

# Unramified Hilbert Modular Forms, with Examples Relating to Elliptic Curves

Jude Socrates and David Whitehouse

June 4, 2004

## Abstract

We give a method to explicitly determine the space of unramified Hilbert cusp forms of weight two, together with the action of Hecke, over a totally real number field of even degree and narrow class number one. In particular, one can determine the eigenforms in this space and compute their Hecke eigenvalues to any reasonable degree. As an application we compute this space of cusp forms for  $\mathbf{Q}(\sqrt{509})$ , and determine each eigenform in this space which has rational Hecke eigenvalues. We find that not all of these forms arise via base change from classical forms. To each such eigenform  $\mathbf{f}$  we attach an elliptic curve with good reduction everywhere whose  $L$ -function agrees with that of  $\mathbf{f}$  at every place.

## 1 Introduction

In general finding unramified cuspidal representations for a given group is a difficult problem. If one tries to tackle this problem using, for example, the trace formula then one usually needs to shrink the discrete group and hence allow some ramification. In this paper we are concerned with computing the space of unramified Hilbert cusp forms for a totally real field of even degree.

Let  $F$  be a totally real number field of narrow class number one and of even degree over  $\mathbf{Q}$ . In Section 2 we explain how, by results of Jacquet, Langlands and Shimizu, the construction of the space of Hilbert cusp forms, of weight 2 (i.e. of weight  $(2, \dots, 2)$ ) and full level for  $F$ , can be done on the quaternion algebra  $\mathbf{B}$  over  $F$  which is ramified precisely at the infinite places of  $F$ . In fact the space of such cusp forms can be identified with a certain space of functions on the set of equivalence classes of ideals for a maximal order in  $\mathbf{B}$ .

In Sections 3 and 4 we extend the definition of  $\Theta$ -series and Brandt matrices, as found in [Pi3], to this case. Furthermore, we show that each simultaneous eigenvector for the family of modified Brandt matrices, corresponds to a Hilbert cusp form which is an eigenvector for all the Hecke operators. In order to compute the Brandt matrices, and hence the space of cusp forms, we need to be able to find representatives for all the ideal classes for a maximal order, we outline our strategy to find these representatives in Section 5.

In the following two sections we specialize to the case of a real quadratic field of narrow class number one. In Section 6, using a result of Pizer, we give an explicit formula for the type number of  $\mathbf{B}$  and the class number of a maximal order in  $\mathbf{B}$ . In the following section we give defining relations for the quaternion algebra  $\mathbf{B}$  over a real quadratic field  $\mathbf{Q}(\sqrt{m})$ , and when  $m \equiv 5 \pmod{8}$  we give a maximal order in this algebra.

We now turn to our application to elliptic curves. To any Hilbert modular newform  $\mathbf{f}$  over a totally real field  $F$ , of weight 2, level  $\mathbf{n}$  and with rational Hecke eigenvalues one expects to be able to attach an elliptic curve  $E_{\mathbf{f}}$  which is defined over  $F$ , has conductor  $\mathbf{n}$  and whose  $L$ -function agrees with that of  $\mathbf{f}$  at all places of  $F$ . This is known if  $F$  has odd degree over  $\mathbf{Q}$  or if the automorphic representation associated to  $\mathbf{f}$  is discrete series at some finite place (see [Bla, 1.7.1]). In particular the following conjecture is open.

**Conjecture 1.1.** *Let  $F$  be a totally real number field of even degree over  $\mathbf{Q}$ . Then to each unramified Hilbert modular eigenform  $\mathbf{f}$ , over  $F$  and of weight 2, which has rational Hecke eigenvalues one can attach an elliptic curve  $E_{\mathbf{f}}$  defined over  $F$  with good reduction everywhere, such that the  $L$ -functions of  $E_{\mathbf{f}}$  and  $\mathbf{f}$  agree at each place of  $F$ .*

In the case that  $\mathbf{f}$  is the base change of a classical modular form one can sometimes attach an elliptic curve to  $\mathbf{f}$  as in the conjecture by work of Shimura, see [Shi, 7.7]. Also, by work of Blasius [Bla], this conjecture is true under the hypothesis of the Hodge conjecture. In this paper we establish this conjecture for  $F = \mathbf{Q}(\sqrt{509})$ . The reason for this choice of field is, as we shall see, that there exist eigenforms which do not arise via base change from  $\mathrm{GL}_2(\mathbf{Q})$ , and nor are they CM forms since  $h^+(F) = 1$ . To our knowledge this provides the first verification of this conjecture in the case that not all forms arise by base change (cf [Bla, 1.7.3]).

We now outline the verification of Conjecture 1.1 for  $F = \mathbf{Q}(\sqrt{509})$ . In Section 8 we give representatives for the ideal classes in  $\mathbf{B}$  from which we are able to compute the Brandt matrices and therefore the eigenvalues of the unramified eigenforms of weight 2. In particular we find that there are three eigenforms whose Hecke eigenvalues all lie in  $\mathbf{Q}$ . In Section 9 we give the equations for the three elliptic curves over  $F$  which we will show are attached to our three eigenforms. These elliptic curves already exist in the literature (see [Cre] and [Pin]).

In Section 10 we prove Conjecture 1.1 for  $\mathbf{Q}(\sqrt{509})$ . One of our forms is a base change of a classical form given in [Cre]. In this case one knows, by work of Shimura, that an elliptic curve is attached to this form. Now we take  $\mathbf{f}$  to be one of the forms which is not a base change from  $\mathbf{Q}$  and we take  $E$  to be the elliptic curve (or its Galois conjugate) defined over  $F$  given in [Pin].

By work of Taylor, building on work of Carayol and Wiles, and independently by Blasius and Rogawski, there exists for each rational prime  $\ell$  an  $\ell$ -adic representation

$$\sigma_{\mathbf{f},\ell} : \mathrm{Gal}(\overline{F}/F) \rightarrow \mathrm{GL}_2(\mathbf{Q}_{\ell})$$

which is unramified outside  $\ell$ . Furthermore if  $\mathfrak{p}$  is a prime of  $F$  not dividing  $\ell$  and  $\text{Fr}_{\mathfrak{p}}$  is a Frobenius element at  $\mathfrak{p}$  we have  $\text{Tr } \sigma_{\mathbf{f},\ell}(\text{Fr}_{\mathfrak{p}}) = a_{\mathbf{f}}(\mathfrak{p})$ , the eigenvalue of  $\mathbf{f}$  with respect to the  $\mathfrak{p}^{\text{th}}$  Hecke operator, and  $\det \sigma_{\mathbf{f},\ell}(\text{Fr}_{\mathfrak{p}}) = N\mathfrak{p}$ . Similarly for each rational prime  $\ell$  we have a representation

$$\sigma_{E,\ell} : \text{Gal}(\overline{F}/F) \rightarrow \text{GL}_2(\mathbf{Q}_{\ell})$$

given by the action of Galois on the  $\ell$ -adic Tate module of  $E$ . Since  $E$  has good reduction everywhere  $\sigma_{E,\ell}$  is unramified outside  $\ell$  and for each prime  $\mathfrak{p}$  not dividing  $\ell$  we have  $\text{Tr } \sigma_{E,\ell}(\text{Fr}_{\mathfrak{p}}) = a_E(\mathfrak{p})$  and  $\det \sigma_{E,\ell}(\text{Fr}_{\mathfrak{p}}) = N\mathfrak{p}$ .

The verification of Conjecture 1.1 for  $\mathbf{f}$  will therefore be complete if we can show, for some prime  $\ell$ , that these two representations are equivalent. For this we take  $\ell = 2$  and use a result due to Faltings and Serre proven in [Liv]. We cannot apply this result directly since it requires the traces of Frobenii to be even, which is not the case here. So we begin by showing that the extensions of  $F$  cut out by the kernels of the mod 2 representations obtained from the eigenform and the elliptic curve are the same. Having identified these extensions we can apply the theorem of Faltings and Serre to show that these two representations are equivalent, when restricted to this extension of  $F$ . Using Frobenius reciprocity we conclude that these representations of  $\text{Gal}(\overline{F}/F)$  are equivalent.

This work was begun by the first author in his PhD thesis [Soc]. In [Soc], the construction of the space of cusp forms for a real quadratic field of narrow class number one was given. Furthermore the cusp form  $\mathbf{f}$  above, and the elliptic curve  $E$ , were shown to have the same  $L$ -factors at all primes generated by a totally positive element  $a + b\theta$  with  $1 \leq a \leq 64$  where  $\theta = \frac{1+\sqrt{509}}{2}$ . This work was completed by the second author, who extended the methods of [Soc] to any totally real field of narrow class number one with even degree over  $\mathbf{Q}$ , adapted the result of Faltings and Serre, and independently computed the necessary eigenvalues given in Table 6.

*Acknowledgements.* Both authors thank their advisor, Dinakar Ramakrishnan, for his support and guidance through this work. They would also like to thank Don Blasius for comments on an earlier version of this paper, Barry Mazur for his encouragement and the referee for their thorough report which lead to several improvements in the exposition.

## 2 Construction of the Space of Cusp Forms

Throughout this paper  $F$  will be a totally real number field of narrow class number one and of even degree over  $\mathbf{Q}$ . We denote by  $R$  the ring of integers in  $F$ . We let  $F^+$  (resp.  $R^+$ ) denote the totally positive elements in  $F$  (resp.  $R$ ). In this section we explain how one can construct the space of cusp forms for  $F$  of weight 2 and full level.

Let  $\mathbf{B}/F$  be the unique (up to isomorphism) quaternion algebra which is ramified only at the infinite places of  $F$ . We now give some definitions.

An  $R$ -lattice (or ideal)  $V$  in  $\mathbf{B}$  is a finitely generated  $R$ -submodule of  $\mathbf{B}$  such that  $V \otimes_R F \cong \mathbf{B}$ . An element  $\mathbf{b} \in \mathbf{B}$  is *integral* or is said to be an integer, if  $R[\mathbf{b}]$  is an  $R$ -lattice in  $\mathbf{B}$ . An *order* in  $\mathbf{B}$  is a ring  $\mathcal{O}$  consisting of integers and containing  $R$  such that  $F\mathcal{O} = \mathbf{B}$ . A *left ideal*  $I$  for an order  $\mathcal{O}$  is an  $R$ -lattice for which  $\mathcal{O}I \subset I$ . Two left  $\mathcal{O}$ -ideals  $I_1$  and  $I_2$  are said to be *right equivalent* if  $I_1 = I_2\mathbf{b}$  for some  $\mathbf{b} \in \mathbf{B}^\times$ . Similarly, two orders  $\mathcal{O}_1$  and  $\mathcal{O}_2$  are *of the same type* if  $\mathcal{O}_1 = \mathbf{b}\mathcal{O}_2\mathbf{b}^{-1}$  for some  $\mathbf{b} \in \mathbf{B}^\times$ . The number  $H$  of right equivalence classes of left  $\mathcal{O}$ -ideals is called the *class number of  $\mathcal{O}$*  and the number  $T$  of type classes of maximal orders of  $\mathbf{B}$  is called the *type number of  $\mathbf{B}$* . Both of these numbers are finite (for any order  $\mathcal{O}$ ).

We now fix a maximal order  $\mathcal{O}$  in  $\mathbf{B}$ . Let  $\mathbf{G} = \mathbf{B}^\times$  viewed as an algebraic group over  $F$ . Since  $\mathbf{B}$  only ramifies at the infinite places of  $F$  for each finite prime  $\mathfrak{p}$  we have

$$\mathbf{B} \otimes_F F_{\mathfrak{p}} \cong M_2(F_{\mathfrak{p}}).$$

Moreover we can choose these isomorphisms such that they give an isomorphism of  $\mathcal{O}_{\mathfrak{p}} = \mathcal{O} \otimes R_{\mathfrak{p}}$  with  $M_2(R_{\mathfrak{p}})$ . Clearly each of these isomorphisms gives rise to an isomorphism of  $\mathbf{G}(F_{\mathfrak{p}})$  with  $\mathrm{GL}_2(F_{\mathfrak{p}})$  under which  $\mathcal{O}_{\mathfrak{p}}^\times$  corresponds to  $\mathrm{GL}_2(R_{\mathfrak{p}})$ .

We construct the double coset space

$$X = M_{\mathbf{G}} \backslash \mathbf{G}(\mathbf{A}_F^f) / \mathbf{G}(F),$$

where  $\mathbf{A}_F^f$  is the ring of finite adèles, and  $M_{\mathbf{G}} = \prod_{\mathfrak{p} < \infty} \mathrm{GL}_2(R_{\mathfrak{p}})$  is a maximal compact open subgroup of  $\mathbf{G}(\mathbf{A}_F^f)$ . We note that  $M_{\mathbf{G}}$ , as a subgroup of  $\mathbf{G}(\mathbf{A}_F^f)$ , depends on the choice of  $\mathcal{O}$  and hence so does  $X$ . The set  $X$  can be identified with the right equivalence classes of left  $\mathcal{O}$ -ideals in the following way. Given  $(x_{\mathfrak{p}}) \in \mathbf{G}(\mathbf{A}_F^f)$  consider the open compact subset  $\prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}x_{\mathfrak{p}}$  in  $\mathbf{B} \otimes \mathbf{A}_F^f$ . Taking the intersection of  $\prod_{\mathfrak{p}} \mathcal{O}_{\mathfrak{p}}x_{\mathfrak{p}}$  with  $\mathbf{B}$ , embedded diagonally in  $\mathbf{B} \otimes \mathbf{A}_F^f$ , yields a left  $\mathcal{O}$ -ideal. Conversely, given a left  $\mathcal{O}$ -ideal  $I$  one recovers an element of  $\mathbf{G}(\mathbf{A}_F^f)$  by choosing, for each prime  $\mathfrak{p}$ , a generator of the principal left  $\mathcal{O}_{\mathfrak{p}}$ -ideal  $\mathcal{O}_{\mathfrak{p}}I$ .

We denote by  $S$  the space

$$S = \{ \mathbf{f} : X \rightarrow \mathbf{C} \} / \{ \text{constant functions on } X \}.$$

There is a natural definition of Hecke operators on this space given as follows.

Let  $\pi_{\mathfrak{p}}$  be a uniformizer for  $R_{\mathfrak{p}}$ , and  $g_{\mathfrak{p}} \in \mathbf{G}(\mathbf{A}_F^f)$  such that the  $\mathfrak{p}$ -th component of  $g_{\mathfrak{p}}$  is

$$\begin{pmatrix} \pi_{\mathfrak{p}} & 0 \\ 0 & 1 \end{pmatrix}$$

and is the identity otherwise. Since  $\mathrm{GL}_2(R_{\mathfrak{p}})$  is open and compact in  $\mathrm{GL}_2(F_{\mathfrak{p}})$ , we have  $M_{\mathbf{G}}g_{\mathfrak{p}}M_{\mathbf{G}} = \prod_{i=1}^n M_{\mathbf{G}}g_i$ . A classical result states that we can choose the set  $\{g_i\}$  to be

$$\left\{ \begin{pmatrix} \pi_{\mathfrak{p}} & 0 \\ \alpha & 1 \end{pmatrix} : \alpha \in R/\mathfrak{p} \right\} \cup \left\{ \begin{pmatrix} 1 & 0 \\ 0 & \pi_{\mathfrak{p}} \end{pmatrix} \right\}.$$

Define, for  $\mathbf{f} \in S$  and  $h \in \mathbf{G}(\mathbf{A}_F^f)$

$$(\mathbf{T}_p(\mathbf{f}))(h) = \sum_{i=1}^n \mathbf{f}(g_i h).$$

One sees that this gives a well-defined action on  $S$  which is independent of the choices of the  $g_i$  and also of  $\pi_p$ .

