COMPOSITIO MATHEMATICA

ARNOLD PIZER

Theta series and modular forms of level p^2M

Compositio Mathematica, tome 40, nº 2 (1980), p. 177-241

<http://www.numdam.org/item?id=CM_1980__40_2_177_0>

COMPOSITIO MATHEMATICA, Vol. 40, Fasc. 2, 1980, pag. 177–241

THETA SERIES AND MODULAR FORMS OF LEVEL p^2M

Arnold Pizer*

0. Introduction

Let p be an odd prime and M a positive integer prime to p. For a positive integer N, denote by $\Gamma_0(N)$ the congruence subgroup of level N, i.e. $\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2, Z) \mid c \equiv 0 \pmod{N} \right\}$ and let $S_k(N, \chi)$ denote the space of cusp forms of weight k and character χ on $\Gamma_0(N)$, χ a character of $(Z/N)^x$. If $\chi = 1$, we write $S_k(N) = S_k(N, 1)$. The purpose of this paper is to study the subspace of $S_k(N)$ generated by theta series attached to orders of level $N = p^2M$ in quaternion algebras (see [§2]) in the case $N = p^2M$. The analogous question for the case $N = p^{2r+1}M$ was studied in [13]. There we found for example that all newforms in $S_k(p^{2r+1}M)$ are linear combinations of theta series attached to orders of level $p^{2r+1}M$. The case $N = p^2M$ is quite different. If $N = p^2M$ we can construct as linear combinations of theta series attached to orders of level p^2M all newforms in $S_k(p^2M)$ that are not obtained from forms in $S_k(pM, \psi^2)$ by twisting by $\bar{\psi}$ where ψ ranges over all non trivial characters of $(Z/p)^x$ or from forms in $S_k(M)$ by twisting by the quadratic character φ mod p (see Proposition 8.5 below). The most interesting case (since we can handle the non-square level case by [13]) is when $N = p^2M$ is a square. In fact the case $N = p^2$ contains all the essential difficulties and new results.

In addition to identifying the subspace generated by theta series and giving the action of the Hecke operators on this subspace, we explicitly give the action of the R_p operator $\left(\text{twisting by the quadratic character } \left(\frac{-}{p}\right)\right)$ of Atkin–Lehner (see [1]). Also in §9 we define

* Research partially supported by NSF Grant MCS 77-03632.

0010–437X/80/02/0177–66$00.20/0

operators $\tilde{W}_\ell$ for ℓ prime, $\ell \mid N$ which act on the space of theta series by "ideal multiplication" (see Proposition 9.4). We show (Proposition 9.6) that the $\tilde{W}_\ell$ act just like the W_q operators of Atkin–Lehner (see [1]) and in fact we conjecture (see Conjecture 9.24) that they are essentially the W_q-operators. We prove (Corollary 9.23) that the product of the $\tilde{W}_\ell$ for $\ell \mid N$ is essentially equal to the product of the W_ℓ for $\ell \mid N$, i.e. essentially equal to the canonical involution. We keep saying "essentially" because one of the $\tilde{W}_\ell$ (in fact $\tilde{W}_p$) differs from the corresponding W_ℓ by a minus sign. The results of section 9 are applicable to the case of level $p^{2r+1}M$ and in that case they generalize the results of [14] to arbitrary weight $k \geq 2$ and also clearly imply the existence of $\tilde{W}_\ell$ operators in the case of level $p^{2r+1}M$. The final section of the paper contains a very explicit discussion of the case of level $N = p^2$. Theorems 10.1 and 10.3 show that the subspace $S_k^0(p^2)$ of $S_k(p^2)$ generated by newforms is a direct sum of a space of theta series and spaces obtained by twisting certain spaces of forms of level p and level 1 by appropriate characters. Also the results in section 10 on multiplicity 2 may be related to recent results of Labesse and Langlands giving counter examples to a 'multiplicity one' theorem holding for the representation theory for certain inner forms of $SL(2)$, see Remark 10.6.

Jacquet and Langlands in §16 of [6] (see also §10 of [4]) give a correspondence between automorphic representations attached to quaternion algebras and certain automorphic representations of $GL(2)$. The latter correspond to the classical modular forms on $\Gamma_0(N)$ we consider in this paper. Our Theorem 8.2 should afford a concrete realization of their correspondence in a special case.

The history of this paper began with Parry's thesis [11] where he considered the following problem. Can all newforms in $S_2(p^2)$ come from theta series? (As above we know that the answer is yes if the level is not a perfect square). Parry obtained a negative answer by explicitly constructing a basis for the subspace of cusp forms that do come from theta series in the case $p = 13$ and then comparing dimensions. Atkin using Parry's results was then able to determine that the missing forms (i.e. those not obtained from theta series) in the case $p = 13$ where those obtained from forms in $S_2(p, \psi^2)$ by twisting by the character $\bar{\psi}$ where ψ ran over the characters of $(Z/p)^x$ with $\psi^2 \neq 1$. This and other calculations led him to the obvious conjecture as to what the missing forms where in general for the case $S_2(p^2)$ and his questions to the author about this problem led directly to the present paper.

1. Local orders

In this section we begin to develop the theory of orders of higher level in local quaternion division algebras. We are particularly interested in the case of orders of 'level p^2', see Definition 1.3 below.

Fix an odd prime p and let $u \in Z$ be a quadratic non residue mod p. Q_p has two ramified quadratic field extensions $K = Q_p(\sqrt{p})$ and $K' = Q_p(\sqrt{up})$. Using these we define

$$B = \left\{ \begin{pmatrix} \alpha & \beta \\ u\beta^\sigma & \alpha^\sigma \end{pmatrix} \middle| \alpha, \beta \in K \right\} \text{ where } \sigma \text{ denotes}$$

conjugation of K/Q_p and

$$B' = \left\{ \begin{pmatrix} \alpha & \beta \\ u\beta^\sigma & \alpha^\sigma \end{pmatrix} \middle| \alpha, \beta \in K' \right\} \text{ where } \sigma \text{ denotes}$$

conjugation of K'/Q_p. Clearly B (resp. B') with the structure inherited from Mat(2, K) (resp. Mat(2, K')) is an algebra of dimension 4 over Q_p. It is easy to check directly that B(resp. B') is a division algebra and that the reduced norm (N) and reduced trace (tr) of B (resp. B') are just the determinant and trace of Mat(2, K) (resp. Mat(2, K')) restricted to B (resp. B'). Since there is a unique quaternion division algebra over Q_p up to isomorphism (see p. 154 of [8]), B and B' are isomorphic over Q_p. Now let $S = Z_p + Z_p\sqrt{p}$ (resp. $S' = Z_p + Z_p\sqrt{up}$) be the ring of integers of K (resp. K') and $P = (\sqrt{p})$ (resp. $P' = (\sqrt{up})$) be the maximal ideal of S (resp. S'). For non negative integers r we define the orders

$$M_{r+1} = \left\{ \begin{pmatrix} \alpha & \beta \\ u\beta^\sigma & \alpha^\sigma \end{pmatrix} \middle| \alpha \in S, \beta \in P^r \right\} \text{ of } B \tag{1.1}$$

and

$$M'_{r+1} = \left\{ \begin{pmatrix} \alpha & \beta \\ u\beta^\sigma & \alpha^\sigma \end{pmatrix} \middle| \alpha \in S', \beta \in P'^r \right\} \text{ of } B'.$$

Direct computation shows that if $x \in B$ and $N(x) \in Z_p$, then $x \in M_1$ and similarly for M'_1. Hence M_1 (resp. M'_1) is the unique maximal order of B (resp. B').

The notation introduced in the above paragraph will be used throughout the rest of this section. In particular p is always an odd prime.

PROPOSITION 1.1: *Let C be a quaternion division algebra over Q_p and let M be an order of C. Then M is isomorphic to M_s for some s if*

and only if M contains a subring isomorphic to S. Similarly, M is isomorphic to M'_s for some s if and only if M contains a subring isomorphic to S'.

PROOF: We recall that an order of C is a free Z_p submodule of C of rank 4 which is also a subring containing 1. We will prove the statement concerning M_s, the proof of the statement concerning M'_s being similar. We need only show that if M contains a subring isomorphic to S, then M is isomorphic to M_s for some s as the converse is obvious. C is isomorphic to B so we can identify C with B. Then we can assume (by conjugating M if necessary by an element of B^x) that M contains $S = \left\{ \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^\sigma \end{pmatrix} \middle| \alpha \in S \right\}$. Under this assumption we will show $M = M_s$ for some s. But since M_1 is the unique maximal order, $M \subseteq M_1$ and letting s be the greatest integer with $M \subseteq M_s$, we have $M = M_s$.

PROPOSITION 1.2: *M_s contains a subring isomorphic to S' if and only if $s = 1$ or 2. Similarly M'_s contains a subring isomorphic to S if and only if $s = 1$ or 2.*

PROOF: We again prove only the first statement. Clearly it suffices to show that S' can be embedded in M_2 but not in M_3. $S' = Z_p + Z_p\sqrt{up}$, so S' can be embedded in M_s if and only if M_s contains an element γ with $\mathrm{tr}(\gamma) = \mathrm{tr}(\sqrt{up}) = 0$ and $N(\gamma) = N(\sqrt{up}) = -up$. For M_2 such an element is given by $\gamma = \begin{pmatrix} b\sqrt{p} & c\sqrt{p} \\ -cu\sqrt{p} & -b\sqrt{p} \end{pmatrix}$ where $b, c \in Z_p$ satisfy $b^2 - uc^2 = u$. Such b and c exist since $Q_p(\sqrt{u})$ is an unramified extension of Q_p and every unit of Z_p is the norm of an element of $Z_p + Z_p\sqrt{u}$. Now suppose $\gamma = \begin{pmatrix} b\sqrt{p} & p(c + d\sqrt{p}) \\ up(c - d\sqrt{p}) & -b\sqrt{p} \end{pmatrix} \in M_3$ has $N(\gamma) = -up$. Then we have $u \equiv b^2 \pmod{p}$, a contradiction.

Combining Proposition 1.1 and 1.2, we see that we have the following arrangement of the orders M_s and M'_s in the quaternion division algebra over Q_p:

$$\begin{array}{ccccccc} M_1 & \supset & M_2 & \supset & M_3 & \supset & \cdots \\ \| & \neq & \| & \neq & & \neq & \\ M'_1 & \supset & M'_2 & \supset & M'_3 & \supset & \cdots \end{array}$$

and except for $s = 1$ or 2, M_s is never isomorphic to M'_s. Also it is obvious that M_s can not be isomorphic to M'_t if $s \neq t$. Thus considering $s = 2$, we have a canonical choice for the definition of an 'order of level p^2', so we give

DEFINITION 1.3: Let A be the quaternion division algebra over Q_p, p an odd prime. An order M of A is said to *level* p^2 if M is isomorphic (over Z_p) to the order M_2 in (1.1).

Henceforth we will be exclusively interested in orders of level p^2. We will show shortly that there is a unique order of index p in the maximal order of A and it is the unique order of level p^2 in A. First we need to give one last representation of A.

Let $L = Q_p(\sqrt{u})$ be the unique unramified quadratic field extension of Q_p, $R = Z_p + Z_p\sqrt{u}$ its ring of integers, and σ its conjugation over Q_p. We also let $v = \sqrt{u}$. Then as is easily checked

$$A = \left\{ \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix} \middle| \alpha, \beta \in L \right\} \tag{1.2}$$

is the (unique) quaternion division algebra over Q_p and

$$M_1 = \left\{ \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix} \middle| \alpha, \beta \in R \right\}$$

is the unique maximal order of A. The notation being as above, we have

LEMMA 1.4: *M_1, the maximal order of A, contains a unique suborder of index p.*

PROOF: Let M be a suborder of index p. We embed R into M_1 by $R \ni \alpha \mapsto \begin{pmatrix} \alpha & 0 \\ 0 & \alpha^\sigma \end{pmatrix} \in M_1$. Then $M \cap R$ is a subring of R, say T. Now $R/T = R/M \cap R \cong R + M/M \subseteq M_1/M$ as additive groups. Hence $|R/T| \leq p$ and so either $T = R = Z_p + Z_p v$ or $T = Z_p + Z_p pv$. If $T = R$, then M contains R and so by Proposition 2 of [12], M must be an order of level p^{2r+1} for some $r \geq 0$ (see Definition 1 of [12]). Thus the index of M in M_1 must be p^{2r}, a contradiction. Hence $T = Z_p + Z_p pv$.

Now suppose $\gamma' = \begin{pmatrix} a + bv & c + dv \\ p(c - dv) & a - bv \end{pmatrix} \in M$ with b a unit. Then

$\gamma = \begin{pmatrix} bv & c+dv \\ p(c-dv) & -bv \end{pmatrix} \in M$ and $\mathrm{tr}(\gamma) = 0$ while $N(\gamma) = -u(b^2 + p(c^2 - d^2u)/u) = -u\delta^2$ for some unit δ of Z_p. Hence $R \cong Z_p + Z_p\gamma \subseteq M$ and again we have a contradiction as above. Now let $D = \left\{\beta \in R \middle| \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix} \in M\right\}$. D is an additive subgroup of R and it followed from the above work that $M \cong T \oplus D$ as an additive group. But $M_1 \cong R \oplus R$ and $[M_1 : M] = [R : T][R : D] = p[R : D]$. Hence $R = D$ and we have

$$M = \left\{\begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix} \middle| \alpha \in T = Z_p + Z_p pv, \beta \in R\right\} \tag{1.3}$$

This completes the proof of Lemma 1.4.

THEOREM 1.5: *Let A be the quaternion division algebra over Q_p, p an odd prime. Then A contains a unique order of level p^2. In fact it is the unique order of index p in the maximal order of A.*

PROOF: Clearly an order of level p^2 has index p in the maximal order of A. Since the maximal order is unique, Lemma 1.4 shows that there is a unique order of level p^2 and it is given by (1.3) if A is given by (1.2). Existence of an order of level p^2 is clear from the definition or one can check directly that (1.3) gives an order of level p^2 by using Proposition 1.1.

REMARK 1.6: From now on we will use exclusively the representation of the unique quaternion division algebra over Q_p given by (1.2) and the corresponding representation of its unique order of level p^2 given by (1.3).

We will need to determine the structure of the unit group of the maximal order modulo the unit group of the order of level p^2. For any ring S, denote by $U(S)$ the unit group of S. Then we have the well known

LEMMA 1.7: *Let $R = Z_p + Z_p v$ and $T = Z_p + Z_p pv$. Then $U(R)/U(T)$ is cyclic of order $p+1$. A set of coset representatives is given by v and $1 + av$, $a = 0, 1, \ldots, p-1$.*

PROOF: Let $\bar{L}$(resp. $\overline{Q_p}$) be the residue class field of L(resp. Q_p). If φ_L and φ denote the maps to the residue class fields, we have the commutative diagram

$$\begin{array}{ccc} R & \xrightarrow{\varphi_L} & \bar{L} \\ \cup & & \cup \\ Z_p & \xrightarrow{\varphi} & \bar{Q}_p \end{array}$$

Then $\varphi_L^{-1}(\overline{Q_p}) = T$ so we have $U(R)/U(T) \cong \bar{L}^x/\bar{Q}_p^x$ which is a cyclic group of order $p+1$. It is clear that the given set is a set of coset representatives.

PROPOSITION 1.8: *Let A be the quaternion division algebra over Q_p, p an odd prime. Let M_1 be the maximal order of A and M_2 the order of level p^2. Then $U(M_1)/U(M_2)$ is cyclic of order $p+1$. A set of coset representatives is given by* $\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}$ *and* $\begin{pmatrix} 1+av & 0 \\ 0 & 1-av \end{pmatrix}$, $a = 0, 1, \ldots, p-1$.

PROOF: Let the notation be as in Lemma 1.7 above. Let $\psi: M_1 \to \bar{L}$ be given by $\psi\begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix} = \varphi_L(\alpha)$. Then $\psi^{-1}(\bar{Q}_p) = M_2$ and $U(M_1)/U(M_2) \cong \bar{L}^x/\bar{Q}_p^x$. It is easy to see that the given set is in fact a set of coset representatives.

2. Local optimal embedding theory

The major tool we will need in obtaining a trace formula for Brandt Matrices is the optimal embedding theory for orders of level p^2. Let ℓ be a prime. The analogous theory for orders of level ℓ^{2t+1} was developed by Pizer in [12]. The optimal embedding theory for orders in a split quaternion algebra over Q_ℓ was developed by Eichler ([2], [3]) and Hijikata ([5], §2). Let K be a semi-simple algebra of dimension 2 over Q_ℓ (i.e. K is a quadratic field extension of Q_ℓ or $K \cong Q_\ell \oplus Q_\ell$) and let o be an order of K (with $o \otimes_{Z_\ell} Q_\ell = K$). Let C be a quaternion algebra over Q_ℓ and let M be an order of C. Then we have the

DEFINITION 2.1: An embedding (injective Q_ℓ homomorphism) $\varphi: K \to C$ is called an *optimal embedding* of o/K into M/C if $\varphi(K) \cap M = \varphi(o)$. Two such optimal embeddings φ_1 and φ_2 are *equivalent* mod $U(M)$ if there exists $\gamma \in U(M)$ such that $\varphi_1(\alpha) = \gamma^{-1}\varphi_2(\alpha)\gamma$ for all $\alpha \in K$.

REMARK 2.2: In this section we study optimal embeddings in the case $\ell = p$, $C = A$ the unique quaterion division algebra over Q_p, and $M = M_2$.

Let us fix some notation which we will use for the remainder of the paper. p is always an odd prime. u is a quadratic non-residue mod p and $v = \sqrt{u}$. $L = Q_p(v)$, $R = Z_p + Z_p v$ and $T = Z_p + Z_p pv$. We identify A as in (1.2) and M_2 as in (1.3).

PROPOSITION 2.3: *Let $K = Q_p(g)$ be a semi-simple algebra of dimension 2 over Q_p where $Z_p + Z_p g$ is an order of K. Then an isomorphism φ is an optimal embedding of $Z_p + Z_p g/K$ into M_2/A if and only if $\varphi(g) = \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix}$ with $\alpha = a + pbv \in T$ and $\beta \in R$ where either b or β is a unit.*

PROOF: $Z_p + Z_p g$ is optimally embedded in M_2 if and only if $Z_p + Z_p \varphi(g) = M_2 \cap (Q_p + Q_p \varphi(g))$ and from this the proposition follows easily.

Let K, $\mathcal{o}$ be as in Definition 2.1. We denote by $\Delta(\mathcal{o})$ the discriminant of $\mathcal{o}$. $\Delta(\mathcal{o})$ is defined mod $U(Z_p)^2$ and we write $\Delta(\mathcal{o}) = d$ to mean $\Delta(\mathcal{o}) = dU(Z_p)^2$. If $K = Q_p(g)$ and $\mathcal{o} = Z_p + Z_p g$, then $\Delta(\mathcal{o}) = \mathrm{tr}(g)^2 - 4N(g)$.

PROPOSITION 2.4: *Let $\mathcal{o}$, K be as in Definition 2.1. Assume there exists an optimal embedding of $\mathcal{o}/K$ into M_2/A. Then $\Delta(\mathcal{o}) = p, pu,$ or p^2u.*

PROOF: Let φ be an optimal embedding of $\mathcal{o} = Z_p + Z_p g$ into M_2. Then by Proposition 2.3 $\varphi(g) = G = \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix}$ where $\alpha = a + pbv \in T$, $\beta \in R$ and either b or β is a unit. Thus $\Delta(\mathcal{o}) = \mathrm{tr}(G)^2 - 4N(G) = 4p(\beta\beta^\sigma + pb^2u)$ where either (i) β is a unit or (ii) $p \mid \beta$ and b is a unit. The first case gives discriminants p and pu, the second case gives p^2u.

PROPOSITION 2.5: *Let $\mathcal{o}$ be an order in a quadratic extension of Q_p with $\Delta(\mathcal{o}) = p^2u$. Then $\mathcal{o}$ has exactly two inequivalent* mod $U(M_2)$ *optimal embedding into M_2.*

PROOF: We can assume $\mathcal{o} = Z_p + Z_p pv$. Let φ be an optimal embedding of $\mathcal{o}$ into M_2 and set $\varphi(pv) = G$. Then G is conjugate by an element of A^x to $p\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}$. Now any element of A^x is in $U(M_1)$

$\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}^t$ for some t, so G is conjugate by an element of $U(M_1)$ to

$$p\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix} \text{ or to } p\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}\begin{pmatrix} 0 & 1/p \\ 1 & 0 \end{pmatrix} = -p\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}.$$

Hence G is conjugate by an element of $U(M_2)$ to some $\pm p\alpha\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}\alpha^{-1}$ where α runs over a set of coset representatives of $U(M_1)/U(M_2)$. By Proposition 1.8, a set of coset representatives is given by $\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}$ and $\begin{pmatrix} 1+av & 0 \\ 0 & 1-av \end{pmatrix}$, $a = 0, 1, \ldots, p-1$. But these are all in $Q_p\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}$, so they commute with $\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}$. Hence G is conjugate by an element of $U(M_2)$ to $\pm p\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}$. $p\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}$ and $-p\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}$ are never conjugate by $U(M_2)$ since if $\gamma \in U(M_2)$, then $\gamma\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}\gamma^{-1} = -\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}$ would imply (by reducing mod p) that $v \equiv -v \bmod p$, a contradiction. Finally both these representatives yield optimal embedding by Proposition 2.3. This completes the proof.

PROPOSITION 2.6: *Let $\mathfrak{o}$ be an order in a quadratic extension of Q_p with $\Delta(\mathfrak{o}) = p$ or pu. Then $\mathfrak{o}$ has exactly $p+1$ inequivalent* mod $U(M_2)$ *optimal embedding into M_2.*

PROOF: We can assume $\mathfrak{o} = Z_p + Z_p g$ where $g = \sqrt{p}$ or $\sqrt{up}$. Let φ be an optimal embedding of $\mathfrak{o}$ into M_2 and set $\varphi(g) = G$. Then G is conjugate by an element of A^x to $\begin{pmatrix} 0 & \beta \\ p\beta^\sigma & 0 \end{pmatrix} = H$ (say) where $\beta \in R$ and $\beta\beta^\sigma = 1$ (if $\Delta(\mathfrak{o}) = p$) or $\beta\beta^\sigma = u$ (if $\Delta(\mathfrak{o}) = pu$). Now $N(H) = -p\beta\beta^\sigma$ so H is a prime element of A. Hence any element of A^x is contained in $U(M_1)H^t$ for some $t \in Z$. Thus G is conjugate by an element of $U(M_1)$ to H. Thus by Proposition 1.8 G is conjugate by an element of $U(M_2)$ to some $\alpha H\alpha^{-1}$ where $\alpha = \begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}$ or $\begin{pmatrix} 1+av & 0 \\ 0 & 1-av \end{pmatrix}$ $a = 0, 1, \ldots, p$. That is G is conjugate by an element of $U(M_2)$ to one of

$$\begin{pmatrix} 0 & -\beta \\ -p\beta^\sigma & 0 \end{pmatrix} = C \text{ (say)}$$

or

$$\frac{1}{1-a^2u}\begin{pmatrix} 0 & \beta(1+av)^2 \\ p\beta^\sigma(1-av)^2 & 0 \end{pmatrix} = D_a \text{ (say)}, \quad a = 0, 1, \ldots, p-1.$$

Thus we have at most $p+1$ inequivalent mod $U(M_2)$ optimal embeddings and all these representatives yield optimal embeddings by Proposition 2.3. To show that we have exactly $p+1$, we must only show that no C or D_a $a = 0, 1, \ldots, p-1$ can be conjugate by an element of $U(M_2)$ to some other C or D_a. First suppose C is conjugate to some D_a by $\gamma = \begin{pmatrix} x & y \\ py^\sigma & x^\sigma \end{pmatrix} \in U(M_2)$. Thus working mod p, $\gamma C\gamma^{-1} = D_a$ implies $\begin{pmatrix} 0 & -x^2\beta \\ 0 & 0 \end{pmatrix}\frac{1}{xx^\sigma} \equiv \begin{pmatrix} 0 & -\beta \\ 0 & 0 \end{pmatrix} \equiv D_a \pmod p$. Thus $-\beta \equiv \beta\frac{(1+av)^2}{1-a^2u} \pmod p$ or $a^2u - 1 \equiv 1 + 2av + a^2u \pmod p$, a contradiction. Now suppose D_a is conjugate to D_b by $\gamma \in U(M_2)$. Again working mod p we see that this implies $\beta(1+av)^2/1-a^2u \equiv \beta(1+bv)^2/1-b^2u. \pmod p$. This leads to

$$(2.1) \qquad (1+a^2u)(1-b^2u) \equiv (1+b^2u)(1-a^2u) \pmod p$$

and

$$(2.2) \qquad 2a(1-b^2u) \equiv 2b(1-a^2u) \pmod p$$

(2.1) implies either $a \equiv b$ which gives $a = b$ and we are done or $a \equiv -b$ which by (2.2) implies $b \equiv 0 \pmod p$ which gives $a = b = 0$ and again we are done.

Combining Propositions 2.4, 2.5 and 2.6 we obtain

THEOREM 2.7: *Let $\mathfrak{o}$, K, A and M_2 be as in Definition* 2.1. *If $\Delta(\mathfrak{o}) = p$ or pu, there are exactly $p+1$ inequivalent* mod $U(M_2)$ *optimal embeddings of $\mathfrak{o}/K$ into M_2/A. If $\Delta(\mathfrak{o}) = p^2u$, there are exactly* 2 *inequivalent* mod $U(M_2)$ *optimal embedding of $\mathfrak{o}/K$ into M_2/A. If $\Delta(\mathfrak{o}) \neq p, pu$ or p^2u, $\mathfrak{o}/K$ has no optimal embedding into M_2/A.*

3. Orders of level p^2M and the Mass formula

We fix some notation which we will use throughout the remainder of the paper. p will always denote an *odd* prime. $\mathfrak{A}$ will always denote

the (unique) quaternion (division) algebra over Q ramified precisely at p and ∞. We let $\mathfrak{A}_\ell = \mathfrak{A} \otimes_Q Q_\ell$ for any prime ℓ of Q and also let $L_\ell = L \otimes_Z Z_\ell$ for any finite prime ℓ of Q and lattice L of $\mathfrak{A}$. If $\ell \neq p$ or ∞, then $\mathfrak{A}_\ell$ is split, i.e. $\mathfrak{A}_\ell \cong \mathrm{Mat}(2, Q_\ell)$ and all maximal orders of $\mathfrak{A}_\ell$ are conjugate by an element of $\mathfrak{A}_\ell^\times$ to $\mathrm{Mat}(2, Z_\ell)$ (see e.g. [16], Theorem 17.3). Thus for convenience we can and *do assume* from now on that $\mathfrak{A}_\ell$, $\ell \neq p$ or ∞ is identified with $\mathrm{Mat}(2, Q_\ell)$ in such a way that there exists a maximal order of $\mathfrak{A}$, say D, such that $D_\ell = \mathrm{Mat}(2, Z_\ell)$ for all $\ell \neq p$ or ∞. Let $u \in Z$ be a quadratic non residue mod p and let $v = \sqrt{u}$. Then $L = Q_p(v)$ is the unique unramified quadratic extension of Q_p and $R = Z_p + Z_p v$ is its ring of integers. Then $\mathfrak{A}_p$ can and will be identified with (see (1.2)) $\mathfrak{A}_p = \left\{ \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix} \middle| \alpha, \beta \in L \right\}$ where σ denotes conjugation of L/Q_p. Let M denote a positive integer prime to p.

DEFINITION 3.1: Let p, M, and $\mathfrak{A}$ be as above. An order $\mathcal{M}$ of $\mathfrak{A}$ is said to have level p^2M if (i) $\mathcal{M}_p$ is an order of level p^2 in $\mathfrak{A}_p$ and (ii) $\mathcal{M}_\ell$ is isomorphic (over Z_ℓ) to $\begin{pmatrix} Z_\ell & Z_\ell \\ MZ_\ell & Z_\ell \end{pmatrix}$ for all primes $\ell \neq p$.

