**UNRAMIFIED HILBERT MODULAR FORMS,
WITH EXAMPLES RELATING TO ELLIPTIC CURVES**

JUDE SOCRATES AND DAVID WHITEHOUSE

UNRAMIFIED HILBERT MODULAR FORMS, WITH EXAMPLES RELATING TO ELLIPTIC CURVES

JUDE SOCRATES AND DAVID WHITEHOUSE

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 $\mathbb{Q}(\sqrt{509})$, 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 f we attach an elliptic curve with good reduction everywhere whose L-function agrees with that of 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 the trace formula, for example, 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 $\mathbb{Q}$. 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 $(2, \ldots, 2)$) and full level for F can be done on the quaternion algebra $\boldsymbol{B}$ over F that 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 $\boldsymbol{B}$.

In Sections 3 and 4 we extend the definition of Θ-series and Brandt matrices, as found in [Pizer 1980a], to this case. We show that each simultaneous eigenvector for the family of modified Brandt matrices corresponds to a Hilbert cusp form that 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.

Next 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 B and the class number of a maximal order in B. In Section 7 we give defining relations for the quaternion algebra B over a real quadratic field $\mathbb{Q}(\sqrt{m})$, and when $m \equiv 5 \bmod 8$ we give a maximal order in this algebra.

We now turn to our application to elliptic curves. To any Hilbert modular newform f over a totally real field F, having weight 2, level $\mathfrak{n}$ and rational Hecke eigenvalues, one expects to be able to attach an elliptic curve E_f that is defined over F, has conductor $\mathfrak{n}$ and whose L-function agrees with that of f at all places of F. This is known if F has odd degree over $\mathbb{Q}$ or if the automorphic representation associated to f belongs to the discrete series at some finite place (see [Blasius 2004, 1.7.1]).

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

When f is the base change of a classical modular form one can sometimes attach an elliptic curve to f as in Conjecture 1.1; see [Shimura 1971, 7.7]. Also, by [Blasius 2004], this conjecture is true under the hypothesis of the Hodge conjecture. In this paper we establish this conjecture for $F = \mathbb{Q}(\sqrt{509})$. The reason for this choice of field is, as we shall see, that there exist eigenforms that do not arise via base change from $\mathrm{GL}_2(\mathbb{Q})$, 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; see [Blasius 2004, 1.7.3].

We now outline the verification of Conjecture 1.1 for $F = \mathbb{Q}(\sqrt{509})$. In Section 8 we give representatives for the ideal classes in B from which we are able to compute the Brandt matrices and therefore the eigenvalues of the unramified eigenforms of weight 2. We find that there are three eigenforms whose Hecke eigenvalues all lie in $\mathbb{Q}$. In Section 9 we give the equations for the three elliptic curves over F that are attached to our three eigenforms. These elliptic curves already exist in the literature [Cremona 1992; Pinch 1982].

In Section 10 we prove Conjecture 1.1 for $\mathbb{Q}(\sqrt{509})$. One of our forms is a base change of a classical form given in [Cremona 1992]. In this case one knows, by work of Shimura, that an elliptic curve is attached to this form. Now we take f to be one of the forms that is not a base change from $\mathbb{Q}$ and we take E to be the elliptic curve (or its Galois conjugate) defined over F given in [Pinch 1982].

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

$$\sigma_{f,\ell} : \mathrm{Gal}(\bar{F}/F) \to \mathrm{GL}_2(\mathbb{Q}_\ell)$$

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

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

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

The verification of Conjecture 1.1 for f will therefore be complete if we can show, for some prime ℓ, that these two representations are equivalent. For this we take $\ell = 2$ and use a result of Faltings and Serre proved in [Livné 1987]. We cannot apply this result directly since it requires the traces of all Frobenius elements 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 $\mathrm{Gal}(\bar{F}/F)$ are equivalent.

This work was begun by the first author in his PhD thesis [Socrates 1993], which gave a construction of the space of cusp forms for a real quadratic field of narrow class number one. The cusp form f above and the elliptic curve E were shown there to have the same L-factors at all primes generated by a totally positive element $a + b\theta$ with $1 \le a \le 64$, where $\theta = \frac{1}{2}(1 + \sqrt{509})$.

This work was completed by the second author, who extended the methods of [Socrates 1993] to any totally real field of narrow class number one with even degree over $\mathbb{Q}$, adapted the result of Faltings and Serre, and independently computed the necessary eigenvalues given in Table 4.

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 $\mathbb{Q}$. We denote by R the ring of integers in F, by F^+ the set of totally positive elements in F, and likewise for R^+. We now explain how one can construct the space of cusp forms for F of weight 2 and full level.

Let B/F be the unique (up to isomorphism) quaternion algebra that is ramified only at the infinite places of F. We now give some definitions.

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

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

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

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

We construct the double coset space

$$X = M_G \backslash G(A_F^f)/G(F),$$

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

We denote by S the space

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

There is a natural definition of Hecke operators on this space, as follows. Let $\pi_\mathfrak{p}$ be a uniformizer for $R_\mathfrak{p}$ and let $g_\mathfrak{p} \in G(A_F^f)$ be 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 $M_G g_\mathfrak{p} M_G = \coprod_{i=1}^n M_G g_i$. 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 $f \in S$ and $h \in G(A_F^f)$,

$$\big(T_{\mathfrak{p}}(f)\big)(h) = \sum_{i=1}^{n} f(g_i h).$$

This gives a well-defined action on S, which is independent of the choices of the g_i and also of $\pi_{\mathfrak{p}}$.

Let $\mathcal{S}$ be the $\mathbb{C}$-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 [Gelbart and Jacquet 1979], 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 $\mathbb{Q}$ and later used to construct cusp forms for congruence subgroups of $\mathrm{SL2}(\mathbb{Z})$.

3. Θ-series of an ideal

The notion and construction of a Θ-series for an ideal in a quaternion algebra is discussed in several papers, including [Pizer 1976; 1980a; 1980b; Gross 1987]. In this section we extend these definitions to ideals in a totally definite quaternion algebra B defined over F.

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

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

We define the Θ-series of J for $\tau \in \mathcal{H}^{\mathrm{Hom}(F,\mathbb{R})}$ 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 β in J with $\mathcal{N}_J(\beta) = \xi$. This sum converges since composing $\mathcal{N}_J$ with the trace map from F to $\mathbb{Q}$ gives a positive definite quadratic form on J as a $\mathbb{Z}$-lattice.

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

Proof. Any two choices for $\mathrm{nr}(J)_+$ 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 $\xi \, \mathrm{nr}(J)_+$ and those of norm $\xi v \, \mathrm{nr}(J)_+$.   □

We note that if $J' = \gamma_1 J \gamma_2$ with $\gamma_i \in \boldsymbol{B}^\times$ the Θ-series of J and J' are identical. The proof in [Pizer 1980a, 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 $\{\beta_1, \ldots, \beta_4\}$ be a basis for J over R and let $\{\omega_1, \ldots, \omega_n\}$ be a basis for R over $\mathbb{Z}$. We can write $\beta \in J$ uniquely as

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

with $x_{ij} \in \mathbb{Z}$. 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 $\mathbb{Q}$ gives a positive definite quadratic form in the $\{x_{ij}\}$. Therefore, given a basis of an ideal J and $M \in \mathbb{R}$ we can use [Cohen 1993, Algorithm 2.7.7] to compute $c_{\xi, J}$ for all $\xi \in R^+$ with $\mathrm{Tr}\, \xi \leq M$.

