Explicit Computations of Hilbert Modular Forms on $\mathbb{Q}(\sqrt{5})$

Lassina Dembélé

CONTENTS

2000 AMS Subject Classification: Primary 11-xx; Secondary 11Gxx

Keywords: Hilbert modular forms, automorphic forms, Brandt matrices

This article presents an algorithm to compute Hilbert modular forms on the quadratic field $\mathbb{Q}(\sqrt{5})$. It also provides a list of all modular abelian varieties defined over $\mathbb{Q}(\sqrt{5})$ with prime level of norm less than 100 (up to $\mathbb{Q}$-isogeny).

1. INTRODUCTION

In this paper, we present an algorithm that allows one to compute Hilbert modular forms of parallel weight 2 and level $\mathfrak{c}$ on $\mathbf{GL}_2(F)$, where $F = \mathbb{Q}(\sqrt{5})$ is the real quadratic field of smallest discriminant. Though our calculations have mainly focused on forms of parallel weight 2, we have included some examples of forms of weight (2, 4) in order to show that this algorithm can easily be generalized to compute forms of arbitrary weights. Our presentation also indicates that there should be no major problem in generalizing our algorithm to compute forms of arbitrary weight and level over any totally real field of narrow class number 1. However, we have concentrated on the simplest case of forms of parallel weight 2, the main reason being that, in this case, one knows where to look for some of the corresponding geometric objects (such as elliptic curves or hypergeometric abelian varieties studied in [Darmon 00] in connection with the equation $x^n + y^n = z^5$), at least conjecturally.

Our method of computation draws on the Jacquet-Langlands correspondence like others (see, for example, [Pizer 80, Consani and Scholten 01, Socrates and Whitehouse 05]). To briefly explain it, let $\mathbf{f}$ be a normalized eigenform of parallel weight 2 and level $\mathfrak{c}$ (see [van der Geer 88, Chapter I, Section 6] and [Shimura 78, Sections 1 and 2] for the precise definitions; see also Sections 2 and 3 in this paper for further definitions) and let B be the Hamilton quaternion algebra on F. Then, B has class number 1. We consider its maximal order R consisting of the icosians; we fix an Eichler order $\mathrm{R}_{\mathfrak{c}}$ of level $\mathfrak{c}$ in R. By the Jacquet-Langlands correspondence, there

1058-6458/2005 $ 0.50 per page

is a eigenform on $B^\times\backslash B_{\mathbb{A}}^\times/R_{\mathfrak{c},\mathbb{A}}^\times$, which shares the same eigenvalues as $\mathbf{f}$ (here, for any F-algebra R, we denote its adelization by $R_{\mathbb{A}}$). So, it is enough to compute the latter space. However, this computation requires an explicit description of the double coset space $B^\times\backslash B_{\mathbb{A}}^\times/R_{\mathfrak{c},\mathbb{A}}^\times$. The most natural approach would be to view $B^\times\backslash B_{\mathbb{A}}^\times/R_{\mathfrak{c},\mathbb{A}}^\times$ as parameterizing (right) ideal classes of $R_{\mathfrak{c}}$ and find representatives for those classes. This is what is done in Pizer's algorithm in [Pizer 80], which is the most used one when it comes to computing forms on fields bigger than $\mathbb{Q}$ (see, for example, [Consani and Scholten 01, Socrates and Whitehouse 05]). Unfortunately, this has the drawback that, from the start, the algorithm depends on the choice of the Eichler order $R_{\mathfrak{c}}$, which itself depends on the level $\mathfrak{c}$. Therefore, it is very slow, since one has to start all over again every time that the level changes.

By observing that there is a natural bijection between $B^\times\backslash B_{\mathbb{A}}^\times/R_{\mathfrak{c},\mathbb{A}}^\times$ and $R^\times\backslash\hat{R}^\times/R_{\mathfrak{c},\mathbb{A}}^\times$, we are able to give a much nicer description of this double coset space that is independent of the explicit knowledge of an Eichler order $R_{\mathfrak{c}}$. One then gets a description of the Hecke action in terms of invariants of the maximal order R (or equivalently of B). We can then precompute those invariants and store them. This gives an algorithm that is more efficient, especially for the systematic computation of Hilbert modular forms.

Section 2 recalls preliminary results about automorphic forms on definite quaternion algebras together with the Jacquet-Langlands correspondence. In Section 3, we describe our algorithm. By direct investigations, we obtain a few of the elliptic curves corresponding to some of the forms we have computed. Their modularity is studied in Section 4.

2. AUTOMORPHIC FORMS ON DEFINITE QUATERNION ALGEBRAS AND THE JACQUET-LANGLANDS CORRESPONDENCE

We fix a totally real number field F of degree g. We assume that the narrow class number of F is 1. We let I be the set of all real embeddings of F and, for each $\tau \in I$, we denote the corresponding embedding by $a \mapsto a^\tau$. Also, we let $\mathcal{O}_F$ be the ring of integers of F, $\mathbb{A}$ its adèle ring, and $\mathbb{A}_f$ the ring of finite adèles. We fix an integral ideal $\mathfrak{c}$ of F. We let B be a totally definite quaternion algebra of center F. We fix a maximal order R in B. We fix a Galois extension K of F contained in $\mathbb{C}$, which splits B. We also fix an isomorphism $B \otimes_F K \cong M_2(K)^I$ and let $j : B^\times \hookrightarrow \mathbf{GL}_2(\mathbb{C})^I$ be the resulting embedding. We assume that $(\mathfrak{c}, \mathrm{disc}(B)) = 1$. For any prime $\mathfrak{p} \nmid \mathrm{disc}(B)$, we fix a local isomorphism $B_{\mathfrak{p}} \cong M_2(F_{\mathfrak{p}})$ such that $R_{\mathfrak{p}} \cong M_2(\mathcal{O}_{\mathfrak{p}})$. Then, we define $U = U_0(\mathfrak{c}) = \prod_{\mathfrak{p}} U_{\mathfrak{p}}$, with

$$U_{\mathfrak{p}} = \begin{cases} \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}}), & \mathfrak{p} \nmid \mathrm{disc}(B)\mathfrak{c}, \\ \left\{ \begin{pmatrix} a & b \\ \pi_{\mathfrak{p}}^e c & d \end{pmatrix} \in \mathrm{GL}_2(\mathcal{O}_{\mathfrak{p}}) \mid c \in \mathcal{O}_{\mathfrak{p}};\ e \geq 1 \right\}, & \mathfrak{p} \mid \mathfrak{c}, \\ R_{\mathfrak{p}}^\times, & \mathfrak{p} \mid \mathrm{disc}(B), \end{cases}$$

where we let $R_{\mathfrak{p}}$ be the (unique) maximal order in $B_{\mathfrak{p}}$ when $\mathfrak{p} \mid \mathrm{disc}(B)$. We then let $R_{\mathfrak{c}}$ be an Eichler order of level $\mathfrak{c}$ contained in R such that $\hat{R}_{\mathfrak{c}}^\times = U$, where $\hat{R}_{\mathfrak{c}} = R_{\mathfrak{c}} \otimes \hat{\mathcal{O}}_F$.