Let $\mathfrak{A}$ be as above and let $\mathcal{M}$ be an order of level p^2M of $\mathfrak{A}$. Just as in Eichler [3], chapter 2 or Pizer [14], §2 $\mathcal{M}$ has an ideal theory. The ideal class number of left $\mathcal{M}$-ideals is finite (see Proposition 2.13 of [14]) and depends only on the level, not on the particular order $\mathcal{M}$ (see Proposition 2.13 of [14] and Theorem 4.18 below) and is denoted by $H = H(p^2M)$. Let $I_1, \ldots, I_H$ be representatives of all the distinct left $\mathcal{M}$-ideal classes and let $\mathcal{M}_i = \{x \in \mathfrak{A} \mid I_i x \subseteq I_i\}$ be the right order of I_i. The $\mathcal{M}_i$ are all orders of level p^2M (see e.g. [14], p. 103) and we have the following

DEFINITION 3.2: The Mass (p^2M) (for $\mathcal{M}$-ideals, $\mathcal{M}$ an order of level p^2M) is

$$\mathrm{Mass}(p^2M) = 2 \sum_{i=1}^{H} 1/|U(\mathcal{M}_i)|$$

REMARK 3.3: The Mass depends only on the level, not on the particular order of level p^2M or on the choice of ideal class representatives (see Theorem 3.4 below). The 2 in the definition comes from that fact that we really should consider $|U(\mathcal{M}_i)/U(Z)|$, at least if we want our definition to extend naturally to quaternion algebras over totally real number fields.

THEOREM 3.4: $\text{Mass}(p^2M) = \dfrac{(p^2-1)M}{12} \prod_{\ell \mid M} (1+1/\ell)$

the product being over all primes ℓ of M.

PROOF: This follows immediately by the same techniques as in Pizer [12], Propositions 24 and 25 once we take into account Proposition 1.8 of this paper.

For convenience of exposition we give the following normalization.

DEFINITION 3.5: Let p be an odd prime and M a positive integer prime to p. We denote by $\mathcal{O}$ the order of level p^2M of $\mathfrak{A}$ given by

(i) $\mathcal{O}_\ell = \begin{pmatrix} Z_\ell & Z_\ell \\ MZ_\ell & Z_\ell \end{pmatrix}$ for all $\ell < \infty$, $\ell \neq p$

(ii) $\mathcal{O}_p = \left\{ \begin{pmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{pmatrix} \middle| \alpha \in T = Z_p + Z_p pv,\ \beta \in R = Z_p + Z_p v \right\}$.

REMARK 3.6: It is clear that $\mathcal{O}$ is an order of level p^2M. In general an order $\mathcal{M}$ of $\mathfrak{A}$ has level p^2M if and only if $\mathcal{M}_\ell \cong \mathcal{O}_\ell$ (over Z_ℓ) for all $\ell < \infty$. For the remainder of the paper $\mathcal{M}$ will denote some order of level p^2M of $\mathfrak{A}$ while $\mathcal{O}$ will always denote the order given by Definition 3.5. Note that by adjusting the identification of $\mathfrak{A}_\ell$ with $\text{Mat}(2, Q_\ell)$, $\ell \neq p$, any preselected order of level p^2M can be taken as $\mathcal{O}$.

4. The Brandt Matrices and their traces

Let p, M, $\mathcal{O}$, and $\mathfrak{A}$ as in §3. Using $\mathcal{O}$, we define Brandt Matrices $B(n) = B_s(n; p^2, M)$ in exactly the same way as Eichler (see [3], equation 15 and 15a on p. 105 or Pizer [15], Definition 2.13). For the convenience of the reader we briefly recall the definition.

Let $\alpha \mapsto X_s(\alpha)$ denote the $s+1$ dimensional matrix representation of $\mathfrak{A}^x$ induced by taking the sth symmetric product of the two dimensional representation $\mathfrak{A}^x \subseteq (\mathfrak{A} \otimes \mathbf{C})^x = GL(2, \mathbf{C})$. $X_0(\alpha)$ denotes the trivial one dimensional representation, i.e. $X_0(\alpha) = 1$ for all $\alpha \in \mathfrak{A}^x$. Let $I_1, \ldots, I_H$ be a set of representatives of all the left $\mathcal{O}$-ideal classes. Let $\mathcal{O}_j = \{\alpha \in \mathfrak{A}^x \mid I_j\alpha \subseteq I_j\}$ denote the right order of I_j and let $e_j = |U(\mathcal{O}_j)|$. By Proposition 5.12 below $e_j = 2$ or 6 and is often 2 (always if $p > 3$). For $n > 0$, let

$$b_{ij}^s(n) = e_j^{-1} \sum_{\alpha} X_s^t(\alpha) \tag{4.1}$$

where the sum is over all $\alpha \in I_j^{-1}I_i$ with $N(\alpha) = nN(I_i)/N(I_j)$. Here the superscript t denotes transpose. Further let $b_{ij}^0(0) = 1/e_j$ and let $b_{ij}^s(0) = 0$, $s > 0$. Then the $b_{ij}^s(n)$ are $s+1$ by $s+1$ complex matrices and the Brandt Matrix $B_s(n; p^2, M)$ is the $H(s+1)$ by $H(s+1)$ matrix given by

$$B_s(n; p^2, M) = (b_{ij}^s(n)) \tag{4.2}$$

that is the ith, jth block, $1 \leq i, j \leq H$ of $B_s(n; p^2, M)$ is the $s+1$ by $s+1$ matrix $b_{ij}^s(n)$.

REMARK 4.1: If s is odd, then $X_s^t(-\alpha) = -X_s^t(\alpha)$ and it follows from (4.1) that the Brandt Matrices $B_s(n; p^2, M)$ for s odd are identically zero.

Note that the Brandt Matrices depend (slightly) on the choice of ideal class representatives $I_1, \ldots, I_H$ and also on the choice of the order $\mathcal{O}$. We now show how this dependence works. Let $J_1, \ldots, J_H$ be another set of representatives of all the distinct left $\mathcal{O}$ ideal classes. Then $J_i = I_{\epsilon(i)}a_i$ for some $a_i \in \mathfrak{A}^x$ and some permutation ϵ of the indices $1, \ldots, H$. Let $B_s^I(n)$ (resp. $B_s^J(n)$) be the Brandt Matrix corresponding to the choice of $I_1, \ldots, I_H$ (resp. $J_1, \ldots, J_H$) as ideal class representatives. Finally let P be the $H(s+1)$ by $H(s+1)$ matrix consisting of blocks ρ_{ij} of $s+1$ by $s+1$ matrices where the ith, jth block $\rho_{ij} = \begin{cases} X_s^t(a_i) & \text{if } j = \epsilon(i) \\ 0 & \text{otherwise} \end{cases}$. Then we have

PROPOSITION 4.2: *In the above notation* $B_s^J(n) = PB_s^I(n)P^{-1}$ *for all* n.

PROOF: This follows easily from (4.1) and (4.2).

Let $J_{\mathfrak{A}}$ be the idele group of $\mathfrak{A}$. $J_{\mathfrak{A}}$ acts transitively by conjugation on orders of level p^2M of $\mathfrak{A}$, the action being $\tilde{\alpha} : \mathcal{M} \mapsto \tilde{\alpha}^{-1}\mathcal{M}\tilde{\alpha}$. If $\mathcal{M}$ is any fixed order of level p^2M, then $J_{\mathfrak{A}}$ acts transitively on left $\mathcal{M}$-ideals, the action being $\tilde{\alpha} : I \mapsto I\tilde{\alpha}$. For details see section 2 of [14].

PROPOSITION 4.3: *The Brandt Matrices do not depend on the particular order* $\mathcal{O}$ *of level* p^2M *which is used to define them.*

PROOF: Let $\mathcal{O}$ and $I_1, \ldots, I_H$ be as above. Let $\mathcal{M}$ be some other

order of level p^2M. Then $\mathcal{M} = \tilde{\alpha}\mathcal{O}\tilde{\alpha}^{-1}$ for some $\tilde{\alpha} \in J_{\mathbb{A}}$ and it is clear that $\tilde{\alpha}I_1, \ldots, \tilde{\alpha}I_H$ is a complete set of representatives for the distinct left $\mathcal{M}$-ideal classes. By (4.1), the ith, jth entry block of the Brandt Matrix associated to $\mathcal{O}$ (resp. $\mathcal{M}$) is obtained by summing over all $\alpha \in I_j^{-1}I_i$ (resp. $(\tilde{\alpha}I_j)^{-1}(\tilde{\alpha}I_i)$). But $(\tilde{\alpha}I_j)^{-1}(\tilde{\alpha}I_i) = I_j^{-1}I_i$, so the Brandt Matrices for $\mathcal{O}$ and $\mathcal{M}$ are identical (if we choose corresponding sets of ideal class representatives).

REMARK 4.4: It follows from Proposition 4.2 and 4.3 above that the Brandt Matrices depend upto conjugation by a fixed matrix only on the level p^2M. In particular, if $s = 0$ they are independent upto conjugation by a permutation matrix of the particular order of level p^2M and the particular choice of ideal class representatives used to define them.

The Brandt Matrices $B_s(n; p^2, M)$ with $(n, pM) = 1$ generate a commutative semi-simple ring (see [3] or [15]) and for $(n, pM) = 1$, $B_s(n; p^2, M)$ gives a matrix representation of the Hecke operator $T_{s+2}(n)$ acting on a space of generalized theta series (see Proposition 2.23 of [15] and the Proposition on p. 138 of [3]. Our major result on the representation of cusp forms on $\Gamma_0(p^2M)$ by theta series (see §8) will follow from a relation involving the traces of Brandt Matrices. For this we need the formula for the trace of Brandt Matrices given in this section.

Eichler first obtained a trace formula for Brandt Matrices attached to orders of square free level in [2]. Since then it has been implicit in the literature that given the optimal embedding theory and the mass formula for a particular kind of order, one can then obtain the trace formula for Brandt Matrices attached to that kind of order by methods similar to Eichler's. We think it is worthwhile to make this principle explicit. The proof of the trace formula given below is valid for any order (with finite class number) in a definite quaternion algebra over Q (in fact over any totally real number field with obvious modifications) and does not require any knowledge of the two-sided ideal theory of the order. For simplicity we will treat the case of the order $\mathcal{O}$ of level p^2M (which is what we really need), but we make no essential use of the fact that $\mathcal{O}$ has level p^2M (see Remark 4.15).

DEFINITION 4.5: Let A be a quaternion algebra over Q and let D be an order of A. Let K be a semi-simple algebra of dimension 2 over Q and let $\mathfrak{o}$ be an order of K. An isomorphism $\varphi : K \to A$ is said to be an *optimal embedding* of $\mathfrak{o}/K$ into D/A if $\varphi(\mathfrak{o}) = D \cap \varphi(K)$. Two such optimal embeddings φ_1 and φ_2 of $\mathfrak{o}/K$ into D/A are said to be

equivalent mod $U(D)$ if and only if there exists a $u \in U(D)$ such that $\varphi_1(x) = u^{-1}\varphi_2(x)u$ for all $x \in K$.

REMARK 4.6: Note that this is just a global version of Definition 2.1. Note in particular that now K denotes a global algebra and $\mathcal{o}$ a global order.

REMARK 4.7: Let A be a quaternion division algebra over Q. Then by the Brauer–Hasse–Noether Theorem on splitting fields of central simple algebras over global fields, we know that there exists an isomorphism φ of K into A if and only if K is a quadratic field such that no ramified prime of A splits in K. In particular if $\mathfrak{A}$ is the quaternion algebra over Q ramified precisely at p and ∞, there exists an isomorphism $\varphi: K \to \mathfrak{A}$ if and only if K is an imaginary quadratic field such that p does not split in K, i.e. such that $K_p = K \otimes_Q Q_p$ is a field.

We need to set some notation. Let K be an imaginary quadratic number field and $\mathcal{o}$ an order of K. Let $\mathfrak{A}$ be the quaternion algebra over Q ramified precisely at p and ∞ and D an order of level p^2M of $\mathfrak{A}$. Denote by $A(\mathcal{o}, D)$ the number of mod $U(D)$ equivalence classes of optimal embedding of $\mathcal{o}/K$ into $D/\mathfrak{A}$. Note that $A(\mathcal{o}, D)$ depends only on the isomorphism classes of $\mathcal{o}$ and D. For a prime ℓ, denote by $C_\ell(\mathcal{o})$ the number of mod $U(D_\ell)$ equivalence classes of optimal embedding of $\mathcal{o}_\ell/K_\ell$ into $D_\ell/\mathfrak{A}_\ell$ (see Definition 2.1). Note that $C_\ell(\mathcal{o})$ depends only on $\mathcal{o}$ and the level of D_ℓ since all local orders of the same level are isomorphic by definition.

Let $\mathcal{O}$ be an order of level p^2M of $\mathfrak{A}$. Let $I_1, \ldots, I_H$ be a set of representatives of all the left $\mathcal{O}$-ideal classes and let $\mathcal{O}_j$ be the right order of I_j. The key result connecting the local optimal embedding theory to the trace of the Brandt Matrices is

THEOREM 4.8: *In the above notation we have*

$$\sum_{i=1}^{H} A(\mathcal{o}, \mathcal{O}_i) = h(\mathcal{o}) \prod_{\ell \mid pM} C_\ell(\mathcal{o})$$

where $h(\mathcal{o})$ is the class number of locally principal $\mathcal{o}$-ideals and the product is over all primes ℓ dividing pM.

PROOF: Note that by the tables on p. 692–694 of [13] $C_\ell(\mathcal{o}) = 1$ if $\ell \nmid pM$. Thus we will prove the more aesthetically pleasing result

$$\sum_{i=1}^{H} A(\mathfrak{o}, \mathcal{O}_i) = h(\mathfrak{o}) \prod_{\ell<\infty} C_\ell(\mathfrak{o}) \tag{4.3}$$

If K can not be embedded in $\mathfrak{A}$, clearly (by Remark 4.7) both sides of (4.3) are zero, so for convenience we assume $K \subseteq \mathfrak{A}$, hence $K_\ell \subseteq \mathfrak{A}_\ell \forall \ell$ and $J_K \subseteq J_{\mathfrak{A}}$, where J_K denotes the idele group of K.

If φ is an optimal embedding of $\mathfrak{o}_\ell/K_\ell$ into $\mathcal{O}_\ell/\mathfrak{A}_\ell$, then $\varphi(x) = bxb^{-1}$ for some $b \in \mathfrak{A}_\ell^\times$ with $b\mathfrak{o}_\ell b^{-1} = \mathcal{O}_\ell \cap bK_\ell b^{-1}$. Clearly conjugating by b or b' gives the same optimal embedding if and only if $b' \in bK_\ell^\times$. Also conjugating by b or b' yield mod $U(\mathcal{O}_\ell)$ equivalent optimal embeddings if and only if $b' \in U(\mathcal{O}_\ell)bK_\ell^\times$. Thus $C_\ell(\mathfrak{o})$ is equal to the number of double cosets $U(\mathcal{O}_\ell)bK_\ell^\times$ in $\mathfrak{A}_\ell^\times$ such that $K_\ell \cap b^{-1}\mathcal{O}_\ell b = \mathfrak{o}_\ell$. We need the little

LEMMA 4.9: *Let $\mathfrak{o}$, K, $\mathcal{O}$ and $\mathfrak{A}$ be as in Theorem* 4.8. *Then $K \cap \mathcal{O} = \mathfrak{o}$ if and only if $K_\ell \cap \mathcal{O}_\ell = \mathfrak{o}_\ell$ $\forall \ell < \infty$.*

PROOF: By the elementary divisor theorem we can choose a Z-basis f_1, f_2, f_3, f_4 of $\mathcal{O}$ such that f_1, f_2 is a Z-basis for $K \cap \mathcal{O}$. From this it follows that $(K \cap \mathcal{O})_\ell = K_\ell \cap \mathcal{O}_\ell$ and now the lemma is clear.

We continue with the proof of Theorem 4.8. From the above we see that $\Pi_{\ell<\infty} C_\ell(\mathfrak{o})$ is equal to the number of double cosets $\mathcal{U}(\mathcal{O})\tilde{b}J_K$ in $J_{\mathfrak{A}}$ such that $\tilde{b} = (b_\ell)$ and $K_\ell \cap b_\ell^{-1}\mathcal{O}_\ell b_\ell = \mathfrak{o}_\ell$ $\forall \ell$. Here $\mathcal{U}(\mathcal{O}) = \{\tilde{u} = (u_\ell) \in J_{\mathfrak{A}} \mid u_\ell \in U(\mathcal{O}_\ell) \forall \ell < \infty\}$. Hence by Lemma 4.9

$$\prod_{\ell<\infty} C_\ell(\mathfrak{o}) \text{ is equal to the number of double cosets}$$

$$\mathcal{U}(\mathcal{O})\tilde{b}J_K \text{ in } J_{\mathfrak{A}} \text{ with } K \cap \tilde{b}^{-1}\mathcal{O}\tilde{b} = \mathfrak{o} \tag{4.4}$$

Now let

$$J_K = \bigcup_{i=1}^{h} \mathcal{U}(\mathfrak{o})\tilde{a}_i K^\times \quad \text{(disjoint)} \tag{4.5}$$

where $h = h(\mathfrak{o})$ is (by definition) the ideal class number of locally principal $\mathfrak{o}$-ideals. Here $\mathcal{U}(\mathfrak{o}) = \{\tilde{u} = (u_\ell) \in J_K \mid u_\ell \in U(\mathfrak{o}_\ell) \forall \ell < \infty\}$. Consider a double coset $\mathcal{U}(\mathcal{O})\tilde{b}J_K$ with $K \cap \tilde{b}^{-1}\mathcal{O}\tilde{b} = \mathfrak{o}$. $\mathcal{U}(\mathcal{O})\tilde{b}J_K = \bigcup_{i=1}^{h} \mathcal{U}(\mathcal{O})\tilde{b}\mathcal{U}(\mathfrak{o})\tilde{a}_i K^\times = \bigcup_{i=1}^{h} \mathcal{U}(\mathcal{O})\tilde{b}\tilde{a}_i K^\times$ since $\mathfrak{o} \subseteq \tilde{b}^{-1}\mathcal{O}\tilde{b}$ implies $\tilde{b}\mathcal{U}(\mathfrak{o}) \subseteq \mathcal{U}(\mathcal{O})\tilde{b}$. We claim that this gives $h(\mathfrak{o})\Pi_{\ell<\infty} C_\ell(\mathfrak{o})$ distinct double cosets $\mathcal{U}(\mathcal{O})\tilde{c}K^\times$ such that $K \cap \tilde{c}^{-1}\mathcal{O}\tilde{c} = \mathfrak{o}$. Clearly we have at most this many. As above any two such double cosets must be of the form $\mathcal{U}(\mathcal{O})\tilde{b}\tilde{a}_i K^\times$ for some $\tilde{b}$ in (4.4) and $\tilde{a}_i$ in (4.5). If $\mathcal{U}(\mathcal{O})\tilde{b}\tilde{a}_i K^\times =$

$\mathcal{U}(\mathcal{O})\tilde{b}'\tilde{a}_jK^x$, then $\mathcal{U}(\mathcal{O})\tilde{b}J_K = \mathcal{U}(\mathcal{O})\tilde{b}'J_K$ hence $\tilde{b} = \tilde{b}'$. Thus $\tilde{b}^{-1}\mathcal{U}(\mathcal{O})\tilde{b}\tilde{a}_jK^x = \tilde{b}^{-1}\mathcal{U}(\mathcal{O})\tilde{b}\tilde{a}_iK^x$ or $\tilde{a}_j = w\tilde{a}_ik$ with $w \in \tilde{b}^{-1}\mathcal{U}(\mathcal{O})\tilde{b} = \mathcal{U}(\tilde{b}^{-1}\mathcal{O}\tilde{b})$ and $k \in K$. Thus $w \in J_K \cap \mathcal{U}(\tilde{b}^{-1}\mathcal{O}\tilde{b}) = \mathcal{U}(\mathfrak{o})$ (since $\tilde{b}^{-1}\mathcal{O}\tilde{b} \cap K = \mathfrak{o}$), so $\tilde{a}_j = w\tilde{a}_ik$ implies $j = i$.

We now give a bijective map from the $h(\mathfrak{o})\prod_{\ell<\infty} c_\ell(\mathfrak{o})$ double cosets $\mathcal{U}(\mathcal{O})\tilde{c}K^x$ with $K \cap \tilde{c}^{-1}\mathcal{O}\tilde{c} = \mathfrak{o}$ onto the mod $U(\mathcal{O}_i)$ equivalence classes of optimal embeddings φ of $\mathfrak{o}/K$ into $\mathcal{O}_i/\mathfrak{A}$ as i ranges over $1, 2, \ldots, H$. Let

$$J_{\mathfrak{A}} = \bigcup_{i=1}^{H} \mathcal{U}(\mathcal{O})\tilde{\gamma}_i\mathfrak{A}^x \quad \text{(disjoint)} \tag{4.6}$$

be the decomposition of $J_{\mathfrak{A}}$ given by the ideals $I_1, \ldots, I_H$, i.e. we let $I_i = \mathcal{O}\tilde{\gamma}_i$. Note that $\mathcal{O}_i = \tilde{\gamma}_i^{-1}\mathcal{O}\tilde{\gamma}_i$. Let $K \cap \tilde{c}^{-1}\mathcal{O}\tilde{c} = \mathfrak{o}$ and consider the map

$$\mathcal{U}(\mathcal{O})\tilde{c}K^x \mapsto (\tilde{\gamma}_i, U(\mathcal{O}_i)aK^x) \tag{4.7}$$

where $\tilde{c} = \tilde{u}\tilde{\gamma}_i a$, $\tilde{u} \in \mathcal{U}(\mathcal{O})$, $a \in \mathfrak{A}^x$ in (4.6). We claim (4.7) is well defined. $\mathcal{U}(\mathcal{O})\tilde{c}K^x \subseteq \mathcal{U}(\mathcal{O})\tilde{\gamma}_i\mathfrak{A}^x$, so clearly $\tilde{\gamma}_i$ is uniquely determined by $\mathcal{U}(\mathcal{O})\tilde{c}K^x$. Suppose $\tilde{c} = \tilde{u}\tilde{\gamma}_i a$ and $\tilde{\omega}\tilde{c}k = \tilde{u}'\tilde{\gamma}_i a'$ with $\tilde{u}, \tilde{u}', \tilde{\omega} \in \mathcal{U}(\mathcal{O})$; $a, a' \in \mathfrak{A}^x$; and $k \in K^x$. Then $a'k^{-1}a^{-1} = \tilde{\gamma}_i^{-1}\tilde{u}'^{-1}\tilde{\omega}\tilde{u}\tilde{\gamma}_i \in \mathcal{U}(\mathcal{O}_i) \cap \mathfrak{A}^x = U(\mathcal{O}_i)$, hence $a' \in U(\mathcal{O}_i)aK^x$ and so (4.7) is well defined.

Now $K \cap \tilde{c}^{-1}\mathcal{O}\tilde{c} = \mathfrak{o}$ implies that $K \cap a^{-1}\mathcal{O}_i a = \mathfrak{o}$, so $\varphi(x) = axa^{-1}$ gives an optimal embedding of $\mathfrak{o}/K$ into $\mathcal{O}_i/\mathfrak{A}$ and clearly φ is well defined upto equivalence mod $U(\mathcal{O}_i)$ by the double coset $U(\mathcal{O}_i)aK^x$. To complete the proof we need only show that the map (4.7) is a bijection onto the set of double cosets $U(\mathcal{O}_i)aK^x$ with $K \cap a^{-1}\mathcal{O}_i a = \mathfrak{o}$, $i = 1, \ldots, H$.

onto: $K \cap a^{-1}\mathcal{O}_i a = \mathfrak{o}$ implies $K \cap a^{-1}\tilde{\gamma}_i^{-1}\mathcal{O}\tilde{\gamma}_i a = \mathfrak{o}$ so this comes from $\mathcal{U}(\mathcal{O})\tilde{\gamma}_i aK^x$ by (4.7).

one to one: Let $\mathcal{U}(\mathcal{O})\tilde{c}K^x$ and $\mathcal{U}(\mathcal{O})\tilde{d}K^x$ have the same image under (4.7). Let $\tilde{c} = \tilde{u}\tilde{\gamma}_i a$ and $\tilde{d} = \tilde{\omega}\tilde{\gamma}_j b$ with $a, b \in \mathfrak{A}^x$, $\tilde{u}, \tilde{\omega} \in \mathcal{U}(\mathcal{O})$. Then clearly $i = j$ and $U(\mathcal{O}_i)aK^x = U(\mathcal{O}_i)bK^x$. Thus for some $u \in U(\mathcal{O}_i)$, $ub \in aK^x$ and $\mathcal{U}(\mathcal{O})\tilde{c}K^x = \mathcal{U}(\mathcal{O})\tilde{\gamma}_i aK^x = \mathcal{U}(\mathcal{O})\tilde{\gamma}_i ubK^x = \mathcal{U}(\mathcal{O})\tilde{\gamma}_i bK^x = \mathcal{U}(\mathcal{O})\tilde{d}K^x$ since $u \in U(\mathcal{O}_i) = \tilde{\gamma}_i^{-1}U(\mathcal{O})\tilde{\gamma}_i$ implies $\tilde{\gamma}_i u \in U(\mathcal{O})\tilde{\gamma}_i$. This completes the proof of Theorem 4.8.

The following Corollary should be compared with Proposition 5 on p. 102 of Eichler [3].

COROLLARY 4.10: *Let the notation be as in Theorem* 4.8. *Let* $a_i(\mathfrak{o})$ *denote the number of optimal embeddings of* $\mathfrak{o}/K$ *into* $\mathcal{O}_i/\mathfrak{A}$. *Then*

$$\sum_{i=1}^{H} \frac{a_i(\mathcal{O})}{e_i} = \frac{h(\mathcal{O})}{|U(\mathcal{O})|} \prod_{\ell | pM} c_\ell(\mathcal{O})$$

where $e_i = |U(\mathcal{O}_i)|$.

PROOF: Let $\varphi(x) = axa^{-1}$ be an optimal embedding of $\mathcal{O}/K$ into $\mathcal{O}_i/\mathfrak{A}$. Then for each $u \in U(\mathcal{O}_i)$, $\varphi_u(x) = uaxa^{-1}u^{-1}$ gives an optimal embedding of $\mathcal{O}/K$ into $\mathcal{O}_i/\mathfrak{A}$ which is mod $U(\mathcal{O}_i)$ equivalent to φ. Further $\varphi_u(x) = \varphi_w(x)$ if and only if $w^{-1}u \in \varphi(K) \cap U(\mathcal{O}_i) = \varphi(U(\mathcal{O}))$. Thus $a_i(\mathcal{O}) = A(\mathcal{O}, \mathcal{O}_i)e_i/|U(\mathcal{O})|$ and the Corollary follows directly from the theorem.

We need one last

LEMMA 4.11: *Let* $\alpha \in \mathfrak{A}^x$ *with* $\mathrm{tr}(\alpha) = s$, $N(\alpha) = n$ *and let* $x^2 - sx + n = (x - \zeta)(x - \bar{\zeta}) \in \mathbb{C}[x]$. *Then if* $\alpha \notin Q^x$, $\mathrm{tr}(X_s(\alpha)) = \dfrac{\zeta^{s+1} - \bar{\zeta}^{s+1}}{\zeta - \bar{\zeta}}$ *while if* $\alpha \in Q^x$, $\mathrm{tr}(X_s(\alpha)) = (s+1)\alpha^s$.

PROOF: If $\alpha \notin Q^x$, α as an element of $\mathfrak{A} \otimes \mathbb{C}$ is conjugate to $\begin{pmatrix} \zeta & 0 \\ 0 & \bar{\zeta} \end{pmatrix}$ and $\mathrm{tr}\left(X_s\begin{pmatrix} \zeta & 0 \\ 0 & \bar{\zeta} \end{pmatrix}\right) = \sum_{t=0}^{s} \zeta^t \bar{\zeta}^{s-t} = \dfrac{\zeta^{s+1} - \bar{\zeta}^{s+1}}{\zeta - \bar{\zeta}}$. If $\alpha \in Q^x$, the result is obvious.

