JOURNAL OF ALGEBRA 64, 340–390 (1980)

An Algorithm for Computing Modular Forms on $\Gamma_0(N)$*

ARNOLD PIZER

Department of Mathematics, University of Rochester, Rochester, New York 14627

Communicated by N. Jacobson

Received April 15, 1977

INTRODUCTION

A more complete title might be "a survey of the arithmetic of quaternion algebras and their connection with modular forms on $\Gamma_0(N)$ together with an algorithm for computing modular forms on $\Gamma_0(N)$." Consider the modular subgroup $\Gamma_0(N)$ of level N, $\Gamma_0 = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL(2, Z) \mid c \equiv 0 \pmod{N}\}$. It is well-known that there is a close connection between the theory of modular forms of even weight $k \geqslant 2$ on $\Gamma_0(N)$ and the arithmetical theory of rational quaternion algebras. This connection was first noticed by Hecke [18] in 1940 when he conjectured that all cusp forms of weight 2 on $\Gamma_0(p)$, p a prime, are linear combinations of certain (explicit) theta series attached to the norm form of a certain quaternion algebra. Hecke's conjecture (or rather a slightly weakened version of it, the original conjecture being false—see Remark 2.16 below) was proved Eichler [12] in 1956. Eichler's results have now been generalized by Eichler [13, 14], Hijikata and Saito [21], and Pizer [36] so that we now can handle the case of cusp forms of even weight $k \geqslant 2$ on $\Gamma_0(N)$, N not a perfect square. In general, if N is not prime, we do not obtain all cusp forms of given weight on $\Gamma_0(N)$ as linear combinations of (generalized) theta series, but only those cusp forms that lie in a certain subspace (which does however contain all the "newforms"—see Section 2) which can be described (see Corollary 2.29) in terms of the "newforms" and "oldforms" of Atkin and Lehner (see [2]).

The purpose of this paper is to present an explicit algorithm based on the above theory, which is suitable for computer implementation, for computing the subspace of the space of cusp forms on $\Gamma_0(N)$ that is generated by theta series and for computing the matrix representation of the Hecke operators on this subspace. Sections 1 and 2 give a rather complete survey of the relevant theory of quaternion algebras and modular forms. The remainder of the paper

* Research partially supported by NSF grants MCS74-08108A02 and MCS77-03632.

0021-8693/80/060340–51$02.00/0
Copyright © 1980 by Academic Press, Inc.
All rights of reproduction in any form reserved.

is devoted to developing procedures for doing arithmetical calculations in rational quaternion algebras.

A major tool in our algorithm is a procedure for calculating the number of times a positive definite integral quadratic form represents the positive integers 1, 2, 3,... (the so-called representation numbers of the quadratic form). This procedure, which we believe is quite efficient, may be of independent interest. It is given in Section 6. In Section 5, we give a canonical basis for a maximal order in any rational quaternion algebra ramified at precesely one finite prime. This is very well-known for the quaternion algebra ramified precisely at 2 and ∞, ("Hamilton's quaternions with coefficients in Q"), but does not seem to be known in general and may be of interest.

The contents of the sections are as follows. In Section 1 we give a sketch of the algebraic and arithmetic theory of rational quaternion algebras. Section 2 contains a sketch of a little of the theory of modular forms on $\Gamma_0(N)$ and its connection with theta series arising from quaternion algebras. Section 3 gives a sketch of the algorithm and Sections 4 through 8 give in detail the major components of the algorithm. The titles of these sections are: Section 4: Some Needed Procedures; Section 5: Finding an Order of Level N; Section 6: Calculating the Representation Numbers; Section 7: Finding Representatives of the Ideal Classes; Section 8: Calculating the Theta Series and the Brandt Matrices. It is the Brandt matrices that give the action of the Hecke operators (see Section 2). In Section 9 we give several numerical examples computed using the algorithm. These illustrate important points in the theory of Brandt matrices. Also Theorem 9.1 shows that the action of the canonical involution on $S_2(p)$ is given by the Brandt matrix $B_0(p; p, 1)$ and hence is explicitly computable.

From Definition 1.7 on the notational conversion preceding Definition 1.7 will always be in effect, Also we let $\exp(x) = e^{2\pi ix}$ and use this notation throughout the paper.

The algorithm has been implemented in Dec 10 Algol 60 at the Brandeis University Computer Center and also at the Medical Center Computing Facility at the University of Rochester.

1. Quaternion Algebras

Let F denote either the field Q of rational numbers, the field Q_p of p-adic numbers (p a prime), or the field $\mathbb{R}$ of real numbers. A *quaternion algebra* A over F is a central simple algebra of dimension 4 over F. It is well-known (since A contains a field of degree 2 over F) that any quaternion algebra A over F has a basis $1, i, j, k$ over F such that multiplication in A is given in terms of the basis by the following relations: 1 is (obviously) the identity of A, $i^2 = a$, $j^2 = b$, $ij = k = -ji$, where a and b are some nonzero elements of F (see

[7, Chap. 8, Sect. 11, No. 2]). Conversely, given any $a, b \in F^x$ (in general for any ring R, we denote by R^x the invertible elements of R), the above basis and relations define a quaternion algebra over F (see [24, p. 52]). We denote this quaternion algebra by $(a, b)_F$ or more simply by (a, b) if $F = Q$, $(a, b)_p$ if $F = Q_p$, or $(a, b)_\infty$ if $F = \mathbb{R}$. We will be careful so that there should be no confusion as to whether (a, b) denotes the rational quaternion algebra or the greatest common division of a and b. For example $(-1, -1)_\infty$ is Hamilton's quaternions and $(1, 1)$ is just the (quaternion) algebra of 2×2 matrices over Q. All our computations will be done in terms of the basis $1, i, j, k$ of the quaternion algebra $A = (a, b)$.

Unfortunately there does not seem to exist a good reference for the algebraic and arithmetic theory of quaterion algebras that we require. Thus it seems worthwile to sketch the theory we need giving references for most proofs. We begin with the algebraic theory.

If A is a quaternion algebra over Q, we let $A_p = A \otimes_Q Q_p$ which is a quaternion algebra over Q_p. Similarly we let $Q_\infty = \mathbb{R}$, $A_\infty = A \otimes_Q \mathbb{R}$ and call the absolute value on Q the "infinite prime" on Q. If $A = (a, b)$, obviously $A_p = (a, b)_p$. Over Q_p or $\mathbb{R}$ there is up to isomorphism only two quaternion algebras: the 2×2 matrix algebra and a unique quaternion division algebra (see [24, p. 154; 48, p. 184]). We can write $(a, b)_p = 1$ if $(a, b)_p$ is the 2×2 matrix algebra and $(a, b)_p = -1$ if $(a, b)_p$ is the unique quaternion division algebra over Q_p. Similarly for $(a, b)_\infty$. With this convention $(a, b)_p$ becomes the Hilbert symbol (see [24, p. 157]).

Let $A = (a, b)$ be a quaternion algebra over Q. A prime p of Q is said to *ramify* in A if A_p is a division algebra and is said to *split* in A if A_p is the 2×2 matrix algebra. The set of primes ramifying in A is finite and even in number (if we count the infinite prime) because of the product formula for Hilbert symbols $\prod_p (a, b)_p = 1$ for $a, b \in Q^x$ where the product is over all primes p, including ∞ (see [24, p. 181]). Further, the set of ramified primes determines A up to isomorphism and conversely given any set S consisting of an even number of distinct primes, there exists a (unique) quaternion algebra over Q ramified precisely at the primes in S (see [30, Theorems 71.19, 66.6, and 57.8]). Given a and $b \in Q^x$, determining which primes ramify in $A = (a, b)$ is an easy exercise in evaluating Hilbert (or Legendre) symbols (see [24, pp. 164 and 186]). In this paper we will only be concerned with quaternion algebras that ramify at precisely one finite prime (and hence also at ∞). Proposition 5.1 below gives for each finite prime the corresponding algebra.

Let $A = (a, b)_F$. We define *conjugation* on A by the following: if $\alpha = w + xi + yj + zk \in A$, $w, x, y, z, \in F$, then $\bar{\alpha} = w - xi - yj - zk$. Conjugation depends only on A and is independent of the particular choice of a, b used to define A (see [30, p. 145]). Easy calculations show that $\overline{\alpha\alpha} = \alpha\bar{\alpha}$, $\overline{\alpha + \beta} = \bar{\alpha} + \bar{\beta}$, $\bar{\alpha}\bar{\beta} = \bar{\beta}\bar{\alpha}$, $\bar{\bar{\alpha}} = \alpha$, and $\alpha = \bar{\alpha}$ if and only if $\alpha \in F$ for all $a \in F$, $\alpha, \beta \in A$. The (reduced) *norm* N and (reduced) *trace* Tr of A are defined by $N(\alpha) = \alpha\bar{\alpha}$ and $\mathrm{Tr}(\alpha) =$

$\alpha + \bar{\alpha}$. Clearly if $\alpha = w + xi + yj + zk \in A = (a, b)_F$, then $N(\alpha) = w^2 - ax^2 - by^2 + abz^2$ and $\mathrm{Tr}(\alpha) = 2w$. For example if $A = \mathrm{Mat}(2, F)$, then

$$\overline{\begin{pmatrix} a & b \\ c & d \end{pmatrix}} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}, \; N = \det, \text{ and } \mathrm{Tr} = \text{trace}.$$

Note that N can (and will) be viewed as a quadratic form on the four-dimensional vector space A over F. Further if $A = (a, b)$ is a rational quaternion algebra, then N is a positive definite form if and only if ∞ ramified in A if and only if $a < 0$ and $b < 0$.

The above covers the algebraic theory that we need. We now sketch the (less well-known) arithmetic theory. Let A be a quaternion algebra over Q (or Q_p). A *lattice* on A is a free Z (or Z_p) submodule of A of rank 4. An *order* $\mathcal{O}$ of A is a lattice on A which is also a subring containing the identity. For example, Mat(2, Z)is an order of Mat(2, Q). It is easy to see that if α belongs to some order of A, then $\mathrm{Tr}(\alpha)$ and $N(\alpha)$ belong to Z (or Z_p) (see [41, Theorem 10.1]).

Now let $\mathfrak{A}$ be a quaternion algebra over Q. If L is a lattice on $\mathfrak{A}$, we denote by L_p the lattice $L \otimes_Z Z_p$ of $\mathfrak{A}_p$. An order $\mathcal{O}$ of $\mathfrak{A}$ (or of $\mathfrak{A}_p$) is said to be *maximal* if it is not properly contained in any other order of $\mathfrak{A}$ (or $\mathfrak{A}_p$). $\mathcal{O}$ is a maximal order of $\mathfrak{A}$ if and only if $\mathcal{O}_p$ is a maximal order of $\mathfrak{A}_p$ for all $p < \infty$, i.e., for all "finite" or non-Archimedian primes (see [41, Corollary 11.6]). If $\mathfrak{A}_p$ is a division algebra ($p < \infty$), there is a unique maximal order $= \{x \in \mathfrak{A}_p \mid N(x) \in Z_p\}$ (see [41, Theorem 12.8] or the sentence preceding Proposition 1.1 below). If $\mathfrak{A}_p$ is split, then all maximal orders of $\mathfrak{A}_p$ are conjugate to the order $\left(\begin{smallmatrix} Z_p & Z_p \\ Z_p & Z_p \end{smallmatrix}\right)$ by an element of $\mathfrak{A}_p^{\times}$ (see [41, Theorem 17.3]). Also any order is contained in a maximal order (see [41, Corollary 10.4]).

Fix a prime p and let L denote the unique unramified quadratic field extension of Q_p. $L = Q_2(5^{1/2})$ if $p = 2$ and $L = Q_p(u^{1/2})$ for $p > 2$ where $u \in Z$ is a quadratic nonresidue mod p (see [24, p. 161, Corollary 2.24 and p. 151, Remark 2.7]). Consider the Q_p-subalgebra A of Mat(2, L) given by

$$A = \left\{ \begin{pmatrix} \alpha & \beta \\ p\beta^{\sigma} & \alpha^{\sigma} \end{pmatrix} \;\middle|\; \alpha, \beta \in L \right\}, \tag{1.1}$$

where σ denotes conjugation of L/Q_p. A direct calculation shows that A is a quaternion division algebra over Q_p. The norm N and trace Tr of A are respectively the determinant and trace of Mat(2, L) restricted to A. Let R denote the set of integers of L ($R = Z_2 + Z_2((1 + 5^{1/2})/2)$ if $p = 2$ and $R = Z_p + Z_p u^{1/2}$ if $p > 2$ in the above representation of L). A direct calculation shows that

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

is the (unique) maximal order of A since if α belongs to an order, then $N(\alpha) \in Z_p$ which implies $\alpha \in \mathcal{O}$.

