

# Computing Hilbert modular forms over fields with nontrivial class group

Lassina Dembélé and Steve Donnelly

Institut für Experimentelle Mathematik, Ellernstrasse 29, 45326 Essen, Germany  
`lassina.dembele@uni-due.de`  
School of Mathematics and Statistics F07, University of Sydney NSW 2006, Sydney,  
Australia  
`donnelly@maths.usyd.edu.au`

**Abstract.** We exhibit an algorithm for the computation of Hilbert modular forms over an arbitrary totally real number field of even degree, extending results of the first author. We present some new instances of the conjectural Eichler-Shimura construction for totally real number fields over the fields  $\mathbb{Q}(\sqrt{10})$  and  $\mathbb{Q}(\sqrt{85})$  and their Hilbert class fields, and in particular some new examples of modular abelian varieties with everywhere good reduction over those fields.

## Introduction

Let  $F$  be a totally real number field of even degree. Let  $B$  be the quaternion algebra over  $F$  which is ramified at all infinite places and no finite places. The Jacquet-Langlands correspondence ([10, Chap. XVI] and [9]), establishes isomorphisms of Hecke modules between spaces of Hilbert modular forms over  $F$  and certain spaces of automorphic forms on  $B$ . The latter objects are combinatorial by nature and can be computed by using the theory of Brandt matrices. In [4] and [5], the first author presented an algorithm which adopts an alternative approach to the theory of Brandt matrices that is computationally more efficient than the classical one. Both papers considered only fields with narrow class number one.

In this paper we present a general algorithm that is practical for a large range of fields and levels. This opens the possibility of experimenting systematically, especially over fields with nontrivial class group. One technical difficulty arising from nontrivial class groups is that ideals in  $B$  are no longer free  $\mathcal{O}_F$ -modules. This is now handled smoothly in the package for quaternion algebras over number fields contained in the Magma computational algebra system [2] (version 2.14). Our computations rely heavily on this package, in which algorithms from [23] and [14] are implemented.

There are not many explicit examples in the literature of Hilbert modular forms in the nontrivial class group case. Okada [17] provides several examples of systems of Hecke eigenvalues of level 1 and parallel weight 2 on the quadratic fields  $\mathbb{Q}(\sqrt{257})$  and  $\mathbb{Q}(\sqrt{401})$ , computed using explicit trace formulae. One drawback with this method is that it computes the characteristic polynomials of the

Hecke operators rather than the matrices themselves, and it seems difficult to recover the eigenforms from this. Also, it would not be easy to use the trace formula as the basis of an algorithm for arbitrary totally real number fields, levels and weights.

In the last few years, there has been tremendous progress towards the Langlands correspondence for  $\mathbf{GL}_2/\mathbb{Q}$ , culminating in the recent proof of the Serre conjecture for mod  $p$  Galois representations by Khare and Wintenberger [13], and Kisin [12] et al, which in turn led to a proof of the Shimura-Taniyama-Weil conjecture for abelian varieties of  $\mathbf{GL}_2$ -type over  $\mathbb{Q}$ . We hope that our algorithm, which we implemented in Magma, will be helpful in gaining more insight as to the natural generalizations of those conjectures to the totally real case, as well as the Birch and Swinnerton-Dyer conjecture. In fact, such a project is currently under way in Dembélé, Diamond and Roberts [7] in which we use a mod  $\mathfrak{p}$  version of this algorithm to investigate the Serre conjecture for some totally real number fields. See also Schein [18] for another such application.

The paper is organized as follows. Section 1 contains the necessary theoretical background. In section 2 we state the general algorithm, and describe some improvements to its implementation. Section 3 provides some numerical data over the real quadratic fields  $\mathbb{Q}(\sqrt{10})$  and  $\mathbb{Q}(\sqrt{85})$  and their Hilbert class fields. We also revisit the results in [17]. In section 4 we use our data to give new examples of the Eichler-Shimura construction over totally real number fields.

**Acknowledgements.** This project was started when the first author was a PIMS postdoctoral fellow at the University of Calgary, and parts of it were written during his visit to the University of Sydney in August 2007. He would like to thank both PIMS and the University of Calgary for their financial support and the Department of Mathematics and Statistics of the University of Sydney for its hospitality. In particular, he would like to thank Anne and John Cannon for their invitation to visit the Magma group. He would also like to thank Clifton Cunningham for his constant support and encouragement in the early stage of the project. Finally, the authors would like to thank Fred Diamond, Noam Elkies and Haruzo Hida for helpful email exchanges.

## 1 Theoretical background

In this section, we give an explicit presentation of Hilbert modular forms as Hecke modules. By the Jacquet-Langlands correspondence, it is equivalent to give an explicit presentation of certain spaces of automorphic forms on a quaternion algebra  $B$ , which are in turn given in terms of automorphic forms on quaternion orders. A good reference for the material on Hilbert modular forms is [22]. For the theory of Brandt matrices, we refer to [8], and also to [5] for the adelic framework used here.

Let  $F$  be a totally real number field of even degree  $g$ . Let  $v_i$ ,  $i = 1, \dots, g$ , be all the real embeddings of  $F$ . For every  $a \in F$ , we let  $a_i = v_i(a)$  be the image of  $a$  under  $v_i$ . We let  $\mathcal{O}_F$  be the ring of integers of  $F$ , and fix an integral ideal  $\mathfrak{N}$  of  $F$ .

We let  $B$  be the quaternion algebra over  $F$  ramified at all infinite places and no finite places. We choose a maximal order  $R$  of  $B$ . Let  $K$  be a finite extension of  $F$  contained in  $\mathbb{C}$  which splits  $B$ . We choose an isomorphism  $B \otimes_F K \cong \mathbf{M}_2(K)^g$ , and let  $j : B^\times \hookrightarrow \mathbf{GL}_2(\mathbb{C})^g$  be the resulting embedding. For each prime  $\mathfrak{p}$  in  $\mathcal{O}_F$ , we choose a local isomorphism  $B_{\mathfrak{p}} \cong \mathbf{M}_2(F_{\mathfrak{p}})$  which sends  $R_{\mathfrak{p}}$  to  $\mathbf{M}_2(\mathcal{O}_{F, \mathfrak{p}})$ . Combining these local isomorphisms, one obtains an isomorphism  $\hat{B} \cong \mathbf{M}_2(\hat{F})$  under which  $\hat{R}$  goes to  $\mathbf{M}_2(\hat{\mathcal{O}}_F)$ , where  $\hat{F}$  and  $\hat{\mathcal{O}}_F$  are the finite adeles of  $F$  and  $\mathcal{O}_F$  respectively. We define the compact open subgroup  $U_0(\mathfrak{N})$  of  $\hat{R}^\times$  by

$$U_0(\mathfrak{N}) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{GL}_2(\hat{\mathcal{O}}_F) : c \equiv 0 \pmod{\mathfrak{N}} \right\}.$$

Let  $\text{Cl}(R)$  denote a complete set of representatives of all the right ideal classes of  $R$ ; it is in bijection with the double coset space  $B^\times \backslash \hat{B}^\times / \hat{R}^\times$ . Let  $S$  be a finite set of primes of  $\mathcal{O}_F$  that generate the narrow class group  $\text{Cl}^+(F)$  and such that  $\mathfrak{q}$  is coprime with  $\mathfrak{N}$  for any  $\mathfrak{q} \in S$ . Applying the strong approximation theorem, we choose the representatives  $\mathfrak{a} \in \text{Cl}(R)$  such that the primes dividing  $\text{nr}(\mathfrak{a})$  belong to  $S$ . For any  $\mathfrak{a} \in \text{Cl}(R)$ , we let  $R_{\mathfrak{a}}$  be the left (maximal) order of  $\mathfrak{a}$ . Then there are well-defined surjective reduction maps  $\hat{R}_{\mathfrak{a}}^\times \rightarrow \mathbf{GL}_2(\mathcal{O}_F/\mathfrak{N})$  that all differ by conjugation in  $\mathbf{GL}_2(\mathcal{O}_F/\mathfrak{N})$ . From this, we obtain a transitive action of each  $\hat{R}_{\mathfrak{a}}^\times$  on  $\mathbf{P}^1(\mathcal{O}_F/\mathfrak{N})$ .

