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 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 $\infty$.

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 (for non-square free level say) to effectively work with smaller dimensional Hecke stable subspaces of modular forms. This appears to be a useful principle that could be exploited further.

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 $\infty$ (such an algebra is unique up to isomorphism). We write $N(x)$ for the reduced norm of an element $x \in B$, and $Tr(x)$ for its reduced trace.

Definitions:

The first named 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.
(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 $O_l(I) := \{x \in B \mid xI \subset I\}$; similarly, its right order is $O_r(I) := \{x \in B \mid Ix \subset I\}$.
(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 $I_q = O_qa_q$ for some $a_q \in (B \otimes \mathbb{Q}_q)$. 
(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 $N_I : I \to \mathbb{Z}$ as $x \mapsto N(x)/N(I)$.
(8) Given a lattice $I$ its dual is $I^* := \{b \in B \mid Tr(bI) \subset \mathbb{Z}\}$
(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, page 86]. □

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

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

**Remark** It is not hard to verify that $I^\# = \mathcal{P}I$, 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 $\alpha$ 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 $I^\# = \mathcal{I}^\#$ and replacing $I$ by $\mathcal{I}$ we get that $O_r(I) \subset O_l(I^\#)$. 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 $\mathbb{Z}_q^*$ the determinant of multiplication by $\alpha_q$, 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 $I^\# \subset J \subset I$. Then $O_l(J) = \mathbb{Z} + O^* \subset O$ with index $p$. Furthermore $OJ = I$ and $N(J) = N(I)$. 

Proof: Clearly \( O_l(J) \) contains \( \mathbb{Z} + O' \). Since \( I/I' \) is a one dimensional vector space over \( O/O' \cong \mathbb{F}_p \) (by Theorem 1), and \( J/I' \) is a submodule of index \( p \), necessarily \( O_l(J) \) must equal the proper submodule \( \mathbb{Z} + O' \) 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 \( \hat{O} = \mathbb{Z} + \mathcal{P} \) the unique suborder of level \( p^2 \) in \( O \) (see [Pi, Lemma 1.4 p. 181]) and \( h, \hat{h} \) the class numbers of \( O, \hat{O} \) respectively.

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

Proof: Let \( I \) be such a lattice. By Proposition 1, for all primes \( q \neq p \), \( I_q \) is principal, since \( \hat{O}_q = O_q \). 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, \( \hat{O}_p a_p \subset I_p \subset O_p I_p \). Since \( O_p I_p \) is an ideal for \( O_p \) of the same norm as \( I_p \) we have by Lemma 1 that \( O_p I_p = \hat{O}_p a_p \). On the other hand, the index of \( \hat{O}_p \) in \( O_p \) is \( p \), hence, \( I_p = \hat{O}_p a_p \). \( \square \)

Proposition 4. Let \( I \) be a left \( \hat{O} \)-ideal then

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 \( \left( \cdot \right) \) 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 \( \chi(I) = \chi(I) \) where the bar denotes conjugation.\( \chi(I^{-1}) = \chi(I) \).

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 \( O_1(I_1) = O_2 \) then \( \chi(I_1 I_2) = \chi(I_1) \chi(I_2) \).

Proof: Pick \( x_j \in I_j \) for \( j = 1, 2 \) with \( p \mid N_I(x_j) \) 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 \( \hat{O} \)-ideals representatives

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

\begin{itemize}
  \item \( (\frac{1}{2}(1 + j), \frac{1}{2}(pi + k), j, k) \) with \( a = -1, b = -p \) if \( p \equiv 3 \) mod 4
  \item \( (\frac{1}{2}(1 + j + k), \frac{1}{2}(pi + 2j + k), j, k) \) with \( a = -2, b = -p \) if \( p \equiv 5 \) mod 8
  \item \( (\frac{1}{2} + \frac{pj}{2}, \frac{i}{2} + \frac{k}{2}, k, \frac{p}{2}, \frac{\bar{k}}{2} + \frac{s}{q}) \) with \( a = -p, b = -q \) if \( p \equiv 1 \) mod 8 where \( q \) is a prime such that \( \left( \frac{q}{p} \right) = -1 \), \( q \equiv 3 \) mod 4 and \( s \) is an integer with \( s^2 \equiv -p \) mod \( q \) and \( s \equiv -q \) mod \( p \)
\end{itemize}

Proof: This is just an easy but tedious computation. Note that in the case \( p \equiv 1 \) mod 8 the maximal order we are considering is \( M = (\frac{1}{2} + \frac{j}{2}, \frac{i}{2} + \frac{k}{2}, k, \frac{p}{2}, \frac{\bar{k}}{2} + \frac{s}{q}) \).

