Computing automorphic forms on Shimura curves over fields with arbitrary class number

John Voight
University of Vermont

Ninth Algorithmic Number Theory Symposium (ANTS-IX)
INRIA, Nancy, France
20 July 2010

Main algorithm

Main algorithm

Our paper is concerned with the following theorem.

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which,

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which, given a totally real field F,

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which, given a totally real field F, a weight $k \in (2\mathbb{Z}_{>0})^{[F:\mathbb{Q}]}$,

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which, given a totally real field F, a weight $k \in (2\mathbb{Z}_{>0})^{[F:\mathbb{Q}]}$, and a nonzero ideal $\mathfrak{N} \subset \mathbb{Z}_F$,

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which, given a totally real field F*, a weight* $k \in (2\mathbb{Z}_{>0})^{[F:\mathbb{Q}]}$*, and a nonzero ideal* $\mathfrak{N} \subset \mathbb{Z}_F$*, computes the system of Hecke eigenvalues for the space* $S_k(\mathfrak{N})$

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which, given a totally real field F, a weight $k \in (2\mathbb{Z}_{>0})^{[F:\mathbb{Q}]}$, and a nonzero ideal $\mathfrak{N} \subset \mathbb{Z}_F$, computes the system of Hecke eigenvalues for the space $S_k(\mathfrak{N})$ of Hilbert modular cusp forms of weight k and level $\mathfrak{N}$ over F.

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which, given a totally real field F, a weight $k \in (2\mathbb{Z}_{>0})^{[F:\mathbb{Q}]}$, and a nonzero ideal $\mathfrak{N} \subset \mathbb{Z}_F$, computes the system of Hecke eigenvalues for the space $S_k(\mathfrak{N})$ of Hilbert modular cusp forms of weight k and level $\mathfrak{N}$ over F.

In other words,

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which, given a totally real field F, a weight $k \in (2\mathbb{Z}_{>0})^{[F:\mathbb{Q}]}$, and a nonzero ideal $\mathfrak{N} \subset \mathbb{Z}_F$, computes the system of Hecke eigenvalues for the space $S_k(\mathfrak{N})$ of Hilbert modular cusp forms of weight k and level $\mathfrak{N}$ over F.

In other words, there exists an explicit finite procedure which takes as input

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which, given a totally real field F, a weight $k \in (2\mathbb{Z}_{>0})^{[F:\mathbb{Q}]}$, and a nonzero ideal $\mathfrak{N} \subset \mathbb{Z}_F$, computes the system of Hecke eigenvalues for the space $S_k(\mathfrak{N})$ of Hilbert modular cusp forms of weight k and level $\mathfrak{N}$ over F.

In other words, there exists an explicit finite procedure which takes as input the field F,

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which, given a totally real field F, a weight $k \in (2\mathbb{Z}_{>0})^{[F:\mathbb{Q}]}$, and a nonzero ideal $\mathfrak{N} \subset \mathbb{Z}_F$, computes the system of Hecke eigenvalues for the space $S_k(\mathfrak{N})$ of Hilbert modular cusp forms of weight k and level $\mathfrak{N}$ over F.

In other words, there exists an explicit finite procedure which takes as input the field F, the ideal $\mathfrak{N} \subset \mathbb{Z}_F$,

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which, given a totally real field F, a weight $k \in (2\mathbb{Z}_{>0})^{[F:\mathbb{Q}]}$, and a nonzero ideal $\mathfrak{N} \subset \mathbb{Z}_F$, computes the system of Hecke eigenvalues for the space $S_k(\mathfrak{N})$ of Hilbert modular cusp forms of weight k and level $\mathfrak{N}$ over F.

In other words, there exists an explicit finite procedure which takes as input the field F, the ideal $\mathfrak{N} \subset \mathbb{Z}_F$, and the vector k encoded in bits (in the usual way),

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which, given a totally real field F, a weight $k \in (2\mathbb{Z}_{>0})^{[F:\mathbb{Q}]}$, and a nonzero ideal $\mathfrak{N} \subset \mathbb{Z}_F$, computes the system of Hecke eigenvalues for the space $S_k(\mathfrak{N})$ of Hilbert modular cusp forms of weight k and level $\mathfrak{N}$ over F.

In other words, there exists an explicit finite procedure which takes as input the field F, the ideal $\mathfrak{N} \subset \mathbb{Z}_F$, and the vector k encoded in bits (in the usual way), and outputs:

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which, given a totally real field F, a weight $k \in (2\mathbb{Z}_{>0})^{[F:\mathbb{Q}]}$, and a nonzero ideal $\mathfrak{N} \subset \mathbb{Z}_F$, computes the system of Hecke eigenvalues for the space $S_k(\mathfrak{N})$ of Hilbert modular cusp forms of weight k and level $\mathfrak{N}$ over F.

In other words, there exists an explicit finite procedure which takes as input the field F, the ideal $\mathfrak{N} \subset \mathbb{Z}_F$, and the vector k encoded in bits (in the usual way), and outputs: a finite set of sequences $(a_f(\mathfrak{p}))_{\mathfrak{p}}$

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which, given a totally real field F, a weight $k \in (2\mathbb{Z}_{>0})^{[F:\mathbb{Q}]}$, and a nonzero ideal $\mathfrak{N} \subset \mathbb{Z}_F$, computes the system of Hecke eigenvalues for the space $S_k(\mathfrak{N})$ of Hilbert modular cusp forms of weight k and level $\mathfrak{N}$ over F.

In other words, there exists an explicit finite procedure which takes as input the field F, the ideal $\mathfrak{N} \subset \mathbb{Z}_F$, and the vector k encoded in bits (in the usual way), and outputs: a finite set of sequences $(a_f(\mathfrak{p}))_{\mathfrak{p}}$ encoding the Hecke eigenvalues for each constituent f in $S_k(\mathfrak{N})$,

Main algorithm

Our paper is concerned with the following theorem.

Theorem (Dembélé-Donnelly, Greenberg-V)

There exists an algorithm which, given a totally real field F, a weight $k \in (2\mathbb{Z}_{>0})^{[F:\mathbb{Q}]}$, and a nonzero ideal $\mathfrak{N} \subset \mathbb{Z}_F$, computes the system of Hecke eigenvalues for the space $S_k(\mathfrak{N})$ of Hilbert modular cusp forms of weight k and level $\mathfrak{N}$ over F.

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

Example 1: Hecke eigenvalues

Example 1: Hecke eigenvalues

Let F be the (totally real) cubic field with $d_F = 1101 = 3 \cdot 367$.

Example 1: Hecke eigenvalues

Let F be the (totally real) cubic field with $d_F = 1101 = 3 \cdot 367$.
Then $F = \mathbb{Q}(w)$ with $w^3 - w^2 - 9w + 12 = 0$.

Example 1: Hecke eigenvalues

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 and strict class number 1.

Example 1: Hecke eigenvalues

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 and strict class number 1.

We find that the space $S_2(1)$ of Hilbert cusp forms of parallel weight 2 (i.e. $k = (2,2,2)$) and level (1) has $\dim_{\mathbb{C}} S_2(1) = 1$.

Example 1: Hecke eigenvalues

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 and strict class number 1.

We find that the space $S_2(1)$ of Hilbert cusp forms of parallel weight 2 (i.e. $k = (2, 2, 2)$) and level (1) has $\dim_{\mathbb{C}} S_2(1) = 1$.

$N\mathfrak{p}$	π	$a(\mathfrak{p})$
2	$w - 2$	0
3	$w - 3$	-3
3	$w - 1$	-1
4	$w^2 + w - 7$	-3
19	$w + 1$	-6
23	$w^2 - 2w - 1$	6

Example 1: Hecke eigenvalues

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 and strict class number 1.

We find that the space $S_2(1)$ of Hilbert cusp forms of parallel weight 2 (i.e. $k = (2, 2, 2)$) and level (1) has $\dim_{\mathbb{C}} S_2(1) = 1$.

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

Example 1: Hecke eigenvalues

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 and strict class number 1.

We find that the space $S_2(1)$ of Hilbert cusp forms of parallel weight 2 (i.e. $k = (2, 2, 2)$) and level (1) has $\dim_{\mathbb{C}} S_2(1) = 1$.

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

There exists a (modular!) elliptic curve J over F such that $\#J(\mathbb{F}_\mathfrak{p}) = N\mathfrak{p} + 1 - a(\mathfrak{p})$...