THEOREM 4.12: *Let* k *be an even integer* ≥ 2. *The trace of the Brandt Matrix* $B_{k-2}(n; p^2, M)$ *is given by*

$$\mathrm{tr}\, B_{k-2}(n; p^2, M) = \sum_s a_k(s) \sum_f b(s, f) \prod_{\ell | pM} c(s, f, \ell)$$
$$+ \zeta(\sqrt{n}) \frac{k-1}{12} (p^2 - 1) M \prod_{\ell | M} (1 + 1/\ell)$$

where $\zeta(\sqrt{n}) = \begin{cases} n^{k-2/2} & \text{if } n \text{ is a perfect square} \\ 0 & \text{otherwise} \end{cases}$

The meaning of s, $a_k(s)$, f, $b(s, f)$, and $c(s, f, \ell)$ are given as follows.

Let s run over all integers such that $s^2 - 4n$ is negative. Hence with some positive integer t and square free negative integer m we can classify $s^2 - 4n$ into cases by

$$s^2-4n=\begin{cases}t^2m & m\equiv 1 \pmod 4\\ t^2 4m & m\equiv 2,3 \pmod 4\end{cases}$$

Let $\Phi_s(X)=X^2-sX+n$ and let x and y be the roots of $\Phi_s(X)=0$ in $\mathbb{C}$. Put $a_k(s)=1/2(x^{k-1}-y^{k-1})(x-y)^{-1}$.

For each s (fixed), let f run over all positive divisions of t.

Let K denote the quotient field $Q[X]/(\Phi_s(X))$ and ξ the canonical image of X in K. K is an imaginary quadratic number field and ξ generates the order $Z+Z\xi$ of K. For each f there is a uniquely determined order $\mathfrak{o}_f$ containing $Z+Z\xi$ as a submodule of index f. $\Delta(\mathfrak{o}_f)=s^2-4n/f^2=\Delta(f)$ (say). Let $h(\Delta(f))$ (resp. $\omega(\Delta(f))$) denote the class number of locally principal $\mathfrak{o}_f$-ideals (resp. $1/2|U(\mathfrak{o}_f)|$). Then $b(s,f)=h(\Delta(f))/\omega(\Delta(f))$.

Finally let $\mathfrak{O}$ be an order of level p^2M of $\mathfrak{A}$. Then $c(s,f,\ell)$ is the number of inequivalent mod $U(\mathfrak{O}\otimes Z_\ell)$ optimal embeddings of $\mathfrak{o}_f\otimes Z_\ell$ into $\mathfrak{O}\otimes Z_\ell$.

REMARK 4.13: The trace formula given in Theorem 4.12 is very easy to evaluate. It is well known how to write $h(\Delta(f))$ in terms of 'standard' class numbers of maximal orders (see Corollary 4.17 below). Also it is well known and trivial that $\omega(\Delta(f))=1$ with two exceptions ($\omega(-4)=2$ and $\omega(-3)=3$). $c(s,f,p)$ is given by Theorem 2.7 above and the $c(s,f,\ell)$, $\ell\neq p$ were computed by Hijikata in [5] and are given explicitly by Pizer in [13], p. 692–694. Note that in [13] $c(s,f,\ell)$, $\ell\neq p$ is denoted by $c'(s,f,\ell)$ to distinguish the split case from the ramified case.

REMARK 4.14: The great similarity between the formula for the trace of the Brandt Matrix $B_{k-2}(n,p^2,M)$ and the formula for the trace of the Hecke Operator $T(n)$ actings on cusp forms of weight k on $\Gamma_0(N)$, $N=p^2M$ (see Hijikata [5], p. 57) should be noted. This similarity will be exploited in §7.

REMARK 4.15: To any order D (with finite class number) in a definite quaternion algebra over Q one can associate Brandt matrices. The trace of these Brandt matrices will be given by the formula of Theorem 4.12 with the following changes: (i) The product $\Pi_{\ell|pM}$ will be replaced by $\Pi_{\ell|S}$ where S is the product of all the finite primes ℓ of Q such that D_ℓ is not isomorphic with $\mathrm{Mat}(2,Z_\ell)$; (ii) $c(s,f,\ell)$ denotes the number of inequivalent mod $U(D_\ell)$ optimal embeddings of $\mathfrak{o}_f\otimes Z_\ell$ into D_ℓ; and (iii) $\dfrac{(p^2-1)M}{12}\prod_{\ell|M}(1+1/\ell)$ is replaced by the Mass of D.

PROOF OF THEOREM 4.12: Let $a_i(s, n)$ denote the number of $\alpha \in \mathcal{O}_i$ with $\mathrm{tr}(\alpha) = s$ and $N(\alpha) = n$ and with $X^2 - sX + n$ irreducible over Q. Using the notation of (4.1), it follows from the fact that $I_i^{-1} I_i = \mathcal{O}_i$ using (4.1), (4.2) and Lemma 4.11 that

$$\mathrm{tr}B_{k-2}(n; p^2, M) = \sum_s \sum_{i=1}^{H} \frac{a_i(s, n)}{e_i} \frac{x^{k-1} - y^{k-1}}{x - y} + \zeta(\sqrt{n}) \frac{k-1}{12} (p^2 - 1) M \prod_{\ell | M} (1 + 1/\ell)$$

where $\zeta(\sqrt{n}) = \begin{cases} n^{k-2/2} & \text{if } n \text{ is a perfect square} \\ 0 & \text{otherwise} \end{cases}$

The first sum is over all integers s. However, clearly $a_i(s, n) = 0$ if $s^2 - 4n \geq 0$. The second term occurs only if n is a perfect square since then $\alpha = \pm\sqrt{n} \in \mathcal{O}_i$ for all i and these give a contribution of

$$2(k-1) n^{k-2/2} \left(\sum_{i=1}^{H} 1/e_i \right) = n^{k-2/2} \frac{k-1}{12} (p^2 - 1) M \prod_{\ell | M} (1 + 1/\ell)$$

by Theorem 3.4 and Lemma 4.11. Let $K = Q[X]/(X^2 - sX + n)$ and let x be a root of $X^2 - sX + n$ in K. Then $a_i(s, n)$ is equal to the number of isomorphisms φ of K into $\mathfrak{A}$ with $\varphi(x) \in \mathcal{O}_i$. Let $\mathfrak{o}_0 = Z + Zx$ and let $\mathfrak{o}$ be an order of K with $\mathfrak{o}_0 \subseteq \mathfrak{o} \subseteq K$. If φ is an optimal embedding of $\mathfrak{o}/K$ into $\mathcal{O}_i/\mathfrak{A}$, then $\varphi(\mathfrak{o}) = \mathcal{O}_i \cap \varphi(K)$ and $x \in \mathfrak{o}_0 \subseteq \mathfrak{o}$ implies $\varphi(x) \in \mathcal{O}_i$. Thus every optimal embedding of some order $\mathfrak{o}$, $\mathfrak{o}_0 \subseteq \mathfrak{o} \subseteq K$ into $\mathcal{O}_i/\mathfrak{A}$ is an isomorphism that is counted in $a_i(s, n)$. Conversely, if $\varphi : K \to \mathfrak{A}$ is an isomorphism with $\varphi(x) \in \mathcal{O}_i$, then $\mathcal{O}_i \cap \varphi(K) = \mathfrak{o}'$ is an order of $\varphi(K)$ containing $\varphi(x)$. Hence $\varphi^{-1}(\mathfrak{o}')$ is an order of K which contains $\mathfrak{o}_0$ and such that φ gives an optimal embedding of $\varphi^{-1}(\mathfrak{o}')$ into $\mathcal{O}_i$. Thus $a_i(s, n) = \Sigma_{\mathfrak{o} \supseteq \mathfrak{o}_0} a_i(\mathfrak{o})$, the sum being over all orders $\mathfrak{o}$ of K which contain $\mathfrak{o}_0$ and $a_i(\mathfrak{o})$ is as in Corollary 4.10. So we have

$$\sum_{i=1}^{H} \frac{a_i(s, n)}{e_i} = \sum_{\mathfrak{o} \supseteq \mathfrak{o}_0} \sum_{i=1}^{H} \frac{a_i(\mathfrak{o})}{e_i} = \sum_{\mathfrak{o} \supseteq \mathfrak{o}_0} \frac{h(\mathfrak{o})}{|U(\mathfrak{o})|} \prod_{\ell | pM} c_\ell(\mathfrak{o})$$

by Corollary 4.10. Now $\Delta(\mathfrak{o}_0) = s^2 - 4n$ so $\Delta(\mathfrak{o}) = s^2 - 4n/f^2$ where $s^2 - 4n/f^2 \equiv 0$ or $1 \pmod 4$ and $f > 0, f \in Z$. Taking into account the fact that K must be imaginary quadratic and that an order of K is uniquely determined by its discriminant and writing $h(\Delta(\mathfrak{o})) = h(\mathfrak{o})$, $\omega(\Delta(\mathfrak{o})) = 1/2|U(\mathfrak{o})|$, and $c(s, f, \ell) = c_\ell(\mathfrak{o})$ where $\Delta(\mathfrak{o}) = s^2 - 4n/f^2$ and

noting the 1/2 in the definition of $a_k(s)$ we obtain the given formula.

LEMMA 4.16: *Let K be an imaginary quadratic number field. Let $\mathfrak{o}$ be an order of K of discriminant Δ and let $\mathfrak{o}'$ be the suborder of $\mathfrak{o}$ of index f. Then* $\frac{h(\mathfrak{o}')}{\omega(\mathfrak{o}')} = \frac{h(\mathfrak{o})}{\omega(\mathfrak{o})} f \prod_{\ell \mid f} \left(1 - \left\{\frac{\Delta}{\ell}\right\} 1/\ell\right)$

where $\left\{\frac{\Delta}{\ell}\right\} = \begin{cases} 0 & \text{if } \ell^2 \mid \Delta \text{ and } \ell^{-2}\Delta \equiv 0 \text{ or } 1 \pmod 4 \\ \left(\frac{\Delta}{\ell}\right), & \text{the Kronecker symbol, otherwise} \end{cases}$

PROOF: $h(\mathfrak{o}') = [J_K : \mathcal{U}(\mathfrak{o}')K^x] = h(\mathfrak{o})[\mathcal{U}(\mathfrak{o})K^x : \mathcal{U}(\mathfrak{o}')K^x]$
$= h(\mathfrak{o})[\mathcal{U}(\mathfrak{o})/U(\mathfrak{o}) : \mathcal{U}(\mathfrak{o}')/U(\mathfrak{o}')]$. Therefore
$\frac{h(\mathfrak{o}')}{|U(\mathfrak{o}')|} = \frac{h(\mathfrak{o})}{|U(\mathfrak{o})|}[\mathcal{U}(\mathfrak{o}) : \mathcal{U}(\mathfrak{o}')]$. Now
$|U(\mathfrak{o}')| = 2\omega(\mathfrak{o}')$ and $|U(\mathfrak{o})| = 2\omega(\mathfrak{o})$ by definition and
$[\mathcal{U}(\mathfrak{o}) : \mathcal{U}(\mathfrak{o}')] = \prod_{\ell < \infty} [U(\mathfrak{o}_\ell) : U(\mathfrak{o}'_\ell)] = f \prod_{\ell \mid f} \left(1 - \left\{\frac{\Delta}{\ell}\right\} 1/\ell\right)$.

COROLLARY 4.17: *Let K be an imaginary quadratic number field. Let $\mathfrak{o}$ be the maximal order of K and $\mathfrak{o}'$ a suborder of index f. Then* $\frac{h(\mathfrak{o}')}{\omega(\mathfrak{o}')} = \frac{h(\mathfrak{o})}{\omega(\mathfrak{o})} f \prod_{\ell \mid f} \left(1 - \left(\frac{K}{\ell}\right) 1/\ell\right)$ *where*

$\left(\frac{K}{\ell}\right) = \begin{cases} 1 & \text{if } \ell \text{ splits in } K \\ 0 & \text{if } \ell \text{ ramifies in } K \\ -1 & \text{if } \ell \text{ remains prime in } K \end{cases}$

is the Kronecker symbol. Note that $h(\mathfrak{o})$ is the "standard" class number of K.

THEOREM 4.18: *Let p be an odd prime and let M be any positive integer prime to p. The class number $H(p^2M)$ of orders of level p^2M is given by the formula*

$$H(p^2M) = \left(\frac{p^2-1}{12}\right) M \prod_{\ell \mid M} (1 + 1/\ell) + \begin{cases} 0 \text{ if } p \neq 3 \\ 4/3 \prod_{\ell \mid M} \left(1 + \left(\frac{-3}{\ell}\right)\right) \text{ if } p = 3 \end{cases}$$

Note that $\left(\frac{-3}{2}\right) = -1$. $\left(\frac{-3}{\ell}\right)$ is the Legendre symbol if $\ell \neq 2$.

PROOF: From the definition of the Brandt Matrices we see that

$H(p^2M) = \operatorname{tr} B_0(1; p^2, M)$ (see Remark 2.20 of [15]) and the theorem follows from Theorem 4.12 – just note Remark 4.13.

5. The structure of the Brandt Matrices

In this section we develop the structure of the Brandt Matrices for orders of level p^2M. The structure we study in this section is new (it does not occur in the study of Brandt Matrices of level $p^{2r+1}M, p \nmid M$ – see e.g. [15] or [3]) and depends somewhat on whether $p \equiv 1$ or $3 \pmod 4$. The difference between the cases $p \equiv 1$ and $p \equiv 3 \pmod 4$ will become clearer when we study the action of the $\tilde{W}$-operator $\tilde{W}_p$ in section 9 below.

PROPOSITION 5.1: *Let $\mathcal{M}$ be an order of level p^2M of $\mathfrak{A}$ and let I be a left $\mathcal{M}$-ideal. Set $S_I = \{c = N(x)/N(I)$ with $p \nmid c \mid x \in I\}$. Then $S_I \subseteq Z$, $S_I \neq \phi$ and either S_I consists entirely of residues* mod p *or S_I consists entirely of non-residues* mod p. *Further whether S_I consists of residues or non-residues depends only on the class of I.*

PROOF: Recall that $N(I)$, the norm of I, is the positive rational number that generates the fractional ideal of Q generated by $\{N(x) \mid x \in I\}$. Hence $N(x)/N(I) \in Z$ for $x \in I$ and the ideal generated by $\{N(x)/N(I) \mid x \in I\}$ is Z, so $S_I \subseteq Z$ and $S_I \neq \phi$. Now $I_p = \mathcal{M}_p\alpha$ for some $\alpha \in \mathfrak{A}_p^x$ and $\mathcal{M}_p = \beta^{-1}\mathcal{O}_p\beta$ for some $\beta \in \mathfrak{A}_p^x$. Let $x \in I$ with $p \nmid N(x)/N(I)$. Then $x \in I \subseteq I_p = \beta^{-1}\mathcal{O}_p\beta\alpha$, so $N(x)/N(I) = N(y)N(\alpha)/N(I)$ for some $y = \begin{pmatrix} a + bpv & c + dv \\ p(c - dv) & a - bpv \end{pmatrix} \in \mathcal{O}_p$ where $a, b, c, d \in Z_p$. Thus $N(y) \equiv a^2 \bmod p$ is a quadratic residue mod p. Since $\operatorname{ord}_p(N(\alpha)) = \operatorname{ord}_p(N(I))$, $N(\alpha)/N(I)$ is a unit of Z_p. Further if we write $I_p = \mathcal{M}_p\alpha'$, then $\alpha' = u\alpha$ for some unit u of $\mathcal{M}_p$ and as above $N(u)$ is a quadratic residue mod p. Thus $N(\alpha)/N(I)$ is a unit of Z_p and whether it is a residue or a non-residue mod p depends only on I. Since $N(x)/N(I) \equiv a^2N(\alpha)/N(I)$, we see that S_I consists entirely of residues or non-residues mod p according as $N(\alpha)/N(I)$ is a residue or a non-residue mod p. Finally, if J is in the same class as I, then $J = Ib$ for some $b \in \mathfrak{A}^x$ and $x \in J$ if and only if $x = yb$ for some $y \in I$. Hence $N(x)/N(J) = N(y)/N(I)$ and $S_J = S_I$.

DEFINITION 5.2: Let $\mathcal{M}$ be an order of level p^2M and let I be a left $\mathcal{M}$-ideal. I is said to be of *positive character* if S_I consists entirely of residues mod p and to be of *negative character* if S_I consists entirely of non-residues mod p.

Note that the character of an ideal depends only on the class of the ideal, so we can speak of the *character of an ideal class.*

REMARK 5.3: The phenomenon noted in Proposition 5.1 and Definition 5.2 was discussed by Parry in his thesis [11] where in section 3 he talks about the 'quadratic residue symbol' assigned to certain quadratic forms – in our case the form would be $q(x) = N(x)/N(I)$ as x varies over I. As in [11], we will see in Lemma 5.23 below that the character of an ideal will determine the behavior of its associated theta series $\Theta_I(\tau) = \Sigma_{x\in I} \exp(\tau N(x)/N(I))$ at the cusps of $\Gamma_0(p^2M)$.

DEFINITION 5.4: If $p \equiv 1(4)$, let $\delta_p = \begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix} \in \mathfrak{A}_p$ while if $p \equiv 3(4)$, let $\delta_p = \begin{pmatrix} 0 & -v \\ pv & 0 \end{pmatrix} \in \mathfrak{A}_p$. Let $\delta_\ell = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in \mathfrak{A}_\ell$ for all $\ell < \infty$, $\ell \neq p$ and let $\delta_\infty = 1 \in \mathfrak{A}_\infty$. Recall $v = \sqrt{u}$ where $u \in Z$, $\left(\frac{u}{p}\right) = -1$. Finally let $\tilde{\delta} = (\delta_\ell) \in J_{\mathfrak{A}}$.

LEMMA 5.5: *Let $\mathcal{M}$ be an order of level p^2M of $\mathfrak{A}$ and let $\tilde{\delta}$ be as in Definition 5.4. Then $\tilde{\delta}^{-1}\mathcal{M}\tilde{\delta} = \mathcal{M}$, $\mathcal{M}\tilde{\delta}^2 = \mathcal{M}\epsilon$ and $N(\mathcal{M}\tilde{\delta}) = \epsilon$ where*

$$\epsilon = \begin{cases} 1 \text{ if } p \equiv 1(\text{mod } 4) \\ p \text{ if } p \equiv 3(\text{mod } 4) \end{cases}$$

PROOF: $\tilde{\delta}^{-1}\mathcal{M}\tilde{\delta} = \mathcal{M}$ if and only if $\tilde{\delta}_\ell^{-1}\mathcal{M}_\ell\tilde{\delta}_\ell^{-1} = \mathcal{M}_\ell$ for all $\ell < \infty$. Clearly this is true for all $\ell \neq p$. Now by Theorem 1.5, $\mathcal{M}_p$ is the unique order of level p^2 in $\mathfrak{A}_p$, so $a^{-1}\mathcal{M}_p a = \mathcal{M}_p$ for all $a \in \mathcal{M}_p^\times$, in particular for δ_p. For the second statement $\mathcal{M}\tilde{\delta}^2 = \mathcal{M}\epsilon$ if and only if $\mathcal{M}_\ell\delta_\ell^2 = \mathcal{M}_\ell\epsilon$ for all $\ell < \infty$ and this is clear. Finally if $I = \mathcal{M}\tilde{\alpha}$, then $N(I)$ is the positive rational number that represents the coset $N(\tilde{\alpha})\mathcal{U}(Z)$ in $J_Q/\mathcal{U}(Z)$. Here if $\tilde{\alpha} = (\alpha_p)$, then $N(\tilde{\alpha}) = (N(\alpha_p)) \in J_Q$ and $\mathcal{U}(Z) = \{\tilde{\beta} = (\beta_\ell) \in J_Q \mid \beta_\ell \in U(Z_\ell) \text{ for all } \ell < \infty\}$. Now the third statement is clear.

PROPOSITION 5.6: *Let $\mathcal{M}$ be an order of level p^2M and I some left $\mathcal{M}$-ideal. Let $\tilde{\delta}$ be as in Definition 5.4. Then $\tilde{\delta}I$ is also a left $\mathcal{M}$-ideal and I is of positive character if and only if $\tilde{\delta}I$ is of negative character. Conversely I is of negative character if and only if $\tilde{\delta}I$ is of positive character.*

PROOF: $I = \mathcal{M}\tilde{\alpha}$ for some $\tilde{\alpha} \in J_{\mathfrak{A}}$. Then $\tilde{\delta}I = \tilde{\delta}\mathcal{M}\tilde{\alpha} = \mathcal{M}\tilde{\delta}\tilde{\alpha}$ (by Lemma 5.5) is again a left $\mathcal{M}$-ideal. Now let ϵ be as in Lemma 5.5.

Then $\tilde{\delta}^2 I = \mathcal{M}\tilde{\delta}^2\tilde{\alpha} = I\epsilon$ is in the same class as I and so the second statement follows from the first. We prove the first statement. Note that $N(\tilde{\delta}I) = \epsilon N(I)$. Let $I_p = \mathcal{M}_p\alpha_p$. Then by the proof of Proposition 5.1 the fact that I has positive character implies that $N(\alpha_p)/N(I)$ is a quadratic residue mod p. Now $(\tilde{\delta}I)_p = \delta_p I_p = \mathcal{M}_p\delta_p\alpha_p$ and so $N(\delta_p\alpha_p)/N(\tilde{\delta}I) = (N(\delta_p)/\epsilon)(N(\alpha_p)/N(I))$ is a residue or non-residue according as $N(\delta_p)/\epsilon$ is a residue or non-residue. But $N(\delta_p)/\epsilon = \begin{cases} -u \text{ if } p \equiv 1 (\text{mod } 4) \\ u \text{ if } p \equiv 3 (\text{mod } 4) \end{cases}$ is a non-residue, so again by the proof of Proposition 5.1, we are done.

REMARK 5.7: Clearly we do not have to consider the separate cases $p \equiv 1(\text{mod } 4)$ and $p \equiv 3(\text{mod } 4)$ to prove the above result. It would suffice to use the definition given for δ_p in the case $p \equiv 3(\text{mod } 4)$ for all cases. The reason we have chosen $\tilde{\delta}$ as we have is so that the action of the $\tilde{W}$-operator $\tilde{W}_p$ will be nice – see section 9 below.

COROLLARY 5.8: *Let $\mathcal{M}$ be an order of level p^2M and let I be a left $\mathcal{M}$-ideal. Then I and $\tilde{\delta}I$ are never in the same class.*

PROOF: Ideals in the same class have the same character.

THEOREM 5.9: *Let $\mathcal{M}$ be an order of level p^2M. Let $I_1, \ldots, I_G$ be a set of representatives of all the distinct left $\mathcal{M}$-ideal classes of positive character. Let $\tilde{\delta}$ be as in Definition 5.4. Then $\tilde{\delta}I_1, \ldots, \tilde{\delta}I_G$ represent all the distinct left $\mathcal{M}$-ideal classes of negative character. Also $I_1, \ldots, I_G$, $\tilde{\delta}I_1, \ldots, \tilde{\delta}I_G$ is a complete set of representatives of all the distinct left $\mathcal{M}$-ideal classes.*

PROOF: Clearly the $\tilde{\delta}I_i$, $i = 1, \ldots, G$ represent distinct ideal classes since $\tilde{\delta}I_i = \tilde{\delta}I_j a$ with $a \in \mathfrak{A}^x$ implies $I_i = I_j a$ which implies $i = j$. Thus $I_1, \ldots, I_G$, $\tilde{\delta}I_1, \ldots, \tilde{\delta}I_G$ represent distinct ideal classes. Let I be any left $\mathcal{M}$-ideal. If I is of positive character, then $I = I_i a$ for some i, $1 \le i \le G$ and some $a \in \mathfrak{A}^x$. If I is of negative character, then $\tilde{\delta}I$ is of positive character, so $\tilde{\delta}I = I_j b$ for some j, $1 \le j \le G$ and some $b \in \mathfrak{A}^x$. Hence $\tilde{\delta}^2 I = \epsilon I = \tilde{\delta}I_j b$ or $I = \tilde{\delta}I_j b\epsilon^{-1}$. Thus $I_1, \ldots, I_G$, $\tilde{\delta}I_1, \ldots, \tilde{\delta}I_G$ represent all the left $\mathcal{M}$-ideal classes.

COROLLARY 5.10: *The ideal class number $H(p^2M)$ for orders of level p^2M is even.*

REMARK 5.11: We have an explicit formula for $H(p^2M)$ given by

Theorem 4.18 and it is easy to see from that formula that $H(p^2M)$ is always even.

PROPOSITION 5.12: *Let $\mathcal{M}$ be an order of level p^2M. If $p>3$, then $|U(\mathcal{M})|=2$. If $p=3$, then $|U(\mathcal{M})|=2$ or 6. Further if $p=3$ and M is divisible by 2 or by a prime $\equiv 2 \pmod 3$, then $|U(\mathcal{M})|=2$.*

PROOF: Suppose u is a unit of $\mathcal{M}$ with $u \neq \pm 1$ and consider $Q(u)$, the subfield of $\mathfrak{A}$ generated by u. $Q(u)$ is an imaginary quadratic number field and u is a unit of that field. Hence $u \sim \pm i$ or $u \sim \frac{\pm 1 \pm \sqrt{-3}}{2}$ where $\sim$ means 'has the same minimal polynomial as.' Thus we can assume $\mathcal{M}$ contains an element ω' with either $\omega' \sim i$ or $\omega' \sim \frac{-1+\sqrt{-3}}{2}$. Now $\omega' \epsilon \mathcal{M} \subseteq \mathcal{M}_p$ which is isomorphic to $\mathcal{O}_p$, so finally we can assume $\mathcal{O}_p$ contains an element ω with either $\omega \sim i$ or $\omega \sim \frac{-1+\sqrt{-3}}{2}$. But then $\omega = \begin{pmatrix} a+bpv & c+dv \\ p(c-dv) & a-bpv \end{pmatrix} \in \mathcal{O}_p$ for some $a, b, c, d \in Z_p$. In the first case $\operatorname{tr}(\omega)=0$ and $N(\omega)=1$ imply $1 \equiv 0 \pmod p$, a contradiction. In the second case $\operatorname{tr}(\omega)=-1$ and $N(\omega)=1$ imply $a=-\frac{1}{2}$ and $4=4N(\omega) \equiv 1 \pmod p$, that is $p=3$. Thus we need only consider the case $p=3$. There is upto isomorphism only one order of level $3^2 \cdot 1$. This is true since by Theorem 4.18, the class number of an order of level $3^2 \cdot 1$ is 2. Thus if $\mathcal{M}$ is an order of level $3^2 \cdot 1$ and $\tilde{\delta}$ is as in Theorem 5.9, $\mathcal{M}$ and $\tilde{\delta}\mathcal{M} = \mathcal{M}\tilde{\delta}$ are representatives of the two left $\mathcal{M}$-ideal classes. But then, by the proof of Proposition 2.15 of [14], any order of level $3^2 \cdot 1$ must be isomorphic to $\mathcal{M}$. Now an 'easy' calculation (see [15]) shows that $|U(\mathcal{M})|=6$ if $\mathcal{M}$ has level $3^2 \cdot 1$. Since any order of level 3^2M, $3 \nmid M$ is contained in an order of level $3^2 \cdot 1$, $|U(\mathcal{M})| \leq 6$ for any order $\mathcal{M}$ of level 3^2M. But $\mathcal{M}$ can not contain an element $\sim i$, so $|U(\mathcal{M})|=2$ or $|U(\mathcal{M})|=6$. Now assume $\mathcal{M}$ has level $3^2 \cdot M$ and $\mathcal{M}$ contains an element $\omega \sim \frac{-1+\sqrt{-3}}{2}$. Let ℓ be a prime dividing M. Then $\mathcal{M}_\ell \cong \begin{pmatrix} Z_\ell & Z_\ell \\ MZ_\ell & Z_\ell \end{pmatrix} \subseteq \begin{pmatrix} Z_\ell & Z_\ell \\ \ell Z_\ell & Z_\ell \end{pmatrix}$ so $\begin{pmatrix} Z_\ell & Z_\ell \\ \ell Z_\ell & Z_\ell \end{pmatrix}$ contains an element with trace -1 and norm 1, which implies $-x(x+1) \equiv 1$ has a solution in Z_ℓ, that is $\ell \equiv 1 \pmod 3$. This completes the proof.