Fix a vector $\underline{k} \in \mathbb{Z}^I$ such that $k_\tau \geq 2$ for all τ, with all the components having the same parity. Set $\underline{t} = (1, \ldots, 1)$ and $\underline{m} = \underline{k} - 2\underline{t}$, then choose $\underline{v} \in \mathbb{Z}^I$ such that each $v_\tau \geq 0$, $v_\tau = 0$ for some τ and $\underline{m} + 2\underline{v} = \mu\underline{t}$ for some nonnegative $\mu \in \mathbb{Z}$.

For every nonnegative integer $a, b \in \mathbb{Z}$, we let $\mathbf{S}_{a,b}(\mathbb{C})$ denote the right $M_2(\mathbb{C})$-module $\mathbf{Sym}^a(\mathbb{C}^2)$ (the ath symmetric power of the standard right $M_2(\mathbb{C})$-module $\mathbb{C}^2$) with the $M_2(\mathbb{C})$-action

$$x \cdot m := (\det m)^b x \mathrm{Sym}^a(m).$$

Then, we define

$$L_{\underline{k}} = \bigotimes_{\tau \in I} \mathbf{S}_{m_\tau, v_\tau}(\mathbb{C}).$$

We let $G = \mathrm{Res}_{F/\mathbb{Q}}(B^\times)$ be the algebraic group obtained by restriction of scalars à la Weil. Via the obvious extension of the embedding j, $G(\mathbb{R})$ acts on $L_{\underline{k}}$. On the complex space of functions $f : G(\mathbb{Q})\backslash G(\mathbb{A}) \to L_{\underline{k}}$, we define an action of $G(\mathbb{A})$ by

$$(f\|_{\underline{k}}u)(g) := f(gu)u_\infty^{-1}, \quad g, u \in G(\mathbb{A}).$$

Similarly, on the space of functions $f : G(\mathbb{A}_f)/\hat{R}_{\mathfrak{c}}^\times \to L_{\underline{k}}$, we define an action of $G(\mathbb{Q})$ by

$$(f\|_{\underline{k}}\gamma)(g) := f(\gamma g)\gamma, \quad g \in G(\mathbb{A}_f),\ \gamma \in G(\mathbb{Q}).$$

The following definition is from Hida (see [Taylor 88, Section 1]).

Definition 2.1. The space of *automorphic forms* of *level* $\mathfrak{c}$ and *weight* $\underline{k}$ on B is

$$S_{\underline{k}}^{B}(\mathfrak{c}) := \left\{ f : G(\mathbb{Q})\backslash G(\mathbb{A}) \to L_{\underline{k}} : \ f\|_{\underline{k}}u = f, \quad u \in G(\mathbb{R}) \times \hat{R}_{\mathfrak{c}}^\times \right\}.$$

Take $f \in S^{\mathrm{B}}_{\underline{k}}(\mathfrak{c})$ and let

$$\tilde{f}(g) = f(g)g_\infty^{-1}, \quad g \in G(\mathbb{A}).$$

We see, by the left $G(\mathbb{Q})$-invariance of f, that

$$\begin{aligned}\tilde{f}(\gamma g) &= f(\gamma g)(\gamma g)_\infty^{-1} = f(\gamma g)g_\infty^{-1}\gamma^{-1} \\ &= f(g)g_\infty^{-1}\gamma^{-1} = \tilde{f}(g)\gamma^{-1},\end{aligned}$$

for all $\gamma \in G(\mathbb{Q})$ and $g \in G(\mathbb{A})$; and by the $G(\mathbb{R}) \times \hat{\mathrm{R}}_{\mathfrak{c}}^\times$-equivariance, we see that

$$\begin{aligned}\tilde{f}(gu) &= f(gu)(gu)_\infty^{-1} = f(gu)u_\infty^{-1}g_\infty^{-1} = f(g)g_\infty^{-1} \\ &= \tilde{f}(g),\end{aligned}$$

for all $g \in G(\mathbb{A})$ and $u \in G(\mathbb{R}) \times \hat{\mathrm{R}}_{\mathfrak{c}}^\times$. So, we can equivalently define the space of automorphic forms as

$$S^{\mathrm{B}}_{\underline{k}}(\mathfrak{c}) = \left\{ f : G(\mathbb{A}_f)/\hat{\mathrm{R}}_{\mathfrak{c}}^\times \to L_{\underline{k}} \,:\, f\|_{\underline{k}}\gamma = f, \quad \gamma \in G(\mathbb{Q}) \right\}.$$

We will use both definitions with no distinction.

Definition 2.2. (Hecke operators.) Let $\mathfrak{p}$ be a prime ideal of F and $\pi_{\mathfrak{p}}$ a uniformizer of $\mathfrak{p}$. When $\mathfrak{p}\nmid \mathrm{disc}(\mathrm{B})$, we write the disjoint union

$$\hat{\mathrm{R}}_{\mathfrak{c}}^\times \begin{pmatrix} 1 & 0 \\ 0 & \pi_{\mathfrak{p}} \end{pmatrix} \hat{\mathrm{R}}_{\mathfrak{c}}^\times = \coprod u_i \hat{\mathrm{R}}_{\mathfrak{c}}^\times, \quad \text{with } u_i \in \hat{\mathrm{R}} = \mathrm{R} \otimes \hat{\mathcal{O}}_F,$$

and define the *Hecke operator* $T_{\mathfrak{p}}$ on $S^{\mathrm{B}}_{\underline{k}}(\mathfrak{c})$ by

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

If, further, $\mathfrak{p}\nmid\mathfrak{c}$, we define the *Hecke operator* $S_{\mathfrak{p}}$ by

$$f\|S_{\mathfrak{p}} = f\|_{\underline{k}} \begin{pmatrix} \pi_{\mathfrak{p}} & 0 \\ 0 & \pi_{\mathfrak{p}} \end{pmatrix}.$$

When $\mathfrak{p} \mid \mathrm{disc}(\mathrm{B})$, we define

$$f\|S_{\mathfrak{p}} = f\|_{\underline{k}} \varpi_{\mathfrak{p}},$$

where $\varpi_{\mathfrak{p}}$ is a prime in $\mathrm{R}_{\mathfrak{p}}$. We denote by $\mathbf{T}^{\mathrm{B}}_{\underline{k}}(\mathfrak{c})$ the (commutative) $\mathbb{Z}$-subalgebra of $\mathrm{End}(S^{\mathrm{B}}_{\underline{k}}(\mathfrak{c}))$ generated by the $T'_{\mathfrak{p}}s$ and $S'_{\mathfrak{p}}s$, $(\mathfrak{p},\, \mathfrak{c}) = 1$.