4. Brandt matrices and eigenforms

Brandt matrices were classically constructed from a complete set of representatives of left $\mathbb{O}$-ideal classes of an Eichler order $\mathbb{O}$ of $\boldsymbol{B}'$, a definite quaternion algebra over $\mathbb{Q}$ with $\mathrm{Ram}(\boldsymbol{B}') = \{\infty, p\}$. For such a $\boldsymbol{B}'$, [Pizer 1980a; 1980b] show that terms appearing in a so-called Brandt matrix series are actually modular forms (for $\mathbb{Q}$) of a given weight and level p. In this section we extend these definitions to a totally definite quaternion algebra $\boldsymbol{B}$ defined over F. We then give an adelic construction of the Brandt matrices and show that each eigenvector for the family of modified Brandt matrices corresponds to a cusp form.

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

$$\mathbb{O}_r(I_k) = \{\boldsymbol{b} \in \boldsymbol{B} : I_k \boldsymbol{b} \subset I_k\}$$

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

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

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

In the notation of Section 3, let

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

which is simply the number of elements of norm 1 in the order $\mathbb{O}_r(I_j)$. 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 $\mathbb{O}_r(I_j)$-ideal $I_j^{-1} I_i$ of norm $\xi \, \mathrm{nr}(I_i)_+ / \mathrm{nr}(I_j)_+$. Now define the ξ-th Brandt matrix for $\mathbb{O}$ by

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

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

The following properties of the Brandt matrices are stated in [Pizer 1980a] and proved there for quaternion algebras over $\mathbb{Q}$. The proofs carry 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 $\mathbb{O}$ ideals of norm ξ.

(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 proved in [Pizer 1980a], with the proof carrying over here. The submatrix $B'(\xi)$ will be called the ξ-th modified Brandt matrix.

We now show that each simultaneous eigenvector for the family of modified Brandt matrices corresponds to a cusp form. Shimizu [1965] constructed a representation of the Hecke algebra acting on the space of automorphic forms, and

in [Hijikata et al. 1989, Chapter 5] it is shown that this can be used to provide another construction of Brandt matrices. We follow the discussion in this latter source, simplifying it for the case that we are interested in.

Fix a maximal order $\mathbb{O}$ in $\boldsymbol{B}$. Let $\boldsymbol{G}$ be the multiplicative group $\boldsymbol{B}^{\times}$, viewed as an algebraic group over F. Every left $\mathbb{O}$-ideal is of the form $\mathbb{O}\tilde{a}$ for some $\tilde{a} \in \boldsymbol{G}(\boldsymbol{A}_F)$. Let

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

Since $\tilde{\alpha}\mathcal{U}\tilde{\alpha}^{-1}$ is commensurable with $\mathcal{U}$ for all $\tilde{\alpha} \in \boldsymbol{G}(\boldsymbol{A}_F)$, we can define the usual Hecke ring $R(\mathcal{U}, \boldsymbol{G}(\boldsymbol{A}_F))$; see [Shimura 1971]. Put

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

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

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

$$f(u\tilde{a}\boldsymbol{b}) = f(\tilde{a}) \quad \text{for all } u \in \mathcal{U}, \tilde{a} \in \boldsymbol{G}(\boldsymbol{A}_F), \text{ and } \boldsymbol{b} \in \boldsymbol{G}(F).$$

We define a representation of $R(\mathcal{U}, \boldsymbol{G}(\boldsymbol{A}_F))$ on $\mathcal{M}$ as follows. For

$$\mathcal{U}y\mathcal{U} \in R(\mathcal{U}, \boldsymbol{G}(\boldsymbol{A}_F)),$$

let $\mathcal{U}y\mathcal{U} = \bigcup_i \mathcal{U}y_i$ be its decomposition into disjoint right cosets. Now write

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

and extend ρ to $R(\mathcal{U}, \boldsymbol{G}(\boldsymbol{A}_F))$ by linearity. It is shown in [Hijikata et al. 1989, p. 31] that this representation is independent of the choice of a maximal order, in the sense that, if $\mathbb{O}'$ is another maximal order, there is an isomorphism between $R(\mathcal{U}, \boldsymbol{G}(\boldsymbol{A}_F))$ and $R(\mathcal{U}', \boldsymbol{G}(\boldsymbol{A}_F))$ preserving the Hecke operators $\boldsymbol{T}(\xi)$, and also an isomorphism $\mathcal{M}_2(\mathbb{O})$ and $\mathcal{M}_2(\mathbb{O}')$, such that the representation of $R(\mathcal{U}, \boldsymbol{G}(\boldsymbol{A}_F))$ on $\mathcal{M}_2(\mathbb{O})$ induced by these isomorphisms is equivalent to the original representation of $R(\mathcal{U}, \boldsymbol{G}(\boldsymbol{A}_F))$ on $\mathcal{M}_2(\mathbb{O})$.

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

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

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

$$(1) \qquad\qquad\qquad f \mapsto (f_1, \ldots, f_H)$$

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

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

where multiplication by $\rho_{i,j}(\xi) : \mathbb{C}_j \to \mathbb{C}_i$ is the composition of the injection of $\mathbb{C}_j$ into $\mathbb{C}^H$, the inverse of map (1), $\rho(\mathcal{U}\xi\mathcal{U})$, map (1), and the projection of $\mathbb{C}^H$ into $\mathbb{C}_i$. The following is proved in [Hijikata et al. 1989, 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 $\mathbb{O}$ and set of left $\mathbb{O}$-ideal representatives I_λ.*

We shall now make explicit the isomorphism as Hecke modules between the spaces of Hilbert modular cusp forms and $\mathbb{C}$-valued functions on the finite set X modulo constant functions, which was mentioned in Section 2. We will follow the construction of Hida [1988], which is also discussed in [Taylor 1989]. As before, we shall be interested only in the weight 2, full level case.

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

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

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

$$\mathrm{nr} : G(A_F^f) \to I_F^f$$

and f is an appropriate $\mathbb{C}$-valued function on I_F^f, the finite idèles of F. The map nr, when restricted to the image of $B^\times$, surjects into the totally positive elements of F (this is the Theorem of Norms in [Vignéras 1980, p. 80]). Hence we can view $\mathrm{inv}(U)$ as consisting of functions of the form

$$G(A_F^f) \xrightarrow{\mathrm{nr}} I_F^f \longrightarrow \mathcal{U}(R_\mathfrak{p}) \backslash I_F^f / F^+ \xrightarrow{\cong} \mathrm{Cl}^+(F) \longrightarrow \mathbb{C},$$

where $\mathrm{Cl}^+(F)$ is the ray class group of F. Since we are assuming that $h^+(F) = 1$, $\mathrm{inv}(U)$ 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 $S_2(U)$ preserved by the Hecke algebra.

