MATHEMATICS OF COMPUTATION
Volume 74, Number 251, Pages 1545–1557
S 0025-5718(04)01709-0
Article electronically published on September 10, 2004

COMPUTING WEIGHT 2 MODULAR FORMS OF LEVEL p^2

ARIEL PACETTI AND FERNANDO RODRIGUEZ VILLEGAS,
WITH AN APPENDIX BY B. GROSS

ABSTRACT. For a prime p we describe an algorithm for computing the Brandt matrices giving the action of the Hecke operators on the space V of modular forms of weight 2 and level p^2. For $p \equiv 3 \bmod 4$ we define a special Hecke stable subspace V_0 of V which contains the space of modular forms with CM by the ring of integers of $\mathbb{Q}(\sqrt{-p})$ and we describe the calculation of the corresponding Brandt matrices.

1. INTRODUCTION

The main goal of this paper is to describe an effectively computable Hecke stable subspace V_0 of the space V of modular forms of weight 2 and level p^2, with $p \equiv 3 \bmod 4$ prime, containing the space V_{CM} of forms with CM by the ring of integers of $\mathbb{Q}(\sqrt{-p})$. The space V_0 is constructed in terms of the Brandt matrices associated to ideal classes of an order (of index p in a maximal order) in the quaternion algebra over $\mathbb{Q}$ ramified at p and ∞.

Computationally this approach to study V_{CM} has several positive features. First, the total space V has dimension that grows proportionally to p^2 whereas V_0 has dimension that grows proportionally to p. This means that in practice calculations with V_0 can be carried out for much larger primes p than with V itself. Second, the space V_0 is indeed effectively computable; more concretely, V_0 can be cut out from V in a straightforward manner.

Ultimately, the reason for studying the questions discussed here is to effectively compute a Shimura lift of the CM forms of level p^2. In the present paper we describe how to compute the corresponding eigenvector of all Brandt matrices, In a later publication we will describe how this can be used, in a generalization of methods of Gross for level p, to obtain a Shimura lift.

In conclusion the main computational principle in this paper is that by using Brandt matrices it is possible (say, for nonsquarefree level) to effectively work with smaller dimensional Hecke stable subspaces of modular forms. This appears to be a useful principle that could be exploited further.

Received by the editor February 18, 2003 and, in revised form, December 16, 2003.
2000 *Mathematics Subject Classification.* Primary 11F11; Secondary 11E20, 11Y99.
The first and second authors were supported in part by grants from TARP and NSF (DMS-99-70109); they would like to thank the Department of Mathematics at Harvard University, where part of this work was done, for its hospitality.

2. Preliminaries on quaternion algebras

Notation. Fix a prime $p > 2$ and let B be the quaternion algebra over $\mathbb{Q}$ ramified at p and at ∞ (such an algebra is unique up to isomorphism). We write $N(x)$ for the reduced norm of an element $x \in B$, and we write $\mathrm{Tr}(x)$ for its reduced trace.

Definitions.
(1) A *lattice* $I \subset B$ is a $\mathbb{Z}$-module of rank 4.
(2) An *order* $O \subset B$ is a ring which is a lattice.
(3) Given a lattice I, its *left order* is $O_l(I) := \{x \in B \ / \ xI \subset I\}$; similarly, its *right order* is $O_r(I) := \{x \in B \ / \ Ix \subset I\}$.
(4) For a lattice I and a prime q we let $I_q := I \otimes \mathbb{Z}_q$.
(5) Given an order O, a *left O-ideal* is a lattice I such that I is locally principal; i.e., for all primes q we have $I_q = O_q a_q$ for some $a_q \in (B \otimes \mathbb{Q}_q)^\times$.
(6) For a left O-ideal I of B, its *norm* $N(I)$ is the positive generator of the ideal of $\mathbb{Z}$ generated by $N(x)$ with $x \in I$.
(7) Given a left O-ideal I of B, we define $N_I : I \longrightarrow \mathbb{Z}$ as $x \mapsto N(x)/N(I)$.
(8) Given a lattice I, its *dual* is $I^\# := \{b \in B \ / \ \mathrm{Tr}(bI) \subset \mathbb{Z}\}$.
(9) A lattice is *integral* if it is contained in its left and right orders.

We fix a maximal order O once and for all.

Proposition 1. *If I is a lattice such that $O_l(I)$ is maximal, then I is a left $O_l(I)$-ideal.*

Proof. See [Vi, p. 86]. □

Theorem 1. *Let I be a left O-ideal and $I^\#$ its dual. Then $I^\#$ is a right O-ideal and $I^\iota := N(I)p\overline{I}^\#$ is a left O-ideal contained in I with $I/I^\iota \simeq \mathbb{Z}/p\mathbb{Z} \oplus \mathbb{Z}/p\mathbb{Z}$ as abelian groups and $N(I^\iota) = N(I)p$. If $I = O$, then $O/O^\iota \simeq \mathbb{F}_{p^2}$ as rings.*

Proof. If O is an order, then, by definition, O^ι is its different. Since B has only one ramified prime, $\mathcal{P} = O^\iota$ is the unique maximal 2-sided prime over p. Since all ideals are locally principal, we have that if $I_q = O_q a_q$, then $\overline{I_q} = \overline{a_q}\overline{O_q} = \overline{a_q}O_q$ for all primes q; also, it is not hard to check that $I_q^\iota = O_q^\iota a_q$. By [Vi, Lemma 4.7, p. 24], the different is a bilateral O-ideal of norm p. It follows that $O/O^\iota \simeq O_p/O_p^\iota \simeq \mathbb{F}_{p^2}$ and it is now easy to finish the proof. □

Remark. It is not hard to verify that $I^\iota = \mathcal{P}I$, where $\mathcal{P}$ is the different, which could have been used as its definition.

