Computing Hilbert modular forms

John Voight
Dartmouth College

Curves and Automorphic Forms
Arizona State University
10 March 2014

Hilbert modular forms

Let F be a totally real field with $[F:\mathbb{Q}] = n$ and let $\mathbb{Z}_F$ be its ring of integers. Assume F has narrow class number 1. Let $v_1, \dots, v_n : F \to \mathbb{R}$ be the real places of F, and write $v_i(x) = x_i$. For $\gamma \in \mathrm{M}_2(F)$ we write $\gamma_i = v_i(\gamma) \in \mathrm{M}_2(\mathbb{R})$.

The group $\mathrm{GL}_2^+(F) = \{\gamma \in \mathrm{GL}_2(F) : \det \gamma_i > 0 \text{ for } i = 1, \dots, n\}$ acts on $\mathcal{H}^n$ by coordinatewise linear fractional transformations $\gamma z = (\gamma_i z_i)_i$. For a nonzero ideal $\mathfrak{N} \subseteq \mathbb{Z}_F$, let

$$\Gamma_0(\mathfrak{N}) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathbb{Z}_F) : c \in \mathfrak{N} \right\} \subseteq \mathrm{GL}_2^+(F).$$

A *Hilbert cusp form* of parallel weight 2 and level $\mathfrak{N}$ is a (holomorphic) function $f : \mathcal{H}^n \to \mathbb{C}$ such that

$$f(\gamma z) = f\left(\frac{a_1 z_1 + b_1}{c_1 z_1 + d_1}, \dots, \frac{a_n z_n + b_n}{c_n z_n + d_n} \right) = \left(\prod_{i=1}^{n} \frac{(c_i z_i + d_i)^2}{\det \gamma_i} \right) f(z)$$

for all $\gamma \in \Gamma_0(\mathfrak{N})$ and such that f vanishes at the cusps.

Hecke modules

The space $S_2(\mathfrak{N})$ of Hilbert cusp forms of level $\mathfrak{N}$ is equipped with an action of Hecke operators $T_{\mathfrak{p}}$ for primes $\mathfrak{p} \nmid \mathfrak{N}$. For a normalized eigenform $f \in S_2(\mathfrak{N})$ with Hecke eigenvalues $a_{\mathfrak{p}}$, we have a q-expansion

$$f(z) = a_0 + \sum_{\mu \in (\mathfrak{d}^{-1})_+} a_\mu q^{\mathrm{Tr}(\mu z)}$$

(which will play no role for us), an L-function

$$L(f,s) = \sum_{\mathfrak{n} \subseteq \mathbb{Z}_F} \frac{a_{\mathfrak{n}}}{N\mathfrak{n}^s},$$

and $\mathfrak{l}$-adic Galois representations $\mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbb{Z}}_{F,\mathfrak{l}})$.

Conjecturally, if $a_{\mathfrak{p}} \in \mathbb{Z}$, then f corresponds to an isogeny class of elliptic curves over F; the *modularity conjecture* predicts that this is a bijection.

The space $S_2(\mathfrak{N})$ is often computed as a *Hecke module*: a vector space equipped with an action of Hecke operators.

Main algorithm

Theorem (Dembélé, Dembélé-Donnelly, Greenberg-V, V)

There exists an algorithm that, on input a totally real field F, a weight $k \in (\mathbb{Z}_{\geq 2})^n$, and a nonzero ideal $\mathfrak{N} \subseteq \mathbb{Z}_F$, computes as output the system of Hecke eigenvalues for the space $S_k(\mathfrak{N})$ of Hilbert cusp forms of weight k and level $\mathfrak{N}$ over F.

In other words, there exists an explicit finite procedure that takes as input the field F and the ideal $\mathfrak{N} \subseteq \mathbb{Z}_F$ encoded in bits (in the usual way), and outputs: a finite set of sequences $(a_{\mathfrak{p}}(f))_{\mathfrak{p}}$ encoding the Hecke eigenvalues for each cusp form constituent f in $S_2(\mathfrak{N})$, where $a_{\mathfrak{p}}(f) \in E_f \subseteq \overline{\mathbb{Q}}$.