PROPOSITION 1.1. *Let $\mathfrak{A}$ be a rational quaternion algebra ramified precisely at $p_1, p_2, \ldots, p_e$, and ∞. Then an order $\mathcal{O}$ of $\mathfrak{A}$ is maximal if and only if* $\operatorname{disc}(\mathcal{O}) = (p_1 \cdots p_e)^2$, *the discriminant being taken respect to the norm form N of $\mathfrak{A}$.*

Proof. $\operatorname{Tr}(x\bar{y}) = N(x + y) - N(x) - N(y)$ is the bilinear form associated to N. If $e_1, \ldots, e_4$ is a Z-basis for a lattice L, then by definition $\operatorname{disc}(L) = \det(\operatorname{Tr}(e_i\bar{e}_j))$. If M is an order, obviously $\operatorname{disc}(M) \in Z$ and $\operatorname{disc}(M) > 0$ as N is positive definite. Thus we need only show (since $\mathcal{O}$ is maximal if and only if $\mathcal{O}_p$ is maximal for all p) that for p split, $\mathcal{O}_p$ is maximal in $\mathfrak{A}_p$ if and only if $\operatorname{disc}(\mathcal{O}_p) = 1 \pmod{U_p^2}$, U_p the units of Z_p and for p ramified, $\mathcal{O}_p$ is maximal in $\mathfrak{A}_p$ if and only if $\operatorname{disc}(\mathcal{O}_p) = p^2 \pmod{U_p^2}$. But easy calculations show that $\operatorname{disc}\left(\begin{smallmatrix} Z_p & Z_p \\ Z_p & Z_p \end{smallmatrix}\right) = 1$ and $\operatorname{disc}(\mathcal{O}_p) = p^2$, where $\mathcal{O}_p = \{\left(\begin{smallmatrix} \alpha & \beta \\ p\beta^\sigma & \alpha^\sigma \end{smallmatrix}\right) \mid \alpha, \beta \in R\}$ is the maximal order of A given by (1.1). This shows the "only if" part. The "if" part then follows from 82.11 of [30] as any order is contained in a maximal order.

DEFINITION 1.2. Fix a prime p. Let $\mathfrak{A}$ be the rational quaternion algebra ramified precisely at p and ∞. Let r be a nonnegative integer and let M be any positive integer prime to p. An order $\mathcal{O}$ of $\mathfrak{A}$ is said to have *level* $N = p^{2r+1}M$ if $\mathcal{O}_q$ is isomorphic over Z_q (i.e., conjugate by an element of $\mathfrak{A}_q^{\times}$) to $\left(\begin{smallmatrix} Z_q & Z_q \\ NZ_q & Z_q \end{smallmatrix}\right)$ for all $q \neq p$ and if $\mathcal{O}_p$ is isomorphic over Z_p to $\{\left(\begin{smallmatrix} \alpha & \beta \\ p^{r+1}\beta^\sigma & \alpha^\sigma \end{smallmatrix}\right) \mid \alpha, \beta \in R\}$ where $\mathfrak{A}_p$ is identified with A as in (1.1) and R is the set of integers in L, the unramified quadratic field extension of Q_p.

Remark 1.3. Any positive integer N, not a perfect square, can be represented as $N = p^{2r+1}M$ for some p and M, $p \nmid M$.

Remark 1.4. The orders defined in Definition 1.2 are maximal if and only if $r = 0$ and $M = 1$. The case $r = 0$ and M square free was first studied by Eichler [11] and are now called Eichler orders. The case $r = 0$ and M arbitrary was studied by Hijikata in [19]. The general case has been studied by Pizer in [35].

Remark 1.5. Let N be a positive integer, not a perfect square. The orders of level N are of interest principally because of their connection with modular forms on $\Gamma_0(N)$. One reason this may be so is because of the following. Consider $\mathcal{O}' = \left(\begin{smallmatrix} Z & Z \\ NZ & Z \end{smallmatrix}\right)$, an order of $\operatorname{Mat}(2, Q)$. Then $\Gamma_0(N)$ is "essentially" (i.e., has index 2 in) the unit group of $\mathcal{O}'$. Now let $N = p^{2r+1}M$, $p \nmid M$ for some prime p. Let $\mathfrak{A}$ be the quaternion algebra over Q ramified precisely at p and ∞ and let $\mathcal{O}$ be an order of level $p^{2r+1}M$ in $\mathfrak{A}$. Then $\mathcal{O}'_q \cong \mathcal{O}_q$ for all $q \neq p$. Further $\mathcal{O}'_p \otimes_{Z_p} R = \left(\begin{smallmatrix} R & R \\ p^{2r+1}R & R \end{smallmatrix}\right) \cong \left(\begin{smallmatrix} R & p^rR \\ p^{r+1}R & R \end{smallmatrix}\right) \cong \mathcal{O}_p \otimes_{Z_p} R$ where R is the ring of integers of L, the unramified quadratic field extension of Q_p. Thus $\mathcal{O}'_p$ and $\mathcal{O}_p$ are both essentially subrings of $\left(\begin{smallmatrix} R & R \\ p^{2r+1}R & R \end{smallmatrix}\right)$ fixed by certain (different!) Galois actions induced by the Galois group of L/Q_p and thus they can be viewed as twisted versions of each other. Hence $\mathcal{O}$ and $\mathcal{O}'$ are locally isomorphic at all primes $q \neq p$ while at p they are almost isomorphic. Thus it should not be too surprising that there are

close connections between theories involving $\mathcal{O}$ and $\mathcal{O}'$. We should note that we do not have to restrict our attention to quaternion algebras which have only one finite ramified prime. We can define orders analogous to those defined in Definition 2.1 for any rational quaternion algebra (definite or not) and the arithmetic of all of these orders is closely connected with the theory of modular forms on $\Gamma_0(N)$ (see [20, 36]). However, as this added generality does not allow us to generate any more modular forms, for simplicity we restrict our attention to the case covered by Definition 1.2.

PROPOSITION 1.6. *Let $\mathfrak{A}$ be as in Definition* 1.2. *An order $\mathcal{O}$ of $\mathfrak{A}$ has level $p^{2r+1}M$ if and only if*

(i) $\operatorname{disc}(\mathcal{O}) = (p^{2r+1}M)^2$,

(ii) *$\mathcal{O}_p$ contains a subring isomorphic over Z_p to R, the integers in L, the unramified quadratic field extension of Q_p, and*

(iii) *$\mathcal{O}_q$ contains a subring isomorphic over Z_q to $Z_q \times Z_q$ for all primes $q \mid M$.*

Proof. Assume $\mathcal{O}$ has level $p^{2r+1}M$. Then (ii) and (iii) are obvious and (i) is shown by easy local calculations after Proposition 1.1. Conversely, by [35, Proposition 2; 19, 2.2 on p. 65], (ii) and (iii) imply that $\mathcal{O}$ is an order of level $p^{2s+1}M'$ for some s and M', $p \nmid M'$. Then (i) implies $s = r$ and $M' = M$.

For the remainder of this paper fix a positive integer N, not a perfect square, and a prime p such that $N = p^{2r+1}M$ with $p \nmid M$. $\mathfrak{A}$ will then always denote the quaternion algebra over Q ramified precisely at p and ∞. An order of level N will always mean an order of level $p^{2r+1}M$ in $\mathfrak{A}$.

DEFINITION 1.7. Let $\mathcal{O}$ be an order of level N in $\mathfrak{A}$. A *left $\mathcal{O}$-ideal* I is a lattice on $\mathfrak{A}$ such that $I_p = \mathcal{O}_p a_p$ (for some $a_p \in \mathfrak{A}_p^{\times}$) for all $p < \infty$. Two left $\mathcal{O}$-ideals I and J are said to belong to the same *class* if $I = Ja$ for some $a \in \mathfrak{A}^{\times}$. One has the obvious analogous definitions for *right $\mathcal{O}$-ideals*.

DEFINITION 1.8. The *class numbers* of left ideals for any order $\mathcal{O}$ of level $N = p^{2r+1}M$ is the number of distinct classes of such ideals. We denote this class number by $H(p^{2r+1}M)$.

DEFINITION 1.9. The *type number* of orders of level $N = p^{2r+1}M$ in $\mathfrak{A}$ is the number of distinct isomorphism classes of orders of level N in $\mathfrak{A}$. We denote the type number by $T(p^{2r+1}M)$.

THEOREM 1.10. *The class number $H(p^{2r+1}M)$ is finite and independent of the particular order of level $N = p^{2r+1}M$ used in its definition. Further the type number always satisfies $T(p^{2r+1}M) \leqslant H(p^{2r+1}M)$.*

Proof. This is classical for maximal orders (see Artin [1] and Eichler [10]). For the general case see Pizer [37, Propositions 2.13 and 2.15]. See also Proposition 1.21 below.

Remark 1.11. Explicit formulas for the class and type numbers exist. For $H(pM)$, M square free see Eichler [11]; for $H(pM)$, M arbitrary see Pizer [34]; for $T(p1)$ see Deuring [9]; for $T(pM)$, M square free see Pizer [33] or Peters [32]; and for $T(pM)$, M arbitrary see Pizer [34]. A formula for the type number in the most general case is not yet known. However the class number formula is known in the general case. As we need that result, we record it here as:

THEOREM 1.12. *Let p be a prime and M a positive integer prime to p. Let r be a nonnegative integer. Let $\mathcal{O}$ be an order of level $N = p^{2r+1}M$ in the quaternion algebra over Q ramified precisely at p and ∞. Then the class number $H(p^{2r+1}M)$ of left $\mathcal{O}$-ideals is given by*

$$H(p^{2r+1}M) = \frac{N}{12}\left(1-\frac{1}{p}\right)\prod_{q|M}\left(1+\frac{1}{q}\right) + \begin{cases} \frac{1}{4}\left(1-\left(\frac{-4}{p}\right)\right)\prod_{q|M}\left(1+\left(\frac{-4}{q}\right)\right) & \text{if } 4 \nmid N \\ 0 & \text{if } 4 \mid N \end{cases} + \begin{cases} \frac{1}{3}\left(1-\left(\frac{-3}{p}\right)\right)\prod_{q|M}\left(1+\left(\frac{-3}{q}\right)\right) & \text{if } 9 \nmid N \\ 0 & \text{if } 9 \mid N. \end{cases}$$

Here the product is over all distinct primes q dividing M and $(*/*)$ is the Kronecker symbol. In particular $(-4/2) = (-3/3) = 0$ and $(-3/2) = -1$.

Proof. The Brandt matrix $B_0(1; p^{2r+1}, M)$, see Definition 2.13 below, is the $H \times H$ ($H = H(p^{2r+1}M)$) identity matrix (see Remark 2.20 below). Hence $H = \mathrm{Tr}(B_0(1; p^{2r+1}, M))$ and we need only employ the general trace formula for Brandt matrices given by Theorem 26 of Pizer [35].

Remark 1.13. Note the similarity of the formula for the class number with the formula for the dimension of the space of cusp forms of weight 2 on $\Gamma_0(N)$ (=genus of $H^*/\Gamma_0(N)$), see Ogg [29, Chap. IV, Proposition 14]. The reason for this is given by Corollary 2.29 below.

DEFINITION 1.14. Let I be a (left or right) $\mathcal{O}$-ideal for some order $\mathcal{O}$ of level N in $\mathfrak{A}$. The *left order* of $I = \{a \in \mathfrak{A} \mid aI \subseteq I\}$ and the *right order* of $I = \{a \in \mathfrak{A} \mid Ia \subseteq I\}$.

Remark 1.15. If I is an ideal of an order of level N, then its left and right orders have level N (see [37, Definition 2.14 and following]). Also if I is a left $\mathcal{O}$-ideal, its left order is obviously $\mathcal{O}$ and similarily for right ideals.

DEFINITION 1.16. The *norm* of an ideal, denoted by $N(I)$, is the positive rational number which generates the fractional ideal of Q generated by $\{N(a) \mid a \in I\}$. The *conjugate* of an ideal I, denoted by $\bar{I}$, is given by $\bar{I} = \{\bar{a} \mid a \in I\}$. The *inverse* of an ideal, denoted by I^{-1}, is given by $I^{-1} = \{a \in \mathfrak{A} \mid IaI \subseteq I\}$.