The conditions on \( s \) makes this an order, and is easy to check it is maximal, but it differs from the one defined in [Pi] Proposition 5.2 \( \square \)
Given a left $O$-ideal $I$, by Lemma 2 and Proposition 3 there are $p + 1$ $\tilde{O}$-left ideals $J$ with
\[ I' \subset J \subset I, \quad [I : J] = [J : I'] = p. \]
We call any such $J$ a p-subideal of $I$.

**Proposition 6.** Any p-subideal $J$ is of the form $I'[v]$ for some $v \in I$ and for any such $v$ we have $p \not| N_I(v)$.

**Proof:** Since $J$ has index $p$ in $I$, it is clear that $J = I'[v]$ for some $v \in I$, $v \not\in I'$, and locally all these ideals are equal for all primes $q \neq p$. Let $I_p = O_p a_p$, then we saw that $I_p' = O_p a_p$; since $v \in I$, $v = ua_p$ with $u \in O_p$. If $p|N_I(v)$, then $p|N(u)$ hence $u \in O_p$ and we would have that $J \subset I'$. $\square$

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 $J_i \subset I_i$, for $i = 1, 2$ corresponding $p$-subideals. If $I_1$ and $I_2$ are non-equivalent 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. $\square$

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 $\alpha$ 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 $O_q J_q = J_q = I^j_q$, 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 $I^j_p = O_p a_p$. Since $O_p J_p = I_p$, we have that $O_p a_p = O_p a_p$ so $I^j_p = O_p a_p$; therefore $|I^j_p/(J_p\alpha^{-1})| = |O_p a_p/O_p a_p| = p$.

Since $J\alpha^{-1} \subset I^j$ with index $p$, to see that $I^j \subset J\alpha^{-1}$ it is enough to check locally $p$. 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 $I^j_p = O_p a_p$. Also $O_p^h \subset \tilde{O}_p$, therefore $O_p^h a_p \subset O_p b_p a^{-1} = \tilde{O}_p b_p \alpha^{-1} = J_p\alpha^{-1}$. $\square$

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 $u \in O_v(I)^\times$.

**Corollary 3.** Given a left $O$-ideal $I$ the number of non-equivalent $p$-subideals $J \subset I$ is $(p + 1)|O_v(I)^\times|/|O_v(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 [Pt2]. $\square$

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

**Corollary 4.** We have
\[ \tilde{h} = (p + 1) \sum_{j=1}^{h} \frac{|\tilde{O}_j^\times|}{|O_v(I)^\times|}. \]
If \( p > 3 \) then \( \hat{h} = (p^2 - 1)/12 \).

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

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

The components \( \alpha_q \) of \( \alpha \) are as follows: for \( q \neq p \) we set \( \alpha_q = 1 \) and for \( q = p \) we want \( \alpha_p \) 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 \( \delta \) the involution

\[
\delta : J \mapsto \alpha J
\]

Note that if \( J \) and \( J' \) are equivalent then so are \( \delta J \) and \( \delta J' \).

3.1. **Construction of \( \alpha_p \).** 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 \( \alpha_p \) to be one of \( i \) or \( j \).
2. If \( p \equiv 3 \mod 4 \) then \( -1 \) is a non-square and we look for \( \alpha_p \) with norm \(-p\). If \( \alpha = x_1i + x_2j + x_3k \), with \( i^2 = -1, j^2 = -p = k^2 \), then \( N(\alpha_p) = x_1^2 + p(x_2^2 + x_3^2) \). 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 \( x_2^2 + x_3^2 = 0 \mod p \), and then lifting the solution using Hensel’s lemma.