Hecke module example

Let $F = \mathbb{Q}(\sqrt{5})$. Then $\mathbb{Z}_F = \mathbb{Z}[w]$ where $w = (1+\sqrt{5})/2$. Let $\mathfrak{N} = (3w - 14) \subseteq \mathbb{Z}_F$; we have $N(\mathfrak{N}) = 229$ is prime.

We compute that $\dim S_2(\mathfrak{N}) = 4$. There are 2 Hecke irreducible subspaces of dimensions 1 and 3, corresponding to newforms f and g (and its Galois conjugates).

$\mathfrak{p}$	(2)	$(w+2)$	(3)	$(w+3)$	$(w-4)$
$N\mathfrak{p}$	4	5	9	11	11
$a_{\mathfrak{p}}(f)$	-3	-4	-1	0	-2
$a_{\mathfrak{p}}(g)$	t	$t^2 - 4t + 1$	$-t^2 + 2t + 2$	$t^2 - 2t - 3$	$-3t^2 + 8t + 1$

Here, the element $t \in \overline{\mathbb{Q}}$ satisfies $t^3 - 3t^2 - t + 1 = 0$ and $E = \mathbb{Q}(t)$ is an S_3-field of discriminant 148.

Data computed

In joint work with Steve Donnelly, we have computed over 240 000 Hilbert modular forms over fields F of degree $n \leq 6$ (discriminant $d_F \leq 2 \cdot 10^n$) in a large range of levels $\mathfrak{N}$.

The calculations were performed on the Vermont Advanced Computing Cluster (VACC), and the raw data (172 GB) is kept by the NECC Shared Data Center. The total computing time was 6 CPU years.

The data is available on the LMFDB and contains additional information (Atkin-Lehner involutions, CM or base change, etc.).

The largest Hecke-irreducible space in the database has dimension 286 and occurs for the field $F = \mathbb{Q}(\sqrt{296})$ and level $\mathfrak{N}$ with norm 29.

Geometry

To compute with the space $S_2(N)$ of classical modular forms ($F = \mathbb{Q}$), one approach is to use the geometry of the modular curve $X_0(N) = \Gamma_0(N)\backslash\mathcal{H}^*$, where $\mathcal{H}^* = \mathcal{H} \cup \mathbb{P}^1(\mathbb{Q})$ denotes the completed upper half-plane.

A cusp form $f \in S_2(N)$ corresponds to a holomorphic differential form $f(z)\,dz$ on $X_0(N)$ and so by the theorem of Eichler-Shimura arises naturally in the space $H^1(X_0(N), \mathbb{C})$.

In a similar way, a Hilbert cusp form $f \in S_2(\mathfrak{N})$ gives rise to a holomorphic differential n-form $f(z_1, \dots, z_n)\,dz_1 \dots dz_n$ on the *Hilbert modular variety* $X_0(\mathfrak{N})$, a desingularization of $\Gamma_0(\mathfrak{N})\backslash\mathcal{H}^{n*}$. But now $X_0(\mathfrak{N})$ has dimension n and f arises in $H^n(X_0(\mathfrak{N}), \mathbb{C})$. Yikes!

Computing with higher dimensional varieties (and higher degree cohomology groups) is not an easy task.

General strategy

Langlands functoriality predicts that $S_2(\mathfrak{N})$ as a Hecke module occurs in the cohomology of other "modular" varieties. We use a principle called the *(Eichler-Shimizu-)Jacquet-Langlands correspondence*, which allows us to work with varieties of complex dimension 0 or 1 by considering twisted forms of GL_2 over F.

Let B be the quaternion algebra over F which is split at all finite places and ramified at all or all but one real place according as $n = [F : \mathbb{Q}]$ is even or odd. The Jacquet-Langlands correspondence is the isomorphism of Hecke modules

$$S_2(\mathfrak{N}) \xrightarrow{\sim} S_2^B(\mathfrak{N})$$

where $S_2^B(\mathfrak{N})$ denotes the space of quaternionic cusp forms for B (of weight 2) and level $\mathfrak{N}$. The explicit description of the Hecke module $S_2^B(\mathfrak{N})$ varies accordingly as n is even or odd.

(There is also a method over real quadratic fields using Voronoï theory due to Gunnells–Yasaki.)

Definite method

First suppose that $n = [F : \mathbb{Q}]$ is even.

