COMPUTING HILBERT MODULAR FORMS OVER REAL QUADRATIC FIELDS

LASSINA DEMBÉLÉ

Introduction

These notes are a short survey of the algorithm the author developed in [4, 5] in order to compute with Hilbert modular forms over real quadratic fields. Unlike classical modular forms, computational results on Hilbert modular forms are still very limited. Our goal is to create a database of Hilbert modular forms over real quadratic fields in order to compensate for that lack of numerical results. And, in writing these notes for the MSRI graduate summer school, we hope to motivate students to join this long term project.

Our approach to the computation of Hilbert modular forms is via the Eichler-Shimizu or Jacquet-Langlands correspondence. So after giving the definitions and the basic properties of Hilbert modular forms in Section 1 and Section 3 and discussing some applications of them in Section 2, we state this correspondence for weight 2 forms in Section 4. We then present our algorithm and make few comments on how to implement it. In the last section, we explain how one can compute the elliptic curve corresponding to a Hilbert normalized eigenform that has rational Fourier expansion. The computations in that section are based on [6] and uses results from Oda [10]. Namely, we use the 2-cycles constructed by Oda in order to compute the periods of a given cusp form. I our application, however, we use the stronger assumption made in Conjecture 3.

1. Hilbert modular forms and varieties

We fix a totally real number field F of degree g and let J_F be the set of all real embeddings of F. For each $\tau \in J_F$, we denote the corresponding embedding into $\mathbb{R}$ by $a \mapsto a^\tau$. Also, we let $\mathcal{O}_F$ be the ring of integers of F, and $\mathfrak{d}$ its different. For an integral $\mathfrak{p}$ of F, we denote by $F_\mathfrak{p}$ and $\mathcal{O}_{F,\,\mathfrak{p}}$ the completions of F and $\mathcal{O}_F$, respectively, at $\mathfrak{p}$. We let $\mathbb{A}$ be the ring of adèles of F and denote it finite part by $\mathbb{A}_f$. We say that an element $a \in F$ is totally positive if, for all $\tau \in J_F$, $a^\tau > 0$. We denote this by $a \gg 0$. We fix an integral ideal $\mathfrak{n}$ of F.

1.1. **Congruence subrgroups of $\mathrm{GL}_2^+(F)$.** The set J_F induces an embedding $\mathrm{GL}_2(F) \hookrightarrow \prod_{\tau\in J_F} \mathrm{GL}_2(\mathbb{R})$ by $\gamma \mapsto (\gamma^\tau)_{\tau\in J_F}$. For any subring A of F, we let

$$\mathrm{GL}_2^+(A) = \left\{\gamma \in \mathrm{GL}_2(A) : (\gamma^\tau)_{\tau\in J_F} \in \prod_{\tau\in J_F} \mathrm{GL}_2^+(\mathbb{R})\right\}.$$

We have the restriction $\mathrm{GL}_2^+(F) \to \mathrm{PGL}_2^+(F)$, $\gamma \mapsto \tilde{\gamma}$, of the projection map onto $\mathrm{PGL}_2(F)$. We let $\Gamma(1) = \mathrm{GL}_2^+(\mathcal{O}_F)$.

Definition 1. *A* congruence subgroup *of* $\mathrm{GL}_2^+(F)$ *is a subgroup* Γ *such that* $\widetilde{g\Gamma g^{-1} \cap \Gamma(1)}$ *has finite index in both* $\widetilde{g\Gamma g^{-1}}$ *and* $\widetilde{\Gamma(1)}$ *for some* $g \in \mathrm{GL}_2^+(F)$.

As we will see later, the motivation for such a definition relies in the fact that the arithmetic of Hilbert modular forms on the field F needs to take its narrow class group into account.

Example 1. Let $\mathfrak{c}$ be a fractional ideal of F, and put

$$\Gamma_0(\mathfrak{c}, \mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \begin{pmatrix} \mathcal{O}_F & \mathfrak{c}^{-1} \\ \mathfrak{c}\mathfrak{n} & \mathcal{O}_F \end{pmatrix} : ad - bc \in \mathcal{O}_F^{\times +},\, d \equiv 1(\mod \mathfrak{n}) \right\}.$$

Then, $\Gamma_0(\mathfrak{c}, \mathfrak{n})$ is a congruence subgroup of $\mathrm{GL}_2^+(F)$. This is the only type of congruence subgroups that will be interested in for the rest of this lecture.

1.2. **Classical Hilbert modular forms.** Let $\mathfrak{H}$ be the Poincaré upper-half plane and put $\mathfrak{H}_F = \mathfrak{H}^{J_F}$. Then $\prod_{\tau \in J_F} \mathrm{GL}_2^+(\mathbb{R})$ acts on $\mathfrak{H}_F$ as follows. For any $\gamma = (\gamma_\tau)_{\tau \in J_F} \in \prod_{\tau \in J_F} \mathrm{GL}_2^+(\mathbb{R})$ and $z = (z_\tau)_{\tau \in J_F} \in \mathfrak{H}_F$,

$$\gamma_\tau \cdot z_\tau = \frac{a_\tau z_\tau + b_\tau}{c_\tau z_\tau + d_\tau}, \text{ where } \gamma_\tau = \begin{pmatrix} a_\tau & b_\tau \\ c_\tau & d_\tau \end{pmatrix}.$$

Definition 2. *An element* $\underline{k} = (k_\tau)_\tau \in \mathbb{Z}^{J_F}$ *is called a* weight vector. *We always assume that the components* $k_\tau \geq 2$ *have the same parity.*

From now on, we fix a weight $\underline{k}$. For each function $f : \mathfrak{H}_F \to \mathbb{C}$, put

$$f\|_{\underline{k}}\gamma = \left(\prod_{\tau \in J_F} \det(\gamma_\tau)^{k_\tau/2} (c_\tau z_\tau + d_\tau)^{-k_\tau} \right) f(\gamma z),\ \gamma \in \Gamma_0(\mathfrak{c}, \mathfrak{n}).$$

This defines an action of $\Gamma_0(\mathfrak{c}, \mathfrak{n})$ on the space of such functions.

Definition 3. *A* classical Hilbert modular form *of level* $\Gamma_0(\mathfrak{c}, \mathfrak{n})$ *and weight* $\underline{k}$ *is a holomorphic function* $f : \mathfrak{H}_F \to \mathbb{C}$ *such that* $f\|_{\underline{k}}\gamma = f$, *for all* $\gamma \in \Gamma_0(\mathfrak{c}, \mathfrak{n})$. *The space of all classical Hilbert modular forms of level* $\Gamma_0(\mathfrak{c}, \mathfrak{n})$ *and weight* $\underline{k}$ *is denoted by* $M_{\underline{k}}(\mathfrak{c}, \mathfrak{n})$.

Let $f : \mathfrak{H}_F \to \mathbb{C}$ be a Hilbert modular form. Since it is $\Gamma_0(\mathfrak{c}, \mathfrak{n})$-invariant, we have in particular

$$f(z + \mu) = f(z), \quad \text{for all } z \in \mathfrak{H}_F,\ \mu \in \mathfrak{c}^{-1}.$$

Therefore, it admits a Fourier expansion of the form

$$f(z) = \sum_{\mu \in \mathfrak{d}^{-1}} a_\mu e^{2\pi i \mathrm{Tr}(\mu z)},$$

where $\mathrm{Tr}(\mu z) = \sum_{\tau \in J_F} \mu^\tau z_\tau$. When $g > 1$, every Hilbert modular form is automatically holomorphic at cusps as the next lemma shows.