Let  $\mathcal{S}$  be the  $\mathbf{C}$ -vector space of holomorphic Hilbert cusp forms over  $F$  of weight 2 and full level. Then  $\mathcal{S}$  is a multiplicity free direct sum of simultaneous 1-dimensional Hecke eigenspaces. A similar decomposition holds for  $S$ . By Jacquet, Langlands and Shimizu (see [GJ]), there is a Hecke-equivariant isomorphism between  $\mathcal{S}$  and  $S$ .

Our goal now is to give a method to compute the action of the Hecke operators on the space  $S$ . This will be done by constructing Brandt matrices  $B(\xi)$  and modified Brandt matrices  $B'(\xi)$ , which are families of rational matrices indexed by  $\xi \in R^+$ . These are objects that were first defined over  $\mathbf{Q}$  and later used to construct cusp forms for congruence subgroups of  $\mathrm{SL}_2(\mathbf{Z})$ .

### 3 $\Theta$ -Series of an Ideal

The notion and construction of a  $\Theta$ -series for an ideal in a quaternion algebra is discussed in several papers, including [Pi2], [Pi3], [Pi4] and [Gro]. In this section we extend these definitions to ideals in a totally definite quaternion algebra  $\mathbf{B}$  defined over  $F$ .

Let  $J$  be an ideal in the totally definite quaternion algebra  $\mathbf{B}$ . Let  $\mathbf{nr}$  denote the reduced norm from  $\mathbf{B}$  to  $F$ . The norm of any non-zero element in  $\mathbf{B}$  is totally positive. We denote by  $\mathbf{nr}(J)_+$  a totally positive generator of  $\mathbf{nr}(J)$ , the fractional ideal of  $F$  generated by the norms of the elements in  $J$ . For any  $\beta \in J$  we define

$$\mathcal{N}_J(\beta) = \mathbf{nr}(\beta)/\mathbf{nr}(J)_+.$$

We define the  $\Theta$ -series of  $J$  for  $\tau \in \mathcal{H}^{\mathrm{Hom}(F, \mathbf{R})}$  by

$$\Theta_J(\tau) = \sum_{\beta \in J} \exp(\tau \mathcal{N}_J(\beta)) = \sum_{\xi \in R^+} c_{\xi, J} \exp(\tau \xi)$$

where  $c_{\xi, J}$  is the number of elements  $\beta$  in  $J$  with  $\mathcal{N}_J(\beta) = \xi$ . We note that this sum converges since composing  $\mathcal{N}_J$  with the trace map from  $F$  to  $\mathbf{Q}$  gives a positive definite quadratic form on  $J$  as a  $\mathbf{Z}$ -lattice.

**Proposition 3.1.** *The definition of  $c_{\xi, J}$  is independent of the choice of  $\mathbf{nr}(J)_+$ .*

*Proof.* Any two choices for  $\mathbf{nr}(J)_+$  will differ by a totally positive unit  $v$ . Since  $F$  has narrow class number one,  $v = u^2$  for some unit  $u$ . Thus multiplication by  $u \in R^\times$  gives a bijection between the set of elements in  $J$  of norm  $\xi \mathbf{nr}(J)_+$

and those of norm  $\xi \mathbf{vnr}(J)_+$ .  $\square$

We note that if  $J' = \gamma_1 J \gamma_2$  with  $\gamma_i \in \mathbf{B}^\times$  then the  $\Theta$ -series of  $J$  and  $J'$  are identical, the proof as in [Pi3, Proposition 2.17] holds in this case.

Suppose that we are given an ideal  $J$  in terms of a basis over  $R$ . We give an effective algorithm to determine the  $c_{\xi, J}$ . Let  $\{\beta_1, \dots, \beta_4\}$  be a basis for  $J$  over  $R$  and let  $\{\omega_1, \dots, \omega_n\}$  be a basis for  $R$  over  $\mathbf{Z}$ . Then we can write  $\beta \in J$  uniquely as

$$\beta = \sum_{i=1}^4 \sum_{j=1}^n x_{ij} \omega_j \beta_i$$

with  $x_{ij} \in \mathbf{Z}$ . Then  $\mathcal{N}_J(\beta)$  is a totally positive element of  $R$ , provided  $\beta \neq 0$ , and composing  $\mathcal{N}_J$  with the trace map from  $F$  to  $\mathbf{Q}$  gives a positive definite quadratic form in the  $\{x_{ij}\}$ . Therefore, given a basis of an ideal  $J$  and  $M \in \mathbf{R}$  we can use [Co1, Algorithm 2.7.7] to compute  $c_{\xi, J}$  for all  $\xi \in R^+$  with  $\text{Tr}(\xi) \leq M$ .

## 4 Brandt Matrices and Eigenforms

Brandt matrices were classically constructed from a complete set of representatives of left  $\mathcal{O}$ -ideal classes of an Eichler order  $\mathcal{O}$  of  $\mathbf{B}'$ , a definite quaternion algebra over  $\mathbf{Q}$  with  $\text{Ram}(\mathbf{B}') = \{\infty, p\}$ . For such a  $\mathbf{B}'$ , [Pi3] and [Pi4] show that terms appearing in a so-called Brandt matrix series are actually modular forms (for  $\mathbf{Q}$ ) of a given weight and level  $p$ . In this section we extend these definitions to a totally definite quaternion algebra  $\mathbf{B}$  defined over  $F$ . We then give an adélic construction of the Brandt matrices and show that each eigenvector for the family of modified Brandt matrices corresponds to a cusp form.

Let  $\mathcal{O}$  be a maximal order in  $\mathbf{B}$ , and  $\{I_1, \dots, I_H\}$  a complete (ordered) set of representatives of distinct left  $\mathcal{O}$ -ideal classes. For each  $k$  let

$$\mathcal{O}_r(I_k) = \{\mathbf{b} \in \mathbf{B} : I_k \mathbf{b} \subset I_k\}$$

denote the right order of  $I_k$ , this is another maximal order in  $\mathbf{B}$ . The inverse of  $I_k$  is defined by

$$I_k^{-1} = \{\mathbf{b} \in \mathbf{B} : I_k \mathbf{b} I_k \subset I_k\}.$$

Then, for each  $k$ ,  $\{I_k^{-1} I_1, \dots, I_k^{-1} I_H\}$  represent the left  $\mathcal{O}_r(I_k)$ -ideal classes.

In the notation of Section 3, let

$$e_j = e(I_j) = c_{1, \mathcal{O}_r(I_j)}$$

which is simply the number of elements of norm 1 in the order  $\mathcal{O}_r(I_j)$ . We define  $b_{i,j}(0) = 1/e_j$  and for  $\xi \in R^+$

$$b_{i,j}(\xi) = \frac{1}{e_j} c_{\xi, I_j^{-1} I_i}$$

which is  $1/e_j$  times the number of elements in the left  $\mathcal{O}_r(I_j)$ -ideal  $I_j^{-1}I_i$  of norm  $\xi \mathbf{nr}(I_i)_+ / \mathbf{nr}(I_j)_+$ . Now define the  $\xi$ -th Brandt matrix for  $\mathcal{O}$  by

$$B(\xi, \mathcal{O}) = (b_{i,j}(\xi)).$$

We note that the construction of  $B(\xi, \mathcal{O})$  is well defined up to conjugation by a permutation matrix. Moreover, if  $\mathcal{O}'$  is another maximal order then the matrices  $B(\xi, \mathcal{O})$  and  $B(\xi, \mathcal{O}')$  are conjugate by a permutation matrix independent of  $\xi$ . In view of this, we shall denote by  $B(\xi) = B(\xi, \mathcal{O})$  the  $\xi$ -th Brandt matrix, for some fixed maximal order  $\mathcal{O}$ .

The following properties of the Brandt matrices are stated in [Pi3] and proven there for quaternion algebras over  $\mathbf{Q}$  with the proofs carrying over for the Brandt matrices defined above.

- Theorem 4.1.**
1.  $e_j b_{i,j}(\xi) = e_i b_{j,i}(\xi)$
  2.  $\sum_{j=1}^H b_{i,j}(\xi)$  is independent of  $i$ . Denote this value by  $b(\xi)$ . Then  $b(\xi)$  is the number of integral left  $\mathcal{O}$  ideals of norm  $\xi$ .
  3. The Brandt matrices generate a commutative semisimple ring.

Define the  $H \times H$  matrix  $A$  by

$$A = \begin{pmatrix} 1 & e_1/e_2 & e_1/e_3 & \dots & e_1/e_H \\ 1 & -1 & 0 & \dots & 0 \\ 1 & 0 & -1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & -1 \end{pmatrix}.$$

Then for  $\xi \in R^+$  or  $\xi = 0$  we have

$$AB(\xi)A^{-1} = \begin{pmatrix} b(\xi) & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & B'(\xi) & \\ 0 & & & \end{pmatrix}$$

This is proven in [Pi3] with the proof carrying over here. The submatrix  $B'(\xi)$  will be referred to as the  $\xi$ -th modified Brandt matrix.

We now show that each simultaneous eigenvector for the family of modified Brandt matrices corresponds to a cusp form. In [Sh] Shimizu constructs a representation of the Hecke algebra acting on the space of automorphic forms, and in [HPS, Chapter 5] it is shown that this can be used to provide another construction of Brandt matrices. We follow the discussion in [HPS], and simplify it for the case that we are interested in.

We now fix a maximal order  $\mathcal{O}$  in  $\mathbf{B}$ . Let  $\mathbf{G} = \mathbf{B}^\times$  viewed as an algebraic group over  $F$ . Every left  $\mathcal{O}$ -ideal is of the form  $\mathcal{O}\tilde{a}$  for some  $\tilde{a} \in \mathbf{G}(\mathbf{A}_F)$ . Let

$$\mathcal{U} = \mathcal{U}(\mathcal{O}) = \{\tilde{u} = (u_{\mathfrak{p}}) \in \mathbf{G}(\mathbf{A}_F) : u_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}^\times \text{ for all } \mathfrak{p} < \infty\}.$$

Since  $\tilde{a}\mathcal{U}\tilde{a}^{-1}$  is commensurable with  $\mathcal{U}$  for all  $\tilde{a} \in \mathbf{G}(\mathbf{A}_F)$ , we can define the usual Hecke ring  $R(\mathcal{U}, \mathbf{G}(\mathbf{A}_F))$  (see [Shi]). Put

$$\mathcal{U}(\mathbf{A}_F) = \{\tilde{u} = (u_{\mathfrak{p}}) \in \mathbf{I}_F : u_{\mathfrak{p}} \in R_{\mathfrak{p}}^{\times} \text{ for all } \mathfrak{p} < \infty\}$$

where  $\mathbf{I}_F$  is the group of idèles of  $F$ . For  $\xi \in R^+$ , denote by  $\mathbf{T}(\xi)$  the element of  $R(\mathcal{U}, \mathbf{G}(\mathbf{A}_F))$  which is the sum of all double cosets  $\mathcal{U}\tilde{a}\mathcal{U}$  such that  $a_{\mathfrak{p}} \in \mathcal{O}_{\mathfrak{p}}$  for all  $\mathfrak{p} < \infty$  and  $\mathbf{nr}(\tilde{a}) \in \xi\mathcal{U}(\mathbf{A}_F)$ .

Denote by  $\mathcal{M} = \mathcal{M}_2(\mathcal{O})$  the space of continuous  $\mathbf{C}$ -valued functions  $f$  on  $\mathbf{G}(\mathbf{A}_F)$ , satisfying

$$f(u\tilde{a}\mathbf{b}) = f(\tilde{a})$$

for all  $u \in \mathcal{U}, \tilde{a} \in \mathbf{G}(\mathbf{A}_F)$ , and  $\mathbf{b} \in \mathbf{G}(F)$ . We define a representation of  $R(\mathcal{U}, \mathbf{G}(\mathbf{A}_F))$  on  $\mathcal{M}$  as follows. For  $\mathcal{U}y\mathcal{U} \in R(\mathcal{U}, \mathbf{G}(\mathbf{A}_F))$ , let  $\mathcal{U}y\mathcal{U} = \cup_i \mathcal{U}y_i$  be its decomposition into disjoint right cosets. Now, let

$$\rho(\mathcal{U}y\mathcal{U})f(\tilde{a}) = \sum_i f(y_i\tilde{a})$$

and extend  $\rho$  to  $R(\mathcal{U}, \mathbf{G}(\mathbf{A}_F))$  by linearity. It is shown in [HPS, pg 31] that this representation is independent of the choice of maximal order. This is in the sense that if  $\mathcal{O}'$  is another maximal order then there are isomorphisms between  $R(\mathcal{U}, \mathbf{G}(\mathbf{A}_F))$  and  $R(\mathcal{U}', \mathbf{G}(\mathbf{A}_F))$ , which preserves the Hecke operators  $\mathbf{T}(\xi)$ , and between  $\mathcal{M}_2(\mathcal{O})$  and  $\mathcal{M}_2(\mathcal{O}')$ . Such that the representation of  $R(\mathcal{U}, \mathbf{G}(\mathbf{A}_F))$  on  $\mathcal{M}_2(\mathcal{O})$  induced by these isomorphisms is equivalent to the original representation of  $R(\mathcal{U}, \mathbf{G}(\mathbf{A}_F))$  on  $\mathcal{M}_2(\mathcal{O})$ .

If  $H$  is the class number of  $\mathcal{O}$ , we have

$$\mathbf{G}(\mathbf{A}_F) = \bigcup_{\lambda=1}^H \mathcal{U}\tilde{x}_{\lambda}\mathbf{G}(F).$$

Note that the  $I_{\lambda} = \mathcal{O}\tilde{x}_{\lambda}$  give a complete set of representatives of left  $\mathcal{O}$ -ideal classes. Since the elements of  $\mathcal{M}$  are determined by their values at the  $x_{\lambda}$  the map

$$f \mapsto (f_1, \dots, f_H) \tag{1}$$

gives an isomorphism of  $\mathcal{M}$  with  $\mathbf{C}^H = \mathbf{C}_1 \oplus \dots \oplus \mathbf{C}_H$ , where each  $\mathbf{C}_i$  is a copy of  $\mathbf{C}$ . We can use the isomorphism (1) to give a matrix representation for  $\rho$ . For  $\xi \in R^+$ , let

$$B(\xi) = (\rho_{i,j}(\xi))_{i,j=1\dots H}$$

where multiplication by  $\rho_{i,j}(\xi)$  is the map from  $\mathbf{C}_j$  to  $\mathbf{C}_i$  which is the composition of the injection of  $\mathbf{C}_j$  into  $\mathbf{C}^H$ , the inverse of map (1),  $\rho(\mathcal{U}\xi\mathcal{U})$ , map (1), and the projection of  $\mathbf{C}^H$  into  $\mathbf{C}_i$ . The following is proven in [HPS, Proposition 5.1] with the proof carrying over here.