We describe the Hecke action on $\mathrm{inv}(U)$. Let $\boldsymbol{T}_{\mathfrak{p}}$ 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 $\boldsymbol{G}(A_F)$ that yield, upon multiplying to the right of $\mathbb{O}$, the set of integral left $\mathbb{O}$-ideals of norm $\mathfrak{p}$. Thus $\boldsymbol{T}_{\mathfrak{p}}(f)$ is the function with constant value equal to the number of such ideals.

We have seen that the matrix A transforms the Brandt matrices into two blocks consisting of a 1×1 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 $\mathbb{O}$-ideals of norm ξ. Thus we have:

Proposition 4.3. *Let $\{\boldsymbol{v}_i\}$ be a basis for $\mathbb{C}^{H-1}$ consisting of eigenvectors for all the modified Brandt matrices. Then each $\boldsymbol{v}_i$ corresponds to a (normalized) holomorphic Hilbert modular eigenform $\boldsymbol{f}_i$ of weight 2 and full level whose eigenvalue with respect to the $\mathfrak{p}$-th Hecke operator is precisely the eigenvalue of $\boldsymbol{v}_i$ with respect to $B'(\pi)$, where π is a totally positive generator of $\mathfrak{p}$.*

To find a basis of $\mathbb{C}^{H-1}$ of simultaneous eigenvectors for all the modified Brandt matrices one computes the matrices $B'(\xi)$, ordered by the trace of ξ, and successively decomposes the space $\mathbb{C}^{H-1}$ 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 $F/\mathbb{Q}$ 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 $F/\mathbb{Q}$. Using this one can then determine precisely which forms arise via base change once one has found a basis of $\mathbb{C}^{H-1}$ of simultaneous eigenvectors of the $B'(\xi)$ using the procedure described above. In the case that $F/\mathbb{Q}$ 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 that do not descend; see [Rajan 2002].

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 $\mathbb{O}$ in $\boldsymbol{B}$. In this section we give a strategy to find these representatives.

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

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

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

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

$$X = M_{\boldsymbol{G}} \backslash \boldsymbol{G}(A_F^f) / \boldsymbol{G}(F),$$

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

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

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

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

1. Determine the class number H. (This can be done; see [Pizer 1973]. We will make this explicit in the case of a quadratic field in Section 6 below.)

2. Initialize the list of representatives of left $\mathbb{O}$-ideal classes to $L = \{\mathbb{O}\}$.

3. Find an element $\alpha \in \boldsymbol{B}$ 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,

<div align="center">OR</div>

   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 $J_i = \mathbb{O}I_i$.
   (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 α 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 $\mathbb{O}$-ideals belong to different ideal classes, which is step 5(b) of the algorithm. In Section 3 we saw that the Θ-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 $\mathbb{O}$-ideals for an Eichler order $\mathbb{O}$. Then I and J belong to the same left ideal class if and only if there is an $\alpha \in M = \bar{J} I$ (where $\bar{J}$ denotes the conjugate ideal of J) such that $\mathrm{nr}(\alpha) = \mathrm{nr}(I) \, \mathrm{nr}(J)$, i.e., with $\mathcal{N}_M(\alpha) = 1$.*

This is proved in [Pizer 1980a], 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 $F = \mathbb{Q}(\sqrt{m})$ of narrow class number one. As is well known, this condition 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 $\boldsymbol{B}$ and the class number of a maximal order $\mathbb{O}$ in $\boldsymbol{B}$. The most important tool will be the main theorem in [Pizer 1973], which we restate here:

Theorem 6.1 (Pizer). *Let F be a totally real number field of degree n over $\mathbb{Q}$, and let R be its ring of integers. Let $\boldsymbol{B}$ be a positive definite quaternion algebra over F. Let q_1 be the product of the finite primes in F that ramify in $\boldsymbol{B}$ and q_2 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 $\boldsymbol{B}$ is*

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

where

- *e is the number of primes dividing $q_1 q_2$;*
- *M is Eichler's mass, given by*

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

  where ζ_F is the zeta function of F;
- *$h(\mathscr{S}_a)$ is the ideal class number of locally principal $\mathscr{S}_a$-fractional ideals;*
- *$w(\mathscr{S}_a)$ is the index of the group of units of R in the group of units in $\mathscr{S}_a$;*

- $E_{q_1q_2}(\mathscr{S}_a) = \prod_{\mathfrak{p}|q_1}\left(1 - \left\{\frac{\mathscr{S}_a}{\mathfrak{p}}\right\}\right)\prod_{\mathfrak{p}|q_2}\left(1 + \left\{\frac{\mathscr{S}_a}{\mathfrak{p}}\right\}\right);$

- *C is the collection of all orders defined by the following procedure:*

    1. *Let $e_1, \ldots, e_s$ be a compete set of representatives of $U \bmod U^2$, where U are the units of R;*
    2. *let $d_1, \ldots, d_k$ be a complete set of integral ideal representatives of*

    $$E \cdot \mathrm{Fr}(F)^2 \bmod (\mathrm{Pr}(F)^2),$$

    where E is the subgroup of $\mathrm{Fr}(F)$ (the divisor group of F) generated by all the $\mathfrak{p}$ which divide q_1q_2, and $\mathrm{Pr}(F)$ is the subgroup of principal divisors of $\mathrm{Fr}(F)$.
    3. *Let $n_1, \ldots, n_t$ be a set of all elements of R such that*

        (a) *$(n_j) = d_{j'}$ for some j' with $1 \leq j' \leq k$, and*
        (b) *$(n_i) \neq (n_j)$ for $i \neq j$.*
    4. *Consider the collection of all polynomials over R of the form*

    $$f_{\mu,\rho,\tau}(x) = x^2 - \tau x + n_\mu e_\rho \quad \text{with } 1 \leq \rho \leq s \text{ and } 1 \leq \mu \leq t,$$

    where

        (a) *$f_{\mu,\rho,\tau}$ is irreducible over F,*
        (b) *$F[x]/f_{\mu,\rho,\tau}(x)$ cannot be embedded in any F_{∞_i}, $i = 1, \ldots, n$,*
        (c) *$\mathfrak{p}^{s_\mathfrak{p}} \mid \tau$ for all $\mathfrak{p} < \infty$, where $s_\mathfrak{p} = \left[\frac{1}{2}v_\mathfrak{p}(n_\mu)\right]$ (floor function), and*
        (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 $C = \{\mathscr{S}_a : \mathscr{S}_a \text{ is an order of } F(a)\}$ such that*

        (a) *$R[a] \subset \mathscr{S}_a$, and*
        (b) *if $\mathfrak{p} < \infty$ then $a\pi_\mathfrak{p}^{-s_\mathfrak{p}} \in \mathscr{S}_{a,\mathfrak{p}}$, where $s_\mathfrak{p} = \left[\frac{1}{2}v_\mathfrak{p}(N(a))\right]$.*

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

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

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

For completeness we note that if $m = 5$ the type number of $\boldsymbol{B}$ is 1; see [Socrates 1993, Theorem 5.2].