Lemma 1 (Koecher's principle)**.** *Assume that* $g > 1$. *Then,* f *is* holomorphic *at the cusp* ∞ *(hence at all cusps) in the following sense:*

$$a_\mu \neq 0 \Rightarrow \mu = 0 \text{ or } \mu \gg 0.$$

Proof. The stabilizer of the cusp at ∞ is the semi-direct product $\mathcal{O}_F^{\times +}$ and $\mathfrak{c}^{-1}$. And so, $\gamma(\varepsilon) = \begin{pmatrix} \varepsilon & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(\mathfrak{c},\, \mathfrak{n})$, which means that $f\|_{\underline{k}}\gamma(\varepsilon) = f$. Equating the q–expansion of both members of this equality, it follows that

$$a_{\varepsilon\mu} = \mathrm{N}(\varepsilon)^{\underline{k}/2} a_\mu, \quad \text{for all } \mu \in \mathfrak{c}\mathfrak{d}^{-1},$$

where we use the notation $\mathrm{N}(\varepsilon)^{\underline{k}} = \prod_{\tau \in J_F} (\varepsilon^\tau)^{k_\tau}$. Now, let us assume that there is a non–zero $\mu_0 \in \mathfrak{c}\mathfrak{d}^{-1}$ not totally positive such that $a_{\mu_0} \neq 0$. We choose τ_0 such that $\mu_0^{\tau_0} < 0$. By the Dirichlet units theorem, we can find $\varepsilon \in \mathcal{O}_F^{\times +}$ such that

$$\varepsilon^{\tau_0} > 1 \quad \text{and} \quad \varepsilon^\tau < 1, \text{ for all}\, \tau \neq \tau_0.$$

We now consider the subseries of $f(z) = \sum_{\mu \in \mathfrak{c}\mathfrak{d}^{-1}} a_\mu e^{2\pi i \mathrm{Tr}(\mu z)}$ index by the set $\{\mu_0 \varepsilon^m,\ m \in \mathbb{N}\}$, in which we put $z = \underline{i}$. Then

$$a_{\mu_0 \varepsilon^m} e^{-2\pi \mathrm{Tr}(\mu_0 \varepsilon^m)} = \mathrm{N}(\varepsilon)^{m\underline{k}/2} a_{\mu_0} e^{-2\pi \mathrm{Tr}(\mu_0 \varepsilon^m)}.$$

But, as $m \to \infty$, $e^{-2\pi \mathrm{Tr}(\mu_0 \varepsilon^m)} \sim e^{-2\pi \mu_0^{\tau_0} (\varepsilon^{\tau_0})^m}$, and the exponential growth ensures that $\mathrm{N}(\varepsilon)^{m\underline{k}/2} a_{\mu_0} e^{-2\pi \mathrm{Tr}(\mu_0 \varepsilon^m)} \to \infty$. Therefore the series does not converge, which is a contradiction. So we must have $a_{\mu_0} = 0$. □

Definition 4. *We say that f is a* cusp *form if the constant term a_0 in the Fourier expansion is equal to 0 for any $f\|_{\underline{k}}\gamma$, $\gamma \in \mathrm{GL}_2^+(F)$ (i.e., if f vanishes at all cusps). We will denote by $S_{\underline{k}}(\mathfrak{c},\, \mathfrak{n})$) the space of cusp forms of weight $\underline{k}$ and level $\Gamma_0(\mathfrak{c},\, \mathfrak{n})$.*

Corollary 1. $S_{\underline{k}}(\mathfrak{c},\, \mathfrak{n}) = M_{\underline{k}}(\mathfrak{c},\, \mathfrak{n})$ *unless $k_\tau = k_{\tau'}$ for all $\tau,\, \tau' \in J_F$.*

Proof. Let assume that there is $f \in M_{\underline{k}}(\mathfrak{c},\, \mathfrak{n})$ that is not a cusp form. Then at some cusp σ, the q–expansion must give $a_0 \neq 0$. From

$$a_0 = \mathrm{N}(\varepsilon)^{\underline{k}/2} a_0, \quad \text{for all } \varepsilon \in \mathcal{O}_F^{\times +},$$

it follows that we must have $\mathrm{N}(\varepsilon)^{\underline{k}/2} = 1$ for all $\varepsilon \in \mathcal{O}_F^{\times +}$. But this is possible only if we have $k_\tau = k_{\tau'}$ for all $\tau,\, \tau \in J_F$. □

Proposition 2. (i) $M_{\underline{k}}(\mathfrak{c},\, \mathfrak{n}) = 0$ *unless $k_\tau \geq 0$ for all $\tau \in J_F$.*
(ii) $M_0(\mathfrak{c},\, \mathfrak{n}) = \mathbb{C}$ *and* $S_0(\mathfrak{c},\, \mathfrak{n}) = 0$.

Proof. van der Geer [7, Chap. I. sec. 6.] □

Example 2. *Eisenstein series.* Let $\mathcal{C}$ be an ideal class and choose a representative $\mathfrak{c} \in \mathcal{C}$. Let $k \geq 2$ be even. Put

$$G_{k,\, \mathcal{C}}(z) = \mathbf{N}(\mathfrak{c})^k \sum_{(c,d) \in \mathbf{P}^1(\mathfrak{a}\mathfrak{c} \times \mathfrak{c})} \mathbf{N}(cz + d)^{-k},$$

where $\mathbf{P}^1(\mathfrak{a}\mathfrak{c} \times \mathfrak{c}) = \{(c,\, d) \in \mathfrak{a}\mathfrak{c} \times \mathfrak{c} | (c,\, d) \neq (0,\, 0)\}/\mathcal{O}_F^\times$. This series does not depend on $\mathfrak{c} \in \mathcal{C}$, and it can be shown to be modular form of weight $\underline{k} = (k, \cdots, k)$ with respect to $\Gamma_0(\mathfrak{c},\, \mathcal{O}_F)$. As in the one–dimensional case, one can find the expansion at ∞ by making use of Poisson summation (see van der Geer [7, Chap. 1, sec. 6]). We call $G_{k,\, \mathcal{C}}$ the *Eisenstein series* of weight k and class $\mathcal{B}$ with repect to $\Gamma_0(\mathfrak{c},\, \mathcal{O}_F)$.

1.3. **Adelic Hilbert modular forms.** We recall that $\prod_{\tau\in J_F}\mathrm{GL}_2^+(\mathbb{R})$ acts transitively on $\mathfrak{H}_F$ by linear fractional transforms and that the stabilizer of $\underline{i}=(i,\,\ldots,\,i)$ is given by $K_\infty^+=(\mathbb{R}^\times\mathrm{SO}_2(\mathbb{R}))^{J_F}$. We consider the unique action of $\prod_{\tau\in J_F}\mathrm{GL}_2(\mathbb{R})$ on $\mathfrak{H}_F$ that extends the action of $\prod_{\tau\in J_F}\mathrm{GL}_2^+(\mathbb{R})$. Namely, on each copy of $\mathfrak{H}$, we let the element $\left(\begin{smallmatrix}-1 & 0\\ 0 & 1\end{smallmatrix}\right)$ acts by $z\mapsto -\bar{z}$. We consider the following compact open subgroup of $\mathrm{GL}_2(\mathbb{A}_f)$:

$$K_0(\mathfrak{n}):=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\mathrm{GL}_2(\widehat{\mathcal{O}_F})\,:\,c\in\mathfrak{n}\right\},$$

where $\widehat{\mathcal{O}_F}=\prod_{\mathfrak{p}}\mathcal{O}_{F,\,\mathfrak{p}}$. We set $\underline{t}=(1,\,\ldots,\,1)$ and $\underline{m}=\underline{k}-2\underline{t}$, then choose $\underline{v}\in\mathbb{Z}^{J_F}$ such that each $v_\tau\geq 0$, $v_\tau=0$ for some τ, and $\underline{m}+2\underline{v}=n\underline{t}$ for some non-negative $n\in\mathbb{Z}$.