In this case, the quaternion algebra B is ramified at all real places and so is totally definite. In this case, the Shimura variety associated to B is zero-dimensional: it consists of a finite set of points labelled by the (right) $\mathcal{O}$-ideal classes, where $\mathcal{O} = \mathcal{O}_0(\mathfrak{N})$. We write $X = \mathrm{Cl}\,\mathcal{O}$ for this set and $H = \#X$.

A *quaternionic cusp form* for B of level $\mathfrak{N}$ (and parallel weight 2) is just an element of the space

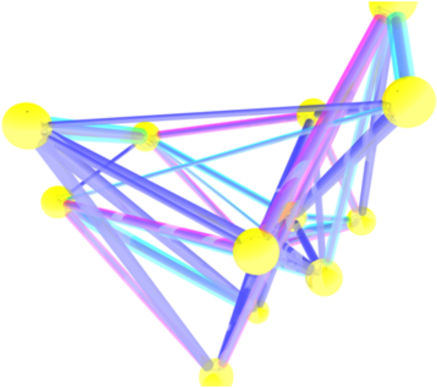
$$S_2^B(\mathfrak{N}) = \mathrm{Map}(X, \mathbb{C})/\mathbb{C} \cong \mathbb{C}^{H-1}$$

where $\mathbb{C}$ is the space of constant functions.

The Hecke operators acting on $\bigoplus_i \mathbb{C} I_i = \mathrm{Map}(\mathrm{Cl}\,\mathcal{O}, \mathbb{C})$ are given by Brandt matrices. This method goes back to Brandt and has been developed by many people (including Kohel, Socrates–Whitehouse, Dembélé, . . .), and will be described by Deines.

Definite method: Brandt matrices

The Brandt matrix is just a compact way of writing down the adjacency matrix of the graph with vertices $X = \mathrm{Cl}\,\mathcal{O}$ where there is an edge (weighted by units) from I_i to each ideal class which represents an ideal of index $N\mathfrak{p}$ in I_i.



Here, $F = \mathbb{Q}(\sqrt{3})$, $\mathfrak{N} = (11)$, and $\mathfrak{p}$ is an ideal of norm 23.

Example

Let $F = \mathbb{Q}(w)$ with $w = (1+\sqrt{5})/2$. Let $\mathfrak{N} = (3w+7)\mathbb{Z}_F$ be a prime of norm 61. Consider the (Hamilton) quaternion algebra $B = \left(\dfrac{-1,-1}{F}\right)$ over F of discriminant $\mathfrak{D} = (1)$. We have the maximal order

$$\mathcal{O}_0(1) = \mathbb{Z}_F \oplus i\mathbb{Z}_F \oplus k\mathbb{Z}_F \oplus ik\mathbb{Z}_F, \qquad \text{where } k = \frac{(1+w)+wi+j}{2},$$

and the Eichler order $\mathcal{O} \subseteq \mathcal{O}_0(1)$ of level $\mathfrak{N}$ given by

$$\mathcal{O} = \mathbb{Z}_F \oplus (3w+7)i\mathbb{Z}_F \oplus (-30i+k)\mathbb{Z}_F \oplus (w+20i+ik)\mathbb{Z}_F.$$

Example

The class number of $\mathcal{O}$ is $H = 3$. The following ideals give a set of representatives for $\operatorname{Cl}\mathcal{O}$: we take $I_1 = \mathcal{O}$,

$$\begin{aligned} I_2 &= 2\mathcal{O} + ((w+2) - (2w+2)i + (-1+3w)ik)\mathcal{O}, \\ I_3 &= 2\mathcal{O} + ((w+1) + (1-w)i + (2-2w)k)\mathcal{O}. \end{aligned}$$

The first few Brandt matrices are:

$$T(2) = \begin{pmatrix} 1 & 5 & 3 \\ 2 & 0 & 0 \\ 2 & 0 & 2 \end{pmatrix}, \quad T(\sqrt{5}) = \begin{pmatrix} 4 & 0 & 3 \\ 0 & 1 & 3 \\ 2 & 5 & 0 \end{pmatrix}, \quad T(3) = \begin{pmatrix} 4 & 5 & 6 \\ 2 & 0 & 3 \\ 4 & 5 & 1 \end{pmatrix}.$$

For example, the first column of the matrix $T(2)$ records the fact that of the $5 = N(2) + 1$ right $\mathcal{O}$-ideals of norm (2), there is exactly one which is principal, two are isomorphic to I_2 and the other two are isomorphic to I_3.