Let  $\underline{k} \in \mathbb{Z}^g$  be a vector such that  $k_i \geq 2$  and  $k_i \equiv k_j \pmod{2}$  for all  $i, j = 1, \dots, g$ . Set  $\underline{t} = (1, \dots, 1)$  and  $\underline{m} = \underline{k} - 2\underline{t}$ , then choose  $\underline{n} \in \mathbb{Z}^g$  such that each  $n_i \geq 0$ ,  $n_i = 0$  for some  $i$ , and  $\underline{m} + 2\underline{n} = \mu \underline{t}$  for some  $\mu \in \mathbb{Z}_{\geq 0}$ . Let  $L_{\underline{k}}$  be the representation of  $\mathbf{GL}_2(\mathbb{C})^g$  given by

$$L_{\underline{k}} := \bigotimes_{i=1}^g \det^{n_i} \otimes \text{Sym}^{m_i}(\mathbb{C}^2).$$

We then obtain a representation of  $B^\times$  by composing with  $j : B^\times \hookrightarrow \mathbf{GL}_2(\mathbb{C})^g$ .

The space of automorphic forms of level  $\mathfrak{N}$  and weight  $\underline{k}$  on  $B$  is defined as

$$M_{\underline{k}}^B(\mathfrak{N}) := \left\{ f : \hat{B}^\times / U_0(\mathfrak{N}) \rightarrow L_{\underline{k}} : f|_{\underline{k}}\gamma = f \text{ for all } \gamma \in B^\times \right\},$$

where  $f|_{\underline{k}}\gamma(x) := f(\gamma x)\gamma$ .

By the Jacquet-Langlands correspondence [10, Chap. XVI], there is an isomorphism of Hecke modules between  $M_{\underline{k}}^B(\mathfrak{N})$  and  $M_{\underline{k}}(\mathfrak{N})$ , the space of Hilbert modular forms of weight  $\underline{k}$  and level  $\mathfrak{N}$  over  $F$ . On the other hand, we will now describe  $M_{\underline{k}}^B(\mathfrak{N})$  in terms of automorphic forms on maximal orders of  $B$ .

The space of automorphic forms of level  $\mathfrak{N}$  and weight  $\underline{k}$  on the order  $R_{\mathfrak{a}}$  is defined as

$$M_{\underline{k}}^{R_{\mathfrak{a}}}(\mathfrak{N}) := \left\{ f : \mathbf{P}^1(\mathcal{O}_F/\mathfrak{N}) \rightarrow L_{\underline{k}} : f|_{\underline{k}}\gamma = f \text{ for all } \gamma \in \Gamma_{\mathfrak{a}} \right\},$$

where  $\Gamma_{\mathfrak{a}} = R_{\mathfrak{a}}^{\times} / \mathcal{O}_F^{\times}$  is a finite arithmetic group. For each  $\mathfrak{a}, \mathfrak{b} \in \text{Cl}(R)$  and any prime  $\mathfrak{p}$  in  $\mathcal{O}_F$ , put

$$\Theta^{(S)}(\mathfrak{p}; \mathfrak{a}, \mathfrak{b}) := R_{\mathfrak{a}}^{\times} \setminus \left\{ u \in \mathfrak{a}\mathfrak{b}^{-1} : \frac{(\text{nr}(u))}{\text{nr}(\mathfrak{a})\text{nr}(\mathfrak{b})^{-1}} = \mathfrak{p} \right\},$$

where  $R_{\mathfrak{a}}^{\times}$  acts by multiplication on the left. We define the linear map

$$\begin{aligned} T_{\mathfrak{a}, \mathfrak{b}}(\mathfrak{p}) : M_{\underline{k}}^{R_{\mathfrak{b}}}(\mathfrak{N}) &\rightarrow M_{\underline{k}}^{R_{\mathfrak{a}}}(\mathfrak{N}) \\ f &\mapsto \sum_{u \in \Theta^{(S)}(\mathfrak{p}; \mathfrak{a}, \mathfrak{b})} f|_{\underline{k}} u. \end{aligned}$$

The following result, relating the spaces  $M_{\underline{k}}^B(\mathfrak{N})$  and  $M_{\underline{k}}^{R_{\mathfrak{a}}}(\mathfrak{N})$ , was proved by the first author in [5], without restriction on the class group.

**Proposition 1 ([5, Theorem 2]).** *There is an isomorphism of Hecke modules*

$$M_{\underline{k}}^B(\mathfrak{N}) \rightarrow \bigoplus_{\mathfrak{a} \in \text{Cl}(R)} M_{\underline{k}}^{R_{\mathfrak{a}}}(\mathfrak{N}),$$

where the action of the Hecke operator  $T(\mathfrak{p})$  on the right is given by the collection of linear maps  $(T_{\mathfrak{a}, \mathfrak{b}}(\mathfrak{p}))$  for all  $\mathfrak{a}, \mathfrak{b} \in \text{Cl}(R)$ .

**Remark 1.** Proposition 1 may also be deduced from [6, Theorem 1] as a special case.

We now describe the action of the class group  $\text{Cl}(F)$  on  $M_{\underline{k}}^B(\mathfrak{N})$ . Note that  $\text{Cl}(F)$  acts on the set  $\text{Cl}(R)$  via ideal multiplication, with the class  $[\mathfrak{m}] \in \text{Cl}(F)$  sending  $[\mathfrak{a}] \mapsto [\mathfrak{m}\mathfrak{a}]$ . We then let  $\text{Cl}(F)$  act on  $M_{\underline{k}}^B(\mathfrak{N})$  by permuting the direct summands: the class  $[\mathfrak{m}] \in \text{Cl}(F)$  sends an element  $(f_{\mathfrak{a}})_{\mathfrak{a}} \in \bigoplus M_{\underline{k}}^{R_{\mathfrak{a}}}(\mathfrak{N})$  to  $(f_{\mathfrak{m}\mathfrak{a}})_{\mathfrak{a}}$ .

For each character  $\chi$  of the abelian group  $\text{Cl}(F)$ , let  $M_{\underline{k}}^B(\mathfrak{N}, \chi)$  denote the  $\chi$ -equivariant subspace  $\{f \in M_{\underline{k}}^B(\mathfrak{N}) : \mathfrak{m} \cdot f = \chi(\mathfrak{m})f\}$ . One then has the decomposition

$$M_{\underline{k}}^B(\mathfrak{N}) = \bigoplus_{\chi} M_{\underline{k}}^B(\mathfrak{N}, \chi).$$

## 2 Algorithmic issues

Our algorithm for computing Brandt matrices using the adelic framework has already been discussed in the case of real quadratic fields in [4, sec. 2] and [5, sec. 6]. Here, we give an outline of the algorithm for any totally real number field  $F$  of even degree and any weight and level. We then discuss new optimisations to some of the key steps.