Definition 5. *For any* $\gamma=\begin{pmatrix}a & b\\ c & d\end{pmatrix}\in\prod_\tau\mathrm{GL}_2(\mathbb{R})$ *and* $z\in\mathfrak{H}_F$, *put*

$$j(\gamma,\,z)=\prod_{\tau\in J_F}(c_\tau z_\tau+d_\tau).$$

The map $(\gamma,\,z)\mapsto j(\gamma,\,z)$ *is called an* automorphy factor.

Definition 6. *An* adelic Hilbert modular form *of weight* $\underline{k}$ *and level* $\mathfrak{n}$ *is a function* $f:\mathrm{GL}_2(\mathbb{A})\to\mathbb{C}$ *satisfying the following conditions:*

(i) $f(\gamma gu)=f(g)$ *for all* $\gamma\in\mathrm{GL}_2(F)$, $u\in K_0(\mathfrak{n})$ *and* $g\in\mathrm{GL}_2(\mathbb{A})$.
(ii) $f(gu)=\det(\gamma^\tau)^{\underline{k}-\underline{v}-\underline{t}}j(u,\,\underline{i})^{-\underline{k}}f(g)$ *for all* $u\in K_\infty^+$ *and* $g\in\mathrm{GL}_2(\mathbb{A})$.

For all $x\in\mathrm{GL}_2(\mathbb{A}_f)$, *define* $f_x:\mathfrak{H}_F\to\mathbb{C}$ *by* $z\mapsto\det(g)^{\underline{t}-\underline{v}-\underline{k}}j(g,\,\underline{i})f(xg)$, *where we choose* $g\in\prod_{\tau\in J_F}\mathrm{GL}_2^+(\mathbb{R})$ *such that* $z=g\cdot\underline{i}$. *By (ii)* f_x *does not depend on the choice of* g.

(iii) f_x *is holomorphic (when* $F=\mathbb{Q}$, *an extra holomorphy condition at cusps is needed).*
(iv) *In addition, when* $\int_{U(\mathbb{A})/U(\mathbb{Q})}f(ux)du=0$ *for all* $x\in\mathrm{GL}_2(\mathbb{A})$ *and all additive Haar measures* du *on* $U(\mathbb{A})$, *where* U *is the unipotent radical of* GL_2/F, *we say that* f *is an* adelic cusp form.

We will denote the space of all Hilbert modular forms (resp. cusp forms) of weight $\underline{k}$ and level $\mathfrak{n}$ by $M_{\underline{k}}(\mathfrak{n})$ (resp. $S_{\underline{k}}(\mathfrak{n})$). There is a relation between classical and adelic Hilbert modular forms which proves important when dealing with questions that relate to the arithmetic of these forms. To explain this relationship, let $\mathfrak{c}_\lambda$, $\lambda=1,\,\ldots,\,h^+$, be representatives of the narrow ideal classes of F. For each $\lambda=1,\,\ldots,\,h^+$, take $x_\lambda\in\mathrm{GL}_2(\mathbb{A})$, so that $t_\lambda=\det(x_\lambda)$ generates the ideal $\mathfrak{c}_\lambda$. Then, by the strong approximation theorem,

$$\mathrm{GL}_2(\mathbb{A})=\coprod_{\lambda=1}^{h^+}\mathrm{GL}_2(F)x_\lambda\left(\prod_\tau\mathrm{GL}_2^+(\mathbb{R})\times K_0(\mathfrak{n})\right),$$

and we see that

$$\Gamma_\lambda=\Gamma(\mathfrak{c}_\lambda,\,\mathfrak{n})=x_\lambda\left(\prod_\tau\mathrm{GL}_2^+(\mathbb{R})\times K_0(\mathfrak{n})\right)x_\lambda^{-1}\cap\mathrm{GL}_2(F).$$

To each adelic Hilbert modular form f, we associated the h^+-tuple $(f_1,\,\ldots,\,f_{h^+})\in\oplus_{\lambda=1}^{h^+}S_{\underline{k}}(\mathfrak{c}_\lambda,\,\mathfrak{n})$, where $f_\lambda=f_{x_\lambda}$ is given by Definition 6. Then, we have

Proposition 3. *The map*

$$\begin{array}{rcl} S_{\underline{k}}(\mathfrak{n}) & \to & \bigoplus_{\lambda=1}^{h^+} S_{\underline{k}}(\mathfrak{c}_\lambda,\, \mathfrak{n}) \\ f & \mapsto & (f_1,\, \ldots,\, f_{h^+}) \end{array}$$

is an isomorphism of complex vector spaces.

Proof. The converse of the map is given by the $\mathbb{C}$-valued function f on $\mathrm{GL}_2(\mathbb{A})$ defined by

$$f(\gamma x_\lambda g) = (f_\lambda \|_{\underline{k}} g_\infty)(\underline{i}), \quad \gamma \in \mathrm{GL}_2(F) \,\text{and}\, g \in \mathrm{GL}_2^+(\mathbb{R}) \times K_0(\mathfrak{n}).$$

□

2. Applications of Hilbert modular forms

The theory of Hilbert modular forms has a wide range of applications. Here we list few of them.

2.1. **Diophantine equations.** After Wiles proof of the Fermat Last Theorem, a strategy has been outlined by Darmon [3] in order to solve the generalized Fermat equation $x^p+y^q = z^r$, for p, q, r a set of arbitrary primes. In his framework, Hilbert modular play a central rôle. For example, to solve the generalized Fermat equation $x^p + y^p = z^5$ one is led to the natural consideration of Galois representations associated to Hilbert modular forms over the real quadratic field $\mathbb{Q}(\sqrt{5})$.

2.2. **Ramanujan graphs and construction of communication networks.** R. Livné, K. Lauter et al. have constructed Ramanujan graphs using Hilbert modular forms. Their works find some application to the construction of robust networks.

2.3. **The Serre conjecture for Hilbert modular forms.** Many conjectures relating the classical modular forms find their natural generalization to the setting of Hilbert modular forms. One such conjecture is the Serre conjecture. In this case it is stated as follows.

Conjecture 1. *Let $\rho : \mathrm{Gal}(\overline{F}/F) \to \mathrm{GL}_2(\overline{\mathbb{F}_\ell})$ be a continous irreducible Galois representation such that $\det(\rho(c_\tau)) = -1$, where c_τ is complex conjugation at $\tau \in J_F$, ane which is unramified outside a finite set of primes. Then ρ comes form a Hilbert cusp form.*

The Serre conjecture for Hilbert modular forms is still far from a complete proof as the key ingredient used by Khare and others in the classical setting quickly breaks down in this case.

3. The Hecke action on Hilbert modular forms

In the rest of these notes, we will make some simplifying assumptions. We will assume that F is a quadratic field of narrow class number one. This assumption have the advantage of making the analogy between Hilbert modular forms and their classical counterpart more transparent.

Let

$$\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2^+(\mathcal{O}_F) : \, c \in \mathfrak{n} \right\}.$$

Then Definition 6 and Proposition 3 now specialize to give the following.