**Proposition 4.2.** *The definition of  $B(\xi)$  yields the same matrix as the Brandt matrices defined above, assuming that we use the same maximal order  $\mathcal{O}$  and set of left  $\mathcal{O}$ -ideal representatives  $I_{\lambda}$ .*

We shall now make explicit the isomorphism as Hecke modules between the spaces of Hilbert modular cusp forms and  $\mathbf{C}$ -valued functions on the finite set  $X$  modulo constant functions, which was mentioned in Section 2. We will follow the construction of Hida ([Hid]), which is also discussed in [Tay]. As before, we shall be interested only in the weight 2, full level case.

Having fixed isomorphisms between  $\mathbf{G}(F_{\mathfrak{p}})$  and  $\mathrm{GL}_2(F_{\mathfrak{p}})$  as in section 2 we let

$$U = M_{\mathbf{G}} = \prod_{\mathfrak{p} < \infty} \mathrm{GL}_2(R_{\mathfrak{p}}),$$

an open subgroup of the finite part of the adelization of  $\mathcal{O}$ . Denote by  $S(U)$  the space of  $\mathbf{C}$ -valued functions on  $X$ , the set of right equivalence classes of left  $\mathcal{O}$ -ideals. Via the identification of  $X$  as a double coset space  $S(U)$  is just  $\mathcal{M}_2(\mathcal{O})$  defined above. The Hecke action on  $S(U)$  is that given in Section 2. Let  $\mathrm{inv}(U)$  be the subspace of  $S(U)$  of functions of the form  $f \circ \mathbf{nr}$ , where  $\mathbf{nr}$  is the reduced norm map

$$\mathbf{nr} : \mathbf{G}(\mathbf{A}_F^f) \rightarrow \mathbf{I}_F^f$$

and  $f$  is an appropriate  $\mathbf{C}$ -valued function on  $\mathbf{I}_F^f$ , the finite idèles of  $F$ . The map  $\mathbf{nr}$ , when restricted to the image of  $\mathbf{B}^{\times}$ , surjects into the totally positive elements of  $F$  (this is the Theorem of Norms in [Vig, pg 80]). Hence we can view  $\mathrm{inv}(U)$  as functions of the form

$$\mathbf{G}(\mathbf{A}_F^f) \xrightarrow{\mathbf{nr}} \mathbf{I}_F^f \rightarrow \mathcal{U}(R_{\mathfrak{p}}) \setminus \mathbf{I}_F^f / F^+ \xrightarrow{\cong} \mathrm{Cl}^+(F) \rightarrow \mathbf{C}$$

where  $\mathrm{Cl}^+(F)$  is the ray class group of  $F$ . Since we are assuming that  $h^+(F) = 1$ , so  $\mathrm{inv}(U)$  is the space of constant functions on  $X$ .

The Hecke operators certainly fix  $\mathrm{inv}(U)$ . Thus, in order to examine the Hecke action on the space of cusp forms, we must decompose  $S(U)$  into a direct sum of  $\mathrm{inv}(U)$  and a space  $S_2(U)$  which is preserved by the Hecke algebra.

Let us describe the Hecke action on  $\mathrm{inv}(U)$ . Let  $\mathbf{T}_{\mathfrak{p}}$  be the  $\mathfrak{p}$ -th Hecke operator, and  $f$  the function which is 1 on all elements of  $X$ . In Section 2, we saw the decomposition of

$$\left( \prod_{\mathfrak{p} < \infty} \mathrm{GL}_2(R_{\mathfrak{p}}) \right) g_{\mathfrak{p}} \left( \prod_{\mathfrak{p} < \infty} \mathrm{GL}_2(R_{\mathfrak{p}}) \right)$$

into disjoint right cosets. Note, though, that in this decomposition, we also obtain exactly the elements in  $\mathbf{G}(\mathbf{A}_F)$  which yield, upon multiplying to the right of  $\mathcal{O}$ , the set of integral left  $\mathcal{O}$ -ideals of norm  $\mathfrak{p}$ . Thus,  $\mathbf{T}_{\mathfrak{p}}(f)$  is the function with constant value equal to the number of such ideals.

We have seen above that the matrix  $A$  transforms the Brandt matrices into two blocks consisting of a  $1 \times 1$  cell containing  $b(\xi)$  and the modified Brandt matrix  $B'(\xi)$ . And in Theorem 4.1 we noted that  $b(\xi)$  is precisely the number of integral left  $\mathcal{O}$ -ideals of norm  $\xi$ . Thus we have the following.

**Proposition 4.3.** *Let  $\{\mathbf{v}_i\}$  be a basis for  $\mathbf{C}^{H-1}$  consisting of eigenvectors for all the modified Brandt matrices. Then each  $\mathbf{v}_i$  corresponds to a (normalized)*

holomorphic Hilbert modular eigenform  $\mathbf{f}_i$  of weight 2 and full level whose eigenvalue with respect to the  $\mathfrak{p}$ -th Hecke operator is precisely the eigenvalue of  $\mathbf{v}_i$  with respect to  $B'(\pi)$ , where  $\pi$  is a totally positive generator of  $\mathfrak{p}$ .

In order to find a basis of  $\mathbf{C}^{H-1}$  of simultaneous eigenvectors for all the modified Brandt matrices one computes the matrices  $B'(\xi)$ , ordered by the trace of  $\xi$ , and successively decomposes the space  $\mathbf{C}^{H-1}$  into simultaneous eigenspaces until one is left with one-dimensional eigenspaces.

It is, of course, desirable to know which of these forms do not arise by base change. Suppose that  $F/\mathbf{Q}$  is a cyclic extension with Galois group  $G$ . Then  $G$  acts on the set of eigenforms via permutation of the primes of  $F$ . And one knows that a form does not arise by base change from an intermediate field if and only if its Galois orbit has order equal to the degree of the extension  $F/\mathbf{Q}$ . Using this one can then determine precisely which forms arise via base change once one has found a basis of  $\mathbf{C}^{H-1}$  of simultaneous eigenvectors of the  $B'(\xi)$  using the procedure described above. In the case that  $F/\mathbf{Q}$  is solvable there are added complications to determining which forms don't arise by base change coming from the existence of Galois fixed Hecke characters which do not descend, see [Ra].

## 5 Finding Type and Ideal Class Representatives

In order to use Proposition 4.3 to compute the space of cusp forms we need to be able to find representatives for the ideal classes of a maximal order  $\mathcal{O}$  in  $\mathbf{B}$ . In this section we give a strategy to find these representatives.

We continue with  $\mathbf{B}$ , the quaternion algebra over  $F$  ramified only at the infinite places of  $F$ , and we take  $\mathcal{O}$  to be a maximal order in  $\mathbf{B}$ . It is easy to manufacture ideals of  $\mathcal{O}$  when they are of a particular form. Let  $\alpha \in \mathbf{B} \setminus F$ . Then  $K = F(\alpha)$  is a quadratic extension of  $F$  contained in  $\mathbf{B}$ . Let  $I$  be an ideal in the ring of integers  $S$  of  $K$ . Then  $J = \mathcal{O}I$  is a left ideal of  $\mathcal{O}$ . Moreover we have  $\mathbf{nr}(J) = N_{K/F}(I)$  since  $1 \in \mathcal{O}$ . Clearly, if  $I$  and  $I'$  are in the same ideal class in  $K$  then  $J$  and  $J'$  are in the same left  $\mathcal{O}$ -ideal class.

We will now see that it suffices to consider ideals of the form  $\mathcal{O}I$  as in the construction above, in order to find representatives of left  $\mathcal{O}$ -ideal classes.

**Proposition 5.1.** *Every left  $\mathcal{O}$ -ideal class of a maximal order  $\mathcal{O}$  contains an ideal of the form  $\mathcal{O}I$  where  $I$  is an ideal in a field extension  $K = F(\mathbf{b})$  contained in  $\mathbf{B}$ .*

*Proof.* The left  $\mathcal{O}$ -ideal classes are in bijection with

$$X = M_{\mathbf{G}} \setminus \mathbf{G}(\mathbf{A}_F^f) / \mathbf{G}(F)$$

as stated in Section 2. Since this is a finite set, there is a finite set of primes  $S$  such that  $\mathbf{G}(\mathbf{A}_F^f) = M_{\mathbf{G}} \mathbf{B}_S^{\times} \mathbf{G}(F)$  where  $\mathbf{B}_S = \prod_{\mathfrak{p} \in S} \mathbf{B}_{\mathfrak{p}}$ . Now

$$i_S(\mathbf{B}) := \{(\mathbf{b}, \dots, \mathbf{b}) \in \mathbf{B}_S : \mathbf{b} \in \mathbf{B}\}$$

is dense in  $\mathbf{B}_S$ , hence  $i_S(\mathbf{B}^\times)$  is dense in  $\mathbf{B}_S^\times$ . Since  $M_{\mathbf{G}}$  is open in  $\mathbf{G}(\mathbf{A}_F^f)$  we have by strong approximation  $\mathbf{G}(\mathbf{A}_F^f) = M_{\mathbf{G}}i_S(\mathbf{B}^\times)\mathbf{G}(F)$ . Thus every  $\beta \in \mathbf{G}(\mathbf{A}_F^f)$  is of the form  $\beta = \mu i_S(\mathbf{b})\mathbf{b}_0$  for some  $\mu \in M_{\mathbf{G}}$  and  $\mathbf{b}, \mathbf{b}_0 \in \mathbf{B}^\times$ . Thus, under the local-global correspondence the left  $\mathcal{O}$ -ideal  $\mathcal{O}\beta$  is in the same class as  $\mathcal{O}i_S(\mathbf{b})$  where  $i_S(\mathbf{b})$  can be viewed as a fractional ideal in  $F(\mathbf{b})$ .  $\square$

We now outline the algorithm for finding representatives for left  $\mathcal{O}$ -ideal classes.

1. Determine the class number  $H$ . (This can be done, see [Pi1]. We will make this explicit in the case of a quadratic field in Section 6 below.)
2. Initialize the list of representatives of left  $\mathcal{O}$ -ideal classes to  $L = \{\mathcal{O}\}$ .
3. Find an element  $\alpha \in \mathbf{B}$  such that the ring of integers of  $K = F[\alpha]$  is exactly  $R[\alpha]$ .
4. Determine  $h = h(K)$  and  $S = \{I_1 \dots I_h\}$ , ideal representatives for the class group of  $K$ ,

OR,

Generate a large list  $S = \{I_i\}$  of prime ideals of  $K$ .

5. Now, for  $I_i \in S$ , do:
  - (a) Find a basis for  $J_i = \mathcal{O}I_i$ .
  - (b) Determine if  $J_i$  is in the same class as any of the ideals in  $L$  obtained so far. If not, add  $J$  to  $L$ , and keep a note of  $\alpha$  and  $I_i$ .
6. Stop if  $H$  representatives have been found, otherwise resume from Step 3.

We would like to know how to determine if two left  $\mathcal{O}$ -ideals belong to different ideal classes, which is step 5b of the algorithm. In Section 3 we saw that the  $\Theta$ -series gives a necessary test for two ideals to be in the same class. We now give a necessary and sufficient condition for two ideals to be in the same class.

**Proposition 5.2.** *Let  $I$  and  $J$  be left  $\mathcal{O}$ -ideals for an Eichler order  $\mathcal{O}$ . Then  $I$  and  $J$  belong to the same left ideal class if and only if there is an  $\alpha \in M = \overline{J}I$ , where  $\overline{J}$  denotes the conjugate ideal of  $J$ , such that  $\mathbf{nr}(\alpha) = \mathbf{nr}(I)\mathbf{nr}(J)$ , i.e. with  $\mathcal{N}_M(\alpha) = 1$ .*

This is proven in [Pi3] with the proof valid for any quaternion algebra over a number field. To use this proposition we will need to construct a basis for  $M$ , then compute the normalized norm  $\mathcal{N}_M$  as in Section 3.

## 6 Computing $T$ and $H$

We now specialize to the case of a real quadratic field  $F = \mathbf{Q}(\sqrt{m})$  of narrow class number one. As is well known this implies that either  $m = 2$  or  $m$  is prime and congruent to 1 mod 4. In this section we give an explicit formula for the type number of  $\mathbf{B}$  and the class number of a maximal order  $\mathcal{O}$  in  $\mathbf{B}$ . The most important tool will be the main theorem in [Pi1] stated below.

**Theorem 6.1.** (*Pizer*) *Let  $F$  be a totally real number field of degree  $n$  over  $\mathbf{Q}$ ,  $R$  the ring of integers of  $F$ . Let  $\mathbf{B}$  be a positive definite quaternion algebra over  $F$ . Let  $q_1$  be the product of the finite primes in  $F$  which ramify in  $\mathbf{B}$  and let  $q_2$  be a finite product of distinct finite primes of  $F$  such that  $(q_1, q_2) = 1$ . Then the type number  $T_{q_1 q_2}$  of Eichler orders of level  $q_1 q_2$  in  $\mathbf{B}$  is*

$$T_{q_1 q_2} = \frac{1}{2^e h(F)} \left( M + \frac{1}{2} \sum_{\mathcal{S}_a \in C} E_{q_1 q_2}(\mathcal{S}_a) \frac{h(\mathcal{S}_a)}{w(\mathcal{S}_a)} \right) \quad (2)$$

where

- $e$  is the number of primes dividing  $q_1 q_2$ .
- $M$  is Eichler's mass and is given by

$$M = \frac{2h(F)\zeta_F(2)\text{disc}(F)^{\frac{3}{2}}}{(2\pi)^{2n}} \prod_{\mathfrak{p}|q_1} (N(\mathfrak{p}) - 1) \prod_{\mathfrak{p}|q_2} (N(\mathfrak{p}) + 1)$$

where  $\zeta_F$  is the zeta function of  $F$ .