REMARK 5.13: The reason we have given Proposition 5.12 is that when $|U(\mathcal{M})|$ depends only on the level of $\mathcal{M}$, not on its isomorphism class, the Brandt Matrices become simpler and also isolating the two

Eisenstein series in the case of weight 2 (see Remark 5.26 below) becomes simpler. Also if $|U(\mathcal{M})| = 2$ for all orders of level p^2M, then for all weights $k \geq 2$ all modular forms given in Theorem 5.31 below are non-zero. Unfortunately it is not true in general that $|U(\mathcal{M})|$ depends only on the level. The simplest possible example (taking into account Lemma 5.12) $p = 3$, $M = 7$ provides examples of orders $\mathcal{M}$ and $\mathcal{M}'$, both of level $3^2 \cdot 7$, with $|U(\mathcal{M})| = 2$ and $|U(\mathcal{M}')| = 6$.

We now begin to determine the structure of the Brandt Matrices $B_s(n; p^2, M)$

DEFINITION 5.14: Let $I_1, \ldots, I_G, \tilde{\delta}I_1, \ldots, \tilde{\delta}I_G$ be a complete set of representatives of all the left $\mathcal{O}$-ideal classes as in Theorem 5.9. Here $I_1, \ldots, I_G$ represent the ideals of positive character and $\tilde{\delta}I_1, \ldots, \tilde{\delta}I_G$ represent the ideals of negative character. Let $I_{G+i} = \tilde{\delta}I_i$ for $i = 1, \ldots, G$. Letting $b_{ij}^s(n)$ be as in (4.1) we define

$$C_s(n) = C_s(n; p^2, M) = (b_{ij}^s(n)), \quad 1 \leq i, j \leq G$$

and

$$D_s(n) = D_s(n; p^2, M) = (b_{ij}^s(n)), \quad G+1 \leq i \leq 2G = H, \quad 1 \leq j \leq G$$

Note that $C_s(n)$ and $D_s(n)$ are $G(s+1)$ by $G(s+1)$ matrices.

THEOREM 5.15: *Let $\mathcal{O}$ be an order of level p^2M, and let $I_1, \ldots, I_G$, $I_{G+1} = \tilde{\delta}I_1, \ldots, I_H = \tilde{\delta}I_G$ be a set of representatives of the left $\mathcal{O}$-ideal classes as in Definition 5.14 above. Then the corresponding Brandt Matrices $B_s(n) = B_s(n; p^2, M)$ are composed of four blocks as follows:*

$$B_s(n) = \left(\begin{array}{c|c} C_s(n) & \epsilon^s D_s(n) \\ \hline D_s(n) & C_s(n) \end{array}\right)$$

where the $C_s(n)$ and $D_s(n)$ are given in Definition 5.14

and

$$\epsilon = \begin{cases} 1 \text{ if } p \equiv 1 \pmod 4 \\ p \text{ if } p \equiv 3 \pmod 4. \end{cases}$$

PROOF: Note first that $\mathcal{O}_{j+G} = I_{j+G}^{-1} I_{j+G} = I_j^{-1} \tilde{\delta}^{-1} \tilde{\delta} I_j = I_j^{-1} I_j = \mathcal{O}_j$ for $j = 1, \ldots, G$. We first show that $b_{ij}^s(n) = b_{i+G,j+G}^s(n)$ for all $1 \leq i, j \leq G$. By (4.1) $b_{ij}^s(n) = e_j^{-1} \Sigma_\alpha X_s^t(\alpha)$ where the sum is over all $\alpha \in I_j^{-1} I_i$ with

$N(\alpha) = nN(I_i)/N(I_j)$. But $I_j^{-1}I_i = I_j^{-1}\tilde{\delta}^{-1}\tilde{\delta}I_i = I_{j+G}^{-1}I_{i+G}$ and $e_j = |U(\mathcal{O}_j)| = |U(\mathcal{O}_{j+G})| = e_{j+G}$, so $b_{ij}^s(n) = b_{i+G,j+G}^s(n)$. We next consider the relation between $b_{i+G,j}^s(n)$ and $b_{i,j+G}^s(n)$, $1 \le i, j \le G$. Note that $I_j^{-1}I_{i+G} = I_j^{-1}\tilde{\delta}I_i = I_j^{-1}\tilde{\delta}^{-1}\tilde{\delta}^2 I_i = I_{j+G}^{-1}I_i\epsilon$ by Lemma 5.5. Thus $\alpha \in I_{j+G}^{-1}I_i$ with $N(\alpha) = nN(I_i)/N(I_{j+G}) = nN(I_i)/\epsilon N(I_j)$ if and only if $\epsilon\alpha \in I_j^{-1}I_{i+G}$ with $N(\epsilon\alpha) = nN(I_{i+G})/N(I_j)$. Hence $b_{i+G,j}^s(n) = \Sigma_\alpha X_s^t(\epsilon\alpha) = \epsilon^s \Sigma_\alpha X_s^t(\alpha) = \epsilon^s b_{i,j+G}^s(n)$ where the sum is over all $\alpha \in I_{j+G}^{-1}I_i$ with $N(\alpha) = nN(I_i)/N(I_{j+G})$.

PROPOSITION 5.16: *Assume* $p \equiv 1 \pmod 4$ *and* $p \mid n$. *Then* $C_s(n) = D_s(n)$ *for all* n.

PROOF: Note that as $p \equiv 1 \pmod 4$, $\epsilon = 1$. We need to show that $b_{ij}^s(n) = b_{i+G,j}^s(n)$ for all $1 \le i, j \le G$ in the notation of Theorem 5.15 above. We claim that $\alpha \in I_j^{-1}I_i$ with $p \mid N(\alpha)N(I_j)/N(I_i)$ if and only if $\alpha \in I_j^{-1}I_{i+G}$ with $p \mid N(\alpha)N(I_j)/N(I_{i+G})$. Since $N(I_i) = N(I_{i+G})$, we need only show that for $\alpha \in \mathfrak{A}$ with $p \mid N(\alpha)N(I_j)/N(I_i)$, then $\alpha \in I_j^{-1}I_i$ if and only if $\alpha \in I_j^{-1}I_{i+G}$. Now $\alpha \in I_j^{-1}I_i$ if and only if $\alpha \in (I_j^{-1}I_i)_\ell$ for all $\ell < \infty$ and similarly for $I_j^{-1}I_{i+G}$. But $(I_j^{-1}I_i)_\ell = (I_j^{-1}I_{i+G})_\ell$ for all $\ell \neq p$, so we need only worry about $(I_j^{-1}I_i)_p$ and $(I_j^{-1}I_{i+G})_p$. Letting $I_{kp} = \mathcal{O}_p\gamma_{kp}$ for $k = 1, \ldots, G$, we have $(I_j^{-1}I_i)_p = \gamma_{jp}^{-1}\mathcal{O}_p\gamma_{ip}$ and $(I_j^{-1}I_{i+G})_p = \gamma_{jp}^{-1}\mathcal{O}_p\delta_p\gamma_{ip}$ where $\delta_p = \begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix} \in \mathfrak{A}_p^\times$ by Definition 5.4. Thus $\alpha \in (I_j^{-1}I_i)_p$ if and only if $\alpha = \gamma_{jp}^{-1}\beta\gamma_{ip}$ for some $\beta \in \mathcal{O}_p$. Further $p \mid N(\alpha)N(I_j)/N(I_i)$ if and only if $p \mid N(\beta)$. Similarly $\alpha \in (I_j^{-1}I_{i+G})_p$ with $p \mid N(\alpha)N(I_j)/N(I_i)$ if and only if $\alpha = \gamma_{jp}^{-1}\beta^1\gamma_{ip}$ with $\beta^1 \in \mathcal{O}_p\delta_p$ where $p \mid N(\beta^1)$. But it is easy to check using the definition of $\mathcal{O}_p$ that if $p \mid N(\beta)$, then $\beta \in \mathcal{O}_p$ if and only if $\beta \in \mathcal{O}_p\delta_p$ and this proves our claim. The proposition now follows easily from the claim and the definition of the $b_{ij}^s(n)$.

REMARK 5.17: If $p \equiv 3(4)$, at least in several cases it is true that $C_0(n) = D_0(n)$ when $p \mid n$. If it were true in general that $D_s(n) = \epsilon^{s/2}C_s(n)$ when $p \mid n$, then the statements of many results to follow could be simplified. It seems that if $D_s(n) = \epsilon^{s/2}C_s(n)$ when $p \mid n$ is true in general, then it should be easy to prove. However, we have not found a proof.

THEOREM 5.18: *Let* $C_s(n)$ *and* $D_s(n)$ *be as in Definition* 5.14. *If* n *is a quadratic residue* mod p, *then* $D_s(n) = 0$. *If* n *is a quadratic non-residue* mod p, *then* $C_s(n) = 0$.

PROOF: A typical entry block of $C_s(n)$ is $b_{ij}^s(n)$, $1 \le i, j \le G$. $e_j b_{ij}^s(n) = \Sigma_\alpha X_s^t(\alpha)$ where the sum is over all $\alpha \in I_j^{-1} I_i$ with $N(\alpha)/N(I_j^{-1} I_i) = n$. Now I_i and I_j are both ideals of positive character and so $I_j^{-1} I_i$ is also an ideal of positive character. Hence if n is a non-residue mod p, there are no $\alpha \in I_j^{-1} I_i$ with $N(\alpha)/N(I_j^{-1} I_i) = n$ and so $b_{ij}^s(n) = 0$. Thus $C_s(n) = 0$ if n is a non-residue mod p. A typical entry block of $D_s(n)$ is $b_{i+G,j}^s(n)$ $1 \le i, j \le G$. This corresponds to the ideal $I_j^{-1} I_{i+G}$ which is of negative character, so $D_s(n) = 0$ if n is a residue mod p.

PROPOSITION 5.19: *Let p be an odd prime and M a positive integer prime to p. Let $C_s(n) = C_s(n; p^2, M)$ and $D_s(n) = D_s(n; p^2, M)$. Then the entries of the matrix series $\Sigma_{n=0}^\infty C_s(n) \exp(n\tau)$ and $\Sigma_{n=0}^\infty D_s(n) \exp(n\tau)$ are modular forms of weight $2+s$ on $\Gamma_0(N)$, $N = p^2 M$. If $s > 0$, they are cusp forms. Recall that $\exp(n\tau) = e^{2\pi i n \tau}$.*

PROOF: This follows by the methods used in the proof of Theorem 2.14 of [15]. See also Eichler [3], Theorem 1, on p. 105 and Ogg [10], Theorem 20 on p. VI-22.

Now consider the case $s = 0$, i.e. we consider modular forms of weight 2. We want to show how to obtain cusp forms in this case also.

LEMMA 5.20: *Let $\mathcal{M}$ be an order of level $p^2 M$ and let I and J be left $\mathcal{M}$-ideals. Let $\Theta_I = \Sigma_{\alpha \in I} \exp(\tau N(\alpha)/N(I))$ be the theta series attached to I and similarly for J. If I and J have the same character, then $\Theta_I(\tau) - \Theta_J(\tau)$ is a cusp form of weight 2 on $\Gamma_0(N)$, $N = p^2 M$.*

PROOF: As in Proposition 5.19 $\Theta_I(\tau)$ and $\Theta_J(\tau)$ are modular forms of weight 2 on $\Gamma_0(N)$. $\Theta_I(\tau)$ is the theta series associated to the quadratic form $N(x)/N(I)$, $x \in I$ and similarly for $\Theta_J(\tau)$. Since I and J have the same character, the quadratic forms $N(x)/N(I)$, $x \in I$ and $N(x)/N(J)$, $x \in J$ belong to the same genus, i.e. they are locally equivalent for all primes ℓ. This is clear if $\ell = \infty$. If $\ell < \infty$, then fixing ℓ we have $I_\ell = \mathcal{M}_\ell a$ and $J_\ell = \mathcal{M}_\ell b$ for some $a, b \in \mathfrak{A}_\ell^\times$ and

$$uN(b)/N(J) = N(a)/N(I) \tag{5.1}$$

for some unit u of Z_ℓ. If $\ell \neq p$, then every unit of Z_ℓ is the norm of some unit of $\mathcal{M}_\ell$ so $N(u') = u$ for some $u' \in U(\mathcal{M}_\ell)$. Then letting $b' = u'b$, we have $J_\ell = \mathcal{M}_\ell b'$ and the map $x \mapsto xa^{-1}b'$ is a local isometry from I_ℓ to J_ℓ (i.e. $N(x)/N(I) = N(xa^{-1}b')/N(J)$). If $\ell = p$, then by the proof of Proposition 5.1, $N(a)/N(I)$ and $N(b)/N(J)$ are both residues

or both non-residues mod p. Thus the unit u in (5.1) is a residue mod p and hence u is the norm of some unit, say u', of $\mathcal{M}_p$. So again letting $b' = u'b$ we have $J_p = \mathcal{M}_p b'$ and the map $x \mapsto xa^{-1}b'$ is a local isometry. Now it is a classical result (see Siegel [18], p. 376) that theta series associated to quadratic forms in the same genus have the same behavior at all cusps, so the difference of two such theta series is a cusp form. This completes the proof of the Lemma.

REMARK 5.21: If I and J are left $\mathcal{M}$-ideals of different character, then the quadratic forms $N(x)/N(I)$, $x \in I$ and $N(x)/N(J)$, $x \in J$ are in different genera (since one represents residues and the other non-residues mod p) and their associated theta series have different behaviors at the cusps (see Parry [11], section 3 and Theorem 5.34 below).

LEMMA 5.22: *The difference of two theta series appearing in the same column of the matrix series* $\Sigma_{n=0}^{\infty} C_0(n) \exp(n\tau)$ (resp. $\Sigma_{n=0}^{\infty} D_0(n) \exp(n\tau)$) *is a cusp form.*

PROOF: In the notation of Lemma 5.20, the ith, jth entry of $\Sigma_{n=0}^{\infty} C_0(n) \exp(n\tau)$ is $\frac{1}{e_j} \Theta_{I_j^{-1}I_i}(\tau)$. Now $I_j^{-1}I_i$ and $I_j^{-1}I_k$ for $1 \le i, j, k \le G$ are both left $\mathcal{O}_j$-ideals of positive character, so the present lemma follows from Lemma 5.20. Similarly the ith, jth entry of $\Sigma_{n=0}^{\infty} D_0(n) \exp(n\tau)$ is $1/e_j \Theta_{I_j^{-1}I_{i+G}}(\tau)$ and $I_j^{-1}I_{i+G}$ and $I_j^{-1}I_{k+G}$ for $1 \le i, j, k \le G$ are both of negative character, so again the lemma follows from Lemma 5.20.

LEMMA 5.23: *Let* $C_0(n) = (c_{ij}(n))$, $D_0(n) = (d_{ij}(n))$, $1 \le i, j \le G$. *Then*

(a) $e_j c_{ij}(n) = e_i c_{ji}(n)$ *and* $e_j d_{ij}(n) = e_i d_{ji}(n)$ *for all* $i, j, 1 \le i, j \le G$ *and all* $n \ge 0$.

(b) $\sum_{j=1}^{G} c_{ij}(n) = c(n)$ *(say) is independent of* i *and* $\sum_{j=1}^{G} d_{ij}(n) = d(n)$ *(say) is independent of* i.

(c) $c(0) = d(0)$.

PROOF: (a), (b), and (c) are clear for $n = 0$. Thus we assume $n \ge 1$. $c_{ij}(n)$ equals $1/e_j$ times the number of elements $\alpha \in I_j^{-1}I_i$ with $N(\alpha) = nN(I_i)/N(I_j)$. But $I_j^{-1} = (1/N(I_j))\bar{I}_j$ where $\bar{}$ denotes the canonical involution of $\mathfrak{A}$. Hence $e_j c_{ij}(n)$ is equal to the number of elements $\beta \in \bar{I}_j I_i$ with $N(\beta) = nN(I_j)N(I_i)$. Similarly $e_i c_{ji}(n)$ is equal to the number of elements $\beta' \in \bar{I}_i I_j$ with $N(\beta') = nN(I_i)N(I_j)$. But $\beta \in \bar{I}_j I_i$ if

and only if $\bar{\beta} \in \bar{I}_i I_j$, so $e_j c_{ij}(n) = e_i c_{ji}(n)$. Now consider $D_0(n)$. $d_{ij}(n) = b_{i+G,j}(n)$ where $b_{\nu,\mu}(n) = b^0_{\nu,\mu}(n)$. The above argument shows that $e_j b_{i+G,j}(n) = e_{i+G} b_{j,i+G}(n)$. But from Theorem 5.15 we know that $e_{i+G} = e_i$ and $b_{j,i+G}(n) = b_{j+G,i}(n)$, so we obtain $e_j d_{ij}(n) = e_i d_{ji}(n)$ which finishes the proof of (a). Now consider (b). If $\alpha \in I_j^{-1} I_i$ with $N(\alpha) = nN(I_i)/N(I_j)$, then $I_i^{-1} I_j \alpha$ is an integral left $\mathcal{O}_i$-ideal (recall $\mathcal{O}_i$ is the right order of I_i) of norm n. Integral means that $I_i^{-1} I_j \alpha \subseteq \mathcal{O}_i$. Conversely all integral left $\mathcal{O}_i$-ideals in the same class as $I_i^{-1} I_j$ having norm n must be of the form $I_i^{-1} I_j \alpha$ for some $\alpha \in I_j^{-1} I_i$ with $N(\alpha) = nN(I_i)/N(I_j)$. Further two such ideals $I_i^{-1} I_j \alpha$ and $I_i^{-1} I_j \beta$ are equal if and only if $I_j \alpha = I_j \beta$ if and only if $\alpha = u\beta$ for some $u \in U(\mathcal{O}_j)$. Thus $c_{ij}(n)$ is precisely the number of integral left $\mathcal{O}_i$-ideals in the same class as $I_i^{-1} I_j$ which have norm n. It is clear that $I_i^{-1} I_1, \ldots, I_i^{-1} I_G$ are a complete set of representatives of all the distinct left $\mathcal{O}_i$-ideal classes of positive character. Thus $\sum_{j=1}^{G} c_{ij}(n)$ is equal to the number of integral left $\mathcal{O}_i$-ideals of positive character having norm n and we need only show that this number depends only on the level, not on the particular order $\mathcal{O}_i$ we happen to choose. Let $\mathcal{M}$ be an arbitrary order of level $p^2 M$. Then $\mathcal{M} = \tilde{\alpha} \mathcal{O} \tilde{\alpha}^{-1}$ for some $\tilde{\alpha} \in J_{\mathfrak{P}}$ and the map $\mathcal{O}\tilde{\beta} \mapsto \tilde{\alpha}\mathcal{O}\beta\tilde{\alpha}^{-1} = \mathcal{M}\tilde{\alpha}\beta\tilde{\alpha}^{-1}$ gives a bijection from integral left $\mathcal{O}$-ideals of positive character with norm n onto the set of integral left $\mathcal{M}$-ideals of positive character with norm n. This proves (b) for $c(n)$. The proof that $\sum_{j=1}^{G} d_{ij}(n)$ is independent of i is completely analogous to the above except that we must of course consider ideals of negative character.

LEMMA 5.24: *Let the notation be as in Lemma* 5.23.

Consider the matrix $A = \begin{pmatrix} 1 & e_1 e_2^{-1} & \ldots & e_1 e_G^{-1} \\ \vdots & -1 & 0 & \\ \vdots & & \ddots & \\ 1 & 0 & & \cdot\ -1 \end{pmatrix}$

that is $A = (a_{ij})$ *where* $a_{i1} = 1$ *for* $i = 1, \ldots, G$, $a_{1j} = e_1 e_j^{-1}$ *for* $j = 1, \ldots, G$; $a_{ii} = -1$ *for* $i = 2, \ldots, G$ *and all other* $a_{ij} = 0$ $(i \neq 1,\ j \neq 1,\ i \neq j)$. *Then*

$$AC_0(n)A^{-1} = \begin{pmatrix} c(n) & 0 & \ldots & 0 \\ 0 & & & \\ \vdots & & C_0'(n) & \\ \vdots & & & \\ 0 & & & \end{pmatrix}$$

$$\text{and } AD_0(n)A^{-1} = \begin{pmatrix} d(n) & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & D_0'(n) & \\ 0 & & & \end{pmatrix}$$

where $C_0'(n)$ *and* $D_0'(n)$ *are* $G-1$ *by* $G-1$ *matrices. Further letting* $C_0'(n) = (c_{ij}'(n))$ *and* $D_0'(n) = (d_{ij}'(n))$, *we have* $c_{ij}'(n) = c_{i+1,j+1}(n) - c_{1,j+1}(n)$ *and* $d_{ij}'(n) = d_{i+1,j+1}(n) - d_{1,j+1}(n)$ *for all* i, j, $1 \le i, j \le G-1$ *and all* $n \ge 0$.

PROOF: Let $m = \Sigma_{i=1}^{G} e_i^{-1}$. Then $A^{-1} = (1/m)F$ where $F = (f_{ij})$ is given by $f_{ij} = e_j^{-1}$ if $i \neq j$; $f_{11} = e_1^{-1}$; and $f_{ii} = e_i^{-1} - m$ for $i = 2, \dots, G$. The lemma now follows from Lemma 5.23 by an easy exercise in manipulating summation symbols – if the reader needs help, he can peek at the proof of Lemma 2.22 in [15].

REMARK 5.25: Note that by Theorem 2.21, $c(n) = 0$ and $C_0'(n) = 0$ if n is a non-residue mod p where as $d(n) = 0$ and $D_0'(n) = 0$ if n is a residue mod p. Further if $p \equiv 1 \pmod 4$ and $p \mid n$, then by Proposition 5.16, $c(n) = d(n)$ and $C_0'(n) = D_0'(n)$.

REMARK 5.26: If $p > 3$ or M is divisible by 2 or by a prime $\equiv 2 \pmod 3$, then it follows from Lemma 5.12 that all $e_i = 2$. Thus the matrix A becomes quite simple in these cases.

Now we are finally able to obtain cusp forms in the case of weight 2. In fact they are given by

PROPOSITION 5.27: *Let the notation be as in Lemma* 5.24. *Then the entries of the matrix series* $\Sigma_{n=0}^{\infty} C_0'(n) \exp(n\tau)$ *and* $\Sigma_{n=0}^{\infty} D_0'(n) \exp(n\tau)$ *are cusp forms of weight* 2 *on* $\Gamma_0(N)$, $N = p^2M$.

PROOF: This follows immediately from Lemmas 5.22 and 5.24.

PROPOSITION 5.28: *Fix* p, M, $N = p^2M$, *and* $s \ge 0$ *as above. Then the* $C_s(n)$ *and* $D_s(n)$ *with* $(n, N) = 1$ *generate a commutative semi-simple ring. Similarly, the* $C_0'(n)$ *and* $D_0'(n)$ *with* $(n, N) = 1$ *generate a commutative semi-simple ring.*

PROOF: From Theorem 2 on p. 106 of Eichler [3], the $B(n) = B_s(n; p^2, M)$ with $(n, N) = 1$ generate a commutative ring. Thus it follows from Theorems 5.15 and 5.18 above that $C_s(n)$ and $D_s(n)$ with

$(n, N) = 1$ generate a commutative ring and clearly, by Lemma 5.24, so do the $C_0'(n)$ and $D_0'(n)$ with $(n, N) = 1$. By a proof similar to that of Theorem 2 on p. 106 of [3] we see that the rings generated are in fact semi-simple.

Fix p, M, $N = p^2M$, and $s \geq 0$. Then by Proposition 5.28 there exists a $G(s+1)$ by $G(s+1)$ matrix E such that $EC_s(n)E^{-1}$ and $ED_s(n)E^{-1}$ are simultaneously diagonal matrices for all n with $(n, N) = 1$. Similarly there exists $G-1$ by $G-1$ matrix E' such that $E'C_0'(n)E'^{-1}$ and $E'D_0'(n)E'^{-1}$ are simultaneously diagonal matrices for all n with $(n, N) = 1$.

LEMMA 5.29: *Fix p, M, $N = p^2M$ and s an even positive integer as above. Let E_1 denote the $H(s+1)$ by $H(s+1)$ matrix* $\left(\begin{array}{c|c} E & \epsilon^t E \\ \hline E & -\epsilon^t E \end{array}\right)$ *where E is the $G(s+1)$ by $G(s+1)$ matrix given in the above paragraph and $t = s/2$. Recall $\epsilon = 1$ if $p \equiv 1 \pmod 4$ and $\epsilon = p$ if $p \equiv 3 \pmod 4$. Finally let $B_s(n) = B_s(n; p^2M)$, $C_s(n) = C_s(n; p^2, M)$, and $D_s(n) = D_s(n; p^2, M)$. Then*

$$E_1B_s(n)E_1^{-1} = E_1\left(\begin{array}{c|c} C_s(n) & \epsilon^s D_s(n) \\ \hline D_s(n) & C_s(n) \end{array}\right)E_1^{-1}$$

$$= \left(\begin{array}{c|c} E(C_s(n) + \epsilon^t D_s(n))E^{-1} & 0 \\ \hline 0 & E(C_s(n) - \epsilon^s D_s(n))E^{-1} \end{array}\right)$$

$$= B_s'(n) \text{ (say).}$$

Further $B_s'(n) = B_s'(n; p^2, M)$ is a diagonal matrix for all n with $(n, N) = 1$.

PROOF: The first equality is Theorem 5.15 above and the second just follows by matrix multiplication. The fact that $B_s'(n)$ is diagonal for $(n, N) = 1$ follows from the definition of E.

LEMMA 5.30: *Fix p, M, and $N = p^2M$. Let E_2 denote the $H \times H$ matrix given on the next page*

where E' is the $G-1$ by $G-1$ matrix given in the paragraph preceeding Lemma 5.29 above. Let E_1' denote the $H \times H$ matrix $E_1' =$ $E_2\left(\begin{array}{c|c} A & A \\ \hline -A & A \end{array}\right)$ *where A is the $G \times G$ matrix given in Lemma 2.27. Finally let $B_0(n) = B_0(n; p^2, M)$, $C_0'(n) = C_0'(n)p^2, M)$, and $D_0'(n) = D_0'(n; p^2, M)$.*

$$E_2 = \left(\begin{array}{c|c} \begin{matrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & E' & \\ 0 & & & \end{matrix} & \begin{matrix} & & & \\ & & 0 & \\ & & & \end{matrix} \\ \hline \begin{matrix} & & & \\ & & 0 & \\ & & & \end{matrix} & \begin{matrix} 1 & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & E' & \\ 0 & & & \end{matrix} \end{array}\right)$$

Then $E_1' B_0(n) E_1'^{-1}$

$$= \left(\begin{array}{c|c} \begin{matrix} c(n)+d(n) & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & E'(C_0'(n)+D_0'(n))E'^{-1} & \\ 0 & & & \end{matrix} & \begin{matrix} & & & \\ & & 0 & \\ & & & \end{matrix} \\ \hline \begin{matrix} & & & \\ & & 0 & \\ & & & \end{matrix} & \begin{matrix} c(n)-d(n) & 0 & \dots & 0 \\ 0 & & & \\ \vdots & & E'(C_0'(n)-D_0'(n))E'^{-1} & \\ 0 & & & \end{matrix} \end{array}\right)$$

$= B_0'(n)$ *(say).* $B_0'(n) = B_0'(n; p^2, M)$ *is a diagonal matrix for all* n *with* $(n, N) = 1$.

PROOF: The first statement follows from Lemma 5.24 and matrix multiplication. The second follows from the definition of E'.