The set of ideals, left and right, attached to all orders of (a fixed) level N in $\mathfrak{A}$ form a Brandt grouppoid (see [41, p. 201]). If we have two ideals I and J with the right order of I equal to the left order of J, then IJ (=all finite sums $\sum_k i_k j_k$ with $i_k \in I$, $j_k \in J$) is an ideal with left order equal to the left order of I and right order equal to the right order of J (see [41, p. 201]). Relations which hold among the above concepts are given by:

PROPOSITION 1.17. *Let $\mathcal{O}$ be an order of level N. Let I be a left $\mathcal{O}$-ideal with right order $\mathcal{O}'$. Then*

(a) *$\bar{I}$ is a left $\mathcal{O}'$-ideal with right order $\mathcal{O}$ and $N(\bar{I}) = N(I)$.*

(b) *I^{-1} is a left $\mathcal{O}'$-ideal with right order $\mathcal{O}$ and $N(I^{-1}) = N(I)^{-1}$*

(c) *$II^{-1} = \mathcal{O}$ and $I^{-1}I = \mathcal{O}'$*

(d) *$I\bar{I} = \mathcal{O}N(I)$ and $\bar{I}I = \mathcal{O}'N(I)$.*

(e) *$I^{-1} = \bar{I}/N(I)$*

(f) *if J is a left $\mathcal{O}'$-ideal, then $N(IJ) = N(I)\,N(J)$.*

Proof. These facts are almost obvious. For help with the proofs one can see [37].

PROPOSITION 1.18. *Let I and J be left $\mathcal{O}$-ideals. Then I and J belong to the same class if and only if there exists an element $\alpha \in \bar{J}I$ such that $N(\alpha) = N(I)\,N(J)$.*

Proof. Let $\mathcal{O}'$ be the right order of J. Assume I and J belong to the same class, i.e., there is a $\beta \in \mathfrak{A}^\times$ such that $I = J\beta$. Note that $N(\beta) = N(I)/N(J)$. Then $\bar{J}I = \bar{J}J\beta = \mathcal{O}'(N(J)\beta)$. Thus $\alpha = N(J)\beta \in \bar{J}I$ and $N(\alpha) = N(J)^2\,N(I)/N(J) = N(I)\,N(J)$. Conversely if $\alpha \in \bar{J}I$ with $N(\alpha) = N(I)\,N(J) = N(\bar{J})\,N(I) = N(\bar{J}I)$, then $\mathcal{O}'\alpha \subseteq \bar{J}I$ and $N(\mathcal{O}'\alpha) = N(\bar{J}I)$. Then an easy local calculation (see, e.g., [37]) shows that $\mathcal{O}'\alpha = \bar{J}I$. Hence $N(J)I = J\bar{J}I = J\mathcal{O}'\alpha = J\alpha$ and $I = J\beta$ with $\beta = \alpha/N(J)$.

Remark 1.19. All elements of $\bar{J}I$ have norm divisible by $N(I)\,N(J)$ so that an α as in Proposition 1.18, if it exists, would be a nonzero element of $\bar{J}I$ of minimal possible norm. Thus our procedure REPRESENTATION. NO (see Section 6) will quickly determine whether or not such an α exists.

Note that in the proof of Proposition 1.18 we have also proved

COROLLARY 1.20. *A left $\mathcal{O}$-ideal I contains an element α with $N(\alpha) = N(I)$ if and only if I is in the same class as $\mathcal{O}$ (in fact if and only if $I = \mathcal{O}\alpha$).*

PROPOSITION 1.21. *Let $\mathcal{O}$ be an order of level N in $\mathfrak{A}$. Let $I_1,\ldots, I_H$ be a complete set of representatives of all the distinct left $\mathcal{O}$-ideal classes. Let $\mathcal{O}_j$ be the right order of I_j, $j = 1,\ldots, H$. Then $I_j^{-1}I_1,\ldots, I_j^{-1}I_H$ is a complete set of representatives of all the distinct left $\mathcal{O}_j$-ideal classes (for $j = 1,\ldots, H$). Further, the $\mathcal{O}_j$ represent (with possible duplication) all the types (i.e., conjugacy classes by elements of $\mathfrak{A}^x$) of orders of level N in $\mathfrak{A}$.*

Proof. See Propositions 2.13 and 2.15 of [37].

2. MODULAR FORMS ON $\Gamma_0(N)$ AND THEIR CONNECTION WITH QUATERNION ALGEBRAS

There are many good references for the theory of modular forms on $\Gamma_0(N)$. For example Ogg [29], Shimura [46], Atkin–Lehner [2], Schoeneberg [43], Gelbart [15], Gunning [16], and Serre [44]. Thus we can and will be very brief in our description of this part of the theory. The connections with quaternion algebras are less well-known (the best reference being Eichler [14]) and we will explain this more fully.

Let $H = \{\tau \in \mathbb{C} \mid \mathrm{Im}(\tau) > 0\}$ denote the complex upper half plane and let $H^* = H \cup Q \cup \{i\infty\}$, i.e., H^* consists of all complex numbers with imaginary part > 0, the rational numbers on the real axis and, a point $i\infty$ at infinity. $\Gamma = \Gamma_0(N) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL(2, Z) \mid c \equiv O(N)\}$ acts on H^* by fractional linear transformations: $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ sends τ to $(a\tau + b)/(c\tau + d)$. $Q \cup \{i\infty\}$ are the *cusps* of $\Gamma = \Gamma_0(N)$. We will continue to write Γ for $\Gamma_0(N)$ if there is no confusion. Modular forms on Γ are certain functions on H that behave nicely with respect to the action of Γ. Specifically, we have (see Gelbart [15, p. 4])

DEFINITION 2.1. A *modular form* $f(\tau)$ of *weight* k ($k \in Z$, $k \geqslant 0$) on $\Gamma_0(N)$ is a complex-valued function on H such that

(i) f is holomorphic on H,

(ii) f is holomorphic at every cusp of $\Gamma_0(N)$, i.e., on $Q \cup \{i\infty\}$, and

(iii) $f((a\tau + b)/(c\tau + d)) = (c\tau + d)^k f(\tau)$ for all $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(N)$.

The complex vector space of all modular forms of weight k on $\Gamma_0(N)$ is denoted by $M_k(N)$.

We explain the meaning of (ii) above. Note that by (iii), $f(\tau) = f(\tau + 1)$ for all τ and hence the function $\hat{f}(q) = f(\tau)$ with $q = \exp(\tau)$ $(= e^{2\pi i\tau})$ is well-defined for $0 < |q| < 1$ and is holomorphic in the punctured disc $0 < |q| < 1$ by (i). To say that $f(\tau)$ is "holomorphic at the cusp $i\infty$" means that $\hat{f}(q)$ can be extended to a holomorphic function at $q = 0$. Note that the map $\tau \mapsto q$ "sends" $i\infty$ to 0. As any rational point on the real axis is sent to $i\infty$

by some element of $SL(2, Z)$, we can translate the above to obtain the meaning of "$f(\tau)$ is holomorphic at a cusp" (see [15]).

Remark 2.2. If k is odd, then by (iii) $f(\tau) = f((-\tau + 0)/(0 - 1)) = -f(\tau)$. Hence, nonzero modular forms can exist on $\Gamma_0(N)$ only if k is even. Henceforth we assume this. The reader is warned that different authors mean different things by "the weight of a modular form" (and some call it the "dimension"). One is usually safe in assuming the weight means one of $\pm k$, $\pm k/2$ (with respect to our k), but beyond this one should be careful.

Assume $f(\tau)$ is a modular form on $\Gamma_0(N)$. Hence $f(\tau)$ is holomorphic at $i\infty$, i.e., $\hat{f}(q)$ is holomorphic at 0. The Taylor series expansion of $\hat{f}(q)$ at 0, $\hat{f}(q) = \sum_{n=0}^{\infty} a_n q^n$ is called the *Fourier series expansion of f at the cusp $i\infty$* (or the q expansion of f). a_n is called the nth Fourier coefficient of f (at $i\infty$). It is by computing these Fourier coefficients of f (up to some limit) that we will "compute" the modular form f. By sending a cusp to $i\infty$ by means of an element of $SL(2, Z)$, we obtain the notion of the Fourier series expansion of a modular form at any cusp (see [15, p. 6]).

DEFINITION 2.3. A modular form f (of any weight) on $\Gamma_0(N)$ is called a *cusp form* if it vanishes at every cusp, i.e., if its zeroth Fourier coefficient is zero in the Fourier series expansion of f at every cusp.

The space of cusp forms of weight k on $\Gamma_0(N)$ is denoted by $S_k(N)$.

In studying modular forms one is primarily interested in the space of cusp forms $S_k(N)$. This is because $M_k(N) = S_k(N) \oplus E_k(N)$ where $E_k(N)$ is the space of Eisenstein series, at least if $k > 2$ (see Schoeneberg [43, Chap. VII, Theorems 4 and 9]) and one feels "that we know" Eisenstein series reasonably well.

The major tool in the study of cusp forms is the notion of the *Hecke operators* $T_k(n)$. For each $n > 0$, $(n, N) = 1$ one has the Hecke operator $T_k(n)$ which is a linear mapping on the space $S_k(N)$. The Hecke operators bear the same relation to the theory of cusp forms as the concept of an Euler product does to the theory of Dirichlet series (see [29]). For the definition of the Hecke operators see Atkin–Lehner [2] or Shimura [46]. One has the major

THEOREM 2.4 (Hecke–Petersson). *The Hecke operators $T_k(n)$, $(n, N) = 1$ acting on $S_k(N)$ generate a commutative, semisimple ring. Thus there exists a basis $f_i(\tau)$, $1 \leqslant i \leqslant \dim S_k(N)$, of $S_k(N)$ consisting of eigen functions for all $T_k(n)$, $(n, N) = 1$.*

Proof. See [2, Lemmas 13 and 15, and Theorem 2].

Let N be a positive integer. Let M be a positive integer dividing N and let d be a positive integer dividing the quotient N/M. As $\Gamma_0(N) \subseteq \Gamma_0(M)$, any cusp form $f(\tau)$ on $\Gamma_0(M)$ is a cusp form on $\Gamma_0(N)$ (see [13, p. 7] or [2, p. 135]). Further $f(d\tau)$ is also a cusp form on $\Gamma_0(N)$ (see [2, p. 145]). Let $C^-(N)$ denote the sub-

space of $S_k(N)$ spanned by all $f(d\tau)$ where $f(\tau)$ is a cusp form on some $\Gamma_0(M)$ with M a (positive) proper divisor of N and d any (positive) divisor of N/M. Denote by $S_k^0(N)$ the orthogonal complement of $C^-(N)$ in $S_k(N)$ with respect to the Petersson inner product (see [2, Eq. 1.3]) on $S_k(N)$. (See Atkin–Lehner [2, p. 145].) Following Atkin and Lehner we call $S_k^0(N)$ the *space of newforms* on $\Gamma_0(N)$. A *newform* on $\Gamma_0(N)$ is an element of $S_k^0(N)$ which is an eigenfunction for all the Hecke operators. A major result of Atkin and Lehner is

THEOREM 2.5.

$$S_k(N) = \bigoplus \sum_{M|N} \sum_{d|N/M} S_k^0(M)^d,$$

the direct sum being over all (positive) divisors M of N and d of N/M. Here if $S_k^0(M)$ is generated by $f_1(\tau),\ldots, f_r(\tau)$, then $S_k^0(M)^d$ is the space generated by $f_1(d\tau),\ldots, f_r(d\tau)$.

Proof. See Theorem 5 of [2].

We now give the connection with quaternion algebras. Let $Q(x)$ be a positive definite integral quadratic form in an even number $r = 2k$ of variables. Integral means that $Q(x) \in Z$ for all $x \in Z^r$. Such a form can always be written as $Q(x) = \frac{1}{2}x^tAx$, where $x^t = (x_1,\ldots, x_n)$ and $A = (a_{ij})$ is a positive definite symmetric matrix with $a_{ij} \in Z$ and $a_{ii} \equiv 0 \pmod 2$. In fact A is just the matrix of the bilinear form $(x, y) = Q(x + y) - Q(x) - Q(y)$. A is called the matrix *associated* to Q. Recall that $\operatorname{disc}(Q) = (-1)^k \det(A)$.

DEFINITION 2.6. Let Q and A be as above. The *level* (or Stufe) of Q (or A) is the least positive integer N such that the matrix NA^{-1} has integer entries with diagonal entries even integers. $Q^*(x) = \frac{1}{2}x^tNA^{-1}x$ is called the *adjoint* form to Q.

Remark 2.7. One easily sees that the level of A is equal to the level of U^tAU for any matrix $U \in GL(r, Z)$.