We keep the notation of section 1. Our goal is to compute the space  $M_{\underline{k}}^B(\mathfrak{N})$  as a Hecke module, meaning we determine its dimension, and matrices representing

the Hecke operators  $T(\mathfrak{p})$  for primes  $\mathfrak{p}$  with  $N\mathfrak{p} \leq b$ , for a given bound  $b$  (which must be chosen at the outset). When  $b$  is large enough, this data enables us to compute the Hecke constituents, thus the eigenforms. The precomputation stage is independent of the level and weight. Algorithms for steps (2), (3) and (4) of the precomputation are given in [23].

**Precomputation.** The input is a field  $F$  as above, and a bound  $b$ .

1. Find a set of prime ideals  $S$  not dividing  $\mathfrak{N}$  that generate  $\text{Cl}^+(F)$ .
2. Find a presentation of the quaternion algebra  $B/F$  ramified at precisely the infinite places, and compute a maximal order  $R$  of  $B$ .
3. Compute a complete set  $\text{Cl}(R)$  of representatives  $\mathfrak{a}$  for the right ideal classes of  $R$  such that the primes dividing  $\text{nr}(\mathfrak{a})$  belong to  $S$ .
4. For each representative  $\mathfrak{a} \in \text{Cl}(R)$ , compute its left order  $R_{\mathfrak{a}}$ , and compute the unit group  $\Gamma_{\mathfrak{a}} = R_{\mathfrak{a}}^{\times} / \mathcal{O}_F^{\times}$ .
5. Compute the sets  $\Theta^{(S)}(\mathfrak{p}; \mathfrak{a}, \mathfrak{b})$ , for all primes  $\mathfrak{p}$  with  $N\mathfrak{p} \leq b$  and all  $\mathfrak{a}, \mathfrak{b} \in \text{Cl}(R)$ . (See Section 2.1 for details.)

**Algorithm.** The input consists of  $F$  and  $b$  together with the precomputed data, and also  $\mathfrak{N}$  and  $\underline{k}$ . The output consists of a matrix  $T(\mathfrak{p})$  for each prime  $\mathfrak{p}$  with  $N\mathfrak{p} \leq b$  (and possibly additional primes), and also the Hecke constituents.

1. Compute splitting isomorphisms  $R_{\mathfrak{p}}^{\times} \cong \mathbf{GL}_2(\mathcal{O}_{F, \mathfrak{p}})$ , for each prime  $\mathfrak{p} \mid N$ .
2. For each  $\mathfrak{a} \in \text{Cl}(R)$ , compute  $M_{\underline{k}}^{R_{\mathfrak{a}}}(\mathfrak{N})$  as a module of coinvariants

$$M_{\underline{k}}^{R_{\mathfrak{a}}}(\mathfrak{N}) = K[\mathbf{P}^1(\mathcal{O}_F/\mathfrak{N})] \otimes L_{\underline{k}} / \langle x - \gamma x, \gamma \in \Gamma_{\mathfrak{a}} \rangle.$$

3. Combine the results of step (2), forming the direct sum

$$M_{\underline{k}}^B(\mathfrak{N}) = \bigoplus_{\mathfrak{a} \in \text{Cl}(R)} M_{\underline{k}}^{R_{\mathfrak{a}}}(\mathfrak{N}).$$

4. For each prime  $\mathfrak{p}$  with  $N\mathfrak{p} \leq b$ , compute the families of linear maps  $(T_{\mathfrak{a}, \mathfrak{b}}(\mathfrak{p}))$ . (These determine the Hecke operator  $T(\mathfrak{p})$  as a block matrix.)
5. Find a common basis of eigenvectors of  $M_{\underline{k}}^B(\mathfrak{N})$  for the  $T(\mathfrak{p})$ .
6. If Step (5) does not completely diagonalize  $M_{\underline{k}}^B(\mathfrak{N})$ , increase  $b$  and extend the precomputation, obtaining  $\Theta^{(S)}(\mathfrak{p}; \mathfrak{a}, \mathfrak{b})$  for  $N\mathfrak{p} \leq b$ . Then return to Step (4).

**Remark 2.** In practice, it is extremely rare that one resorts to Step (6) since very few Hecke operators  $T(\mathfrak{p})$  are required to diagonalize the space  $M_{\underline{k}}^B(\mathfrak{N})$ . In the cases we tested, which included levels with norm as large as 5000, we never needed more than 10 primes.

The steps in the main algorithm involve only local computations and linear algebra. The expensive steps in the process all occur in the precomputation; these involve lattice enumeration and are discussed below. For a given field  $F$ , if one wishes to compute forms of all levels up to some large bound, it is practical to simply take the primes in  $S$  to be larger than that bound, so the precomputation need only be done once.

## 2.1 Computing $\Theta^{(S)}(\mathfrak{p}; \mathfrak{a}, \mathfrak{b})$

**Lemma 2.** *The correspondence  $u \leftrightarrow u^{-1}\mathfrak{a}$  gives a bijection between  $\Theta^{(S)}(\mathfrak{p}; \mathfrak{a}, \mathfrak{b})$  and the set of fractional right  $R$ -ideals  $\mathfrak{c} \supset \mathfrak{b}$  such that  $\text{nr}(\mathfrak{b}) = \text{nr}(\mathfrak{c})\mathfrak{p}$  and  $\mathfrak{c} \cong \mathfrak{a}$  as right  $R$ -ideals.*

*Proof.* The fractional right  $R$ -ideals  $\mathfrak{c}$  isomorphic to  $\mathfrak{a}$  are the ideals  $u^{-1}\mathfrak{a}$  for  $u \in B^\times$ . Note that  $u^{-1}\mathfrak{a} = v^{-1}\mathfrak{a}$  if and only if  $v \in R_\mathfrak{a}^\times u$ . It is clear that  $u^{-1}\mathfrak{a}$  contains  $\mathfrak{b}$  if and only if  $u \in \mathfrak{a}\mathfrak{b}^{-1}$ , and that  $\text{nr}(\mathfrak{b}) = \text{nr}(u^{-1}\mathfrak{a})\mathfrak{p}$  if and only if  $\text{nr}(u)\mathcal{O}_F = \text{nr}(\mathfrak{a})\text{nr}(\mathfrak{b})^{-1}\mathfrak{p}$ .

**Algorithm.** This computes  $\Theta^{(S)}(\mathfrak{p}; \mathfrak{a}, \mathfrak{b})$  for all  $\mathfrak{a} \in \text{Cl}(R)$ , where  $\mathfrak{p}$  and  $\mathfrak{b}$  are fixed.

1. Compute the fractional right  $R$ -ideals  $\mathfrak{c} \supset \mathfrak{b}$  with  $\text{nr}(\mathfrak{b}) = \text{nr}(\mathfrak{c})\mathfrak{p}$ .
2. For each such  $\mathfrak{c}$ , compute the representative  $\mathfrak{a} \in \text{Cl}(R)$  and some  $u \in B$  such that  $\mathfrak{c} = u^{-1}\mathfrak{a}$ . Append  $u$  to  $\Theta^{(S)}(\mathfrak{p}; \mathfrak{a}, \mathfrak{b})$ .