- $h(\mathcal{S}_a)$  is the ideal class number of locally principal  $\mathcal{S}_a$ -fractional ideals.
- $w(\mathcal{S}_a)$  is the index of the group of units of  $R$  in the group of units in  $\mathcal{S}_a$ .
- $E_{q_1 q_2}(\mathcal{S}_a) = \prod_{\mathfrak{p}|q_1} \left( 1 - \left\{ \frac{\mathcal{S}_a}{\mathfrak{p}} \right\} \right) \prod_{\mathfrak{p}|q_2} \left( 1 + \left\{ \frac{\mathcal{S}_a}{\mathfrak{p}} \right\} \right)$ .
- $C$  is the collection of all orders defined by the following procedure:
  1. Let  $e_1, \dots, e_s$  be a complete set of representatives of  $U \bmod U^2$  where  $U$  are the units of  $R$ ;
  2. let  $d_1, \dots, d_k$  be a complete set of integral ideal representatives of  $E \cdot \text{Fr}(F)^2 \bmod (\text{Pr}(F)^2)$  where  $E$  is the subgroup of  $\text{Fr}(F)$  (the divisor group of  $F$ ) generated by all the  $\mathfrak{p}$  which divide  $q_1 q_2$ , and  $\text{Pr}(F)$  is the subgroup of principal divisors of  $\text{Fr}(F)$ .
  3. Let  $n_1, \dots, n_t$  be a set of all elements of  $R$  such that
    - (a)  $(n_j) = d_{j'}$  for some  $j'$  with  $1 \leq j' \leq k$
    - (b)  $(n_i) \neq (n_j)$  for  $i \neq j$ .

4. Consider the collection of all polynomials over  $R$  of the form

$$f_{\mu,\rho,\tau}(x) = x^2 - \tau x + n_\mu e_\rho$$

with  $1 \leq \rho \leq s$ ,  $1 \leq \mu \leq t$  where

- (a)  $f_{\mu,\rho,\tau}$  is irreducible over  $F$
  - (b)  $F[x]/f_{\mu,\rho,\tau}(x)$  cannot be embedded in any  $F_{\infty_i}$ ,  $i = 1, \dots, n$
  - (c) for all  $\mathfrak{p} < \infty$ ,  $\mathfrak{p}^{s_{\mathfrak{p}}} \mid \tau$  where  $s_{\mathfrak{p}} = \left\lceil \frac{v_{\mathfrak{p}}(n_\mu)}{2} \right\rceil$
  - (d) if  $v_{\mathfrak{p}}(n_\mu)$  is odd then  $\mathfrak{p}^{s_{\mathfrak{p}}+1} \mid \tau$ .
5. Let  $a$  be a root of some  $f_{\mu,\rho,\tau}$  and for each  $f_{\mu,\rho,\tau}$  choose only one root. Then  $C = \{\mathcal{S}_a : \mathcal{S}_a \text{ is an order of } F(a)\}$  such that
- (a)  $R[a] \subset \mathcal{S}_a$
  - (b) if  $\mathfrak{p} < \infty$  then  $a\pi_{\mathfrak{p}}^{-s_{\mathfrak{p}}} \in \mathcal{S}_{a,\mathfrak{p}}$  where  $s_{\mathfrak{p}} = \left\lceil \frac{v_{\mathfrak{p}}(N(a))}{2} \right\rceil$ .

We now use this theorem of Pizer to derive a more explicit formula for the algebra  $\mathbf{B}$  over any real quadratic field of narrow class number one.

**Theorem 6.2.** *Let  $m \equiv 1 \pmod{4}$  be a positive squarefree number greater than 5,  $F = \mathbf{Q}(\sqrt{m})$  and  $R$  the ring of integers in  $F$ . Assume furthermore that  $F$  has narrow class number one. Let  $\mathbf{B}$  be the totally definite quaternion algebra which is unramified at all the finite primes of  $F$ . Then the type number  $T$  of  $\mathbf{B}$  is given by*

$$T = \frac{1}{48m} \sum_{u=1}^m \binom{u}{m} u^2 + \frac{1}{8}h(\mathbf{Q}(\sqrt{-m})) + \frac{1}{6}h(\mathbf{Q}(\sqrt{-3m})).$$

For completeness we note that if  $m = 5$  the type number of  $\mathbf{B}$  is one, see [Soc, Theorem 5.2]

*Proof of Theorem 6.2.* We proceed to determine the quantities in Theorem 6.1. We have  $h(F) = 1$ . Since  $\mathbf{B}$  is unramified at all finite primes,  $q_1 = 1$  and for maximal orders  $q_2 = 1$ . Thus  $e = 0$  and the two products in the definition of Eichler's mass  $M$  are thus both empty. Since  $m \equiv 1 \pmod{4}$  so  $\text{disc}(F) = m$  and

$$M = \frac{2\zeta_F(2)m^{\frac{3}{2}}}{(2\pi)^4} = \frac{m^{\frac{3}{2}}}{8\pi^4}\zeta_F(2).$$

We shall further simplify  $M$  by explicitly calculating  $\zeta_F(2)$ . Our method will be that of [Leo] which uses generalized Bernoulli numbers, see also [Neu, Chapter VII]. Define the  $n$ th Bernoulli number,  $B_n$ , by

$$\frac{te^t}{e^t - 1} = \sum_{n \geq 0} B_n \frac{t^n}{n!}.$$

For a character  $\chi \bmod f$ , define  $B_{n,\chi}$  by

$$\sum_{u=1}^f \chi(u) \frac{te^{ut}}{e^{ft} - 1} = \sum_{n \geq 0} B_{n,\chi} \frac{t^n}{n!}.$$

For  $F = \mathbf{Q}(\sqrt{m})$ ,  $m > 0$  we define

$$B_{n,F} = \prod_{\chi} B_{n,\chi}$$

where the product runs over the characters mod  $d = |\text{disc}(F)| = m$  which correspond to characters of  $\text{Gal}(F/\mathbf{Q})$ . Hence this product involves only the trivial character and  $\chi$  the Legendre symbol mod  $m$ . Thus  $B_{n,F} = B_n B_{n,\chi}$ . In [Leo] it is shown that

$$\zeta_F(n) = \frac{(2\pi)^{2n} \sqrt{d} B_{n,F}}{4d^n (n!)^2}$$

if  $n$  is a positive even integer. Thus we have  $M = \frac{1}{48} B_{2,\chi}$  since  $B_2 = 1/6$ . Now

$$B_{2,\chi} = \frac{1}{m} \sum_{u=1}^m \left(\frac{u}{m}\right) u^2$$

and hence

$$M = \frac{1}{48m} \sum_{u=1}^m \left(\frac{u}{m}\right) u^2.$$

Now we proceed with the rest of the algorithm. The product defining  $E_{q_1 q_2}(\mathcal{S}_a) = E_1(\mathcal{S}_a)$  is also empty regardless of  $\mathcal{S}_a$ , so  $E_1(\mathcal{S}_a) = 1$ . Equation (2) then becomes

$$T = M + \frac{1}{2} \sum_{\mathcal{S}_a \in C} \frac{h(\mathcal{S}_a)}{w(\mathcal{S}_a)}.$$

We now follow the algorithm to find the collection  $C$ .

1. Since  $U = \langle -1 \rangle \langle u \rangle$  where  $u$  is a fundamental unit of  $F$  and  $U^2 = \langle u^2 \rangle$  we get  $s = 4$ , and a set of representatives for  $U \bmod U^2$  is given by  $\{\pm 1, \pm u\}$ .
2. Since  $q_1 q_2 = 1$  and  $\text{Fr}(F) = \text{Pr}(F)$  we have  $k = 1$ ,  $E = (1)$  and  $\{(1)\}$  is a complete set of representatives for  $E \cdot \text{Fr}(F)^2 \bmod \text{Pr}(F)^2$ .
3. From (2), we can take  $t = 1$  and  $n = n_1 = 1$ .
4. We shall call the polynomials obtained in this step *contributing polynomials*, and denote this set by  $\Psi$ . Since  $\mu = 1 = t$  and  $n = n_1 = 1$  we shall abbreviate

$$f_{\rho,\tau}(x) = x^2 - \tau x + e_\rho.$$

since  $v_{\mathfrak{p}}(n) = 0$  for any  $v_{\mathfrak{p}}$ , we have  $s_{\mathfrak{p}} = 0$  for every finite  $\mathfrak{p}$ , so condition (4.c) is always satisfied by any  $\tau$ . Condition (4.d) is vacuous. Now we look at condition (4.b). Since  $F$  is totally real this condition requires that the discriminant of  $f_{\rho,\tau}$

$$\Delta(f_{\rho,\tau}) = \tau^2 - 4e_{\rho}$$

be totally negative. But for any  $\tau$ ,  $\Delta(f_{-1,\tau})$  and  $\Delta(f_{-u,\tau})$  are always positive, since  $u > 0$ . Hence we need only consider  $f_{1,\tau}$  and  $f_{u,\tau}$ . But  $N_{F/\mathbf{Q}}(u) = -1$  tells us that  $\sigma(u) < 0$ , where  $\sigma$  is the non-trivial element of  $\text{Gal}(F/\mathbf{Q})$ . So for any  $\tau$ ,  $\sigma(\tau)^2 - 4\sigma(u) > 0$ . So only  $e_{\rho} = 1$  remains. We further abbreviate

$$f_{\tau}(x) = x^2 - \tau x + 1.$$

Our problem is therefore to find all  $\tau = a + b\theta \in R$ , where  $\theta = 1/2(1 + \sqrt{m})$ , such that  $\tau^2 - 4 < 0$  and  $\sigma(\tau)^2 - 4 < 0$ , i.e. such that

$$-2 < a + b\theta, a + b - b\theta < 2.$$

Thus we see that we necessarily need  $-4 < (2\theta - 1)b < 4$  which is  $-4 < \sqrt{m}b < 4$ . Hence if  $m > 16$  then  $b = 0$  is the only possible value. In this case,  $\tau = a = 0, \pm 1$ . Note that these three values yield a contributing  $f_{\tau}$ . On the other hand if  $m < 16$  then the only possible value for  $m$  is 13 and in this case we must have  $b = 0$  or  $\pm 1$ . But for  $b = 1$  we must have

$$\frac{-5 + \sqrt{13}}{2} < a < \frac{3 - \sqrt{13}}{2}$$

and there are no such integers  $a$ . On the other hand if  $b = -1$  then we must have

$$\frac{-3 + \sqrt{13}}{2} < a < \frac{5 - \sqrt{13}}{2}$$

and again there are no such integers. Clearly condition (4.a), irreducibility, is satisfied by all the  $f_{\tau}$  above since the roots are imaginary. We summarize step 4 in the following.

**Lemma 6.3.** *Assume the hypotheses in Theorem 6.2 above. The only contributing polynomials in  $\Psi$  are  $f_{\tau}$  with  $\tau = 0, \pm 1$ .*

The roots of these polynomials and the fields they generate over  $\mathbf{Q}(\sqrt{m})$  are shown below.

$\tau$	Roots $a_{\tau}, a'_{\tau}$ of $f_{\tau}$	$F(a_{\tau})$
0	$\zeta_4, \zeta_4^3$	$\mathbf{Q}(\sqrt{m}, \zeta_4)$
1	$\zeta_6, \zeta_6^5$	$\mathbf{Q}(\sqrt{m}, \zeta_6)$
-1	$\zeta_6^2, \zeta_6^3$	$\mathbf{Q}(\sqrt{m}, \zeta_6)$

5. We proceed to the last step of the algorithm: finding the orders  $\mathcal{S}_a$ . Condition (5.a) says that  $R[a_\tau]$  must be contained in  $\mathcal{S}_a$ . However, we find that  $R[a_\tau]$  is the maximal order of  $F(a_\tau)$ .

**Lemma 6.4.** *Let  $m$  be as in Theorem 6.2,  $R$  the ring of integers of  $\mathbf{Q}(\sqrt{m})$  and  $u$  a fundamental unit in  $R$ . Then*

- (a) *The ring of integers of  $\mathbf{Q}(\sqrt{m}, \zeta_4)$  is  $R[\zeta_4]$  and  $R[\zeta_4]^\times = \langle \zeta_4 \rangle \langle u \rangle$ .*  
(b) *The ring of integers of  $\mathbf{Q}(\sqrt{m}, \zeta_6)$  is  $R[\zeta_6]$  and  $R[\zeta_6]^\times = \langle \zeta_6 \rangle \langle u \rangle$ .*

*Proof.* (a) Let  $S$  denote the ring of integers in  $K = \mathbf{Q}(\sqrt{m}, \zeta_4)$ . Then by [Ma, Ex 42 pg 51] we have  $S = R[\zeta_4]$ . Now let  $\alpha = \omega_1 + \omega_2 \zeta_4 \in S$ . We compute

$$N_{K/\mathbf{Q}}(\alpha) = N_{F/\mathbf{Q}}(\omega_1)^2 + (\omega_1^\sigma \omega_2)^2 + (\omega_1 \omega_2^\sigma)^2 + N_{F/\mathbf{Q}}(\omega_2)^2$$

where  $\sigma$  is the non-trivial element of  $\text{Gal}(F/\mathbf{Q})$ . Hence we deduce that  $\alpha$  is a unit if and only if either,  $\omega_1 = 0$  and  $N_{F/\mathbf{Q}}(\omega_2) = \pm 1$ , or  $\omega_2 = 0$  and  $N_{F/\mathbf{Q}}(\omega_1) = \pm 1$ . The result now follows.

(b) Let  $S$  denote the ring of integers in  $K = \mathbf{Q}(\sqrt{m}, \zeta_6)$ . Then by [Ma, Ex 42 pg 51] we have  $S = R[\zeta_6]$ , since  $3 \nmid m$  as  $\mathbf{Q}(\sqrt{m})$  has narrow class number one. Let  $\alpha = a + b\theta + c\zeta_6 + d\theta\zeta_6 \in S$  where  $\theta = \frac{1+\sqrt{m}}{2}$ . We compute

$$16N_{K/\mathbf{Q}}(\alpha) = N_{F/\mathbf{Q}}(\omega_1)^2 + 3((\omega_1\omega_2^\sigma)^2 + (\omega_1^\sigma\omega_2)^2) + 9N_{F/\mathbf{Q}}(\omega_2)^2$$

where  $\omega_1 = 2a + c + (2b + d)\theta$ ,  $\omega_2 = c + d\theta$  and  $\sigma$  is the non-trivial element of  $\text{Gal}(F/\mathbf{Q})$ . Assume that  $\alpha \in S^\times$ . Then we have  $N_{F/\mathbf{Q}}(\omega_2) = 0$  or  $\pm 1$ . If  $N_{F/\mathbf{Q}}(\omega_2) = 0$  then  $\alpha \in R^\times$ . Now assume that  $N_{F/\mathbf{Q}}(\omega_2) = \pm 1$ . In this case we must have  $N_{F/\mathbf{Q}}(\omega_1) = \pm 1$  since  $N_{F/\mathbf{Q}}(\omega_1) \equiv N_{F/\mathbf{Q}}(\omega_2) \pmod{2}$  rules out the possibility that  $N_{F/\mathbf{Q}}(\omega_1) = \pm 2$ . So we can write  $\omega_1 = \pm u^r$  and  $\omega_2 = \pm u^s$ . Now  $\alpha$  is a unit if and only if

$$16 = 1 + 3((\omega_1\omega_2^\sigma)^2 + (\omega_1^\sigma\omega_2)^2) + 9$$

that is, if and only if

$$2 = u^{2(r-s)} + u^{-2(r-s)}.$$

This is true if and only if  $r = s$ . Thus, we deduce that if  $N_{F/\mathbf{Q}}(\omega_2) = \pm 1$ , then  $\alpha$  is a unit in  $S$  if and only if

$$\alpha = \frac{\omega_1 - \omega_2}{2} + \omega_2 \zeta_6 = u^r \zeta_6^k$$

with  $k \in \{1, 2, 4, 5\}$ . The result now follows.  $\square$

**Lemma 6.5.** *The set of orders  $C$  consists of the rings of integers  $\mathcal{S}$  of the extensions  $F(a_\tau)$  where  $a_\tau$  is a chosen root of a contributing polynomial  $f_\tau$  as determined by Lemma 6.3.*

*Proof.* Only condition (5.b) needs to be verified. Our computations show that all of the roots  $a_\tau$  of  $f_\tau$  are roots of unity and  $N_{F(a_\tau)/F}(a_\tau) = 1$ . Thus  $s_{\mathfrak{p}} = 0$  for every  $\mathfrak{p}$  and  $a_\tau \in \mathcal{S}_{a_\tau, \mathfrak{p}}$  is always satisfied.  $\square$

Hence, equation (2) becomes:

$$T = M + \frac{1}{2} \sum_{\mathcal{S}_{a_\tau} \in C} \frac{h(\mathcal{S}_{a_\tau})}{w(\mathcal{S}_{a_\tau})}$$

We now study the contributions in this sum from the biquadratic fields (1)  $\mathbf{Q}(\sqrt{m}, \sqrt{-1})$  and (2)  $\mathbf{Q}(\sqrt{m}, \sqrt{-3})$ . For this we need the following result due to Hasse from [Has].