Let $\mathbf{f} \in S_{\underline{k}}(\mathfrak{c})$ be a cusp form, where $S_{\underline{k}}(\mathfrak{c})$ is the space of cusp forms and $\pi_{\mathbf{f}}$ the cuspidal automorphic representation associated to $\mathbf{f}$. (For the definitions, we refer to [van der Geer 88, Chapter I, Section 6] and [Shimura 78, Sections 1 and 2]). By [Flath 79, Thereom 4], $\pi_{\mathbf{f}}$ factors into a restricted tensor product of unitary representations $\pi_{\mathbf{f}} = \otimes_v \pi_v$. We let $\mathcal{A}_{\underline{k}}(\mathfrak{c})$ (respectively, $\mathcal{A}^{\mathrm{B}}_{\underline{k}}(\mathfrak{c})$) be the set of all cuspidal representations that arise from forms in $S_{\underline{k}}(\mathfrak{c})$ (respectively, $S^{\mathrm{B}}_{\underline{k}}(\mathfrak{c})$).

Theorem 2.3. (Jacquet-Langlands.) *There is an injection*

$$\begin{aligned} JL: \mathcal{A}^{\mathrm{B}}_{\underline{k}}(\mathfrak{c}) &\to \mathcal{A}_{\underline{k}}(\mathfrak{c}) \\ \pi &\mapsto \pi' := JL(\pi). \end{aligned}$$

The image of JL consists of all representations π' such that π'_v is special or supercuspidal for all $v \mid \mathrm{disc}(\mathrm{B})$.

Proof: See [Jacquet and Langlands 70, Section 16] and [Gelbart 75, Chapter X]. □

As a consequence of Theorem 2.3, we see that for any eigenform in $S^{\mathrm{B}}_{\underline{k}}(\mathfrak{c})$, there is a form in $S_{\underline{k}}(\mathfrak{c})$ that has the same eigenvalues.

3. COMPUTING HILBERT MODULAR FORMS ON $\mathbb{Q}(\sqrt{5})$

For an eigenform f, we denote by $a_{\mathfrak{p},\,f}$ the eigenvalue of the Hecke operator $T_{\mathfrak{p}}$. We would like to write a computer program that returns enough eigenvalues $a_{\mathfrak{p},\,f}$ to determine all the normalized Hecke eigenforms f for a level $\mathfrak{c}$ of reasonable norm and parallel weight 2 or weight (2, 4) on $F = \mathbb{Q}(\sqrt{5})$. To this end, let us consider the (unique, up to isomorphism) totally definite quaternion algebra B over F that is unramified at all finite places. The algebra B can be identified with the standard Hamilton quaternion algebra, since 2 is inert in F:

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

By [Körner 87, Theorem 2] or [Socrates and Whitehouse 05, Theorem 6.2], the class number of B is 1. Every maximal order in B is then conjugate to the icosian ring

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

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 $\mathrm{R}^\times$ is the semidirect product of $\mathrm{R}_1^\times$ with $\mathbb{Z}$, where $\mathrm{R}_1^\times$ the subgroup of norm 1 elements is isomorphic to the binary icosahedral group of order 120 (see [Conway and Sloane 93, Chapter 8, Section 2.1]). Since B ramifies only at the two infinite places, by Theorem 2.3,

$$\mathcal{A}_{\underline{k}}^{\mathrm{B}}(\mathfrak{c}) = \mathcal{A}_{\underline{k}}(\mathfrak{c}).$$

Therefore, the computation of $S_{\underline{k}}(\mathfrak{c})$ amounts to the one of $S_{\underline{k}}^{\mathrm{B}}(\mathfrak{c})$.

Now turning to the explicit computation of $S_{\underline{k}}^{\mathrm{B}}(\mathfrak{c})$, we first recall that $\mathrm{B}^\times\backslash\hat{\mathrm{B}}^\times/\hat{\mathrm{R}}^\times$ parameterizes the set of right ideal classes of R. Thus, since B has class number 1,

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

Hence, we have the following bijections:

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

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

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

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

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

Now, let us define

$$S_{\underline{k}}^{\mathrm{R}}(\mathfrak{c}) = \Big\{f : \mathrm{R}^\times\backslash G(\mathbb{R}) \times \hat{\mathrm{R}}^\times \to L_{\underline{k}} : \ f\|_{\underline{k}}u = f, \ u \in G(\mathbb{R}) \times \hat{\mathrm{R}}_{\mathfrak{c}}^\times\Big\}.$$

As in Definition 2.1, we can equivalently define $S_{\underline{k}}^{\mathrm{R}}(\mathfrak{c})$ by

$$S_{\underline{k}}^{\mathrm{R}}(\mathfrak{c}) = \left\{f : \mathbf{P}^1(\mathcal{O}_F/\mathfrak{c}) \to L_{\underline{k}} : \ f\|_{\underline{k}}\gamma = f, \ \gamma \in \mathrm{R}^\times\right\},$$

where $f\|_{\underline{k}}\gamma(x) := f(\gamma x)\gamma$; and again, we will not make any distinction between the two definitions.

We will now define a Hecke action on the space $S_{\underline{k}}^{\mathrm{R}}(\mathfrak{c})$. To this end, take $u \in \hat{\mathrm{R}}$, $u \neq 0$, and write the finite disjoint union

$$\hat{\mathrm{R}}_{\mathfrak{c}}^\times u\hat{\mathrm{R}}_{\mathfrak{c}}^\times = \coprod_i u_i\hat{\mathrm{R}}_{\mathfrak{c}}^\times, \quad u_i \in \hat{\mathrm{R}}.$$

Take $f \in S_{\underline{k}}^{\mathrm{R}}(\mathfrak{c})$ and for each $x \in G(\mathbb{R}) \times \hat{\mathrm{R}}^\times$, let

$$f\|_{\underline{k}}[\hat{\mathrm{R}}_{\mathfrak{c}}^\times u\hat{\mathrm{R}}_{\mathfrak{c}}^\times](x) := \sum_{u_i} f\|_{\underline{k}}u_i(x),$$

where, for any $u' \in \hat{\mathrm{B}}^\times$, we choose $\gamma_{u'} \in \mathrm{B}^\times$ and $x_{u'} \in \hat{\mathrm{R}}^\times$ such that $xu' = \gamma_{u'}x_{u'}$, and set

$$f\|_{\underline{k}}u'(x) := f(x_{u'}).$$

It is not hard to verify that $f\|_{\underline{k}}u'$ is well defined and that $f\|_{\underline{k}}[\hat{\mathrm{R}}_{\mathfrak{c}}^\times u\hat{\mathrm{R}}_{\mathfrak{c}}^\times] \in S_{\underline{k}}^{\mathrm{R}}(\mathfrak{c})$. We thus obtain a linear map

$$[\hat{\mathrm{R}}_{\mathfrak{c}}^\times u\hat{\mathrm{R}}_{\mathfrak{c}}^\times] : S_{\underline{k}}^{\mathrm{R}}(\mathfrak{c}) \to S_{\underline{k}}^{\mathrm{R}}(\mathfrak{c}),$$

which we call the Hecke operator $[\hat{\mathrm{R}}_{\mathfrak{c}}^\times u\hat{\mathrm{R}}_{\mathfrak{c}}^\times]$. We can now state the following proposition.