Shimura curves

Shimura curves

In analogy with the classical modular curves $X_0(N)$, there are curves called *Shimura curves* whose cohomology contains the Hecke module $S_k(\mathfrak{N})$,

Shimura curves

In analogy with the classical modular curves $X_0(N)$, there are curves called *Shimura curves* whose cohomology contains the Hecke module $S_k(\mathfrak{N})$, in accordance with the Langlands philosophy.

Shimura curves

In analogy with the classical modular curves $X_0(N)$, there are curves called *Shimura curves* whose cohomology contains the Hecke module $S_k(\mathfrak{N})$, in accordance with the Langlands philosophy.

Suppose that $n = [F : \mathbb{Q}]$ is odd.

Shimura curves

In analogy with the classical modular curves $X_0(N)$, there are curves called *Shimura curves* whose cohomology contains the Hecke module $S_k(\mathfrak{N})$, in accordance with the Langlands philosophy.

Suppose that $n = [F : \mathbb{Q}]$ is odd. Let B be the quaternion algebra over F which is split at all finite places

Shimura curves

In analogy with the classical modular curves $X_0(N)$, there are curves called *Shimura curves* whose cohomology contains the Hecke module $S_k(\mathfrak{N})$, in accordance with the Langlands philosophy.

Suppose that $n = [F : \mathbb{Q}]$ is odd. Let B be the quaternion algebra over F which is split at all finite places and ramified at all but one real place,

Shimura curves

In analogy with the classical modular curves $X_0(N)$, there are curves called *Shimura curves* whose cohomology contains the Hecke module $S_k(\mathfrak{N})$, in accordance with the Langlands philosophy.

Suppose that $n = [F : \mathbb{Q}]$ is odd. Let B be the quaternion algebra over F which is split at all finite places and ramified at all but one real place, corresponding to $\iota_\infty : B \hookrightarrow \mathrm{M}_2(\mathbb{R})$.

Shimura curves

In analogy with the classical modular curves $X_0(N)$, there are curves called *Shimura curves* whose cohomology contains the Hecke module $S_k(\mathfrak{N})$, in accordance with the Langlands philosophy.

Suppose that $n = [F : \mathbb{Q}]$ is odd. Let B be the quaternion algebra over F which is split at all finite places and ramified at all but one real place, corresponding to $\iota_\infty : B \hookrightarrow \mathrm{M}_2(\mathbb{R})$.

For the moment, suppose that F has strict class number 1.

Shimura curves

In analogy with the classical modular curves $X_0(N)$, there are curves called *Shimura curves* whose cohomology contains the Hecke module $S_k(\mathfrak{N})$, in accordance with the Langlands philosophy.

Suppose that $n = [F : \mathbb{Q}]$ is odd. Let B be the quaternion algebra over F which is split at all finite places and ramified at all but one real place, corresponding to $\iota_\infty : B \hookrightarrow \mathrm{M}_2(\mathbb{R})$.

For the moment, suppose that F has strict class number 1. Further, assume $B \not\cong M_2(\mathbb{Q})$ for uniformity of presentation.

Shimura curves

Shimura curves

Shimura curves can be described by quotients of the upper half-plane by (arithmetic) Fuchsian groups.

Shimura curves

Shimura curves can be described by quotients of the upper half-plane by (arithmetic) Fuchsian groups.

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

Shimura curves

Shimura curves can be described by quotients of the upper half-plane by (arithmetic) Fuchsian groups.

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

$$\mathcal{O}_0(\mathfrak{N})_1^\times = \{\gamma \in \mathcal{O}_0(\mathfrak{N}) : \mathrm{nrd}(\gamma) = 1\},$$

Shimura curves

Shimura curves can be described by quotients of the upper half-plane by (arithmetic) Fuchsian groups.

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

$$\mathcal{O}_0(\mathfrak{N})_1^\times = \{\gamma \in \mathcal{O}_0(\mathfrak{N}) : \mathrm{nrd}(\gamma) = 1\},$$

and let

$$\Gamma_0(\mathfrak{N}) = \iota_\infty(\mathcal{O}_0(\mathfrak{N})_1^\times)/\{\pm 1\} \subset \mathrm{PSL}_2(\mathbb{R}).$$

Shimura curves

Shimura curves can be described by quotients of the upper half-plane by (arithmetic) Fuchsian groups.

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

$$\mathcal{O}_0(\mathfrak{N})_1^\times = \{\gamma \in \mathcal{O}_0(\mathfrak{N}) : \mathrm{nrd}(\gamma) = 1\},$$

and let

$$\Gamma_0(\mathfrak{N}) = \iota_\infty(\mathcal{O}_0(\mathfrak{N})_1^\times)/\{\pm 1\} \subset \mathrm{PSL}_2(\mathbb{R}).$$

Then $\Gamma_0(\mathfrak{N})$ is a discrete and cocompact subgroup of $\mathrm{PSL}_2(\mathbb{R})$;

Shimura curves

Shimura curves can be described by quotients of the upper half-plane by (arithmetic) Fuchsian groups.

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

$$\mathcal{O}_0(\mathfrak{N})_1^\times = \{\gamma \in \mathcal{O}_0(\mathfrak{N}) : \mathrm{nrd}(\gamma) = 1\},$$

and let

$$\Gamma_0(\mathfrak{N}) = \iota_\infty(\mathcal{O}_0(\mathfrak{N})_1^\times)/\{\pm 1\} \subset \mathrm{PSL}_2(\mathbb{R}).$$

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

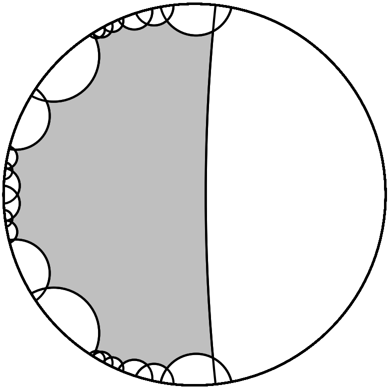
Example: The Shimura curve

Example: The Shimura curve

The Shimura curve $X(1) = X_0^B(1)$ associated to F has signature $(1; 2^2, 3^5)$.

Example: The Shimura curve

The Shimura curve $X(1) = X_0^B(1)$ associated to F has signature $(1; 2^2, 3^5)$.



Jacquet-Langlands correspondence

Jacquet-Langlands correspondence

The Jacquet-Langlands correspondence yields an isomorphism of Hecke modules

Jacquet-Langlands correspondence

The Jacquet-Langlands correspondence yields an isomorphism of Hecke modules

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

Jacquet-Langlands correspondence

The Jacquet-Langlands correspondence yields an 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 modular forms over B of level $\mathfrak{N}$.

Jacquet-Langlands correspondence

The Jacquet-Langlands correspondence yields an 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 modular forms over B of level $\mathfrak{N}$.

A *quaternionic cusp form* for B of parallel weight 2 and level $\mathfrak{N}$

Jacquet-Langlands correspondence

The Jacquet-Langlands correspondence yields an 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 modular forms over B of level $\mathfrak{N}$.

A *quaternionic cusp form* for B of parallel weight 2 and level $\mathfrak{N}$ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$

Jacquet-Langlands correspondence

The Jacquet-Langlands correspondence yields an 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 modular forms over B of level $\mathfrak{N}$.

A *quaternionic cusp form* for B of parallel weight 2 and level $\mathfrak{N}$ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that

$$f(\gamma z) = (cz + d)^2 f(z) \text{ for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\mathfrak{N}).$$

Jacquet-Langlands correspondence

The Jacquet-Langlands correspondence yields an 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 modular forms over B of level $\mathfrak{N}$.

A *quaternionic cusp form* for B of parallel weight 2 and level $\mathfrak{N}$ is a holomorphic function $f : \mathcal{H} \to \mathbb{C}$ such that

$$f(\gamma z) = (cz+d)^2 f(z) \text{ for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(\mathfrak{N}).$$

(No cusps!)

Example: Identifying the elliptic curve

Example: Identifying the elliptic curve

We find our elliptic curve J with $\#J(\mathbb{F}_{\mathfrak{p}}) = N\mathfrak{p} + 1 - a(\mathfrak{p})$ as the Jacobian of $X(1)$.

Example: Identifying the elliptic curve

We find our elliptic curve J with $\#J(\mathbb{F}_{\mathfrak{p}}) = N\mathfrak{p} + 1 - a(\mathfrak{p})$ as the Jacobian of $X(1)$.

Using a method of Cremona and Lingham, in fact we can find a candidate elliptic curve A to represent the isogeny class of J:

Example: Identifying the elliptic curve

We find our elliptic curve J with $\#J(\mathbb{F}_{\mathfrak{p}}) = N\mathfrak{p} + 1 - a(\mathfrak{p})$ as the Jacobian of $X(1)$.