Definition 7. *A* Hilbert modular form *of level* $\mathfrak{n}$ *and weight* $\underline{k}$ *is a holomorphic function* $f : \mathfrak{H}_F \to \mathbb{C}$ *such that* $f\|_{\underline{k}}\gamma = f$*, for all* $\gamma \in \Gamma_0(\mathfrak{n})$*.*

Again, we recall that the space of Hilbert modular forms of level $\mathfrak{n}$ and weight $\underline{k}$ will be denoted by $M_{\underline{k}}(\mathfrak{n})$. Now, let $f \in M_{\underline{k}}(\mathfrak{n})$ be a Hilbert modular form. We recall that, by Koecher's principle, f is holomorphic at cusps, so that it admits a Fourier expansion

$$f(z) = \sum_{\substack{\mu=0,\\ \mu\gg 0}} a_\mu e^{2\pi i \mathrm{Tr}(\mu z)}.$$

For any integral ideal $\mathfrak{a}$, choose a totally positive generator μ of $\mathfrak{a}$ and put

$$c(\mathfrak{a},\, f) := \mathrm{N}(\mu)^{\underline{k}}/2a_\mu.$$

Lemma 2 (Lemma-Definition)**.** *The coefficient* $c(\mathfrak{a},\, f)$ *does not depend on the choice of the generator* $\mu \gg 0$*. We call it the* Fourier coefficient *of the form* f associated to the integral ideal $\mathfrak{a}$*. The L-series attached to* f *is given by*

$$L(f,\, s) := \sum_{\mathfrak{a}\subseteq \mathcal{O}_F} \frac{c(\mathfrak{a},\, f)}{\mathrm{N}(\mathfrak{a})^{-s}},\ s \in \mathbb{C}.$$

The L-series of a modular cusp form is an entire function; i.e., it is holomorphic on the whole complex plane. We will see later that, for a particular class of cusp forms, it encodes lot of arithmetic properties.

3.1. The Hecke operators.

Let $\mathfrak{p} \not| \mathfrak{n}$ be a prime ideal and $\pi_{\mathfrak{p}}$ a totally positive generator of $\mathfrak{p}$. We write the finite disjoint union

$$\Gamma_0(\mathfrak{n}) \begin{pmatrix} 1 & 0 \\ 0 & \pi_{\mathfrak{p}} \end{pmatrix} \Gamma_0(\mathfrak{n}) = \coprod_i \Gamma_0(\mathfrak{n}) u_i,$$

and for each $f \in M_{\underline{k}}(\mathfrak{n})$, we put

$$f\|_{\underline{k}} T_{\mathfrak{p}} := \sum_i f\|_{\underline{k}} u_i.$$

This gives a well defined linear map $T_{\mathfrak{p}} : M_{\underline{k}}(\mathfrak{n}) \to M_{\underline{k}}(\mathfrak{n})$ which preserves the cusp space $S_{\underline{k}}(\mathfrak{n})$. We call $T_{\mathfrak{p}}$ the *Hecke operator at the prime* $\mathfrak{p}$. This definition can be extended to the primes $\mathfrak{p}$ that divide the level $\mathfrak{n}$. The Hecke operators $\mathfrak{p}$, as $\mathfrak{p}$ runs through all the primes in F, generate a finite $\mathbb{Z}$-subalgebra of $\mathrm{End}(S_{\underline{k}}(\mathfrak{n}))$ which we call the Hecke algebra of level $\mathfrak{n}$ and denote by $\mathbb{T}_0(\mathfrak{n})$.

3.2. Eigenforms and Hecke action.

The Hecke algebra $\mathbb{T}_0(\mathfrak{n})$ is a commutative algebra which is (almost) self-adjoint with respect to an inner product on $S_{\underline{k}}(\mathfrak{n})$ called the *Petersson inner product.* As a result, it is diagonalizable and admits a common basis of eigenvectors.

Definition 8. *Let* f *be a Hilbert modular cusp form. We say that* f *is an* eigenform *if it is a common eigenvector for the Hecke algebra. A* normalized eigenform *is an eigenform* f *such that* $c(\mathcal{O}_F,\, f) = 1$*.*

Thanks to Shimura [12], we have the following result.

Theorem 4 (Shimura)**.** *Let* $f \in S_{\underline{k}}(\mathfrak{n})$ *be a normalized eigenform. Then for each integral ideal* $\mathfrak{a}$*, the Fourier coefficient* $c(\mathfrak{a},\, f)$ *is an* algebraic integer *which satisfies the relation:*

$$T_{\mathfrak{a}} f = c(\mathfrak{a},\, f) f.$$

Moreover, the field $K_f = \mathbb{Q}(c(\mathfrak{a},\, f),\, \mathfrak{a} \subseteq \mathcal{O}_F)$ generated by the $c(\mathfrak{a},\, f)$ is a number field (i.e. $[K_f : \mathbb{Q}] < \infty$).

The L-series of a normalized eigenform f encodes lot of arithmetic properties related to it. And so, by computing the Fourier expansion of the form f, one expects to gain access to some of that arithmetic.

4. **The Jacquet-Langlands correspondence and the space of Hilbert modular forms**

In this section, we will assume that $\underline{k} = (2,\, 2)$.

4.1. **Automorphic forms on definite quaternion algebras.** We choose a quaternion algebra B/F such that $\mathrm{Ram}(B) = J_F$ i.e., $B \otimes_{\mathbb{Q}} \mathbb{R} \cong \mathbb{H}^2$ and for each finite prime $\mathfrak{p}$, $B_{\mathfrak{p}} = B \otimes_F F_{\mathfrak{p}} \cong M_2(F_{\mathfrak{p}})$ (this is possible thanks to the classification theorem of quaternion algebras over global fields. See Vignéras [14, Théorème 2.2]). We fix a maximal order R of B and for each prime $\mathfrak{p}$, we choose the isomorphism $B_{\mathfrak{p}} \cong M_2(F_{\mathfrak{p}})$ such that $R = M_2(\mathcal{O}_{F,\,\mathfrak{p}})$. We let $\nu : B \to F$ denote the reduced norm map on B. The local isomorphisms $B_{\mathfrak{p}} = M_2(F_{\mathfrak{p}})$ piece together to give identifications $\hat{B} = M_2(\mathbb{A}_f)$ and $\hat{R} = M_2(\widehat{\mathcal{O}_F})$, where $\hat{B}$ (resp. $\hat{R}$) is the finite part of the adelization of $B_{\mathbb{A}}$ (resp. $R_{\mathbb{A}}$). The reduced norm map extends to $\nu : \hat{B} \to \mathbb{A}_f$.

Definition 9. *The* space of automorphic forms *of weight* 2 *and level* $\mathfrak{n}$ *on* B *is defined by*

$$M_2^B(\mathfrak{n}) = \left\{ B^\times \backslash \hat{B}^\times / K_0(\mathfrak{n}) \to \mathbb{C} \right\}.$$

We put

$$\begin{aligned} I_2(\mathfrak{n}) &= \left\{ f \in M_2^B(\mathfrak{n}) : f \,\text{factors through}\, \hat{B}^\times / K_0(\mathfrak{n}) \xrightarrow{\nu} \mathbb{A}_f^\times / \nu(K_0(\mathfrak{n})) \right\}, \\ S_2^B(\mathfrak{c}) &= M_2^B(\mathfrak{n}) / I_2(\mathfrak{n}). \end{aligned}$$

4.2. **Hecke action on automorphic forms.** The space of automorphic forms come equipped with a Hecke action that is given as follows. For any $u \in \hat{B}^\times$, $u \neq 0$, write the finite disjoint union $K_0(\mathfrak{n}) u K_0(\mathfrak{n}) = \coprod_i u_i K_0(\mathfrak{n})$ and, for each element $f \in M_2^B(\mathfrak{n})$ put

$$f \| [K_0(\mathfrak{n}) u K_0(\mathfrak{n})](x) = \sum_i f(x u_i),\ x \in \hat{B}^\times.$$

This gives a linear operator on $M_2^B(\mathfrak{n})$ which preserves $S_2^B(\mathfrak{n})$. We call this the Hecke operator $[K_0(\mathfrak{n}) u K_0(\mathfrak{n})]$. They generated a finite $\mathbb{Z}$-subalgebra of $\mathrm{End}(S_2^B(\mathfrak{n}))$ called the Hecke algebra $\mathbb{T}_0^B(\mathfrak{n})$ of level $\mathfrak{n}$. The space $S_2^B(\mathfrak{n})$ equipped with the action of $\mathbb{T}_0^B(\mathfrak{n})$ is sometime called a *Brandt module.*

4.3. **The Jacquet-Langlands correspondence.** If one wishes to experiment on Hilbert modular forms, one needs to be able to explicitly compute them. In order to do so, one must strip them of their purely analytic nature which, *a priori*, seems very rigid. This is somewhat achieved via the following theorem which is due to several people including Eichler, Shimizu, Jacquet and Langlands. The theorem is stated in this form in Hida [**?**].