Proposition 3.1. *The map*

$$\begin{aligned} S_{\underline{k}}^{\mathrm{B}}(\mathfrak{c}) &\to S_{\underline{k}}^{\mathrm{R}}(\mathfrak{c}),\\ f &\mapsto \tilde{f},\end{aligned}$$

where $\tilde{f}$ is the restriction of f to $\hat{\mathrm{R}}^\times/\hat{\mathrm{R}}_{\mathfrak{c}}^\times$, is an isomorphism of Hecke modules.

Proof: Since every element in $S_{\underline{k}}^{\mathrm{B}}(\mathfrak{c})$ is completely determined by its values on a complete set of representatives of the double coset space $\mathrm{B}^\times\backslash\hat{\mathrm{B}}^\times/\hat{\mathrm{R}}_{\mathfrak{c}}^\times$, and we have a bijection $\mathrm{B}^\times\backslash\hat{\mathrm{B}}^\times/\hat{\mathrm{R}}_{\mathfrak{c}}^\times \cong \mathrm{R}^\times\backslash\mathbf{P}^1(\mathcal{O}_F/\mathfrak{c})$, we see that the map $f \mapsto \tilde{f}$ is an isomorphism of complex spaces. So, we only have to show that the Hecke action is compatible with this isomorphism. However, for all $x \in \hat{\mathrm{R}}^\times$, we have by definition,

$$\begin{aligned}\widetilde{f\|_{\underline{k}}[\hat{\mathrm{R}}_{\mathfrak{c}}^\times u\hat{\mathrm{R}}_{\mathfrak{c}}^\times]}(x) &= \sum_{u_i} f\|_{\underline{k}}u_i(x) = \sum_{u_i} f(xu_i)\\ &= \sum_{xu_i=\gamma_ix_i} f(x_i) = \sum_{xu_i=\gamma_ix_i}\tilde{f}(x_i)\\ &= \sum_{u_i}\tilde{f}\|_{\underline{k}}u_i(x) = \tilde{f}\|_{\underline{k}}[\hat{\mathrm{R}}_{\mathfrak{c}}^\times u\hat{\mathrm{R}}_{\mathfrak{c}}^\times](x).\end{aligned}$$

This completes the proof. □

Let $\mathfrak{p}$ be a prime of F and $\pi_{\mathfrak{p}} \in \mathcal{O}_F$, a totally positive generator of $\mathfrak{p}$ (such a choice is possible, since $F = \mathbb{Q}(\sqrt{5})$ has narrow class number 1). Let

$$\mathbf{\Theta}(\mathfrak{p}) := \{u \in \mathrm{R} \text{ such that } \mathbf{N}(u) = \pi_{\mathfrak{p}}\}/\mathrm{R}^\times,$$

where we let $\mathrm{R}^\times$ act by multiplication on the left. Then, the action of Hecke in terms of global elements is given by

$$f\|_{\underline{k}}T_{\mathfrak{p}} = \sum_{u\in\mathbf{\Theta}(\mathfrak{p})} f\|_{\underline{k}}u.$$

When acting on elements in $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{c})$, one must restrict the summation to the u whose action is nondegenerate.

The best analogy for Proposition 3.1 when $\mathrm{B} = M_2(F)$ is the passage from the adelic definition of Hilbert modular forms to tuples of classical Hilbert modular forms (see, for example, [Shimura 78, Section 1]). By further exploiting this analogy, there should be no major difficulty in generalizing our algorithm to totally definite quaternion algebras with class number greater than 1. The main advantage of this approach, from a computational point of view, is that it does not require an explicit knowledge of the Eichler order $\mathrm{R}_\mathfrak{c}$ as in [Pizer 80]. This dramatically cuts down the amount of computation needed for each level. This will become clearer after we give our definition of the Brandt matrices.

Definition 3.2. (Brandt matrices.) Now, let $S = \{x_1, \ldots, x_s\}$ be a fundamental domain for the action of $\mathrm{R}^\times$ on $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{c})$ and, for each $i = 1, \ldots, s$, let Γ_i be the stabilizer of x_i in $\mathrm{R}_1^\times/\{\pm 1\}$. Since any element $f \in S_{\underline{k}}^{\mathrm{R}}(\mathfrak{c})$ is completely determined by its values on S, we have the following standard isomorphism of complex spaces:

$$\begin{aligned} S_{\underline{k}}^{\mathrm{R}}(\mathfrak{c}) &\to \bigoplus_{i=1}^{s} L_{\underline{k}}^{\Gamma_i}, \\ f &\mapsto (f(x_i))_{1\le i\le s}, \end{aligned}$$

where $L_{\underline{k}}^{\Gamma_i}$ is the subspace of Γ_i-invariants.
For each $x, y \in \mathbf{P}^1(\mathcal{O}_F/\mathfrak{c})$, let

$$\mathbf{\Theta}(x, y, \mathfrak{p}) = \left\{u \in \mathbf{\Theta}(\mathfrak{p}) : ux = \gamma_u y, \text{ for some } \gamma_u \in \mathrm{R}^\times\right\}.$$

Then, we have

$$\begin{aligned} (f\|T_\mathfrak{p})(x_i) &= \sum_{u\in\mathbf{\Theta}(\mathfrak{p})} (f\|_{\underline{k}} u)(x_i) = \sum_{u\in\mathbf{\Theta}(\mathfrak{p})} f(ux_i)u \\ &= \sum_{j=1}^{s} \sum_{u\in\mathbf{\Theta}(x_i, x_j, \mathfrak{p})} f(ux_i)u \\ &= \sum_{j=1}^{s} \sum_{u\in\mathbf{\Theta}(x_i, x_j, \mathfrak{p})} f(\gamma_u x_j)u \\ &= \sum_{j=1}^{s} f(x_j) \left(\sum_{u\in\mathbf{\Theta}(x_i, x_j, \mathfrak{p})} \gamma_u^{-1} u \right). \end{aligned}$$

So, we can define the *Brandt matrix* $\mathcal{B}_\mathfrak{p} = (b_{ij})$ of the operator $T_\mathfrak{p}$, with $b_{ij} \in \mathrm{Hom}(L_{\underline{k}}^{\Gamma_i}, L_{\underline{k}}^{\Gamma_j})$, by

$$\begin{aligned} b_{ji} : L_{\underline{k}}^{\Gamma_j} &\to L_{\underline{k}}^{\Gamma_i}, \\ v &\mapsto v \cdot \left(\sum_{u\in\mathbf{\Theta}(x_i, x_j, \mathfrak{p})} \gamma_u^{-1} u \right). \end{aligned}$$

It is not hard to verify that these matrices do not depend on the choice of the fundamental domain S.

Remark 3.3. Our definition of the Brandt matrices differs from the standard one in that it only uses invariants of the quaternion algebra B, and no explicit knowledge of representatives of ideal classes of an Eichler order is required (compare with [Pizer 80, Khuri-Makdisi 01]).