Let $P(x) = P(x_1,\ldots, x_r)$ be a homogeneous harmonic polynomial of degree ν in $r = 2k$ variables. Harmonic means that $p(x)$ satisfies Laplace's equation $\Delta p(x) = (\partial^2/\partial x_1^2 + \cdots + \partial^2/\partial x_r^2)\, p(x) = 0$. Further let $Q(x)$ be a positive definite integral quadratic form in r variables with $Q(x) = \frac{1}{2}x^tAx$ as above. As $Q(x)$ can be diagonalized over $\mathbb{R}$, there exists a real matrix S such that $(S^{-1})^t\, AS^{-1} = I$ or $A = S^tS$. With this we have the

DEFINITION 2.8. *Let Q, S, and P* be as above. The (generalized) *theta series* attached to Q and P is

$$\theta(\tau, Q, P) = \sum_{n \in Z^r} P(Sn) \exp(Q(n)\tau). \tag{2.1}$$

Recall that $\exp(x) = e^{2\pi i x}$.

Remark 2.9. If $P(x)$ is a constant, then our theta series are "regular" or "nongeneralized" theta series. The generalized theta series were first studied by Schoenberg [42]. The important result is that they are modular forms of weight $k + \deg(P) = r/2 + \deg(P)$ on $\Gamma_0(N)$, $N =$ level of Q, but with a character (see Ogg [29, Chap. VI]). In the case we will consider, this character is trivial (see Theorem 2.14 below).

The harmonic polynomials of Definition 2.8 will in our case arise as follows. Let A be Hamilton's quaternions. Then in analogy with (1.1), A can be represented as the subalgebra of Mat(2, $\mathbb{C}$) given by $A = \{\left(\begin{smallmatrix} z & w \\ -\bar{w} & \bar{z} \end{smallmatrix}\right) \mid z, w \in \mathbb{C}\}$ where the overbar denotes conjugation of $\mathbb{C}$ over $\mathbb{R}$. In this representation a basis of A is given by $1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$, $I = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$, $J = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, and $K = \left(\begin{smallmatrix} 0 & i \\ i & 0 \end{smallmatrix}\right)$. This gives a representation Φ of A^x on $V = \mathbb{C}^2$. Following Eichler [14] we denote by X_1 the corresponding matrix representation in terms of the canonical basis $e_1 = (1, 0)$ and $e_2 = (0, 1)$ of V: $X_1(x_1 + x_2 I + x_3 J + x_4 K) = \left(\begin{smallmatrix} z & w \\ -\bar{w} & \bar{z} \end{smallmatrix}\right)$ with $z = x_1 + x_2 i$ and $w = x_3 + x_4 i$. $\Phi = \Phi_1$ induces a representation Φ_s of A^x on the sth symmetric power $\mathrm{Sym}_s(V)$ of V. $\mathrm{Sym}_s(V) = V \otimes \cdots \otimes V/K$, the product s times with K the "symmetric kernal." A basis for $\mathrm{Sym}_s(V)$ is given by the set of elements $\{e_1 \otimes \cdots \otimes e_1 \otimes e_2 \otimes \cdots \otimes e_2 \pmod K\}$ which we write as $\{e_1^i e_2^{s-i} \mid i = 0,..., s\}$ (where we can consider the product as being in the Tensor algebra (or rather symmetric algebra) if we wish). Then the representation Φ_s is given by

$$\Phi_s(\alpha)(e_1 \otimes \cdots \otimes e_1 \otimes e_2 \otimes \cdots \otimes e_2) = (\Phi_1(\alpha)\, e_1) \otimes \cdots \otimes (\Phi_1(\alpha)\, e_1) \otimes (\Phi_1(\alpha)\, e_2) \otimes \cdots \otimes (\Phi_1(\alpha)\, e_2),$$

all read modulo K. The corresponding matrix representation of A^x with respect to the basis $\{e_1^i e_2^{s-i} \mid i = 0,..., s\}$ we denote by X_s. Thus X_s is a $s + 1$-dimensional representation. We denote by X_0 the trivial one-dimensional representation of A^x. With this we have

PROPOSITION 2.10. *The entries of the matrix $X_s(\alpha) = X_s(x_1 + x_2 I + x_3 J + x_4 K)$ are harmonic homogeneous polynomials $p(x_1,..., x_4)$ of degree s.*

Proof. In terms of the matrix representation $\alpha = \left(\begin{smallmatrix} z & w \\ -\bar{w} & \bar{z} \end{smallmatrix}\right)$, $\Phi_1(\alpha)\, e_1 = z e_1 + w e_2$, and $\Phi_1(\alpha)\, e_2 = -\bar{w} e_1 + \bar{z} e_2$. Thus $\Phi_s(\alpha)(e_1^i e_2^{s-i}) = (z e_1 + w e_2)^i \times (-\bar{w} e_1 + \bar{z} e_2)^{s-i}$. We must expand this last expression and show that the coefficients of $e_1^j e_2^{s-j}$ satisfy Laplace's equation for $j = 0,..., s$. However, this is very easy to do without expanding by treating e_1 and e_2 formally as variables and then just checking that $\Delta((z e_1 + w e_2)^i(-\bar{w} e_1 + \bar{z} e_2)^{s-i}) = 4(\partial^2/\partial z \partial \bar{z} + \partial^2/\partial w \partial \bar{w})((z e_1 + w e_2)^i(-\bar{w} e_1 + \bar{z} e_2)^{s-i}) = 0$. Here $\partial/\partial z = \frac{1}{2}(\partial/\partial x_0 - i\, \partial/\partial x_1)$, $\partial/\partial \bar{z} = \frac{1}{2}(\partial/\partial x_0 + i\, \partial/\partial x_1)$, etc. (see [17, p. 4] and [14, p. 104]).

PROPOSITION 2.11. *Let I be a left $\mathcal{O}$-ideal for some order $\mathcal{O}$ of level $N = p^{2r+1}M$ in a (positive definite) quaternion algebra $\mathfrak{A}$ over Q. Then the quadratic*

form $N(x)/N(I)$ for $x \in I$ is a positive definite integral quadratic form with level N and discriminant N^2.

Remark 2.12. What this means is the following. Let $e_1, \ldots, e_4$ be any Z-basis for I. Then $Q(x_1, \ldots, x_4) = N(x_1e_1 + \cdots + x_4e_4)/N(I)$ is a positive definite integral quadratic form with level N and discriminant N^2. Since any other Z-basis of I is obtained from $e_1, \ldots, e_4$ by operating on $(e_1, \ldots, e_4)$ by a matrix $U \in GL(4, Z)$, the level (see Remark 2.7) and discriminant are independent of which particular Z-basis of I we choose.

Proof. $Q(x) = N(x)/N(I)$ is positive definite since $\mathfrak{A}_\infty$ is Hamilton's quaternions and the norm form there is positive definite. Q is integral since by definition $N(I) \mid N(x)$ for all $x \in I$. Let A be the matrix associated to $Q(x)$. We first show that the level is N. As the level is a positive integer, we need only determine the level locally at all primes of $q < \infty$. First consider the case $q \neq p$. Then $I_q = \mathcal{O}_q\beta$ for some $\beta \in \mathfrak{A}_q{}^x = GL(2, Q_p)$. By Definition 1.2,

$$\mathcal{O}_q = \alpha \begin{pmatrix} Z_q & Z_q \\ NZ_q & Z_q \end{pmatrix} \alpha^{-1}$$

for some $\alpha \in GL(2, Q_q)$. Let $e_1 = \left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$, $e_2 = \left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$, $e_3 = \left(\begin{smallmatrix} 0 & 0 \\ N & 0 \end{smallmatrix}\right)$, and $e_4 = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Then $\alpha e_i \alpha^{-1}\beta$, $i = 1, \ldots, 4$ gives a Z_q-basis for I_q. Note that by Remark 2.12, read locally, we can choose any basis of I_q we wish! Further $N(I) = N(\beta)$ (mod U_q). Then the matrix A is of the form $A = U^tBU$ where $U \in GL(2, Z_q)$ and

$$\begin{aligned} B &= \frac{1}{N(\beta)} \operatorname{Tr}((\alpha e_i \alpha^{-1}\beta)(\overline{\alpha e_j \alpha^{-1}\beta})) \\ &= \frac{1}{N(\beta)} \operatorname{Tr}(\beta\bar{\beta}\alpha^{-1}\bar{\alpha}^{-1}\alpha\, e_i\bar{e}_j\alpha^{-1}\alpha\bar{\alpha}) \\ &= \operatorname{Tr}(e_i\bar{e}_j)) \\ &= \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -N & 0 \\ 0 & -N & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \end{aligned}$$

which has level N in Z_q. Hence by Remark 2.7, A has level N (mod U_q) in Z_q. For the case $q = p$, we have $I_p = \mathcal{O}_p\beta$ for some $\beta \in \mathfrak{A}_p{}^x$. Here $\mathcal{O}_p$ is conjugate to $\{\left(\begin{smallmatrix} p^r+1\delta^\sigma & p^r\delta \\ \gamma & \gamma^\sigma \end{smallmatrix}\right) \mid \gamma, \delta \in R\}$ (see Definition 1.2). Thus using the fact that $R = Z_p \oplus Z_pu^{1/2}$ where $u \in Z$, u a quadratic nonresidue mod p if $p \neq 2$ and $R = Z_2 + Z_2((1 + 5^{1/2})/2)$ if $p = 2$, a calculation exactly analogous to the one above shows that A has level N (mod U_p) in Z_p also. Thus the level must be N. Now for the discriminant. Proposition 1.6 shows that if $I = \mathcal{O}$, then $\operatorname{disc}(Q) = N^2$ as required. We can assume (by multiplying I by some integer if necessary)

that $I \subseteq \mathcal{O}$. Let $e_1, \ldots, e_4$ be a Z-basis of $\mathcal{O}$, $f_1, \ldots, f_4$ a Z-basis of I, and M the matrix such that $M(e_1, \ldots, e_4)^t = (f_1, \ldots, f_4)^t$. Then $N(I)^2 = \det(M)$ (see [8, pp. 10 and 14] and recall that the determinant of the regular representation of $\mathfrak{A}$ is the square of the reduced norm N). Thus $\operatorname{disc}(Q) = \operatorname{disc}(N(x)/N(I) \text{ on } I) = 1/N(I)^4 \operatorname{disc}(N(x) \text{ on } I) = 1/N(I)^4(\det(M))^2 \operatorname{disc}(N(x) \text{ on } \mathcal{O}) = N^2$. Alternatively, if one does not like and/or believe this proof, the discriminant can be calculated by a series of local computations analogous to those performed in Proposition 1.1 and in the level computation above. This completes the proof of Proposition 2.11.

We are now able to define the Brandt matrices which are the central objects of the theory. Let $\mathcal{O}$ be an order of level $N = p^{2r+1}M$, $p \nmid M$, in a quaternion algebra $\mathfrak{A}$ over Q ramified precisely at p and ∞. Let $I_1, \ldots, I_H$, $H = H(p^{2r+1}M)$, be representatives of all the distinct left $\mathcal{O}$-ideal classes. Let $\mathcal{O}_j$ be the right order of I_j and let e_j denote the number of units of $\mathcal{O}_j$ ($u \in \mathcal{O}_j$ is a unit if and only if $N(u) = 1$. Thus e_j is just the number of times the positive definite quadratic form $N(x)$, $x \in \mathcal{O}_j$ represents 1 and hence e_j is finite. In fact $e_j \leqslant 24$ and is "usually" 2.). Let $s \geqslant 0$ and let X_s be the matrix representation of $\mathfrak{A}^\times$ given in Proposition 2.10. For any positive integer n and $1 \leqslant i, j \leqslant H$, $H = H(p^{2r+1}M)$, let

$$b_{ij}^s(n) = e_j^{-1} \sum X_s^t(\alpha), \tag{2.2}$$

where the sum is over all $\alpha \in I_j^{-1}I_i$ with $N(\alpha) = nN(I_i)/N(I_j)$ and the superscript t denotes "transpose." The $b_{ij}^s(n)$ are $s+1$ by $s+1$ matrices. Further let $b_{ij}^0(0) = 1/e_j$ and $b_{ij}^s(0) = 0$ for $s > 0$.

DEFINITION 2.13. Let the notation be as above and let s be a nonnegative integer. The *Brandt matrices* $B_s(n; p^{2r+1}, M)$ for $n \geqslant 0$ are given by

$$B_s(n; p^{2r+1}, M) = (b_{ij}^s(n)).$$

Thus the $B_s(n; p^{2r+1}, M)$ are $H(s+1) \times H(s+1)$ matrices where $H = H(p^{2r+1}M)$. They are divided into H^2 blocks each block being an $s+1$ by $s+1$ matrix. The ith, jth block is the matrix $b_{ij}^s(n)$.