Theorem 5 (Eichler-Shimizu). *There is an isomorphism of Hecke modules*

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

From its definition, we see that the space $S_2^B(\mathfrak{n})$ is purely combinatorial in nature, thus is relatively simple and reasonably computable. However, that relative simplicity is in sharp constrast with the content of Theorem 5 which says that it encodes lots of the arithmetic of Hilbert modular forms via its Hecke module structure.

4.4. **Expliciting the Brandt module $S_2^B(\mathfrak{n})$.** In this section, we describe the Brandt module $S_2^B(\mathfrak{n})$ in a way that lends itself better to computation. This will provide us with an efficient algorithm to compute the space of Hilbert modular forms. In order to simplify the exposition, we will assume that the quadratic field F is chosen such that the quaternion algebra B has class number one (examples of such quadratic fields are $\mathbb{Q}(\sqrt{5})$, $\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{13})$ and $\mathbb{Q}(\sqrt{17})$. To see how one can relax those conditions, we refer to [4].

We start by recalling that $B^\times\backslash\hat{B}^\times/\hat{R}^\times$ parameterizes the set of right ideal classes of R. Thus, since B has class number one,

$$B^\times\backslash\hat{B}^\times/\hat{R}^\times = \{B^\times\hat{R}^\times\}, \quad \text{and} \quad \hat{B}^\times = B^\times\hat{R}^\times.$$

Hence, we have the following bijections.

$$\begin{aligned} B^\times\backslash\hat{B}^\times/K_0(\mathfrak{n}) &\cong R^\times\backslash\hat{R}^\times/K_0(\mathfrak{n}) = R^\times\backslash\left(\prod_{\mathfrak{q}|\mathfrak{n}} R_{\mathfrak{q}}^\times/K_0(\mathfrak{q}^{e_\mathfrak{q}})\right) \\ &\cong R^\times\backslash\left(\prod_{\mathfrak{q}|\mathfrak{n}} \mathbf{P}^1(\mathcal{O}_{F,\mathfrak{q}}/\mathfrak{q}^{e_\mathfrak{q}})\right) = R^\times\backslash\mathbf{P}^1(\mathcal{O}_F/\mathfrak{n}), \end{aligned}$$

where $\mathfrak{n} = \prod_{\mathfrak{q}|\mathfrak{n}} \mathfrak{q}^{e_\mathfrak{q}}$ and

$$\mathbf{P}^1(A) = \left\{(a,\, b) \in A^2 :\ \alpha a + \beta b = 1 \text{ for some } (\alpha,\, \beta) \in A^2\right\}/A^\times,$$

for any ring A. We now recall the action of $\mathbf{GL}_2(A)$ on $\mathbf{P}^1(A)$:

$$m\cdot(x:y) := (ax+by : cx+dy), \quad m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Letting $X_0^B(\mathfrak{n}) = R^\times\backslash\mathbf{P}^1(\mathcal{O}_F/\mathfrak{n})$, we can reinterpret the Hecke action on the free module $\mathbb{Z}[X_0^B(\mathfrak{n})]$ as follows. For each prime $\mathfrak{p}$, let

$$\Theta(\mathfrak{p}) = R^\times\backslash\left\{u \in R : \mathrm{N}(u) = \pi_\mathfrak{p}\right\}.$$

Then, for each $f \in S_2^B(\mathfrak{n})$, we let

$$f\|T_p(x) = \sum_{u\in\Theta(\mathfrak{p})} u\cdot x,\ x \in X_0^B(\mathfrak{n}),$$

and extend it linearly to $\mathbb{Z}[X_0^B(\mathfrak{n})]$.

4.5. **Algorithm and implementation.** We describe the main steps of the algorithm below.

(1) Find a maximal order $R = \mathbb{Z}e_1 \oplus \mathbb{Z}e_2 \oplus \mathbb{Z}e_3 \oplus \mathbb{Z}e_4$ in B and compute its group of norm 1 elements $R_1^\times$.

(2) Let $\mathfrak{p}$ be a prime in F, and $\pi_{\mathfrak{p}}$ a totally positive generator at $\mathfrak{p}$. To compute $T_{\mathfrak{p}}$, we need to find representatives for $\Theta(\mathfrak{p})$. This amounts to finding quaternions

$$q = xe_1 + ye_2 + ze_3 + we_4 \quad \text{with } x,\, y,\, z,\, w \in \mathbb{Z}[\omega],$$

which represent $\pi_{\mathfrak{p}}$ under the reduced norm map of B. We find all such elements up to equivalence by a unit. We compute a collection of sets $\Theta(\mathfrak{p})$ that we store once and for all.

(3) For each prime $\mathfrak{p} \mid \mathfrak{n}$, we need to find a local isomorphism

$$R \otimes (\mathcal{O}_F/\mathfrak{p}^{e_{\mathfrak{p}}}) = M_2(\mathcal{O}_F/\mathfrak{p}^{e_{\mathfrak{p}}}).$$

This amounts to finding a set of generators for $M_2(\mathcal{O}_F/\mathfrak{p}^{e_{\mathfrak{p}}})$ which satisfies the appropriate relations corresponding to the basis we have chosen for R.

(4) Compute the space $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{n})$ alongside with the orbits and a fundamental domain under the action of $R_1^\times$. We have chosen to work with the product

$$\mathbf{P}^1(\mathcal{O}_F/\mathfrak{n}) = \prod_{\mathfrak{p}\mid\mathfrak{n}} \mathbf{P}^1(\mathcal{O}_F/\mathfrak{p}^{e_{\mathfrak{p}}}).$$

Then the coset representatives for each local factor $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{p}^{e_{\mathfrak{p}}})$ are taken to be all pairs

$$(1,\, a), \quad a \in \mathfrak{p}/\mathfrak{p}^{e_{\mathfrak{p}}}, \quad \text{and} \quad (a,\, 1), \quad a \in (\mathcal{O}_F/\mathfrak{p}^{e_{\mathfrak{p}}}).$$

This representation of the projective line $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{n})$ has the advantage of facilitating look up. Also splitting R at one prime at the time is more efficient.

(5) Compute the action of the Hecke operator $T_{\mathfrak{p}}$.