3.1 Algorithm and Implementation

Generating the icosian group. We do this by finding all 4-tuples $(x_1, \ldots, x_4) \in \mathbb{Z}[\omega]^4$ such that the quaternion $q = x_1e_1 + x_2e_2 + x_3e_3 + x_4e_4$ has reduced norm 1. We could have used a set of generators for the icosian group and their relations (see [Conway and Sloane 93, Chapter 8, Section 2.1]) to generate this group instead.

Finding a fundamental domain. We first find a set of representatives of the space $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{c})$. We have chosen to work with the product

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

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

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

Let the group $\mathrm{R}_1^\times/\{\pm 1\}$ act on the projective space $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{p}^{e_\mathfrak{p}})$ via the local isomorphism $\mathrm{R}_\mathfrak{p} = \mathrm{M}_2(\mathcal{O}_{F,\mathfrak{p}})$, which reduces to

$$\mathrm{R} \otimes (\mathcal{O}_F/\mathfrak{p}^{e_\mathfrak{p}}) = \mathrm{M}_2(\mathcal{O}_F/\mathfrak{p}^{e_\mathfrak{p}}).$$

Note that by Hensel's lemma, we only need to find the reduced isomorphism. This amounts to finding a set of generators for $\mathrm{M}_2(\mathcal{O}_F/\mathfrak{p}^{e_\mathfrak{p}})$ that satisfies the appropriate relations corresponding to the basis we have chosen for R. By putting these local actions together, we get the action of $\mathrm{R}_1^\times/\{\pm 1\}$ on $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{c})$. This allows us to find a fundamental domain.

Generating the Hecke operators. Let $\mathfrak{p}$ be a prime in $F = \mathbb{Q}(\sqrt{5})$ and $\pi_\mathfrak{p}$ a totally positive generator at $\mathfrak{p}$. To compute $T_\mathfrak{p}$, we need to find representatives for $\mathbf{\Theta}(\mathfrak{p})$. 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 quadratic form, which gives the norm map of B. We find all such elements up to equivalence by a unit. This part of the algorithm is identical to the one in [Pizer 80], since F is Euclidean. We

$\mathfrak{p}$	2	$\sqrt{5}$	3	$(4-\omega)$	$(4+\omega)$	$(5-\omega)$
$a_{\mathfrak{p}}(f)$	$4\omega-12$	-10ω	$12\omega-6$	$30\omega+2$	$-88\omega-16$	$-30\omega+70$

TABLE 1.

$\mathfrak{p}$	2	$\sqrt{5}$	3	$(3+\omega)$	$(4-\omega)$
$a_{\mathfrak{p}}(f_1)$	-14	$-\omega-17$	$24\omega-21$	$14\omega-23$	$-53\omega+28$
$a_{\mathfrak{p}}(f_2)$	4ω	$-4\omega+2$	$-12\omega+30$	$-12\omega+4$	$16\omega+4$
$a_{\mathfrak{p}}(f_3)$	$-4\omega+6$	$3\omega+11$	$12\omega-45$	$30\omega+1$	$-21\omega-30$

TABLE 2.

refer to [Pizer 80, Section 6] and [Consani and Scholten 01, Section 7] for more details.

The implementation of the algorithm is as follows:

1. Compute and store, once and for all, the icosian group and a collection of $\mathbf{\Theta}(\mathfrak{p})$ of global elements depending on a chosen bound on $\mathbf{N}(\mathfrak{p})$. In our computations, we chose that bound to be 100, and this was enough to discriminate between all forms of level of norm up to 1000.

2. For each level $\mathfrak{c}$, compute $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{c})$.

3. Compute the local factors of the isomorphism $\mathrm{R}\otimes(\mathcal{O}_F/\mathfrak{c})\cong \mathrm{M}_2(\mathcal{O}_F/\mathfrak{c})$ at primes $\mathfrak{p}\mid\mathfrak{c}$.

4. Compute the orbits of the action of the icosian group on $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{c})$, together with a fundamental domain, and create look up (or hashing) tables for these orbits (the latter is only necessary when the dimension of the space of cusp forms is big). For forms of non-parallel weight 2 we need the following: for each element, we store an icosian which sends it to the unique element of the fundamental domain which belongs to the same orbit.

5. For forms of non-parallel weight 2, compute the stabilizer of each element in the fundamental domain and the corresponding invariant space.

6. Compute the Brandt matrices $\mathcal{B}_{\mathfrak{p}}$.

Example 3.4. $\mathfrak{c}=(5+2\omega)$, so that $\mathbf{N}(\mathfrak{c})=31$. 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 $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{c})$ is $S=\{(1:0),(1:10)\}$. This means that $\dim S_{\underline{k}}(\mathfrak{c})=2$, and the space $S_{\underline{k}}(\mathfrak{c})$ is generated by a Eisenstein series and a new form that corresponds to a modular elliptic curve of conductor $(5+2\omega)$ (see Section 4). Here is the list of the first few Brandt matrices:

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

and $$\mathcal{B}_3=\begin{pmatrix}7&3\\5&5\end{pmatrix}.$$

Example 3.5. $\mathfrak{c}=(3+\omega)$, $\underline{k}=(2,4)$; here $\mathbf{N}(\mathfrak{c})=11$. For our computations, $\underline{m}=(0,2)$, $\underline{v}=(1,0)$,

$$L_{\underline{k}}=\mathbf{S}_{0,1}(\mathbb{C})\otimes\mathbf{S}_{2,0}(\mathbb{C}),$$

and j is the standard embedding of the Hamilton quaternion algebra over the reals into $\mathrm{GL}_2(\mathbb{C})$. The representation $L_{\underline{k}}$ has dimension 3. Here again, this is the smallest norm for which there is a Hilbert modular cusp form of weight (2, 4). A fundamental domain for the action of the icosian group on $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{c})$ is $S=\{(1:0)\}$. Its stabilizer Γ_1 has cardinality 5, and we compute that $S_{\underline{k}}(\mathfrak{c})=L_{\underline{k}}^{\Gamma_1}$ has dimension 1. The first few coefficients of the corresponding form ($\omega=(1+\sqrt{5})/2$) are given in Table 1.

Example 3.6. $\mathfrak{c}=(7+2\omega)$, $\underline{k}=(2,4)$; here $\mathbf{N}(\mathfrak{c})=59$. A fundamental domain for the action of the icosian group on $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{c})$ is $S=\{(1:0)\}$, and its stabilizer Γ_1 is trivial. So, $S_{\underline{k}}(\mathfrak{c})=L_{\underline{k}}^{\Gamma_1}$ is three-dimensional. The first few eigenvalues of these forms ($\omega=(1+\sqrt{5})/2$) are given in Table 2.

We remark in passing that, since $\mathrm{R}^\times\backslash\mathbf{P}^1(\mathcal{O}_F/\mathfrak{c})$ consists of one element, the only cusp form of weight (2, 2) is the Eisenstein series. Therefore, there is no modular elliptic curve defined over $\mathbb{Q}(\sqrt{5})$ whose conductor has norm 59.