As in Atkin and Lehner [1] we define an operator R_p (twisting by the quadratic character $\left(\frac{-}{p}\right)$) acting on modular forms by: if $f(\tau) = \Sigma\, a(n) \exp(n\tau)$, then $f \mid R_p(\tau) = \sum \left(\frac{n}{p}\right) a(n) \exp(n\tau)$. Here $\left(\frac{n}{p}\right)$ is the Legendre Symbol. Then we have

THEOREM 5.31: *Fix an odd prime* p, *a positive integer* M *prime to* p

and a positive even integer s. Let $N = p^2M$. In the notation of Lemma 5.29 let

$$\sum_{n=0}^{\infty} B'_s(n; p^2, M)\exp(n\tau) = \left(\begin{array}{c|c} f_1(\tau) \quad * & \\ * \;\ddots & 0 \\ \quad\ddots\; f_r(\tau) & \\ \hline & g_1(\tau) \quad * \\ 0 & * \;\ddots \\ & \quad\ddots\; g_r(\tau) \end{array}\right)$$

where $r = G(s+1)$ and $G = H(p^2M)/2$. $*$ indicates that we are not interested in any off diagonal entries. Then

(a) *All f_i and g_i are cusp forms of weight $2+s$ on $\Gamma_0(N)$.*

(b) *All f_i and g_i are eigen forms for all the Hecke Operators $T_{2+s}(n)$ with $(n, N) = 1$.*

(c) *All non-zero f_i and g_i are normalized so that their first (not zeroth) Fourier coefficient is 1. If $p > 3$ or M is divisible by 2 or a prime $\equiv 2 \pmod 3$, then all f_i and g_i are non-zero.*

(d) *If $p \equiv 1(4)$, then $g_i = f_i \mid R_p$ for all $i = 1, \ldots, r$.*

(e) *If $p \equiv 3(4)$, let $g_i - f_i \mid R_p = \Sigma_{n=1}^{\infty} a(n)\exp(n\tau)$. Then $a(n) = 0$ if $p \nmid n$.*

(f) *The off diagonal entries, if any, can have non-zero nth Fourier coefficients only for n with $(n, N) > 1$.*

REMARK 5.32: It is possible to modify the f_i and g_i in Theorem 5.31 so that in addition to satisfying all the above properties, they are also eigen forms for the $\tilde{W}_p$ and $\tilde{W}_q$, $q \mid M$ operators. See Proposition 9.9 below. We will determine the subspace of the space of cusp forms $S_{s+2}(N)$ of weight $s+2$ on $\Gamma_0(N)$ spanned by $\{f_1, \ldots, f_r, g_1, \ldots, g_r\}$ in section 8 below.

PROOF OF THEOREM 5.31:

(a): This follows from Proposition 5.19 and the definition of the $B'_s(n)$ in Lemma 5.29.

(b): This follows from the Proposition on p. 138 of [3] which states that for $(n, N) = 1$, $B_s(n)$ gives the action of the Hecke Operator $T_{s+2}(n)$ on the entries of the matrix series $\Sigma_{m=0}^{\infty} B_s(m)\exp(m\tau)$. So $B'_s(n)$ gives the action of $T_{s+2}(n)$ on the entries of the matrix series $\Sigma_{m=0}^{\infty} B'_s(m)\exp(m\tau)$. By Lemma 5.29, $B'_s(n)$ is a diagonal matrix, so the f_i and g_i are eigen forms.

(c): $B'(1)$ gives the action of the identity operator $T_{s+2}(1)$, so if $f_i \neq 0$, $T_{s+2}(1)f_i = f_i$ and the corresponding entry of $B'_s(1)$ must be 1, i.e. the first Fourier coefficient of f_i must be 1 and similarly for the g_i. Now assume $p > 3$ or M is divisible by 2 or by a prime $\equiv 2 \pmod 3$. Then by Proposition 5.12, the only units in any order of level p^2M are ± 1. Consider the Brandt Matrix $B_s(1; p^2, M)$. A left ideal I of some order $\mathcal{M}$ of level p^2M contains an element α with $N(\alpha) = N(I)$ if and only if I is in the same class as $\mathcal{M}$ (this is easy, see e.g. Corollary 1.20 of [15]). Thus letting $B_s(1; p^2, M) = (b^s_{ij}(1))$ as in (4.2) we see that the only possible non-zero blocks are the diagonal blocks $b^s_{ii}(1)$. By (4.1) and the above $b^s_{ii}(1) = \frac{1}{2}(X^t_s(1) + X^t_s(-1))$. Now $X_s(1)$ is the identity matrix and so is $X_s(-1)$ since s is even. Thus all $b^s_{ii}(1)$ are identity matrices and so is $B_s(1; p^2, M)$ and hence also $B'_s(1; p^2, M)$. Thus the first Fourier coefficient of all f_i and g_i is 1, in particular they are all non-zero.

(d): If $p \equiv 1 \pmod 4$, it follows from Proposition 5.16 and Theorem 5.18 that $(C_s(n) - \epsilon^t D_s(n)) = \left(\frac{n}{p}\right)(C_s(n) + \epsilon^t D_s(n))$ for all $n \geq 0$ and so $g_i = f_i \mid R_p$ for all i.

(e): If $p \equiv 3 \pmod 4$, we know only (by Theorem 5.18) that $(C_s(n) - \epsilon^t D_s(n)) = \left(\frac{n}{p}\right)(C_s(n) + \epsilon^t D_s(n))$ for all n with $p \nmid n$ and thus we obtain a weaker version of (d).

(f): $B'_s(n)$ is a diagonal matrix for all n with $(n, N) = 1$.

REMARK 5.33: If $p = 3$ and M is not divisible by 2 nor by a prime $\equiv 2 \pmod 3$, then by Proposition 5.12 the unit group of $\mathcal{O}_i = I_i^{-1} I_i$ is either ± 1 or is isomorphic to the cyclic group of 6th roots of unity. If $U(\mathcal{O}_i) = \pm 1$, then as in the proof of part (c) above, the corresponding block $b^s_{ii}(1)$ of $B_s(1)$ always diagonalizes (in fact is) the identity matrix. If $|U(\mathcal{O}_i)| = 6$, then since a unit of order six of $\mathcal{O}_i$ is not in the center of $\mathfrak{A}$, its eigen values when represented as an element of $GL(2, \mathbb{C})$ are ξ and ξ^5 where ξ is a primitive 6th root of unity. Now diagonalizing $X_s\begin{pmatrix} \xi & 0 \\ 0 & \xi^5 \end{pmatrix}$, we obtain a matrix whose diagonal entries are $\xi^{s-j}\xi^{5j} = \xi^{s+4j}$ for $j = 0, \ldots, s$. Recall that s is an even positive integer. Now $\Sigma_{k=1}^6 (\xi^{s+4j})^k = \begin{cases} 6 & \text{if } s + 4j \equiv 0 \pmod 6 \\ 0 & \text{otherwise} \end{cases}$ so $1/6\ \Sigma_{k=1}^6 (\xi^{s+4j})^k = \begin{cases} 1 & \text{if } j \equiv s/2 \pmod 3 \\ 0 & \text{otherwise} \end{cases}$. Thus if u is a unit of order 6 of $\mathcal{O}_i$, the $s+1$ by $s+1$ matrix $b_{ii}(1) = 1/6\ \Sigma_{k=1}^6 X^t_s(u^k)$ diagonalizes to a matrix with $2\left[\frac{s}{6}\right] + 1$ ones on the diagonal and all other entries zero.

Hence if precisely μ of the orders $\mathcal{O}_i$, $i = 1, \ldots, G$ have $|U(\mathcal{O}_i)| = 6$, then the $H(s+1)$ by $H(s+1)$ diagonal matrix $B'_s(1)$, which acts as the identity matrix on $f_1, \ldots, f_G, g_1, \ldots, g_G$ has $2\mu\left(s - 2\left[\frac{s}{6}\right]\right)$ zeros on its diagonal and the remaining diagonal entries are 1's. Hence $2\mu\left(s - 2\left[\frac{s}{6}\right]\right)$ of the $f_1, \ldots, f_G, g_1, \ldots, g_G$ are identically zero. Knowing the dimension of $S_4(p^2M)$, Theorem 8.2 below allows us to calculate μ.

Now we give the analogue of Theorem 5.31 for the case of forms of weight 2, i.e. $s = 0$.

THEOREM 5.34: *Fix an odd prime p and a positive integer M prime to p. Let* $N = p^2M$. *In the notation of Lemma* 5.30 *let*

$$\sum_{n=0}^{\infty} B'_0(n; p^2, M) = \left(\begin{array}{c|c} \begin{matrix} f_1(\tau) & * \\ * & \ddots \\ & f_G(\tau) \end{matrix} & 0 \\ \hline 0 & \begin{matrix} g_1(\tau) & * \\ * & \ddots \\ & g_G(\tau) \end{matrix} \end{array}\right)$$

where $G = \frac{1}{2}H(p^2M)$. $*$ *indicates that we are not interested in any off diagonal entries. Then*

(a) *All* f_i *and* g_i *are modular forms of weight* 2 *on* $\Gamma_0(N)$.
(b) f_1 *is the transform of the zeta function of orders of level* p^2M *of* $\mathfrak{A}$. *It is not a cusp form.* g_1 *is a non-cusp form which is linearly independent from* f_1.
(c) $f_2, \ldots, f_G, g_2, \ldots, g_G$ *are all cusp forms.*
(d) *All* f_i *and* g_i *are eigen forms for all the Hecke Operators* $T_2(n)$, $(n, N) = 1$.
(e) *All* f_i *and* g_i *are normalized so that their first (not zeroth) Fourier coefficient is* 1.
(f) *If* $p \equiv 1 \pmod 4$, *then* $g_i = f_i \mid R_p$ *for all* $i = 1, \ldots, G$.
(g) *If* $p \equiv 3 \pmod 4$, *let* $g_i - f_i \mid R_p = \Sigma_{n=0}^{\infty} a(n) \exp(n\tau)$. *Then* $a(n) = 0$ *if* $p \nmid n$.
(h) *The off diagonal entries, if any, can have non-zero* nth *Fourier coefficients only for* n *with* $(n, N) > 1$.

REMARK 5.35: The content of Remark 5.32 also applies to the f_i and g_i in Theorem 5.34.

PROOF OF THEOREM 5.34:

(a): This follows from Proposition 5.19.

(b): $f_1(\tau) = \sum_{n=0}^{\infty} (c(n) + d(n)) \exp(n\tau)$ is by definition the transform of the zeta function. Its zeroth Fourier coefficient $c(0) + d(0)$ is the mass for orders of level p^2M and is clearly non-zero – an explicit formula for the mass is given by Theorem 3.4 above. Thus $f_1(\tau)$ is not a cusp form. By part (f) or (g) of the present theorem, the nth Fourier coefficient of $g_1(\tau)$ is $\left(\frac{n}{p}\right)$ times the nth Fourier coefficient of $f_1(\tau)$ for all n with $p \nmid n$. Hence the Fourier coefficients of $g_1(\tau)$ are too large for it to be a cusp form. The zeroth Fourier coefficient of $g_1(\tau)$ is $c(0) - d(0)$ which is zero by Lemma 5.23, so $g_1(\tau)$ is linearly independent from $f_1(\tau)$.

(c): This follows from Proposition 5.27.

(d): This is the same as the proof of part (b) of Theorem 5.31 above.

(e): As in the proof of part (c) of Theorem 5.31 $B_0(1)$ must be a diagonal matrix. The entry $b_{ii}(1)$ is just $1/e_i$ times the number of units of $\mathcal{O}_i$, i.e. $b_{ii}(1) = 1$ always, so $B_0(1)$ is the identity matrix.

(f): If $p \equiv 1 \pmod 4$, it follows from Remark 5.25 that $(C_0'(n) - D_0'(n)) = \left(\frac{n}{p}\right)(C_0'(n) + D_0'(n))$ for all n and so $g_i = f_i \mid R_p$ for all $i = 1, \ldots, G$.

(g): If $p \equiv 3 \pmod 4$, we know only (by Remark 5.25) that $(C_0'(n) - D_0'(n)) = \left(\frac{n}{p}\right)(C_0'(n) + D_0'(n))$ for all n with $p \nmid n$ and thus we obtain a weaker version of (*f*).

(h): The $B_0'(n; p^2, M)$ are diagonal matrices for $(n, N) = 1$.

6. The trace of the Hecke Operators and the Brandt Matrices

We now know how to construct some cusp forms on $\Gamma_0(N)$, $N = p^2M$. The main question now becomes: what cusp forms have we in fact constructed? The answer is given in section 8 and is a consequence of a certain trace identity (see section 7) involving the traces of the Hecke Operators and the traces of the Brandt Matrices. In this section we reproduce the needed trace formulas. First we introduce some notation.

Let $S_k(N, \chi)$ denote the space of cusp forms of weight k with character χ on $\Gamma_0(N)$. χ is a character on $(Z/N)^x$. We will write $S_k(N) = S_k(N, \chi)$ if χ is the trivial character. We denote by $\mathrm{tr}_{N,\chi} T_k(n)$ the trace of the Hecke Operator $T(n)$ acting on the space $S_k(N, \chi)$. Again we write $\mathrm{tr}_N T_k(n)$ if χ is trivial.

Hijikata in [5] has computed the traces of the Hecke Operators in a quite general setting. We copy here the case of his Theorem (see [5], p. 57) which we require.

THEOREM 6.1: (*Hijikata*): *Let k be an even integer ≥ 2. Let χ be an even character* mod N *with* $\chi(n) = \prod_{\ell|N} \chi_\ell(n)$ *where χ_ℓ is a character* mod ℓ^r, $r = \mathrm{ord}_\ell(N)$. *Then for* $(n, N) = 1$ *we have*

$$\mathrm{tr}_{N,\chi} T_k(n) = -\Sigma_s\, a(s)\, \Sigma_f\, b(s,f)\, \prod_{\ell|N} c'(s,f,\ell)$$

$$+ \delta(\chi)\deg T_k(n) + \delta(\sqrt{n})\frac{k-1}{12} N \prod_{\ell|N}(1+1/\ell) \prod_{\ell|N} \chi_\ell(\sqrt{n})$$

where $\delta(\chi) = \begin{cases} 1 & \text{if } k = 2 \text{ and } \chi \text{ is trivial} \\ 0 & \text{otherwise} \end{cases}$

and $\delta(\sqrt{n}) = \begin{cases} n^{k/2-1} & \text{if } n \text{ is a perfect square} \\ 0 & \text{otherwise} \end{cases}$

The meaning of s, $a(s)$, f, $b(s,f)$ and $c'(s,f,\ell)$ are given as follows:

Let s run over all integers such that $s^2 - 4n$ is not a positive non-square. Hence by some *positive* integer t and *square free negative* integer m, $s^2 - 4n$ has one of the following forms which we classify into the cases (p), (h), (e1), or (e23) as follows:

$$s^2 - 4n = \begin{cases} 0 & & \ldots.(\mathrm{p}) \\ t^2 & & \ldots.(\mathrm{h}) \\ t^2 m & 0 > m \equiv 1 \pmod 4 & \ldots.(\mathrm{e1}) \\ t^2 4m & 0 > m \equiv 2,3 \pmod 4 & \ldots.(\mathrm{e23}) \end{cases} \Big\}(\mathrm{e})$$

Let $\Phi(X) = \Phi_s(X) = X^2 - sX + n$ and let x and y be the roots in $\mathbb{C}$ of $\Phi(X) = 0$. Corresponding to the classification of s put

$$a(s) = \begin{cases} |x| n^{k/2-1}(4N)^{-1} & \ldots.(\mathrm{p}) \\ (\mathrm{Min}\{|x|,|y|\})^{k-1}|x-y|^{-1} & \ldots.(\mathrm{h}) \\ 1/2(x^{k-1} - y^{k-1})/(x-y) & \ldots.(\mathrm{e}) \end{cases}$$

For each fixed s, corresponding to its classification, let f run over the following set

$$f = \begin{cases} 1, 2, \ldots, N & \ldots.(p) \\ \text{all positive divisors of } t & \ldots.(\mathrm{h}) \text{ and } (\mathrm{e}) \end{cases}$$

$$\text{and let } b(s,f)=\begin{cases}1 & \dots\text{(p)}\\ 1/2\varphi((s^2-4n)^{1/2}/f) & \dots\text{(h)}\\ h(s^2-4n/f^2)/\omega(s^2-4n/f^2) & \dots\text{(e)}\end{cases}$$

where φ is Euler's function, $h(d)$ (resp. $\omega(d)$) denotes the class number of locally principal ideals (resp. 1/2 the cardinality of the unit group) of the order of $Q(\sqrt{d})$ with discriminant d.

For a pair (s,f) fixed and a prime divisor ℓ of N, let $\nu=\operatorname{ord}_\ell(N)$, $\rho=\operatorname{ord}_\ell(f)$ and put $\tilde{A}=\{x\in Z \mid \Phi(x)\equiv 0 \pmod{\ell^{\nu+2\rho}},\ 2x\equiv s \pmod{\ell^\rho}\}$ and $\tilde{B}=\{x\in\tilde{A}\mid \Phi(x)\equiv 0 \pmod{\ell^{\nu+2\rho+1}}\}$. Let $A=A(s,f,\ell)$ (resp. $B=B(s,f,\ell)$) be a complete set of representatives of $\tilde{A}$ (resp. $\tilde{B}$) mod $\ell^{\nu+\rho}$. Put

$$\text{Put } c'(s,f,\ell)=\begin{cases}\sum_x \chi_\ell(x) & \text{if } s^2-4n/f^2\not\equiv 0 \pmod{\ell}\\ \sum_x \chi_\ell(x)+\sum_y \chi_\ell(y) & \text{if } s^2-4n/f^2\equiv 0 \pmod{\ell}\end{cases}$$

where x runs over all elements of $A(s,f,\ell)$ and y runs over all $s-z$, $z\in B(s,f,\ell)$.

REMARK 6.2: Our $T_k(n)$ differ from Hijikata's by a factor of $n^{k/2-1}$.

PROPOSITION 6.3: *Let* $\mathcal{O}_\ell=\begin{pmatrix}Z_\ell & Z_\ell\\ NZ_\ell & Z_\ell\end{pmatrix}$ *and keep the notation of Theorem* 6.1 *above. Assume* χ_ℓ *is the trivial character. Then the corresponding* $c'(s,f,\ell)$ *is just the number of inequivalent* mod $U(\mathcal{O}_\ell)$ *optimal embeddings of an order of discriminant* s^2-4n/f^2 *into* $\mathcal{O}_\ell$.

PROOF: See section 2 of Hijikata [5].

For p an odd prime and χ_p the trivial character, it will be convenient to tabulate the corresponding $c'(s,f,p)$. We write $c'_\mu(s,f,p)_\mu$ to denote $c'(s,f,p)$ in the case χ_p is trivial and we are considering the group $\Gamma_0(N)$ with $\mu=\operatorname{ord}_p(N)$. Then using Hijikata's Theorem 6.1 (or the tables on pp. 692–693 of [13]), we obtain the following tables.

Let p be an odd prime. Let u be a quadratic non-residue mod p. Set $\Delta=s^2-4n/f^2 \bmod U(Z_p)^2$. Then the values of $c'_\mu(s,f,p)_\mu$ for $\mu=1$ and 2 are given by the tables on the next page.

The trace formula for the Hecke operator $T_k(n)$ given by Theorem 6.1 is very similar to the trace formula for the Brandt matrix $B_{k-2}(n)$ given by Theorem 4.12. In fact the notation used in both theorems is identical. The difference between $c(s,f,\ell)$ and $c'(s,f,\ell)$ is explained in Remark 6.4.

$\Delta = p^{2m}$

	$m=0$	$m=1$	$m>1$
$c'_1(s,f,p)_1$	2	2	2
$c'_1(s,f,p)_2$	2	$p+2$	$p+1$

$\Delta = p^{2m}u$

	$m=0$	$m=1$	$m>1$
$c'_1(s,f,p)_1$	0	2	2
$c'_1(s,f,p)_2$	0	p	$p+1$

$\Delta = p^{2m+1}a$ where $a = 1$ or u

	$m=0$	$m=1$	$m>1$
$c'_1(s,f,p)_1$	1	2	2
$c'_1(s,f,p)_2$	0	$p+1$	$p+1$

REMARK 6.4: Let $\mathcal{O}$ be an order of level p^2M. Then according to Theorem 4.12, $c(s,f,\ell)$ is the number of inequivalent mod $U(\mathcal{O}_\ell)$ optimal embeddings of an order of discriminant s^2-4n/f^2 into $\mathcal{O}_\ell$. But for $\ell \neq p$, $\mathcal{O}_\ell \cong \begin{pmatrix} Z_\ell & Z_\ell \\ NZ_\ell & Z_\ell \end{pmatrix}$ by definition where $N = p^2M$. Thus letting $\mu = \mathrm{ord}_\ell(N)$ we have $c(s,f,\ell) = c'_1(s,f,\ell)_\mu$ if $\ell \neq p$ by Proposition 6.3. If $\ell = p$, the value of $c(s,f,p)$ is given by Theorem 2.7. We tabulate those values here.

Let p be an odd prime. Let u be a quadratic non-residue mod p. Set $\Delta = s^2-4n/f^2$ mod $U(Z_p)^2$. Then the value of the $c(s,f,p)$ appearing in Theorem 4.12 is given by the table

$$c(s,f,p) = \begin{cases} p+1 & \text{if } \Delta = p \text{ or } pu \\ 2 & \text{if } \Delta = p^2u \\ 0 & \text{otherwise} \end{cases}$$

7. The Trace Identity

We are now able to state the important

THEOREM 7.1 (*The Trace Identity*): *Let p be an odd prime and let M be a positive integer prime to p. Let $N = p^2M$ and let k be an even integer ≥ 2. Then for all $n > 0$, $(n, N) = 1$ we have*

$$\begin{aligned} &2\mathrm{tr}_{p^2M} T_k(n) - 2\mathrm{tr}_{pM} T_k(n) - \mathrm{tr} B_{k-2}(n; p^2, M) \\ &+ \begin{cases} \left(1 + \left(\frac{n}{p}\right)\right) \deg T_2(n) & \text{if } k = 2 \\ 0 & \text{if } k > 2 \end{cases} \\ &= \sum_{\psi} \bar{\psi}(n) \, \mathrm{tr}_{pM,\psi^2} T_k(n) \end{aligned} \tag{7.1}$$

where the sum is over all the $p-1$ characters ψ of $(Z/p)^x$.

REMARK 7.2: Note that in the sum we are taking the trace of $T_k(n)$ on $S_k(pM, \psi^2)$ and since ψ^2 is an even character, $S_k(pM, \psi^2)$ is (in general) non zero. Also note that $\psi^2(\bar{\psi})^2$ is the trivial character, so that if $f(\tau) = \Sigma_{n=1}^{\infty} a(n) \exp(n\tau)$ is in $S_k(pM, \psi^2)$, then $g(\tau) = \Sigma_{n=1}^{\infty} \bar{\psi}(n) a(n) \exp(n\tau)$ is in $S_k(p^2M)$ (see [17], Proposition 3.64).

PROOF OF THEOREM 7.1: The above formulas for $\mathrm{tr}_{p^2M} T_k(n)$, $\mathrm{tr}_{pM} T_k(n)$, $\mathrm{tr} B_{k-2}(n; p^2, M)$, and $\mathrm{tr}_{pM,\psi^2} T_k(n)$ all involve summations over the same index set. We will show that the equality (7.1) holds almost term by term. For simplicity we write $M = \Pi_{\ell \mid M} \ell^{\nu}$.

First consider the deg $T_k(n)$ terms. These do not occur in $\mathrm{tr} B_{k-2}(n)$ and occur in $\mathrm{tr}_{R,\chi} T_k(n)$ only if $k = 2$ and χ is the trivial character. Hence the contribution of the deg $T_2(n)$ terms to the L.H.S. (left hand side) of (7.1) is $2 \deg T_2(n) - 2 \deg T_2(n) + \left(1 + \left(\frac{n}{p}\right)\right) \deg T_2(n)$. Since ψ^2 is trivial if and only if ψ is trivial or $\psi = \left(\frac{-}{p}\right)$, the contribution of the deg $T_2(n)$ terms to the R.H.S. (right hand side) of (7.1) is also $\left(1 + \left(\frac{n}{p}\right)\right) \deg T_2(n)$.

Next we consider the 'mass' terms, i.e. those with $\delta(\sqrt{n})$. They occur only if n is a perfect square. Their contribution to the L.H.S. of (7.1) is

$$2\frac{k-1}{12}M\prod_{\ell\mid M}(1+1/\ell)\cdot p^2(1+1/p)-2\frac{k-1}{12}M\prod_{\ell\mid M}(1+1/\ell)\cdot p(1+1/p)$$
$$-\frac{k-1}{12}M\prod_{\ell\mid M}(1+1/\ell)\cdot(p^2-1)=\frac{k-1}{12}M\prod_{\ell\mid M}(1+1/\ell)\cdot(p^2-1)$$

while the contribution to the R.H.S. of (7.1) is

$$\sum_{\psi}\bar{\psi}(n)\frac{k-1}{12}M\prod_{\ell\mid M}(1+1/\ell)\cdot p(1+1/p)\psi^2(\sqrt{n})$$
$$=\frac{k-1}{12}M\prod_{\ell\mid M}(1+1/\ell)\cdot(p+1)\sum_{\psi}\bar{\psi}(n)\psi(n)$$
$$=\frac{k-1}{12}M\prod_{\ell\mid M}(1+1/\ell)\cdot(p^2-1)$$

Next we consider the case where s is fixed and $s^2-4n=0$. Then $\Phi(X)=(X-s/2)^2$. The contribution to $2\mathrm{tr}_{p^2M}T_k(n)$ is

$$2\left[-\left|\frac{s}{2}\right|n^{k/2-1}\frac{1}{4p^2M}\sum_{f=1}^{p^2M}\prod_{\ell\mid Mp}c'(s,f,\ell)\right]$$
$$=-2\left[\left|\frac{s}{2}\right|n^{k/2-1}\left(\frac{1}{4}\right)\prod_{\ell\mid M}c_1'(s,f,\ell)_\nu\cdot(p+1)\right]$$

since in this case $c'(s,f,\ell)$ is independent of f. The contribution to $-2\mathrm{tr}_{pM}T_k(n)$ is

$$-2\left[-\left|\frac{s}{2}\right|n^{k/2-1}\left(\frac{1}{4pM}\right)\sum_{f=1}^{pM}\prod_{\ell\mid pM}c'(s,f,\ell)\right]$$
$$=2\left[\left|\frac{s}{2}\right|n^{k/2-1}\left(\frac{1}{4}\right)\prod_{\ell\mid M}c_1'(s,f,\ell)_\nu\cdot 2\right].$$

The contribution to $\mathrm{tr}B_{k-2}(n)$ is zero (since $\Delta=0$), so the total contribution to the L.H.S. of (7.1) is $-\frac{|s|}{4}n^{k/2-1}\prod_{\ell\mid M}c_1'(s,f,\ell)_\nu\cdot(p-1)$. The contribution to $\mathrm{tr}_{pM,\psi^2}T_k(n)$ is

$$-\frac{|s|}{2}n^{k/2-1}\frac{1}{4pM}\sum_{f=1}^{pM}\prod_{\ell\mid Mp}c'(s,f,\ell)$$
$$=-\frac{|s|}{2}n^{k/2-1}\left(\frac{1}{4}\right)\prod_{\ell\mid M}c_1'(s,f,\ell)_\nu\cdot 2\psi^2(s/2)$$

since again in this case $c'(s, f, \ell)$ is independent of f. Thus the total contribution to the R.H.S of (7.1) is

$$\left(-\frac{|s|}{4} n^{k/2-1} \prod_{\ell \mid M} c'(s, f, \ell)_\nu\right) \sum_{\psi} \psi^2(s/2)\bar{\psi}(n)$$
$$= -\frac{|s|}{4} n^{k/2-1} \prod_{\ell \mid M} c'_1(s, f, \ell)_\nu \cdot (p-1) \text{ since } n = (s/2)^2.$$

Now we consider the remaining terms, those classified into the cases (h) and (e). Note that for these terms, once we fix s and f, the $a(s)$ and $b(s, f)$ are independent of which particular trace formulas they occur in. Note also that in case (h), $\Delta = s^2 - 4n/f^2$ is a square, so $c(s, f, p) = 0$ always (by the table in section 6), and it does not matter that we have not written down the contribution of the (h) terms in the formula for $\mathrm{tr}B_{k-2}(n; p^2M)$ in Theorem 4.12 – they always contribute nothing. Similarly by Remark 6.4, $c'(s, f, \ell) = c(s, f, \ell) = c'_1(s, f, \ell)_\nu$ for all primes ℓ which divide M and hence these are also independent of which particular trace formula they occur in. Thus if we fix s and f, to show that the corresponding contribution to the L.H.S. and R.H.S. of (7.1) are equal, we need only prove that

$$2c'_1(s, f, p)_2 - 2c'_1(s, f, p)_1 + c(s, f, p)$$
$$= \sum_{\psi} \bar{\psi}(n) c'(s, f, p)_{\psi^2} \tag{7.2}$$

where the $c'_1(s, f, p)_i$, $i = 1$ or 2 and $c(s, f, p)$ have been defined above and we write $c'(s, f, p)_{\psi^2}$ to denote the $c'(s, f, p)$ occuring in the formula for $\mathrm{tr}_{pM,\psi^2} T_k(n)$. In fact with the exception of the last case below, this is exactly what we will do. We shorten $c'_1(s, f, p)_2$ to c'_2, $c'_1(s, f, p)_1$ to c'_1, $c(s, f, p)$ to c and $c'(s, f, p)_{\psi^2}$ to c'_{ψ^2}.