Example 3. Let $F = \mathbb{Q}(\sqrt{5})$, $\omega = \frac{1+\sqrt{5}}{2}$, and B be the standard Hamilton quaternion algebra over F:

$$B = \{x + yi + zj + wk, \quad x,\, y,\, z,\, w \in F\}.$$

Since 2 is inert in F, B is only ramified at both infinite places. By Körner [9, Theorem 2] or Socrates and Whitehouse [13, Theorem 6.2], the class number of B is *one*. Every maximal order in B is then conjugate to the icosian ring

$$R = \mathbb{Z}[\omega][e_1,\, e_2,\, e_3,\, e_4],$$

with

$$\begin{aligned} e_1 &= \frac{1}{2}(1 - \bar{\omega}i + \omega j),\\ e_2 &= \frac{1}{2}(-\bar{\omega}i + j + \omega k),\\ e_3 &= \frac{1}{2}(\omega i - \bar{\omega}j + k),\\ e_4 &= \frac{1}{2}(i + \omega j - \bar{\omega}k), \end{aligned}$$

and $\omega = (1+\sqrt{5})/2$. The group of units $R^\times$ is the semi-direct product of $R_1^\times$ with $\mathbb{Z}$, where $R_1^\times$ is the subgroup of norm 1 elements is isomorphic to the binary icosahedral group of order 120. (Cf. [2, Chap. 8, sec. 2.1]).

Now, let $\mathfrak{n} = (5 + 2\omega)$, so that $\mathrm{N}(\mathfrak{n}) = 31$. This is the smallest norm for which there exist Hilbert modular cusp forms of parallel weight $(2, 2)$ on $F = \mathbb{Q}(\sqrt{5})$. A fundamental domain for the action of the icosian group on $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{n})$ is $S = \{e_1 = (1 : 0),\, e_2 = (1 : 10)\}$. This means that $\dim M_2(\mathfrak{n}) = 2$. The first few Brandt matrices are:

$$\mathcal{B}_2 = \begin{pmatrix} 2 & 3 \\ 5 & 0 \end{pmatrix}, \quad \mathcal{B}_{\sqrt{5}} = \begin{pmatrix} 3 & 3 \\ 5 & 1 \end{pmatrix}, \quad \text{and} \quad \mathcal{B}_3 = \begin{pmatrix} 7 & 3 \\ 5 & 5 \end{pmatrix}.$$

The space $M_2(\mathfrak{n})$ decomposes into two one-dimensional eigenspaces given by $v_1 = e_1 + \frac{3}{5}e_2$ and $v_2 = e_1 - e_2$. The vector v_1 corresponds to the Eisentein series, while the vector v_2 corresponds to a normalized eigenform f. We will compute the modular elliptic curve of conductor $(5 + 2\omega)$ corresponding to f (see Section 3).

5. An algorithm for modular elliptic curves over real quadratic fields

For simplicity, we will assume in this section that their is a fundamental unit $\omega \in F$ whose norm is -1. Let f be a Hilbert eigenform whose L-series is denoted by $L(f,\, s)$. Then we have the following conjecture known as the Eichler-Shimura construction in the classical setting.

Conjecture 2. *Let f be a Hilbert eigenform with rational Fourier coefficients. Then there exists an elliptic curve E_f such that $L(E_f,\, s) = L(f,\, s)$.*

This conjecture is known for $F = \mathbb{Q}$ and the proof uses the arithmetic theory of the modular curve $X_0(\mathfrak{n})$ and its Jacobian $\mathrm{Jac}(X_0(\mathfrak{n}))$. Unfortunately, the theory of modular Jacobians does not generalized very well to higher dimension as Hilbert-Blumenthal modular varieties prove not to be good substitutes to the modular curve. Nonetheless, one expects this conjecture to be true and wishes to have an explicit algorithm that constructs the curve E_f given the Fourier expansion of the form f as in the classical setting. Our goal in this section is to provide such an algorithm assuming that the corresponding curve has square-free conductor, i.e. is *semi-stable.*

5.1. The strategy of the algorithm.

In [10], Oda gives the elliptic curve E_f as a complex curve. We intend to use the Weierstrass uniformization theorem in order to find an equation for E_f over F. First, let $\omega_f = (2\pi i)^2 f(z_1,\, z_2)dz_1dz_2$ be the differential form attached to f. The period lattice of the form f is given by

$$\Lambda_f = \mathbb{Z}\Omega_f^{++} \oplus \mathbb{Z}\Omega_f^{+-}i \oplus \mathbb{Z}\Omega_f^{-+}i \oplus \mathbb{Z}\Omega_f^{--},$$

where $\Omega_f^{ss'}$, $s,\, s' \in \{-,\, +\}$ are positive real numbers. This lattice is only well-defined up to a rational multiple and, as one sees, its rank is double the one of the elliptic curve E_f. This phenomenon illustrates the fact that the periods of the form f are actually mixes of the periods of E_f and its Galois conjugate $\overline{E}_f$. Unfortunately, there is no known method to seperate the periods of Λ_f. So in order to get the curve E_f, we need a way to overcome this problem. Our approach is to compute the j-invariant of the curve E_f. The j-invariant of E_f as a modular function is given by $j(\tau)$ where

$$\tau = \frac{\Omega_f^{+-}}{2\Omega_f^{++}}i \text{ or } \tau = \frac{1}{2}\left(1 + \frac{\Omega_f^{+-}}{\Omega_f^{++}}i\right),$$

depending on wether the real locus of E_f has one or two connected components. We can assume without loss of generality that the curve $E = E_f$ is a global minimal Weierstrass equation. Then $j(\tau) = j(E) = \frac{c_4^3}{\Delta_E}$. Since we assume E to be semi-stable as well, we can look for E such that

$$\Delta_E = \varepsilon N, \text{ where } \varepsilon \in \mathcal{O}_F^\times / \left(\mathcal{O}_F^\times\right)^{12},$$

and N is a totally positive generator of $\mathfrak{n}$. So knowing $j(\tau)$ to enough precision, we can obtain c_4 and also c_6 from the relation $c_4^3 - c_6^2 = 1728\Delta_E$ and reconstruct a minimal Weierstrass equation for E from its invariants c_4 and c_6.

5.2. **The oda periods lattice.** Let $\chi : (\mathcal{O}_F/\mathfrak{c})^\times \to \mathbb{C}^\times$ be a primitive quadratic character of conductor $\mathfrak{c} = (\nu)$ that is prime to $\mathfrak{n}$, where $\nu \gg 0$. Also let $V \subset \mathcal{O}_F^{\times +}$ be a subgroup of finite index such that $V \subset 1 + \mathfrak{c}$. We extend the character χ to non-units in the obvious way. The twisted L-series of f by χ is given by

$$L(f, \chi, s) := \sum_{\mathfrak{a} \subseteq \mathcal{O}_F} \frac{\chi(\mathfrak{a}) c(\mathfrak{a}, f)}{\mathrm{N}(\mathfrak{a})^{-s}}.$$

Proposition 6 (Oda). *Let*

$$\Omega^{ss'}_{f,\chi,V} = -4\pi^2 \mathrm{disc}(F)[\mathcal{O}_F^{\times +} : V] G(\overline{\chi}) L(f, \chi, 1),$$

where $G(\chi)$ is the Gauss sum of the character χ, and $\chi(\omega) = s$ and $\chi(\bar{\omega}) = s'$. Then $\Omega^{ss'}_{f,\chi,V}$ is a rational multiple of $\Omega^{ss'}_f$ when $\chi(-1) = ss'$.

By making use of Proposition 6, it is easy to compute the period lattice Λ_f up to homothety. But in analogy with the classical settting, one expects a stronger statement to be true. Namely, we make the following conjecture.