Example 3.7. $\mathfrak{c}=(30)$, $\underline{k}=(2,4)$; here $\mathbf{N}(\mathfrak{c})=900$. A fundamental domain S for the action of the icosian group on $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{c})$ contains 26 elements, with two of

$\mathbf{N}(\mathfrak{c})$		31	36	41	45	49	55	61	64	71	76		79	80	81
$\mathbf{N}(\mathfrak{p})$	$\mathfrak{p}$	$a_{\mathfrak{p},f}$	$a_{\mathfrak{p},f}$	$a_{\mathfrak{p},f}$	$a_{\mathfrak{p},f}$	$a_{\mathfrak{p},f}$	$a_{\mathfrak{p},f}$	$a_{\mathfrak{p},f}$	$a_{\mathfrak{p},f}$	$a_{\mathfrak{p},f}$	$a_{\mathfrak{p},f_1}$	$a_{\mathfrak{p},f_2}$	$a_{\mathfrak{p},f}$	$a_{\mathfrak{p},f}$	$a_{\mathfrak{p},f}$
4	2	-3	-1	-2	-3	0	-1	$2\omega_5-2$	0	-1	-1	1	1	0	-1
5	ω_5+2	-2	-4	-1	1	-4	-1	$-3\omega_5+1$	-2	0	1	-3	-2	-1	0
9	3	2	-1	-4	1	5	-2	$-\omega_5-2$	2	-2	-5	1	-2	-2	0
11	ω_5+3	-4	2	-2	-4	-3	-1	$4\omega_5-2$	-4	0	-3	3	-4	0	0
	$-\omega_5+4$	4	2	5	-4	-3	0	$-\omega_5$	-4	0	2	-6	0	0	0
19	ω_5+4	4	0	-1	4	0	8	$3\omega_5-6$	4	-4	-1	1	4	-4	-4
	$-\omega_5+5$	-4	0	6	4	0	-4	ω_5+1	4	2	5	-7	8	-4	-4
29	ω_5+5	-2	0	9	-2	5	-6	$-2\omega_5+6$	-2	-6	-10	-6	6	6	0
	$-\omega_5+6$	-2	0	2	-2	5	6	$-5\omega_5+1$	-2	6	5	3	-2	6	0
31	$2\omega_5+5$	-1	-8	4	0	2	8	$5\omega_5-1$	0	8	-3	5	-8	-4	8
	$-2\omega_5+7$	8	-8	-10	0	2	-4	$-2\omega_5+8$	0	2	7	5	0	-4	8
41	ω_5+6	-6	2	-1	10	2	-6	$-4\omega_5-6$	2	12	2	6	2	6	0
	$-\omega_5+7$	-6	2	0	10	2	6	$2\omega_5+4$	2	6	2	6	-2	6	0
49	7	2	10	-6	-14	-1	14	$-4\omega_5+2$	10	-4	0	-4	-2	-10	14
59	$2\omega_5+7$	12	-10	4	-4	-10	-12	$10\omega_5-6$	12	6	10	6	-4	12	0
	$-2\omega_5+9$	-4	-10	-3	-4	-10	0	$-7\omega_5+7$	12	-12	0	-12	4	12	0
61	$3\omega_5+7$	6	2	-8	-2	-8	-10	-1	-10	-10	12	8	14	2	2
	$-3\omega_5+10$	-2	2	6	-2	-8	2	0	-10	-4	-8	8	10	2	2
71	ω_5+8	-8	12	9	-8	-8	0	$4\omega_5-4$	8	-1	7	-9	-16	-12	0
	$-\omega_5+9$	0	12	-12	-8	-8	0	$-3\omega_5+5$	8	6	-8	0	12	-12	0
79	$3\omega_5+8$	16	0	-11	0	5	8	$4\omega_5+4$	-16	14	5	-1	8	8	-16
	$-3\omega_5+11$	0	0	-4	0	5	-4	$-2\omega_5-6$	-16	-4	15	-1	-1	8	-16
89	ω_5+9	10	10	-8	-6	0	-18	$-3\omega_5-8$	-6	18	-15	9	-14	-6	0
	$-\omega_5+10$	-6	10	-1	-6	0	6	$-2\omega_5+4$	-6	6	0	0	18	-6	0

TABLE 3. Modular forms.

them having a stabilizer with cardinality 2 and the rest of them having trivial stabilizers. The spaces of invariants of both elements with stabilizer of cardinality 2 are one-dimensional. As a result, $S_{\underline{k}}(\mathfrak{c})$ has dimension $24{\cdot}3+1+1 = 74$. We checked that the first few coefficients of one of the forms defined over $\mathbb{Q}(\sqrt{5})$ match the coefficients of the form computed by Consani and Scholten in [Consani and Scholten 01]. One advantage in favor of our algorithm is that the computations in [Consani and Scholten 01] required a careful study of an Eichler order of level 30 in the totally definite quaternion algebra over $\mathbb{Q}(\sqrt{5})$, which is ramified at both infinite places and at 2 and 3. In fact, a variant of our algorithm applied to the definite quaternion algebra they chose could have worked as well. This has the additional advantage of reducing the dimension of the space we need to compute.

3.2 Table 3

The first row of Table 3 contains the norms of the levels listed in increasing order from 31 to 100. The tables start at 31 because it is the smallest norm for which there is a Hilbert cusp form of parallel weight 2. The first and second columns contain, respectively, the norms $\mathbf{N}(\mathfrak{p})$ and the primes $\mathfrak{p}$ for which the eigenvalues $a_{\mathfrak{p},f}$ have been computed. For each level $\mathfrak{c}$, the corresponding rows contain all the normalized eigenforms (up to Galois conjugation). For quadratic fields, we use the notation

$$\omega_D = \begin{cases} \sqrt{D}, & \text{if } D \neq 1 \mod 4, \\ \frac{1+\sqrt{D}}{2}, & \text{if } D = 1 \mod 4. \end{cases}$$

The listing of the levels is done up to Galois conjugation. For more forms, see [Dembélé 02].