Proposition 2. *If I is a lattice, then $(I^\#)^\# = I$.*

Proof. This is standard. □

Corollary 1. *If I is a lattice, then $O_l(I^\#) = O_r(I)$ and $O_r(I^\#) = O_l(I)$.*

Proof. It is clear that if α is in $I^\#$ and x is in $O_l(I)$, then $\alpha x \in I^\#$, which implies that $O_l(I) \subset O_r(I^\#)$; using that $\overline{I^\#} = \bar{I}^\#$ and replacing I by $\bar{I}$, we get that $O_r(I) \subset O_i(I^\#)$. Applying the same argument to $I^\#$ and using the previous proposition, we get the other inclusion. □

Lemma 1. *Let $J \subset I$ be two left O-ideals. Then $(N(J)/N(I))^2 = |I/J| = [I : J]$.*

Proof. It is enough to check locally the case $I = O$. If $J_q = O_q\alpha_q$, then $N(J_q) = N(\alpha_q)$. Since J is integral, $O_q\alpha_q \subset O_q$; its index is up to a unit in $\mathbb{Z}_q^\times$ the determinant of multiplication by α_q, which equals $N(\alpha_q)^2$. □

Lemma 2. *Let I be a left O-ideal and $J \subset I$ a sublattice of index p, such that $I^\iota \subset J \subset I$. Then $O_l(J) = \mathbb{Z} + O^\iota \subset O$ with index p. Furthermore $OJ = I$ and $N(J) = N(I)$.*

Proof. Clearly $O_l(J)$ contains $\mathbb{Z} + O^\iota$. Since I/I^ι is a 1-dimensional vector space over $O/O^\iota \simeq \mathbb{F}_{p^2}$ (by Theorem 1) and J/I^ι is a submodule of index p, necessarily $O_l(J)$ must equal the proper submodule $\mathbb{Z} + O^\iota$ (of index p in O). $\square$

Definition. An order has level p^2 if it has index p in some maximal order.

We denote by $\tilde{O} = \mathbb{Z} + \mathcal{P}$ the unique suborder of level p^2 in O (see [Pi, Lemma 1.4, p. 181]) and by $h, \tilde{h}$ the class numbers of $O, \tilde{O}$, respectively.

Proposition 3. *Any lattice I with $O_l(I) = \tilde{O}$ is an $\tilde{O}$-ideal.*

Proof. Let I be such a lattice. By Proposition 1, for all primes $q \neq p$, I_q is principal, since $\tilde{O}_q = O_q$. For the ramified prime, since $\mathbb{Z}_p$ is a PID, there exists $a_p \in I_p$ with $(N(a_p)) = N(I_p)$. Therefore, $\tilde{O}_p a_p \subset I_p \subset O_p I_p$. Since $O_p I_p$ is an ideal for O_p of the same norm as I_p, we have by Lemma 1 that $O_p I_p = O_p a_p$. On the other hand, the index of $\tilde{O}_p$ in O_p is p; hence, $I_p = \tilde{O}_p a_p$. $\square$

Proposition 4. *Let I be a left $\tilde{O}$-ideal. Then the following hold.*

(1) *If $x \in I$ is such that $p \nmid N_I(x)$, then $\left(\frac{N_I(x)}{p}\right)$ is independent of x, where $(\div)$ denotes the Kronecker symbol.*
(2) *$\left(\frac{N_I(x)}{p}\right)$ only depends on the equivalence class of I.*
(3) *If I is principal, then $\left(\frac{N_I(x)}{p}\right) = 1$.*

Proof. The proofs are quite elementary; see [Pi, Proposition 5.1, p. 198]. $\square$

Elements $x \in I$ as in the proposition always exist; we let $\chi(I)$ denote the common value of $\left(\frac{N_I(x)}{p}\right)$. It is easy to check that $\chi(\overline{I}) = \chi(I)$ where the bar denotes conjugation and $\chi(I^{-1}) = \chi(I)$.

Corollary 2. *Given two orders O_j of level p^2 for $j = 1, 2$ and left O_j-ideals I_j for $j = 1, 2$ such that $O_r(I_1) = O_2$, then $\chi(I_1 I_2) = \chi(I_1)\chi(I_2)$.*

Proof. Pick $x_j \in I_j$ for $j = 1, 2$ with $p \nmid N_{I_j}(x_j)$ and take $x_1 x_2 \in I_1 I_2$; note that $N(I_1 I_2) = N(I_1)N(I_2)$. $\square$

3. Computing left $\tilde{O}$-ideal representatives

Proposition 5. *Let p be a prime and let $B = (a, b)$ be the quaternion algebra ramified at p and infinity with $i^2 = a$ and $j^2 = b$. Then a $\tilde{O}$ order is given by the basis:*

- $\langle \frac{1}{2}(1 + j), \frac{1}{2}(pi + k), j, k \rangle$ *with $a = -1$, $b = -p$ if $p \equiv 3 \bmod 4$,*
- $\langle \frac{1}{3}(1 + j + k), \frac{1}{4}(pi + 2j + k), j, k \rangle$ *with $a = -2$, $b = -p$ if $p \equiv 5 \bmod 8$,*
- $\langle \frac{1}{2} + \frac{pj}{2}, \frac{i}{2} + \frac{k}{2}, k, \frac{pj}{q} + \frac{sk}{q} \rangle$ *with $a = -p$, $b = -q$ if $p \equiv 1 \bmod 8$ where q is a prime such that $\left(\frac{p}{q}\right) = -1$, $q \equiv 3 \bmod 4$ and s is an integer with $s^2 \equiv -p \bmod q$ and $s \equiv -q \bmod p$.*

Proof. This is just an easy but tedious computation. Note that in the case $p \equiv 1 \bmod 8$ the maximal order we are considering is $M = \langle \frac{1}{2} + \frac{j}{2}, \frac{i}{2} + \frac{k}{2}, k, \frac{j}{q} + \frac{(s+q)k}{pq} \rangle$. The conditions on s make this an order, and it is easy to check that it is maximal, but it differs from the one defined in [Pi, Proposition 5.2]. □

Given a left O-ideal I, by Lemma 2 and Proposition 3 there are $p+1$ $\tilde{O}$-left ideals J with

$$I^\iota \subset J \subset I, \qquad [I : J] = [J : I^\iota] = p. \tag{1}$$

We call any such J a *p-subideal* of I.