Proof of Theorem 6.2. We proceed to determine the quantities in Theorem 6.1. We have $h(F) = 1$. Since $\boldsymbol{B}$ 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 both empty. Since $m \equiv 1 \bmod 4$ we have disc $F = m$ and

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

We shall further simplify M by explicitly calculating $\zeta_F(2)$. Our method will be that of [Leopoldt 1958], which uses generalized Bernoulli numbers; see also [Neukirch 1999, 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 $F = \mathbf{Q}(\sqrt{m})$, with $m > 0$, define

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

where the product runs over the characters mod $d = |\text{disc } F| = m$ that correspond to characters of $\text{Gal}(F/\mathbb{Q})$. Hence this product involves only the trivial character and χ the Legendre symbol mod m. Thus $B_{n,F} = B_n B_{n,\chi}$. In [Leopoldt 1958] 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 $M = \frac{1}{48}B_{2,\chi}$, since $B_2 = \frac{1}{6}$. 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 mod U^2 is given by $\{\pm 1, \pm u\}$.

2. Since $q_1 q_2 = 1$ and $\mathrm{Fr}(F) = \mathrm{Pr}(F)$, we have $k = 1$, $E = (1)$ and $\{(1)\}$ is a complete set of representatives for $E.\mathrm{Fr}(F)^2 \bmod \mathrm{Pr}(F)^2$.

3. From step 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 Ψ. Since $\mu = 1 = t$ and $n = n_1 = 1$ we shall use the abbreviation

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

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 τ. Condition 4(d) is vacuous. Now we look at condition 4(b). Since F is totally real this condition requires that the discriminant

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

of $f_{\rho,\tau}$ be totally negative. But for any τ, $\Delta(f_{-1,\tau})$ and $\Delta(f_{-u,\tau})$ are always positive, since $u > 0$. Hence we need only consider $f_{1,\tau}$ and $f_{u,\tau}$. But $N_{F/\mathbb{Q}}(u) = -1$ tells us that $\sigma(u) < 0$, where σ is the nontrivial element of $\mathrm{Gal}(F/\mathbb{Q})$. So $\sigma(\tau)^2 - 4\sigma(u) > 0$ for any τ. Thus 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 $\theta = \frac{1}{2}(1 + \sqrt{m})$, 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_τ. On the other hand, if $m < 16$

the only possible value for m is 13 and in this case we must have $b = 0$ or ± 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_τ above since the roots are imaginary. We summarize step 4 in the following result:

Lemma 6.3. *Assume the hypotheses in Theorem 6.2. The only contributing polynomials in Ψ are f_τ with $\tau = 0, \pm 1$.*

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

τ	Roots a_τ, a'_τ of f_τ	$F(a_\tau)$
0	ζ_4, ζ_4^3	$\mathbb{Q}(\sqrt{m}, \zeta_4)$
1	ζ_6, ζ_6^5	$\mathbb{Q}(\sqrt{m}, \zeta_6)$
-1	ζ_6^2, ζ_6^3	$\mathbb{Q}(\sqrt{m}, \zeta_6)$

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.*

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

(2) *The ring of integers of $\mathbb{Q}(\sqrt{m}, \zeta_6)$ 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 $K = \mathbb{Q}(\sqrt{m}, \zeta_4)$. Then by [Marcus 1977, Ex. 42, p. 51] we have $S = R[\zeta_4]$. Now let $\alpha = \omega_1 + \omega_2 \zeta_4 \in S$. We compute

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

where σ is the nontrivial element of $\mathrm{Gal}(F/\mathbb{Q})$. We deduce that α is a unit if and only if either $\omega_1 = 0$ and $N_{F/\mathbb{Q}}(\omega_2) = \pm 1$ or $\omega_2 = 0$ and $N_{F/\mathbb{Q}}(\omega_1) = \pm 1$. The result now follows.

(b) Let S denote the ring of integers in $K = \mathbb{Q}(\sqrt{m}, \zeta_6)$. Then by [Marcus 1977, Ex. 42, p. 51] we have $S = R[\zeta_6]$, since $3 \nmid m$ as $\mathbb{Q}(\sqrt{m})$ has narrow class number one. Let $\alpha = a + b\theta + c\zeta_6 + d\theta\zeta_6 \in S$, where $\theta = \frac{1}{2}(1 + \sqrt{m})$. We compute

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

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

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

that is, if and only if $2 = u^{2(r-s)} + u^{-2(r-s)}$. This is true if and only if $r = s$. We deduce that if $N_{F/\mathbb{Q}}(\omega_2) = \pm 1$, then α 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 follows. $\qquad \square$

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

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

Hence, equation (2) becomes

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

We now study the contributions from the biquadratic fields $\mathbb{Q}(\sqrt{m}, \sqrt{-1})$ and $\mathbb{Q}(\sqrt{m}, \sqrt{-3})$ to this sum. For this we need the following result of Hasse [1952].

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 $F_i = \mathbb{Q}(\sqrt{m_i})$, w_i the number of roots of unity in F_i, h_i the order of the class group of F_i. Let $K = \mathbb{Q}(\sqrt{m_1}, \sqrt{m_2})$, 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:

(1) For $\mathbb{Q}(\sqrt{m}, \sqrt{-1})$: Let $m_1 = -1$, $m_2 = -m$, $m_0 = m$, $K = \mathbb{Q}(\sqrt{-1}, \sqrt{-m})$. Hence $h_0 = 1$, by hypothesis. It is well known that the class group order of $\mathbb{Q}(\sqrt{-1})$ 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 $\mathbb{Q}(\sqrt{-m})$, with $m \neq 1, 3$, are ± 1, so $w_2 = 2$. Then $w = 4$ and $u_0 = u$. Thus we obtain $h = \frac{1}{2}h(\sqrt{-m})$.

(2) For $\mathbb{Q}(\sqrt{m}, \sqrt{-3})$: Let $m_1 = -3$, $m_2 = -3m$, $m_0 = 9m$, $K = \mathbb{Q}(\sqrt{-3}, \sqrt{-3m})$. Similarly, it is know that the class group order of $\mathbb{Q}(\sqrt{-3})$ is 1, and the only roots of unity are powers of ζ_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, $[\mathscr{S}^\times : U] = 2$ and 3, respectively, for $\mathbb{Q}(\sqrt{m}, \sqrt{-1})$ and $\mathbb{Q}(\sqrt{m}, \sqrt{-3})$. We can now finish proving Theorem 6.2. The field $\mathbb{Q}(\sqrt{m}, \sqrt{-3})$ contributes twice in the sum (for $\tau = 1, -1$), so equation (2) becomes

$$T = M + \frac{1}{2}\left(\frac{h\big(\mathbb{Q}(\sqrt{m}, \sqrt{-1})\big)}{2} + 2\frac{h\big(\mathbb{Q}(\sqrt{m}, \sqrt{-3})\big)}{3}\right)$$
$$= M + \frac{1}{8}h\big(\mathbb{Q}(\sqrt{-m})\big) + \frac{1}{6}h\big(\mathbb{Q}(\sqrt{-3m})\big)$$

and this completes the proof of Theorem 6.2. $\qquad\square$

We can also determine H. Following the proof of Theorem 6.1 given in [Pizer 1973], we see that