**Remark 3.** In step (1), the number of ideals  $\mathfrak{c}$  obtained is  $N\mathfrak{p} + 1$ . Thus for each  $\mathfrak{p}$  and  $\mathfrak{b}$

$$\sum_{\mathfrak{a} \in \text{Cl}(R)} \#\Theta^{(S)}(\mathfrak{p}; \mathfrak{a}, \mathfrak{b}) = N\mathfrak{p} + 1,$$

however this fact is not used in the algorithm.

Step (1) is a local computation; the ideals are obtained by pulling back local ideals under a splitting homomorphism  $R_\mathfrak{p} \cong \mathbf{M}_2(F_\mathfrak{p})$ . Step (2) is the standard problem of isomorphism testing for right ideals; we discuss below an improvement to the standard algorithm for this, such that the complexity of each isomorphism test will not depend on  $\mathfrak{p}$ .

## 2.2 Lattice-based algorithms for definite quaternion algebras

In this section, we let  $B$  be any definite quaternion algebra over a totally real number field  $F$ , and let  $R$  be an order of  $B$ . Two basic computational problems are:

1. to find an isomorphism between given right  $R$ -ideals  $\mathfrak{a}$  and  $\mathfrak{b}$ , and
2. to compute the unit group of  $R$  (modulo the unit group of  $\mathcal{O}_F$ ).

The standard approach to both problems (as in [23]) reduces them to finitely many instances of the following problem.

**Quaternionic Norm Equation:** *Let  $L \cong \mathbb{Z}^d$  be a lattice contained in  $B$  (not necessarily of full rank). Given a totally positive element  $\alpha \in F$ , compute all  $x \in L$  with  $\text{nr}(x) = \alpha$ .*

In the context of isomorphism testing,  $L$  is the fractional ideal  $\mathfrak{a}\mathfrak{b}^{-1}$  and  $\alpha$  is some generator of  $\text{nr}(\mathfrak{a}\mathfrak{b}^{-1})$ . (One can show that it suffices to consider a finite set

of candidates for  $\alpha$ .) In the context of computing units,  $L$  is  $R$  (or occasionally an  $\mathcal{O}_F$ -submodule of  $R$ ), and  $\alpha$  is some unit of  $\mathcal{O}_F$ .

One may solve this by considering the positive definite quadratic form on  $L$  given by  $\text{Tr}(\text{nr}(x))$ . (Note that its values are positive since  $\text{nr}(x)$  is a totally positive element of  $F$ , for all  $0 \neq x \in B$ .) One captures all  $x \in L$  with  $\text{nr}(x) = \alpha$  by enumerating all  $x$  for which the quadratic form takes value  $\text{Tr}(\alpha)$  (using the standard Fincke-Pohst algorithm for enumeration). The drawback is that  $\text{Tr}(\alpha)$  might not be particularly small in relation to the determinant of the lattice (even when  $\alpha$  is a unit), in which case the lattice enumeration can be very time-consuming.

We now present a variation which avoids this bottleneck. For any nonzero  $c \in F$ , one may instead consider the lattice  $cL \subset B$ , again under the positive definite quadratic form given by  $\text{Tr}(\text{nr}(x))$ . One captures all  $x \in L$  with  $\text{nr}(x) = \alpha$  by enumerating all  $y \in cL$  with  $\text{Tr}(\text{nr}(y)) = \text{Tr}(c^2\alpha)$  and taking  $x = y/c$ . In the special case that  $c \in \mathbb{Q}$ , this merely rescales the enumeration problem. However, we will see that  $c \in F$  may be chosen so that, in the applications (1) and (2) above, one only needs to find relatively short vectors in the lattice.

Let  $g = \deg(F)$  and  $d = \dim(L)$ . Note that  $\det(cL) = |\mathbf{N}(c)|^{d/g} \det(L)$ . Heuristically, as  $c$  varies, the complexity of the enumeration process will be roughly proportional to the number of lattice elements with length up to the desired length, and this is asymptotically equal to

$$\frac{\text{Tr}(c^2\alpha)^{d/2}}{\det(cL)} = \frac{\text{Tr}(c^2\alpha)^{d/2}}{|\mathbf{N}(c)|^{d/g} \det(L)} = \frac{\text{Tr}(c^2\alpha)^{d/2}}{\mathbf{N}(c^2\alpha)^{d/2g}} \frac{\mathbf{N}(\alpha)^{d/2g}}{\det(L)}.$$

Given that  $\alpha$  is totally positive,  $\text{Tr}(c^2\alpha)/\mathbf{N}(c^2\alpha)^{1/g}$  cannot be less than  $g$ , and is close to  $g$  when all the real embeddings of  $c^2\alpha$  lie close together. It is straightforward to find  $c \in \mathcal{O}_F$  with this property, as follows.

**Algorithm.** Given some totally positive  $\alpha \in F$ , and some  $\epsilon > 0$ , this returns  $c \in \mathcal{O}_F$  such that  $\text{Tr}(c^2\alpha)/\mathbf{N}(c^2\alpha)^{1/g} < g + \epsilon$ .

1. Fix a  $\mathbb{Z}$ -module basis  $\mathbf{bas}(\mathcal{O}_F)$  of  $\mathcal{O}_F$ .
2. Initialize  $C := 100$ .
3. Calculate  $r_i := C/\sqrt{v_i(\alpha)}$  (note that the real embeddings of  $\alpha$  are positive).
4. Represent the vector  $(r_i)$  in terms of the basis  $\mathbf{bas}(\mathcal{O}_F)$ , then round the coordinates to integers, thus obtaining an element  $c \in \mathcal{O}_F$ .
5. If  $c$  does not have the desired property, multiply  $C$  by 100 and return to step (3).

*Proof.* Fix  $\alpha$  and let  $C \rightarrow \infty$ , regarding  $r_i \in \mathbb{R}$  and  $c \in \mathcal{O}_F$  as functions of  $C$ . Since we use a fixed basis of  $\mathcal{O}_F$ ,  $v_i(c) - r_i$  is bounded by a constant independent of  $C$ . Therefore as  $C \rightarrow \infty$ ,  $v_i(c^2\alpha) = r_i^2\alpha_i + O(C) = C^2 + O(C)$ . This implies that for any  $i$  and  $j$ , the ratio  $v_i(c^2\alpha)/v_j(c^2\alpha) \rightarrow 1$  as  $C \rightarrow \infty$ , and the lemma follows.

The complexity of the enumeration thus depends on the ratio  $\mathbf{N}(\alpha)^{d/2g}/\det(L)$ . In both the applications above, this ratio is small: in computing units,  $\alpha$  is a unit, and in isomorphism testing,  $\alpha$  generates the fractional ideal  $\text{nr}(L)$  where  $L = \mathfrak{a}\mathfrak{b}^{-1}$ .

### 3 Examples of Hilbert modular forms

In this section we give some examples of Hilbert modular forms computed using our algorithm, which we have implemented in Magma (and which will be available in a future version of Magma).