Using a method of Cremona and Lingham, in fact we can find a candidate elliptic curve A to represent the isogeny class of J:

$$A : y^2 + w(w+1)xy + (w+1)y = x^3 + w^2x^2 + a_4x + a_6$$

where a_4 is equal to

$$-139671409350296864w^2 - 235681481839938468w + 623672370161912822$$

and a_6 is equal to

$$1107260540564019301821064 63w^2 + 1866839095087977344668356726w - 4944231842528186971355327 43.$$

Example: Identifying the elliptic curve

We find our elliptic curve J with $\#J(\mathbb{F}_\mathfrak{p}) = N\mathfrak{p} + 1 - a(\mathfrak{p})$ as the Jacobian of $X(1)$.

Using a method of Cremona and Lingham, in fact we can find a candidate elliptic curve A to represent the isogeny class of J:

$$A : y^2 + w(w+1)xy + (w+1)y = x^3 + w^2x^2 + a_4x + a_6$$

where a_4 is equal to

$$-139671409350296864w^2 - 235681481839938468w + 623672370161912822$$

and a_6 is equal to

$$1107260540564019301821064 63w^2 + 1868390950879773446683567 26w - 4944231842528186971355327 43.$$

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

Algorithmic methods

Algorithmic methods

When $n = [F : \mathbb{Q}]$ is odd, the method used to compute these Hecke eigenvalues can be viewed as a generalization of the method of modular symbols:

Algorithmic methods

When $n = [F : \mathbb{Q}]$ is odd, the method used to compute these Hecke eigenvalues can be viewed as a generalization of the method of modular symbols: for the group $\Gamma_0(N) \subset \mathrm{PSL}_2(\mathbb{Z})$,

Algorithmic methods

When $n = [F : \mathbb{Q}]$ is odd, the method used to compute these Hecke eigenvalues can be viewed as a generalization of the method of modular symbols: for the group $\Gamma_0(N) \subset \mathrm{PSL}_2(\mathbb{Z})$, one computes with

$$S_2(N)$$

Algorithmic methods

When $n = [F : \mathbb{Q}]$ is odd, the method used to compute these Hecke eigenvalues can be viewed as a generalization of the method of modular symbols: for the group $\Gamma_0(N) \subset \mathrm{PSL}_2(\mathbb{Z})$, one computes with

$$S_2(N) \cong H_1(X_0(N), \mathbb{C}; \mathrm{cusps})^+$$

Algorithmic methods

When $n = [F : \mathbb{Q}]$ is odd, the method used to compute these Hecke eigenvalues can be viewed as a generalization of the method of modular symbols: for the group $\Gamma_0(N) \subset \mathrm{PSL}_2(\mathbb{Z})$, one computes with

$$S_2(N) \cong H_1(X_0(N), \mathbb{C}; \mathrm{cusps})^+$$

where the $+$ indicates the $+$-space for complex conjugation.

Algorithmic methods

When $n = [F : \mathbb{Q}]$ is odd, the method used to compute these Hecke eigenvalues can be viewed as a generalization of the method of modular symbols: for the group $\Gamma_0(N) \subset \mathrm{PSL}_2(\mathbb{Z})$, one computes with

$$S_2(N) \cong H_1(X_0(N), \mathbb{C}; \mathrm{cusps})^+$$

where the $+$ indicates the $+$-space for complex conjugation.

When $B \not\cong \mathrm{M}_2(\mathbb{Q})$ (no cusps),

Algorithmic methods

When $n = [F : \mathbb{Q}]$ is odd, the method used to compute these Hecke eigenvalues can be viewed as a generalization of the method of modular symbols: for the group $\Gamma_0(N) \subset \mathrm{PSL}_2(\mathbb{Z})$, one computes with

$$S_2(N) \cong H_1(X_0(N), \mathbb{C}; \mathrm{cusps})^+$$

where the $+$ indicates the $+$-space for complex conjugation.

When $B \not\cong \mathrm{M}_2(\mathbb{Q})$ (no cusps), we can still identify

Algorithmic methods

When $n = [F : \mathbb{Q}]$ is odd, the method used to compute these Hecke eigenvalues can be viewed as a generalization of the method of modular symbols: for the group $\Gamma_0(N) \subset \mathrm{PSL}_2(\mathbb{Z})$, one computes with

$$S_2(N) \cong H_1(X_0(N), \mathbb{C}; \mathrm{cusps})^+$$

where the $+$ indicates the $+$-space for complex conjugation.

When $B \not\cong \mathrm{M}_2(\mathbb{Q})$ (no cusps), we can still identify

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

Algorithmic methods

When $n = [F : \mathbb{Q}]$ is odd, the method used to compute these Hecke eigenvalues can be viewed as a generalization of the method of modular symbols: for the group $\Gamma_0(N) \subset \mathrm{PSL}_2(\mathbb{Z})$, one computes with

$$S_2(N) \cong H_1(X_0(N), \mathbb{C}; \mathrm{cusps})^+$$

where the $+$ indicates the $+$-space for complex conjugation.

When $B \not\cong \mathrm{M}_2(\mathbb{Q})$ (no cusps), we can still identify

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

Algorithmic methods

When $n = [F : \mathbb{Q}]$ is odd, the method used to compute these Hecke eigenvalues can be viewed as a generalization of the method of modular symbols: for the group $\Gamma_0(N) \subset \mathrm{PSL}_2(\mathbb{Z})$, one computes with

$$S_2(N) \cong H_1(X_0(N), \mathbb{C}; \mathrm{cusps})^+$$

where the $+$ indicates the $+$-space for complex conjugation.

When $B \not\cong \mathrm{M}_2(\mathbb{Q})$ (no cusps), we can still identify

$$S_2^B(\mathfrak{N}) \cong H^1(X_0(\mathfrak{N}), \mathbb{C})^+ \cong H^1(\Gamma_0(\mathfrak{N}), \mathbb{C})^+$$

Algorithmic methods

When $n = [F : \mathbb{Q}]$ is odd, the method used to compute these Hecke eigenvalues can be viewed as a generalization of the method of modular symbols: for the group $\Gamma_0(N) \subset \mathrm{PSL}_2(\mathbb{Z})$, one computes with

$$S_2(N) \cong H_1(X_0(N), \mathbb{C}; \text{cusps})^+$$

where the $+$ indicates the $+$-space for complex conjugation.

When $B \not\cong \mathrm{M}_2(\mathbb{Q})$ (no cusps), we can still identify

$$S_2^B(\mathfrak{N}) \cong H^1(X_0(\mathfrak{N}), \mathbb{C})^+ \cong H^1(\Gamma_0(\mathfrak{N}), \mathbb{C})^+ \cong \mathrm{Hom}(\Gamma_0(\mathfrak{N}), \mathbb{C})^+;$$

Algorithmic methods

When $n = [F : \mathbb{Q}]$ is odd, the method used to compute these Hecke eigenvalues can be viewed as a generalization of the method of modular symbols: for the group $\Gamma_0(N) \subset \mathrm{PSL}_2(\mathbb{Z})$, one computes with

$$S_2(N) \cong H_1(X_0(N), \mathbb{C}; \mathrm{cusps})^+$$

where the $+$ indicates the $+$-space for complex conjugation.

When $B \not\cong \mathrm{M}_2(\mathbb{Q})$ (no cusps), we can still identify

$$S_2^B(\mathfrak{N}) \cong H^1(X_0(\mathfrak{N}), \mathbb{C})^+ \cong H^1(\Gamma_0(\mathfrak{N}), \mathbb{C})^+ \cong \mathrm{Hom}(\Gamma_0(\mathfrak{N}), \mathbb{C})^+;$$

we compute this space as a Hecke module by working explicitly with a presentation for the group $\Gamma_0(\mathfrak{N})$, using an algorithm for quaternionic ideal principalization for the Hecke operators.

Extensions

Extensions

If $n = [F : \mathbb{Q}]$ is even, a different method using the theory of Brandt matrices is used;

Extensions

If $n = [F : \mathbb{Q}]$ is even, a different method using the theory of Brandt matrices is used; it was extended to totally real fields F of arbitrary class number by Dembélé and Donnelly in ANTS VIII.

Extensions

If $n = [F : \mathbb{Q}]$ is even, a different method using the theory of Brandt matrices is used; it was extended to totally real fields F of arbitrary class number by Dembélé and Donnelly in ANTS VIII. (See also work by Gunnells and Yasaki.)