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

where $C_2 = C - C_1$ and $C_1 = \{\mathscr{S}_a \in C \mid (N(a)) = (1)\}$. 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 $\mathrm{Ram}(\mathbf{B}) = \{\infty_1, \infty_2\}$. Then $H = T$. Consequently, if $I_1, \ldots, I_H$ is a complete set of representatives of distinct left $\mathbb{O}$-ideal classes for a fixed maximal order $\mathbb{O}$, then the corresponding right orders $\mathbb{O}_r(I_1), \ldots, \mathbb{O}_r(I_H)$ 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 $C_2 = \varnothing$. Substitute these in (3) to get the result. $\qquad\square$

7. The algebra B and a maximal order $\mathcal{O}$

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

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

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

In the case that $F = \mathbb{Q}(\sqrt{m})$ has narrow class number 1 and $m \equiv 1 \bmod 8$ one can take B' to be the quaternion algebra over $\mathbb{Q}$ ramified precisely at $\{m, \infty\}$. By [Pizer 1980a, Proposition 5.1], one has $B' = (-m, -q)$ where q is a prime with $q \equiv 3 \bmod 4$ and $\left(\frac{m}{q}\right) = -1$. The same argument as above shows that $B = B' \otimes_{\mathbb{Q}} F$. We now give a maximal order $\mathcal{O}$ in B when $m \equiv 5 \bmod 8$.

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

Proof. It is clear that $\mathcal{O}$ is a full lattice in 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 [Socrates 1993, Theorem 4.2]. $\qquad\square$

8. Cusp form calculations

We now compute the space of cusp forms for the field $F = \mathbb{Q}(\sqrt{509})$. From Theorem 6.2 and Proposition 6.7 we compute that the class number for 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 α. The α that eventually led us to distinct ideal classes were i together with

$$\alpha_1 = \tfrac{1}{2} + 5i + \tfrac{1}{2}(1+\theta)j + \left(1 - \tfrac{1}{2}\theta\right)k = \delta_1 + 9\delta_2 - 4\theta j - (4+5\theta)k$$
$$\left(\mathrm{nr}(\alpha_1) = 90, \quad k_1 = -359, \quad h(\mathbb{Q}(\sqrt{-359})) = 19\right)$$

and

$$\alpha_2 = \tfrac{1}{2} + (4 - \tfrac{1}{2}\theta)i + 2j + \tfrac{1}{2}(7+\theta)k = \delta_1 + (7-\theta)\delta_2 + (65-3\theta)j + (63-2\theta)k$$
$$\left(\mathrm{nr}(\alpha_2) = 96, \quad k_2 = -383, \quad h(\mathbb{Q}(\sqrt{-383})) = 17\right).$$

Let $K = F(\alpha_i)$. 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 that 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 $\mathrm{nr}(\mathcal{O}I) = (a + b\theta)$.

Since the class number of $\mathcal{O}$ is rather large, we first used the Θ-series of $\mathcal{O}I$ for various prime ideals I in the extensions $K = F(\alpha_i)$ above. We computed the Θ-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 Θ-series, are listed in the tables below.

After a lengthy search that did not yield another ideal with a distinct Θ-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 Θ-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 Ψ_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 Ψ_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

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

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

Now that we have concrete representatives of left ideal classes, we are able to construct explicitly the first few Brandt matrices $B(\xi)$ and the modified Brandt

matrices $B'(\xi)$ using the algorithm [Cohen 1993, Algorithm 2.7.7] mentioned at the end of Section 3. This involves computing the Θ-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 $\mathbb{Q}$. We found that the characteristic polynomial of $B'(19 + \theta)$ has three distinct rational roots and an irreducible factor of degree 20. Hence, although $\mathbb{C}^{23}$ has a basis of eigenvectors for all the $B'(\xi)$, only three eigenvectors have eigenvalues that are all rational. The three rational eigenvectors are

$$v_1 = (0, 0, 0, 0, 1, 0, -2, -1, 1, 1, 0, -2, 0, 0, -3, 1, 0, 0, 0, -1, 2, 0, 2),$$

$$v_2 = (0, 0, 0, 0, -1, 0, 2, 1, -1, 1, 0, 2, 0, 0, -2, -1, 0, 0, 0, 1, -2, 0, 3),$$

$$v_3 = (45, 45, 25, 60, 23, 40, 34, 27, 18, 28, 30, 19, 35, 20, 31, 28, 20,$$
$$15, 25, 37, 51, 40, 31).$$

We let f_1, f_2 and f_3 denote the forms corresponding to the vectors v_1, v_2 and v_3 by Proposition 4.3. The initial Fourier coefficients of these forms are tabulated in Table 3. From this table we note that $f_1 = f_2^\sigma$, where σ is the nontrivial element of $\mathrm{Gal}(F/\mathbb{Q})$, while $f_3 = f_3^\sigma$ and hence 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 f be a Hilbert eigenform of full level for a totally real number field F of narrow class number one. Then f is not a CM form.*

Proof. Recall that f is a CM form if and only if there exists a quadratic character ε corresponding to an imaginary quadratic extension K/F such that $f = f \otimes \varepsilon$. So suppose we have $f = f \otimes \varepsilon$ for such a character ε. Let π denote the cuspidal representation of $\mathrm{GL}_2(A_F)$ corresponding to π. Then we have $\pi \cong \pi \otimes (\varepsilon \circ \det)$. By a theorem of Labesse and Langlands [1979] we have an equality of L-series $L(\pi, s) = L(\chi, s)$ for some grössencharakter χ of K, and it is known that $\mathrm{cond}\,\pi = N_{K/F}(\mathrm{cond}\,\chi)\,\mathrm{disc}(K/F)$. Since π 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. $\square$

9. The elliptic curves

In this section we give equations for the elliptic curves that we will show are attached to the forms f_1, f_2 and f_3 of the previous section.

Let E_3 be the elliptic curve given by the Weierstrass equation

$$y^2 + (1 + \theta)xy + (1 + \theta)y$$
$$= x^3 + (-4051846 + 343985\theta)x + 4312534180 - 3660733300\theta.$$

This curve is found in [Cremona 1992] and is a $\mathbb{Q}$-curve (that is, 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 1982], among other curves that 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 [Cremona 1992]. We take E_2 to be the curve E_1^σ, where σ is the nontrivial element of $\mathrm{Gal}(F/\mathbb{Q})$.

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

I_i	K	$a_i + b_i\theta$	γ_i	$I_i \mid p \in \mathbb{Z}$
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 the $\mathbb{O}I_i$ have distinct Θ-series.

Proof. If E_1 and E_1^σ are isogenous, the local factors of the L-series of E_1 and E_1^σ 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 $\mathbb{Z}/5$ that maps θ to

	1	2	3	4	5	6	7	8	9	10	11	11+θ	12−θ	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, J_5	0	0	0	24	0	0	0	24	0	0	0	0	0	96
J_6, J_7, 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}, 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

	12+θ	13−θ	13	13+θ	14−θ	14	14+θ	15−θ	15	15+θ
J_4, 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

	16−θ	16	16+θ	17−θ	17	17+θ	18−θ	18	18+θ
J_4	0	24	0	0	48	0	0	24	24
J_5	0	48	0	0	0	0	0	0	0

Table 2. Beginning coefficients c_{ξ, J_i} of the Θ-series of J_1 to J_{23}. More are given for ideals whose early coefficients agree.