Case (1): $s^2 - 4n = w$ is a non-residue mod p. Then $\Phi(X) = (X - s/2)^2 - \dfrac{s^2 - 4n}{4}$ has no solution mod p. Hence for any f, c'_2, c'_1, c, and c'_{ψ^2} are all zero so (7.2) holds.

Case (2): $s^2 - 4n \equiv d^2 \pmod{p}$ where d is a unit mod p. Then any f must be a unit mod p. Fix one. From the tables in section 6 we find that $c'_2 = 2$, $c'_1 = 2$, and $c = 0$. Hence the contribution to the L.H.S. of (7.2) is zero. $4\Phi(X) = 4(X^2 - sX + n) \equiv (2X - s)^2 - d^2 \pmod{p}$ has roots $\dfrac{s \pm d}{2} \bmod p$. Thus by Theorem 6.1, $c'_{\psi^2} = \psi^2\left(\dfrac{s+d}{2}\right) + \psi^2\left(\dfrac{s-d}{2}\right)$. Letting $a = \dfrac{s+d}{2}$ and $b = \dfrac{s-d}{2}$, $ab = \dfrac{s^2 - d^2}{4} \equiv n \pmod{p}$ and the

contribution to the R.H.S. of (7.2) is

$$\sum_{\psi} \bar{\psi}(ab)(\psi^2(a)+\psi^2(b)) = \sum_{\psi} (\psi(ab^{-1})+\psi(a^{-1}b)) = 0.$$

Case (3): $p \mid s^2-4n/f^2$ but $p^2 \nmid s^2-4n/f^2$. From the tables we find $c_2'=0$, $c_1'=1$, and $c=p+1$. Hence the contribution to the L.H.S. of (7.2) is $p-1$. $2\Phi(X)=(2X-s)^2-(s^2-4n)\equiv 0$ has only the solution $s/2 \bmod p^{1+2\rho}$ and no solution $\bmod p^{2+2\rho}$ where $\rho=\mathrm{ord}_p(f)$. Hence $c'_{\psi^2}=\psi^2(s/2)$ and the contribution to the R.H.S. of (7.2) is $\Sigma_\psi \bar{\psi}(n)\psi^2(s/2)=\Sigma_\psi \bar{\psi}(n)\psi(n)=p-1$.

Case (4): $(s^2-4n)/f^2=p^r a$ where a is a unit $\bmod p$ and $r\geq 3$. From the tables we find $c_2'=p+1$, $c_1'=2$, and $c=0$. Hence the contribution to the L.H.S of (7.2) is $2(p-1)$. We also find that in Theorem 6.1, $A(s,f,p)=\{s/2\}$ and $B(s,f,p)=\{s/2\}$, so $c'_{\psi^2}=2\psi^2(s/2)$. Thus the contribution to the R.H.S. of (7.2) is $\Sigma_\psi \bar{\psi}(n)2\psi^2(s/2)=2(p-1)$.

Case (5): $(s^2-4n)/f^2=p^2 d$ where d is a non-residue $\bmod p$. From the tables we find $c_2'=p$, $c_1'=2$, and $c=2$. Hence the contribution to the L.H.S. of (7.2) is $2(p-1)$. Again we find $A(s,f,p)=\{s/2\}$ and $B(s,f,p)=\{s/2\}$, so $c'_{\psi^2}=2\psi^2(s/2)$ and the contribution to the R.H.S. of (7.2) is $\Sigma_\psi \bar{\psi}(n)2\psi^2(s/2)=2(p-1)$.

Case (6): $p \mid (s^2-4n)$ and $(s^2-4n)/f^2=w$ is a non-residue $\bmod p$. From the tables we find $c_2'=c_1'=c=0$, so the contribution to the L.H.S. of (7.2) is zero. But $\Phi(X)\equiv 0 \pmod{p^{1+2\rho}}$, $\rho=\mathrm{ord}_p(f)$ has no solutions, so the contribution to the R.H.S. of (7.2) is also zero.

Case (7): The only cases remaining to be checked are (i) $(s^2-4n)/f^2=p^2d^2$ for some unit $d \bmod p$ and (ii) $p \mid (s^2-4n)$ and $(s^2-4n)/f^2=d^2$ for some unit $d \bmod p$. These two cases always occur in pairs, so we consider at the same time the pair of cases: $(s^2-4n)/f^2=p^2d^2$ and $(s^2-4n)/(pf)^2=d^2$ for some unit $d \bmod p$. Since $c_1'(s,pf,\ell)_\nu=c_1'(s,f,\ell)_\nu$ for all primes $\ell\neq p$, in order to show that these cases give the same contribution to the L.H.S. and R.H.S. of (7.1) it suffices to prove that

$$\begin{aligned} &2(b(s,pf)c_1'(s,pf,p)_2+b(s,f)c_1'(s,f,p)_2)\\ &-2(b(s,pf)c_1'(s,pf,p)_1+b(s,f)c_1'(s,f,p)_1)\\ &+b(s,pf)c(s,pf,p)+b(s,f)c(s,f,p)\\ =&\sum_{\psi} \bar{\psi}(n)(b(s,pf)c'_{\psi^2}(s,pf,p)+b(s,f)c'_{\psi^2}(s,f,p)). \end{aligned} \tag{7.3}$$

From the tables we find $c_1'(s,pf,p)_2=2$, $c_1'(s,f,p)_2=p+2$, $c_1'(s,pf,p)_1=2$, $c_1'(s,f,p)_1=2$ and $c(s,pf,p)=c(s,f,p)=0$. Hence

the L.H.S. of (7.3) is $2pb(s, f)$. On the other hand it is easy to see that $c'_{\psi^2}(s, pf, p) = c'_{\psi^2}(s, f, p) = 2\psi^2(s/2)$, so that the right hand side of (7.3) is

$$\sum_{\psi} \bar{\psi}(n)2\psi^2(s/2)(b(s, pf) + b(s, f)) = 2(p-1)(b(s, pf) + b(s, f)).$$

Thus to show equality in (7.3) we must prove that

$$b(s, f) = (p-1)b(s, pf) \tag{7.4}$$

We must consider two cases: if $s^2 - 4n = t^2$ is a perfect square, then $b(s, f) = 1/2\varphi(t/f)$ and $b(s, pf) = 1/2\varphi(t/pf)$.
But $\left(p, \frac{t}{pf}\right) = 1$ assumption, so $b(s, f) = 1/2\varphi(t/f) = 1/2\varphi((p)(t/pf)) = 1/2(p-1)\varphi(t/pf) = (p-1)b(s, pf)$ which establishes the equality in (7.4). If $s^2 - 4n$ is not a perfect square, then $b(s, f) = h(\mathcal{O}_1)/w(\mathcal{O}_1)$ and $b(s, pf) = h(\mathcal{O}_2)/w(\mathcal{O}_2)$ where $\mathcal{O}_2$ is the order in the imaginary quadratic number field $Q(\sqrt{s^2 - 4n})$ with $\mathrm{disc}(\mathcal{O}_2) = (s^2 - 4n)/p^2f^2$ and $\mathcal{O}_1$ is the unique suborder of $\mathcal{O}_2$ of index p. But then by Lemma 4.16

$$\frac{h(\mathcal{O}_1)}{w(\mathcal{O}_1)} = p\left(1 - \left\{\frac{\Delta}{p}\right\}\frac{1}{p}\right)\frac{h(\mathcal{O}_2)}{w(\mathcal{O}_2)} \text{ where } \Delta = s^2 - 4n/p^2f^2 \text{ and}$$

$$\left\{\frac{\Delta}{p}\right\} = \left\{\frac{d^2}{p}\right\} = 1, \text{ so again } b(s, f) = (p-1)b(s, pf).$$

This completes the proof of Theorem 7.1.

8. Representing modular forms by theta series

In this section we determine the subspace of $S_k(p^2M)$ generated by theta series. First if φ is a primitive character of $(Z/sZ)^x$, we denote by R_φ the operator 'twisting by φ', i.e. if $f(\tau) = \Sigma_{n=1}^{\infty} a(n)\exp(n\tau)$, then $f \mid R_\varphi = \Sigma\, \varphi(n)a(n)\exp(n\tau)$. Here $\exp(n\tau) = e^{2\pi i n\tau}$. If $f \in S_k(N, \chi)$, then $f \mid R_\varphi \in S_k(N', \chi\varphi^2)$ where N' is the least common multiple of $N, \mathrm{cond}(\varphi)^2$, and $\mathrm{cond}(\varphi)\,\mathrm{cond}(\chi)$ (see Proposition 3.64 of [17]). Let $S_k^0(N, \chi)$ denote the subspace of $S_k(N, \chi)$ generated by newforms (see [1] and [9a]). We denote by $S_k(N, \chi)^\varphi$ (respectively $S_k^0(N, \chi)^\varphi$) the space $\{f | R_\varphi | f \in S_k(N, \chi)$ (respectively $S_k^0(N, \chi))\}$. Note that $S_k(N, \chi)^\varphi \subseteq S_k(N', \chi\varphi^2)$.

LEMMA 8.1: *Let the notation be as above. Then for* $(m, N') = 1$ *the trace of* $T(m)$ *on* $S_k^0(N, \chi)^\varphi$ *considered as a subspace of* $S_k(N', \chi\varphi^2)$ *is equal to* $\varphi(m)$ *times the trace of* $T(m)$ *on* $S_k^0(N, \chi)$.

PROOF: Let $x = \exp(\tau)$. If $q(\tau) = \Sigma\, c(n)x^n \in S_k(M, \psi)$, then $q \mid T(m) = \Sigma\, c'(n)x^n$ where $c'(n) = \Sigma_{a \mid (m,n)}\, \psi(a)a^{k-1}c(mn/a^2)$ (see p. 80 of [17] or p. 287 of [9a]). Hence if $f \in S_k^0(N, \chi)$, we have $(f \mid R_\varphi) \mid T(m) = \varphi(m)((f \mid T(m)) \mid R_\varphi)$. Thus if $f = \Sigma\, a(n)x^n$ is a newform in $S_k^0(N, \chi)$ normalized so that $a(1) = 1$ and $(m, N') = 1$, then $(f \mid R_\varphi) \mid T(m) = \varphi(m)((a(m)f) \mid R_\varphi) = a(m)\varphi(m)(f \mid R_\varphi)$. Let $f_1, \ldots, f_t$ be a basis of $S_k^0(N, \chi)$ consisting of normalized newforms. Then $f_1 \mid R_\varphi, \ldots, f_t \mid R_\varphi$ are linearly independent since $f_i \mid R_\varphi \neq 0$ and distinct newforms have different eigenvalues for $T(m)$ for infinitely many m – see Theorem 5 of [9a]. Thus they form a basis of $S_k^0(N, \chi)$ and the lemma follows.

Note that Lemma 8.1 is not necessarily true if we replace S_k^0 by S_k. For example consider $S_k(p)$ and let $\varphi = \left(\frac{-}{p}\right)$. If $f \in S_k(1)$, then $g(\tau) = f(p\tau) \in S_k(p)$, but $g \mid R_\varphi = 0$. Since $S_k(p)$ is generated by newforms and the oldforms $f(\tau)$ and $f(p\tau)$ where f ranges over a basis of eigen forms in $S_k(1)$, we see $\dim S_k(p)^\varphi = \dim S_k(p) - \dim S_k(1) \neq \dim S_k(p)$ in general, so that the Lemma fails for $T(1)$. I wish to thank H. Hijikata for pointing out to me my blindness on this point.

We can now state our main

THEOREM 8.2: *Let* p *be an odd prime and* M *a positive integer prime to* p. *Let* k *be an even integer* ≥ 2. *Let* φ *denote the quadratic character* $\left(\frac{-}{p}\right)$. *If* $k = 2$, *then in the notation of Theorem* 5.34 *we have*

$$2S_2(p^2M) \cong \langle f_2(\tau)\rangle \oplus \ldots \oplus \langle f_G(\tau)\rangle \oplus \langle g_2(\tau)\rangle \oplus \ldots \oplus \langle g_G(\tau)\rangle$$

(8.1)

$$\oplus\, 3S_2(pM) \oplus \sum_{\substack{\psi \\ \psi^2 \neq 1}} S_2(pM, \psi^2)^{\bar{\psi}} \oplus \sum_{a \mid M} \delta(M/a)(S_2^0(pa)^\varphi \oplus 2S_2^0(a)^\varphi)$$

while if $k > 2$, *we have in the notation of Theorem* 5.31

$$2S_k(p^2M) \cong \langle f_1(\tau)\rangle \oplus \ldots \oplus \langle f_r(\tau)\rangle \oplus \langle g_1(\tau)\rangle \oplus \ldots \oplus \langle g_r(\tau)\rangle$$

(8.2)

$$\oplus\, 3S_k(pM) \oplus \sum_{\substack{\psi \\ \psi^2 \neq 1}} S_k(pM, \psi^2)^{\bar{\psi}} \oplus \sum_{a \mid M} \delta(M/a)(S_k^0(pa)^\varphi \oplus 2S_k^0(a)^\varphi)$$

Here the first sum is over all the $p - 3$ *characters* ψ *of* $(Z/pZ)^x$ *with* ψ^2 *non-trivial and the second sum is over all positive divisors of* M. $\delta(M/a)$ *denotes the number of positive divisors of* M/a. *The isomor-*

phisms in (8.1) *and* (8.2) *are as modules for the Hecke Algebra* H *generated by the Hecke Operators* $T_k(n)$ *with* $(n, pM) = 1$ *acting on* $S_k(p^2M)$. *Finally* $2S_k(p^2M) = S_k(p^2M) \oplus S_k(p^2M)$, *etc. and* $\langle f_2(\tau)\rangle$ *e.g. denotes the* 1*-dimensional complex vector space generated by* $f_2(\tau)$. *Also note that* $r = G(k-1)$.

PROOF: First note that by Proposition 3.64 of [17] $S_k(pM, \psi^2)^{\bar\psi}$, $S_k(pa)^\varphi$, and $S_k(a)^\varphi$ are all contained in $S_k(p^2M)$.

As H is a semi-simple ring we need only check (see e.g. Theorem 3, p. 458 of [9]) that the trace of the transformations induced by the $T_k(n)$, $(n, pM) = 1$ on both sides of (8.1) and (8.2) are equal. By the proof of part (d) of Theorem 5.34 (resp. part (b) of Theorem 5.31) the action of $T_k(n)$ for $k = 2$ on $\langle f_2(\tau)\rangle \oplus \ldots \oplus \langle f_G(\tau)\rangle \oplus \langle g_2(\tau)\rangle \oplus \ldots \oplus \langle g_G(\tau)\rangle$ (resp. for $k > 2$ on $\langle f_1(\tau)\rangle \oplus \ldots \oplus \langle f_r(\tau)\rangle \oplus \langle g_1(\tau)\rangle \oplus \ldots \oplus \langle g_r(\tau)\rangle$) is given by the diagonal matrix

$$B_0''(n) = \left(\begin{array}{c|c} E'(C_0'(n) + D_0'(n)E'^{-1} & 0 \\ \hline 0 & E'(C_0'(n) - D_0'(n)E'^{-1} \end{array}\right)$$

(resp. $B_{k-2}'(n; p^2, M)$) where the notation is as in Lemma 5.30 (resp. Lemma 5.29). By Theorem 5 of [1], $S_k(pM) \cong \Sigma_{a \mid M}\, \delta(M/a)(S_k^0(pa) \oplus 2S_k^0(a))$ and it follows from Lemma 8.1 that $\varphi(n)$ times the trace of $T(n)$ on $S_k(pM)$ equals the trace of $T(n)$ on $\Sigma_{a|M}\, \delta(M/a)(S_k^0(pa)^\varphi \oplus 2S_k^0(a)^\varphi)$. It is implicit in [9a], see p. 294, that if $\psi^2 \neq 1$, hence the conductor $\mathrm{cond}(\psi^2) = p$, then $S_k(pM, \psi^2) \cong \Sigma_{a|M}\, \delta(M/a)S_k^0(pa, \psi^2)$ and so by Lemma 8.1 $\bar\psi(n)$ times the trace of $T(n)$ on $S_k(pM, \psi^2)$, $\psi^2 \neq 1$, is equal to the trace of $T(n)$ on $S_k(pM, \psi^2)^{\bar\psi}$. Now for $k > 2$ (7.1) provides exactly the equality of traces that is required to establish (8.2). For $k = 2$, we need to find the trace of $B_0''(n)$. Now Lemma 5.30 and Remark 5.25 imply that $\mathrm{tr}B_0''(n) = \mathrm{tr}B_0(n) - \left(1 + \left(\frac{n}{p}\right)\right)(c(n) + d(n))$. But $c(n) + d(n)$ is the nth Fourier coefficient of the zeta function and we have $c(n) + d(n) = \deg T_2(n)$ for all $(n, pM) = 1$ (since $c(\ell) + d(\ell) = \ell + 1 = \deg T_2(\ell)$ for all primes ℓ, $\ell \nmid pM$ – see Shimura [17], p. 63 and Eichler [3], p. 94). Thus again (7.1) provides exactly the equality of traces that is required to establish (8.1).

REMARK 8.3: In section 10 below we determine explicitly the $f_i(\tau)$ and $g_i(\tau)$ occurring in (8.1) and (8.2) in the case $M = 1$. In general Theorem 8.2 is only strong enough to determine the nth Fourier coefficients of $f_i(\tau)$ and $g_i(\tau)$ for $(n, pM) = 1$.

LEMMA 8.4: $S_k(pM, \psi^2)^{\bar{\psi}} \cong S_k(pM, \bar{\psi}^2)^{\psi}$ as modules for the Hecke Algebra H generated by $T_k(n)$, $(n, pM) = 1$.

PROOF: We let complex conjugation act on modular forms by acting on their Fourier coefficients: if $f(\tau) = \sum_{n=1}^{\infty} a(n) \exp(n\tau)$, then $\bar{f}(\tau) = \sum_{n=1}^{\infty} \overline{a(n)} \exp(n\tau)$ where of course $\bar{a}$ is the complex conjugate of a. Then since $\overline{f(\tau)} = \bar{f}(-\bar{\tau})$, it is easy to see that $f \to \bar{f}$ maps $S_k(pM, \chi)$ onto $S_k(pM, \bar{\chi})$, hence it maps $S_k(pM, \psi^2)^{\bar{\psi}}$ onto $S_k(pM, \bar{\psi}^2)^{\psi}$. As $S_k(pM, \psi^2)$ is invariant under the Hecke operators $T_{k,\psi^2}(n)$, $(n, pM) = 1$, $S_k(pM, \psi^2)^{\bar{\psi}}$ is invariant under the Hecke Operators $T_k(n)$, $(n, pM) = 1$ (of course we have already implicitly used this fact in proving Theorem 8.2). It is now obvious that $f \to \bar{f}$ is an isomorphism of $S_k(pM, \psi^2)^{\bar{\psi}}$ onto $S_k(pM, \bar{\psi}^2)^{\psi}$ as H-modules.

PROPOSITION 8.5: All new forms in $S_k(p^2M)$ that are neither obtained from forms in $S_k(pM, \psi^2)^{\bar{\psi}}$ for ψ a non-trivial character of $(Z/p)^x$ nor from forms is $S_k(M)^{\varphi}$ where φ is the quadratic character $\left(\frac{-}{p}\right)$ occur among the $f_j(\tau)$ and $g_j(\tau)$ of Theorem 8.2 In particular, they all come from theta series.

PROOF: By Theorem 8.2 and Lemma 8.4 we have

$$2S_k(p^2M) \cong \langle f_i(\tau)\rangle \oplus \ldots \langle f_r(\tau)\rangle \oplus \langle g_i(\tau)\rangle \oplus \ldots \oplus \langle g_r(\tau)\rangle$$
$$\oplus 3S_k(pM) \oplus 2 \sum_{\substack{\{\psi\} \\ \psi^2 \neq 1}} S_k(pM, \psi^2)^{\bar{\psi}})$$
$$\oplus \sum_{a \mid M} \delta(M/a)(S_k^0(pa)^{\varphi} \oplus 2S_k^0(a)^{\varphi}) \text{ where}$$

$i = \begin{cases} 2 & \text{if } k = 2 \\ 1 & \text{if } k > 2, \end{cases}$ $r = G(k-1)$, φ is the quadratic character $\left(\frac{-}{p}\right)$ and the sum $\Sigma_{\{\psi\}}$ is over a set of representatives of the pairs $\{\psi, \bar{\psi}\}$, where $\psi^2 \neq 1$. This shows immediately that all new forms in $S_k(p^2M)$ that are not contained in any $S_k(pM, \psi^2)^{\bar{\psi}}$ where $\psi \neq 1$ must occur among the $f_i(\tau)$ or $g_i(\tau)$.

Following Atkin we make the following

DEFINITION 8.6: A new form in $S_k(N)$ is said to be *primitive* if it can not be obtained from a form in $S_k(M, \chi)$, $M < N$ by twisting by a suitable character $(\chi^{-1/2})$.

REMARK 8.7: Note that our usage of the word 'primitive' is different from the recent usage of the word 'primitive' by Serre. By 'primitive', Serre just means a new form.

COROLLARY 8.8: All primitive forms in $S_k(p^2M)$, p odd, $p \nmid M$ are linear combinations of theta series. More precisely, they occur among the $f_j(\tau)$ and $g_j(\tau)$ of Theorem 8.2.

PROOF: This follows immediately from Proposition 8.5.

9. The $\widetilde{W}$ operators

In this section we define and study certain operators that act on the space of theta series appearing in Theorem 8.2. They are analogous to the W-operators of Atkin–Lehner (see [1]); in fact we conjecture that they essentially are the W-operators – see Conjecture 9.24 below.

As always let p be an odd prime; M a positive integer prime to p and $\mathcal{O}$ an order of level p^2M. Let $I_1, \ldots, I_H$ be a set of representatives of all the distinct left $\mathcal{O}$-ideal classes, $H = H(p^2M)$. Let J be a *two-sided* $\mathcal{O}$-ideal (two-sided means that $\mathcal{O}$ is both the left and right order of J or equivalently, $J = \mathcal{O}\tilde{\beta}$ for some $\tilde{\beta} \in J_{\mathfrak{A}}$ with $\tilde{\beta}^{-1}\mathcal{O}\tilde{\beta} = \mathcal{O}$). Then $JI_1, \ldots, JI_H$ is also a set of representatives of all the distinct left $\mathcal{O}$-ideal classes. Thus $JI_i = I_{\epsilon(i)}\alpha_i$ for some permutation $\epsilon = \epsilon(J)$ of the indices $1, \ldots, H$ and some elements $\alpha_i = \alpha_i(J) \in {}^{\mathfrak{A}}x$. Note that the α_i are well defined upto multiplication on the right by an element of $U(\mathcal{O}_i)$ where $\mathcal{O}_i$ is the right order of I_i.

DEFINITION 9.1: Let s be an even integer ≥ 0 and maintain the notation as above. We define an $H(s+1)$ by $H(s+1)$ matrix $\tilde{W}_s(J)$ by letting $\tilde{W}_s(J) = N(J)^{-s/2}(\rho_{ij})$, $1 \leq i, j \leq H(p^2M)$ where ρ_{ij} is the $s+1$ by $s+1$ matrix

$$\rho_{ij} = \begin{cases} X_s^t(\alpha_i) & \text{if } j = \epsilon(i) \\ 0 & \text{otherwise.} \end{cases}$$

PROPOSITION 9.2: *Let J and L be any two two-sided $\mathcal{O}$-ideals where $\mathcal{O}$ is the order of level p^2M. Then*

(a) *The product $\tilde{W}_s(J)B_s(n)$, $B_s(n) = B_s(n; p^2, M)$ depends only on J, not on the choice of α_i used in Definition 9.1. Here $B_s(n)$ is defined using the same set $I_1, \ldots, I_H$ of left $\mathcal{O}$-ideal classes used to define $\tilde{W}_s(J)$.*

(b) *$\tilde{W}_s(J)$ commutes with $B_s(n)$ for all $n \geq 0$.*

(c) *$\tilde{W}_s(J)\tilde{W}_s(L) = \tilde{W}_s(LJ)$.*

(d) *$\tilde{W}_s(J)$ is the identity matrix if $J = \mathcal{O}m$, $m \in Q^x$.*

PROOF:
(a): By (4.1), the ith, jth block of $\tilde{W}_s(J)B_s(n)$ is

$$(N(J)^{-s/2}X_s^t(\alpha_i))\Big(1/e_j \sum_{\alpha} X_s^t(\alpha)\Big) = (1/e_j)N(J)^{-s/2} \sum_{\alpha} X_s^t(\alpha\alpha_i)$$

where the sum is over all $\alpha \in I_j^{-1}I_{\epsilon(i)}$ with $N(\alpha) = nN(I_{\epsilon(i)})/N(I_j)$. But $I_{\epsilon(i)} = JI_i\alpha_i^{-1}$, so $N(I_{\epsilon(i)}) = N(J)N(I_i)/N(\alpha_i)$ and $\alpha \in I_j^{-1}I_{\epsilon(i)} = I_j^{-1}JI_i\alpha_i^{-1}$ with $N(\alpha) = nN(I_{\epsilon(i)})/N(I_j)$ if and only if $\alpha\alpha_i \in I_j^{-1}JI_i$ with $N(\alpha\alpha_i) = nN(J)N(I_i)/N(I_j)$. Hence the ith, jth block of $\tilde{W}_s(J)B_s(n)$ is $(1/e_j)N(J)^{-s/2}\,\Sigma_\beta\, X_s^t(\beta)$ where the sum is over all $\beta \in I_j^{-1}JI_i$ with $N(\beta) = nN(J)N(I_i)/N(I_j)$ and so $\tilde{W}_s(J)B_s(n)$ depends only on J.

(b): The ith, jth block of $B_s(n)\tilde{W}_s(J)$ is $(1/e_k\,\Sigma_\alpha\, X_s^t(\alpha))$ $(N(J)^{-s/2}X_s^t(\alpha_k))$ where $k = \epsilon^{-1}(j)$ and the sum is over all $\alpha \in I_k^{-1}I_i$ with $N(\alpha) = nN(I_i)/N(I_k)$. But $I_k^{-1}I_i = (J^{-1}I_j\alpha_k)^{-1}I_i = \alpha_k^{-1}I_j^{-1}JI_i$, so the ith, jth entry block of $B_s(n)\tilde{W}_s(J)$ is $(1/e_kN(J)^{-s/2}\,\Sigma_\beta\, X_s^t(\beta)$ where the sum is over all $\beta \in I_j^{-1}JI_i$ with $N(\beta) = nN(J)N(I_i)/N(I_j)$. Finally, $e_k = e_{\epsilon^{-1}(j)} = e_j$ since $JI_i = I_{\epsilon(i)}\alpha_i$ implies that the right order $\mathcal{O}_i$ of JI_i is equal to $\alpha_i^{-1}\mathcal{O}_{\epsilon(i)}\alpha_i$, hence $U(\mathcal{O}_i) \cong U(\mathcal{O}_{\epsilon(i)})$ and $e_i = e_{\epsilon(i)}$ for all $i = 1, \ldots, H$. Thus taking into account the proof of part (a) above, part (b) is proved.

(c): Let $JI_i = I_{\epsilon(i)}\alpha_i$ and $LI_i = I_{\rho(i)}\beta_i$ as in Definition 9.1. Then $(LJ)I_i = I_{\rho\epsilon(i)}\beta_{\epsilon(i)}\alpha_i$. Now $\tilde{W}_s(J)\tilde{W}_s(L)$ has non-zero entry blocks only for the (ith, $\rho\epsilon(i)$th) blocks and in these blocks the entries are $X_s^t(\alpha_i)X_s^t(\beta_{\epsilon(i)}) = X_s^t(\beta_{\epsilon(i)}\alpha_i)$. Thus $\tilde{W}_s(LJ) = \tilde{W}_s(J)\tilde{W}_s(L)$.