Extensions

If $n = [F : \mathbb{Q}]$ is even, a different method using the theory of Brandt matrices is used; it was extended to totally real fields F of arbitrary class number by Dembélé and Donnelly in ANTS VIII. (See also work by Gunnells and Yasaki.)

So the case left is when $n = [F : \mathbb{Q}]$ is odd and F with (strict) class number > 1;

Extensions

If $n = [F : \mathbb{Q}]$ is even, a different method using the theory of Brandt matrices is used; it was extended to totally real fields F of arbitrary class number by Dembélé and Donnelly in ANTS VIII. (See also work by Gunnells and Yasaki.)

So the case left is when $n = [F : \mathbb{Q}]$ is odd and F with (strict) class number > 1; in this case, the natural object with an action of Hecke operators is

$$X(\mathbb{C})$$

Extensions

If $n = [F : \mathbb{Q}]$ is even, a different method using the theory of Brandt matrices is used; it was extended to totally real fields F of arbitrary class number by Dembélé and Donnelly in ANTS VIII. (See also work by Gunnells and Yasaki.)

So the case left is when $n = [F : \mathbb{Q}]$ is odd and F with (strict) class number > 1; in this case, the natural object with an action of Hecke operators is

$$X(\mathbb{C}) = \bigsqcup_{[\mathfrak{b}] \in \mathrm{Cl}^+ \mathbb{Z}_F} X_{\mathfrak{b}}(1)(\mathbb{C}),$$

a disjoint union of curves indexed by the strict class group of F.

Example 2

Example 2

Let $F = \mathbb{Q}(w)$ where $w^3 - 11w - 11 = 0$.

Example 2

Let $F = \mathbb{Q}(w)$ where $w^3 - 11w - 11 = 0$. The discriminant of F is equal to $2057 = 11^2 17$ and $\mathbb{Z}_F = \mathbb{Z}[w]$.

Example 2

Let $F = \mathbb{Q}(w)$ where $w^3 - 11w - 11 = 0$. The discriminant of F is equal to $2057 = 11^2 17$ and $\mathbb{Z}_F = \mathbb{Z}[w]$. We have $\mathrm{Cl}(\mathbb{Z}_F) = \{1\}$ and $\mathrm{Cl}^+(\mathbb{Z}_F) \cong \mathbb{Z}/2\mathbb{Z}$

Example 2

Let $F = \mathbb{Q}(w)$ where $w^3 - 11w - 11 = 0$. The discriminant of F is equal to $2057 = 11^2 17$ and $\mathbb{Z}_F = \mathbb{Z}[w]$. We have $\mathrm{Cl}(\mathbb{Z}_F) = \{1\}$ and $\mathrm{Cl}^+(\mathbb{Z}_F) \cong \mathbb{Z}/2\mathbb{Z}$ with the nontrivial class represented by the ideal $\mathfrak{b} = (w^2 - 2w - 6)\mathbb{Z}_F$ with $\mathrm{N}(\mathfrak{b}) = 7$.

Example 2

Let $F = \mathbb{Q}(w)$ where $w^3 - 11w - 11 = 0$. The discriminant of F is equal to $2057 = 11^2 17$ and $\mathbb{Z}_F = \mathbb{Z}[w]$. We have $\mathrm{Cl}(\mathbb{Z}_F) = \{1\}$ and $\mathrm{Cl}^+(\mathbb{Z}_F) \cong \mathbb{Z}/2\mathbb{Z}$ with the nontrivial class represented by the ideal $\mathfrak{b} = (w^2 - 2w - 6)\mathbb{Z}_F$ with $\mathrm{N}(\mathfrak{b}) = 7$.

The quaternion algebra $B = \left(\dfrac{w+1, -1}{F}\right)$,

Example 2

Let $F = \mathbb{Q}(w)$ where $w^3 - 11w - 11 = 0$. The discriminant of F is equal to $2057 = 11^2 17$ and $\mathbb{Z}_F = \mathbb{Z}[w]$. We have $\mathrm{Cl}(\mathbb{Z}_F) = \{1\}$ and $\mathrm{Cl}^+(\mathbb{Z}_F) \cong \mathbb{Z}/2\mathbb{Z}$ with the nontrivial class represented by the ideal $\mathfrak{b} = (w^2 - 2w - 6)\mathbb{Z}_F$ with $\mathrm{N}(\mathfrak{b}) = 7$.

The quaternion algebra $B = \left(\dfrac{w+1, -1}{F}\right)$, generated by i, j subject to $i^2 = w + 1$, $j^2 = -1$, and $ji = -ij$,

Example 2

Let $F = \mathbb{Q}(w)$ where $w^3 - 11w - 11 = 0$. The discriminant of F is equal to $2057 = 11^2 17$ and $\mathbb{Z}_F = \mathbb{Z}[w]$. We have $\mathrm{Cl}(\mathbb{Z}_F) = \{1\}$ and $\mathrm{Cl}^+(\mathbb{Z}_F) \cong \mathbb{Z}/2\mathbb{Z}$ with the nontrivial class represented by the ideal $\mathfrak{b} = (w^2 - 2w - 6)\mathbb{Z}_F$ with $\mathrm{N}(\mathfrak{b}) = 7$.

The quaternion algebra $B = \left(\dfrac{w+1, -1}{F}\right)$, generated by i, j subject to $i^2 = w + 1$, $j^2 = -1$, and $ji = -ij$, is ramified at only two of three real places of F.

Example 2

Let $F = \mathbb{Q}(w)$ where $w^3 - 11w - 11 = 0$. The discriminant of F is equal to $2057 = 11^2 17$ and $\mathbb{Z}_F = \mathbb{Z}[w]$. We have $\mathrm{Cl}(\mathbb{Z}_F) = \{1\}$ and $\mathrm{Cl}^+(\mathbb{Z}_F) \cong \mathbb{Z}/2\mathbb{Z}$ with the nontrivial class represented by the ideal $\mathfrak{b} = (w^2 - 2w - 6)\mathbb{Z}_F$ with $\mathrm{N}(\mathfrak{b}) = 7$.

The quaternion algebra $B = \left(\dfrac{w+1, -1}{F}\right)$, generated by i, j subject to $i^2 = w + 1$, $j^2 = -1$, and $ji = -ij$, is ramified at only two of three real places of F. A maximal order $\mathcal{O} = \mathcal{O}(1)$ is generated over $\mathbb{Z}_F$ by i and the element $k = (1 + (w^2 + 1)i + ij)/2$.

Example 2

Let $F = \mathbb{Q}(w)$ where $w^3 - 11w - 11 = 0$. The discriminant of F is equal to $2057 = 11^2 17$ and $\mathbb{Z}_F = \mathbb{Z}[w]$. We have $\mathrm{Cl}(\mathbb{Z}_F) = \{1\}$ and $\mathrm{Cl}^+(\mathbb{Z}_F) \cong \mathbb{Z}/2\mathbb{Z}$ with the nontrivial class represented by the ideal $\mathfrak{b} = (w^2 - 2w - 6)\mathbb{Z}_F$ with $\mathrm{N}(\mathfrak{b}) = 7$.

The quaternion algebra $B = \left(\dfrac{w+1, -1}{F}\right)$, generated by i, j subject to $i^2 = w + 1$, $j^2 = -1$, and $ji = -ij$, is ramified at only two of three real places of F. A maximal order $\mathcal{O} = \mathcal{O}(1)$ is generated over $\mathbb{Z}_F$ by i and the element $k = (1 + (w^2 + 1)i + ij)/2$.

The right $\mathcal{O}$-ideal $J_\mathfrak{b}$ generated by $w^2 - 2w - 6$ and the element $2 + 2i + k$ has $\mathrm{nrd}(J_\mathfrak{b}) = \mathfrak{b}$.

Example 2

Let $F = \mathbb{Q}(w)$ where $w^3 - 11w - 11 = 0$. The discriminant of F is equal to $2057 = 11^2 17$ and $\mathbb{Z}_F = \mathbb{Z}[w]$. We have $\mathrm{Cl}(\mathbb{Z}_F) = \{1\}$ and $\mathrm{Cl}^+(\mathbb{Z}_F) \cong \mathbb{Z}/2\mathbb{Z}$ with the nontrivial class represented by the ideal $\mathfrak{b} = (w^2 - 2w - 6)\mathbb{Z}_F$ with $\mathrm{N}(\mathfrak{b}) = 7$.

The quaternion algebra $B = \left(\dfrac{w+1, -1}{F}\right)$, generated by i, j subject to $i^2 = w + 1$, $j^2 = -1$, and $ji = -ij$, is ramified at only two of three real places of F. A maximal order $\mathcal{O} = \mathcal{O}(1)$ is generated over $\mathbb{Z}_F$ by i and the element $k = (1 + (w^2 + 1)i + ij)/2$.