**Proposition 6.6.** *Let  $m_1, m_2$  be negative squarefree integers and set  $m_0 = m_1 m_2$ . For each  $i$  we set  $F_i = \mathbf{Q}(\sqrt{m_i})$ ,  $w_i$  the number of roots of unity in  $F_i$ ,  $h_i$  the order of the class group of  $F_i$ . Let  $K = \mathbf{Q}(\sqrt{m_1}, \sqrt{m_2})$ ,  $h$  the order of the class group of  $K$ ,  $w$  the number of roots of unity in  $K$  and  $u$  the fundamental unit in  $K$ . Let  $u_0$  be the fundamental unit of  $F_0$ . Then*

$$h = \frac{w}{w_1 w_2} h_0 h_1 h_2 \frac{\log(u_0)}{\log(|u|)}.$$

From this Proposition, we get the following.

1. For  $\mathbf{Q}(\sqrt{m}, \sqrt{-1})$ : Let  $m_1 = -1, m_2 = -m, m_0 = m, K = \mathbf{Q}(\sqrt{-1}, \sqrt{-m})$ . Hence  $h_0 = 1$ , by hypothesis. It is well known that the class group order of  $\mathbf{Q}(\sqrt{-1})$  is 1, and the only roots of unity are powers of  $\sqrt{-1}$ , i.e.  $h_1 = 1, w_1 = 4$ . Also, the only roots of unity in  $\mathbf{Q}(\sqrt{-m}), m \neq 1, 3$ , are  $\pm 1$ , i.e.  $w_2 = 2$ . Then,  $w = 4$  and  $u_0 = u$ . So we obtain  $h = \frac{1}{2} h(\sqrt{-m})$ .
2. For  $\mathbf{Q}(\sqrt{m}, \sqrt{-3})$ : Let  $m_1 = -3, m_2 = -3m, m_0 = 9m, K = \mathbf{Q}(\sqrt{-3}, \sqrt{-3m})$ . Similarly, it is known that the class group order of  $\mathbf{Q}(\sqrt{-3})$  is 1, and the only roots of unity are powers of  $\zeta_6$ , i.e.,  $h_1 = 1, w_1 = 6$ . Then,  $w = 6$  and  $u_0 = u$ . Again  $w_2 = 2$  and we obtain  $h = \frac{1}{2} h(\sqrt{-3m})$ .

Next,  $[\mathcal{S}^\times : U] = 2$  and  $3$ , respectively, for  $\mathbf{Q}(\sqrt{m}, \sqrt{-1})$  and  $\mathbf{Q}(\sqrt{m}, \sqrt{-3})$ . We can now finish proving Theorem 6.2. The field  $\mathbf{Q}(\sqrt{m}, \sqrt{-3})$  contributes twice in the sum (for  $\tau = 1, -1$ ), so equation (2) becomes:

$$\begin{aligned} T &= M + \frac{1}{2} \left( \frac{h(\mathbf{Q}(\sqrt{m}, \sqrt{-1}))}{2} + 2 \frac{h(\mathbf{Q}(\sqrt{m}, \sqrt{-3}))}{3} \right) \\ &= M + \frac{1}{8} h(\mathbf{Q}(\sqrt{-m})) + \frac{1}{6} h(\mathbf{Q}(\sqrt{-3m})) \end{aligned}$$

and this completes the proof of theorem 6.2.  $\square$

We can also determine  $H$ . Following the proof of Theorem 6.1 in [Pi1], we see that

$$T_{q_1 q_2} = \frac{1}{2^e h(F)} \left( H_{q_1 q_2} + \frac{1}{2} \sum_{\mathcal{S}_a \in C_2} E_{q_1 q_2}(\mathcal{S}_a) \frac{h(\mathcal{S}_a)}{w(\mathcal{S}_a)} \right), \quad (3)$$

where  $C_2 = C - C_1$ , and  $C_1 = \{ \mathcal{S}_a \in C \mid (N(a)) = (1) \}$ . That is,  $a$  is a root of  $f_{\mu, \varrho, \tau}(x)$  with  $(n_\mu) = (1)$ . From this, we have

**Proposition 6.7.** *Let  $m$  be a positive squarefree integer,  $F = \mathbf{Q}(\sqrt{m})$ , with  $h(F) = 1$ , and  $\mathbf{B}$  the unique quaternion algebra with  $\text{Ram}(\mathbf{B}) = \{\infty_1, \infty_2\}$ . Then  $H = T$ . Consequently, if  $I_1, \dots, I_H$  is a complete set of representatives of distinct left  $\mathcal{O}$ -ideal classes for a fixed maximal order  $\mathcal{O}$ , then the corresponding right orders  $\mathcal{O}_r(I_1), \dots, \mathcal{O}_r(I_H)$  form a complete set of distinct representatives of maximal orders of different types.*

*Proof.* We have  $h(F) = 1$ ,  $q_1 = q_2 = 1$ ,  $2^e = 1$  and  $n_\mu = n_1 = 1$  in the algorithm to find  $C$ . Thus  $C_2 = \emptyset$ . Substitute these in (3) to get the result.  $\square$

## 7 The Algebra $\mathbf{B}$ and a Maximal Order $\mathcal{O}$

In this section we obtain defining relations for  $\mathbf{B}$ , the positive definite quaternion algebra over  $F = \mathbf{Q}(\sqrt{m})$  which is ramified precisely at the infinite places of  $F$ . We also find a basis over  $R$  for a maximal order  $\mathcal{O}$  in  $\mathbf{B}$  when  $m \equiv 5 \pmod{8}$ .

**Definition 7.1.** *Over a field  $K$  of characteristic not equal to two, let  $(a, b)$  for  $a, b \in K^\times$  denote the quaternion algebra over  $K$  with basis  $\{1, i, j, k\}$  and relations  $k = ij$ ,  $i^2 = a$ ,  $j^2 = b$  and  $ij = -ji$ .*

**Proposition 7.2.** *Let  $m \not\equiv 1 \pmod{8}$  be a positive squarefree integer. Then  $\mathbf{B} = (-1, -1)$  is the unique quaternion algebra defined over  $\mathbf{Q}(\sqrt{m})$  which is ramified precisely at the infinite places of  $\mathbf{Q}(\sqrt{m})$ .*

*Proof.* It is clear that  $\mathbf{B} = (-1, -1)$  is positive definite. We shall show that at every finite prime  $\mathfrak{p}$  of  $F$  the algebra  $\mathbf{B}_\mathfrak{p} = \mathbf{B} \otimes_F F_\mathfrak{p}$  is the matrix algebra. Let  $\mathbf{B}'$  be the quaternion algebra over  $\mathbf{Q}$  given by  $\mathbf{B}' = (-1, -1)$ . Then  $\mathbf{B} = \mathbf{B}' \otimes_{\mathbf{Q}} F$ . As is well known  $\text{Ram}(\mathbf{B}') = \{2, \infty\}$ . Hence  $\mathbf{B}$  is split at every prime  $\mathfrak{p}$  of  $F$  not above 2. Since  $m \not\equiv 1 \pmod{8}$  there is only one prime in  $F$  lying above 2. But now  $\text{Ram}(\mathbf{B})$  has even cardinality and contains the two infinite places of  $F$  and hence  $\mathbf{B}$  must be unramified at the prime of  $F$  above 2.  $\square$

In the case that  $F = \mathbf{Q}(\sqrt{m})$  has narrow class number one and  $m \equiv 1 \pmod{8}$  one can take  $\mathbf{B}'$  to be the quaternion algebra over  $\mathbf{Q}$  ramified precisely at  $\{m, \infty\}$ . By [Pi3, Proposition 5.1], one has  $\mathbf{B}' = (-m, -q)$  where  $q$  is a prime with  $q \equiv 3 \pmod{4}$  and  $\left(\frac{m}{q}\right) = -1$ . The same argument as above shows that  $\mathbf{B} = \mathbf{B}' \otimes_{\mathbf{Q}} F$ . We now give a maximal order  $\mathcal{O}$  in  $\mathbf{B}$  when  $m \equiv 5 \pmod{8}$ .

**Proposition 7.3.** *Let  $m \equiv 5 \pmod{8}$  be a positive squarefree integer. Let  $F = \mathbf{Q}(\sqrt{m})$  with ring of integers  $R = \mathbf{Z}[\theta]$ , where  $\theta = \frac{1+\sqrt{m}}{2}$ . Let  $\mathbf{B} = (-1, -1)$ . Then  $\mathcal{O} = R[\delta_1, \delta_2, j, k]$  is a maximal order in  $\mathbf{B}$ , where  $\delta_1 = \frac{1+i+j+k}{2}$  and  $\delta_2 = \frac{i+\theta j+(1+\theta)k}{2}$ .*

*Proof.* It is clear that  $\mathcal{O}$  is a full lattice in  $\mathbf{B}$ . It is simple, but tedious, to check that  $\mathcal{O}$  is a ring and that every element of  $\mathcal{O}$  is integral. Finally one can check that  $\mathcal{O}$  is maximal by computing its discriminant. For all the details see [Soc, Theorem 4.2].  $\square$

## 8 Cusp Form Calculations

In this section we compute the space of cusp forms for the field  $F = \mathbf{Q}(\sqrt{509})$ . From Theorem 6.2 and Proposition 6.7 we compute that the class number for  $\mathbf{B}$  is 24. We will give representatives for each of the 24 ideal classes which will then enable us to compute the necessary Brandt matrices using the algorithm from Section 3.

In the algorithm of Section 5, we first find suitable  $\alpha$ . The  $\alpha$  which eventually led us to distinct ideal classes were  $i$  together with  $\alpha_1$  and  $\alpha_2$  below.

$$\begin{aligned}
\alpha_1 &= \frac{1}{2} + 5i + \frac{1+\theta}{2}j + (1 - \frac{1}{2}\theta)k \\
&= \delta_1 + 9\delta_2 - 4\theta j - (4 + 5\theta)k \\
\mathbf{nr}(\alpha_1) &= 90 \\
k_1 &= -359 \\
h(\mathbf{Q}(\sqrt{-359})) &= 19 \\
\alpha_2 &= \frac{1}{2} + (4 - \frac{1}{2}\theta)i + 2j + \frac{7+\theta}{2}k \\
&= \delta_1 + (7 - \theta)\delta_2 + (65 - 3\theta)j + (63 - 2\theta)k \\
\mathbf{nr}(\alpha_2) &= 96 \\
k_2 &= -383 \\
h(\mathbf{Q}(\sqrt{-383})) &= 17
\end{aligned}$$

Let  $K = F(\alpha_i)$  then we note that  $R[\sqrt{k_i}]$  has index 2 in the ring of integers of  $K$ . We set  $\alpha'_i = 2\alpha_i - 1$ , which satisfies  $x^2 - k_i = 0$ . Since  $F$  has class number one, we will be interested only in prime ideals of  $F$  which split in  $K$ . If  $x^2 - k_i$  splits into two distinct factors  $(x - \beta_1)(x - \beta_2)$  modulo the prime ideal  $\mathfrak{p} = (a + b\theta)$  of  $F$ , then as an ideal in  $K$

$$\mathfrak{p} = (a + b\theta, \alpha'_i - \beta_1)(a + b\theta, \alpha'_i - \beta_2)$$

and it suffices to consider only one of the ideals  $I$  on the right, as they belong to the same  $K$ -ideal class. Moreover we have  $\mathbf{nr}(\mathcal{O}I) = (a + b\theta)$ .

Since the class number of  $\mathcal{O}$  is rather large, we first used the  $\Theta$ -series of  $\mathcal{O}I$  for various prime ideals  $I$  in the extensions  $K = F(\alpha_i)$  above. We computed the  $\Theta$ -series of these ideals up to  $30 + 2\theta$ . Using this method we found 23 of the 24 ideal classes. These ideals, together with the initial coefficients of their  $\Theta$ -series are listed in the tables below.

After a lengthy search which did not yield another ideal with a distinct  $\Theta$ -series, we switched to using the necessary and sufficient conditions of Proposition 5.2. Let  $I$  be an ideal in  $S$  the ring of integers in some  $F(\alpha_i)$ . Assume that the initial coefficients of the  $\Theta$ -series of  $\mathcal{O}I$  are the same as those of one of the left ideals above, say  $J_s$ . Construct a basis for  $I' = I^{-1}J_s$ , and construct  $\mathcal{N}_{I'}(\alpha) = \Psi_1(X) + \Psi_2(X)\theta$ , with  $\Psi_1$  in Hermite normal form. Proposition 5.2 then says that  $\mathcal{O}I$  is actually in a *different* class as  $J_s$  if and only if  $a_{1,1}$ , the leading term of  $\Psi_1$ , is greater than 1. (Note that  $1 + b\theta$  is totally positive if and only if  $b = 0$ ). Using this condition, we quickly determined that we could take  $J_{24} = \mathcal{O}I_{24}$  with

$$I_{24} = (46 + 5\theta, 334 - 10i - (1 + \theta)j + (-2 + \theta)k)$$

a prime ideal in  $F(\alpha_1)$  dividing 829.