#### 3.1 The quadratic field $\mathbb{Q}(\sqrt{85})$

Let  $F = \mathbb{Q}(\sqrt{85})$ . The class number of  $F$  is the same as its narrow class number:  $h_F = h_F^+ = 2$ . The maximal order in  $F$  is  $\mathcal{O}_F = \mathbb{Z}[\omega_{85}]$ , where  $\omega_{85} = \frac{1+\sqrt{85}}{2}$ . Let  $B$  be the Hamilton quaternion algebra over  $F$ . As an  $F$ -algebra,  $B$  is generated by  $i, j$  subject to the relations  $i^2 = j^2 = (ij)^2 = -1$ . Since the prime 2 is inert in  $F$ , the algebra  $B$  is ramified only at the two infinite places. Using Magma, we find that the class number of  $B$  is 8. The Hecke module of Hilbert modular forms of level 1 and weight  $(2, 2)$  over  $F$  is therefore an 8-dimensional  $\mathbb{Q}$ -space, and it can be diagonalized by using the Hecke operator  $T_2$ . There are two Eisenstein series and two Galois conjugacy classes of newforms. The eigenvalues of the Hecke operators for the first few primes are given in Table 1 (only one eigenform in each Galois conjugacy class of newforms is listed). Each newform is given by a column, and we use the following labeling. For a quadratic field  $F$ , we label each form by a roman letter preceded by the discriminant of  $F$ . For the Hilbert class field of  $F$ , everything is just preceded by an H. For example, 85A is the first newform of level 1 over  $\mathbb{Q}(\sqrt{85})$ , and H85A is the first newform of level 1 over the Hilbert class field of  $\mathbb{Q}(\sqrt{85})$ .

The Hilbert class field of  $\mathbb{Q}(\sqrt{85})$  is  $H := \mathbb{Q}(\sqrt{5}, \sqrt{17}) = \mathbb{Q}(\alpha)$ , where the minimal polynomial of  $\alpha$  is  $x^4 - 4x^3 - 5x^2 + 18x - 1$ . The narrow class number of  $H$  is 1, and  $B \otimes_F H$  (the quaternion algebra over  $H$  ramified at the four infinite places) has class number 4. Thus the space of Hilbert modular forms of level 1 and weight  $(2, 2)$  is 4-dimensional. The eigenvalues of the Hecke action for the first few primes are listed in Table 1. There is one Eisenstein series and two classes of newforms. Elements of  $\mathcal{O}_H$  are expressed in terms of the integral basis

$$1, \quad \frac{1}{6}(\alpha^3 - 3\alpha^2 - 5\alpha + 10), \quad \frac{1}{6}(-\alpha^3 + 3\alpha^2 + 11\alpha - 10), \quad \frac{1}{6}(-\alpha^3 + 14\alpha + 5),$$

which we use to write generators of the ideals in the table.

We also computed some spaces over  $\mathbb{Q}(\sqrt{85})$  with nontrivial level. The dimensions of the spaces with prime level of norm less than 100 are given in Table 2. (It suffices to consider just one prime in each pair of conjugate primes, and for the precomputation we took  $S = \{(3, -1 + \omega_{85})\}$ .) For example, for level  $\mathfrak{N} = (5, \sqrt{85})$ ,  $M_2(\mathfrak{N})$  has dimension 20, and the Hecke operator  $T_{\mathfrak{p}}$  with  $\mathfrak{p} = (7, 2\omega_{85})$  acting on  $M_2(\mathfrak{N})$  has characteristic polynomial

$$(x - 8)(x + 8)(x^2 + 4)^2(x^4 - 10x^2 + 18)^2(x^6 + 28x^4 + 104x^2 + 100).$$

$N(\mathfrak{p})$	$\mathfrak{p}$	EIS1	EIS2	85A	85B	$N(\mathfrak{p})$	$\mathfrak{p}$	EIS	H85A	H85B
3	$(3, 2\omega_{85})$	4	-4	$2\sqrt{-1}$	$\beta$	4	$[1, -1, 0, 1]$	5	1	$3 + \beta'$
3	$(3, 4 + 2\omega_{85})$	4	-4	$-2\sqrt{-1}$	$\beta$	4	$[0, 2, -1, 1]$	5	1	$3 + \beta'$
4	$(2)$	5	5	1	$-\beta^3 + 3$	9	$[0, 1, -1, 0]$	10	2	$\beta'$
5	$(5, -1 + 2\omega_{85})$	6	-6	0	$-\beta^3 + 4\beta$	9	$[1, -1, -1, 0]$	10	2	$\beta'$
7	$(7, 2\omega_{85})$	8	-8	$-2\sqrt{-1}$	$\beta^3 - 5\beta$	19	$[0, 1, 0, -1]$	20	-4	2
7	$(7, 12 + 2\omega_{85})$	8	-8	$2\sqrt{-1}$	$\beta^3 - 5\beta$	19	$[-1, 2, 0, 1]$	20	-4	2
17	$(17, -1 + 2\omega_{85})$	18	-18	0	$2\beta^3 - 14\beta$	19	$[1, -1, -1, 1]$	20	-4	2
19	$(19, 2 + 2\omega_{85})$	20	20	-4	2	19	$[-1, 2, -1, 1]$	20	-4	2

**Table 1.** Hilbert modular forms of level 1 and parallel weight 2 over  $\mathbb{Q}(\sqrt{85})$  and its Hilbert class field  $H$ . The minimal polynomial of  $\beta$  (resp.  $\beta'$ ) is  $x^4 - 6x^2 + 2$  (resp.  $x^2 + 6x + 2$ ).

Comparing this with the space  $M_2(1)$  of level 1, on which  $T_{\mathfrak{p}}$  has characteristic polynomial

$$(x - 8)(x + 8)(x^2 + 4)(x^4 - 10x^2 + 18),$$

one sees that the Hecke action on the subspace of newforms  $M_2(\mathfrak{N})$  is irreducible, and the cuspidal oldform space embeds in  $M_2(\mathfrak{N})$  under two degeneracy maps (as expected).

$N(\mathfrak{N})$	$\dim M_2(\mathfrak{N})$	$\dim S_2(\mathfrak{N})$	$\dim S_2^{\text{new}}(\mathfrak{N})$
3	16	14	8
4	24	22	16
5	20	18	12
7	32	30	24
17	56	54	48
19	68	66	60
23	72	70	64
37	124	122	116
59	180	178	172
73	232	230	224
89	272	270	264
97	304	302	296

**Table 2.** Dimensions of spaces of Hilbert modular forms over  $\mathbb{Q}(\sqrt{85})$  with weight  $(2, 2)$  and prime level of norm less than 100

### 3.2 The quadratic field $\mathbb{Q}(\sqrt{10})$

Let  $F = \mathbb{Q}(\sqrt{10})$ . The Hilbert class field of  $F$  is  $H := \mathbb{Q}(\sqrt{2}, \sqrt{5}) = \mathbb{Q}(\alpha)$ , where the minimal polynomial of  $\alpha$  is  $x^4 - 2x^3 - 5x^2 + 6x - 1$ . The narrow class number of  $H$  is 1. We computed the space of Hilbert modular forms of level 1 and weight  $(2, 2)$  over  $F$  and  $H$ , and the Hecke eigenvalues for the first few primes are listed in Table 3 (only one eigenform in each Galois conjugacy class of newforms is

listed). Elements of  $\mathcal{O}_H$  are expressed in terms of the integral basis

$$1, \frac{1}{3}(2\alpha^3 - 3\alpha^2 - 10\alpha + 7), \frac{1}{3}(-2\alpha^3 + 3\alpha^2 + 13\alpha - 7), \frac{1}{3}(-\alpha^3 + 3\alpha^2 + 5\alpha - 8).$$

N(p)	p	EIS1	EIS2	40A	N(p)	p	EIS	H40A
2	$(2, \omega_{40})$	-3	3	$-\sqrt{2}$	4	$[0, 0, 1, 0]$	5	-2
3	$(3, \omega_{40} + 4)$	-4	4	$\sqrt{2}$	9	$[1, 1, -1, 0]$	10	-4
3	$(3, \omega_{40} + 2)$	-4	4	$\sqrt{2}$	9	$[0, 1, -1, 1]$	10	-4
5	$(5, \omega_{40})$	-6	6	$-2\sqrt{2}$	25	$[1, -2, 0, 0]$	26	-2
13	$(13, \omega_{40} + 6)$	-14	14	0	31	$[1, 1, 1, -1]$	32	4
13	$(13, \omega_{40} + 7)$	-14	14	0	31	$[1, -1, -1, -1]$	32	4
31	$(31, \omega_{40} + 14)$	32	32	4	31	$[1, 1, -1, 1]$	32	4
31	$(31, \omega_{40} + 17)$	32	32	4	31	$[-3, 2, -1, 0]$	32	4

**Table 3.** Hilbert modular forms of level 1 and parallel weight 2 over  $\mathbb{Q}(\sqrt{10})$  and its Hilbert class field.