The right $\mathcal{O}$-ideal $J_\mathfrak{b}$ generated by $w^2 - 2w - 6$ and the element $2 + 2i + k$ has $\mathrm{nrd}(J_\mathfrak{b}) = \mathfrak{b}$. Let $\mathcal{O}_\mathfrak{b}$ be the left order of $J_\mathfrak{b}$.

Example 2: Shimura curve

Example 2: Shimura curve

We take the splitting $B \hookrightarrow \mathrm{M}_2(\mathbb{R})$ by

$$i, j \mapsto \begin{pmatrix} s & 0 \\ 0 & -s \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

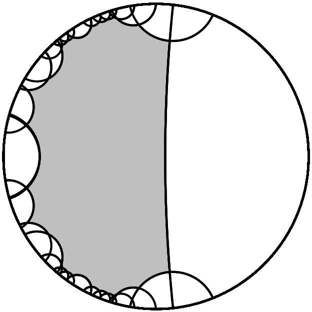
where $s = \sqrt{w+1}$ (taken with respect to the split real place).

Example 2: Shimura curve

We take the splitting $B \hookrightarrow M_2(\mathbb{R})$ by

$$i, j \mapsto \begin{pmatrix} s & 0 \\ 0 & -s \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

where $s = \sqrt{w+1}$ (taken with respect to the split real place). A fundamental domain for $\Gamma(1)$ is as follows.



Example 2: Group

Example 2: Group

$\Gamma(1)$ is generated by $\alpha, \beta, \gamma_1, \ldots, \gamma_7$

Example 2: Group

$\Gamma(1)$ is generated by $\alpha, \beta, \gamma_1, \ldots, \gamma_7$ subject to

$$\gamma_1^2 = \gamma_2^2 = \gamma_3^3 = \gamma_4^2 = \gamma_5^3 = \gamma_6^2 = \gamma_7^2 = \alpha\beta\alpha^{-1}\beta^{-1}\gamma_1\cdots\gamma_7 = 1.$$

Example 2: Group

$\Gamma(1)$ is generated by $\alpha, \beta, \gamma_1, \ldots, \gamma_7$ subject to

$$\gamma_1^2 = \gamma_2^2 = \gamma_3^3 = \gamma_4^2 = \gamma_5^3 = \gamma_6^2 = \gamma_7^2 = \alpha\beta\alpha^{-1}\beta^{-1}\gamma_1 \cdots \gamma_7 = 1.$$

Let $\Gamma_{\mathfrak{b}}(1) = \iota_\infty(\mathcal{O}_{\mathfrak{b}})/\{\pm 1\}$. Then

$$X(\mathbb{C}) = \Gamma(1)\backslash\mathcal{H} \sqcup \Gamma_{\mathfrak{b}}(1)\backslash\mathcal{H}$$

Example 2: Group

$\Gamma(1)$ is generated by $\alpha, \beta, \gamma_1, \ldots, \gamma_7$ subject to

$$\gamma_1^2 = \gamma_2^2 = \gamma_3^3 = \gamma_4^2 = \gamma_5^3 = \gamma_6^2 = \gamma_7^2 = \alpha\beta\alpha^{-1}\beta^{-1}\gamma_1 \cdots \gamma_7 = 1.$$

Let $\Gamma_{\mathfrak{b}}(1) = \iota_\infty(\mathcal{O}_{\mathfrak{b}})/\{\pm 1\}$. Then

$$X(\mathbb{C}) = \Gamma(1)\backslash\mathcal{H} \sqcup \Gamma_{\mathfrak{b}}(1)\backslash\mathcal{H} = X(1)(\mathbb{C}) \sqcup X_{\mathfrak{b}}(1)(\mathbb{C}).$$

Example 2: Group

$\Gamma(1)$ is generated by $\alpha, \beta, \gamma_1, \ldots, \gamma_7$ subject to

$$\gamma_1^2 = \gamma_2^2 = \gamma_3^3 = \gamma_4^2 = \gamma_5^3 = \gamma_6^2 = \gamma_7^2 = \alpha\beta\alpha^{-1}\beta^{-1}\gamma_1 \cdots \gamma_7 = 1.$$

Let $\Gamma_{\mathfrak{b}}(1) = \iota_\infty(\mathcal{O}_{\mathfrak{b}})/\{\pm 1\}$. Then

$$X(\mathbb{C}) = \Gamma(1)\backslash\mathcal{H} \sqcup \Gamma_{\mathfrak{b}}(1)\backslash\mathcal{H} = X(1)(\mathbb{C}) \sqcup X_{\mathfrak{b}}(1)(\mathbb{C}).$$

The groups $\Gamma = \Gamma(1)$ and $\Gamma' = \Gamma_{\mathfrak{b}} = \Gamma_{\mathfrak{b}}(1)$ have isomorphic presentations.

Example 2: Group

$\Gamma(1)$ is generated by $\alpha, \beta, \gamma_1, \ldots, \gamma_7$ subject to

$$\gamma_1^2 = \gamma_2^2 = \gamma_3^3 = \gamma_4^2 = \gamma_5^3 = \gamma_6^2 = \gamma_7^2 = \alpha\beta\alpha^{-1}\beta^{-1}\gamma_1 \cdots \gamma_7 = 1.$$

Let $\Gamma_{\mathfrak{b}}(1) = \iota_\infty(\mathcal{O}_{\mathfrak{b}})/\{\pm 1\}$. Then

$$X(\mathbb{C}) = \Gamma(1)\backslash\mathcal{H} \sqcup \Gamma_{\mathfrak{b}}(1)\backslash\mathcal{H} = X(1)(\mathbb{C}) \sqcup X_{\mathfrak{b}}(1)(\mathbb{C}).$$

The groups $\Gamma = \Gamma(1)$ and $\Gamma' = \Gamma_{\mathfrak{b}} = \Gamma_{\mathfrak{b}}(1)$ have isomorphic presentations. We have

$$H^1(\Gamma, \mathbb{C})$$

Example 2: Group

$\Gamma(1)$ is generated by $\alpha, \beta, \gamma_1, \ldots, \gamma_7$ subject to

$$\gamma_1^2 = \gamma_2^2 = \gamma_3^3 = \gamma_4^2 = \gamma_5^3 = \gamma_6^2 = \gamma_7^2 = \alpha\beta\alpha^{-1}\beta^{-1}\gamma_1 \cdots \gamma_7 = 1.$$

Let $\Gamma_{\mathfrak{b}}(1) = \iota_\infty(\mathcal{O}_{\mathfrak{b}})/\{\pm 1\}$. Then

$$X(\mathbb{C}) = \Gamma(1)\backslash\mathcal{H} \sqcup \Gamma_{\mathfrak{b}}(1)\backslash\mathcal{H} = X(1)(\mathbb{C}) \sqcup X_{\mathfrak{b}}(1)(\mathbb{C}).$$

The groups $\Gamma = \Gamma(1)$ and $\Gamma' = \Gamma_{\mathfrak{b}} = \Gamma_{\mathfrak{b}}(1)$ have isomorphic presentations. We have

$$H^1(\Gamma, \mathbb{C}) \cong \mathrm{Hom}(\Gamma, \mathbb{C})$$

Example 2: Group

$\Gamma(1)$ is generated by $\alpha, \beta, \gamma_1, \ldots, \gamma_7$ subject to

$$\gamma_1^2 = \gamma_2^2 = \gamma_3^3 = \gamma_4^2 = \gamma_5^3 = \gamma_6^2 = \gamma_7^2 = \alpha\beta\alpha^{-1}\beta^{-1}\gamma_1 \cdots \gamma_7 = 1.$$

Let $\Gamma_{\mathfrak{b}}(1) = \iota_\infty(\mathcal{O}_{\mathfrak{b}})/\{\pm 1\}$. Then

$$X(\mathbb{C}) = \Gamma(1)\backslash\mathcal{H} \sqcup \Gamma_{\mathfrak{b}}(1)\backslash\mathcal{H} = X(1)(\mathbb{C}) \sqcup X_{\mathfrak{b}}(1)(\mathbb{C}).$$

The groups $\Gamma = \Gamma(1)$ and $\Gamma' = \Gamma_{\mathfrak{b}} = \Gamma_{\mathfrak{b}}(1)$ have isomorphic presentations. We have

$$H^1(\Gamma, \mathbb{C}) \cong \mathrm{Hom}(\Gamma, \mathbb{C}) \cong \mathbb{C}f_\alpha \oplus \mathbb{C}f_\beta$$