THEOREM 2.14. *The entries of the Brandt matrix series.*

$$\Theta_s(\tau; p^{2r+1}, M) = \sum_{n=0}^{\infty} B_s(n; p^{2r+1}, M) \exp(n\tau) \tag{2.3}$$

are modular forms of weight $s+2$ on $\Gamma_0(N)$. If $s > 0$, they are cusp forms. Here $N = p^{2r+1}M$.

Proof. Fix an entry, say in the ith, jth block and let $p(x_1,\dots,x_4) = p(x_1 + x_2I + x_3J + x_4K)$ be the corresponding polynomial entry of X_s in the notation of Proposition 2.10. Then the entry of the Brandt matrix series which we are considering is given by

$$\theta(\tau) = e_j^{-1} \sum_{\alpha \in I_j^{-1}I_i} p(\alpha) \exp(\tau N(\alpha)\, N(I_j)/N(I_i)). \tag{2.4}$$

Let $f_1,\dots,f_4$ be a Z-basis for $I_j^{-1}I_i$ and let $Q(x) = N(x_1f_1 + \cdots + x_4f_4) \times N(I_j)/N(I_i)$ for $x \in Z^4$. Let $A = (a_{ij})$ be the matrix associated to $Q(x)$, i.e., $a_{ij} = \mathrm{Tr}(f_i\bar{f}_j)\, N(I_j)/N(I_i)$. Let $q_1 = 1$, $q_2 = I$, $q_3 = J$, $q_4 = K$ be the canonical basis of $\mathfrak{A} \otimes_Q \mathbb{R}$ as in Proposition 2.10 and let $T = (t_{ij})$ be the matrix which takes $\{q_i\}$ to $\{f_i\}$, i.e., $f_j = \sum_i t_{ij}q_i$. Then an easy calculation shows that $A = 2N(I_j)/N(I_i)\, T^tT$ or $A = S^tS$ with $S = aT$, $a = (2N(I_j)/N(I_i))^{1/2}$. Now if $x_1f_1 + \cdots + x_4f_4 = y_1q_1 + \cdots + y_4q_4$, then $Tx = y$. Thus (2.4) can be rewritten as

$$\begin{aligned}\theta(\tau) &= e_j^{-1} \sum_{x \in Z^4} p(Tx) \exp(\tau Q(x)) \\ &= e_j^{-1}a^{-s} \sum_{x \in Z^4} p(Sx) \exp(\tau Q(x))\end{aligned}$$

as $p(x)$ is a homogeneous polynomial of degree s. Theorem 20 of Ogg [29, p. VI-22] then shows that $\theta(\tau)$ is a modular form of weight $2 + s$ on $\Gamma_0(N)$. Note that $P(Sx)$ for $x \in \mathbb{R}^4$ is a spherical function with respect to $Q(x)$ in the notation of Ogg [29, p. VI-5]. The level of $\theta(\tau)$ is N since by Proposition 2.11, the level of $Q(x)$ is N. The character associated to $\theta(\tau)$ by Theorem 20 of [29] is trivial since by Proposition 2.11, $\mathrm{disc}(Q(x)) = N^2$ and Theorem 20$^+$ of [29] shows that the character $\epsilon(d) = (\mathrm{sgn}(d))^2(N^2/d) = 1$. Thus $\theta(\tau)$ is a modular form on $\Gamma_0(N)$ in the sense of Definition 2.1. Finally, Theorem 20 of [29] shows that $\theta(\tau)$ is a cusp form if $s > 0$.

We 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. For convenience we drop the "zero" from our notation and write $b_{ij}(n) = b_{ij}^0(n)$. Then

$$B_0(n;\, p^{2r+1},\, M) = (b_{ij}(n))$$

and $b_{ij}(n)$ is just $1/e_j$ times the number of elements $\alpha \in I_j^{-1}I_i$ with $N(\alpha) = nN(I_i)/N(I_j)$. Thus in the notation of (2.3) we have

$$\Theta_0(\tau;\, p^{2r+1},\, M) = (\theta_{ij}(\tau)) \tag{2.5}$$

where

$$\begin{aligned}\theta_{ij}(\tau) &= \sum_{n=0}^{\infty} b_{ij}(n) \exp(n\tau) \\ &= e_j^{-1} \sum_{x \in I_j^{-1}I_i} \exp(\tau N(x)\, N(I_j)/N(I_i))\end{aligned}$$

and the $\theta_{ij}(\tau)$ are modular forms of weight 2 on $\Gamma_0(N)$ by Theorem 2.14. None of the $\theta_{ij}(\tau)$ are cusp forms as the zeroth Fourier coefficient at $i\infty$ of $\theta_{ij}(\tau)$ is $1/e_j$. However we have

PROPOSITION 2.15. *The difference of any two theta series appearing in the same column of the Brandt matrix series $\Theta_0(\tau; p^{2r+1}, M)$ is a cusp form. That is $f(\tau) = \theta_{ij}(\tau) - \theta_{kj}(\tau)$ is a cusp form for all $1 \leqslant i, j, k \leqslant H = H(p^{2r+1}M)$ in the notation of* (2.5).

Proof.

$$\theta_{hj}(\tau) = e_j^{-1} \sum_{x \in I_j^{-1} I_h} \exp(\tau N(x)\, N(I_j)/N(I_h))$$

is (except for the constant multiple e_j^{-1}) the theta series attached to the quadratic form $N(x)\, N(I_j)/N(I_h)$, $x \in I_j^{-1} I_h$. But for $1 \leqslant h \leqslant H$, these quadratic forms all lie in the same genus, i.e., they are locally equivalent for all primes. This follows from Definition 1.7 since for all p there exists $a_p \in \mathfrak{A}_p^{\times}$ such that $I_{hp} = I_{ip} a_p$ and the map $x \to x a_p$ is a local isometry from $N(x)\, H(I_j)/N(I_i)$, $x \in (I_j^{-1} I_i)_p$ to $N(x)\, N(I_j)/N(I_k)$, $x \in (I_j^{-1} I_k)_p$. But it is a classical result that theta series of quadratic forms in the same genus have the same behavior at all cusps, that is, their differences are cusp forms (see Siegel [47, p. 376]).

Remark 2.16. In the case of cusp forms of weight 2 on $\Gamma_0(p)$, p a prime we have $\dim(S_2(p)) = H - 1$, where $H = H(p1)$ is the class number. This follows from Theorem 1.12 and [29, Chap. IV, Proposition 14]. Thus it is nautral to ask if the cusp forms $\theta_{ij}(\tau) - \theta_{1j}(\tau)$, $i = 2, \ldots, H$ and j fixed ($1 \leqslant j \leqslant H$) are a basis of the space $S_2(p)$ of cusp forms of weight 2 on $\Gamma_0(p)$. In fact, Hecke [18, Staz 53, p. 884] conjectured this to be true for any fixed j. However, the conjecture is true only for $p \leqslant 31$ and $p = 41$, 47, 59, and 71 (see [12, 38, 40] and Example 1 in Section 9). The reason for this is as follows. Recall that $I_1, \ldots, I_H$ are a complete set of representatives of the left $\mathcal{O}$-ideal classes ($\mathcal{O}$ an order of level p, hence a maximal order) and $\mathcal{O}_j$ is the right order of I_j, $j = 1, \ldots, H$. As $\mathcal{O}_j$ is a maximal order, there is a unique left $\mathcal{O}_j$-ideal P_j (in fact P_j is a two-sided ideal) such that $N(P_j) = p$. If P_j is a principal ideal, at most $T = T(p1)$, the type number, of the $\theta_{ij}(\tau)$, $1 \leqslant i \leqslant H$ are distinct (see Eichler [12, p. 169] and also Proposition 2.17 below). If P_j is not principal, there is no (known) theoretical reason that the $\theta_{ij}(\tau)$, $1 \leqslant i \leqslant H$, should not be linearly independent. Since $T(p1) < H(p1)$, except when $p \leqslant 31$ and $p = 41$, 47, 59, and 71 (see, e.g., [27]) and there always exists an order $\mathcal{O}_j$ such that P_j is principal, we see that Hecke's original conjecture cannot hold. Eichler proved however (see Corollary 2.29 below) that the $H(H-1)$ cusp forms $\theta_{ij}(\tau) - \theta_{1j}(\tau)$, $2 \leqslant i \leqslant H$, $1 \leqslant j \leqslant H$, do span the space $S_2(p)$. In all our computations we have observed that when P_j is a principal ideal, the $T = T(p1)$ distinct theta series among the H theta series $\theta_{ij}(\tau)$ $1 \leqslant i \leqslant H$ have always been linearly independent

and when P_j is not principal, the H theta series $\theta_{ij}(\tau)$, $1 \leqslant i \leqslant H$, have always been linearly independent. It is easy to see that there always exists an $\mathcal{O}_j$ such that the corresponding P_j is nonprincipal when $T < H$, i.e., when $p \geqslant 37$, $p \neq 41, 47, 59$, or 71. One can obviously ask if the above observed phenomenon always occurs. We do not know the answer. However, the possibility that it does has influenced some of our algorithms.

We shall need

PROPOSITION 2.17. *Let $\mathcal{O}$ be an order of level N in $\mathfrak{A}$. Let I be a left $\mathcal{O}$-ideal and let $J = aIb$ for some a, $b \in \mathfrak{A}^x$ (J is a left $a\mathcal{O}a^{-1}$-ideal) Let $\theta_I(\tau) = \sum_{x \in I} \exp(\tau N(x)/N(I))$ and $\theta_J(\tau) = \sum_{x \in J} \exp(\tau N(x)/N(J))$. Then the theta series $\theta_I(\tau)$ and $\theta_J(\tau)$ are identical.*

Proof.

$$\theta_J(\tau) = \sum_{x \in aIb} \exp(\tau N(x)/N(aIb))$$

$$= \sum_{y \in I} \exp(\tau N(ayb)/N(aIb))$$

$$= \sum_{y \in I} \exp(\tau N(y)/N(I) = \theta_I(\tau).$$

LEMMA 2.18. *Consider the Brandt matrices $B_0(n; p^{2r+1}, M) = (b_{ij}(n))$. Recall e_j is the number of units in $\mathcal{O}_j$, $b_{ij}(0) = 1/e_j$. Then* (a) *$e_j b_{ij}(n) = e_i b_{ji}(n)$ for all i, j, $1 \leqslant i, j \leqslant H$ and all $n \geqslant 0$ and* (b) *$\sum_{j=1}^{H} b_{ij}(n) = b(n)$ (say) is independent of i.*

Proof. Both (a) and (b) are clear for $b_{ij}(0)$. Thus we assume $n \geqslant 1$. $b_{ij}(n)$ is $1/e_j$ times the number of elements $\alpha \in I_j^{-1} I_i$ with $N(\alpha) = nN(I_i)/N(I_j)$. By Proposition 1.17, $I_j^{-1} I_i = N(I_j)^{-1}\, \bar{I}_j I_i$ and $\alpha \in N(I_j)^{-1}\, \bar{I}_j I_i$ with $N(\alpha) = nN(I_i)/N(I_j)$ if and only if $N(I_j)\alpha = \beta \in \bar{I}_j I_i$ and $N(\beta) = nN(I_i)\, N(I_j)$. Thus $e_j b_{ij}(n)$ is just the number of $\beta \in \bar{I}_j I_i$ with $N(\beta) = nN(I_i)\, N(I_j)$. Likewise $e_i b_{ji}(n)$ is just the number of $\beta' \in \bar{I}_i I_j$ with $N(\beta') = nN(I_i)\, N(I_j)$. But $\beta \in \bar{I}_j I_i$ if and only if $\bar{\beta} \in \bar{I}_i I_j$ and $N(\beta) = N(\bar{\beta})$ so (a) is proved. 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 ($\mathcal{O}_i$ 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 $I_i^{-1} I_j \alpha$ with $\alpha \in I_j^{-1} I_i$ and $N(\alpha) = nN(I_i)/(N(I_j)$. Further, two such ideals $I_i^{-1} I_j \alpha$ and $I_i^{-1} I_j \beta$ are equal if and only if $\mathcal{O}_j \alpha = \mathcal{O}_j \beta$ if and only if $\alpha = u\beta$ with u a unit of $\mathcal{O}_j$. Thus $b_{ij}(n)$ is precisely the number of integral left $\mathcal{O}_i$-ideals in the same class as $I_i^{-1} I_j$ having norm n. In fact, this is how Eichler defines $b_{ij}(n)$ —see [14, p. 105]. By Proposition 1.21 we see that $I_i^{-1} I_1, \ldots, I_i^{-1} I_H$ gives a complete set of representatives of all the distinct left $\mathcal{O}_i$-ideal classes. Hence any

integral left $\mathcal{O}_i$-ideal is of the from $I_i^{-1}I_j\alpha$ for some j and some $\alpha \in I_j^{-1}I_i$. Thus $\sum_{j=1}^{H} b_{ij}(n)$ is just the number of integral left $\mathcal{O}_i$-ideals of norm n and we need only prove that this number depends only on the level $p^{2r+1}M$ and not on the particular order $\mathcal{O}_i$ we choose. Unfortunately while this is very easy to prove adelically (I have been trying very hard to avoid adelic arguments), I do not know an easy nonadelic proof. I will give in and sketch the adelic argument. Let $\mathcal{O}$ and $\mathcal{O}'$ be two orders of level $p^{2r+1}M$. It follows from Definition 1.2 that there exists an idèle $\tilde{\alpha} \in J_{\mathfrak{A}}$, the idèle group of $\mathfrak{A}$, such that $\mathcal{O}' = \tilde{\alpha}^{-1}\mathcal{O}\tilde{\alpha}$. Further, Definition 1.7 implies that any left $\mathcal{O}$-ideal is of the form $\mathcal{O}\tilde{\beta}$ for some idèle $\tilde{\beta} \in J_{\mathfrak{A}}$. Then the map $\mathcal{O}\tilde{\beta} \to \mathcal{O}'\tilde{\alpha}^{-1}\tilde{\beta}\tilde{\alpha}$ induces a 1–1 onto map from integral left $\mathcal{O}$-ideals of norm n onto integral left $\mathcal{O}'$ ideals of norm n. For the real meaning of $\mathcal{O}\tilde{\beta}$, etc., see [34, pp. 2 and 5].