(d): Let $J = \mathcal{O}m$, $m \in Q$. Then $N(J)^{-s/2} = m^{-s}$. Since $\epsilon = \epsilon(J)$ is the identity permutation and $\alpha_i = m$ for all i, $\tilde{W}_s(J)$ consists of diagonal blocks $N(J)^{-s/2}X_s^t(m) = m^{-s}\begin{pmatrix} m^s & 0 \\ 0 & m^s \end{pmatrix}$ and (d) follows.

LEMMA 9.3: *Fix p, M, and s as above. Let J be a fixed two-sided $\mathcal{O}$-ideal. Then $\tilde{W}_s(J)$ and the $B_s(n), (n, pM) = 1$ generate a commutative semi-simple group.*

PROOF: By Theorem 2 on p. 106 of [3], the $B_s(n)$ generate a commutative semi-simple ring. By Proposition 9.2 part (b), $\tilde{W}_s(J)$ and the $B_s(n)$ generate a commutative ring. Thus we need only show that $\tilde{W}_s(J)$ is a diagonalizable matrix. But this is obvious since $X_s(\alpha)$, $\alpha \in \mathfrak{N}^x$ is diagonalizable and a permutation matrix is diagonalizable and $\tilde{W}_s(J)$ is composed of these two types of matrices.

The $\tilde{W}_s(J)$ act on theta series the same way the $B_s(n)$ do (see Theorem 2.23 of [15]), i.e. $\tilde{W}_s(J)$ maps the ℓth, kth entry of the matrix

series $\Sigma_{n=0}^{\infty} B_s(n)\exp(n\tau)$ to the ℓth, kth entry of the matrix series $\Sigma_{n=0}^{\infty}(\tilde{W}_s(J)B_s(n))\exp(n\tau)$. We unravel this action a bit. The ith, jth block of $\Sigma_{n=0}^{\infty} B_s(n)\exp(n\tau)$ is $1/e_j \Sigma_\alpha X_s^t(\alpha)\exp(\tau N(\alpha)N(I_j)/N(I_i))$ where the sum is over all $\alpha \in I_j^{-1}I_i$. On the other hand by the proof of part (a) of Proposition 9.2, the ith, jth block of $\Sigma_{n=0}^{\infty}(\tilde{W}_s(J)B_s(n))\exp(n\tau)$ is

$$1/e_j N(J)^{-s/2}\sum_{\beta} X_s^t(\beta)\exp(\tau N(\beta)N(I_j)/N(I_i)N(J))$$

where the sum is over all $\beta \in I_j^{-1}JI_i$. What is the relation between J, $I_j^{-1}I_i$, and $I_j^{-1}JI_i$? $I_j^{-1}I_i$ and $I_j^{-1}JI_i$ are left $\mathcal{O}_j$-ideals while J is a two sided $\mathcal{O}$-ideal. We have to relate the $\mathcal{O}$-ideal J to the $\mathcal{O}_j$-ideals. $I_j = \mathcal{O}\tilde{\gamma}$ and $J = \mathcal{O}\tilde{\alpha}$ for some $\tilde{\gamma}, \tilde{\alpha} \in J_{\mathfrak{A}}$. Then $\mathcal{O}_j = \tilde{\gamma}^{-1}\mathcal{O}\tilde{\gamma}$ and $\tilde{\gamma}^{-1}J\tilde{\gamma} = \mathcal{O}_j\tilde{\gamma}^{-1}\alpha\tilde{\gamma} = J'$ (say) is a two sided $\mathcal{O}_j$-ideal and $I_j^{-1}J = J'I_j^{-1}$. Thus $I_j^{-1}JI_i = J'I_j^{-1}I_i$. We need to introduce the following notation. Let $\mathcal{M}$ be an order of level p^2M and I a left $\mathcal{M}$-ideal. Then

$$\Theta_{I,s}(\tau) = \sum_{\alpha \in I} X_s^t(\alpha)\exp(\tau N(\alpha)/N(I)) \tag{9.1}$$

where the sum is over all $\alpha \in I$. $\Theta_{I,s}(\tau)$ is an $s+1$ by $s+1$ matrix series all of whose entries are modular forms (cusp forms if $s>0$) of weight $s+2$ on $\Gamma_0(N)$, $N = p^2M$. Then thinking of $\tilde{W}_s(J)$ as an operator on theta series we have

PROPOSITION 9.4: *Let $\mathcal{M}$ be an order of level p^2M and I a left $\mathcal{M}$-ideal. Let J be a two sided $\mathcal{O}$-ideal and J' the two sided $\mathcal{M}$-ideal corresponding to J as above. Then $\tilde{W}_s(J)$ acts on $\Theta_{I,s}(\tau)$ as follows: $\tilde{W}_s(J)(\Theta_{I,s}(\tau)) = N(J)^{-s/2}\Theta_{J'I,s}(\tau)$, i.e. the action of $\tilde{W}_s(J)$ is induced by the ideal multiplication $I \mapsto J'I$. Further $\tilde{W}_s(J)$ commutes with the action of the Hecke Operators $T_{s+2}(n)$, $(n, N) = 1$.*

PROOF: It is clear from the above discussion that the action of $\tilde{W}_s(J)$ is as stated. The $\tilde{W}_s(J)$ commute with the Hecke Operators since the action of the Hecke Operators is given by the Brandt Matrices and the $\tilde{W}_s(J)$ commute with the Brandt Matrices.

Now we define operators analogous to the W-operators of Atkin and Lehner. Let $\mathcal{O}$ be the 'canonical' order of level p^2M given by Definition 3.5 in the rational quaternion algebra $\mathfrak{A}$ ramified precisely at p and ∞. Let $\pi_p = p\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix} \in \mathcal{O}_p$ and $\pi_q = \begin{pmatrix} 0 & 1 \\ q^\nu & 0 \end{pmatrix}$, $\nu = \mathrm{ord}_q(M)$ for $q \mid M$. Let $\tilde{\pi}_p = (a_\ell) \in J_{\mathfrak{A}}$ be given by $a_\ell = 1$ if $\ell \neq p$ and $a_p = \pi_p$.

Similarly, let $\tilde{\pi}_q = (a_\ell) \in J_{\mathfrak{A}}$ be given by $a_\ell = 1$ if $\ell \neq q$ and $a_q = \pi_q$. Finally let $J(p) = \mathcal{O}\tilde{\pi}_p$ and $J(q) = \mathcal{O}\tilde{\pi}_q$ for $q \mid M$. Now a left $\mathcal{O}$-ideal I is two sided if and only if $I = \mathcal{O}\tilde{\alpha}$, $\tilde{\alpha} = (\alpha_\ell) \in J_{\mathfrak{A}}$ where $\tilde{\alpha}^{-1}\mathcal{O}\tilde{\alpha} = \mathcal{O}$ which if true if and only if $\alpha_\ell^{-1}\mathcal{O}_\ell\alpha_\ell = \mathcal{O}_\ell$ for all $\ell < \infty$. Then it follows from 2.2 of [5] that $J(q)$ is a two sided $\mathcal{O}$-ideal for all $q \mid M$. Since $\mathcal{O}_p$ is the unique order of level p^2 of $\mathfrak{A}_p$ (see Theorem 1.5), $\pi_p^{-1}\mathcal{O}_p\pi_p = \mathcal{O}_p$ and $J(p)$ is also a two-sided $\mathcal{O}$-ideal.

DEFINITION 9.5: In the above notation, let $\tilde{W}_{p,s} = \tilde{W}_s(J(p))$ and $\tilde{W}_{q,s} = \tilde{W}_s(J(q))$ for $q \mid M$.

If there is no possibility of confusion we will drop the s and write $\tilde{W}_p$ and $\tilde{W}_q$.

PROPOSITION 9.6: *Fix s an even integer ≥ 0 and maintain the above notation. Then*

(a) $\tilde{W}_p^2 = id$ *and* $\tilde{W}_q^2 = id$ *for* $q \mid M$.

(b) $\tilde{W}_p$, *the* $\tilde{W}_q$, $q \mid M$, *and the* $B_s(n; p^2, M)$ *with* $(n, pM) = 1$ *generate a commutative semi-simple ring.*

PROOF:

(a) This follows from Proposition 9.2 (d) as $(J(p))^2 = \mathcal{O}p^2$ and $(J(q))^2 = \mathcal{O}q^\nu$, $\nu = \mathrm{ord}_q(M)$.

(b) It is clear that the $\tilde{\pi}_p$ and $\tilde{\pi}_q$, $q \mid M$ commute with each other, hence the $J(p)$ and $J(q)$ do and then by Proposition 9.2 (c), so do the $\tilde{W}_p$ and $\tilde{W}_q$. Then (b) follows as in Lemma 9.3.

REMARK 9.7: The properties of the $\tilde{W}_p$ and $\tilde{W}_q$, $q \mid M$ given in Proposition 9.6 should be compared with the properties of the W-operators of Atkin and Lehner (see [1]).

Let $I_1, \ldots, I_G$, $\tilde{\delta}I_1 = I_{G+1}, \ldots, \tilde{\delta}I_G = I_{2G}$ be a complete set of representatives of all the distinct left $\mathcal{O}$-ideal classes as in Definition 5.14. Recall that $\tilde{\delta}$ is given by Definition 5.4. We need

LEMMA 9.8: *With respect to the above set of ideal class representatives,*

$$\tilde{W}_{p,s} = \left(\begin{array}{c|c} & \begin{matrix} 1 & & \\ 0 & \cdot & 0 \\ & & \cdot 1 \end{matrix} \\ \hline \begin{matrix} 0 & & \\ & & \\ & & \end{matrix} & \\ \hline \begin{matrix} 1 & & \\ 0 & \cdot & 0 \\ & \cdot & 1 \end{matrix} & \begin{matrix} 0 & & \\ & & \\ & & \end{matrix} \end{array}\right) \text{ if } p \equiv 1 \pmod 4$$

and $\tilde{W}_{p,s} = \left(\begin{array}{c|c} V & 0 \\ \hline 0 & V \end{array}\right)$ *if* $p \equiv 3 \pmod 4$ *for some* $G(s+1)$ *by* $G(s+1)$ *matrix* V.

PROOF: First consider the case $p \equiv 1 \pmod 4$. Then it follows from Definition 5.4 that $\mathcal{O}\tilde{\delta}p = J(p)$. Thus $J(p)I_i = I_{i+G}p$ for $i \leq G$ and $J(p)I_{i+G} = \mathcal{O}\tilde{\delta}p\tilde{\delta}I_i = I_ip$ for $i \leq G$ by Lemma 5.5. Now $X'_s(p) = \begin{pmatrix} p^s & & 0 \\ & \cdot & \\ 0 & & p^s \end{pmatrix}$ and $N(J(p))^{-s/2} = p^{-s}$ and our result follows directly from the definition of $W_s(J(p))$. Now assume $p \equiv 3 \pmod 4$. From Definition 5.4 we see that $\delta_p = \begin{pmatrix} 0 & -v \\ pv & 0 \end{pmatrix}$. Recall that $\pi_p = p\begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}$. Thus $\pi_p\delta_p = -\delta_p\pi_p$ which implies $J(p)\tilde{\delta}\mathcal{O} = \tilde{\delta}J(p)\mathcal{O}$ Also it is clear that $J(p)$ is an ideal of positive character (since $p \equiv 3 \pmod 4$). Hence $J(p)I_i = I_{\rho(i)}\alpha_i$ and $J(p)I_{i+G} = I_{\rho(i)+G}\alpha_i$ for some permutation ρ of the indices $1, \ldots, G$ and some $\alpha_i \in \mathfrak{A}^\times$. Thus we see from the definition of $\tilde{W}_s(J(p))$ that $\tilde{W}_p = \left(\begin{array}{c|c} V & 0 \\ \hline 0 & V \end{array}\right)$ for some $G(s+1)$ by $G(s+1)$ matrix V.

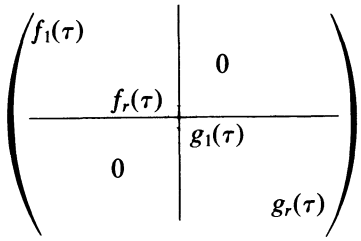
PROPOSITION 9.9: *It is possible to modify the* f_i *and* g_i *of Theorems* 5.31 *and* 5.34 *so that in addition to satisfying all the properties listed in those theorems, the* f_i *and* g_i *are also eigen forms for the* $\tilde{W}_p$ *and* $\tilde{W}_q$, $q \mid M$ *operators.*

PROOF: This follows from Proposition 9.6 (b) and Lemma 9.8 since it is clear that in Lemmas 5.29 and 5.30 we can simultaneously diagonalize the $\tilde{W}_p$ and $\tilde{W}_q$, $q \mid M$ along with the $B_s(n)$, $(n, pM) = 1$.

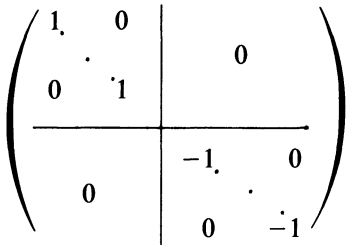
The $\tilde{W}_p$ and $\tilde{W}_q$, $q \mid M$ induce linear transformations on the space $\langle f_i(\tau)\rangle \oplus \ldots \oplus \langle f_r(\tau)\rangle \oplus \langle g_i(\tau)\rangle \oplus \ldots \oplus \langle g_r(\tau)\rangle$ of cusp forms of weight $s+2$ appearing in Theorem 8.2. Here $i = \begin{cases} 2 & \text{if } s = 0 \\ 1 & \text{if } s > 0 \end{cases}$ and $r = G(s+1)$. In the case of $\tilde{W}_p$, we can describe this action rather explicitly.

THEOREM 9.10: *Assume that as in Proposition* 9.9, *the* f_i *and* g_i *of Theorems* 5.31 *and* 5.34 *are eigen forms for the* $\tilde{W}_p$ *and* $\tilde{W}_q$, $q \mid M$. *Then the action of the* $\tilde{W}_p$ *operator is as follows: if* $p \equiv 1 \pmod 4$, *then* $\tilde{W}_p(f_i) = f_i$ *and* $\tilde{W}_p(g_i) = -g_i$; *if* $p \equiv 3 \pmod 4$, *then* f_i *and* g_i *always have the same eigen value under* $\tilde{W}_p$, *i.e.* $\tilde{W}_p(f_i) = \lambda f_i$ *if and only if* $\tilde{W}_p(g_i) = \lambda g_i$. *Here* $\lambda = \pm 1$.

PROOF: First consider the case $p \equiv 1 \pmod 4$. By Lemma 5.29 and 5.30, the action of $\tilde{W}_p$ on



is given by the diagonal matrix $E_1 \tilde{W}_p E_1^{-1}$ if $s > 0$ and by $E_1' \tilde{W}_p E_1'^{-1}$ if $s = 0$. In both cases E_1 and E_1' have the block decomposition of the form $\left(\begin{array}{c|c} F & F \\ \hline F & -F \end{array}\right)$ for some invertible $G(s+1)$ by $G(s+1)$ matrix F. Hence by Lemma 9.8, $E_1 \tilde{W}_p E_1^{-1}$ and $E_1' \tilde{W}_p E_1'^{-1}$ both have the form



Now consider the case $p \equiv 3 \pmod 4$. This works out the same as in the case $p \equiv 1 \pmod 4$ except that by Lemma 9.8, $E_1 \tilde{W}_p E_1^{-1}$ and $E_1' \tilde{W}_p E_1'^{-1}$ both have the form $\left(\begin{array}{c|c} FVF^{-1} & 0 \\ \hline 0 & FVF^{-1} \end{array}\right)$ where by Proposition 9.9 FVF^{-1} is a diagonal matrix. Finally since $\tilde{W}_p^2 = id$, its only eigen values are ± 1.

REMARK 9.11: Notice that in the case $p \equiv 1 \pmod 4$, the f_i and g_i appearing in Theorems 5.31 and 5.34 are automatically eigen forms for the operator $\tilde{W}_p$.

REMARK 9.12: It should be noted that while the $\tilde{W}_p$ and $\tilde{W}_q$, $q \mid M$ induce linear transformations on the space

$$\langle f_i(\tau)\rangle \oplus \ldots \oplus \langle f_r(\tau)\rangle \oplus \langle g_i(\tau)\rangle \oplus \ldots \oplus \langle g_r(\tau)\rangle$$
$$\left(i = \begin{cases} 2 & \text{if } s = 0 \\ 1 & \text{if } s > 0 \end{cases} \text{ and } r = G(s+1)\right)$$

appearing in Theorem 8.2, it is not clear that they induce linear transformations on the subspace of $S_k(p^2M)$, $k = s+2$ generated by the $f_i(\tau)$ and $g_i(\tau)$. The reason for the difficulty is that the f_i and g_i are not linearly independent – in fact they are not all distinct, see Theorem 10.3 below. However we will show that the product $\tilde{W}_p \Pi_{q|M} \tilde{W}_q$ is a linear transformation on the subspace of $S_k(p^2M)$ which is generated by theta series. In fact $\tilde{W}_p \Pi_{q|M} \tilde{W}_q = -E$ where E is the canonical involution (see Corollary 9.23).

Recall that the canonical involution on $S_k(N)$ is given by the matrix $E = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. The action on $S_k(N)$ (denoted by a vertical line $|$) is given by

$$\begin{aligned} f \mid E(\tau) &= (\det E)^{k/2}(N\tau)^{-k} f(-1/N\tau) \\ &= N^{-k/2}\tau^{-k} f(-1/N\tau) \end{aligned} \tag{9.2}$$

DEFINITION 9.13: Let the notation be as in Definition 9.5. Put $L = J(p)J(q_1)\dots J(q_\mu)$, where $q_1, \dots, q_\mu$ are all the distinct primes dividing M. Put $\tilde{E}_s = \tilde{E} = \tilde{W}_s(L)$.

Note that $\tilde{E} = \tilde{W}_p \Pi_{q|M} \tilde{W}_q$ is an $H(s+1)$ by $H(s+1)$ matrix which acts on the entries of the matrix series $\Sigma_{n=0}^{\infty} B_s(n; p^2, M) \exp(n\tau)$ by sending the ℓth, kth entry of that matrix series to the ℓth, kth entry of $\Sigma_{n=0}^{\infty} (\tilde{E}_s B_s(n; p^2, M)) \exp(n\tau)$. Now let I be a left $\mathcal{O}$-ideal. As in the discussion preceeding Proposition 9.4, we see that $\tilde{E}_s$ acts on $\Theta_{I,s}(\tau)$ as follows: $\tilde{E}_s$ sends the ℓth, kth entry of $\Theta_{I,s}(\tau)$ to the ℓth, kth entry of $N(L)^{-s/2}\Theta_{LI,s}(\tau)$. Note that if $s = 0$, $\Theta_{I,0}(\tau)$ is just a single theta series.

In order to show that $\tilde{E} = -E$, we need to translate some results in Ogg's book [10] into a co-ordinate free language. Let $q(x)$ be a positive definite quadratic form on a rational vector space V of even dimension $r = 2k$, i.e. $q: V \to Q$ such that $q(\lambda x) = \lambda^2 q(x)$ for $x \in V$, $\lambda \in Q$ and $\langle x, y \rangle = q(x+y) - q(x) - q(x)$ is bilinear. We call $\langle x, y \rangle$ the bilinear form associated to q. Note that $\langle x, x \rangle = 2q(x)$. A lattice Γ (free Z-submodule of V with $\Gamma \otimes_Z Q = V$) on V is said to be *integral* with respect to $q(x)$ if $q(x) \in Z$ for all $x \in \Gamma$. The dual of a lattice Γ, denoted by Γ', is $\Gamma' = \{y \in V \mid \langle x, y \rangle \in Z \text{ for all } x \in \Gamma\}$. The *level* of Γ is the least positive integer N such that $Nq(x) \in Z$ for all $x \in \Gamma'$. Note that choosing a basis $e_1, \dots, e_r$ for Γ, $A = (\langle e_i, e_j \rangle)$ is a symmetric integral matrix with even diagonal entries and the 'level of Γ' is equal to the classical level of A, i.e. the least positive integer N such that NA^{-1} is integral with even diagonal entries. Following Ogg (see [10],

p. VI-10) we define for Γ an integral lattice on V and x an element of $V \otimes \mathbb{R}$, $\Theta_\Gamma(\tau, x) = \Sigma_{\gamma \in \Gamma} \exp(q(\gamma + x)\tau)$. Then we have

PROPOSITION 9.14:

$$\Theta_\Gamma(\tau, x) = \left(\frac{i}{\tau}\right)^{r/2} \frac{1}{\sqrt{D}} \sum_{\gamma \in \Gamma'} \exp(\langle \gamma, x\rangle - \langle \gamma, \gamma\rangle/2\tau) \tag{9.3}$$

where D is the discriminant of Γ.

PROOF: This is just a co-ordinate free version of Proposition 23 of [10], p. VI-10. Note that if Γ has $e_1, \ldots, e_r$ as a Z-basis, then $D = \det(\langle e_i, e_j\rangle)$.

We need a 'nice' set of generators for the set of homogeneous 'spherical functions' with respect to $q(x)$. For the definition of spherical see page VI-5 of [10]. Our set is given by

PROPOSITION 9.15: *Let $f(x)$ be a homogeneous polynomial function of degree s on $V \otimes_Q \mathbb{C}$. Polynomial means that if we choose a basis, $f(x)$ becomes a polynomial in the coefficients of the basis. Then $f(x)$ is spherical with respect to $q(x) = 1/2\langle x, x\rangle$ if and only if $f(x)$ is a linear combination of functions of the form $\langle \xi, x\rangle^s$ where $\xi \in V \otimes_Q \mathbb{C}$ and $\langle \xi, \xi\rangle = 0$.*

PROOF: See Theorem 18 on p. VI-6 of [10].

PROPOSITION 9.16: *Let the notation be as above. Let $\xi \in V \otimes_Q \mathbb{C}$ with $\langle \xi, \xi\rangle = 0$ and let s be a non-negative integer. Then*

$$\begin{aligned} &\sum_{\gamma \in \Gamma} \langle \xi, \gamma\rangle^s \exp(q(\gamma)\tau) \\ &= (i/\tau)^{r/2} \tau^{-s} D^{-1/2} \sum_{\gamma \in \Gamma'} \langle \xi, \gamma\rangle^s \exp(-q(\gamma)/\tau) \end{aligned} \tag{9.4}$$

PROOF: We mimic the proof of Theorem 19 of [10]. Let D_ξ denote the directional derivative,

$$(D_\xi f)(x) = \lim_{t \to 0} \frac{f(x + t\xi) - f(x)}{t}.$$

Then $D_\xi(q(x)) = \langle \xi, x\rangle$, $D_\xi(\langle \xi, x\rangle) = 0$ and $D_\xi(\langle c, x\rangle) = \langle c, \xi\rangle$ where c is any fixed constant. We apply D_ξ^s to the identity (9.3) obtaining

$$\sum_{\gamma\in\Gamma}(2\pi i\tau)^s\langle\xi,\gamma+x\rangle^s\exp(q(\gamma+x)\tau)$$
$$=\left(\frac{i}{\tau}\right)^{n/2}D^{-1/2}\sum_{\gamma\in\Gamma'}(2\pi i)^s\langle\gamma,\xi\rangle^s\exp(\langle\gamma,x\rangle-\langle\gamma,\gamma\rangle/2\tau).$$

Cancelling the $(2\pi i)^s$ and letting $x=0$, we obtain (9.4).

We need to employ (9.4) in the case $V=\mathfrak{A}$, $q(x)=N(x)/N(I)$, and $\Gamma=I$ where I is some left $\mathcal{O}$-ideal. Thus we need to determine I' and the discriminant of I. We do this in a series of lemmas.

LEMMA 9.17: *Let $\mathcal{O}$ be the canonical order of level p^2M given in Definition* 3.5 *in the quaternion algebra $\mathfrak{A}$. Then the dual of $\mathcal{O}$ with respect to the quadratic form $N(x)$ is L^{-1} where L is the ideal given in Definition* 9.13.

PROOF: By the proof of Lemma 3.4 of Pizer [14], we need only show that $\mathcal{O}_p'=L_p^{-1}=\pi_p^{-1}\mathcal{O}_p=\frac{1}{pu}\begin{pmatrix}v&0\\0&-v\end{pmatrix}\mathcal{O}_p$. Choosing the obvious basis $e_1=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $e_2=\begin{pmatrix}pv&0\\0&-pv\end{pmatrix}$, $e_3=\begin{pmatrix}0&1\\p&0\end{pmatrix}$, and $e_4=\begin{pmatrix}0&v\\-pv&0\end{pmatrix}$ of $\mathcal{O}_p$, then $f_1=\pi_p^{-1}e_2$, $f_2=\pi_p^{-1}e_1$, $f_3=\pi_p^{-1}e_4$, and $f_4=\pi_p^{-1}e_3$ is a basis of L_p^{-1} and $\langle e_i,f_j\rangle=\mathrm{tr}(e_i\bar{f}_j)=\pm2\delta_{ij}$ which establishes the result.

LEMMA 9.18: *Let $\mathcal{O}$ be as in Lemma* 9.17 *and let I be a left $\mathcal{O}$-ideal. Then the dual of I with respect to the quadratic form $N(x)/N(I)$ is given by $I'=L^{-1}I$ where L is as in Definition* 9.13.

PROOF: The proof is identical to the proof of Lemma 3.5 of [14].

The final lemma we need is

LEMMA 9.19: *Let the situation be as in Lemma* 9.18 *above. Then the discriminant of I as a lattice on $\mathfrak{A}$ with respect to the quadratic form $q(x)=N(x)/N(I)$ is given by $\mathrm{disc}(I)=p^4M^2$.*

PROOF: The proof is the same as the proof of Lemma 3.7 of [14].

Finally we are able to state

THEOREM 9.20: *Let p be an odd prime and M a positive integer prime to p. Let k be an even integer ≥2. Let $\mathcal{O}$ be the order of level p^2M given by Definition* 3.5 *and let L be the two sided $\mathcal{O}$-ideal given in Definition* 9.13. *Let $\Theta_{I,k-2}(\tau)$ be the matrix of theta series defined by* (9.1). *Then the canonical involution E (acting on $S_k(N)$, $N=p^2M$)*

sends the ℓth, kth entry of $\Theta_{I,k-2}(\tau)$ to the ℓth, kth entry of $-N^{-s/2}\Theta_{LI,k-2}(\tau)$, where $N = p^2M$.

PROOF: Let $s = k-2$. By Proposition 9.15 and an argument similar to that used in the proof of Theorem 2.14 of [15] any fixed entry of $\Theta_{I,s}(\tau)$ is a linear combination of series of the form $h(\tau) = \Sigma_{\alpha\in I}\langle\xi,\alpha\rangle^s \exp(\tau N(\alpha)/N(I))$ where $\langle x, y\rangle = N(I)^{-1}\operatorname{tr}(x\bar{y})$ and $\xi \in \mathfrak{A}\otimes\mathbb{C}$ satisfies $\langle\xi,\xi\rangle = 0$. Then

$$h \mid E(\tau) = N^{k/2}(N\tau)^{-k}h(-1/N\tau)$$

$$= N^{-k/2}\tau^{-k}\sum_{\alpha\in I}\langle\xi,\alpha\rangle^s \exp(-N(\alpha)/N(I)N\tau). \tag{9.5}$$

On the other hand the corresponding (ℓth, kth) entry of $-N^{-s/2}\Theta_{LI,s}(\tau)$ is the same linear combination of series of the form

$$-N^{-s/2}\sum_{\alpha\in LI}\langle\xi,\alpha\rangle^s \exp(\tau N(\alpha)/N(LI)) \tag{9.6}$$

By (9.4) and Lemmas 9.18 and 9.19, (9.6) equals

$$-N^{-s/2}(i/\tau)^2\tau^{-s}N^{-1}\sum_{\alpha\in L^{-1}LI}\langle\xi,\alpha\rangle^s \exp(-N(\alpha)/N(LI)\tau)$$

$$= N^{-k/2}\tau^{-k}\sum_{\alpha\in I}\langle\xi,\alpha\rangle^s \exp(-N(\alpha)/N(I)N\tau)$$

which is equal to (9.5).