Example

The space $S_2^B(\mathfrak{N})$ of cusp forms is an irreducible 2-dimensional Hecke module, represented by a constituent form f. We have the following table of eigenvalues for f:

$\mathfrak{p}$	(2)	$(w+2)$	(3)	$(w+3)$	$(w-4)$
$N\mathfrak{p}$	4	5	9	11	11
$a_\mathfrak{p}(f)$	$2w-2$	$-3w+1$	$-w-2$	$4w-2$	$-w$

(The reappearance of F here is a coincidence!)

One can identify this modular abelian surface: it is the Jacobian of the hyperelliptic curve $C : y^2 + Q(x)y = P(x)$ over F with

$$P(x) = -wx^4 + (w-1)x^3 + (5w+4)x^2 + (6w+4)x + 2w + 1$$
$$Q(x) = x^3 + (w-1)x^2 + wx + 1.$$

Definite method: computational problems

In addition to basic algorithms for working with quaternion orders and ideals, to compute Brandt matrices, we need algorithms to:

1. Compute a set of representatives for $\operatorname{Cl}\mathcal{O}$; and
2. Test if two right $\mathcal{O}$-ideals are isomorphic.

Problems 1 and 2 can be solved using lattice methods (joint work with Kirschmer, with improvements due to Dembélé): we use the fact that $\operatorname{Tr}\operatorname{nrd} : \mathcal{O} \to \mathbb{Z}$ gives $\mathcal{O}$ the structure of a lattice in $B \otimes_F \mathbb{R} \cong \mathbb{R}^{4n}$.

Indefinite method: setup

Suppose first that $n = [F : \mathbb{Q}]$ is odd. (The indefinite method works for $n = [F : \mathbb{Q}]$ even whenever there is a prime $\mathfrak{p} \parallel \mathfrak{N}$.) Then the quaternion algebra B is split at a unique real place corresponding to $\iota_\infty : B \hookrightarrow \mathrm{M}_2(\mathbb{R})$. We call this the *indefinite method*, since B is indefinite, and it is joint work with Matthew Greenberg.

Suppose that F has strict class number 1; then we have $\mathbb{Z}_{F,+}^\times = \{x \in \mathbb{Z}_F^\times : x_i > 0 \text{ for all } i\} = \mathbb{Z}_F^{\times 2}$ and hence $\mathrm{GL}_2^+(\mathbb{Z}_F) = \mathbb{Z}_F^\times \, \mathrm{SL}_2(\mathbb{Z}_F)$. We further assume $B \not\cong \mathrm{M}_2(\mathbb{Q})$ for uniformity of presentation.

Indefinite method: Shimura curve

Let $\mathcal{O}_0(\mathfrak{N}) \subseteq B$ be an Eichler order of level $\mathfrak{N}$ ("upper triangular elements modulo $\mathfrak{N}$"), let

$$\begin{aligned} \mathcal{O}_0(\mathfrak{N})_1^\times &= \{\gamma \in \mathcal{O}_0(\mathfrak{N}) : \mathrm{nrd}(\gamma) = 1\} \\ \Gamma_0(\mathfrak{N}) &= \iota_\infty(\mathcal{O}_0(\mathfrak{N})_1^\times) \subseteq \mathrm{SL}_2(\mathbb{R}). \end{aligned}$$

Then $\Gamma_0(\mathfrak{N})$ is a discrete and cocompact subgroup of $\mathrm{SL}_2(\mathbb{R})$; so $X_0^B(\mathfrak{N}) = \Gamma_0(\mathfrak{N})\backslash\mathcal{H}$ is a Riemann surface, a *Shimura curve*.

A *quaternionic cusp form* for B of parallel weight 2 is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that $f(\gamma z) = (cz + d)^2 f(z)$ for all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\mathfrak{N})$. (No cusps!)