Example 2: Group

$\Gamma(1)$ is generated by $\alpha, \beta, \gamma_1, \ldots, \gamma_7$ subject to

$$\gamma_1^2 = \gamma_2^2 = \gamma_3^3 = \gamma_4^2 = \gamma_5^3 = \gamma_6^2 = \gamma_7^2 = \alpha\beta\alpha^{-1}\beta^{-1}\gamma_1 \cdots \gamma_7 = 1.$$

Let $\Gamma_{\mathfrak{b}}(1) = \iota_\infty(\mathcal{O}_{\mathfrak{b}})/\{\pm 1\}$. Then

$$X(\mathbb{C}) = \Gamma(1)\backslash\mathcal{H} \sqcup \Gamma_{\mathfrak{b}}(1)\backslash\mathcal{H} = X(1)(\mathbb{C}) \sqcup X_{\mathfrak{b}}(1)(\mathbb{C}).$$

The groups $\Gamma = \Gamma(1)$ and $\Gamma' = \Gamma_{\mathfrak{b}} = \Gamma_{\mathfrak{b}}(1)$ have isomorphic presentations. We have

$$H^1(\Gamma, \mathbb{C}) \cong \mathrm{Hom}(\Gamma, \mathbb{C}) \cong \mathbb{C}f_\alpha \oplus \mathbb{C}f_\beta$$

where f_α, f_β are the characteristic functions for α and β,

Example 2: Group

$\Gamma(1)$ is generated by $\alpha, \beta, \gamma_1, \ldots, \gamma_7$ subject to

$$\gamma_1^2 = \gamma_2^2 = \gamma_3^3 = \gamma_4^2 = \gamma_5^3 = \gamma_6^2 = \gamma_7^2 = \alpha\beta\alpha^{-1}\beta^{-1}\gamma_1 \cdots \gamma_7 = 1.$$

Let $\Gamma_{\mathfrak{b}}(1) = \iota_\infty(\mathcal{O}_{\mathfrak{b}})/\{\pm 1\}$. Then

$$X(\mathbb{C}) = \Gamma(1)\backslash\mathcal{H} \sqcup \Gamma_{\mathfrak{b}}(1)\backslash\mathcal{H} = X(1)(\mathbb{C}) \sqcup X_{\mathfrak{b}}(1)(\mathbb{C}).$$

The groups $\Gamma = \Gamma(1)$ and $\Gamma' = \Gamma_{\mathfrak{b}} = \Gamma_{\mathfrak{b}}(1)$ have isomorphic presentations. We have

$$H^1(\Gamma, \mathbb{C}) \cong \mathrm{Hom}(\Gamma, \mathbb{C}) \cong \mathbb{C}f_\alpha \oplus \mathbb{C}f_\beta$$

where f_α, f_β are the characteristic functions for α and β, and a similar description for $H^1(\Gamma_{\mathfrak{b}}, \mathbb{C})$.

Example 2: Group

$\Gamma(1)$ is generated by $\alpha, \beta, \gamma_1, \dots, \gamma_7$ subject to

$$\gamma_1^2 = \gamma_2^2 = \gamma_3^3 = \gamma_4^2 = \gamma_5^3 = \gamma_6^2 = \gamma_7^2 = \alpha\beta\alpha^{-1}\beta^{-1}\gamma_1 \cdots \gamma_7 = 1.$$

Let $\Gamma_{\mathfrak{b}}(1) = \iota_\infty(\mathcal{O}_{\mathfrak{b}})/\{\pm 1\}$. Then

$$X(\mathbb{C}) = \Gamma(1)\backslash\mathcal{H} \sqcup \Gamma_{\mathfrak{b}}(1)\backslash\mathcal{H} = X(1)(\mathbb{C}) \sqcup X_{\mathfrak{b}}(1)(\mathbb{C}).$$

The groups $\Gamma = \Gamma(1)$ and $\Gamma' = \Gamma_{\mathfrak{b}} = \Gamma_{\mathfrak{b}}(1)$ have isomorphic presentations. We have

$$H^1(\Gamma, \mathbb{C}) \cong \mathrm{Hom}(\Gamma, \mathbb{C}) \cong \mathbb{C}f_\alpha \oplus \mathbb{C}f_\beta$$

where f_α, f_β are the characteristic functions for α and β, and a similar description for $H^1(\Gamma_{\mathfrak{b}}, \mathbb{C})$. Thus

$$S_2(1) \cong \left(H^1(\Gamma, \mathbb{C}) \oplus H^1(\Gamma_{\mathfrak{b}}, \mathbb{C})\right)^+$$

Example 2: Group

$\Gamma(1)$ is generated by $\alpha, \beta, \gamma_1, \ldots, \gamma_7$ subject to

$$\gamma_1^2 = \gamma_2^2 = \gamma_3^3 = \gamma_4^2 = \gamma_5^3 = \gamma_6^2 = \gamma_7^2 = \alpha\beta\alpha^{-1}\beta^{-1}\gamma_1 \cdots \gamma_7 = 1.$$

Let $\Gamma_{\mathfrak{b}}(1) = \iota_\infty(\mathcal{O}_{\mathfrak{b}})/\{\pm 1\}$. Then

$$X(\mathbb{C}) = \Gamma(1)\backslash\mathcal{H} \sqcup \Gamma_{\mathfrak{b}}(1)\backslash\mathcal{H} = X(1)(\mathbb{C}) \sqcup X_{\mathfrak{b}}(1)(\mathbb{C}).$$

The groups $\Gamma = \Gamma(1)$ and $\Gamma' = \Gamma_{\mathfrak{b}} = \Gamma_{\mathfrak{b}}(1)$ have isomorphic presentations. We have

$$H^1(\Gamma, \mathbb{C}) \cong \mathrm{Hom}(\Gamma, \mathbb{C}) \cong \mathbb{C}f_\alpha \oplus \mathbb{C}f_\beta$$

where f_α, f_β are the characteristic functions for α and β, and a similar description for $H^1(\Gamma_{\mathfrak{b}}, \mathbb{C})$. Thus

$$S_2(1) \cong \left(H^1(\Gamma, \mathbb{C}) \oplus H^1(\Gamma_{\mathfrak{b}}, \mathbb{C})\right)^+$$

and $\dim S_2(1) = 1 + 1 = 2$.

Example 2: Hecke operators

Example 2: Hecke operators

A Hecke operator $T_{\mathfrak{p}}$ can be understood via correspondences, a double coset description, or as an "averaging operator":

Example 2: Hecke operators

A Hecke operator $T_\mathfrak{p}$ can be understood via correspondences, a double coset description, or as an "averaging operator": it takes the form

$$(f \mid T_\mathfrak{p})(\gamma) = \sum_{a \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})} f(\delta'_a)$$

for $f \in \mathrm{Hom}(\Gamma', \mathbb{C})$ and $\gamma \in \Gamma$.

Example 2: Hecke operators

A Hecke operator $T_{\mathfrak{p}}$ can be understood via correspondences, a double coset description, or as an "averaging operator": it takes the form

$$(f \mid T_{\mathfrak{p}})(\gamma) = \sum_{a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} f(\delta'_a)$$

for $f \in \mathrm{Hom}(\Gamma', \mathbb{C})$ and $\gamma \in \Gamma$.

Consider the prime $\mathfrak{p}_3 = (w+2)\mathbb{Z}_F$ of norm 3, which is nontrivial in $\mathrm{Cl}^+(\mathbb{Z}_F)$.

Example 2: Hecke operators

A Hecke operator $T_{\mathfrak{p}}$ can be understood via correspondences, a double coset description, or as an "averaging operator": it takes the form

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

for $f \in \mathrm{Hom}(\Gamma', \mathbb{C})$ and $\gamma \in \Gamma$.

Consider the prime $\mathfrak{p}_3 = (w+2)\mathbb{Z}_F$ of norm 3, which is nontrivial in $\mathrm{Cl}^+(\mathbb{Z}_F)$.

The sum is over the left ideals of $\mathcal{O}$ of norm $\mathfrak{p}_3$, which are in bijection with $\mathbb{P}^1(\mathbb{F}_3)$.

Example 2: Hecke operators

A Hecke operator $T_{\mathfrak{p}}$ can be understood via correspondences, a double coset description, or as an "averaging operator": it takes the form

$$(f \mid T_{\mathfrak{p}})(\gamma) = \sum_{a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} f(\delta'_a)$$

for $f \in \mathrm{Hom}(\Gamma', \mathbb{C})$ and $\gamma \in \Gamma$.