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

Table 3. Eigenvalues for simultaneous rational eigenvectors for $B'(\xi)$.

2 mod 5. Then the equation for the reduced curve $\widetilde{E}_1$ over $\mathbb{Z}/5$ has affine equation

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

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

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

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

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 now follows from:

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

Proof. Suppose $E(\mathbb{C})$ has CM defined over the field $\mathbb{Q}(\sqrt{n})$, where $n < 0$. Consider the field $L = K(\sqrt{n})$. Then E and its complex multiplications are defined over L. Consider the ℓ-adic representation given by the action of Galois on the ℓ-adic Tate module of E/L

$$\sigma_\ell : \mathrm{Gal}(\overline{\mathbb{Q}}/L) \to \mathrm{GL}_2(\mathbb{Q}_\ell).$$

We construct another representation

$$\begin{aligned} \sigma_\ell^{[\rho]} \,:\, \mathrm{Gal}(\overline{\mathbb{Q}}/L) &\to\ \mathrm{GL}_2(\mathbb{Q}_\ell), \\ \tau &\mapsto\ \sigma_\ell(\rho\tau\rho^{-1}), \end{aligned}$$

where $\rho \in \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ is nontrivial when restricted to L. Now, since E is actually defined over K, this σ_ℓ extends to a representation $\tilde{\sigma}_\ell$ of $\mathrm{Gal}(\overline{\mathbb{Q}}/K)$. However,

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

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

Since E has CM over L, the representation σ_ℓ is abelian, so $\sigma_\ell = \chi_\ell \oplus \chi'_\ell$ for some characters χ_ℓ, χ'_ℓ of H. It can easily be seen from such a decomposition that, in the obvious notation,

$$\sigma_\ell^{[\rho]} = \chi_\ell^{[\rho]} \oplus \chi'^{[\rho]}_\ell$$

as well. Now, χ_ℓ corresponds to a weight 1 grössencharakter ψ of L, and $\chi_\ell = \chi_\ell^{[\rho]}$ if and only if $\psi(z) = \psi(\bar{z})$ for all $z \in L_\infty^* = \mathbb{C}^*$. 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 $\tilde{\sigma}_\ell = \mathrm{Ind}_H^G(\chi_\ell)$. Since the degree of χ_ℓ is 1, we get the formula

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

for the conductor of $\tilde{\sigma}_\ell$; see [Martinet 1977]. Recall that E has good reduction everywhere, so every $\tilde{\sigma}_\ell$ is unramified at all the primes of K not dividing ℓ. Since $\tilde{\sigma}_\ell$ is ramified at all the primes which divide $\mathrm{cond}(\tilde{\sigma}_\ell)$, we see that $\mathrm{disc}(L/K)$ 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 $n < 0$. $\qquad \square$

10. Matching the elliptic curves to the cusp forms

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

We begin by showing that the curve E_3 is attached to the form $\boldsymbol{f}_3$. The curve E_3 is equal to the curve A' that arises from Shimura's construction [1971, 7.7]. This curve is constructed from a pair of eigenforms $\{f_1, f_2\}$ in $S_2(\Gamma_0(509), \chi)$ where χ is the quadratic character of $(\mathbb{Z}/509\mathbb{Z})^\times$. These forms are constructed in [Cremona 1992]. Furthermore we know that

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

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 $\boldsymbol{f}_3$ is the base change of the form f_1 and we have

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

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,

$$\sigma_1 : \mathrm{Gal}(\bar{F}/F) \to \mathrm{GL}_2(\mathbb{Q}_2),$$

is unramified outside 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 $\mathfrak{p}$-th Fourier coefficient of E_1. Moreover $\det \sigma_1(\mathrm{Fr}_\mathfrak{p}) = N\mathfrak{p}$.

Let f_1 denote the unramified cusp form given in Section 8 above. By [Taylor 1989] and [Blasius and Rogawski 1993] there exists a 2-dimensional representation

$$\sigma_2 : \mathrm{Gal}(\bar{F}/F) \to \mathrm{GL}_2(\mathbb{Q}_2)$$

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

$$\mathrm{Tr}\,\sigma_2(\mathrm{Fr}_\mathfrak{p}) = a(f_1)_\mathfrak{p}$$

where again $\mathrm{Fr}_\mathfrak{p}$ denotes a Frobenius element at $\mathfrak{p}$ and $a(f_1)_\mathfrak{p}$ denotes the $\mathfrak{p}$-th Fourier coefficient of f_1. Moreover we have $\det \sigma_2(\mathrm{Fr}_\mathfrak{p}) = N\mathfrak{p}$.

To prove that E_1 is attached to the form f_1 we must show that the representations σ_1 and σ_2 are equivalent. For this we will use the following result of Faltings and Serre as stated and proved in [Livné 1987].

Theorem 10.1. *Let K be a global field, S a finite set of primes of K, and E a finite extension of $\mathbb{Q}_2$. 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*

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

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

1. $\mathrm{Tr}\,\rho_1 \equiv \mathrm{Tr}\,\rho_2 \equiv 0 \bmod \mathfrak{p}$ *and* $\det \rho_1 \equiv \det \rho_2 \bmod \mathfrak{p}$.

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 $\mathbb{Z}/2\mathbb{Z}$-vector space $\mathrm{Gal}(K_S/K)$ is noncubic*;
    - $\mathrm{Tr}\,\rho_1(\mathrm{Fr}_t) = \mathrm{Tr}\,\rho_2(\mathrm{Fr}_t)$ *and* $\det \rho_1(\mathrm{Fr}_t) = \det \rho_2(\mathrm{Fr}_t)$ *for all $t \in T$.*

Then ρ_1 and ρ_2 have isomorphic semi-simplifications.

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

As we can see from Table 3, 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 σ_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.