Proposition 6. *Any p-subideal J is of the form $I^\iota[v]$ for some $v \in I$ and for any such v we have $p \nmid N_I(v)$.*

Proof. Since J has index p in I, it is clear that $J = I^\iota[v]$ for some $v \in I$, $v \notin I^\iota$, and locally all these ideals are equal for all primes $q \neq p$. Let $I_p = O_p a_p$. Then we saw that $I_p^\iota = O_p^\iota a_p$; since $v \in I$, $v = u a_p$ with $u \in O_p$. If $p | N_I(v)$, then $p | N(u)$; hence $u \in O_p^\iota$ and we would have that $J \subset I^\iota$. □

We now show how to obtain a set of representatives of left $\tilde{O}$-ideals by considering these index p sublattices for a set of representatives of left O-ideals. We then use these ideals to construct the Brandt matrices for $\tilde{O}$.

Proposition 7. *Let I_i for $i = 1, 2$ be left O-ideals and let $J_i \subset I_i$ for $i = 1, 2$ corresponding p-subideals. If I_1 and I_2 are nonequivalent, then so are J_1 and J_2.*

Proof. If $J_1 = J_2\alpha$ for some $\alpha \in \tilde{O}$, then $I_1 = OJ_1 = OJ_2\alpha = I_2\alpha$ (by Lemma 2) which is a contradiction. □

We fix a set of representatives $I^1, \ldots, I^h$ of left O-ideals.

Proposition 8. *Every $\tilde{O}$-ideal is equivalent to some p-subideal $J \subset I^j$ for some j.*

Proof. The left O-ideal OJ is equivalent to some I^j; i.e., $OJ = I^j\alpha$ for some α and hence $OJ\alpha^{-1} = I^j$. Therefore $J\alpha^{-1} \subset I^j$ and $OJ\alpha^{-1} = I^j$. A simple calculation shows that $J\alpha^{-1}$ has index p in I^j. For a prime $q \neq p$, we have that $O_q = \tilde{O}_q$. Then $O_q J_q = J_q = I_q^j$, so no primes other than p appear in the index. As for the ramified prime, let us say that $J_p\alpha^{-1} = \tilde{O}_p a_p$, and $I_p^j = O_p c_p$. Since $O_p J_p = I_p$, we have that $O_p a_p = O_p c_p$ so $I_p^j = O_p a_p$; therefore $\left| I_p^j/(J_p\alpha^{-1}) \right| = \left| O_p a_p / \tilde{O}_p a_p \right| = p$.

Since $J\alpha^{-1} \subset I^j$ with index p, to see that $I^\iota \subset J\alpha^{-1}$, it is enough to check locally at p. Let $J_p = \tilde{O}_p b_p$, $I_p = O_p a_p$. Without loss of generality we may assume that $b_p\alpha^{-1} = a_p$. By the proof of Theorem 1, we see that $I_p^\iota = O_p^\iota a_p$. Also $O_p^\iota \subset \tilde{O}_p$; therefore $O_p^\iota a_p \subset \tilde{O}_p a_p = \tilde{O}_p b_p \alpha^{-1} = J_p\alpha^{-1}$. □

The following lemma is easy to check.

Lemma 3. *Two p-subideals $J, J' \subset I$ are equivalent if and only if $Ju = J'$ for $u \in O_r(I)^\times$.*

Corollary 3. *Given a left O-ideal I, the number of nonequivalent p-subideals $J \subset I$ is $(p+1)|O_r(J)^\times|/|O_r(I)^\times|$.*

Proposition 9. *If $p > 3$, then the number of units in $\tilde{O}$ is 2, and if $p = 3$ the number of units is 2 or 6.*

Proof. See Proposition 5.12 of [Pi2]. □

For $j = 1, \dots, h$ we let $O_j = O_r(I^j)$ and let $\tilde{O}_j$ be its suborder of index p.

Corollary 4. *We have*

$$\tilde{h} = (p+1) \sum_{j=1}^{h} \frac{|\tilde{O}_j^\times|}{|O_j^\times|}. \tag{2}$$

If $p > 3$, then $\tilde{h} = (p^2 - 1)/12$.

Proof. This is clear from Proposition 9 and Eichler's mass formula for maximal ideals. □

There are the same number of $\tilde{O}$-ideals with character χ equal to 1 as with character -1. The proof given in [Pi, Proposition 5.6, p. 199] uses the action of a certain element α of the idele group of B on ideals. We now describe an algorithmic version of this action.

The components α_q of α are as follows: for $q \neq p$ we set $\alpha_q = 1$ and for $q = p$ we want α_p with zero trace such that

$$\left(\frac{a}{p}\right) = -1,$$

where $a = N(\alpha_p)/p^n$ and $n = v_p(N(\alpha_p))$ with v_p the valuation at p. We then have that $\chi(\alpha_p J) = -\chi(J)$. We denote by δ the involution

$$\delta : \quad J \mapsto \alpha J. \tag{3}$$

Note that if J and J' are equivalent, then so are δJ and $\delta J'$.

3.1. **Construction of α_p.** From now on we fix the specific basis i, j for the algebra B and the maximal order O as in [Pi2, Proposition 5.2, p.369].

There are two cases.

(1) If $p \equiv 1 \mod 4$, then by our very choice of basis for the quaternion algebra we may take α_p to be one of i or j.
(2) If $p \equiv 3 \mod 4$, then -1 is a nonsquare and we look for α_p with norm $-p$. If $\alpha = x_1 i + x_2 j + x_3 k$, with $i^2 = -1, j^2 = -p = k^2$, then $N(\alpha_p) = x_1^2 + p(x_2^2 + x_3^3)$. We can take $x_1 = 0$ and look for a solution to the equation $x_2^2 + x_3^2 = -1$ in $\mathbb{Z}_p$, which is achieved by finding a solution to $x_2^2 + x_3^2 \equiv -1 \mod p$ and then lifting the solution using Hensel's lemma.