Consider the prime $\mathfrak{p}_3 = (w+2)\mathbb{Z}_F$ of norm 3, which is nontrivial in $\mathrm{Cl}^+(\mathbb{Z}_F)$.

The sum is over the left ideals of $\mathcal{O}$ of norm $\mathfrak{p}_3$, which are in bijection with $\mathbb{P}^1(\mathbb{F}_3)$. For $I_{[1:0]} \subset \mathcal{O}$, we principalize

$$J_{\mathfrak{b}} I_{[1:0]}$$

Example 2: Hecke operators

A Hecke operator $T_{\mathfrak{p}}$ can be understood via correspondences, a double coset description, or as an "averaging operator": it takes the form

$$(f \mid T_{\mathfrak{p}})(\gamma) = \sum_{a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} f(\delta'_a)$$

for $f \in \mathrm{Hom}(\Gamma', \mathbb{C})$ and $\gamma \in \Gamma$.

Consider the prime $\mathfrak{p}_3 = (w+2)\mathbb{Z}_F$ of norm 3, which is nontrivial in $\mathrm{Cl}^+(\mathbb{Z}_F)$.

The sum is over the left ideals of $\mathcal{O}$ of norm $\mathfrak{p}_3$, which are in bijection with $\mathbb{P}^1(\mathbb{F}_3)$. For $I_{[1:0]} \subset \mathcal{O}$, we principalize

$$J_{\mathfrak{b}} I_{[1:0]} = \mathcal{O}'((w+1) + i + ij) = \mathcal{O}' \pi'_{[1:0]}.$$

Example 2: Hecke operators

A Hecke operator $T_{\mathfrak{p}}$ can be understood via correspondences, a double coset description, or as an "averaging operator": it takes the form

$$(f \mid T_{\mathfrak{p}})(\gamma) = \sum_{a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} f(\delta'_a)$$

for $f \in \operatorname{Hom}(\Gamma', \mathbb{C})$ and $\gamma \in \Gamma$.

Consider the prime $\mathfrak{p}_3 = (w+2)\mathbb{Z}_F$ of norm 3, which is nontrivial in $\operatorname{Cl}^+(\mathbb{Z}_F)$.

The sum is over the left ideals of $\mathcal{O}$ of norm $\mathfrak{p}_3$, which are in bijection with $\mathbb{P}^1(\mathbb{F}_3)$. For $I_{[1:0]} \subset \mathcal{O}$, we principalize

$$J_{\mathfrak{b}} I_{[1:0]} = \mathcal{O}'((w+1) + i + ij) = \mathcal{O}'\pi'_{[1:0]}.$$

For the generator α, we find $\pi'_{[1:0]}\alpha = \delta'_{[1:0]}\pi'_{[1:0]}$

Example 2: Hecke operators

A Hecke operator $T_{\mathfrak{p}}$ can be understood via correspondences, a double coset description, or as an "averaging operator": it takes the form

$$(f \mid T_{\mathfrak{p}})(\gamma) = \sum_{a \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} f(\delta'_a)$$

for $f \in \mathrm{Hom}(\Gamma', \mathbb{C})$ and $\gamma \in \Gamma$.

Consider the prime $\mathfrak{p}_3 = (w+2)\mathbb{Z}_F$ of norm 3, which is nontrivial in $\mathrm{Cl}^+(\mathbb{Z}_F)$.

The sum is over the left ideals of $\mathcal{O}$ of norm $\mathfrak{p}_3$, which are in bijection with $\mathbb{P}^1(\mathbb{F}_3)$. For $I_{[1:0]} \subset \mathcal{O}$, we principalize

$$J_{\mathfrak{b}} I_{[1:0]} = \mathcal{O}'((w+1) + i + ij) = \mathcal{O}' \pi'_{[1:0]}.$$

For the generator α, we find $\pi'_{[1:0]}\alpha = \delta'_{[1:0]}\pi'_{[1:0]}$ where

$$14\delta'_{[1:0]} = (7w^2 - 98) + \cdots + (-2w^2 + 5w + 20)ij \in \mathcal{O}'$$

Example 2: Hecke operators

A Hecke operator $T_{\mathfrak{p}}$ can be understood via correspondences, a double coset description, or as an "averaging operator": it takes the form

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

for $f \in \operatorname{Hom}(\Gamma', \mathbb{C})$ and $\gamma \in \Gamma$.

Consider the prime $\mathfrak{p}_3 = (w+2)\mathbb{Z}_F$ of norm 3, which is nontrivial in $\operatorname{Cl}^+(\mathbb{Z}_F)$.

The sum is over the left ideals of $\mathcal{O}$ of norm $\mathfrak{p}_3$, which are in bijection with $\mathbb{P}^1(\mathbb{F}_3)$. For $I_{[1:0]} \subset \mathcal{O}$, we principalize

$$J_{\mathfrak{b}} I_{[1:0]} = \mathcal{O}'((w+1)+i+ij) = \mathcal{O}'\pi'_{[1:0]}.$$

For the generator α, we find $\pi'_{[1:0]}\alpha = \delta'_{[1:0]}\pi'_{[1:0]}$ where

$$14\delta'_{[1:0]} = (7w^2 - 98) + \cdots + (-2w^2 + 5w + 20)ij \in \mathcal{O}'$$

We write $\delta'_{[1:0]}$ as a word in the generators for Γ', repeat, and sum.

Example 2: Hecke operators

Example 2: Hecke operators

We obtain

$$T_{\mathfrak{p}_3} \mid H = \begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix}.$$

In a similar way, we find that $T_{\mathfrak{p}_5}$ is the identity matrix

Example 2: Hecke operators

We obtain

$$T_{\mathfrak{p}_3} \mid H = \begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix}.$$

In a similar way, we find that $T_{\mathfrak{p}_5}$ is the identity matrix and that complex conjugation acts by

$$W_\infty \mid H = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

Example 2: Hecke operators

We obtain

$$T_{\mathfrak{p}_3} \mid H = \begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix}.$$

In a similar way, we find that $T_{\mathfrak{p}_5}$ is the identity matrix and that complex conjugation acts by

$$W_\infty \mid H = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

We conclude that $T_{\mathfrak{p}_3} \mid H^+ = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$ and $T_{\mathfrak{p}_5} \mid H^+ = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

Example 2: Hecke operators

We obtain

$$T_{\mathfrak{p}_3} \mid H = \begin{pmatrix} 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 2 \\ 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \end{pmatrix}.$$

In a similar way, we find that $T_{\mathfrak{p}_5}$ is the identity matrix and that complex conjugation acts by

$$W_\infty \mid H = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & -1 \end{pmatrix}.$$

We conclude that $T_{\mathfrak{p}_3} \mid H^+ = \begin{pmatrix} 0 & 2 \\ 2 & 0 \end{pmatrix}$ and $T_{\mathfrak{p}_5} \mid H^+ = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

H^+ breaks up, yielding two one-dimensional eigenforms f and g.

Example 2: Hecke eigenvalues

Example 2: Hecke eigenvalues

We have the following Hecke eigenvalues for the forms f and g.

Example 2: Hecke eigenvalues

We have the following Hecke eigenvalues for the forms f and g.

$\mathfrak{p}$	$\mathrm{N}\mathfrak{p}$	$a_{\mathfrak{p}}(f)$	$a_{\mathfrak{p}}(g)$
$w+2$	3	2	-2
$w+3$	5	1	1
2	8	-5	-5
$2w+7$	9	-2	2
w	11	0	0
w^2-w-8	17	-5	5
$w-3$	17	-5	-5
$2w^2-5w-10$	23	2	-2
w^2-3w-2	25	-9	-9

Example 2: Hecke eigenvalues

We have the following Hecke eigenvalues for the forms f and g.

$\mathfrak{p}$	$N\mathfrak{p}$	$a_{\mathfrak{p}}(f)$	$a_{\mathfrak{p}}(g)$
$w+2$	3	2	-2
$w+3$	5	1	1
2	8	-5	-5
$2w+7$	9	-2	2
w	11	0	0
w^2-w-8	17	-5	5
$w-3$	17	-5	-5
$2w^2-5w-10$	23	2	-2
w^2-3w-2	25	-9	-9

The form g is visibly a quadratic twist of f.

Example 2: Identifying the curves

Example 2: Identifying the curves

By work of Deligne, the curves $X = X(1)$ and $X_{\mathfrak{b}}$ are defined over the strict class field F^+ of F and that $\mathrm{Gal}(F^+/F)$ permutes them.