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 unramified outside of $2R$. Moreover 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 $a(\boldsymbol{f}_1)_{\mathfrak{p}}$'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 next 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 [Cohen 2000, Corollary 3.5.12] we deduce that $\mathfrak{f}(L/F)$ divides $2R$. But now using Pari [Cohen et al. 2004] we compute that the ray class group for the modulus $2R\infty_1\infty_2$, where ∞_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 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 $a(\boldsymbol{f}_1)_{\mathfrak{p}}$ 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 [Cohen 2000, 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 ∞_i denote the real places of F_1, is three, from which we deduce that L is unique. $\square$

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

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 α 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 α satisfies the equation

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

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

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

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

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

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

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

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

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

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

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

where $\mathrm{Fr}_{\mathfrak{P}}$ denotes the Frobenius element in $\mathrm{Gal}(K_S/K)$ at $\mathfrak{P}$. Let T_0 denote the primes of F generated by the elements of F in the left hand column of Table 4. 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	$54+5\theta$	11	3	$92+\theta$	8429	100
7	inert	−6	$59-5\theta$	11	−2	$93-\theta$	8429	−110
$11+\theta$	5	3	$55+4\theta$	1213	−46	$95+2\theta$	8707	−28
$12-\theta$	5	−2	$59-4\theta$	1213	34	$97-2\theta$	8707	182
$12+\theta$	29	0	$56+5\theta$	241	2	$95+6\theta$	5023	76
$13-\theta$	29	10	$61-5\theta$	241	−8	$101-6\theta$	5023	86
$14+\theta$	83	14	$57+5\theta$	359	−6	$95+8\theta$	1657	28
$15-\theta$	83	9	$62-5\theta$	359	9	$103-8\theta$	1657	−22
$15+\theta$	113	11	59	inert	−22	$100+3\theta$	9157	98
$16-\theta$	113	6	$60+\theta$	3533	6	$103-3\theta$	9157	73
$17+\theta$	179	0	$61-\theta$	3533	−84	$101+4\theta$	8573	66
$18-\theta$	179	25	$62+\theta$	3779	30	$105-4\theta$	8573	−79
19	inert	−12	$63-\theta$	3779	0	$105+\theta$	11003	116
$20+\theta$	293	16	$62+3\theta$	2887	−73	$106-\theta$	11003	36
$21-\theta$	293	26	$65-3\theta$	2887	62	$108+5\theta$	9029	−54
$22+\theta$	379	−20	$65+2\theta$	3847	82	$113-5\theta$	9029	96
$23-\theta$	379	20	$67-2\theta$	3847	32	$109+\theta$	11863	−66
$23+2\theta$	67	−7	$66+5\theta$	1511	−8	$110-\theta$	11863	24
$25-2\theta$	67	8	$71-5\theta$	1511	−13	$109+6\theta$	7963	−16
$25+\theta$	523	36	$67+3\theta$	3547	−68	$115-6\theta$	7963	59
$26-\theta$	523	11	$70-3\theta$	3547	2	$110+3\theta$	11287	208
$25+2\theta$	167	22	$68+5\theta$	1789	−34	$113-3\theta$	11287	178
$27-2\theta$	167	−8	$73-5\theta$	1789	−14	$111+8\theta$	5081	−30
$29+\theta$	743	44	$69+2\theta$	4391	130	$119-8\theta$	5081	90
$30-\theta$	743	−36	$71-2\theta$	4391	75	$112+5\theta$	9929	−146
31	inert	−18	$71+3\theta$	4111	−35	$117-5\theta$	9929	−96
$32+\theta$	929	40	$74-3\theta$	4111	100	$113+5\theta$	10159	76
$33-\theta$	929	10	$71+5\theta$	2221	−18	$118-5\theta$	10159	56
$33+2\theta$	647	18	$76-5\theta$	2221	−53	$114+5\theta$	10391	98
$35-2\theta$	647	43	$74+5\theta$	2671	−72	$119-5\theta$	10391	−117
$34+\theta$	1063	4	$79-5\theta$	2671	−12	$122+\theta$	14879	0
$35-\theta$	1063	−1	$76+3\theta$	4861	70	$123-\theta$	14879	−75
$37+\theta$	1279	−20	$79-3\theta$	4861	−30	$122+3\theta$	14107	152
$38-\theta$	1279	25	79	inert	−32	$125-3\theta$	14107	32
$37+3\theta$	337	−28	$79+5\theta$	3461	−2	$124+11\theta$	1373	34
$40-3\theta$	337	2	$84-5\theta$	3461	−57	$135-11\theta$	1373	−6
$39+2\theta$	1091	60	$79+6\theta$	2143	24	$137+11\theta$	4909	20
$41-2\theta$	1091	0	$85-6\theta$	2143	−56	$148-11\theta$	4909	40
41	inert	−18	$79+7\theta$	571	−20	$139+6\theta$	15583	−156
$41+3\theta$	661	−20	$86-7\theta$	571	10	$145-6\theta$	15583	4
$44-3\theta$	661	−10	$82+3\theta$	5827	−28	$143+7\theta$	15227	108
$45+2\theta$	1607	42	$85-3\theta$	5827	22	$150-7\theta$	15227	−122
$47-2\theta$	1607	57	$84+\theta$	7013	−6	$164+7\theta$	21821	−210
$50+\theta$	2423	−24	$85-\theta$	7013	−16	$171-7\theta$	21821	−150
$51-\theta$	2423	−69	$85+3\theta$	6337	78	$169+11\theta$	15053	−6
$51+4\theta$	773	−24	$88-3\theta$	6337	48	$180-11\theta$	15053	−106
$55-4\theta$	773	−4	$85+6\theta$	3163	86	$171+10\theta$	18251	−68
$54+\theta$	2843	−6	$91-6\theta$	3163	−4	$181-10\theta$	18251	−198
$55-\theta$	2843	−61	$91+3\theta$	7411	−55	$178+5\theta$	29399	56
			$94-3\theta$	7411	100	$183-5\theta$	29399	96

Table 4. $a(\mathfrak{p})$'s for the elliptic curve E_1 and cusp form $\boldsymbol{f}_1$.

For each $\mathfrak{p} \in T_0$ we have computed $a(E_1)_{\mathfrak{p}}$ and $a(f_1)_{\mathfrak{p}}$ and found that they are the same. Hence we deduce that for all $\mathfrak{P} \in T$ we have

$$\operatorname{Tr} \sigma_1(\operatorname{Fr}_{\mathfrak{P}}) = \operatorname{Tr} \sigma_2(\operatorname{Fr}_{\mathfrak{P}}).$$

Thus by Theorem 10.1 σ_1 and σ_2 are isomorphic.

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 Proposition 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 χ of $\operatorname{Gal}(\bar{F}/F_1)$ trivial on $\operatorname{Gal}(\bar{F}/L)$. 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 $\operatorname{Fr}_{\mathfrak{P}}$ be a Frobenius element at $\mathfrak{P}$ in $\operatorname{Gal}(\bar{F}/F_1)$. Then

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

and hence $\chi(\operatorname{Fr}_{\mathfrak{P}}) = 1$. But since $\mathfrak{P}$ is inert in L we deduce that χ must be trivial. Therefore we have $\sigma_1|_{F_1} = \sigma_2|_{F_1}$. Now using Frobenius reciprocity again we deduce that σ_1 is isomorphic to $\sigma_2 \otimes \delta$ for some character δ of $\operatorname{Gal}(\bar{F}/F)$ trivial on $\operatorname{Gal}(\bar{F}/F_1)$. If we take $\mathfrak{p} = (12 - \theta)R$ then $\mathfrak{p}$ is inert in F_1. Now

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

and hence $\delta(\operatorname{Fr}_{\mathfrak{p}}) = 1$. We deduce that δ is trivial and hence that $\sigma_1 = \sigma_2$.

Thus we conclude that E_1 is attached to the form f_1. It immediately follows that the curve E_2 is attached to the form f_2. The verification of Conjecture 1.1 for $F = \mathbb{Q}(\sqrt{509})$ is now complete.