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

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

**Proof:** In order that \( \alpha_p^*J \supset Jp^r \) we must have \( \alpha_p^{-1}p^r \in \hat{O} \). Note that if \( \beta \in O \) then \( p\beta \in \hat{O} \); 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 is enough to take

\[
s \geq \left\lceil \frac{v_p(N(\alpha_p))}{2} \right\rceil + 1. \quad \Box
\]

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 \( \alpha J \). 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

\[
\alpha_p u_j \equiv v_j \mod p^r J_p, \quad j = 1, \ldots, 4,
\]

with \( p^r v_j \in J \) 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
Lemma 5. Given a left \( \bar{O} \)-ideal \( J \) let \( \alpha_p \) be as constructed above. In order to compute \( \alpha_pJ \) it is enough to know \( \alpha_p \) 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 \( \{p, pi, pj, pk\} \subset \bar{O} \). 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, \( p^{r+1}\alpha_pu_t \in p^rI \) and the denominator of the \( x_j \) is at most \( r + 1 \).

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

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 \( O_p/O_p^\times \) is isomorphic to \( \mathbb{F}_p^\times \) and \( \bar{O}_p/O_p^\times \) to \( \mathbb{F}_p \). Let \( S := (O_p/O_p^\times)^\times \), a cyclic group of order \( p^2 - 1 \). Given a \( \bar{O} \)-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 \( \bar{O} \)-ideals with stabilizer \( (O_p/O_p^\times)^\times \). It is also easy to check that \( S \) acts on the set of \( p \)-subideals making it a principal homogeneous space for \( G := (O_p/O_p^\times)/(\bar{O}_p/O_p^\times)^\times \), a cyclic group of order \( p + 1 \).

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

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 \( u^rJ \) is equivalent to \( J \). Note that \( r \) is necessarily even since \( \mathcal{J} \) decomposes into two subsets, according to the value of \( \chi \), which are in bijection by \( \delta \). Also, if \( u \in G \) then \( u^{-1} \) is its inverse since \( u\bar{u} = N(u) \) and \( N(u) \in \bar{O}_1 \).

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 \( \{I^1, \ldots, I^{h(O)}\} \) of left \( O \)-ideals classes (using Pizer’s algorithm for the level \( p \) case) and 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

\[
J_0, J_2, \ldots, J_{r-2}, J_1, J_3, \ldots, J_{r-1}
\]
For Proposition 10.

Consider the following.

One of the important things of ordering the basis in this form is the

where each

in (4).

Proposition 11.

The matrix

respectively.

followed by those with

this relation allows to restrict our attention to the matrix

A

for classes of

p-subideals. First we put the classes with

\( \chi = +1 \)

\( \chi = -1 \)

\( h = h(O) \)

where

\( J_j^i \)

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 \( h(\hat{O})/2 \times h(\hat{O})/2 \). Then the following holds.

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 \( \left( \frac{q}{p} \right) = 1 \) (the other is completely analogous). It is

not hard to see that the group \( G \) and the involution \( \delta \), acting on \( \hat{O} \)-ideals generate a

dihedral group \( D \) of order \( 2(p + 1) \). Concretely, \( \delta u \delta = u^{-1} \). In particular,

this relation allows 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 \( J_i^l \)

and the rows \( J_m^r \) with

\( l = 0, 2, \ldots, r_j \) and \( m = 0, 2, \ldots, r_i \).

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 exists coefficients \( c(k) \) indexed by \( k \) mod \( r \)

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 1 step to the right.

Lemma 6. For \( v \in G \) we have \( v\hat{O}_p = \hat{O}_p v \)
Proof: The order $v\hat{O}_p v^{-1}$ is a suborder of $O_p$ of index $p$ hence $v\hat{O}_p v^{-1} = \hat{O}_p$. □

Proof of Prop: The entry $[l, m]$ of the matrix $A_{i,j}$ corresponds to the ideal $(J_l^1)^{-1}J_m$. The $p$-subideal $(J_l^1)_p = \hat{O}_p \alpha_p$ for some element $\alpha_p \in O_p$ and since we assume that $p$ does not divide the norm of the ideal class representatives, $\alpha_p$ determines an element $n^a \in G$. Hence $(J_l^1)_p = u^a \hat{O}_p$ and similarly $(J_l^1)_p = u^b \hat{O}_p$ for some $0 \leq a, b < p + 1$. Therefore, $(J_l^1)_p = u^{a+2l} \hat{O}_p$ and $(J_m)_p = u^{b+2m} \hat{O}_p$. It follows that the $p$-subideal $((J_l^1)^{-1}J_m)_p$ equals $u^{b-a+2m-2l} \hat{O}_p$, by Lemma 6. We have then that $(J_l^1)^{-1}J_m = u^{2(m-l)}((J_l^1)^{-1}J_l^1)$. Since, by definition, $u^r$ sends $J_l^1$ to an equivalent $p$-subideal and analogously for $u^r$ and $J_l^1$ 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 $\hat{O}$-ideals. The dihedral group $D$ generated by $\delta$ and $G$ defined earlier has a left action on $V$ by means of