3.2. **Action of α_p on I.** We will follow [Ei, Theorem 7, p. 34]. First we need to compute an r such that $\alpha_p J \supset J p^r$.

Lemma 4. *Let $n = v_p(N(\alpha_p))$ be the p-valuation of the norm of α_p. Then $\alpha_p J \supset J p^{\lceil n/2 \rceil + 1}$.*

Proof. In order that $\alpha_p J \supset J p^s$, we must have $\alpha_p^{-1} p^s \in \tilde{O}$. Note that if $\beta \in O$, then $p\beta \in \tilde{O}$; hence it is enough to check when $\alpha_p^{-1} p^{s-1} \in O$ or, equivalently, when $v_p(N(\alpha_p^{-1} p^{s-1})) \geq 0$. It is now straightforward to verify that it is enough to take $s \geq \left\lceil \frac{v_p(N(\alpha_p))}{2} \right\rceil + 1$. □

Set $r = \lceil n/2 \rceil + 1$. Starting with a global basis for Jp^r, we start adjoining elements until we find a generating set for αJ. Say $J = \langle u_1, u_2, u_3, u_4 \rangle$ so that $\alpha_p J = \langle \alpha_p u_1, \alpha_p u_2, \alpha_p u_3, \alpha_p u_4 \rangle$. It is not hard to see that we have

$$\alpha_p u_j \equiv v_j \bmod p^r J_p, \qquad j = 1, \ldots, 4,$$

with $p^s v_j \in J$ for some s. We set $J' = \langle Jp^r, v_1, v_2, v_3, v_4 \rangle$. Clearly $\alpha_p J_p = J'_p$ and for a prime $q \neq p$ we have $v_i \in J_q$ for $i = 1, \ldots, 4$ and hence $J'_q = J_q$.

Having computed representatives for some maximal order (respectively, an order of level p^2), we can get representatives for any other order, if needed, by simply multiplying on the right by an appropriate ideal (see [Pi2, Proposition 1.21, p. 348] for a proof of this elementary fact).

To perform the above computations accurately, we need to know a priori how many terms of the p-expansion of α_p to use.

Lemma 5. *Given a left $\tilde{O}$-ideal J, let α_p be as constructed above. In order to compute $\alpha_p J$, it is enough to know α_p to order $O(p^{r+1})$, where $r = \lceil v_p(N(\alpha_p))/2 \rceil + 1$.*

Proof. For our choice of O, i, j we have $\{1, i, j, k\} \subset O$ and hence $\{p, pi, pj, pk\} \subset \tilde{O}$. Then, with the notation as in the proof of Lemma 4, $\{piu_t, pju_t, pku_t\} \subset I$ for $1 \leq t \leq 4$; hence, $p^{r+1} \alpha_p u_t \in p^r I$ and the denominator of the x_j is at most $r + 1$. □

Note that with our choice of α_p we have $r = 1$ for $p \equiv 1 \bmod 4$ and $r = 2$ for $p \equiv 3 \bmod 4$. By Lemma 5, therefore, it is enough to compute the first two terms in the p-adic expansion of α_p.

3.3. **Further structure.** There is more structure on the ideals J that we are going to use to prove some properties of the Brandt matrices.

It is clear that O_p/O_p^ι is isomorphic to $\mathbb{F}_{p^2}$ and $\tilde{O}_p/O_p^\iota$ to $\mathbb{F}_p$. Let $S := (O_p/O_p^\iota)^\times$, a cyclic group of order $p^2 - 1$. Given a $\tilde{O}$-ideal J and $u \in S$, we define uJ, with some notation abuse, by regarding O_p as a subring of the adeles. It is easy to check that this gives rise to a (left) action of S on left $\tilde{O}$-ideals with stabilizer $(\tilde{O}_p)^\times/(O_p^\iota)^\times$. It is also easy to check that S acts on the set of p-subideals making it a principal homogeneous space for $G := (O_p/O_p^\iota)^\times/(\tilde{O}_p/O_p^\iota)^\times$, a cyclic group of order $p + 1$.

Let u be a generator of G and let J be some p-subideal of I. Then $\{u^i J\}_{i=0}^p$ are all the p-subideals of I. By Proposition 5.6 of [Pi] we know that if $J_p = \tilde{O}_p \alpha_p$, then $\chi(J)$ is the quadratic symbol of $N(\alpha_p)/N(J)$ modulo p. Since the norm map from $\mathbb{F}_{p^2}$ to $\mathbb{F}_p$ is surjective, we must have that $N(u)$ is a nonsquare modulo p and hence $\chi(u^i J) = (-1)^i \chi(J)$.

We form a set of inequivalent p-subideals $\mathcal{J} = \{J, uJ, \ldots, u^{r-1}J\}$ where r is the smallest positive integer such that $u^r J$ is equivalent to J. Note that r is necessarily even since $\mathcal{J}$ decomposes into two subsets, according to the value of χ, which are in bijection by δ. Also, if $u \in G$, then $\overline{u}$ is its inverse since $u\overline{u} = N(u)$ and $N(u) \in \tilde{O}_1$.

4. Constructing the Brandt matrices

Now we can describe the calculation of the Brandt matrices themselves. We should point out that the software package Magma [Ma] includes routines for calculations of Brandt matrices due to D. Kohel and these are described in [Ko] (note, however, that the paper does not treat the case of level p^2 though the routines in Magma do).