### 3.3 Revisiting the examples by Okada

Okada [17] computes systems of Hecke eigenvalues of Hilbert newforms of level 1 and weight  $(2, 2)$  over the fields  $\mathbb{Q}(\sqrt{257})$  and  $\mathbb{Q}(\sqrt{401})$  by using explicit trace formulas. We now compare that data with results obtained using our algorithm.

First, let  $F = \mathbb{Q}(\sqrt{257})$ , which has  $h_F = h_F^+ = 3$ . Using our algorithm, we obtain that  $\dim M_2(1) = 39$  and  $\dim S_2(1) = 36$ . The forms that are base change come from the space of classical modular forms  $S_2(257, (\frac{257}{\cdot}))$  which has dimension 20. Thus the dimension of the subspace of Hilbert newforms that are not base change is  $36 - 20/2 = 26$ . For each character  $\chi : \text{Cl}^+(F) \rightarrow \mathbb{C}^\times$ , let  $S_2(1, \chi)$  be the subspace of  $S_2(1)$  corresponding to  $\chi$ . The space computed in [17] is the 12-dimensional subspace  $S_2(1, \mathbf{1})$ , where  $\mathbf{1}$  is the trivial character. Furthermore, since  $h_F^+ = 3$  is odd,  $S_2(1, \mathbf{1})$  maps isomorphically onto  $S_2(1, \chi)$  by twisting, for all  $\chi$ . Hence  $\dim S_2(1) = 3 \dim S_2(1, \mathbf{1})$ . In Table 4, we list all the eigenforms of level 1 and weight  $(2, 2)$  whose fields of coefficients have degree at most 4. There are two additional newforms 257E and 257F whose fields of coefficients are given respectively by the polynomials:

$$\begin{aligned} f &= x^9 + x^8 - 14x^7 - 10x^6 + 66x^5 + 25x^4 - 114x^3 - x^2 + 39x - 9 \\ g &= x^{18} - x^{17} + 15x^{16} - 6x^{15} + 140x^{14} - 33x^{13} + 771x^{12} + 75x^{11} + 2969x^{10} \\ &\quad + 559x^9 + 7056x^8 + 2982x^7 + 10627x^6 + 2430x^5 + 4672x^4 + 2091x^3 \\ &\quad + 1512x^2 + 351x + 81. \end{aligned}$$

The forms 257A and 257E are base change from  $S_2(257, (\frac{257}{\cdot}))$ , and 257B is the form discussed in [17].

Next, let  $F = \mathbb{Q}(\sqrt{401})$ , in which case  $h_F = h_F^+ = 5$ . Our algorithm gives the dimensions  $\dim M_2(1) = 125$  and  $\dim S_2(1) = 120$ . The forms that are base change come from the space of classical modular forms  $S_2(401, (\frac{401}{\cdot}))$ , which has dimension 32. Thus the dimension of the subspace of newforms that are not base change is  $120 - 32/2 = 104$ .

$N(\mathfrak{p})$	$\mathfrak{p}$	EIS1	257A	257B	257C	EIS2
2	$(2, \omega_{257})$	3	-1	$\frac{1+\sqrt{13}}{2}$	$\frac{1+\sqrt{-3}}{2}$	$\frac{-3+3\sqrt{-3}}{2}$
2	$(2, 1 - \omega_{257})$	3	-1	$\frac{1-\sqrt{13}}{2}$	$\frac{1-\sqrt{-3}}{2}$	$\frac{-3-3\sqrt{-3}}{2}$
9	(3)	10	4	-4	4	10
11	$(11, 4 + \omega_{257})$	12	0	1	0	$-6 + 6\sqrt{-3}$
11	$(11, 5 - \omega_{257})$	12	0	1	0	$-6 - 6\sqrt{-3}$
13	$(13, 9 + \omega_{257})$	14	2	$\sqrt{13}$	$-1 + \sqrt{-3}$	$-7 - 7\sqrt{-3}$
13	$(13, 10 - \omega_{257})$	14	2	$-\sqrt{13}$	$-1 - \sqrt{-3}$	$-7 + 7\sqrt{-3}$
17	$(17, 11 + \omega_{257})$	18	4	$4 + \sqrt{13}$	$-2 - 2\sqrt{-3}$	$-9 + 9\sqrt{-3}$
17	$(17, 12 - \omega_{257})$	18	4	$4 - \sqrt{13}$	$-2 + 2\sqrt{-3}$	$-9 - 9\sqrt{-3}$

  

$N(\mathfrak{p})$	$\mathfrak{p}$	257D
2	$(2, \omega_{257})$	$\beta$
2	$(2, 1 - \omega_{257})$	$(\beta^3 + \beta^2 + 4\beta - 3)/3$
9	(3)	-4
11	$(11, 4 + \omega_{257})$	$(-\beta^3 - 4\beta^2 - 4\beta - 9)/12$
11	$(11, 5 - \omega_{257})$	$(\beta^3 + 4\beta^2 + 4\beta - 3)/12$
13	$(13, 9 + \omega_{257})$	$(-7\beta^3 - 4\beta^2 - 28\beta + 21)/12$
13	$(13, 10 - \omega_{257})$	$(-\beta^3 - 4\beta^2 - 28\beta - 9)/12$
17	$(17, 11 + \omega_{257})$	$(-\beta^3 - 4\beta^2 + 4\beta - 9)/4$
17	$(17, 12 - \omega_{257})$	$(11\beta^3 + 20\beta^2 + 44\beta - 33)/12$

**Table 4.** Hilbert modular forms of level 1 and weight (2, 2) over  $\mathbb{Q}(\sqrt{257})$ . The minimal polynomial of  $\beta$  is  $x^4 + x^3 + 4x^2 - 3x + 9$ .

### 4 Examples of the Eichler-Shimura construction

In the study of Hilbert modular forms, the following conjecture is important and wide open. We refer to Shimura [19] or Knapp [15] for the classical case, and to Oda [16], Zhang [24] and Blasius [1] for the number field case.

**Conjecture 1 (Eichler-Shimura).** *Let  $f$  be a Hilbert newform of level  $\mathfrak{N}$  and parallel weight 2 over a totally real field  $F$ . Let  $K_f$  be the number field generated by the Fourier coefficients of  $f$ . Then there exists an abelian variety  $A_f$  defined over  $F$ , with good reduction outside of  $\mathfrak{N}$ , such that  $K_f \hookrightarrow \text{End}(A_f) \otimes \mathbb{Q}$  and*

$$L(A_f, s) = \prod_{\sigma \in \text{Gal}(K_f/\mathbb{Q})} L(f^\sigma, s),$$

where  $f^\sigma$  is obtained by letting  $\sigma$  act on the Fourier coefficients of  $f$ .