Now that we have concrete representatives of left ideal classes, we are able to explicitly construct the first few Brandt matrices  $B(\xi)$  and the modified Brandt matrices  $B'(\xi)$  using the algorithm [Co1, Algorithm 2.7.7] mentioned at the end of Section 3. This involves computing the  $\Theta$ -series of the 300 ideals  $J_r^{-1}J_s$ ,  $r \geq s$ , due to the symmetry properties in Theorem 4.1. We also computed the characteristic polynomials of the  $B'(\xi)$  and factored them over  $\mathbf{Q}$ . We found that the characteristic polynomial of  $B'(19 + \theta)$  had three distinct rational roots and an irreducible factor of degree 20. Hence, although  $\mathbf{C}^{23}$  has a basis of eigenvectors for all the  $B'(\xi)$ , only three eigenvectors have eigenvalues which are all rational. The three rational eigenvectors are

$$\mathbf{v}_1 = (0, 0, 0, 0, 1, 0, -2, -1, 1, 1, 0, -2, 0, 0, -3, 1, 0, 0, 0, -1, 2, 0, 2)$$

$$\mathbf{v}_2 = (0, 0, 0, 0, -1, 0, 2, 1, -1, 1, 0, 2, 0, 0, -2, -1, 0, 0, 0, 1, -2, 0, 3)$$

$$\mathbf{v}_3 = (45, 45, 25, 60, 23, 40, 34, 27, 18, 28, 30, 19, 35, 20, 31, 28, 20, 15, 25, 37, 51, 40, 31).$$

We let  $\mathbf{f}_1, \mathbf{f}_2$  and  $\mathbf{f}_3$  denote the forms corresponding to the vectors  $\mathbf{v}_1, \mathbf{v}_2$  and  $\mathbf{v}_3$  by Proposition 4.3. The initial Fourier coefficients of these forms are tabulated in Table 5. From this table we note that  $\mathbf{f}_1 = \mathbf{f}_2^\sigma$  where  $\sigma$  is the non-trivial element of  $\text{Gal}(F/\mathbf{Q})$ , while  $\mathbf{f}_3 = \mathbf{f}_3^\sigma$  and hence  $\mathbf{f}_3$  is the base change of a classical form. That none of these forms are CM forms follows from the following Proposition.

**Proposition 8.1.** *Let  $\mathbf{f}$  be a Hilbert eigenform of full level for a totally real number field  $F$  of narrow class number one. Then  $\mathbf{f}$  is not a CM form.*

*Proof.* Recall that  $\mathbf{f}$  is a CM form if and only if there exists a quadratic character  $\varepsilon$  corresponding to an imaginary quadratic extension  $K/F$  such that  $\mathbf{f} = \mathbf{f} \otimes \varepsilon$ . So suppose we have  $\mathbf{f} = \mathbf{f} \otimes \varepsilon$  for such a character  $\varepsilon$ . Let  $\pi$  denote the cuspidal

representation of  $\mathrm{GL}_2(\mathbf{A}_F)$  corresponding to  $\pi$ . Then we have  $\pi \cong \pi \otimes (\varepsilon \circ \det)$ . By a theorem of Labesse and Langlands [LL] we have an equality of  $L$ -series  $L(\pi, s) = L(\chi, s)$  for some grössencharacter  $\chi$  of  $K$ , and it is known that

$$\mathrm{cond}(\pi) = N_{K/F}(\mathrm{cond}(\chi)) \mathrm{disc}(K/F).$$

Since  $\pi$  is assumed to be unramified it follows that  $K/F$  is an unramified extension. But this is impossible since  $F$  has narrow class number one.  $\square$

$I_i$	$K$	$a_i + b_i\theta$	$\gamma_i$	$I_i \mid p \in \mathbf{Z}$
$I_1$	$F$	1		
$I_2$	$F(\alpha_1)$	61	$-23 + 46\theta - 10i - (1 + \theta)j + (-2 + \theta)k$	61
$I_3$	$F(\alpha_1)$	$45 + 4\theta$	$81 - 10i - (1 + \theta)j + (-2 + \theta)k$	173
$I_4$	$F(\alpha_1)$	149	$45 - 10i - (1 + \theta)j + (-2 + \theta)k$	149
$I_5$	$F(\alpha_1)$	$53 + 5\theta$	$34 - 10i - (1 + \theta)j + (-2 + \theta)k$	101
$I_6$	$F(\alpha_1)$	79	$6 - 10i - (1 + \theta)j + (-2 + \theta)k$	79
$I_7$	$F(\alpha_1)$	53	$-22 + 44\theta - 10i - (1 + \theta)j + (-2 + \theta)k$	53
$I_8$	$F(\alpha_2)$	$23 + 2\theta$	$32 + (-8 + \theta)i - 4j - (7 + \theta)k$	67
$I_9$	$F(\alpha_1)$	$9 + \theta$	$14 - 10i - (1 + \theta)j + (-2 + \theta)k$	37
$I_{10}$	$F(\alpha_1)$	$10 + \theta$	$7 - 10i - (1 + \theta)j + (-2 + \theta)k$	17
$I_{11}$	$F(\alpha_1)$	$184 + 17\theta$	$22 - 10i - (1 + \theta)j + (-2 + \theta)k$	281
$I_{12}$	$F(\alpha_1)$	$107 + 10\theta$	$33 - 10i - (1 + \theta)j + (-2 + \theta)k$	181
$I_{13}$	$F(\alpha_2)$	47	$-18 + 36\theta + (-8 + \theta)i - 4j - (7 + \theta)k$	47
$I_{14}$	$F(\alpha_1)$	31	$-1 + 2\theta - 10i - (1 + \theta)j + (-2 + \theta)k$	31
$I_{15}$	$F(\alpha_1)$	$32 + 3\theta$	$3 - 10i - (1 + \theta)j + (-2 + \theta)k$	23
$I_{16}$	$F(\alpha_1)$	131	$54 - 10i - (1 + \theta)j + (-2 + \theta)k$	131
$I_{17}$	$F(\alpha_1)$	59	$-14 + 28\theta - 10i - (1 + \theta)j + (-2 + \theta)k$	59
$I_{18}$	$F(\alpha_2)$	61	$-26 + 52\theta + (-8 + \theta)i - 4j - (7 + \theta)k$	61
$I_{19}$	$F(i)$	$31 + 3\theta$	$34 + i$	89
$I_{20}$	$F(\alpha_1)$	$75 + 7\theta$	$15 - 10i - (1 + \theta)j + (-2 + \theta)k$	73
$I_{21}$	$F(\alpha_1)$	13	$-3 + 6\theta - 10i - (1 + \theta)j + (-2 + \theta)k$	13
$I_{22}$	$F(\alpha_1)$	157	$-6 + 12\theta - 10i - (1 + \theta)j + (-2 + \theta)k$	157
$I_{23}$	$F(i)$	$11 + \theta$	$2 + i$	5

Table 1: Prime Ideals  $I_i = (a_i + b_i\theta, \gamma_i)$ , where  $\mathcal{O}I_i$  have distinct  $\Theta$ -series

	1	2	3	4	5	6	7	8	9	10	11	$11 + \theta$	$12 - \theta$	12
$J_1$	24	24	96	24	144	96	192	24	312	144	288	0	0	96
$J_2$	0	24	0	24	0	96	0	24	0	144	0	0	0	96
$J_3$	0	0	24	0	0	24	0	0	96	0	0	0	0	24
$J_4$	0	0	0	24	0	0	0	24	0	0	0	0	0	96
$J_5$	0	0	0	24	0	0	0	24	0	0	0	0	0	96
$J_6$	0	0	0	0	24	0	0	0	0	24	0	0	0	0
$J_7$	0	0	0	0	24	0	0	0	0	24	0	0	0	0
$J_8$	0	0	0	0	24	0	0	0	0	24	0	0	0	0
$J_9$	0	0	0	0	0	24	0	0	0	0	24	0	0	24
$J_{10}$	0	0	0	0	0	24	0	0	0	0	0	0	0	48
$J_{11}$	0	0	0	0	0	0	24	0	0	24	0	0	0	24
$J_{12}$	0	0	0	0	0	0	24	0	0	24	0	0	0	0
$J_{13}$	0	0	0	0	0	0	24	0	0	0	48	0	0	0
$J_{14}$	0	0	0	0	0	0	24	0	0	0	48	0	0	0
$J_{15}$	0	0	0	0	0	0	0	24	24	0	0	0	0	48
$J_{16}$	0	0	0	0	0	0	0	24	0	24	24	0	0	24
$J_{17}$	0	0	0	0	0	0	0	24	0	24	48	0	0	0
$J_{18}$	0	0	0	0	0	0	0	24	0	48	0	0	0	0
$J_{19}$	0	0	0	0	0	0	0	48	0	0	0	0	0	0
$J_{20}$	0	0	0	0	0	0	0	0	24	48	48	0	0	0
$J_{21}$	0	0	0	0	0	0	0	0	48	24	0	0	0	24
$J_{22}$	0	0	0	0	0	0	0	0	48	0	48	0	0	0
$J_{23}$	0	0	0	0	0	0	0	0	0	48	48	24	24	48

Table 2: Beginning Coefficients  $c_{\xi, J_i}$  of the  $\Theta$ -series of  $J_1$  to  $J_{23}$

	$12 + \theta$	$13 - \theta$	13	$13 + \theta$	$14 - \theta$	14	$14 + \theta$	$15 - \theta$	15	$15 + \theta$
$J_4$	0	0	0	0	0	0	0	0	0	0
$J_5$	0	0	0	0	0	0	0	0	0	0
$J_6$	0	0	24	0	0	0	0	0	96	0
$J_7$	0	0	0	0	0	24	0	0	144	24
$J_8$	0	0	0	0	0	48	0	0	96	0
$J_{13}$	0	0	48	0	0	24	48	48	0	0
$J_{14}$	0	0	24	24	24	48	0	0	24	24

Table 3: continued, for ideals with the same coefficients in the  $\Theta$ -series above

	$16 - \theta$	16	$16 + \theta$	$17 - \theta$	17	$17 + \theta$	$18 - \theta$	18	$18 + \theta$
$J_4$	0	24	0	0	48	0	0	24	24
$J_5$	0	48	0	0	0	0	0	0	0

Table 4: continued, for  $J_4$  and  $J_5$ .

$\xi$	3	7	$11 + \theta$	$12 - \theta$	$12 + \theta$	$13 - \theta$	13	$14 + \theta$	$15 - \theta$	$15 + \theta$	$16 - \theta$
$\xi   p$	3	7	5	5	29	29	13	83	83	113	113
$\mathbf{v}_1$	-4	-6	3	-2	0	10	1	14	9	11	6
$\mathbf{v}_2$	-4	-6	-2	3	10	0	1	9	14	6	11
$\mathbf{v}_3$	1	9	-2	-2	-5	-5	26	14	14	11	11

Table 5: Eigenvalues for simultaneous rational eigenvectors for  $B'(\xi)$

## 9 The Elliptic Curves

In this section we give equations for the elliptic curves that we will show are attached to the forms  $\mathbf{f}_1$ ,  $\mathbf{f}_2$  and  $\mathbf{f}_3$  of the previous section.

Let  $E_3$  be the elliptic curve given by the Weierstrass equation

$$y^2 + (1+\theta)xy + (1+\theta)y = x^3 + (-4051846 + 343985\theta)x + 4312534180 - 366073300\theta.$$

This curve is found in [Cre] and is a  $\mathbf{Q}$ -curve (i.e. it is isogenous to its Galois conjugate). Let  $E_1$  denote the elliptic curve given by the Weierstrass equation

$$y^2 - xy - \theta y = x^3 + (2 + 2\theta)x^2 + (162 + 3\theta)x + 71 + 34\theta.$$

This elliptic curve is in a table found in Pinch's thesis ([Pin]), among other curves which have good reduction everywhere over certain quadratic fields. We show below that  $E_1$  is not  $F$ -isogenous to its Galois conjugate. This is also noted (without proof) in [Cre]. We take  $E_2$  to be the curve  $E_1^\sigma$  where  $\sigma$  is the non-trivial element of  $\text{Gal}(F/\mathbf{Q})$ .

**Proposition 9.1.** *The elliptic curve  $E_1$  is not isogenous over  $F$  to its Galois conjugate.*

*Proof.* We note that if  $E_1$  and  $E_1^\sigma$  are isogenous then the local factors of the  $L$ -series of  $E_1$  and  $E_1^\sigma$  will be the same for all primes of  $F$ . Let  $\mathfrak{p} = (5, 1 + 2\theta)$  denote one of the prime ideals of  $F$  above 5. We have an isomorphism of  $R/\mathfrak{p}$  with  $\mathbf{Z}/5$  that maps  $\theta$  to 2 mod 5. Then the equation for the reduced curve  $\tilde{E}_1$  over  $\mathbf{Z}/5$  has affine equation

$$\tilde{E}_1 : y^2 + 4xy + 3y = x^3 + x^2 + 3x + 4.$$

and we compute that  $\tilde{E}_1(R/\mathfrak{p})$  has order 8. Similarly, the reduction of the curve  $E_1^\sigma$  has equation

$$\tilde{E}_1^\sigma : y^2 + 4xy + y = x^3 + 4x + 2.$$

and we compute that  $\tilde{E}_1^\sigma(R/\mathfrak{p})$  has order 3. Therefore we conclude that  $E_1$  is not isogenous to  $E_1^\sigma$ .  $\square$

Finally we check that our curves  $E_1$ ,  $E_2$  and  $E_3$  do not possess potential complex multiplication. We first remark that  $h^+(F) = 1$ . Our conclusion about these curves is now a consequence of the following.

**Proposition 9.2.** *Let  $K$  be a totally real number field of narrow class number one. Let  $E/K$  be an elliptic curve which has good reduction everywhere. Then  $E$  does not possess potential complex multiplication.*

*Proof.* Suppose  $E(\mathbf{C})$  has CM defined over the field  $\mathbf{Q}(\sqrt{n})$ , where  $n < 0$ . Consider the field  $L = K(\sqrt{n})$ . Then  $E$  and its complex multiplications are

defined over  $L$ . Consider the  $\ell$ -adic representation given by the action of Galois on the  $\ell$ -adic Tate module of  $E/L$

$$\sigma_\ell : \text{Gal}(\overline{\mathbf{Q}}/L) \rightarrow GL_2(\mathbf{Q}_\ell).$$

We construct another representation

$$\begin{array}{ccc} \sigma_\ell^{[\rho]} & : & \text{Gal}(\overline{\mathbf{Q}}/L) \rightarrow GL_2(\mathbf{Q}_\ell) \\ & & \tau \mapsto \sigma_\ell(\rho\tau\rho^{-1}) \end{array}$$

where  $\rho \in \text{Gal}(\overline{\mathbf{Q}}/K)$  is non-trivial when restricted to  $L$ . Now, since  $E$  is actually defined over  $K$ ,  $\sigma_\ell$  extends to a representation  $\tilde{\sigma}_\ell$  of  $\text{Gal}(\overline{\mathbf{Q}}/K)$ . However, we note that

$$\tilde{\sigma}_\ell(\rho\tau\rho^{-1}) = \tilde{\sigma}_\ell(\rho)\tilde{\sigma}_\ell(\tau)\tilde{\sigma}_\ell(\rho)^{-1} = \tilde{\sigma}_\ell(\rho)\sigma_\ell(\tau)\tilde{\sigma}_\ell(\rho)^{-1}$$

and hence  $\sigma_\ell^{[\rho]} \cong \sigma_\ell$ .