LEMMA 2.19. *Let the notation be as in Definition* 2.13. *Let* $B_0(n) = B_0(n; p^{2r+1}, M) = (b_{ij}(n))$. *Consider the matrix*

$$A = \begin{pmatrix} 1 & e_1e_2^{-1} & \cdots & e_1e_H^{-1} \\ & -1 & & 0 \\ \vdots & & \ddots & \\ & & & \ddots \\ 1 & 0 & & -1 \end{pmatrix},$$

i.e., $A = (a_{ij})$ *where* $a_{i1} = 1$ *for* $i = 1,..., H$; $a_{1j} = e_1e_j^{-1}$ *for* $j = 1,..., H$, $a_{ii} = -1$ *for* $i = 2,..., H$ *and all other* $a_{ij} = 0$ $(i \neq 1, j \neq 1, i \neq j)$. *Then* $AB_0(n)\,A^{-1} = C(n)$ *for all* $n \geqslant 0$ *where* $C(n) = (c_{ij}(n))$ *and* $c_{11}(n) = b(n) = \sum_{j=1}^{H} b_{ij}(n)$ (*independent of* i *by Lemma* 2.18); $c_{1i}(n) = c_{i1}(n) = 0$ *for* $i = 2,..., H$; *and* $c_{ij}(n) = b_{ij}(n) - b_{1j}(n)$ *for* $2 \leqslant i, j \leqslant H$.

Proof. Let $m = \sum_{i=1}^{H} e_i^{-1}$, the mass for orders of level $p^{2r+1}M$. $A^{-1} = (1/m)D$ where $D = (d_{ij})$ is given by $d_{ij} = e_j^{-1}$ if $i \neq j$; $d_{11} = e_1^{-1}$; and $d_{ii} = e_i^{-1} - m$ for $i = 2,..., H$. Then $AB_0(n)\,A^{-1} = (1/m)Y$ where $Y = (y_{ij})$ is given by $y_{11} = \sum_{i,j} e_i^{-1}b_{ij}(n) = \sum_i e_i^{-1}(\sum_j b_{ij}(n)) = \sum_i e_i^{-1}b(n) = mb(n)$; $y_{i1} = e_1^{-1}\sum_j (b_{1j}(n) - b_{ij}(n)) = 0$ for $i = 2,..., H$ by Lemma 2.18(b); $y_{1j} = e_1e_j^{-1}\sum_{i,k} e_i^{-1}b_{ik}(n) - e_1m\sum_i e_i^{-1}b_{ij}(n) = e_1e_j^{-1}\sum_i e_i^{-1}(\sum_k b_{ik}(n)) - e_1m \times \sum_i e_j^{-1}b_{ji}(n) = e_1e_j^{-1}mb(n) - e_1me_j^{-1}b(n) = 0$ for $j = 2,..., H$ by Lemmas 2.18(a) and 2.18(b); and finally $y_{ij} = e_j^{-1}\sum_k (b_{1k}(n) - b_{ik}(n)) - m(b_{1j}(n) - b_{ij}(n)) = m(b_{ij}(n) - b_{1j}(n))$ for $i, j = 2,..., H$. This completes the proof of Lemma 2.19.

Remark 2.20. Lemma 2.19 should be compared with Eichler [14, Corollary 1, p. 108 and also the introduction to Chap. IV, p. 138]. Note that $B_0(0)$ is the only Brandt matrix $B_0(n)$ that we know explicitly (other than the identity $B_0(1)$—see Corollary 1.20). Lemma 2.19 says that if we reduce $B_0(0)$ to block form by conjugating by the matrix A, then all other Brandt matrices $B_0(n)$ are also simultaneously reduced to block form by conjugating by A.

We are now finally able to treat the case of cusp forms of weight 2. Let

$$AB_0(n)A^{-1} = \begin{pmatrix} b(n) & 0 & \cdots & 0 \\ 0 & & & \\ \vdots & & B_0'(n) & \\ 0 & & & \end{pmatrix}, \tag{2.6}$$

where $B_0'(n)$ is the $H-1 \times H-1$ matrix given by $B_0'(n) = (d_{ij}(n))$, $d_{ij}(n) = c_{i+1,j+1}(n)$ for $1 \leqslant i, j \leqslant H-1$ in the notation of Lemma 2.19. Then we have

THEOREM 2.21. *Let $B_0'(n; p^{2r+1}, M) = B_0'(n)$ be as in* (2.6). *Then the entries of the modified Brandt matrix series*

$$\Theta_0'(\tau; p^{2r+1}, M) = \sum_{n=0}^{\infty} B_0'(n; p^{2r+1}, M) \exp(n\tau) \tag{2.7}$$

are cusp forms of weight 2 *on $\Gamma_0(N)$, $N = p^{2r+1}M$.*

Proof. After Theorem 2.14, all we need show is that the entries are cusp forms. But this follows immediately from Lemma 2.19 and Proposition 2.15.

The most important fact about the Brandt matrices is that they give a representation of the Hecke operators on a space of theta series. Specifically we have

PROPOSITION 2.22. *Fix s and $N = p^{2r+1}M$, $p \nmid M$. Then the Brandt matrices $B_s(n; p^{2r+1}, M)$ with $(n, N) = 1$ generate a commutative semisimple ring and satisfy the same identities as do the Hecke operators $T_{s+2}(n)$, $(n, N) = 1$.*

Proof. This is Theorem 2 of [14, p. 106]. Note that as we consider only n with $(n, N) = 1$, the proof of Theorem 2 of [14] is valid in our (more general) case.

PROPOSITION 2.23. *Let $N = p^{2r+1}M$, $p \nmid M$. In the notation of* (2.3) *let $\Theta_s(\tau; p^{2r+1}, M) = (\theta_{ij}(\tau))$. Then the action of the Hecke operators $T_{s+2}(n)$, $(n, N) = 1$ on the $\theta_{ij}(\tau)$ is given (formally) by $B_s(n)$, i.e., $T_{s+2}(n)(\theta_{ij}(\tau))$ is the* (ith, jth) *entry of $\sum_{m=0}^{\infty} (B_s(n)\, B_s(m)) \exp(m\tau)$.*

Proof. This follows from Proposition 2.22 and the definition of the Hecke operators. See the Proposition of [14, p. 138].

Remark 2.24. The action of the Brandt matrices given above might seem rather strange. Maybe it is best to think of it in the following manner. Suppose that the theta series $\theta_{11}(\tau),\ldots, \theta_{d1}(\tau)$ ($d = H(s+1)$) in the first column of the Brandt matrix series $\Theta_s(\tau, p^{2r+1}, M)$ are linearly independent (this is not necessarily so—see Remark 2.16). Then $B_s(n)$ is simply the matrix representation

of $T_{s+2}(n)$ on the complex vector space $\langle \theta_{11}(\tau),\ldots, \theta_{d1}(\tau)\rangle$ with respect to the basis $\theta_{11}(\tau),\ldots, \theta_{d1}(\tau)$.

Let $N = p^{2r+1}M$, $p \nmid M$. Denote by $\mathrm{tr}_N\, T_k(n)$ the trace of the Hecke operator $T_k(n)$ acting on the space of cusp forms $S_k(N)$. Then we have the following fundamental

THEOREM 2.25. *For all positive integers n with $(n, N) = 1$ and all even $k \geqslant 2$ we have*

$$\mathrm{tr}_{p^{2r+1}M} T_k(n) + 2\sum_{i=0}^{r-1} \mathrm{tr}_{p^{2i+1}M} T_k(n) + \begin{cases} \deg T_k(n) & \text{if } k = 2 \\ 0 & \text{if } k > 0 \end{cases} \tag{2.8}$$

$$= \mathrm{tr}\, B_{k-2}(n; p^{2r+1}, M) + 2\sum_{i=0}^{r} \mathrm{tr}_{p^{2i}M} T_k(n).$$

Proof. Equation (2.8) is proved by having explicit formulas for the traces of the Hecke operators and the trace of the Brandt matrix. See Theorem 4 of Pizer [36].

Remark 2.26. If $r = 0$, the first summation $\sum_{i=0}^{r-1}$ does not occur in (2.8). If $r = 0$ and M is square free, (2.8) is essentially Eq. (5) of Eichler [14, p. 140]. If $r = 0$, (2.8) is given by Lemma 1 of Hijikata and Saito [21]. The general case is given by Theorem 4 of Pizer [36].

Our main tool now will be the fact that two representations of a semisimple ring are equivalent if and only if their traces are equal (see [25, Theorem 3, p. 458]). In order to employ this tool, we need a space of theta series on which the Hecke operators act. We obtain this as follows. By Proposition 2.22 the $B_{k-2}(n)$ with $(n, N) = 1$ generate a commutative semisimple ring. Thus there exists a matrix C which simultaneously diagonalizes the $B_{k-2}(n)$ with $(n, N) = 1$, i.e., such that $CB_{k-2}(n)C^{-1}$ are diagonal matrices for all $(n, N) = 1$. Further combining this with Lemma 2.19, there exists a matrix C_0 such that in the notation of (2.6), $C_0B_0'(n)\, C_0^{-1}$ is a diagonal matrix for all n with $(n, N) = 1$. Let $\Phi_k(p^{2r+1}, M)$ denote the set of (cusp) forms appearing on the diagonal of the diagonalized Brandt matrix series $\sum_{n=0}^{\infty} CB_{k-2}(n; p^{2r+1}, M)\, C^{-1} \exp(n\tau)$ for $k > 2$. For $k = 2$, let $\Phi_2(p^{2r+1}, M)$ denote the set of (cusp) forms appearing on the diagonal of the diagonalized modified Brandt matrix series

$$\sum_{n=0}^{\infty} C_0B_0'(n; p^{2r+1}, M)C_0^{-1} \exp(n\tau).$$

Remark 2.27. Note that all elements of $\Phi_k(p^{2r+1}, M)$ are eigenforms for all $T_k(n)$ with $(n, N) = 1$. This follows from Proposition 2.23 since the action of the Hecke operators $T_k(n)$ on the elements of $\Phi_k(p^{2r+1}, M)$ is given by the

diagonal matrix $CB_{k-2}(n)\ C^{-1}$ if $k > 2$ and by $C_0B_0'(n)\ C_0^{-1}$ if $k = 2$. Note also that we have not obtained any information about $CB_{k-2}(n)\ C^{-1}$ (or $C_0B_0'(n)\ C_0^{-1}$) if $(n, N) > 1$.