In the classical setting, namely when  $F = \mathbb{Q}$ , this is a theorem known as the Eichler-Shimura construction. In general, many cases of the conjecture are also known. In those cases the abelian variety  $A_f$  is often constructed as a quotient of the Jacobian of some Shimura curve of level  $\mathfrak{N}$ . See, for example, Zhang [24] and references therein. In the case when  $[F : \mathbb{Q}]$  is even, the level of such a Shimura curve must contain at least one finite prime, which means its Jacobian must have

at least one prime of bad reduction. So when  $A_f$  has everywhere good reduction, such a parametrization is simply not available. In this section, we provide new examples of such  $A_f$ . We note that similar examples have already been discussed in Socrates and Whitehouse [21].

**Remark 4.** We refer back to the final paragraph of section 3.1. The characteristic polynomials given there, viewed in terms of Conjecture 1, indicate that the newspace of  $M_2(\mathfrak{N})$  corresponds to a simple abelian variety of dimension 6.

#### 4.1 The quadratic field $\mathbb{Q}(\sqrt{85})$

Keeping the notation of subsection 3.1, let  $E/H$  be the elliptic curve with the following coefficients:

$a_1$	$a_2$	$a_3$	$a_4$	$a_6$
$E : [1, 0, 0, 1]$	$[0, -1, 0, -1]$	$[0, 1, 1, 0]$	$[-5, -6, -1, 0]$	$[-8, -7, -3, 2]$

It is a global minimal model which has everywhere good reduction. Hence, the restriction of scalars  $A = \text{Res}_{H/F}(E)$  is an abelian surface over  $F$  also with everywhere good reduction.

**Remark 5.** The  $j$ -invariant of  $E$  is  $64047678245 - 12534349815\omega_{85} \in F$ , and in fact  $E$  is  $H$ -isomorphic to its conjugate under  $\text{Gal}(H/F)$ . Therefore  $A$  is isomorphic to  $E \times E$  over  $H$ . Let  $E'$  denote one of the other two conjugates with respect to the Galois group  $\text{Gal}(H/\mathbb{Q})$ , which have  $j$ -invariant  $51513328430 + 12534349815\omega_{85}$ ; there is an isogeny of degree 2 from  $E$  to  $E'$ . The restriction of scalars  $\text{Res}_{H/F}(E')$  over  $F$  is isomorphic to  $E' \times E'$  over  $H$ , and is therefore isogenous to  $A$ .

To establish the modularity of  $E$  and  $A$ , we will apply the following result of Skinner and Wiles. Here we state the *nearly ordinary* assumption (Condition (iv)) in a slightly different way.

**Theorem 3 ([20, Theorem A]).** *Let  $F$  be a totally real abelian extension of  $\mathbb{Q}$ . Suppose that  $p \geq 3$  is prime, and let  $\rho : \text{Gal}(\overline{F}/F) \rightarrow \mathbf{GL}_2(\overline{\mathbb{Q}}_p)$  be a continuous, absolutely irreducible and totally odd representation unramified away from a finite set of places of  $F$ . Suppose that the reduction of  $\rho$  is of the form  $\overline{\rho}^{ss} = \chi_1 \oplus \chi_2$ , where  $\chi_1$  and  $\chi_2$  are characters, and suppose that:*

- (i) *the splitting field  $F(\chi_1/\chi_2)$  of  $\chi_1/\chi_2$  is abelian over  $\mathbb{Q}$ ,*
- (ii)  *$(\chi_1/\chi_2)|_{D_v} \neq 1$  for each  $v \mid p$ ,*
- (iii)  *$\rho|_{I_v} \cong \begin{pmatrix} \psi\epsilon_p^{k-1} & * \\ 0 & 1 \end{pmatrix}$  for each prime  $v \mid p$ ,*
- (iv)  *$\det \rho = \psi\epsilon_p^{k-1}$ , with  $k \geq 2$  an integer,  $\psi$  a character of finite order, and  $\epsilon_p$  the  $p$ -adic cyclotomic character.*

Then  $\rho$  comes from a Hilbert modular form.

**Proposition 4.** *a) The elliptic curve  $E$  is modular and corresponds to the form H85A in Table 1.*

*b) The abelian surface  $A$  is modular and corresponds to the form 85A in Table 1.*

*Proof.* a) Let  $\rho_{E,3}$  be the 3-adic representation attached to  $E$ , and  $\bar{\rho}_{E,3}$  the corresponding residual representation. Also, let  $\mathfrak{p} \subset \mathcal{O}_H$  be any prime above 3. Using Magma, we compute the torsion subgroup  $E(H)_{tors} \cong \mathbb{Z}/2 \oplus \mathbb{Z}/2$ , and the trace of Frobenius  $a_{\mathfrak{p}}(E) = 2$ . The latter implies that the representation  $\rho_{E,3}$  is ordinary at  $\mathfrak{p}$ . By direct calculation, we find that  $j(E)$  is the image of a  $H$ -rational point on the modular curve  $X_0(3)$ :

$$j(E) = \frac{(\tau + 27)(\tau + 3)^3}{\tau}, \text{ where } \tau = [2166, 527, -527, 1054].$$

This implies that  $E$  has a Galois-stable subgroup of order 3, so the representation  $\bar{\rho}_{E,3}$  is reducible. Since it is ordinary, there exist characters  $\chi, \chi'$  unramified away from  $\mathfrak{p} \mid 3$ , with  $\chi$  unramified at  $\mathfrak{p}$ , such that  $\bar{\rho}_{E,3}^{ss} = \chi \oplus \chi'$  and  $\chi\chi' = \epsilon_3$  is the mod 3 cyclotomic character. The field  $H(\chi/\chi')$  is clearly abelian. Therefore the representation  $\rho_{E,3}$  satisfies the conditions of Skinner and Wiles, and  $E$  is modular. Comparing traces of Frobenius with the eigenvalues given in Table 1, we see that the corresponding form is H85A.

b) Let  $f$  be the base change from  $F$  to  $H$  of the newform 85A in Table 1. Since the Hilbert class field extension  $H/F$  is totally unramified, the form  $f$  has level 1 and trivial character. By comparing the Fourier coefficients at the split primes above 19, we see that  $f = \text{H85A}$  in Table 2. The result then follows from properties of restriction of scalars and base change.

**Remark 6.** To find  $E$ , we reasoned as follows. The eigenvalues of H85A in Table 1 suggest that the curve corresponding to it admits a 2-isogeny. This curve must have good reduction everywhere, and so must its conjugates; if these are also modular, then they share the same  $L$ -series and are therefore isogenous to each other. This would mean the curve comes from an  $H$ -rational point on  $X_0(2)$  whose  $j$ -invariant is integral. Using a parametrisation of  $X_0(2)$ , we searched for such points. We would like to thank Noam Elkies for suggesting this approach. (Note that it would be extremely arduous to find  $E$  by computing all elliptic curves over  $H$  with trivial conductor, via the general algorithm described in Cremona and Lingham [3].)