Remark. We found after this work was completed that one could use [Skinner and Wiles 1999, 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.

version of this paper, Barry Mazur for his encouragement and the referee for a thorough report that led to several improvements in the exposition.

References

[Blasius 2004] D. Blasius, "Elliptic curves, Hilbert modular forms, and the Hodge conjecture", pp. 83–103 in *Contributions to automorphic forms, geometry, and number theory*, edited by H. Hida et al., Johns Hopkins Univ. Press, Baltimore, MD, 2004. MR MR2058605

[Blasius and Rogawski 1993] D. Blasius and J. D. Rogawski, "Motives for Hilbert modular forms", *Invent. Math.* **114**:1 (1993), 55–87. MR 94i:11033 Zbl 0829.11028

[Cohen 1993] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics **138**, Springer, Berlin, 1993. MR 94i:11105 Zbl 0786.11071

[Cohen 2000] H. Cohen, *Advanced topics in computational number theory*, Graduate Texts in Mathematics **193**, Springer, New York, 2000. MR 2000k:11144 Zbl 0977.11056

[Cohen et al. 2004] H. Cohen et al., "PARI/GP version 2.1.3", software, Bordeaux, 2004, Available at http://pari.math.u-bordeaux.fr.

[Cremona 1992] J. E. Cremona, "Modular symbols for $\Gamma_1(N)$ and elliptic curves with everywhere good reduction", *Math. Proc. Cambridge Philos. Soc.* **111**:2 (1992), 199–218. MR 93e:11065 Zbl 0752.11022

[Gelbart and Jacquet 1979] S. Gelbart and H. Jacquet, "Forms of GL(2) from the analytic point of view", pp. 213–251 in *Automorphic forms, representations and L-functions* (Corvallis, OR, 1977), vol. 1, edited by A. Borel and W. Casselman, Proc. Sympos. Pure Math. **33**, Amer. Math. Soc., Providence, RI, 1979. MR 81e:10024 Zbl 0409.22013

[Gross 1987] B. H. Gross, "Heights and the special values of L-series", pp. 115–187 in *Number theory* (Montreal, 1985), edited by H. Kisilevsky and J. Labute, CMS Conf. Proc. **7**, Amer. Math. Soc., Providence, RI, 1987. MR 89c:11082 Zbl 0623.10019

[Hasse 1952] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Akademie-Verlag, Berlin, 1952. MR 14,141a Zbl 0046.26003

[Hida 1988] H. Hida, "On p-adic Hecke algebras for GL_2 over totally real fields", *Ann. of Math.* (2) **128**:2 (1988), 295–384. MR 89m:11046 Zbl 0658.10034

[Hijikata et al. 1989] H. Hijikata, A. K. Pizer, and T. R. Shemanske, *The basis problem for modular forms on $\Gamma_0(N)$*, Mem. Amer. Math. Soc. **418**, Amer. Math. Soc., Providence, RI, 1989. MR 90d:11056 Zbl 0689.10034

[Labesse and Langlands 1979] J.-P. Labesse and R. P. Langlands, "L-indistinguishability for SL(2)", *Canad. J. Math.* **31**:4 (1979), 726–785. MR 81b:22017 Zbl 0421.12014

[Leopoldt 1958] H.-W. Leopoldt, "Eine Verallgemeinerung der Bernoullischen Zahlen", *Abh. Math. Sem. Univ. Hamburg* **22** (1958), 131–140. MR 19,1161e Zbl 0080.03002

[Livné 1987] R. Livné, "Cubic exponential sums and Galois representations", pp. 247–261 in *Current trends in arithmetical algebraic geometry* (Arcata, CA, 1985), edited by K. A. Ribet, Contemp. Math. **67**, Amer. Math. Soc., Providence, RI, 1987. MR 88g:11032 Zbl 0621.14019

[Marcus 1977] D. A. Marcus, *Number fields*, Springer, New York, 1977. MR 56 #15601 ZBL 0383.12001

[Martinet 1977] J. Martinet, "Character theory and Artin L-functions", pp. 1–87 in *Algebraic number fields: L-functions and Galois properties* (Durham, 1975), edited by A. Fröhlich, Academic Press, London, 1977. MR 56 #5502 Zbl 0359.12015

[Neukirch 1999] J. Neukirch, *Algebraic number theory*, Grundlehren der Math. Wissenschaften **322**, Springer, Berlin, 1999. MR 2000m:11104 Zbl 0956.11021

[Pinch 1982] R. G. E. Pinch, *Elliptic curves over number fields*, Ph.D. thesis, Oxford University, 1982.

[Pizer 1973] A. K. Pizer, "Type numbers of Eichler orders", *J. Reine Angew. Math.* **264** (1973), 76–102. MR 49 #2650 Zbl 0274.12008

[Pizer 1976] A. Pizer, "The representability of modular forms by theta series", *J. Math. Soc. Japan* **28**:4 (1976), 689–698. MR 54 #10154 Zbl 0344.10012

[Pizer 1980a] A. Pizer, "An algorithm for computing modular forms on $\Gamma_0(N)$", *J. Algebra* **64**:2 (1980), 340–390. MR 83g:10020 Zbl 0433.10012

[Pizer 1980b] A. Pizer, "Theta series and modular forms of level $p^2 M$", *Compositio Math.* **40**:2 (1980), 177–241. MR 81k:10040 Zbl 0416.10021

[Rajan 2002] C. S. Rajan, "On the image and fibres of solvable base change", *Math. Res. Lett.* **9**:4 (2002), 499–508. MR 2003g:11054 Zbl 01886044

[Shimizu 1965] H. Shimizu, "On zeta functions of quaternion algebras", *Ann. of Math.* (2) **81** (1965), 166–193. MR 30 #1998 Zbl 0201.37903

[Shimura 1971] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publ. Math. Soc. Japan **11**, Iwanami Shoten, Tokyo, 1971. MR 47 #3318 Zbl 0221.10029

[Skinner and Wiles 1999] C. M. Skinner and A. J. Wiles, "Residually reducible representations and modular forms", *Inst. Hautes Études Sci. Publ. Math.* **89** (1999), 5–126. MR 2002b:11072 Zbl 1005.11030

[Socrates 1993] J. Socrates, *The quaternionic bridge between elliptic curves and Hilbert modular forms*, Ph.D. thesis, California Institute of Technology, Pasadena, CA, 1993.

[Taylor 1989] R. Taylor, "On Galois representations associated to Hilbert modular forms", *Invent. Math.* **98**:2 (1989), 265–280. MR 90m:11176 Zbl 0705.11031

[Vignéras 1980] M.-F. Vignéras, *Arithmétique des algèbres de quaternions*, Lecture Notes in Mathematics **800**, Springer, Berlin, 1980. MR 82i:12016 Zbl 0422.12008

JUDE SOCRATES
DIVISION OF MATHEMATICS
PASADENA CITY COLLEGE
PASADENA, CA 91106
jtsocrates@paccd.cc.ca.us

DAVID WHITEHOUSE
MATHEMATICS 253-37
CALIFORNIA INSTITUTE OF TECHNOLOGY
PASADENA, CA 91125
dw@caltech.edu