THEOREM 2.28. *Let* $\Phi_k(p^{2r+1}, M) = \{\theta_1(\tau),..., \theta_d(\tau)\}$ $(d = H(k-1),\ H = H(p^{2r+1}M)$ *if* $k > 2$ *and* $d = H - 1,\ H = H(p^{2r+1}M)$ *if* $k = 2)$. *Also let* $\langle\theta_i(\tau)\rangle$ *denote the one-dimensional complex vector space generated by* $\theta_i(\tau)$. *Writing* $+$ *for* $\oplus$ (*sometimes*) *we have*

$$S_k(p^{2r+1}M) \oplus 2\sum_{s=0}^{r-1} S_k(p^{2s+1}M)$$

$$\cong \langle\theta_1(\tau)\rangle \oplus \cdots \oplus \langle\theta_d(\tau)\rangle \oplus 2\sum_{s=0}^{r} S_k(p^{2s}M), \tag{2.9}$$

where the $\cong$ *is as modules for the Hecke algebra* H *generated by* $T_k(n)$ *with* $(n, N) = 1$. *Here* $2S_k(p^{2s+1}M) = S_k(p^{2s+1}M) \oplus S_k(p^{2s+1}M)$, *etc. The* $\theta_i(\tau)$ *are eigenforms for all the* $T_k(n)$ *with* $(n, N) = 1$.

Proof. As H is a semisimple ring, we need only check (by Theorem 3 of [25, p. 458]) that the traces of the transformations induced by the $T_k(n)$, $(n, N) = 1$ on both sides of (2.9) are equal. Note that the action of $T_k(n)$ with $(n, N) = 1$ on $\langle\theta_1(\tau),..., \theta_d(\tau)\rangle$ is given by the diagonal matrix $CB_{k-2}(n)\ C^{-1}$ if $k > 2$ and by $C_0B_0'(n)\ C_0^{-1}$ if $k = 2$ in the notation of Remark 2.27. Now for $k > 2$, (2.8) provides precisely the equality of the traces that we require. For $k = 2$, we need to find the trace of $B_0'(n;\ p^{2r+1},\ M)$. But by (2.6), tr $B_0'(n;\ p^{2r+1},\ M) =$ tr $B_0(n;\ p^{2r+1},\ M) - b(n) =$ tr $B_0(n;\ p^{2r+1},\ M) -$ deg $T_2(n)$ for $(n, pM) = 1$ since $b(n) =$ deg $T_2(n)$ for $(n, pM) = 1$ (see Shimura [46, p. 63] and Eichler [14, p. 94]). Thus again (2.8) provides precisely the equality of the traces that we require. Finally Remark 2.27 shows that the $\theta_i(\tau)$ are eigenforms.

COROLLARY 2.29. *Let the notation be as in Theorems* 2.28 *and* 2.5. *Then*

$$\langle\theta_1(\tau)\rangle \oplus \cdots \oplus \langle\theta_d(\tau)\rangle \cong \bigoplus \sum_{a|M} \sum_{d|M/a} \sum_{s=0}^{r} S_k^0(p^{2s+1}a)^d$$

as H*-modules.*

Proof. This follows from Theorems 2.28 and 2.5 by noting that

$$S_k^0(p^{2r+1}a)^d \cong S_k^0(p^{2r+1}a)^{d'}$$

for d and d' dividing M/a as H-modules (see [2, Theorem 5]). For an explicit proof of Corollary 2.29 see Theorem 6 of Pizer [36].

Remark 2.30. Note in particular that Corollary 2.29 implies that all the newforms on $\Gamma_0(N)$, $N = p^{2r+1}M$ occur among the $\theta_i(\tau)$ since the newforms are precisely the eigenforms that occur in $S_k^0(p^{2r+1}M)^1$.

Remark 2.31. The isomorphism of Corollary 2.29 can essentially be replaced by equality. See Hijikata [20, Theorem 4] and Pizer [36, Theorem 10].

Remark 2.32. It is natural to ask if there is an analogous theory for the case $\Gamma_0(N)$, N a perfect square. Let $N = p^{2r}M$, $p \nmid M$. Let $\mathfrak{A}$ be the quaternion algebra over Q ramified precisely at p and ∞. We would like to define orders of "level N" in $\mathfrak{A}$. Of course, we need only obtain a correct local definition in $\mathfrak{A}_p$. Using ramified quadratic extensions of Q_p instead of the unramified extension L of Definition 1.2, we can define orders that should be the orders of level N. These orders have ideals I whose associated quadratic forms $N(x)/N(I)$, $x \in I$ have level N, i.e., we obtain modular forms of level N (where N may be a square). Unfortunately, it does seem that any relation like Theorem 2.25 can hold for this case. This is probably due to the fact (which comes from Jacquet–Langlands theory) that in the case of square level N, not all newforms in $\Gamma_0(N)$ can be obtained as linear combinations of the theta series and thus Remark 2.30 would be false in general if N is a perfect square. In the particular case of forms of weight 2 on $\Gamma_0(13^2)$, Parry in his dissertation [31] has shown that not all newforms on $\Gamma_0(13^2)$ can be obtained from theta series. If one is able to discover what the "missing" newforms are, one could hope to obtain a result analogous to Corollary 2.29 and thus to completely solve the so-called basis problem (see Eichler [14, p. 77]) for modular forms on $\Gamma_0(N)$.

Since the first version of this paper was written in 1976–1977 there have been several advances. I think it is worthwhile to mention them here without altering the main text. Let $S_k(p, \chi)$ denote the space of cusp forms of weight k on $\Gamma_0(p)$ with character χ. Atkin using Parry's results was able to determine that the "missing" newforms in $S_2^0(13^2)$ are those obtained by twisting forms in $S_2(13, \psi^2)$, $\psi^2 \neq 1$, by $\bar{\psi}$ where ψ is a character of $(Z/13Z)^x$. This and other calculations led him to the obvious conjecture as to what the "missing" newforms were in general for the case $S_2^0(p^2)$. His questions to the present author about this led to the "solution" of the basis problem for $S_k(p^2M)$, $(p, M) = 1$ along the lines suggested in the preceding paragraph (see [39] and also Example 4 in Section 9). Finally using ideas from [39], ideas of Eichler and Hijikata on Brandt matrices with character (see [14, p. 110]), and other new concepts, Hijikata, Pizer, and Shemanske in very recent joint work (see [22]) have been able to "solve" the basis problem for forms of weight k on $\Gamma_0(N)$ with character χ for all $k \geq 2$, all N, and all characters χ mod N. The algorithm in this paper can be applied to these new cases with no or (in the cases of Brandt matrices nontrivial character) only minor changes. Example 5 in Section 9 gives an example of computing Brandt matrices with character.

This completes our rather long sketch of the theory behind the "basis pro-

blem" for modular forms on $\Gamma_0(N)$ (see [14, p. 77]). Now we give a sketch of our computational algorithm.

3. Sketch of the Algorithm

Let N be a positive integer, not a perfect square. Then $N = p^{2r+1}M$, $p \nmid M$ for some prime p. We will sketch an algorithm for obtaining the subspace of the space $S_k(N)$ of cusp forms of weight k on $\Gamma_0(N)$ given by Corollary 2.29. We will be primarily concerned with the case of forms of weight 2. The modifications necessary to obtain forms of higher weight will be noted at the appropriate places.

First let us introduce some convenient notation. For any ideal L of an order of level N, we let

$$\theta_L(\tau) = \sum_{x \in L} \exp(\tau N(x)/N(L))) = \sum_{n=0}^{\infty} c(n) \exp(n\tau), \tag{3.1}$$

where $c(n)$ (the so-called representation numbers of the quadratic form $N(x)/N(L)$, $x \in L$) is the number of $x \in L$ with $N(x) = nN(L)$. Given two ideals L and L' we will often want to compare $\theta_L(\tau)$ and $\theta_{L'}(\tau)$. To do this (on a computer) we first select some predetermined number, say LIMIT2 (e.g., LIMIT2 may be 5 or 10). Then when we write $\theta_L(\tau) \neq \theta_{L'}(\tau)$ in the algorithm, it really means that the 1st, 2nd,..., LIMIT2th Fourier coefficients of $\theta_L(\tau)$ and $\theta_{L'}(\tau)$ are not identical.

We will present the algorithm as a series of steps (from step 1 to step 4). The various steps are more fully explained in Sections 5–8 below.

Step 1. Finding the algebra. We first obtain a basis for the quaternion algebra $\mathfrak{A}$ over Q ramified precisely at p and ∞. Theorem 5.1 gives QA and QB such that $\mathfrak{A} = (QA, QB)$, in the notation of the first paragraph of Section 1, is the desired algebra. Thus $\mathfrak{A}$ has a basis 1, I, J, K with relations $I^2 = QA$, $J^2 = QB$ and $IJ = K = -JI$. All our computations will be done in terms of this basis.

Step 2. Finding an order of level N. Let $N = p^{2r+1}q_1^{s_1} \cdots q_f^{s_f}$ with $q_1, \ldots, q_f$ the distinct primes dividing M.

Step 2a. By Proposition 5.2, we obtain a maximal order $\mathcal{O}_1$ of $\mathfrak{A}$, i.e., an order of level p.

Step 2b. $\mathcal{O}_1$ contains an order of level pq_1 by Definition 1.2 and Remark 1.4. Such an order has index q_1 in $\mathcal{O}_1$. To obtain one we find all orders of index q_1 in $\mathcal{O}_1$ and use Proposition 1.6 to select one, say $\mathcal{O}_2$, of level pq_1. $\mathcal{O}_2$ contains an order of level pq_1^2. To obtain one we find all orders of index q_1 in $\mathcal{O}_2$ and again

use Proposition 1.6 to select one of level pq_1^2. We continue in this manner until we obtain an order $\mathcal{O}_3$ of level pM. Then $\mathcal{O}_3$ contains an order of level p^3M. To obtain one we find all orders of index p^2 in $\mathcal{O}_3$ and use Proposition 1.6 to select one of level p^3M. We continue until we obtain our desired order, say $\mathcal{O}_0$, of level N. See Section 5 for details.

Step 3. Finding representatives of the left-ideal classes. This is the critical step. The method we present here is based on the assumption that all left $\mathcal{O}_0$-ideals are induced from ideals in imaginary quadratic subfields of $\mathfrak{A}$. This assumption can be stated explicitly in the adelic language. However, as we are not able to prove the assumption is valid, stating it precisely will not gain us much. It has been valid in all examples we have tried to compute.

Step 3a. Use Theorem 2.12 to compute the class number $H = H(p^{2r+1}M)$ and put $\mathcal{O} = \mathcal{O}_0$.

Step 3b. Let $L_1 = \mathcal{O}$ be the first left $\mathcal{O}$-ideal. Note that $N(L_1) = 1$.

Step 3c. Suppose at this point that we have obtained ideals $L_1, \ldots, L_t$ representing distinct left $\mathcal{O}$-ideal classes (the first time around $t = 1$ of course).

Step 3d. Choose some element $\alpha \in \mathcal{O}$ with $\alpha \notin Z$. Consider the order $S = Z + Z\alpha$ of $Q(\alpha)$ generated by α.

Step 3e. Use Gaussian reduction (see, e.g., Borevich and Shafarevich [6, p. 149]) to obtain a set of representatives $T_1', \ldots, T_h'$ of the S-ideal classes. Also compute $N(T_1'), \ldots, N(T_h')$.

Step 3f. Set $\nu = 1$.

Step 3g. Push the ideal T_ν' up to a left $\mathcal{O}$-ideal $T_\nu = \mathcal{O}T_\nu'$. Note that $N(T_\nu) = N(T_\nu')$.

Step 3h. Compare the theta series $\theta_{T_\nu}(\tau)$ with $\theta_{L_1}(\tau), \ldots, \theta_{L_t}(\tau)$. If $\theta_{T_\nu}(\tau) \neq \theta_{L_i}(\tau)$ for $i = 1, \ldots, t$, then T_ν is in a distinct left $\mathcal{O}$-ideal class form $L_1, \ldots, L_t$ by Proposition 2.17. Thus we put $L_{t+1} = T_\nu$, replace t by $t + 1$, replace ν by $\nu + 1$, and go to Step 3g. If $\theta_{T_\nu}(\tau) = \theta_{L_\gamma}(\tau)$ for $\gamma = i_1, \ldots, i_r$ and only for $\gamma = i_1, \ldots, i_r$ then we test whether or not T_ν' is in the same ideal class as any of the L_γ, $\gamma = i_1, \ldots, i_r$. By Proposition 1.18, if any $\bar{T}_\nu L_\gamma$ for $\gamma = i_1, \ldots, i_r$ contains an element α of norm $N(T_\nu)\,N(L_\gamma)$, then (as T_ν does not determine a new ideal class by Proposition 1.18) replace ν by $\nu + 1$ and go to Step 3g. Otherwise (since by Propositions 1.18 and 2.17, T_ν determines a new ideal class) put $L_{t+1} = T_\nu$, replace t by $t + 1$, replace ν by $\nu + 1$, and go to Step 3g.