**Remark 7.** If we assume Conjecture 1, then there exists a modular abelian surface  $A$  over  $H$  with real multiplication by  $\mathbb{Q}(\sqrt{7})$  which corresponds to the form H85B in Table 1. The restriction of scalars of  $A$  from  $H$  to  $F$  is a modular abelian fourfold with real multiplication by  $\mathbb{Q}(\beta)$  which corresponds to the form 85B in Table 1.

## 4.2 The quadratic field $\mathbb{Q}(\sqrt{10})$

Keeping the notation of subsection 3.2, let  $E/H$  be the elliptic curve with the following coefficients:

$a_1$	$a_2$	$a_3$	$a_4$	$a_6$
$E : [0, 0, 1, 0]$	$[1, 0, 1, -1]$	$[0, 1, 0, 0]$	$-[15, 44, 21, 26]$	$-[91, 123, 48, 97]$

This is a global minimal model with everywhere good reduction over  $H$ . In contrast with the previous example, the four Galois conjugates have distinct  $j$ -invariants. The restriction of scalars  $A = \text{Res}_{H/F}(E)$  is an abelian surface over  $F$  with everywhere good reduction.

**Proposition 5.** *The elliptic curve  $E/H$  and the abelian surface  $A/F$  are modular;  $E$  corresponds to H40A in Table 3, and  $A$  corresponds to 40A in Table 3.*

*Proof.* Let  $\rho_{E,3}$  be the 3-adic representation attached to  $E$ , and  $\bar{\rho}_{E,3}$  its reduction modulo 3. Then  $\bar{\rho}_{E,3}$  is reducible since

$$j(E) = \frac{(\tau + 27)(\tau + 3)^3}{\tau}, \text{ where } \tau = [5, 52, -18, -26].$$

As before, it is easy to see that  $\rho_{E,3}$  satisfies the conditions of Skinner and Wiles. So  $E$  is modular, and hence  $A$  is also modular. Comparing traces of Frobenius with Fourier coefficients, it is easy to see which forms in the tables they correspond to.

Alternatively, we could consider the 7-adic representation  $\rho_{E,7}$ . Its reduction mod 7 is reducible since the point  $([16, 23, 9, 18] : [-157, -268, -119, -184] : [1, 0, 0, 0])$  is an  $H$ -rational point of order 7 on  $E$ . Furthermore, for any prime  $\mathfrak{p} \mid 7$ , we have  $a_{\mathfrak{p}}(E) = 8$ , and it is easy to see that  $\rho_{E,7}$  satisfies the conditions of Skinner and Wiles.

**Remark 8.** It was shown by Kagawa [11, Theorem 3.2] that there is no elliptic curve with everywhere good reduction over  $\mathbb{Q}(\sqrt{10})$ . Our results show that if we assume modularity in addition, there is only one such simple abelian variety: an abelian surface with real multiplication by  $\mathbb{Z}[\sqrt{2}]$ .

**Remark 9.** To find  $E$ , we were again assisted by the eigenvalues of the corresponding form H40A in Table 3, which suggest that  $E$  has an  $H$ -rational point of order 14. The modular curve  $X_0(14)/\mathbb{Q}$  is an elliptic curve (14A1 in Cremona's table), which (using Magma) was found to have rank 1 over  $H$  and also rank 1 over  $\mathbb{Q}(\sqrt{10})$ ; this enabled us to obtain a point of infinite order simply by finding a  $\mathbb{Q}$ -rational point on the quadratic twist by  $\sqrt{10}$ . We considered curves corresponding to points of small height in  $X_0(14)(H)$ , and twists of these curves, until we found one with good reduction everywhere.

**Remark 10.** Although we have restricted the discussion in this paper to fields with even degree, the algorithm can clearly be used over fields with odd degree as well. In that case, the ramification  $Ram(B)$  of the quaternion algebra  $B$  must contain some finite primes, and we only obtain the newforms whose corresponding automorphic representations are special or supercuspidal at the primes in  $Ram(B)$ .

## References

1. D. Blasius, Elliptic curves, Hilbert modular forms, and the Hodge conjecture, in: Hida, Ramakrishnan, Shahidi (eds.): *Contributions to automorphic forms, geometry, and number theory*, 83–103, Johns Hopkins Univ. Press, Baltimore, MD, 2004.
2. Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, **24**(3-4): 235-265, 1997.
3. J. Cremona and M. Lingham, Finding all elliptic curves with good reduction outside a given set of primes: pdf, 15 pages. To appear in: *Experimental Mathematics*.
4. L. Dembélé, 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. *Math. Comp.* **76**, no 258, (2007), 1039–1057.
6. L. Dembélé, On the computation of algebraic modular forms. (submitted).
7. L. Dembélé, F. Diamond and D. Roberts. Examples and numerical evidence for the Serre conjecture over totally real number fields. In preparation.
8. M. Eichler, On theta functions of real algebraic number fields. *Acta Arith.* **33** (1977), no 3, 269–292.
9. S. Gelbart, Automorphic forms on adèle groups. *Annals of Maths. Studies* **83**, Princeton Univ. Press, 1975.
10. H. Jacquet and R. P. Langlands, Automorphic forms on  $GL(2)$ . *Lectures Notes in Math.*, vol. **114**, Springer-Verlag, Berlin and New York, 1970.
11. T. Kagawa, Elliptic curves with everywhere good reduction over real quadratic fields. Ph. D Thesis, Waseda University, 1998.
12. M. Kisin, Modularity of 2-adic Barsotti-Tate representations, preprint. Available at <http://www.math.uchicago.edu/~kisin/preprints.html>.
13. C. Khare and Wintenberger, On Serre’s conjecture for 2-dimensional mod  $p$  representations of the absolute Galois group of the rationals. To appear in *Annals of Mathematics*. Available at <http://www.math.utah.edu/~shekhar/serre.pdf>.
14. M. Kirschmer, Konstruktive Idealtheorie in Quaternionenalgebren. Diplom Thesis, Universität Ulm, 2005.
15. A. W. Knap, *Elliptic curves*. Mathematical Notes, **40**. Princeton University Press, Princeton, NJ, 1992. xvi+427 pp.
16. T. Oda, *Periods of Hilbert modular surfaces*. Progress in Mathematics, **19**. Birkhuser, Boston, Mass., 1982. xvi+123 pp.
17. K. Okada, Hecke eigenvalues for real quadratic fields. *Experiment. Math.* **11** (2002), no. 3, 407–426.
18. M. Schein, Weights in Serre’s conjecture for Hilbert modular forms: the ramified case To appear in the *Israel Journal of Mathematics*. Available at <http://www.math.huji.ac.il/~mschein/wt5rev.pdf>.

19. G. Shimura, *Introduction to the arithmetic theory of automorphic functions*. Kanô Memorial Lectures, No. 1. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971. xiv+267 pp.
20. Skinner, C. M.; Wiles, A. J. Residually reducible representations and modular forms. *Inst. Hautes Études Sci. Publ. Math.* No. **89** (1999), 5–126 (2000).
21. J. Socrates and D. Whitehouse, Unramified Hilbert modular forms, with examples relating to elliptic curves. *Pacific J. Math.* **219** (2005), no. 2, 333–364
22. R. Taylor, On Galois representations associated to Hilbert modular forms. *Invent. Math.* **98** (1989), no. 2, 265–280.
23. J. Voight, Quadratic forms and quaternion algebras: Algorithms and arithmetic. Ph. D thesis, University of California, Berkeley, 2005.
24. S. Zhang, Heights of Heegner points on Shimura curves. *Ann. of Math. (2)* **153** (2001), no. 1, 27–147.