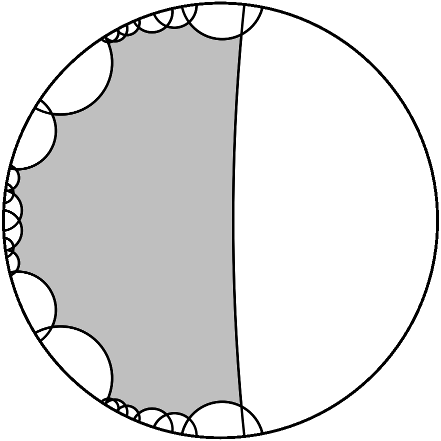
Putting the Jacquet-Langlands correspondence together with the isomorphism of Eichler-Shimura, we have

$$S_2(\mathfrak{N}) \cong S_2^B(\mathfrak{N}) \cong H^1(X_0^B(\mathfrak{N}), \mathbb{C})^+$$

($^+$ for complex conjugation).

Example: fundamental domain

Let F be the (totally real) cubic field with $d_F = 1101 = 3 \cdot 367$. Then $F = \mathbb{Q}(w)$ with $w^3 - w^2 - 9w + 12 = 0$. The field F has Galois group S_3. Here we work with the Shimura curve $X = X_0^B(1)$ associated to F. The curve X has signature $(1; 2^2, 3^5)$.



Example: Hecke data

We obtain the following Hecke data:

$\mathfrak{p}$	$N\mathfrak{p}$	$a(\mathfrak{p})$	$\#J(\mathbb{F}_p)$
$(w-2)$	2	0	3
$(w-3)$	3	-3	7
$(w-1)$	3	-1	5
(w^2+w-7)	4	-3	8
$(w+1)$	19	-6	26
(w^2-2w-1)	23	6	18
$(2w^2-19)$	31	3	29
(w^2-5)	31	0	32
$(3w-5)$	31	4	28

Here, $J = J_0^B(1)$ is the Jacobian of the Shimura curve X.

Equations for elliptic curves

The method of Cremona–Lingham and the methods explained on Tuesday by Deines allow us to find a candidate elliptic curve A to represent the isogeny class of the Jacobian J:

$$\begin{aligned} A : y^2 + wxy + (w^2 + w + 1)y = \\ x^3 + w^2x^2 + (w^2 - 12w + 14)x + (5w^2 - 4w - 9). \end{aligned}$$

We have $j(A) = -1805w^2 - 867w + 14820 \in \mathbb{Z}_F$.

Using the method of Faltings–Serre, we verify that J is indeed isogeneous to A.

However, there is another way to find this equation which gives the conjecturally optimal curve, using power series expansions; we will return to this in a moment.

Modular symbols

The indefinite method can be viewed as a generalization of the method of modular symbols used in the classical case $\Gamma = \Gamma_0(N)$. There, we have a canonical isomorphism

$$\mathcal{S}_2(N) \cong H_1(X_0(N), \mathbb{Z})(\cong H^1(X_0(N), \mathbb{Z}))$$

where $\mathcal{S}_2(N)$ is the space of *cuspidal modular symbols*, the space of paths in $\mathcal{H}^*$ whose endpoints are cusps and which are loops in $X_0(N)$. There is an explicit description of the action of the Hecke operators on the space $\mathcal{S}_2(N)$, and the *Manin trick* (the Euclidean algorithm) gives a method for writing a modular symbol as a $\mathbb{Z}$-linear combination of generating symbols $\gamma_i\{0, \infty\}$. This method has been fruitfully pursued by Cremona, Stein, and others.

Dirichlet modular symbols

The Shimura curves $X = X_0^B(\mathfrak{N})$ do not have cusps, and so the method of modular symbols does not generalize directly. However, the side pairing of a Dirichlet domain for Γ gives an explicit characterization of the gluing relations which describe X as a Riemann surface, hence one obtains a complete description for the homology group $H_1(X, \mathbb{Z})$.

Paths are now written $\{v, \gamma v\}$ for v a vertex on a side paired by $\gamma \in G$. The analogue of the Manin trick in our context is played by the solution to the word problem in Γ. And computationally, these points of view are equivalent.