REMARK 9.21: Theorem 9.20 remains valid for any order $\mathcal{M}$ of level p^2M with the obvious changes. In particular, $\mathcal{M} = \tilde{\gamma}^{-1}\mathcal{O}\tilde{\gamma}$ for some $\gamma \in J_{\mathfrak{A}}$ so letting I be a left $\mathcal{M}$-ideal, the canonical involution E sends the ℓth, kth entry of $\Theta_{I,k-2}(\tau)$ to the ℓth, kth entry of $-N^{-s/2}\Theta_{L'I,k-2}(\tau)$ where $L' = \tilde{\gamma}^{-1}L\tilde{\gamma}$ is the two-sided $\mathcal{M}$-ideal that corresponds to L.

REMARK 9.22: It follows from Remark 9.21 and the discussion preceding Proposition 9.4 that the canonical involution sends the ℓth, kth entry of $E_{n=0}^{\infty}B_s(n;p^2,M)\exp(n\tau)$ to the ℓth, kth entry of $-\Sigma_{n=0}^{\infty}(\tilde{E}_sB_s(n;p^2,M))\exp(n\tau)$.

COROLLARY 9.23: As operators on the subspace of $S_k(p^2M)$ generated by the theta series f_i and g_j appearing in Theorem 8.2, we have $\tilde{E} = -E$.

Corollary 9.23 and Proposition 9.6 (and very little additional evidence) induce us to make the

CONJECTURE 9.24: Let p be an odd prime and M a positive integer prime to p. Then as operators on the subspace of $S_k(p^2M)$ generated by the theta series f_i and g_j appearing in Theorem 8.2, we have $\tilde{W}_{p,k-2} = -W_p$ and $\tilde{W}_{q,k-2} = W_q$ for all $q \mid M$ where W_p and W_q, $q \mid M$ and the W-operators of Atkin–Lehner.

Of course Corollary 9.23 proves the conjecture when $M = 1$.

REMARK 9.25: The analogue of Theorem 9.20 in the case of forms of weight 2 and level $p^{2r+1}M$, $p \nmid M$ was proved by Pizer in [14]. It is clear that the results of this section concerning the higher weight cases and also the $\tilde{W}_{p,s}$ and $\tilde{W}_{q,s}$ can be easily transferred to the case of level $p^{2r+1}M$.

To conclude this section we now consider whether or not there are any other interesting operators $\tilde{W}_s(J)$ other than the $\tilde{W}_p$ and $\tilde{W}_q$, $q \mid M$. We will find that there are some, but not many. Let $\mathcal{N}(\mathcal{O}) = \{\tilde{\alpha} \in J_{\mathfrak{A}} \mid \tilde{\alpha}^{-1}\mathcal{O}\tilde{\alpha} = \mathcal{O}\}$. Then the mapping $\mathcal{N}(\mathcal{O}) \ni \tilde{\alpha} \mapsto \mathcal{O}\tilde{\alpha}$ is clearly a homomorphism from $\mathcal{N}(\mathcal{O})$ onto the group of all two-sided $\mathcal{O}$-ideals. The kernal is $\mathcal{U}(\mathcal{O})$. It follows that $\mathcal{N}(\mathcal{O})/\mathcal{U}(\mathcal{O})Q^x$ is isomorphic to the group of two-sided $\mathcal{O}$-ideals modulo ideals of the form $\mathcal{O}m$, $m \in Q^x$. By Proposition 9.2, we are interested in the structure of $\mathcal{N}(\mathcal{O})/\mathcal{U}(\mathcal{O})Q^x$ and we have

PROPOSITION 9.26: $\mathcal{N}(\mathcal{O})/\mathcal{U}(\mathcal{O})Q^x \cong K \times \Pi_{q \mid M}\, (Z/(2))$ *where K is the dihedral group of order $2(p+1)$.*

PROOF: Let $N(\mathcal{O}_\ell) = \{\alpha \in \mathfrak{A}_\ell^x \mid \alpha\mathcal{O}_\ell\alpha^{-1} = \mathcal{O}_\ell\}$. Then $\mathcal{N}(\mathcal{O})/\mathcal{U}(\mathcal{O})Q^x = \mathcal{N}(\mathcal{O})/\mathcal{U}(\mathcal{O})J_Q \cong \Pi_{\ell \mid pM}\, N(\mathcal{O}_\ell)/U(\mathcal{O}_\ell)Q_\ell^x$ since $N(\mathcal{O}_\ell) = U(\mathcal{O}_\ell)Q_\ell^x$ for all $\ell \nmid pM$. By the proof of Theorem 2.20 of [14], $N(\mathcal{O}_q)/U(\mathcal{O}_q)Q_q^x \cong Z/(2)$ for all $q \mid M$ and in fact $N(\mathcal{O}_q) = U(\mathcal{O}_q)Q_q^x \cup \pi_q U(\mathcal{O}_q)Q_q^x$ for $q \mid M$ where π_q is defined prior to Definition 9.5 above. We need now only consider $N(\mathcal{O}_p)/U(\mathcal{O}_p)Q_p^x$. As $\mathcal{O}_p$ is the unique order of level p^2 of $\mathfrak{A}_p$ (see Theorem 1.5) $\alpha\mathcal{O}_p\alpha^{-1} = \mathcal{O}_p$ for all $\alpha \in \mathfrak{A}_p^x$, so $N(\mathcal{O}_p) = \mathfrak{A}_p^x$. Let D be the (unique) maximal order of $\mathfrak{A}_p$. Then $\mathfrak{A}_p^x/U(\mathbf{D})Q_p^x \cong Z/(2)$ and if $\mathfrak{A}_p$ is identified as in (1.2), $\mathfrak{A}_p^x = U(D)Q_p^x \cup \begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix} U(D)Q_p^x$. Now $U(D)Q_p^x/U(\mathcal{O}_p)Q_p^x \cong U(D)/U(\mathcal{O}_p)$ is a cyclic group of order $p+1$ by Proposition 1.8.

If $\beta \in U(D)$ and $\bar{\beta}$ is its image in $U(D)Q_p^x/U(\mathcal{O}_p)Q_p^x$, then it is clear (e.g. by Proposition 1.8) that $\begin{pmatrix} 0 & 1 \\ p & 0 \end{pmatrix}$ acts by conjugation on

$U(D)Q_p^x/U(\mathcal{O}_p)Q_p^x$ and $\begin{pmatrix}0 & 1\\ p & 0\end{pmatrix}\beta\begin{pmatrix}0 & 1\\ p & 0\end{pmatrix}^{-1} = \beta^{-1}$. Thus $K = \mathfrak{A}_p^x/\mathfrak{A}(\mathcal{O}_p)Q_p^x$ is a semi-direct product of the group ($\cong Z/(2)$) generated by $\begin{pmatrix}0 & 1\\ p & 0\end{pmatrix}$ and the subgroup ($\cong Z/(p+1)$) $U(D)Q_p^x/U(\mathcal{O}_p)Q_p^x$.

By Proposition 9.26 the group of two-sided $\mathcal{O}$-ideals modulo the subgroup of ideals of the form $\mathcal{O}m, m \in Q^x$ is isomorphic to $K \times \Pi_{q|M}(Z/(2))$. It is clear from the proof of Proposition 9.26 and the definition of $J(q)$ that $J(q)$ for $q \mid M$ correspond to the non-identity element of $Z/(2)$ in the copy to $Z/(2)$ that comes from q. It is equally clear that $J(p)$ corresponds to the element of order 2 in the cyclic subgroup $U(D)Q_p^x/U(\mathcal{O}_p)Q_p^x$. Thus the only interesting two-sided $\mathcal{O}$-ideals remaining are those corresponding to the elements of K. Thus we have

PROPOSITION 9.27: *There exists a set of operators which form a dihedral group of order* $2(p+1)$ *which act on the space of theta series*

$$\langle f_i(\tau)\rangle \oplus \ldots \oplus \langle f_r(\tau)\rangle \oplus \langle g_i(\tau)\rangle \oplus \ldots \oplus \langle g_r(\tau)\rangle$$

$\left(i = \begin{cases} 2 & \text{if } s = 0 \\ 1 & \text{if } s > 0 \text{ and } r = G(s+1)\end{cases}\right)$ *appearing in Theorem* 8.2.

These operators commute with all the Hecke Operators $T_{s+2}(n)$, $(n, pM) = 1$ *and also with the operators* $\tilde{W}_q$, $q \mid M$.

PROOF: This follows from Lemma 9.3, Proposition 9.26, and the above discussion.

REMARK 9.28: It would be interesting to identify this group of operators independently of the theory of quaternion algebras.

10. The case of level p^2

In this section we restrict our attention to the case of level p^2, i.e. we assume $M = 1$. Denote by $S_k^0(N)$ the space generated by the new forms of weight k on $\Gamma_0(N)$, see Atkin and Lehner [1]. Denote by $S_k^0(N)^d$ the space of forms $\{f(d\tau) \mid f(\tau) \in S_k^0(N)\}$. Then we have

PROPOSITION 10.1: *Let* p *be an odd prime and let* $M = 1$. *Maintain the notation as in Theorem* 8.2 *where we assume by Proposition* 9.9 *that all* $f_i(\tau)$ *and* $g_i(\tau)$ *are eigen forms for* $\tilde{W}_p$. *If* $k = 2$, *then we have*

$$2S_2^0(p^2) \oplus S_2^0(p) \cong \langle f_2(\tau)\rangle \oplus \ldots \oplus \langle f_G(\tau)\rangle \oplus \langle g_2(\tau)\rangle \oplus \ldots \oplus$$
$$\langle g_G(\tau)\rangle \oplus S_2^0(p)^{\varphi} \oplus 2 \sum_{\substack{\{\psi\} \\ \psi^2 \neq 1}} S_2(p, \psi^2)^{\bar{\psi}} \tag{10.1}$$

while if $k > 2$, we have

$$2S_k^0(p^2) \oplus S_k^0(p) \cong \langle f_1(\tau)\rangle \oplus \ldots \oplus \langle f_r(\tau)\rangle \oplus \langle g_1(\tau)\rangle \oplus \ldots \oplus$$
$$\langle g_r(\tau)\rangle \oplus 2S_k(1)^{\varphi} \oplus S_k^0(p)^{\varphi} \oplus 2 \sum_{\substack{\{\psi\} \\ \psi^2 \neq 1}} S_k(p, \psi^2)^{\bar{\psi}} \tag{10.2}$$

where $r = G(k-1)$, $G = 1/2H(p^2) = p^2 - 1/24$ if $p \geq 5$ and $G = 1$ if $p = 3$. *In both cases φ is the quadratic character $\left(\frac{-}{p}\right)$ and the sum $\sum_{\substack{\{\psi\} \\ \psi^2 \neq 1}}$ is over a set of representatives of the pairs $\{\psi, \bar{\psi}\}$, $\psi^2 \neq 1$ of the characters of $(Z/(p)^x$. The $\cong$ in* (10.1) *and* (10.2) *is an isomorphism as modules for the Hecke algebra H generated by $T_k(n)$, $(n, p) = 1$.*

PROOF: It follows from Theorem 5 of Atkin–Lehner [1] that $S_k(p^2) \cong 3S_k^0(1) \oplus 2S_k^0(p) \oplus S_k^0(p^2)$ and $S_k(p) \cong 2S_k^0(1) \oplus S_k^0(p)$. Also by Lemma 8.4 $S_k(p, \psi^2)^{\bar{\psi}} \cong S_k(p, \bar{\psi}^2)^{\psi}$. Hence taking $M = 1$, (10.1) follows from (8.1) and (10.2) follows from (8.2). The fact that $H = p^2 - 1/12$ follows from Theorem 4.18.

PROPOSITION 10.2: *Let W_p denote the W_p-operator of Atkin-Lehner and maintain the notation and assumptions of Proposition* 10.1. *In particular, the level is p^2. Then for $p \equiv 1 \pmod 4$ we have $f_i \mid W_p = -f_i$ and $g_i \mid W_p = g_i$ while for $p \equiv 3 \pmod 4$ we have $f_i \mid W_p = \lambda_i f_i$ if and only if $g_i \mid W_p = \lambda_i g_i$. Here $\lambda_i = \pm 1$.*

PROOF: As the level is p^2, W_p is the canonical involution E and $\tilde{W}_p = \tilde{E}$, so by Corollary 9.23 $W_p = -\tilde{W}_p$. The proposition now follows from Theorem 9.10.

THEOREM 10.3: *Let $N = p^2$, p an odd prime and maintain the notation and assumptions of Proposition* 10.1. *Let H denote the Hecke Algebra generated by the $T_k(n), (n, p) = 1$. Assume $p \equiv 1 \pmod 4$. Then we have*

(i) *a subset $\{f_{i_1}, \ldots, f_{i_t}\}$, $t = \dim S_k^0(p)$, of the f_i appearing in* (10.1) *if $k = 2$ or in* (10.2) *if $k > 2$ form a basis of a subspace of $S_k(p^2)$ which is H-isomorphic to $S_k^0(p)$.*

(ii) $f_{i_\lambda} \mid W_p = -f_{i_\lambda}$ *for* $\lambda = 1, \ldots, t$.

(iii) *the* $g_{i_1} = f_{i_1} \mid R_p, \ldots, g_{i_t} = f_{i_t} \mid R_p$, f_{i_ν} *as in* (i), *are new forms in* $S_k^0(p^2)$ *and form a basis of* $S_k^0(p)^\varphi$ *where* φ *is the quadratic character* $\left(\frac{-}{p}\right)$.

(iv) *all other non-zero* f_j *and* g_j ($j \notin \{i_1, \ldots, i_t\}$) *are new forms in* $S_k^0(p^2)$ *and each new form appearing in the set* $\{f_j, g_j \mid j \notin \{i_1, \ldots, i_t\}\}$ *appears exactly twice.*

Assume $p \equiv 3 \pmod 4$. *Then we have*

(i′) *a subset* $\{f_{i_1}, \ldots, f_{i_\mu} g_{j_1}, \ldots, g_{j_\nu}\}$, $\mu + \nu = \dim S_k^0(p)$ *of the* f_i *and* g_j *appearing in* (10.1) *if* $k = 2$ *or in* (10.2) *if* $k > 2$ *form a basis of a subspace of* $S_k(p^2)$ *which is* H*-isomorphic to* $S_k^0(p)$

(ii′) $f_{i_\lambda} \mid W_p = -f_{i_\lambda}$ *for* $\lambda = 1, \ldots, \mu$ and $g_{j_\lambda} \mid W_p = -g_{i_\lambda}$ for $\lambda = 1, \ldots, \nu$

(iii′) *the* $g_{i_1} = f_{i_1} \mid R_p, \ldots, g_{i_\mu} = f_{i_\mu} \mid R_p$, $f_{j_1} = g_{j_1} \mid R_p, \ldots, f_{j_\nu} = g_{j_\nu} \mid R_p$ *are all new forms in* $S_k^0(p^2)$ *and form a basis of* $S_k^0(p)^\varphi$ *where* φ *is the quadratic character* $\left(\frac{-}{p}\right)$.

(iv′) *all other non-zero* f_n *and* g_m ($n \notin \{i_1, \ldots, i_\mu\}$, $m \notin \{j_1, \ldots, j_\nu\}$) *are new forms in* $S_k^0(p^2)$ *and each new form appearing in the set* $\{f_n, g_m \mid n \notin \{i_1, \ldots, i_\mu\}, m \notin \{j_1, \ldots, j_\nu\}\}$ *appears exactly twice.*

PROOF: Following Atkin–Lehner we say that two forms h and h' in $S_k(L)$ are equivalent and we write $h \sim h'$ if they are eigenforms for all $T_k(\ell)$, $\ell \nmid L$ with the same eigen values. First we consider the case $p \equiv 1 \pmod 4$. If h is an eigen form in $S_k^0(p)$, then by Lemmas 20 and 24 of [1], h is not equivalent to any other eigen form contained in the L.H.S. of (10.1) or (10.2). Thus by (10.1) or (10.2), h must be equivalent to a form in $S_k^0(p)^\varphi$ or to some f_i or g_i. By Theorem 6 of [1], all eigen forms in $S_k^0(p)^\varphi$ are new forms in $S_k^0(p^2)$, so h must be equivalent to some f_i or g_i. But all g_i are eigen forms for all $T_k(\ell)$, $\ell \neq p$ and for W_p. Further if $g_i(\tau) = \sum_{n=1}^\infty a(n) \exp(n\tau)$, then by Theorem 5.31 (d) or Theorem 5.34 (f), $a(n) = 0$ if $p \mid n$. Thus $g_i \mid U_p = 0$ where U_p is the U operator of Atkin–Lehner (see [1], p. 141). Thus by Theorem 5 of [1], all the g_i are new forms in $S_k^0(p^2)$, so again by Lemma 24 of [1], h must be equivalent to some f_i. Hence a subset $f_{i_1}, \ldots, f_{i_t}$ of the f_i appearing in (10.1) if $k = 2$ or in (10.2) if $k > 2$ form a basis of a subspace of $S_k(p^2)$ which is H-isomorphic to $S_k^0(p)$. This proves (i). Part (ii) follows immediately from Proposition 10.2. Now consider (iii). $g_{i_\nu} = f_{i_\nu} \mid R_p$ by Theorem 5.31 (d) or Theorem 5.34 (f) and they are new forms in $S_k^0(p^2)$ as above. Since R_p is just twisting by $\varphi = \left(\frac{-}{p}\right)$, (iii) is clear. Now consider (iv). It follows from parts (i) and (iii) that (10.1) and (10.2) yield

$$2S_k^0(p^2) \cong \oplus \sum_{\lambda \in \Delta} \langle f_\lambda \rangle \oplus \sum_{\lambda \in \Delta} \langle g_\lambda \rangle \oplus 2S_k(1)^\varphi \oplus 2S_k^0(p)^\varphi \oplus 2 \sum_{\substack{\{\psi\} \\ \psi^2 \neq 1}} S_k(p, \psi^2)^{\bar{\psi}} \tag{10.3}$$

where $\Delta = \{2, \ldots, G\} - \{i_1, \ldots, i_t\}$ if $k = 2$ and $\Delta = \{1, \ldots, r\} - \{i_1, \ldots, i_t\}$ if $k > 2$. A new form in $S_k^0(p^2)$ is just an eigen form for all $T_k(\ell)$, $\ell \neq p$. Each new form in $S_k^0(p^2)$ occurs exactly twice in the L.H.S. of (10.3) hence it occurs exactly twice in the R.H.S. of (10.3) and this proves part (iv). Now consider the case $p \equiv 3 \pmod 4$. The proof of (i') is exactly the same as the proof of part (i) except that we can not say that h is not equivalent to some g_i. Thus we obtain a subset $\{f_{i_1}, \ldots, f_{i_\mu}, g_{i_1}, \ldots, g_{i_\nu}\}$, $\mu + \nu = \dim S_k^0(p)$ which is the basis of a subspace of $S_k(p^2)$ H-isomorphic to $S_k^0(p)$. Consider (ii'). By Theorem 5 of [1], $f_{i_1} \mid R_p$ is a new form in $S_k^0(p^2)$. By Theorems 5.31 (e) or 5.34 (g), $g_{i_1} \sim f_{i_1} \mid R_p$, so by Theorem 5 of [1], $g_{i_1} = f_{i_1} \mid R_p$. Now $g_{i_1} \mid R_p \sim f_{i_1}$, so $g_{i_1} \mid R_p$ is not a new form in $S_k^0(p^2)$. Thus by Theorem 6 (ii) of [1], $g_{i_1} \mid W_p = \left(\frac{-1}{p}\right) g_{i_1} = -g_{i_1}$ so by Proposition 10.2 $f_{i_1} \mid W_p = -f_{i_1}$ also. Similarly for the other f_{i_λ} and g_{i_λ}. For (iii'), we have already shown in (ii') that $g_{i_1} = f_{i_1} \mid R_p$, etc. are all new forms in $S_k^0(p^2)$ and the rest of (iii') is clear. The proof of (iv') is exactly the same as the proof of part (iv).

We now determine the old forms occurring among the f_i and g_j of Theorem 10.1.

THEOREM 10.4: *Let $N = p^2$, p an odd prime and maintain the notation and assumptions of Theorem* 10.3. *Then the subset of old forms occurring among the f_i and g_j is precisely $\{h(\tau) - \lambda'(p)p^{k/2}h(p\tau) \mid h(\tau)$ a new form in $S_k^0(p)\}$. Here $h(\tau) \mid W_p' = \lambda'(p)h(\tau)$ where W_p' is the W_p-operator acting on $S_k(p)$. Note that $\lambda'(p) = \pm 1$. More precisely if $p \equiv 1 \pmod 4$, then every $f_{i_\lambda}(\tau)$ in part* (i) *of Theorem* 10.3 *is of the form $f_{i_\lambda}(\tau) = h(\tau) - \lambda'(p)p^{k/2}h(p\tau)$ for some new form $h(\tau)$ in $S_k^0(p)$ and conversely. If $p \equiv 3(4)$, every $f_{i_\lambda}(\tau)$ and $g_{i_\lambda}(\tau)$ occurring in part* (i') *of Theorem* 10.3 *is of the above form and conversely.*

PROOF: Let $d(\tau)$ be a form occurring in part (i) or (i') of Theorem 10.3. Then $d(\tau)$ is equivalent to some new form $h(\tau)$ in $S_k^0(p)$, so by Theorem 5 of [1], $d(\tau) = ah(\tau) + bh(p\tau)$ for some $a, b \in \mathbb{C}$. As the first Fourier coefficient of $d(\tau)$ is 1 (by Theorem 5.31 (c) or Theorem 5.34 (e)) and the first Fourier coefficient of $h(\tau)$ is also 1 (by definition), we see that $a = 1$. Equation 5.1 on page 149 of [1] shows that the eigen vectors for W_p in the space generated by $h(\tau)$ and $h(p\tau)$ are $c(h(\tau) \pm$

$p^{k/2}h(p\tau)$), $c \in \mathbb{C}^x$ and $c(h(\tau) \pm p^{k/2}h(p\tau))$ has eigen value $\pm\lambda'(p)$. Note that our 'k' is twice Atkin and Lehner's 'k'. As $d(\tau)$ is an eigen form for W_p, we must have $d(\tau) = h(\tau) \pm p^{k/2}h(p\tau)$ and we need only determine the correct sign. But by Theorem 10.3 parts (ii) and (ii'), we know that $d \mid W_p = -d$, hence $\pm\lambda'(p) = -1$, so the correct choice of sign is $-\lambda'(p)$.

REMARK 10.5: Theorems 10.3 and 10.4 effectively determine all the entries of the diagonalized Brandt matrix series $\Sigma_{n=0}^{\infty} B_s'(n; p^2, 1)\exp(n\tau)$ appearing in Theorems 5.31 and 5.34 in the case $N = p^2$ where we can and do assume by Proposition 9.9 and 10.2 that the diagonal entries are also eigen forms for $\tilde{W}_p = -W_p$. If $s = 0$, i.e. if the weight is 2, the diagonal entries consist of the following: the zeta function $f_1(\tau)$, a non cusp form, for orders of level p^2, i.e. $f_1(\tau) = \Sigma_{n=0}^{\infty} b(n)\exp(n\tau)$ where $b(0) = \dfrac{p^2-1}{12}$ is the mass and $b(n)$ is the number of integral left $\mathcal{O}$-ideals of norm n, $\mathcal{O}$ an order of level p^2; another non cusp form, the twist of $f_1(\tau)$ by $\left(\frac{-}{p}\right)$ $g_1(\tau) = \Sigma_{n=0}^{\infty}\left(\frac{n}{p}\right)b(n)\exp(n\tau)$; the forms $h(\tau) - \lambda'(p)ph(p\tau)$ where $h(\tau)$ varies over all new forms of level p in $S_2^0(p)$ and $h(\tau) \mid W_p' = \lambda'(\tau)W_p'$ where W_p' is the W_p-operator on $\Gamma_0(p)$ ($\lambda_p' = \pm 1$); also each new form of level p^2 in $S_2^0(p)^{\varphi}$, $\varphi = \left(\frac{-}{p}\right)$, appears once; and finally each new form in $S_2^0(p^2)$ that is not contained in any $S_2(p, \psi^2)^{\tilde{\psi}}$ or $S_2(1)^{\varphi}$ for any character ψ of $(Z/p)^x$ – i.e. each primitive form in the terminology of Definition 8.6 – appears exactly twice. Note here that of course $S_2(1) = \{0\}$. In the case $s > 0$, i.e. the weight $k = s + 2 > 2$, the story is also the same. In this case all diagonal entries are cusp forms so the zeta function and its twist by the quadratic character $\varphi = \left(\frac{-}{p}\right)$ do not occur. Also if $p = 3$, some of the diagonal entries may be zero. Otherwise we get exactly analogous diagonal entries in the case of weight $k > 2$ as in the case of weight 2 – we just replace 2 everywhere above by k (note that the old forms we obtain are $h(\tau) - \lambda'(p)p^{k/2}h(p\tau)$ where $h(\tau)$ ranges over all new forms in $S_k^0(p)$).

REMARK 10.6: Parts (iv) and (iv') of Theorem 10.3 shows that certain explicit new forms appear with 'multiplicity' 2 when we diagonalize the Brandt matrix series $\Sigma_{n=0}^{\infty} B(n; p^2; 1)\exp(n\tau)$. This may be related to the result of Lebesse and Langlands (see [7]) which

shows that a 'multiplicity one theorem' for the representation theory fails to hold for certain 'inner forms', which come from quaternion algebras, of $SL(2)$.

REFERENCES

[1] A. ATKIN and J. LEHNER: Hecke Operators for $\Gamma_0(m)$. *Math. Ann. 185* (1970) 134–160.

[2] M. EICHLER: Zur Zahlentheorie der Quaternionen-Algebren. *J. reine angew. Math. 195* (1956) 127–151.

[3] M. EICHLER: The Basis problem for modular forms and the traces of the Hecke operators. *Lecture Notes in Math. 320*, Springer-Verlag, pp. 75–151.

[4] S. GELBART: *Automorphic Forms on Adele Groups*, Annals of Math. Studies No. 83, Princeton Univ. Press (1975).

[5] H. HIJIKATA: Explicit formula of the traces of the Hecke operators for $\Gamma_0(N)$: *J. Math. Soc. Japan 26* (1974) 56–82.

[6] H. JACQUET, R. LANGLANDS: *Automorphic Forms on GL(2). Lecture Notes in Math. No. 114*, Springer-Verlag (1970).

[7] J.P. LABESSE and R.P. LANDLANGS: 'L-indistinguishability for SL_2' (preprint) Institute for Advanced Study, Princeton, NJ.

[8] T. LAM: *The Algebraic Theory of Quadratic Forms.* W.A. Benjamin, (1973).

[9] S. LANG: *Algebra.* Addison-Wesley (1971).

[9a] W.W. LI: Newforms and Functional Equations. *Math. Ann. 212* (1975) 285–315.

[10] A. OGG: *Modular Forms and Dirichlet Series*, W.A. Benjamin (1969).

[11] W. PARRY: A negative result on the representation of modular forms by theta series (to appear).

[12] A. PIZER: On the Arithmetic of Quaternion Algebras II. *J. Math. Soc. Japan 28* (1976) 676–688.

[13] A. PIZER: The Representability of Modular Forms by Theta Series. *J. Math. Soc. Japan 28* (1976) 689–698.

[14] A. PIZER: The Action of the Canonical Involution on Modular Forms of Weight 2 on $\Gamma_0(M)$. *Math. Ann. 226* (1977) 99–116.

[15] A. PIZER: An Algorithm for Computing Modular Forms on $\Gamma_0(N)$ (to appear).

[16] I. REINER: *Maximal Orders*, Academic Press (1975).

[17] G. SHIMURA: *Introduction to the Arithmetic Theory of Automorphic Functions*, Princeton Univ. Press (1971).

[18] C. SIEGEL: Uber die analytische Theory der quadratic Formen, Gesammelte Abhandlungen, Band I, Springer-Verlag, (1966).

(Oblatum 21–XI–1977 & 6–II–1979)

Department of Mathematics
University of Rochester
Rochester, NY 14627