Example 2: Identifying the curves

By work of Deligne, the curves $X = X(1)$ and $X_{\mathfrak{b}}$ are defined over the strict class field F^+ of F and that $\mathrm{Gal}(F^+/F)$ permutes them. We compute that $F^+ = F(\sqrt{-3w^2 + 8w + 12})$.

Example 2: Identifying the curves

By work of Deligne, the curves $X = X(1)$ and $X_{\mathfrak{b}}$ are defined over the strict class field F^+ of F and that $\mathrm{Gal}(F^+/F)$ permutes them. We compute that $F^+ = F(\sqrt{-3w^2 + 8w + 12})$. Therefore the Jacobian J_f, corresponding to the cusp form f,

Example 2: Identifying the curves

By work of Deligne, the curves $X = X(1)$ and $X_{\mathfrak{b}}$ are defined over the strict class field F^+ of F and that $\mathrm{Gal}(F^+/F)$ permutes them. We compute that $F^+ = F(\sqrt{-3w^2 + 8w + 12})$. Therefore the Jacobian J_f, corresponding to the cusp form f, is a modular elliptic curve over F^+ with everywhere good reduction,

Example 2: Identifying the curves

By work of Deligne, the curves $X = X(1)$ and $X_{\mathfrak{b}}$ are defined over the strict class field F^+ of F and that $\mathrm{Gal}(F^+/F)$ permutes them. We compute that $F^+ = F(\sqrt{-3w^2 + 8w + 12})$. Therefore the Jacobian J_f, corresponding to the cusp form f, is a modular elliptic curve over F^+ with everywhere good reduction, and the form g is the twist of f by the character χ corresponding to the extension F^+/F.

Example 2: Identifying the curves

By work of Deligne, the curves $X = X(1)$ and $X_{\mathfrak{b}}$ are defined over the strict class field F^+ of F and that $\mathrm{Gal}(F^+/F)$ permutes them. We compute that $F^+ = F(\sqrt{-3w^2 + 8w + 12})$. Therefore the Jacobian J_f, corresponding to the cusp form f, is a modular elliptic curve over F^+ with everywhere good reduction, and the form g is the twist of f by the character χ corresponding to the extension F^+/F.

However,

Example 2: Identifying the curves

By work of Deligne, the curves $X = X(1)$ and $X_{\mathfrak{b}}$ are defined over the strict class field F^+ of F and that $\mathrm{Gal}(F^+/F)$ permutes them. We compute that $F^+ = F(\sqrt{-3w^2 + 8w + 12})$. Therefore the Jacobian J_f, corresponding to the cusp form f, is a modular elliptic curve over F^+ with everywhere good reduction, and the form g is the twist of f by the character χ corresponding to the extension F^+/F.

However, the Jacobian of $X = X(1) \sqcup X_{\mathfrak{b}}(1)$ is an abelian variety of dimension 2 defined over F

Example 2: Identifying the curves

By work of Deligne, the curves $X = X(1)$ and $X_{\mathfrak{b}}$ are defined over the strict class field F^+ of F and that $\mathrm{Gal}(F^+/F)$ permutes them. We compute that $F^+ = F(\sqrt{-3w^2 + 8w + 12})$. Therefore the Jacobian J_f, corresponding to the cusp form f, is a modular elliptic curve over F^+ with everywhere good reduction, and the form g is the twist of f by the character χ corresponding to the extension F^+/F.

However, the Jacobian of $X = X(1) \sqcup X_{\mathfrak{b}}(1)$ is an abelian variety of dimension 2 defined over F which is isogenous to a product $J \times J_\chi$ of an elliptic curve J over F

Example 2: Identifying the curves

By work of Deligne, the curves $X = X(1)$ and $X_{\mathfrak{b}}$ are defined over the strict class field F^+ of F and that $\mathrm{Gal}(F^+/F)$ permutes them. We compute that $F^+ = F(\sqrt{-3w^2 + 8w + 12})$. Therefore the Jacobian J_f, corresponding to the cusp form f, is a modular elliptic curve over F^+ with everywhere good reduction, and the form g is the twist of f by the character χ corresponding to the extension F^+/F.

However, the Jacobian of $X = X(1) \sqcup X_{\mathfrak{b}}(1)$ is an abelian variety of dimension 2 defined over F which is isogenous to a product $J \times J_\chi$ of an elliptic curve J over F with $\#J(\mathbb{F}_{\mathfrak{p}}) = N\mathfrak{p} + 1 - a_f(\mathfrak{p})$

Example 2: Identifying the curves

By work of Deligne, the curves $X = X(1)$ and $X_{\mathfrak{b}}$ are defined over the strict class field F^+ of F and that $\mathrm{Gal}(F^+/F)$ permutes them. We compute that $F^+ = F(\sqrt{-3w^2 + 8w + 12})$. Therefore the Jacobian J_f, corresponding to the cusp form f, is a modular elliptic curve over F^+ with everywhere good reduction, and the form g is the twist of f by the character χ corresponding to the extension F^+/F.

However, the Jacobian of $X = X(1) \sqcup X_{\mathfrak{b}}(1)$ is an abelian variety of dimension 2 defined over F which is isogenous to a product $J \times J_\chi$ of an elliptic curve J over F with $\#J(\mathbb{F}_{\mathfrak{p}}) = N\mathfrak{p} + 1 - a_f(\mathfrak{p})$ and everywhere good reduction,

Example 2: Identifying the curves

By work of Deligne, the curves $X = X(1)$ and $X_{\mathfrak{b}}$ are defined over the strict class field F^+ of F and that $\mathrm{Gal}(F^+/F)$ permutes them. We compute that $F^+ = F(\sqrt{-3w^2 + 8w + 12})$. Therefore the Jacobian J_f, corresponding to the cusp form f, is a modular elliptic curve over F^+ with everywhere good reduction, and the form g is the twist of f by the character χ corresponding to the extension F^+/F.

However, the Jacobian of $X = X(1) \sqcup X_{\mathfrak{b}}(1)$ is an abelian variety of dimension 2 defined over F which is isogenous to a product $J \times J_\chi$ of an elliptic curve J over F with $\#J(\mathbb{F}_{\mathfrak{p}}) = N\mathfrak{p} + 1 - a_f(\mathfrak{p})$ and everywhere good reduction, and its quadratic twist J_χ by χ.

Example 2: Identifying the curves

By work of Deligne, the curves $X = X(1)$ and $X_{\mathfrak{b}}$ are defined over the strict class field F^+ of F and that $\mathrm{Gal}(F^+/F)$ permutes them. We compute that $F^+ = F(\sqrt{-3w^2+8w+12})$. Therefore the Jacobian J_f, corresponding to the cusp form f, is a modular elliptic curve over F^+ with everywhere good reduction, and the form g is the twist of f by the character χ corresponding to the extension F^+/F.

However, the Jacobian of $X = X(1) \sqcup X_{\mathfrak{b}}(1)$ is an abelian variety of dimension 2 defined over F which is isogenous to a product $J \times J_\chi$ of an elliptic curve J over F with $\#J(\mathbb{F}_{\mathfrak{p}}) = N\mathfrak{p} + 1 - a_f(\mathfrak{p})$ and everywhere good reduction, and its quadratic twist J_χ by χ.

In fact, Watkins found that J is the base change to F of

$$121\mathrm{c} : y^2 + xy = x^3 + x^2 - 2x - 7$$

Example 2: Identifying the curves

By work of Deligne, the curves $X = X(1)$ and $X_{\mathfrak{b}}$ are defined over the strict class field F^+ of F and that $\mathrm{Gal}(F^+/F)$ permutes them. We compute that $F^+ = F(\sqrt{-3w^2 + 8w + 12})$. Therefore the Jacobian J_f, corresponding to the cusp form f, is a modular elliptic curve over F^+ with everywhere good reduction, and the form g is the twist of f by the character χ corresponding to the extension F^+/F.

However, the Jacobian of $X = X(1) \sqcup X_{\mathfrak{b}}(1)$ is an abelian variety of dimension 2 defined over F which is isogenous to a product $J \times J_\chi$ of an elliptic curve J over F with $\#J(\mathbb{F}_{\mathfrak{p}}) = N\mathfrak{p} + 1 - a_f(\mathfrak{p})$ and everywhere good reduction, and its quadratic twist J_χ by χ.

In fact, Watkins found that J is the base change to F of

$$121\text{c} : y^2 + xy = x^3 + x^2 - 2x - 7$$

and in particular, J miraculously has an 11-isogeny.

Thanks!