Indefinite method: Hecke operators

Recall we compute with the (Hecke module) $H^1(X, \mathbb{C})$, where $X = X_0^B(\mathfrak{N}) = \Gamma\backslash\mathcal{H}$ and $\Gamma = \Gamma_0(\mathfrak{N})$. We have simply

$$H^1(X, \mathbb{C}) = H^1(\Gamma, \mathbb{C}) = \mathrm{Hom}(\Gamma, \mathbb{C});$$

if X has genus g, then $\mathrm{Hom}(\Gamma, \mathbb{C})$ is a vector space of dimension $2g$ with basis given by the characteristic functions of a set of generators for $\Gamma/[\Gamma, \Gamma]$.

The space $\mathrm{Hom}(\Gamma, \mathbb{C})$ is equipped with Hecke operators $T_{\mathfrak{p}}$ as follows. Let $\mathfrak{p} \subseteq \mathbb{Z}_F$ be a prime with $\mathfrak{p} \nmid \mathfrak{N}$ and let $k_{\mathfrak{p}}$ be its residue field. For $f : \Gamma \to \mathbb{C}$, we define

$$(f \mid T_{\mathfrak{p}})(\gamma) = \sum_{a \in \mathbb{P}^1(k_{\mathfrak{p}})} f(\delta_a)$$

where α_a for $a \in \mathbb{P}^1(k_{\mathfrak{p}})$ are generators of the left $\mathcal{O}$-ideals of norm $\mathfrak{p}$ having totally positive reduced norm and

$$\delta_a = \alpha_a \gamma \alpha_{\gamma^* a}^{-1} \in \Gamma.$$

Indefinite method: computational problems

To compute effectively the systems of Hecke eigenvalues in the cohomology of a Shimura curve, we need algorithms to:

1. Compute an explicit finite presentation of Γ;
2. Compute a generator (with totally positive reduced norm) of a left ideal $I \subseteq \mathcal{O}$; and
3. Given $\delta \in \Gamma$, write δ as an explicit word in the generators for Γ, i.e., solve the word problem in Γ.

Problems 1 and 3 are solved by computing a *Dirichlet domain*, a fundamental domain for Γ equipped with a side pairing. A reduction algorithm is used to solve the word problem. Problem 2 is solved using lattice methods.

Power series expansions

The method of power series expansions for modular forms (V–Willis, Klug), gives an direct and efficient method for computing the elliptic curve associated to f.

There is another recent method, due to Nelson, which directly computes the Shimizu lift of a modular form on a Shimura curve over $\mathbb{Q}$, which could be generalized to totally real fields.

Our method is inspired by the method of Stark and Hejhal, who used the same basic principle to compute Fourier expansions for Maass forms on $\mathrm{SL}_2(\mathbb{Z})$ and the Hecke triangle groups.

Basic idea

Let Γ be a cocompact Fuchsian group. Let $D \subset \mathcal{D}$ be a fundamental domain for Γ contained in a circle of radius $\rho > 0$. Let $f \in S_k(\Gamma)$. We consider an approximation

$$f(z) \approx f_N(z) = (1-w)^k \sum_{n=0}^{N} b_n w^n$$

valid for all $|w| \leq \rho$ to some precision $\epsilon > 0$.

For a point $w = w(z) \notin D$, there exists $g \in \Gamma$ such that $z' = gz \in D$; by the modularity of f we have

$$f_N(z') \approx f(z') = j(g,z)^k f(z)$$

$$(1-w')^k \sum_{n=0}^{N} b_n (w')^n \approx j(g,z)^k (1-w)^k \sum_{n=0}^{N} b_n w^n,$$

imposing a (nontrivial) linear relation on the unknowns b_n.

Example

Let $F = \mathbb{Q}(a) = \mathbb{Q}(\sqrt{5})$ where $a^2 + a - 1 = 0$, and let $\mathbb{Z}_F$ be its ring of integers. Let $\mathfrak{p} = (5a+2)$, so $N\mathfrak{p} = 31$. Let B be the quaternion algebra ramified at $\mathfrak{p}$ and the real place sending $\sqrt{5}$ to its positive real root: we take $B = \left(\dfrac{a, 5a+2}{F}\right)$.

