using Algorithm 2.
7: **end for**
8: Apply Theorem 1.6.7 to compute f_z to B terms.

1.7 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 1.7.1. *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

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

Proof of claim: the first and third case are easy to verify using Theorem 1.6.7. Now assume $p \mid M$ and $a_p(g_\chi) \neq 0$. By Lemma 1.6.5, 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 1.3.2, 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 1.6.7. 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

$$|v_\chi^k u_\chi^{-2}| = p(\widetilde{S_1^*})p(S_2^*)^2. \tag{1.7.1}$$

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. $\square$

1.8 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 ∞). Although this result is well-known, we include a proof for the reader's convenience.

Lemma 1.8.1. *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)

1.9 Denominators

(fixme)

1.10 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

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

1.11 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 γ 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.

1.12 Norm of first terms

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.

(fix: add table)

BIBLIOGRAPHY

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

[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$^+$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.