Conjecture 3 (The period conjecture). *Let $\chi : (\mathcal{O}_F/\mathfrak{c})^\times \to \mathbb{C}^\times$ be a primitive quadratic character of conductor $\mathfrak{c} = (\nu)$ that is prime to $\mathfrak{n}$, where $\nu \gg 0$. Let*

$$\Omega^{ss'}_{f,\chi} = -4\pi^2 \mathrm{disc}(F) G(\overline{\chi}) L(f, \chi, 1),$$

where $G(\chi)$ is the Gauss sum of the character χ, and $\chi(\omega) = s$ and $\chi(\bar{\omega}) = s'$. Then $\Omega^{ss'}_{f,\chi}$ is an integral multiple of $\Omega^{ss'}_f$ when $\chi(-1) = ss'$.

5.3. **Computing the periods lattice.** All that remains in order to compute the elliptic curve E_f is to find an efficient way to compute the period lattice Λ_f. This amounts to finding a way to compute the the special values $L(f, \chi, 1)$.

Let W_N be the Atkin-Lehner involution given by

$$W_N : z = (z_1, z_2) \mapsto (-\frac{1}{N z_1}, -\frac{1}{\bar{N} z_2}),$$

where N is a totally positive generator of $\mathfrak{n}$, and let

$$\begin{aligned} f(z_1, z_2) &= \sum_{\mu \in \mathcal{O}_F^+} c((\mu)) \exp[2\pi i (\mathrm{Tr}(\frac{\mu\omega z}{\sqrt{D}})] \\ &= \sum_{\mu \in \mathcal{O}_F^+ / \mathcal{O}_F^{\times +}} c((\mu)) \sum_{\varepsilon \in \ \mathcal{O}_F^{\times +}} \exp[2\pi i \mathrm{Tr}(\frac{\varepsilon\mu\omega z}{\sqrt{D}})] \end{aligned}$$

be the q-expansion of f. Then $f_\chi = f \otimes \chi \in S_2(\mathfrak{n}\mathfrak{c}^2)$ and its q-expansion is given by

$$\begin{aligned} f \otimes \chi(z_1,\, z_2) &= \sum_{\mu \in \mathcal{O}_F^+} c((\mu))\chi(\mu) \exp[2\pi i \mathrm{Tr}(\frac{\mu\omega z}{\sqrt{D}})] \\ &= \sum_{\mu \in \mathcal{O}_F^+/\mathcal{O}_F^{\times +}} c((\mu))\chi(\mu) \sum_{\varepsilon \in\ \mathcal{O}_F^{\times +}} \exp[2\pi i \mathrm{Tr}(\frac{\varepsilon\mu\omega z}{\sqrt{D}})]. \end{aligned}$$

The following lemma gives an optimized way to compute the special value $L(f,\, \chi,\, 1)$ for a given character χ.

Lemma 3. *Let $f \in S_2(\mathfrak{n})$ be an eigenform. If $W_N f = -f$, then $L(f,\, 1) = 0$; otherwise*

$$\begin{aligned} L(f,\, 1) &= -\frac{D}{2\pi^2} \sum_{\mu \in \mathcal{O}_F^+} \frac{c((\mu))}{\mathrm{N}(\mu)} \left[1 - \exp\left(-\frac{2\pi\mu\omega}{\sqrt{DN}}\right)\right] \times \\ &\quad \exp\left[\frac{2\pi}{\sqrt{D}}\left(\frac{\bar{\mu}\bar{\omega}}{\sqrt{\bar{N}}} - \frac{\mu}{\sqrt{N}}\right)\right]. \end{aligned}$$

Remark 1. Let χ is a quadratic character of conductor $\mathfrak{c}$. Then, by Atkin-Lehner, we know that $f_\chi \in S_2(\mathfrak{n}\mathfrak{c}^2)$ and $W_{N\nu^2} f_\chi = \varepsilon_N \chi(-N) f_\chi$. Therefore, by Lemma 3, when $\varepsilon_N \chi(-N) = 1$,

$$\begin{aligned} L(f,\, \chi,\, 1) &= -\frac{D}{2\pi^2} \sum_{\mu \in \mathcal{O}_F^+} \frac{c((\mu))}{\mathrm{N}(\mu)} \chi(\mu) \left[1 - \exp\left(-\frac{2\pi\mu\omega}{\nu\sqrt{DN}}\right)\right] \times \\ &\quad \exp\left[\frac{2\pi}{\sqrt{D}}\left(\frac{\bar{\mu}\bar{\omega}}{\bar{\nu}\sqrt{\bar{N}}} - \frac{\mu}{\nu N}\right)\right]. \end{aligned}$$

By using the fact that every totally positive element is of the form ω^{2k}, $k \in \mathbb{Z}$, this series can be rearranged as

$$\begin{aligned} L(f,\, \chi,\, 1) &= -\frac{D}{2\pi^2} \sum_{\mu \in \mathcal{O}_F^+/\mathcal{O}_F^{+\times}} \frac{c((\mu))}{\mathrm{N}(\mu)} \chi(\mu) \times \sum_{k \in \mathbb{Z}} \left[1 - \exp\left(-\frac{2\pi\mu\omega^{2k+1}}{\nu\sqrt{DN}}\right)\right] \times \\ &\quad \exp\left[\frac{2\pi}{\sqrt{D}}\left(\frac{\bar{\mu}\bar{\omega}^{2k+1}}{\bar{\nu}\sqrt{\bar{N}}} - \frac{\mu\omega^{2k}}{\nu N}\right)\right]. \end{aligned}$$

5.4. **The algorithm.** We need to solve the following problem: Given a Hilbert eigenform f with rational Fourier coefficients, find an elliptic curve which shares the same L-series. Assuming that we know all the possibilities for the discriminant of E_f, we can proceed as follows in order to find E_f.

1) Try several quadratic characters in order to determine the periods $\Omega_f^{ss'}$, $s,\, s' \in \{-,\, +\}$ for the curve E_f and its Galois conjugate $\overline{E}_f$. We need to try characters χ whose conductors are as small as possible since the size of the conductor of χ affects the speed of convergence of the series that determines $L(f,\, \chi,\, 1)$.
(2) Now choose

$$\Delta_E = \varepsilon N, \text{ where } \varepsilon \in \mathcal{O}_F^\times / \left(\mathcal{O}_F^\times\right)^{12}.$$

(3) For each possible choice of (τ, τ') corresponding to a curve E_f and its Galois conjugate $\overline{E}_f$, compute $(j(\tau), j(\tau'))$ and approximations of c_4 and its conjugate $\bar{c}_4$. In most cases, it will be easy to recognize $c_4 - \bar{c}_4$ and $(c_4 + \bar{c}_4)/\sqrt{D}$ as integers. If c_4 corresponds to an elliptic curve, the equation $c_4^3 - c_6^2 = 1728\Delta_E$ should have a solution $c_6 \in \mathcal{O}_F$.

(4) For each pair (c_4, c_6), find a minimal Weierstrass equation for E and check that its $a_{\mathfrak{p}}(E)$ agree with the Fourier coefficients of f up to a convenient bound.

(5) Repeat Step (2).