We pick a maximal order O and we calculate representatives $\{I^1, \dots, I^{h(O)}\}$ of left O-ideal classes (using Pizer's algorithm for the level p case) and we fix a generator u of G. To compute inequivalent p-subideals of each I^k, we follow Section 2 and we order them as follows. Dropping the k from the notation, we pick a p-subideal J_0 with $\chi(J_0) = 1$ and consider

$$J_0, J_2, \dots, J_{r-2}, J_1, J_3, \dots, J_{r-1} \tag{4}$$

where $J_1 = \delta J_0$ and $J_{i+2j} = u^{2j} J_i$ for $i = 0, 1$, r is the number of nonequivalent p-subideals of I^k and δ is the involution defined in (3). Note that by construction $\chi(J_i) = (-1)^i$.

We will consider the Brandt matrices $B(q)$ defined using the following ordering of classes of p-subideals. First we put the classes with $\chi = +1$ as

$$J_0^1, J_2^1, \dots, J_{r_1-2}^1, J_0^2, J_2^2, \dots, J_{r_2-2}^2, \dots J_0^h, J_2^h, \dots, J_{r_h-2}^h, \tag{5}$$

followed by those with $\chi = -1$,

$$J_1^1, J_3^1, \dots, J_{r_1-1}^1, J_1^2, J_3^2, \dots, J_{r_2-1}^2, \dots J_1^h, J_3^h, \dots, J_{r_h-1}^h, \tag{6}$$

where $h = h(O)$ and J_j^i are the representatives for the p-subideals of I^i as described in (4).

For every prime q we consider the Brandt matrix $B(q)$ with respect to the above chosen basis. One of the important things of ordering the basis in this form is the following.

Proposition 10. *For $q \neq p$ write the Brandt matrix $B(q)$ in block form*

$$B(q) = \begin{pmatrix} A & B \\ C & D \end{pmatrix},$$

where each A, B, C, D has size $h(\tilde{O})/2 \times h(\tilde{O})/2$. Then the following hold.

(1) *If $\left(\frac{q}{p}\right) = 1$, then $B = C = 0$, and $A = D$.*
(2) *If $\left(\frac{q}{p}\right) = -1$, then $A = D = 0$, and $B = C$.*

Proof. This is just a special case of [Pi, Theorem 5.15, Theorem 5.18 p. 203]. □

The above proposition shows that to find the eigenvectors and eigenvalues of $B(q)$ we just need to work with A or B, depending on the case, which have half the size of $B(q)$.

We now restrict to the case $(\frac{q}{p}) = 1$ (the other is completely analogous). It is not hard to see that the group G and the involution δ, acting on $\tilde{O}$-ideals generate a dihedral group D of order $2(p+1)$. Concretely, $\delta u \delta = u^{-1}$. In particular, this relation allows us to restrict our attention to the matrix A. We let $A_{i,j}$ be the $r_i/2 \times r_j/2$ submatrix of A corresponding to the columns J_l^j and the rows J_m^i with $l = 0, 2, \dots, r_j$ and $m = 0, 2, \dots, r_i$.

We index the rows and columns of $A_{i,j}$ by indices l, m modulo $r_i/2$ and $r_j/2$, respectively.

Proposition 11. *The matrix $A_{i,j}$ has the following properties:*

Let $r = \gcd(r_i/2, r_j/2)$. Then there exist coefficients $c(k)$ indexed by $k \bmod r$ such that the l, m entry of $A_{i,j}$ equals $c(m - l)$.

In practice this fact means, in particular, that the successive rows of $A_{i,j}$ are obtained from the first by a shift of one step to the right.

Lemma 6. *For $v \in G$ we have $v\tilde{O}_p = \tilde{O}_p v$.*

Proof. The order $v\tilde{O}_p v^{-1}$ is a suborder of O_p of index p; hence $v\tilde{O}_p v^{-1} = \tilde{O}_p$. □

Proof of Proposition 11. The entry $[l,m]$ of the matrix $A_{i,j}$ corresponds to the ideal $(J_l^j)^{-1}J_m^i$. The p-subideal $(J_1^j)_p = \tilde{O}_p\alpha_p$ for some element $\alpha_p \in O_p$ and since we assume that p does not divide the norm of the ideal class representatives, α_p determines an element $u^a \in G$. Hence $(J_1^j)_p = u^a\tilde{O}_p$ and similarly $(J_1^i)_p = u^b\tilde{O}_p$ for some $0 \le a, b < p+1$. Therefore, $(J_l^j)_p = u^{a+2l}\tilde{O}_p$ and $(J_m^i)_p = u^{b+2m}\tilde{O}_p$. It follows that the p-subideal $((J_l^j)^{-1}J_m^i)_p$ equals $u^{b-a+2m-2l}\tilde{O}_p$, by Lemma 6. We have then that $(J_l^j)^{-1}J_m^i = u^{2(m-l)}((J_1^j)^{-1}J_1^i)$. Since, by definition, u^{r_i} sends J_1^i to an equivalent p-subideal and analogously for u^{r_j} and J_1^j, the $[l,m]$ entry of $A_{i,j}$ depends only on the residue of $m-l$ modulo r. □

5. The subspace V_0

Let V be the vector space of complex valued functions on the classes of left $\tilde{O}$-ideals. The dihedral group D generated by δ and G defined earlier has a left action on V by means of

$$\gamma f(J) := f(\gamma^{-1}J), \qquad \gamma \in D.$$

We consider the subspace V_0 of V of functions f_0 satisfying

$$f_0(u^2J) = -f_0(J),$$

where u is any generator of G.

Note that if $p \equiv 1 \bmod 4$, this space is identically zero as G has order $p+1$. For $p \equiv 3 \bmod 4$ we may describe V_0 in a more conceptual way as the ρ-isotypical component of V with ρ the 2-dimensional irreducible representation of D induced from any of the two characters of G of order 4.

We may further split the space V_0 into two subspaces $V_0^{\pm}$ where δ acts as ± 1. It is easy to verify that any generator u of G takes V_0^+ isomorphically into V_0^- and vice versa.