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

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 $p \equiv 1 \pmod{4}$ this space is identically zero as $G$ has order $p + 1$. For $p \equiv 3 \pmod{4}$ we may describe $V_0$ in a more conceptual way as the $\rho$-isotypical component of $V$ with $\rho$ 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 $\delta$ acts as $\pm 1$. 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 $v_j = (1, -1, \ldots, -1)$ of length $r_j/2$. We consider the case where $\left(\frac{2}{p}\right) = 1$, 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 $\delta$ 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 to consider 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 an appendix, and uses the local and global Jacquet-Langlands correspondence. Concretely, it is the subspace $V_{CM}^+ \subset V_0^+$ characterized by the vanishing of $B_0(q)$ for all primes $q$ with $\left(\frac{2}{q}\right) = -1$; 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 $B(p)/\mathbb{Q}$ obtained as the restriction of scalars of an 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 $p \equiv 3 \mod 4$). 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 $\left(\frac{-3}{p}\right)$ and $\left(\frac{-4}{p}\right)$ 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) $O'^\times$ 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 $p \equiv 7 \mod 8$. The formula now follows. □

6. Tables

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

<table>
<thead>
<tr>
<th>$p$</th>
<th>$\dim V_0^+$</th>
<th>$\dim V^+_{CM}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>31</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>43</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>47</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>59</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>67</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>71</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>79</td>
<td>7</td>
<td>5</td>
</tr>
<tr>
<td>83</td>
<td>7</td>
<td>3</td>
</tr>
<tr>
<td>103</td>
<td>9</td>
<td>5</td>
</tr>
</tbody>
</table>

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

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

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

Here is a table with the abelian varieties $B(p)$ corresponding to $V_{CM}^+$ for small $p$ labeled as in William Stein’s list.
Here is the corresponding table for subspaces of $V_0^+$ stable by the Hecke algebra in the complement of $V_{\text{CM}}^+$. 

<table>
<thead>
<tr>
<th>$p$</th>
<th>Label</th>
<th>dim</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>49A</td>
<td>1</td>
</tr>
<tr>
<td>11</td>
<td>121A</td>
<td>1</td>
</tr>
<tr>
<td>19</td>
<td>361A</td>
<td>1</td>
</tr>
<tr>
<td>23</td>
<td>529F</td>
<td>3</td>
</tr>
<tr>
<td>31</td>
<td>961G</td>
<td>3</td>
</tr>
<tr>
<td>43</td>
<td>1849A</td>
<td>1</td>
</tr>
<tr>
<td>47</td>
<td>2209F</td>
<td>5</td>
</tr>
<tr>
<td>59</td>
<td>3481C</td>
<td>3</td>
</tr>
<tr>
<td>67</td>
<td>4489A</td>
<td>1</td>
</tr>
<tr>
<td>71</td>
<td>5041F</td>
<td>7</td>
</tr>
<tr>
<td>79</td>
<td>6241A</td>
<td>1</td>
</tr>
<tr>
<td>79</td>
<td>6241B</td>
<td>1</td>
</tr>
<tr>
<td>83</td>
<td></td>
<td>3</td>
</tr>
</tbody>
</table>

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

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

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

**Appendix A. by B. Gross**

We will prove that the space of CM modular forms of weight 2 and level $p^2$ injects into the space $V_0$. Let $\hat{O}_p^\times$ (respectively $O_p^\times$) be the group of invertible elements of $\hat{O}_p$ (respectively of $O_p$). Then the quotient $O_p^\times / \hat{O}_p^\times$ 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 $\hat{O}_p^\times / K_p$ 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:

$$M := \{ f : K_p \times \prod_{l \neq p} O_l^\times \backslash \hat{B}_p^\times / B_p^\times \rightarrow \mathbb{C} \}.$$ (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

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

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

Let $[u]$ be a generator of $O_\mathbb{F}_p^\times/K_p$, then we can identify the space $V_0$ with the functions $f \in M^+$ such that $f([u^2]) = -f$.