4. MOTIVES

Using a Pari-GP search, we made a list of all modular elliptic curves of prime conductor of norm less than 100 (see Table 4). We would like to thank N. Elkies for his valuable help in implementing this search. We have only listed one curve for each prime as one gets the other curve by Galois conjugation. For each curve $E/\mathbb{Q}(\sqrt{5})$ of conductor $\mathfrak{c}$, we have checked that all the $a_{\mathfrak{p}}(E)$ match up with the Fourier coefficients of a modular form of level $\mathfrak{c}$

$\mathbf{N}(\mathfrak{c})$		89	95	99	100	
$\mathbf{N}(\mathfrak{p})$	$\mathfrak{p}$	$a_{\mathfrak{p},f}$	$a_{\mathfrak{p},f}$	$a_{\mathfrak{p},f}$	$a_{\mathfrak{p},f_1}$	$a_{\mathfrak{p},f_2}$
4	2	-1	-1	1	-1	1
5	ω_5+2	0	1	-2	0	0
9	3	4	-2	1	5	-5
11	ω_5+3	0	0	1	-3	-3
	$-\omega_5+4$	-6	0	-4	-3	-3
19	ω_5+4	-4	1	4	-5	5
	$-\omega_5+5$	2	-4	-4	-5	5
29	ω_5+5	6	6	6	0	0
	$-\omega_5+6$	6	-6	-2	0	0
31	$2\omega_5+5$	-4	8	-8	2	2
	$-2\omega_5+7$	-4	-4	8	2	2
41	ω_5+6	0	-6	-6	-3	-3
	$-\omega_5+7$	6	-6	2	-3	-3
49	7	-4	2	2	10	-10
59	$2\omega_5+7$	12	12	12	0	0
	$-2\omega_5+9$	0	12	12	0	0
61	$3\omega_5+7$	14	14	-2	2	2
	$-3\omega_5+10$	-4	-10	-2	2	2
71	ω_5+8	0	0	8	12	12
	$-\omega_5+9$	12	12	-8	12	12
79	$3\omega_5+8$	2	-16	8	10	-10
	$-3\omega_5+11$	-16	8	16	10	-10
89	ω_5+9	-1	-6	2	-15	15
	$-\omega_5+10$	6	6	-14	-15	15

TABLE 3. (continued) Modular forms.

given in the table, where $a_{\mathfrak{p}}(E) = \mathbf{N}(\mathfrak{p})+1-\#E(\mathbb{F}_{\mathfrak{p}})$. We are able to show their modularity by combining Lemma 4.1 with results in [Wiles 95, Skinner and Wiles 99, Skinner and Wiles 01]. We are currently working on an algorithm based on a conjecture of Oda [Oda 82], which parallels the Eichler-Shimura construction for modular forms over $\mathbb{Q}$. We hope to be able to extend this list by including all elliptic curves and abelian surfaces corresponding to forms whose level have a reasonable norm. By the conjectures in [Darmon 00], those abelian surfaces with multiplication by $\mathbb{Q}(\sqrt{5})$ should be hypergeometric, and their modularity has some interesting consequences for the generalized Fermat equation $x^n + y^n = z^5$.

Let E be an elliptic curve defined over $F = \mathbb{Q}(\sqrt{5})$. For any prime $\ell \geq 3$, let

$$\rho_{E,\ell} : \operatorname{Gal}(\bar{F}/F) \to \operatorname{GL}_2(\mathbb{Q}_\ell)$$

be the ℓ-adic representation attached to E and

$$\bar{\rho}_{E,\ell} : \operatorname{Gal}(\bar{F}/F) \to \operatorname{GL}_2(\mathbb{F}_\ell)$$

its mod ℓ reduction. The proof of Serre [Serre 96, Proposition 1] carries over to give the following lemma.

Lemma 4.1. *The image of $\bar{\rho}_{E,3}$ is either $\operatorname{GL}_2(\mathbb{F}_3)$ or is contained in a Borel subgroup; the latter case happens if and only if E or a 3-isogenous curve E'/F to it has a 3-torsion point defined over F.*

Proof: Going through the proof of Proposition 1 in [Serre 96], one sees that the only thing we need to check is that there can not be a Galois extension K of $F = \mathbb{Q}(\sqrt{5})$ such that $\operatorname{Gal}(K/F) = D_4$ or a subgroup of index 2 in D_4 and K ramifies only at 3. We recall that $D_4/\mathbb{Z}_2 \cong (\mathbb{Z}/2\mathbb{Z})^2$. But, there can not be an abelian extension of F of degree 4 that is only ramified at 3. $\square$

We have the following result.

Proposition 4.2. *All the curves listed is Table 4 are modular, and each of them (up to Galois conjugation) corresponds to a modular form of prime conductor listed in Table 3.*

Proof: (a) We first consider the curve $E/\mathbb{Q}(\sqrt{5})$ whose conductor has norm 31. By an easy computation in Magma, we find that, for the reduction $\bar{E}$ of E modulo the prime $\mathfrak{p} = 3$, $\#\bar{E}(\mathbb{F}_9) = 8$. Therefore, the curve E cannot have an F-rational 3-torsion point, since $E(F)_{tors}$ embeds into $\bar{E}(\mathbb{F}_9)$. The same argument also shows that E cannot be 3-isogenous to any curve E'/F with an F-rational 3-torsion point. Therefore, by Lemma 4.1, the representation $\bar{\rho}_{E,3}$ is irreducible. It is also modular by [Serre 87, Langlands 80, Tunnell 81], since its image is $\operatorname{GL}_2(\mathbb{F}_3)$, which is solvable. The representation $\rho_{E,3}$ is ordinary, since E has good reduction at 3 and $a_3(E) = 3^2+1-8 = 2$ is not divisible by 3; and it is also absolutely irreducible by [Serre 97, Chapter IV]. Therefore, we can apply [Skinner and Wiles 01, Theorem 5.1] to obtain the modularity of E. Except for the curves of conductor of norm 71 and 89, the same argument yields the modularity of each of the curves listed in Table 4.

$\mathbf{N}(\mathfrak{c})$	a_1	a_2	a_3	a_4	a_6
31	1	$-1-\omega_5$	ω_5	0	0
41	0	$-\omega_5$	ω_5	0	0
49	0	ω_5	1	1	0
71	$1+\omega_5$	$-1+\omega_5$	1	0	0
79	$1+\omega_5$	$-1+\omega_5$	ω_5	0	0
89	ω_5	$-\omega_5$	1	-1	0

TABLE 4. Elliptic curves.

(b) Now, let $E/\mathbb{Q}(\sqrt{5})$ be one of the curves whose conductor has norm 71 or 89. An easy computation in Magma shows that $E(F)_{tors} \cong \mathbb{Z}/6\mathbb{Z}$ and that $a_3(E) = -2$ or $a_3(E) = 4$. Hence, E has good ordinary reduction at $\mathfrak{p} = 3$, with a reducible mod 3 representation $\bar{\rho}_{E,3}$. Therefore, there exist two *distinct* characters $\chi, \chi' : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt{5})) \to \mathbb{F}_3^\times$ such that $\bar{\rho}_{E,3}^{ss} = \chi \oplus \chi'$, with χ' unramified at 3 and $\det \bar{\rho}_{E,3} = \chi\chi' = \epsilon_3$, where ϵ_3 is the mod 3 cyclotomic character. The splitting field of χ/χ' is $\mathbb{Q}(\sqrt{5}, \zeta_3)$, which is clearly abelian. All five conditions in [Skinner and Wiles 99, Theorem A] are clearly satisfied, which implies that E is modular. □

Remark 4.3. Knowing that $\bar{\rho}_{E,5}$ is irreducible (as one can easily see), it is tempting to try to combine an argument of switching the prime (à la Wiles) from 3 to 5, using [Shepherd-Barron and Taylor 97, Theorem 1.2] and [Skinner and Wiles 01, Theorem 5.1] to obtain the modularity of the curves whose conductors have norm 71 or 89. Unfortunately, both curves have supersingular reduction at $\sqrt{5}$ and *ordinariness* is essential in order to apply Theorem 5.1 in [Skinner and Wiles 01]. One can avoid all that heavy machinery by adapting the Faltings-Serre argument to obtain the modularity of all these curves, as is done in [Socrates and Whitehouse 05]. However, this requires computing a large number of $a_{\mathfrak{p}}(E)$.