Example 4. Let $\mathfrak{n} = (5 + 2\omega)$ be one of the primes above 31 in $\mathbb{Q}(\sqrt{5})$, where $\omega = \frac{1+\sqrt{5}}{2}$. In Example 3, we found that there is a normalized eigenform with rational Fourier coefficients of weight 2 and level $\mathfrak{n}$. We want to find an elliptic curve E_f/F of conductor $\mathfrak{n}$. Let $\mathfrak{c}_1 = (2 + \omega)$ be the unique prime above 5 and $\chi_1 : (\mathcal{O}_F)/\mathfrak{c}_1)^\times \to \mathbb{C}^\times$ and the unique quadratic character such that $\chi_1(\omega) = \chi_1(\bar{\omega}) = -1$. Also, let $\mathfrak{c}_2 = (4)$ and $\chi_2 : (\mathcal{O}_F)/\mathfrak{c}_2)^\times \to \mathbb{C}^\times$ be the quadratic character given by $\chi_2(\omega) = -1 = \chi_2(-1)$. By Conjecture 3, Ω^{--}_{f,χ_1} (resp. Ω^{-+}_{f,χ_2}) is an integral multiple of Ω^{--}_f (resp. Ω^{-+}_f). Using all the ideals $\mathfrak{a}$ of norm less than 300, we get

$$\begin{aligned} \Omega^{--}_{f,\chi_1} &\approx 16.8661486239692312162791057502 \\ \Omega^{-+}_{f,\chi_2} &\approx 42.9244848862008074661091868 49. \end{aligned}$$

So the j-invariant for one of the complex values

$$\begin{aligned} \tau &= 0.785852115345537601905542169713i, \text{ or} \\ \tau &= 0.500000000000000000000000000000 + 0.196463028836384400476385542428i \end{aligned}$$

will give an approximation of the j-invariant of E_f. Now, let us consider the unique normalized eigenform g of weight 2 and level $\bar{\mathfrak{n}}$ with rational Fourier coefficients. We let $\mathfrak{c}_3 = (3 + \omega)$ be a prime above 11 and $\chi_3 : (\mathcal{O}_F)/\mathfrak{c}_3)^\times \to \mathbb{C}^\times$ the quadratic character given by $\chi_3(\omega) = -1 = \chi_3(-1)$. Again, by Conjecture 3, Ω^{--}_{g,χ_1} (resp. Ω^{-+}_{g,χ_3}) is an integral multiple of Ω^{--}_g (resp. Ω^{-+}_g). We compute

$$\begin{aligned} \Omega^{--}_{g,\chi_1} &\approx 16.8661486239692312162791057502 \\ \Omega^{-+}_{g,\chi_3} &\approx 45.2616150179158694617966907088. \end{aligned}$$

So the j-invariant for one of the complex numbers

$$\begin{aligned} \tau' &= 0.745273831580827015400644954558i, \text{ or} \\ \tau' &= 0.500000000000000000000000000000 + 0.186318457895206753850161238640i \end{aligned}$$

will give an approximation of the j-invariant of $\overline{E}_f$. For $\Delta_E = \omega^3(5 + 2\omega)$ and

$$\begin{aligned} \tau &= 0.785852115345537601905542169713i, \text{ and} \\ \tau' &= 0.500000000000000000000000000000 + 0.186318457895206753850161238640i, \end{aligned}$$

we get the j-invariants

$$\begin{aligned} j(\tau) &= 3780.04179066913837118227698528 \\ j(\tau') &= -3883.66182805439499524399028631 \\ &\qquad + 5.54997066847859914607241905399E - 27i. \end{aligned}$$

From this, we get that

$$\begin{aligned} \frac{c_4+\bar{c}_4}{2} &\approx 33.006245461892707877380114669 3 \\ \frac{c_4-\bar{c}_4}{2\sqrt{5}} &\approx 8.0027862672444137719105913771 5, \end{aligned}$$

which implies that $c_4 = 25+8\omega$. We solve the discriminant relation for c_6. The only acceptable solution is the $c_6 = -125 - 88\omega$. By applying the Tate-Kraus algorithm to the curve $y^2 = x^3 - c_4x - c_6$, we obtain the minimal integral model

$$E_f : y^2 + xy + \omega y = x^3 - (1+\omega)x^2.$$

Its j-invariant is

$$j(E) = \frac{-54753 + 106208\omega}{31}.$$

Example 5. Let $\mathfrak{n} = (7)$ be the inert prime above 7. There is a unique normalized eigenform of weight 2 and level $\mathfrak{n}$ with rational Fourier coefficients. We want to find a modular elliptic curve E_f that corresponds to f. If such a curve exists, it should be isomorphic to its Galois conjugate as they share the same eigenform. So we can look for a curve whose j-invariant is of the form $\Delta = \pm\frac{c_4^3}{7}$, with $c_4 \in \mathbb{Q}$. Using the character χ_2 and χ_3 of the previous example, we compute the periods

$$\begin{aligned} \Omega_{f,\chi_2}^{--} &\approx -34.441042163916172359753966505295 \\ \Omega_{f,\chi_3}^{-+} &\approx -44.855133493323226425099174201646. \end{aligned}$$

We need to test which one of the complex values

$$\begin{aligned} \tau &= 0.7678283282568490906825541733204421772820584428553372, \text{ or} \\ \tau &= 0.5000000000000000000000000000000000000000000000000000 \\ &\qquad + 0.38391416412842454534127708666022108864102922142i. \end{aligned}$$

determines an elliptic curve that matches f. Here we get that only the first value does. It gives the approximate j-invariant

$$\begin{aligned} j(\tau) &= 586.260662083359821387320007678317020253629313949 63 \\ &\qquad - 1.7952752594709468519103225168226447075093 5E - 97i, \end{aligned}$$

and the approximate

$$c_4 = 16.0101818455325540375430382206961624931269468940836768667013.$$

We get $c_4 = 16$ and $j(E) = \frac{16^3}{7}$. This is the j-invariant of the curve E listed as $175A1$ in Cremona's tables.

References

[1] C. Consani and J. Scholten, Arithmetic on a quintic threefold. *International Journal of Mathematics* **12**, No. 8 (2001), pp. 943-972.

[2] J. H. Conway and Sloane, Sphere packings, lattice and groups. Second edition. Springer Verlag, New York, 1993.

[3] H. Darmon, Rigid local systems, Hilbert modular forms, and Fermat's last theorem. *Duke Math. J.* **102** (2000), no. 3, 413–449.

[4] Dembélé, Lassina; Explicit computations of Hilbert modular forms on $\mathbb{Q}(\sqrt{5})$. *Experiment. Math.* **14** (2005), no. 4, 457–466.

[5] L. Dembélé, Quaternionic M-symbols, Brandt matrices and Hilbert modular forms. To appear in *Mathematics of Computation.*

[6] L. Dembélé, An algorithm for modular semi-stable elliptic curves over real quadratic fields. (In preparation).

[7] G. van der Geer, Hilbert modular surfaces, Springer-Verlag, New York-Berlin, 1988.

[8] H. Jacquet and R. P. Langlands, Automorphic forms on GL(2). Lectures Notes in Math., vol. 114, Springer-Verlag, Berlin and New York, 1970.

[9] O. Körner, Traces of Eichler-Brandt matrices and type numbers of quaternions orders, *Proc. Indian. Acad. Sci.* **97** (1987), 187-199.

[10] Oda, Takayuki Periods of Hilbert modular surfaces. Progress in Mathematics, 19. Birkhuser, Boston, Mass., 1982.

[11] Pizer, Arnold; An algorithm for computing modular forms on $\Gamma_0(N)$. *J. Algebra* **64** (1980), no. 2, 340–390.

[12] G. Shimura, The special values of the zeta functions associated to Hilbert modular forms. *Duke Math. J.* **45**, No. 3 (1978), pp. 637-679.

[13] Socrates, Jude; Whitehouse, David. Unramified Hilbert modular forms, with examples relating to elliptic curves. *Pacific J. Math.* **219** (2005), no. 2, 333–364.

[14] M.–F. Vignéras, Arithmétique des algèbres de quaternions. Lecture Notes in Math., vol. **800**, Springer–Verlag, New York, 1981.

Department of mathematics and statistics, University of Calgary, 2500 University Drive N.W., Calgary, AB, Canada T2N 1N4, e-mail: dembele@math.ucalgary.ca