Since  $E$  has CM over  $L$ , the representation  $\sigma_\ell$  is abelian, so  $\sigma_\ell = \chi_\ell \oplus \chi'_\ell$  for some characters  $\chi_\ell, \chi'_\ell$  of  $H$ . It can easily be seen from such a decomposition that, in the obvious notation,  $\sigma_\ell^{[\rho]} = \chi_\ell^{[\rho]} \oplus \chi'_\ell^{[\rho]}$  as well. Now,  $\chi_\ell$  corresponds to a weight 1 grossencharacter  $\psi$  of  $L$ , and  $\chi_\ell = \chi_\ell^{[\rho]}$  if and only if  $\psi(z) = \psi(\bar{z})$  for all  $z \in L_\infty^* = \mathbf{C}^*$ . But  $\psi(z) = z^{-1}$  and  $\psi(\bar{z}) = \bar{z}^{-1}$ , hence  $\psi(z) \neq \psi(\bar{z})$ , so  $\chi_\ell \neq \chi_\ell^{[\rho]}$ . Thus  $\chi'_\ell = \chi_\ell^{[\rho]}$ , and so  $\sigma_\ell = \chi_\ell \oplus \chi_\ell^{[\rho]}$ , hence  $\tilde{\sigma}_\ell = \text{Ind}_H^G(\chi_\ell)$ . Since the degree of  $\chi_\ell$  is 1, we get the formula for the conductor of  $\tilde{\sigma}_\ell$

$$\text{cond}(\tilde{\sigma}_\ell) = N_{L/K}(\text{cond}(\chi_\ell))\text{disc}(L/K)$$

(see [Mar]). Recall, that  $E$  has good reduction everywhere, so every  $\tilde{\sigma}_\ell$  is unramified at all the primes of  $K$  not dividing  $\ell$ . Since  $\tilde{\sigma}_\ell$  is ramified at all the primes which divide  $\text{cond}(\tilde{\sigma}_\ell)$ , we see that  $\text{disc}(L/K)$  must be the unit ideal. Thus  $L$  is an unramified finite abelian extension of  $K$ . But since  $h^+(K) = 1$  this implies that  $K = L$  which is impossible since  $n < 0$ .  $\square$

## 10 Matching the Elliptic Curves to the Cusp Forms

Continuing with the notation of the previous section we have  $F = \mathbf{Q}(\sqrt{509})$ ,  $R$  the ring of integers in  $F$  and  $\theta = \frac{1+\sqrt{509}}{2}$ .

We begin by showing that the curve  $E_3$  is attached to the form  $\mathbf{f}_3$ . The curve  $E_3$  is equal to the curve  $A'$  which arises from Shimura's construction in [Shi, 7.7]. This curve is constructed from a pair of eigenforms  $\{f_1, f_2\}$  in  $S_2(\Gamma_0(509), \chi)$  where  $\chi$  is the quadratic character of  $(\mathbf{Z}/509\mathbf{Z})^\times$ . These forms are constructed in [Cre]. Furthermore we know that we have

$$L(E_3, s) = L(f_1, s)L(f_2, s).$$

The base change of  $f_1$  to  $\mathrm{GL}_2(F)$  will be a form with rational coefficients of full level, trivial character and weight 2. Hence we see that  $\mathbf{f}_3$  is the base change of the form  $f_1$  and we have

$$L(E_3, s) = L(\mathbf{f}_3, s).$$

Let  $E_1$  be as in Section 9. Since  $E_1$  has good reduction everywhere the 2-adic representation on the Tate module of  $E_1$

$$\sigma_1 : \mathrm{Gal}(\overline{F}/F) \rightarrow \mathrm{GL}_2(\mathbf{Q}_2)$$

is unramified outside of the prime ideal  $2R$  of  $F$ . For each prime ideal  $\mathfrak{p}$  of  $F$  outside  $2R$  we have

$$\mathrm{Tr}(\sigma_1(\mathrm{Fr}_{\mathfrak{p}})) = a(E_1)_{\mathfrak{p}}$$

where  $\mathrm{Fr}_{\mathfrak{p}}$  denotes a Frobenius element at  $\mathfrak{p}$  and  $a(E_1)_{\mathfrak{p}}$  denotes the  $\mathfrak{p}^{\mathrm{th}}$  Fourier coefficient of  $E_1$ . Moreover  $\det \sigma_1(\mathrm{Fr}_{\mathfrak{p}}) = N\mathfrak{p}$ .

Let  $\mathbf{f}_1$  denote the unramified cusp form given in Section 8 above. By the work of Taylor [Tay] and independently of Blasius and Rogawski [BR] there exists a 2-dimensional representation

$$\sigma_2 : \mathrm{Gal}(\overline{F}/F) \rightarrow \mathrm{GL}_2(\mathbf{Q}_2)$$

unramified outside the prime ideal  $2R$  of  $F$  and such that for each prime ideal  $\mathfrak{p}$  of  $F$  outside  $2R$  we have

$$\mathrm{Tr}(\sigma_2(\mathrm{Fr}_{\mathfrak{p}})) = a(\mathbf{f}_1)_{\mathfrak{p}}$$

where again  $\mathrm{Fr}_{\mathfrak{p}}$  denotes a Frobenius element at  $\mathfrak{p}$  and  $a(\mathbf{f}_1)_{\mathfrak{p}}$  denotes the  $\mathfrak{p}^{\mathrm{th}}$  Fourier coefficient of  $\mathbf{f}_1$ . Moreover we have  $\det \sigma_2(\mathrm{Fr}_{\mathfrak{p}}) = N\mathfrak{p}$ .

In order to prove that  $E_1$  is attached to the form  $\mathbf{f}_1$  we need to show that the representations  $\sigma_1$  and  $\sigma_2$  are equivalent. For this we will use the following result of Faltings and Serre as stated and proved in [Liv].

**Theorem 10.1.** *Let  $K$  be a global field,  $S$  a finite set of primes of  $K$ , and  $E$  a finite extension of  $\mathbf{Q}_2$ . Denote the maximal ideal in the ring of integers of  $E$  by  $\mathfrak{p}$  and the compositum of all quadratic extensions of  $K$  unramified outside  $S$  by  $K_S$ . Suppose that*

$$\rho_1, \rho_2 : \mathrm{Gal}(\overline{K}/K) \rightarrow \mathrm{GL}_2(E)$$

are continuous representations, unramified outside  $S$ , and furthermore satisfying

1.  $\mathrm{Tr} \rho_1 \equiv \mathrm{Tr} \rho_2 \equiv 0 \pmod{\mathfrak{p}}$  and  $\det \rho_1 \equiv \det \rho_2 \pmod{\mathfrak{p}}$ .
2. There exists a set  $T$  of primes of  $K$ , disjoint from  $S$ , for which

- The image of the set  $\{\mathrm{Fr}_t : t \in T\}$  in the  $\mathbf{Z}/2\mathbf{Z}$ -vector space  $\mathrm{Gal}(K_S/K)$  is non-cubic.
- $\mathrm{Tr} \rho_1(\mathrm{Fr}_t) = \mathrm{Tr} \rho_2(\mathrm{Fr}_t)$  and  $\det \rho_1(\mathrm{Fr}_t) = \det \rho_2(\mathrm{Fr}_t)$  for all  $t \in T$ .

Then  $\rho_1$  and  $\rho_2$  have isomorphic semi-simplifications.

A subset  $S$  of the  $\mathbf{Z}/2\mathbf{Z}$ -vector space  $\text{Gal}(K_S/K)$  is said to be non-cubic if every homogeneous polynomial of degree three which vanishes on  $S$  vanishes on all of  $\text{Gal}(K_S/K)$ . In particular  $\text{Gal}(K_S/K)$  is itself non-cubic and we will apply this theorem with  $T$  chosen such that the image of  $\{\text{Fr}_t : t \in T\}$  in  $\text{Gal}(K_S/K)$  is the whole space.

As we can see from Table 5 we cannot apply this result immediately since the traces of Frobenius are not all even. Therefore for each  $i$  we let  $\bar{\sigma}_i$  denote the mod 2 representations obtained from  $\sigma_i$  and let  $L_i$  denote the extension of  $F$  cut out by  $\bar{\sigma}_i$ . We begin by showing that we can identify these two extensions.

### 10.1 Matching $L_1$ and $L_2$

We know that  $L_1 = F(E_1[2])$ . Hence  $L_1$  is the splitting field of the polynomial

$$g(x) = 4x^3 + (9 + 8\theta)x^2 + (648 + 14\theta)x + 411 + 137\theta.$$

and is an  $S_3$ -extension of  $F$  which is unramified outside of  $2R$ . Moreover we note that the quadratic extension of  $F$  contained in  $L_1$  is  $F(\sqrt{u})$ , where  $u = 442 + 41\theta$  is a fundamental unit of  $F$ .

We now consider  $L_2$ . We know that  $L_2$  is an extension of  $F$  that is unramified outside of  $2R$ . Moreover since some of the  $a(\mathfrak{f}_1)_{\mathfrak{p}}$ 's are odd we know that  $L_2$  is either a normal cubic extension of  $F$  or else is an  $S_3$  extension. By the following lemma we deduce that  $L_2/F$  must be an  $S_3$  extension.

**Lemma 10.2.** *There are no normal cubic extensions of  $F$  unramified outside of  $2R$ .*

*Proof.* Suppose that  $L/F$  is such an extension. Let  $\mathfrak{f}(L/F)$  denote the conductor of  $F$ . By [Co2, Corollary 3.5.12] we deduce that  $\mathfrak{f}(L/F)$  divides  $2R$ . But now using [Pari] we compute that the ray class group for the modulus  $2R\infty_1\infty_2$ , where  $\infty_i$  denote the infinite places of  $F$ , is trivial. Therefore no such extension  $L$  of  $F$  exists.  $\square$

Let  $F_1$  be the unique quadratic extension of  $F$  contained in  $L_2$ . We let  $u = 442 + 41\theta$  be the fundamental unit of  $F$ . Since  $F_1$  is unramified outside 2 we know that  $F_1$  must be one of the following fields

$$F(\sqrt{-1}), F(\sqrt{u}), F(\sqrt{2}), F(\sqrt{-u}), F(\sqrt{-2}), F(\sqrt{2u}) \text{ or } F(\sqrt{-2u}).$$

Let  $\mathfrak{p}$  be a prime of  $F$  and let  $\mathfrak{P}$  be a prime of  $F_1$  above  $\mathfrak{p}$ . We note that if  $a(\mathfrak{f}_1)_{\mathfrak{p}}$  is odd then  $f(\mathfrak{P}/\mathfrak{p}) = 1$ . We use this criterion to eliminate all the above quadratic extension of  $F$  except for  $F(\sqrt{u})$ . Taking  $\mathfrak{p} = (11 + \theta)R$  eliminates the fields  $F(\sqrt{2}), F(\sqrt{-2}), F(\sqrt{2u})$  and  $F(\sqrt{-2u})$ . While taking  $\mathfrak{p} = (15 - \theta)R$  eliminates the fields  $F(\sqrt{-1})$  and  $F(\sqrt{-u})$ . Therefore we have  $F_1 = F(\sqrt{u})$ .

**Lemma 10.3.** *There is a unique normal cubic extension of  $F_1$  which is unramified outside of  $2R_1$ , where  $R_1$  denotes the ring of integers in  $F_1$ .*

*Proof.* We note that  $2R_1 = \mathfrak{p}^2$ , where  $\mathfrak{p}$  is the unique prime of  $F_1$  above 2. Suppose that  $L/F_1$  is such an extension. Let  $\mathfrak{f}(L/F_1)$  denote the conductor of  $L/F_1$ . By [Co2, Corollary 3.5.12] we deduce that  $\mathfrak{f}(L/F_1)$  divides  $\mathfrak{p}$ . Using [Pari] we compute that the order of the ray class group for the modulus  $\mathfrak{p}\infty_1\infty_2$ , where  $\infty_i$  denote the real places of  $F_1$ , is three, from which we deduce that  $L$  is unique.  $\square$

Therefore since both  $L_1$  and  $L_2$  contain  $F(\sqrt{u})$  we deduce that  $L_1 = L_2$ .

## 10.2 Application of Faltings and Serre

Let  $K$  denote a fixed cubic extension of  $F$  contained in  $L = L_1 = L_2$ . We now apply Theorem 10.1 to the representations  $\sigma_1|_K$  and  $\sigma_2|_K$ . We note that these representations satisfy the conditions of the Theorem.

Now  $K = F(\alpha)$  where  $\alpha$  satisfies the equation

$$\psi_2(x) = 4x^3 + (9 + 8\theta)x^2 + (648 + 14\theta)x + 411 + 137\theta$$

over  $F$ . Using  $\theta^2 - \theta - 127 = 0$  we find that  $\alpha$  satisfies the equation

$$m(x) = 64x^6 + 416x^5 - 10940x^4 - 30552x^3 + 550476x^2 + 560056x - 8633740$$

over  $\mathbf{Q}$ . In fact we can write  $K = \mathbf{Q}(\beta)$  where  $\beta$  satisfies the equation

$$x^6 - 25x^4 - 46x^3 + 29x^2 + 66x + 20.$$

Using [Pari] we find that  $K$  has class number one and  $\mathcal{O}_K^\times \cong \{\pm 1\} \times \mathbf{Z}^4$  with fundamental units given by

$$\begin{aligned} u_1 &= \frac{1}{34}\beta^5 + \frac{3}{17}\beta^4 - \frac{23}{34}\beta^3 - \frac{92}{17}\beta^2 - \frac{293}{34}\beta - \frac{47}{17} \\ u_2 &= \frac{7}{102}\beta^5 - \frac{13}{51}\beta^4 - \frac{31}{34}\beta^3 + \frac{19}{51}\beta^2 + \frac{91}{102}\beta + \frac{11}{51} \\ u_3 &= \frac{10}{51}\beta^5 - \frac{8}{51}\beta^4 - \frac{71}{17}\beta^3 - \frac{361}{51}\beta^2 + \frac{79}{51}\beta + \frac{199}{51} \\ u_4 &= \frac{106}{51}\beta^5 - \frac{44}{51}\beta^4 - \frac{875}{17}\beta^3 - \frac{3745}{51}\beta^2 + \frac{4693}{51}\beta + \frac{5047}{51}. \end{aligned}$$

Now the ideal  $2R_K$  factors as  $\mathfrak{p}_1\mathfrak{p}_2^2$ . A generator for  $\mathfrak{p}_1$  is given by

$$a_1 = \frac{4}{51}\beta^5 + \frac{7}{51}\beta^4 - \frac{42}{17}\beta^3 - \frac{277}{51}\beta^2 + \frac{205}{51}\beta + \frac{304}{51}$$

and a generator for  $\mathfrak{p}_2$  is given by

$$a_2 = \frac{16}{51}\beta^5 - \frac{23}{51}\beta^4 - \frac{117}{17}\beta^3 - \frac{292}{51}\beta^2 + \frac{667}{51}\beta + \frac{349}{51}.$$

Let  $K_S$  denote the compositum of all quadratic extensions of  $K$  which are unramified outside of  $S = \{\mathfrak{p}_1, \mathfrak{p}_2\}$ . Then  $K_S$  is the compositum of the fields

$$K(\sqrt{-1}), K(\sqrt{u_1}), K(\sqrt{u_2}), K(\sqrt{u_3}), K(\sqrt{u_4}), K(\sqrt{a_1}) \text{ and } K(\sqrt{a_2}).$$

Using [Pari] we can find a set  $T$  of primes in  $K$  such that

$$\text{Gal}(K_S/K) = \{\text{Fr}_{\mathfrak{p}} \in \text{Gal}(K_S/K) : \mathfrak{p} \in T\}$$

where  $\text{Fr}_{\mathfrak{p}}$  denotes the Frobenius element in  $\text{Gal}(K_S/K)$  at  $\mathfrak{p}$ . Let  $T_0$  denote the primes of  $F$  generated by the elements of  $F$  in the left hand column of Table 6. Then we can take  $T$  to be the set of primes in  $K$  above those in  $T_0$ .