Remark 4.4. Let $\mathfrak{p} = 7 + 3\omega_5$. Then, $\mathbf{N}(\mathfrak{p}) = 61$ is the smallest norm for which there is a form with coefficients in a field bigger than $\mathbb{Q}$. Let D be the (unique, up to isomorphism) quaternion algebra of center F that is ramified at only one of the real places of F and at $\mathfrak{p}$ and unramified everywhere else. We choose an Eichler order of reduced discriminant $\mathfrak{p}$ in D and let $X_0^{\mathrm{D}}(\mathfrak{p})$ be the corresponding Shimura curve. From the Jacquet-Langlands correspondence and the results in our tables, one deduces that $X_0^{\mathrm{D}}(\mathfrak{p})$ is a curve of genus 2. Therefore, its Jacobian $\mathrm{Jac}(X_0^{\mathrm{D}}(\mathfrak{p}))$ is a modular abelian surface with real multiplication by $\mathbb{Q}(\sqrt{5})$. This completes the list of all modular abelian varieties defined over $\mathbb{Q}(\sqrt{5})$ with prime conductor of norm less than 100 (up to $\mathbb{Q}$-isogeny).

ACKNOWLEDGMENTS

This paper is part of my thesis project that was written under the supervision of H. Darmon at McGill University. I would like to thank him for having suggested this problem to me and for the support he gave me through all my years at McGill. I will always be grateful to him for his patience and for his wonderful personality. I would like to thank N. Elkies who helped me implement the search of the elliptic curves listed in this article. I would also like to thank F. Diamond, the external examiner of my thesis. Some of his suggestions have found their way into this article. My final thanks go to the referees for their helpful comments. The computations in this paper were done using both Pari-GP and Magma.

REFERENCES

[Consani and Scholten 01] C. Consani and J. Scholten. "Arithmetic on a Quintic Threefold." *International Journal of Mathematics* 12:8 (2001), 943–972.

[Conway and Sloane 93] J. H. Conway and N. Sloane. *Sphere Packings, Lattices and Groups,* Second edition. New York: Springer Verlag, 1993.

[Darmon 00] H. Darmon. "Rigid Local Systems, Hilbert Modular Forms, and Fermat's Last Theorem." *Duke Math. J.* 102:3 (2000), 413–449.

[Dembélé 02] L. Dembélé. "Explicit Computations of Hilbert Modular Forms on $\mathbb{Q}(\sqrt{5})$." PhD diss., McGill University. Available from World Wide Web (www.math.mcgill .ca/~darmon), 2002.

[Flath 79] D. Flath. "Decomposition of Representations into Tensor Products." *Proc. Sympos. Pure Math., Part I* 33 (1979), 179–183.

[van der Geer 88] G. van der Geer. *Hilbert Modular Surfaces.* New York: Springer-Verlag, 1988.

[Gelbart 75] S. S. Gelbart. *Automorphic Forms on Adele Groups,* Annals of Mathematics Studies, 83. Princeton, NJ: Princeton Univ. Press, 1975.

[Jacquet and Langlands 70] H. Jacquet and R. P. Langlands. *Automorphic Forms on GL(2),* Lecture Notes in Math., 114. Berlin: Springer-Verlag, 1970.

[Khuri-Makdisi 01] Kamal Khuri-Makdisi. "On the Curves Associated to Certain Rings of Automorphic Forms." *Canad. J. Math.* 53:1 (2001), 98–121.

[Körner 87] O. Körner. "Traces of Eichler-Brandt Matrices and Type Numbers of Quaternion Orders." *Proc. Indian. Acad. Sci.* 97 (1987), 187–199.

[Langlands 80] Robert P. Langlands. *Base Change for* GL(2), Annals of Mathematics Studies, 96. Princeton, NJ: Princeton University Press, and Tokyo: University of Tokyo Press, 1980.

[Oda 82] Takayuki Oda. *Periods of Hilbert Modular Surfaces,* Progress in Mathematics, 19. Boston, MA: Birkhuser, 1982.

[Pizer 80] Arnold Pizer. "An Algorithm for Computing Modular Forms on $\Gamma_0(N)$." *J. Algebra* 64:2 (1980), 340–390.

[Serre 87] Jean-Pierre Serre. "Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$." *Duke Math. J.* 54:1 (1987), 179–230.

[Serre 96] Jean-Pierre Serre. "Travaux de Wiles (et Taylor, ...), I." Séminaire Bourbaki, Vol. 1994/95. *Astérisque* 237:803 (1996), 319–332.

[Serre 97] Jean-Pierre Serre. *Abelian l-Adic Representations and Elliptic Curves,* Research Notes in Mathematics, 7. Wellesley, MA: A K Peters, Ltd., 1997.

[Shepherd-Barron and Taylor 97] N. Shepherd-Barron and R. Taylor. "Mod 2 and Mod 5 Icosahedral Representations." *J.A.M.S.* 10 (1997) 283–298.

[Shimura 71] G. Shimura. *Introduction to the Arithmetic Theory of Automorphic Functions.* Princeton, NJ: Princeton Univ. Press 1971.

[Shimura 78] G. Shimura. "The Special Values of the Zeta Functions Associated to Hilbert Modular Forms." *Duke Math. J.* 45:3 (1978), 637–679.

[Skinner and Wiles 99] C. M. Skinner and A. J. Wiles. "Residually Reducible Representations and Modular Forms." *Inst. Hautes Études Sci. Publ. Math.* 89 (1999), 5–126.

[Skinner and Wiles 01] C. M. Skinner and A. J. Wiles. "Nearly Ordinary Deformations of Irreducible Residual Representations." *Ann. Fac. Sci. Toulouse Math.* 6:1 (2001), 185–215.

[Socrates and Whitehouse 05] J. T. Socrates and D. Whitehouse. "Unramified Hilbert Modular Forms with Examples Relating to Elliptic Curves." *Pacific Journal of Mathematics* 219:2 (2005), 333–364.

[Taylor 88] R. Taylor. "On Galois Representations Associated to Hilbert Modular Forms." *Invent. Math.* 98 (1988), 265–280.

[Tunnell 81] J. Tunnell. "Artin's Conjecture for Representations of Octahedral Type." *Bull. Amer. Math. Soc. (N.S.)* 5:2 (1981), 173–175.

[Wiles 95] A. Wiles. "Modular Elliptic Curves and Fermat's Last Theorem." *Annals of Maths.* 141 (1995), 443–551.

Lassina Dembélé, Department of Mathematics and Statistics, University of Calgary, 2500 University Drive N.W., Calgary, AB, T2N 1N4 Canada (dembele@math.ucalgary.ca)

Received November 18, 2003; accepted June 7, 2005.