Theorem 2. *The subspaces $V_0^{\pm}$ are stable under the action of all Brandt matrices $B(q)$.*

Proof. We first prove that V_0 is stable under the Brandt matrices. Let $v_i = (1, -1, \ldots, -1)$ of length $r_i/2$ and similarly let $v_j = (1, -1, \ldots, -1)$ of length $r_j/2$. We consider the case where $(\frac{q}{p}) = 1$; the other case is completely analogous. Using the choice of basis above, it is enough to prove that $A_{i,j}v_j = \lambda v_i$ for some $\lambda \in \mathbb{Z}$ and this is clear from the form of the matrix $A_{i,j}$ given by Proposition 11. It is also easy to see that $\lambda = 0$ if $r_i/2$ is odd.

Since δ commutes with $B(q)$ (see Proposition 10), the subspaces $V_0^{\pm}$ are also stable under the action of the Brandt matrices. □

We let $B_0(q)$ be the matrix $B(q)$ restricted to V_0^+. One of the main motivations for considering this subspace is that it contains, for $p > 3$, a copy of the space of modular forms of weight 2 and level p^2 with CM by the ring of integers of $\mathbb{Q}(\sqrt{-p})$. The proof of this fact is given by Benedict Gross in the appendix and uses the local and global Jacquet-Langlands correspondence. Concretely, it is the subspace

$V_{\mathrm{CM}}^+ \subset V_0^+$ characterized by the vanishing of $B_0(q)$ for all primes q with $(\frac{q}{p}) = -1$; clearly, V_{CM}^+ is stable under the Hecke algebra. For $p > 3$, V_{CM}^+ has dimension $h(-p)$, the class number of $K = \mathbb{Q}(\sqrt{-p})$, and it can be identified with the tangent space of an abelian variety $\mathcal{B}(p)/\mathbb{Q}$ obtained as the restriction of scalars of a certain elliptic curve $A(p)$ with CM by the ring of integers of K (see [Gr]). For $p = 3$ both V_{CM}^+ and V_0^+ are zero.

We now obtain a formula for the dimension of V_0^+.

Proposition 12. *For a prime $p > 3$ and congruent to 3 modulo 4 the dimension of V_0^+ is given by*

$$\dim(V_0^+) = \frac{1}{12}(p+5) + \frac{1}{3}\left(1 - \left(\frac{-3}{p}\right)\right) - \frac{1}{2}\left(1 - \left(\frac{2}{p}\right)\right).$$

Proof. Note that the first part of the formula is the number of ideals for the maximal order (for $p \equiv 3 \bmod 4$). By Corollary 3 to compute the number of nonequivalent p-subideals of a given ideal $I = I_j$, we need to compute $w' = |O'^{\times}|/|\tilde{O}'^{\times}|$ where O' is the right order of I. We claim that $w' = 1, 2$ or 3. Let $u \in O'$ be a unit. Since all elements in B satisfy a quadratic polynomial, the field $F = \mathbb{Q}[u]$ is an imaginary quadratic field. If $u \neq \pm 1$, then u is a primitive root of order 3 or 4. In both cases, if there is an embedding of $\mathbb{Z}[u]$ into O', it is unique up to conjugation because the class number of $\mathbb{Z}[u]$ is one. The existence of such an embedding into some maximal order is determined by the quadratic symbols $(\frac{-3}{p})$ and $(\frac{-4}{p})$, respectively. It is known that $\mathbb{Z}[i]$ and $\mathbb{Z}[(1+\sqrt{-3})/2]$ embed into the *same* maximal order only for $p = 2$ or 3. Hence, in the first case $w' = 3$ and in the second $w' = 2$ since (by Proposition 9) $\tilde{O}'^{\times}$ is of order 2. By Corollary 3, $r_j = (p+1)/w'$; hence if $w' = 3$, then r_j is always even and if $w' = 2$, then r_j is even if and only if $p \equiv 7 \bmod 8$. The formula now follows. ☐

6. Tables

The calculations in Table 1 were made with PARI-GP [GP] (check the website [PRV] for the corresponding routines).

Table 1.

p	$\dim V_0^+$	$\dim V_{\mathrm{CM}}^+$
7	1	1
11	1	1
19	1	1
23	3	3
31	3	3
43	3	1
47	5	5
59	5	3
67	5	1
71	7	7
79	7	5
83	7	3
103	9	5

Example 1. Let $p = 11$. In this case the class number for maximal orders is 2; hence the matrix $A_{i,j}$ will have four blocks. The first Brandt matrices are below.

$$B(2) = \left[\begin{array}{ccccc|ccccc} 0&0&0&0&0&1&0&0&1&1\\ 0&0&0&0&0&0&1&0&1&1\\ 0&0&0&0&0&0&0&1&1&1\\ 0&0&0&0&0&1&1&1&0&0\\ 0&0&0&0&0&1&1&1&0&0\\ \hline 1&0&0&1&1&0&0&0&0&0\\ 0&1&0&1&1&0&0&0&0&0\\ 0&0&1&1&1&0&0&0&0&0\\ 1&1&1&0&0&0&0&0&0&0\\ 1&1&1&0&0&0&0&0&0&0 \end{array}\right],$$

$$B(3) = \left[\begin{array}{ccccc|ccccc} 2&0&0&1&1&0&0&0&0&0\\ 0&2&0&1&1&0&0&0&0&0\\ 0&0&2&1&1&0&0&0&0&0\\ 1&1&1&0&1&0&0&0&0&0\\ 1&1&1&1&0&0&0&0&0&0\\ \hline 0&0&0&0&0&2&0&0&1&1\\ 0&0&0&0&0&0&2&0&1&1\\ 0&0&0&0&0&0&0&2&1&1\\ 0&0&0&0&0&1&1&1&0&1\\ 0&0&0&0&0&1&1&1&1&0 \end{array}\right].$$