**Theorem 3.** $M^\pm_{CM} \subset V^\pm_0$ 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 Thm 17, [Sel]) 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:

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

of $PGL_2(\mathbb{A})$ with:

- $\pi_{\infty}$ a discrete series of weight 2 for $PGL_2(\mathbb{R})$
- $\pi_p$ an irreducible representation of $PGL_2(\mathbb{Q}_p)$ of conductor $p^2$.
- $\pi_l$ 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 $\pi_\nu$ of $PGL_2(\mathbb{Q}_\nu)$ and finite dimensional, irreducible representations $\pi'_\nu$ of $B_\nu^\times/\mathbb{Q}_\nu^\times$, where $B_\nu$ is the quaternion division algebra over $\mathbb{Q}_\nu$. The local correspondence is characterized by the identity $\text{Tr}(t|_{\pi_\nu}) = \text{Tr}(t|_{\pi'_\nu}) = 0$ for all regular elliptic conjugacy classes $t$.

If $\pi_{\infty}$ is the weight 2 discrete series of $PGL_2(\mathbb{R})$ then $\pi'_{\infty}$ is the trivial representation of $\mathbb{H}^\times/\mathbb{R}^\times = SO_3$.

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

We want to apply this to the local component $\pi_p$ of our CM forms. First, we must check that $\pi_p$ is square-integrable. In fact we will show it is a cuspidal representation, by checking that its Langlands parameter $\sigma(\pi_p): W(\mathbb{Q}_p) \rightarrow GL_2(\mathbb{C})$ gives an irreducible 2-dimensional representation of the local Weil group.

By construction of the CM forms, we have

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

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

$$\chi_p'(\eta_p) = \chi_p(\eta_p) = \chi_p(-\eta_p) = -\chi_p(\eta_p)$$

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

We will now determine the corresponding irreducible representations $\pi'_p$ 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 $G = O_p^\times/(1 + \eta_p O_p)\mathbb{Z}_p^\times \simeq \mathbb{F}_p^\times/\mathbb{F}_p^\times$. Hence any irreducible representation of $D$ has dimension 1 or 2.

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

This is false if $\pi'_p$ is 1-dimensional, so we must have:

$$\pi'_p = \text{Ind}_G^D(\gamma) = \text{Ind}_G^D(\gamma^{-1})$$
for some character \( \gamma \) of \( G \) with \( \gamma \neq \gamma^{-1} \) (so \( \gamma^2 \neq 1 \)). (This is the representation of \( D \) denoted by \( \rho \) at the beginning of \( \S 4 \).) Since \( \epsilon(G) \) on \( \mathbb{F}_p^\times \) is just the quadratic character \( \beta \) of \( G \), we have that \( \gamma \beta = \gamma^{-1} \). Equivalently \( \gamma^2 = \gamma^{-2} = \beta \) and \( (\gamma, \gamma^{-1}) \) are the two characters of order 4 of \( G \). Hence the subgroup \( K_p \) of index 4 in \( O_p^\times \) acts trivially on \( \pi_p' \). Let \( [u] \) be a generator of \( G \). Since the action of \( G \) on \( \text{Ind}_D^G(\gamma) \) is given by \( (\gamma_0 \gamma^{-1}) \) 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 \( \delta \) acts by \( \pm 1 \).

To recapitulate, the local representation \( \pi_\infty \) and \( \pi_p \) occur in the local Jaquet-Langlands correspondence, and we have identified \( \pi'_\infty \) and \( \pi'_p \). By the global correspondence if \( \pi = \pi_\infty \otimes \pi_p \otimes \otimes_{l \neq p} \pi_l \) is an automorphic cuspidal representation of \( \text{PGl}_2(k) \) then \( \pi' = \pi'_\infty \otimes \pi'_p \otimes \otimes_{l \neq p} \pi_l \) is an automorphic cuspidal representation of \( \text{B}_k^\times / \mathbb{A}^\times \) which appears with multiplicity one in the space of automorphic forms. Since we have \( h(-p) \) such irreducible \( \pi' \), and each contributes a 2-dimensional space to \( M_{\text{CM}} \), we get a space of dimension \( 2h(-p) \). Taking \( \pm \)-eigenspaces under \( \delta \) we conclude that \( V_{\text{CM}}^\pm \subset V_0^\pm \) with \( V_{\text{CM}}^\pm \) of dimension \( h(-p) \) as claimed. \( \square \)

References


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


[Vi] M. F. Vigneras, Arithmetique des algebres de quaternions Lecture Notes in mathematics 800.