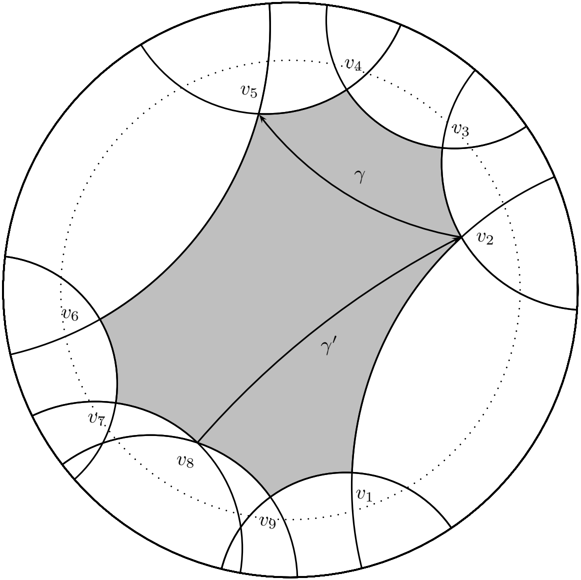
As before, we compute a maximal order $\mathcal{O} \subset B$. Then $\Gamma = \Gamma_0^B(1)$ has signature $(1; 2^2)$, so $X = \Gamma\backslash\mathcal{H}$ can be given the structure of a compact Riemann surface of genus 1. The space $M_2(\Gamma)$ of modular forms on Γ of weight 2 is 1-dimensional.

The field $K = F(\sqrt{-7})$ embeds in $\mathcal{O}$ with

$$\mu = -\frac{1}{2} - \frac{5a+10}{2}i - \frac{a+2}{2}j + \frac{3a-5}{2}ij \in \mathcal{O}$$

and $\mathbb{Z}_F[\mu] = \mathbb{Z}_K$ the maximal order with class number 1. We take $p = -3.1653\ldots + 1.41783\ldots \in \mathcal{H}$ to be the fixed point of μ.

Fundamental domain



An expansion for the form

$$
\begin{aligned}
f(z) = (1-w)^2 \bigg(& 1 + (\Theta w) - \frac{70a+114}{2!}(\Theta w)^2 \\
& - \frac{8064a+13038}{3!}(\Theta w)^3 + \frac{174888a+282972}{4!}(\Theta w)^4 \\
& - \frac{13266960a+21466440}{5!}(\Theta w)^5 \\
& - \frac{1826784288a+2955799224}{6!}(\Theta w)^6 \\
& - \frac{2388004416a+3863871648}{7!}(\Theta w)^7 + \dots \bigg)
\end{aligned}
$$

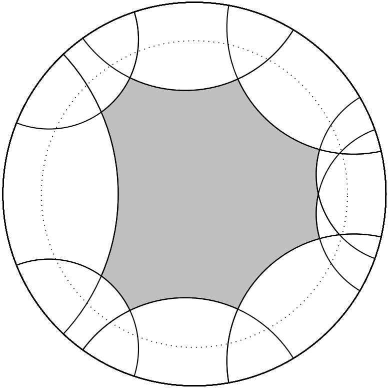
where

$$\Theta = 0.046218579529208499918\ldots - 0.075987317531832568351\ldots i$$

is a period related to the CM abelian variety given by the point p.

The conjugate curve

We further compute the other embedding of this form by repeating the above with an algebra ramified at $\mathfrak{p}$ and the other real place.



The coefficients agree with the conjugates under the nontrivial element of $\mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q})$.

Finding an equation

We can identify the equation of the Jacobian J of the curve X by computing the associated periods. We first identify the group Γ using the sidepairing relations coming from the computation of $D(p)$:

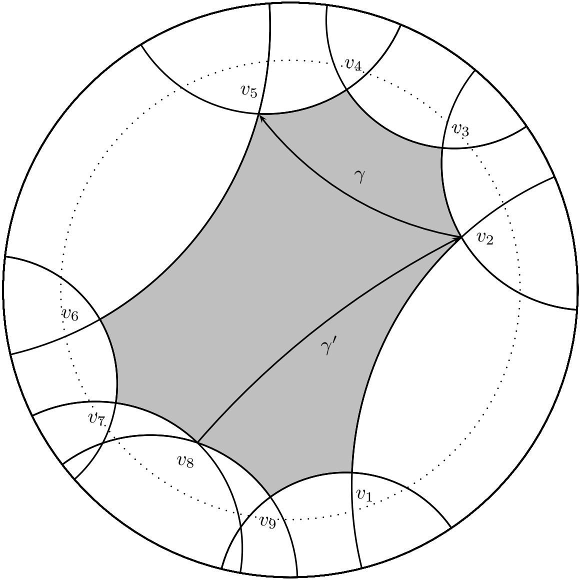
$$\Gamma \cong \langle \gamma, \gamma', \delta_1, \delta_2 \mid \delta_1^2 = \delta_2^2 = \gamma^{-1}\gamma'^{-1}\delta_1\gamma\gamma'\delta_2 = 1 \rangle$$