Example 2. Let $p = 47$. In this case $V_0^+ = V_{\mathrm{CM}}^+$ is of dimension 5. We give some examples of the matrices $B_0(q)$ for q with $(\frac{q}{p}) = 1$; since $V_{\mathrm{CM}}^+ = V_0^+$, we know that $B_0(q)$ vanishes for $(\frac{q}{p}) = -1$.

$$B_0(2) = \begin{pmatrix} 1&2&0&0&0\\ 1&0&1&0&1\\ 0&1&1&1&0\\ 0&0&1&-2&0\\ 0&3&0&0&0 \end{pmatrix}$$

and

$$B_0(3) = \begin{pmatrix} 0&0&2&2&0\\ 0&1&1&-2&0\\ 1&1&-2&0&0\\ 1&-2&0&0&1\\ 0&0&0&3&1 \end{pmatrix}.$$

Table 2 shows the abelian varieties $\mathcal{B}(p)$ corresponding to V_{CM}^+ for small p labeled as in William Stein's list. Table 3 is the corresponding table for subspaces of V_0^+ stable by the Hecke algebra in the complement of V_{CM}^+.

The case of $p = 79$ is interesting. It is the only case with $p \leq 400$ where the complement of V_{CM}^+ in V_0^+ contains 1-dimensional Hecke stable subspaces. By calculations of Cremona the two subspaces correspond to the elliptic curve of the

TABLE 2.

p	Label	dim
7	49A	1
11	121A	1
19	361A	1
23	529F	3
31	961G	3
43	1849A	1
47	2209F	5
59	3481C	3
67	4489A	1
71	5041F	7
79		5
83		3

TABLE 3.

p	Label	dim
43	1849E	2
59	3481A	2
67	4489E	4
79	6241A	1
79	6241B	1
83		4

equation

$$y^2 + xy = x^3 - x^2 - 64x - 179$$

and its quadratic twist by $\mathbb{Q}(\sqrt{-79})$.

APPENDIX

We will prove that the space of CM modular forms of weight 2 and level p^2 injects into the space V_0. Let $\tilde{O}_p^\times$ (respectively $O_p^\times$) be the group of invertible elements of $\tilde{O}_p$ (respectively of O_p). Then the quotient $O_p^\times/\tilde{O}_p^\times$ is isomorphic to the group G; hence $O_p^\times$ contains a unique subgroup K_p such that $O_p^\times/K_p$ is cyclic of order 4. Note that the group $\tilde{O}_p^\times$ is equal to $\mathbb{Z}_p^\times(1+\mathcal{P})$ where $\mathcal{P}$ is the unique integral order of norm p in B_p. Define

$$M := \{f : K_p \times \prod_{l \neq p} O_l^\times \backslash \hat{B}^\times / B^\times \to \mathbb{C}\}. \tag{7}$$

Translating back to the language of ideals of B as in the body of the paper, we can identify M with the subspace of V where u^4 acts trivially with u a generator of G.

Recall that we have defined

$$V_{\mathrm{CM}} := \left\{ f \in M : f|T_l = 0 \text{ for all } \left(\frac{l}{p}\right) = -1 \right\} \tag{8}$$

where T_l is the l-th Hecke operator. Recall the involution δ defined in (3); it acts on M commuting with the T_l and hence also gives an involution of M_{CM}. We may therefore decompose M and M_{CM} into their eigenspaces $M^\pm, M_{\mathrm{CM}}^\pm$ with respect to δ.

Let $[u]$ be a generator of $O_p^\times/K_p$. Then we can identify the space V_0 with the functions $f \in M^+$ such that $f|[u^2] = -f$.

Theorem 3. *$M_{\mathrm{CM}}^\pm \subset V_0^\pm$ and has dimension $h(-p)$ if $p \geq 7$.*

Proof. We know that the space of cusp forms F of weight 2 for $\Gamma_0(p^2)$ with complex multiplication by $\mathbb{Q}(\sqrt{-p})$ has dimension $h(-p)$ (see [Gr]). By a theorem of Serre (see Theorem 17, [Se]) this space is characterized by the condition that $F|T_l = 0$ for all primes l with $\left(\frac{l}{p}\right) = -1$. This gives $h(-p)$ automorphic representations

$$\pi = \pi_\infty \otimes \pi_p \otimes \bigotimes_{l \neq p} \pi_l$$

of $PGl_2(\mathbb{A})$ with

- π_∞ a discrete series of weight 2 for $PGl_2(\mathbb{R})$,
- π_p an irreducible representation of $PGl_2(\mathbb{Q}_p)$ of conductor p^2,
- π_l an irreducible unramified representation of $PGl_2(\mathbb{Q}_l)$ with Hecke eigenvalues $a_l = 0$ if $\left(\frac{l}{p}\right) = -1$.

The local Jaquet-Langlands correspondence gives a bijection between irreducible, square-integrable, representations π_v of $PGl_2(\mathbb{Q}_v)$ and finite dimensional, irreducible representations π_v' of $B_v^\times/\mathbb{Q}_v^\times$, where B_v is the quaternion division algebra over $\mathbb{Q}_v$. The local correspondence is characterized by the identity $\mathrm{Tr}(t|\pi_v) + \mathrm{Tr}(t|\pi_v') = 0$ for all regular elliptic conjugacy classes t.

If π_∞ is the weight 2 discrete series of $PGl_2(\mathbb{R})$, then π_∞' is the trivial representation of $\mathbb{H}^\times/\mathbb{R}^\times = SO_3$.

If π_p has conductor p^{n+1}, then π_p' is trivial on the subgroup $1 + \pi_p^n O_p$ of $B_p^\times$.

We want to apply this to the local component π_p of our CM forms. First, we must check that π_p is square-integrable. In fact we will show it is a cuspidal representation by checking that its Langlands parameter $\sigma(\pi_p) : W(\mathbb{Q}_p) \to Gl_2(\mathbb{C})$ gives an irreducible 2-dimension representation of the local Weil group.