$\xi = a + b\theta$	$p$	$a(\mathfrak{p})$	$\xi = a + b\theta$	$p$	$a(\mathfrak{p})$	$\xi = a + b\theta$	$p$	$a(\mathfrak{p})$
3	inert	-4	54 + 5θ	11	3	92 + θ	8429	100
7	inert	-6	59 - 5θ	11	-2	93 - θ	8429	-110
11 + θ	5	3	55 + 4θ	1213	-46	95 + 2θ	8707	-28
12 - θ	5	-2	59 - 4θ	1213	34	97 - 2θ	8707	182
12 + θ	29	0	56 + 5θ	241	2	95 + 6θ	5023	76
13 - θ	29	10	61 - 5θ	241	-8	101 - 6θ	5023	86
14 + θ	83	14	57 + 5θ	359	-6	95 + 8θ	1657	28
15 - θ	83	9	62 - 5θ	359	9	103 - 8θ	1657	-22
15 + θ	113	11	59	inert	-22	100 + 3θ	9157	98
16 - θ	113	6	60 + θ	3533	6	103 - 3θ	9157	73
17 + θ	179	0	61 - θ	3533	-84	101 + 4θ	8573	66
18 - θ	179	25	62 + θ	3779	30	105 - 4θ	8573	-79
19	inert	-12	63 - θ	3779	0	105 + θ	11003	116
20 + θ	293	16	62 + 3θ	2887	-73	106 - θ	11003	36
21 - θ	293	26	65 - 3θ	2887	62	108 + 5θ	9029	-54
22 + θ	379	-20	65 + 2θ	3847	82	113 - 5θ	9029	96
23 - θ	379	20	67 - 2θ	3847	32	109 + θ	11863	-66
23 + 2θ	67	-7	66 + 5θ	1511	-8	110 - θ	11863	24
25 - 2θ	67	8	71 - 5θ	1511	-13	109 + 6θ	7963	-16
25 + θ	523	36	67 + 3θ	3547	-68	115 - 6θ	7963	59
26 - θ	523	11	70 - 3θ	3547	2	110 + 3θ	11287	208
25 + 2θ	167	22	68 + 5θ	1789	-34	113 - 3θ	11287	178
27 - 2θ	167	-8	73 - 5θ	1789	-14	111 + 8θ	5081	-30
29 + θ	743	44	69 + 2θ	4391	130	119 - 8θ	5081	90
31 - θ	743	-36	71 - 2θ	4391	75	112 + 5θ	9929	-146
31	inert	-18	71 + 3θ	4111	-35	117 - 5θ	9929	-96
32 + θ	929	40	74 - 3θ	4111	100	113 + 5θ	10159	76
33 - θ	929	10	71 + 5θ	2221	-18	118 - 5θ	10159	56
33 + 2θ	647	18	76 - 5θ	2221	-53	114 + 5θ	10391	98
35 - 2θ	647	43	74 + 5θ	2671	-72	119 - 5θ	10391	-117
34 + θ	1063	4	79 - 5θ	2671	-12	122 + θ	14879	0
35 - θ	1063	-1	76 + 3θ	4861	70	123 - θ	14879	-75
37 + θ	1279	-20	79 - 3θ	4861	-30	122 + 3θ	14107	152
38 - θ	1279	25	79	inert	-32	125 - 3θ	14107	32
37 + 3θ	337	-28	79 + 5θ	3461	-2	124 + 11θ	1373	34
40 - 3θ	337	2	84 - 5θ	3461	-57	135 - 11θ	1373	-6
39 + 2θ	1091	60	79 + 6θ	2143	24	137 + 11θ	4909	20
41 - 2θ	1091	0	85 - 6θ	2143	-56	148 - 11θ	4909	40
41	inert	-18	79 + 7θ	571	-20	139 + 6θ	15583	-156
41 + 3θ	661	-20	86 - 7θ	571	10	145 - 6θ	15583	4
44 - 3θ	661	-10	82 + 3θ	5827	-28	143 + 7θ	15227	108
45 + 2θ	1607	42	85 - 3θ	5827	22	150 - 7θ	15227	-122
47 - 2θ	1607	57	84 + θ	7013	-6	164 + 7θ	21821	-210
50 + θ	2423	-24	85 - θ	7013	-16	171 - 7θ	21821	-150
51 - θ	2423	-69	85 + 3θ	6337	78	169 + 11θ	15053	-6
51 + 4θ	773	-24	88 - 3θ	6337	48	180 - 11θ	15053	-106
55 - 4θ	773	-4	85 + 6θ	3163	86	171 + 10θ	18251	-68
54 + θ	2843	-6	91 - 6θ	3163	-4	181 - 10θ	18251	-198
55 - θ	2843	-61	91 + 3θ	7411	-55	178 + 5θ	29399	56
			94 - 3θ	7411	100	183 - 5θ	29399	96

Table 6:  $a(\mathfrak{p})$ 's for the elliptic curve  $E_1$  and cusp form  $\mathbf{f}_1$

For each  $\mathfrak{p} \in T_0$  we have computed  $a(E_1)_{\mathfrak{p}}$  and  $a(\mathbf{f}_1)_{\mathfrak{p}}$  and found that they are the same. Hence we deduce that for all  $\mathfrak{p} \in T$  we have

$$\text{Tr } \sigma_1(\text{Fr}_{\mathfrak{p}}) = \text{Tr } \sigma_2(\text{Fr}_{\mathfrak{p}}).$$

Thus by Theorem 10.1  $\sigma_1$  and  $\sigma_2$  are isomorphic.

### 10.3 End of Proof

We have proved in the previous subsection that  $\sigma_1|_K$  is isomorphic to  $\sigma_2|_K$  and therefore that  $\sigma_1|_L$  is isomorphic to  $\sigma_2|_L$ . We note that since  $E_1$  does not possess potential complex multiplication by Theorem 9.2 so  $\sigma_1|_L$  and hence  $\sigma_2|_L$  are both irreducible. Then by Frobenius reciprocity we know that  $\sigma_1|_{F_1}$  is isomorphic to  $\sigma_2|_{F_1} \otimes \chi$  for some character  $\chi$  of  $\text{Gal}(\overline{F}/F_1)$  trivial on  $\text{Gal}(\overline{F}/L)$ . Let  $\mathfrak{p} = (11 + \theta)R$  then  $a(E_1)_{\mathfrak{p}}$  is odd and  $\mathfrak{p}$  splits in  $F_1$ . Let  $\mathfrak{P}$  be a prime of  $F_1$  above  $\mathfrak{p}$  and let  $\text{Fr}_{\mathfrak{P}}$  be a Frobenius element at  $\mathfrak{P}$  in  $\text{Gal}(\overline{F}/F_1)$ . Then

$$\text{Tr}(\sigma_1|_{F_1}(\text{Fr}_{\mathfrak{P}})) = a(E_1)_{\mathfrak{p}} = \text{Tr}(\sigma_2|_{F_1}(\text{Fr}_{\mathfrak{P}}))$$

and hence  $\chi(\text{Fr}_{\mathfrak{P}}) = 1$ . But since  $\mathfrak{P}$  is inert in  $L$  we deduce that  $\chi$  must be trivial. Therefore we have  $\sigma_1|_{F_1} = \sigma_2|_{F_1}$ . Now using Frobenius reciprocity again we deduce that  $\sigma_1$  is isomorphic to  $\sigma_2 \otimes \delta$  for some character  $\delta$  of  $\text{Gal}(\overline{F}/F)$  trivial on  $\text{Gal}(\overline{F}/F_1)$ . If we take  $\mathfrak{p} = (12 - \theta)R$  then  $\mathfrak{p}$  is inert in  $F_1$ . Now

$$\text{Tr}(\sigma_1(\text{Fr}_{\mathfrak{p}})) = a(E_1)_{\mathfrak{p}} = \text{Tr}(\sigma_2(\text{Fr}_{\mathfrak{p}}))$$

and hence  $\delta(\text{Fr}_{\mathfrak{p}}) = 1$ . Therefore we deduce that  $\delta$  is trivial and hence that  $\sigma_1 = \sigma_2$ .

Therefore we conclude that  $E_1$  is attached to the form  $\mathfrak{f}_1$ . It immediately follows that the curve  $E_2$  is attached to the form  $\mathfrak{f}_2$ . The verification of Conjecture 1.1 for  $F = \mathbf{Q}(\sqrt{509})$  is now complete.

**Remark.** We found that after this work was completed one could use recent results of Skinner and Wiles ([SW, Theorem A]) to prove that the curve  $E_1$  is modular. Here one uses that the Galois representation on the 5-adic Tate module of  $E_1$  is residually reducible. However, our method can, in principle, be used in situations where their results do not apply. Moreover, our interest in this problem arises from attaching elliptic curves to unramified Hilbert modular forms, for which one needs to be able to determine the space of cusp forms. Furthermore, it appears that our method of computing the space of cusp forms can be extended to higher weight, where eigenforms with rational Hecke eigenvalues should correspond to certain other geometric objects.

## References

- [Bla] D. Blasius, *Elliptic curves, Hilbert modular forms, and the Hodge conjecture*, to appear.
- [BR] D. Blasius and J. Rogawski, *Motives for Hilbert Modular Forms*, Invent. Math. 114 (1993), 55-87.
- [Co1] H. Cohen, *A Course in Computational Number Theory*, Graduate Texts in Math. **138**, Springer-Verlag (1993).

- [Co2] H. Cohen, *Advanced Topics in Computational Number Theory*, Graduate Texts in Math. **193**, Springer-Verlag (2000).
- [Cre] J.E. Cremona, *Modular Symbols for  $\Gamma_1(N)$  and Elliptic Curves with Everywhere Good Reduction*, Mathematical Proceedings of the Cambridge Philosophical Society (1992), Vol. 111 (March, 1992), pp. 199-218.
- [GJ] Stephen Gelbart and Hervé Jacquet. *Forms on  $GL(2)$  from the Analytic Point of View*, Proceedings of Symposia in Pure Mathematics. Vol. 33 (1979), part 1, pp. 213-251.
- [Gro] Benedict H. Gross, *Heights and Special Values of  $L$ -series*, Canadian Mathematical Society Conference Proceedings, Vol. 7 (1987).
- [Has] Helmut Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Berlin (1952).
- [Hid] Haruzo Hida, *On  $p$ -adic Hecke Algebras for  $GL_2$  Over Totally Real Fields*, Annals of Mathematics, Vol. 128 (1988), pp. 295-384.
- [HPS] Hiroaki Hijikata, Arnold K. Pizer and Thomas R. Shemanske, *The Basis Problem for Modular Forms on  $\Gamma_0(N)$* , The American Mathematical Society (Memoirs, Volume 82, Number 418), Providence, Rhode Island (November, 1989).
- [LL] J.P. Labesse and R.P. Langlands,  *$L$ -indistinguishability for  $SL(2)$* , Canadian Journal of Mathematics, Vol. XXXI, 4 (1979), pp. 726-785.
- [Leo] Von Heinrich-Wolfgang Leopoldt, *Ein Verallgemeinerung der Bernoullischen Zahlen*, Hamburger Abh., 22 (1958), pp. 131-140.
- [Liv] Ron Livné, *Cubic Exponential Sums and Galois Representation*, Contemporary Mathematics, Vol. 67 (1987).
- [Ma] Daniel A. Marcus, *Number Fields*, Springer-Verlag, New York (1977).
- [Mar] J. Martinet, *Character Theory and Artin  $L$ -functions*, Algebraic Number Fields, Academic Press (1977).
- [Neu] J. Neukirch, *Algebraic number theory*, Springer-Verlag, Berlin (1999).
- [Pari] The Pari computer program, available from <http://pari.math.u-bordeaux.fr/>.
- [Pin] R.G.E. Pinch, *Elliptic Curves over Number Fields*, D.Phil. Thesis, Oxford University (1982).
- [Pi1] Arnold K. Pizer, *Type Numbers of Eichler Orders*, J. Reine Angew. Math., 264 (1973), pp. 76-102.
- [Pi2] Arnold K. Pizer, *The Representability of Modular Forms by Theta Series*, J. Math. Soc. Japan, Vol. 28, No. 4 (1976), pp. 689-698.

- [Pi3] Arnold K. Pizer, *An Algorithm for Computing Modular Forms on  $\Gamma_0(N)$* , Journal of Algebra, Vol. 64 (1980), pp. 340-390.
- [Pi4] Arnold K. Pizer, *Theta Series and Modular Forms of Level  $p^2M$* , Compositio Mathematica, Vol. 40, Fasc. 2 (1980), pp. 177-241.
- [Raj] C. S. Rajan, *On the image and fibres of solvable base change*, Math. Res. Lett. **9** (2002), no. 4, 499-508.
- [Sh] Hideo Shimizu, *On Zeta Functions of Quaternion Algebras*, Annals of Mathematics, Vol. 81 (1965), pp. 166-193.
- [Shi] Goro Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton University Press (1971).
- [SW] C. M. Skinner and A. J. Wiles, *Residually reducible representations and modular forms*, J Inst. Hautes Études Sci. Publ. Math., Vol. 89 (1999), pp. 5-126.
- [Soc] J. Socrates, *The Quaternionic Bridge between Elliptic Curves and Hilbert Modular Forms*, Thesis, Caltech (1993).
- [Tay] Richard Taylor, *On Galois Representations Associated to Hilbert Modular Forms*, Inventiones Mathematicae, 98, 265-280 (1989).
- [Vig] Marie-France Vignéras, *Arithmétique des Algèbres de Quaternions*, Springer-Verlag, Berlin (1980).

Division of Mathematics, Pasadena City College, Pasadena, CA 91106  
 jtsocrates@paccd.cc.ca.us

Mathematics 253-37, California Institute of Technology, Pasadena, CA 91125  
 dw@caltech.edu