where

$$\begin{aligned} \gamma &= \frac{a+2}{2} - \frac{2a+3}{2}i + \frac{a+1}{2}ij \\ \gamma' &= \frac{2a+3}{2} + \frac{7a+10}{2}i + \frac{a+2}{2}j - (3a+5)ij \end{aligned}$$

generate the free part of the maximal abelian quotient of Γ.

Fundamental domain again



Finding an equation

Therefore, we compute two independent periods ω_1, ω_2

$$\omega_1 = \int_{v_2}^{v_5} f(z)\frac{dw}{(1-w)^2} \approx \left(\sum_{n=0}^{N} \frac{b_n}{n+1} w^{n+1}\right)\Bigg|_{v_2}^{v_5}$$

$$= -0.654017\ldots + 0.397799\ldots i$$

$$\omega_2 = \int_{v_8}^{v_2} f(z)\frac{dw}{(1-w)^2} = 0.952307\ldots + 0.829145\ldots i.$$

We then compute the j-invariant

$$j(\omega_1/\omega_2) = -18733.423\ldots$$

$$= -\frac{118896117223833394a + 8629385062119691}{31^8}.$$

We identify the elliptic curve J as

$$y^2 + xy - ay = x^3 - (a-1)x^2 - (31a+75)x - (141a+303).$$

Heegner point

Finally, we compute the image on J of a degree zero divisor on X.

The fixed points w_1, w_2 of the two elliptic generators δ_1 and δ_2 are CM points of discriminant -4. Let $K = F(i)$ and consider the image of $[w_1] - [w_2]$ on J given by the Abel-Jacobi map as

$$\int_{w_1}^{w_2} f(z) \frac{dw}{(1-w)^2} \equiv -0.177051\ldots - 0.291088\ldots i \pmod{\Lambda}$$

where $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ is the period lattice of J. Evaluating the elliptic exponential, we find the point

$$(-10.503797\ldots, 5.560915\ldots - 44.133005\ldots i) \in J(\mathbb{C})$$

which matches to the precision computed $\epsilon = 10^{-20}$ the point

$$Y = \left(\frac{-81a - 118}{16}, \frac{(358a + 1191)i + (194a + 236)}{64} \right) \in J(K).$$

We have $J(K) \cong \mathbb{Z}/4\mathbb{Z} \oplus \mathbb{Z}$ and Y generates the free quotient.

Final comments

Three significant algorithmic improvements on the numerical linear algebra in power series method:

1. There is a “black box” to evaluate the relevant matrix multiplication without writing down the matrix!;
2. “Federalism”: use power series expansions around several points to reduce the required radius;
3. Implicitly restarted Arnoldi iteration on the Krylov subspace.

One can compute in higher weight and arbitrary class number by modifying the coefficient module and working with a disconnected Shimura variety. One can also obtain eigenvalues for the Atkin-Lehner operators.

The Jacquet-Langlands correspondence implies that the definite and indefinite methods overlap when there is a prime $\mathfrak{p} \parallel \mathfrak{N}$. Therefore, in many cases we can use either approach—or both approaches, as a way of verifying the computation.

Work to do

Many projects remain:

1. Provably match up Hilbert modular forms with elliptic curves in the LMFDB;
2. Build a database in higher weight (and with character);
3. Optimize numerical linear algebra in power series method;
4. “Automate” modularity proving (is it in NP?);
5. Compute interesting examples and some statistics;
6. Find unique (reduced) model for elliptic curves over number fields;
7. Investigate Mazur’s theorem (Ogg’s conjecture) for QM abelian varieties.