By construction of the CM forms, we have

$$\sigma(\pi_p) = \mathrm{Ind}_{W(k_p)}^{W(\mathbb{Q}_p)} \chi_p \tag{9}$$

where $k_p = \mathbb{Q}_p(\eta_p)$, with $\eta_p = \sqrt{-p}$, and χ_p is the local component of our Hecke characters of conductor (η_p). Since $\left(\frac{-1}{p}\right) = -1$, we have $\chi_p(-1) = -1$. Hence if τ is the nontrivial automorphism of k_p over $\mathbb{Q}_p$,

$$\chi_p^\tau(\eta_p) = \chi_p(\eta_p^\tau) = \chi_p(-\eta_p) = -\chi_p(\eta_p) \tag{10}$$

and $\chi_p^\tau \neq \chi_p$. This shows that $\sigma(\pi_p)$ is irreducible by Mackey's criterion for induced representations.

We will now determine the corresponding irreducible representations π_p' of $D = B_p^\times/(1 + \eta_p O_p)\mathbb{Q}_p^\times$. D is a dihedral group of order $2(p+1)$, with normal subgroup $G = O_p^\times/(1 + \eta_p O_p)\mathbb{Z}_p^\times \simeq \mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times$. Hence any irreducible representation of D has dimension 1 or 2.

Since π_p satisfies $\pi_p \otimes \epsilon_p(\det) \simeq \pi_p$, where ϵ_p is the quadratic character of $\mathbb{Q}_p$ associated to the extension $k_p = \mathbb{Q}_p(\sqrt{-p})$, the same holds for π_p': $\pi_p' \otimes \epsilon_p(G) \simeq \pi_p'$.

This is false if π_p' is 1-dimensional, so we must have

$$\pi_p' = \mathrm{Ind}_G^D(\gamma) = \mathrm{Ind}_G^D(\gamma^{-1}) \tag{11}$$

for some character γ of G with $\gamma \neq \gamma^{-1}$ (so $\gamma^2 \neq 1$). (This is the representation of D denoted by ρ at the beginning of §4.) Since $\epsilon(G)$ on $\mathbb{F}_{p^2}^\times$ is just the quadratic character β of G, we have that $\gamma\beta = \gamma^{-1}$. Equivalently $\gamma^2 = \gamma^{-2} = \beta$ and (γ, γ^{-1}) are the two characters of order 4 of G. Hence the subgroup K_p of index 4 in $O_p^\times$ acts trivially on π'_p. Let $[u]$ be a generator of G. Since the action of G on $\mathrm{Ind}_G^D(\gamma)$ is given by $\begin{pmatrix} \gamma & 0 \\ 0 & \gamma^{-1} \end{pmatrix}$ in an appropriate basis, $[u^2]$ acts as -1. Therefore, the CM modular forms are actually in the space V_0.

Any D-subrepresentation $W \subset V_0$ splits as a sum $W = W^+ \oplus W^-$ of spaces $W^\pm$ of half the dimension where δ acts by ± 1.

To recapitulate, the local representations π_∞ and π_p occur in the local Jaquet-Langlands correspondence, and we have identified π'_∞ and π'_p. By the global correspondence if $\pi = \pi_\infty \otimes \pi_p \otimes \bigotimes_{l \neq p} \pi_l$ is an automorphic cuspidal representation of $PGl_2(\mathbb{A})$, then $\pi' = \pi'_\infty \otimes \pi'_p \otimes \bigotimes_{l \neq p} \pi_l$ is an automorphic cuspidal representation of $B_{\mathbb{A}}^\times / \mathbb{A}^\times$ which appears with multiplicity one in the space of automorphic forms. Since we have $h(-p)$ such irreducible π''s and each contributes a 2-dimensional space to M_{CM}, we get a space of dimension $2h(-p)$. Taking $\pm$-eigenspaces under δ, we conclude that $V_{\mathrm{CM}}^\pm \subset V_0^\pm$ with $V_{\mathrm{CM}}^\pm$ of dimension $h(-p)$ as claimed. □

References

[Ei] M. Eichler, *Lectures on modular correspondences*, Bombay, Tata Institute of Fundamental Research, 1955-56.

[Gr] B. Gross, *Arithmetic on elliptic curves with complex multiplication*, with an appendix by B. Mazur, Lecture Notes in Mathematics, **776**, Springer, Berlin, 1980. MR81f:10041

[Ma] Magma computational algebra system `http://magma.maths.usyd.edu.au/magma/`.

[GP] PARI-GP `http://www.parigp-home.de/`.

[Ko] D. Kohel, *Hecke module structure of quaternions*, Class field theory—its centenary and prospect (Tokyo, 1998), 177–195, Adv. Stud. Pure Math., **30**, Math. Soc. Japan, Tokyo, 2001. MR2002i:11059

[Pi] A. Pizer, *Theta Series and Modular Forms of Level p^2M*, Compositio Mathematica, Vol. **40**, Fasc. 2, 1980, p. 177–241. MR81k:10040

[Pi2] A. Pizer, *An Algorithm for Computing Modular Forms on $\Gamma_0(N)^*$*, Journal of Algebra **64**, 1980, 340–390. MR83g:10020

[PRV] A. Pacetti and F. Rodriguez-Villegas, `www.ma.utexas.edu/users/villegas/cnt/cnt.html`.

[Se] J.-P., Serre, *Quelques applications du théoreème de Chebotarev*, Publ. Math. IHES, **54** (1981), 123–201. MR83k:12011

[Vi] M. F. Vigneras, *Arithmetique des algebres de quaternions*, Lecture Notes in Mathematics, **800**. MR82i:12016

Department of Mathematics, University of Texas at Austin, Texas 78712
E-mail address: `apacetti@math.utexas.edu`

Department of Mathematics, University of Texas at Austin, Texas 78712
E-mail address: `villegas@math.utexas.edu`

Department of Mathematics, Harvard University, Cambridge, Massacusetts 02138
E-mail address: `gross@math.harvard.edu`