Step 3i. Continue iterating Step 3h until either:

(a) $t = H$ (i.e., we have obtained H ideals $L_1, \ldots, L_H$ which represent distinct left ideal classes and hence represent all the distinct left ideal classes) in which case go to Step 4, or

(b) $\nu > h$ (i.e., we have tested all the ideals $T_1, \ldots, T_h$) in which case go to Step 3d, selecting a different α, or

(c) we have tested a total of LIMIT ideals (LIMIT is some preselected number, e.g., $2H$ or $3H$) in which case go to Option 1.

Option 1. This option is based on Proposition 1.21.

Option 1a. Select some ideal L_μ, $2 \leqslant \mu \leqslant t$. Thus $L_\mu \neq \mathcal{O} = \mathcal{O}_0$.

Option 1b. If $\theta_{(L_\mu^{-1}L_\mu)}(\tau) \neq \theta_{L_1}(\tau)$ (thus $L_\mu^{-1}L_\mu$, which is an order of level N by Proposition 1.17(c) and Remark 1.15, is not isomorphic to $\mathcal{O} = L_1$) then go to Option 1c. Otherwise go to Option 1a, selecting a different μ. If we use up all μ, $2 \leqslant \mu \leqslant t$, without finding a $L_\mu^{-1}L_\mu$ with $\theta_{L_\mu^{-1}L_\mu}(\tau) \neq \theta_{L_1}(\tau)$, then Option 1 fails.

Option 1c. Replace. $\mathcal{O}$ by $L_\mu^{-1}L_\mu$, L_1 by $L_\mu^{-1}L_\mu$, L_μ by $L_\mu^{-1}L_1$, and L_ν by $L_\mu^{-1}L_\nu$ for $2 \leqslant \nu \leqslant t$, $\nu \neq \mu$. Then $L_1, \ldots, L_t$ represent distinct $\mathcal{O} = L_\mu^{-1}L_\mu$ ideal classes by Proposition 1.21.

Option 1d. Go to Step 3d.

Remark. We of course have to select some maximum number (say TRY) of times we will allow Option 1 to be executed. If we have executed Option 1 more than TRY times and still have not obtained representatives of all the distinct left ideal classes, we should admit defeat and stop the program.

Remark 3.1. If Step 3 fails and we do not obtain representations of all the distinct left ideal classes, the alternatives are not attractive. Picking ideals "out of a hat" is no easy trick.

Step 4. Calculating the Brandt matrices. First we consider the case of weight $k = 2$. Calculate $\theta_{\bar{L}_j L_i}(\tau)$ for $i \geqslant j$ (see Section 6). By the proof of Lemma 2.18

$$\Theta_0(\tau; p^{2r+1}, M) = \sum_{n=0}^{\infty} B_0(n) \exp(n\tau) = \left(\frac{1}{e_j}\theta_{\bar{L}_j L_i}(\tau)\right)$$

and $\theta_{\bar{L}_j L_i}(\tau) = \theta_{\bar{L}_i L_j}(\tau)$. Note that e_j is just the number of elements of $L_j^{-1}L_j$ of norm 1, i.e., e_j is the number of elements of $\bar{L}_j L_j$ of norm $N(L_j)^2$, i.e., e_j is the 1st (not the 0th) Fourier coefficient of $\theta_{\bar{L}_j L_j}(\tau)$.

If we are interested in the case of weight $k > 2$, Step 4 becomes more involved. First we have to explicitly determine $X_{k-2}(1)$, $X_{k-2}(I)$, $X_{k-2}(J)$, and $X_{k-2}(K)$. The first is of course trivial. Then we find all $\alpha \in I_j^{-1}I_i = (1/N(I_j))\,\bar{I}_j I_i$ with $N(\alpha) = nN(I_i)/N(I_j)$, α will be given in terms of the basis $1, I, J, K$ (see Remark 6.3). Then we calculate (2.2), $b_{ij}^{k-2}(n) = e_j^{-1}\sum X_{k-2}^t(\alpha)$ and thus obtain the Brandt matrix $B_{k-2}(n; p^{2r+1}, M)$.

In the case of weight $k > 2$, the entries of the Brandt matrix series (2.3) $\Theta_{k-2}(\tau; p^{2r+1}, M) = \sum_{n=1}^{\infty} B_{k-2}(n; p^{2r+1}, M) \exp(n\tau)$ are the theta series we want and the Brandt matrices themselves $B_{k-2}(n; p^{2r+1}, M)$ give a representation of the Hecke operators $T_{k-2}(n)$, $(n, N) = 1$ on the space of theta series given by Corollary 2.29.

In the case of weight 2, we are usually interested in the modified Brandt matrices $B_0'(n; p^{2r+1}, M)$. But by Lemma 2.19, these are very easily obtained from the $B_0(n; p^{2r+1}, M)$. Then the entries of the modified Brandt matrix series (2.7)

$$\Theta_0'(\tau; p^{2r+1}, M) = \sum_{n=1}^{\infty} B_0'(n; p^{2r+1}, M) \exp(n\tau)$$

are cusp forms of weight 2 and the action of the Hecke operator $T_2(n)$, $(n, N) = 1$ on them is given by $B_0'(n)$.

4. Some Needed Procedures

We collect in this section some procedures (as in ALGOL PROCEDURE) that are necessary for our algorithm.

Procedure GCD(N, A, IGCD). Let $A = (A[1],..., A[N])$ be a set of N integers. Then this procedure calculates the (positive) greatest common divisor IGCD of $A[1],..., A[N]$. Several explicit algorithms for doing this can (if needed) be found in the *Communications of the Association for Computing Machinery*.

Procedure HERMITE(C, N, M). Let $C = (c_{ij})$ be a $N \times M$ (i.e., N rows and M columns) integer matrix with $N \leqslant M$ and rank$(C) = N$. (in our case $N = 4$ always). Then by employing column operations (i.e., by multiplying C on the right by unimodular, i.e., det $= \pm 1$, $M \times M$ integer matrices) C can be reduced to Hermite normal form (d_{ij}), i.e., (d_{ij}) is lower triangular ($d_{ij} = 0$ if $i < j$), $d_{ii} > 0$ for $1 \leqslant i \leqslant N$, and d_{ij} is reduced mod d_{ii} for all $j < i$, $i = 2,..., N$. In particular we can and do assume that $0 \leqslant d_{ij} < d_{ii}$ for all $j < i$, $i = 2,..., N$. The Hermite normal form of a matrix is unique (see [28, Theorem II.3]). To obtain the Hermite normal form of a matrix C we proceed as follows. First reduce C to lower triangular form with positive diagonal entries by any method that pleases you, e.g., one could use [5]. Now we only have to reduce the off-diagonal entries. Unfortunately, doing this in the obvious manner seems to sometimes involve numbers too large for a computer to (easily) handle (whereas, strangely, this problem does not seem to occur very often in reducing to lower triangular form). However, we can make use of the uniqueness

of the Hermite normal form for matrices in Z and also in Z (mod m). Consider the matrix F which we assume is in lower triangular form with positive diagonal entries, i.e., $F = (f_{ij})$, $1 \leqslant i, j \leqslant N$ with $f_{ij} \in Z$, $f_{ij} = 0$ if $i < j$, and $f_{ii} > 0$ for $i = 1,..., N$. Let m be the least common multiple of f_{22}, f_{33},..., f_{NN}. Then we can reduce F to Hermite normal form as a matrix with entries in $Z/(m)$, i.e., we perform all operations modulo m, in the obvious (or any other) manner. The resulting matrix, say (d_{ij}), satisfying $d_{ii} = f_{ii}$ for $i = 1,..., N$ (we do not change or reduce f_{11} mod m) and $0 \leqslant d_{ij} < d_{ii} = f_{ii}$ for $j < i$, will be the Hermite normal form of the original matrix F considered as a matrix in Mat(N, Z) by the uniqueness of Hermite normal form for matrices in Z and also in $Z/(m)$ (see Newmann [28, p. 18]). Thus as long as m is not too large, we will not get overflow errors on the computer.

Remark 4.1. It will become apparent that the procedure HERMITE will be used very often in our algorithm. A really efficient procedure for obtaining the Hermite normal form of a matrix would be nice.

Procedure REDUCE(C, D, F). Let $C = (c_{ij})$ be a lower triangular 4×4 integer matrix. D (for denominator) and F (for factor) are integers. The procedure replaces C by C', D by D' and F by F' so that $(F'/D')\ C' = (F/D)C$ and $(c'_{11}, c'_{21},..., c'_{44}) = 1$ and $(D', F') = 1$ with D' and F' positive. Here, of course $C' = (c'_{ij})$. Thus REDUCE simply removes all common factors from C and puts F/D in reduced form.

Procedure GAUSS(DISC, A, B, CLASS. NO). DISC is the discriminant of an order S in an imaginary quadratic number field (thus DISC < 0). The procedure GAUSS calculates the class number CLASS. NO of S and also representatives of the distinct ideal classes of S. The representative ideals are given in the form $Z(2A[n]) + Z(-B[n] + (\text{DISC})^{1/2})$ for $n = 1, 2,...,$ CLASS. NO. Here we assume that $A[n]$ and $B[n]$ are integers for $n = 1,...,$ CLASS. NO and A and B denote the one-dimensional arrays whose nth elements are $A[n]$ and $B[n]$. An explicit procedure for doing this, due to Gauss, can be found in the work of Borevich–Shafarevich [6, pp. 149 and 150]. It is probably best to choose some number, say STOP, such that representatives of only STOP ideal classes will be generated if CLASS. NO $>$ STOP.

Remark 4.2. Note that the norm of the ideal $Z(2A[n]) + Z(-B[n] + (\text{DISC})^{1/2})$ is $4A[n]$ (see the Corollary of [6, p. 137].

Procedure QMULT(E, F, QA, QB, A, B, C). This procedure performs multiplication in the quaternion algebra $\mathfrak{A} = (QA, QB)$. $A = (A[1],..., A[4]) \in Z^4$ represents the element $A' = A[1] + A[2]I + A[3]J + A[4]K$ in the canonical basis 1, I, J, K of $\mathfrak{A} = (QA, QB)$. Similarly for B and C. The procedure calculates C corresponding to the element $C' = A'B'$, multiplication being in $\mathfrak{A} = (QA, QB)$. We assume (for efficiency) that the first $E - 1$ entries

of A and the first $F-1$ entries of B are zero ($1 \leqslant F$, $F \leqslant 4$) since we will often have to multiply such elements.

Procedure QTRACE(A). QTRACE(A) is the trace of A' where the notation is as in Procedure QMULT above. Thus QTRACE(A) $= 2A[1]$. We assume, as always, that $A \in Z^4$.

Procedure QNORM(QA, QB, A). QNORM(QA, QB, A) is the norm of A' in the quaternion algebra (QA, QB). The notation and assumptions are the same as in QTRACE above.

At this point we need to select a convenient way to represent lattices (thus in particular orders and ideals) on the computer. We do this by

Notation 4.3. Let L' be a lattice on a quaternion algebra $\mathfrak{A} = (QA, QB)$ over Q. L' has a Z-basis $f_1, \ldots, f_4$. Each f_j can be written as $f_j =$ (LFAC/LDEN) $(L[1,j] + L[2,j]I + L[3,j]J + L[4,j]K)$ where LFAC, LDEN and $L[i,j]$, $1 \leqslant i, j \leqslant 4$ are all integers. Of course here $\{1, I, J, K\}$ is the canonical basis of $\mathfrak{A} = (QA, QB)$. We thus represent L' by the triple LFAC, LDEN, $L = L[i,j]$ consisting of the integer LFAC (the "common factor"), the integer LDEN (the "common denominator"), and the 4×4 integer matrix L. Thus the columns of (LFAC/LDEN)L give a basis of L' in terms of the canonical basis $1, I, J, K$. We can and do write $(f_1, \ldots, f_4) = (1, I, J, K)$((LFAC/LDEN) (L)). Note that multiplying L on the right by a unimodular matrix does not change the lattice L' which LFAC, LDEN, L represents. Thus we can and usually do assume that L is in lower triangular (or even Hermite) form. Finally at times we need to consider ideals in imaginary quadratic number fields contained in $\mathfrak{A}$. These ideals, which are free Z-modules of rank 2, will be represented the same way as are lattices on $\mathfrak{A}$, except that the matrix corresponding to the matrix L above will have only 2 columns, i.e., will be a 4×2 matrix.

Let $L_1 = Zf_1 + \cdots + Zf_4$ and $L_2 = Zg_1 + \cdots + Zg_4$ be two lattices on $\mathfrak{A} = (QA, QB)$. We need a procedure for obtaining the lattice $L_1L_2 = \sum_{i,j} Zf_ig_j$. For example L_1 and L_2 might be ideals and then L_1L_2 is their product in the Brandt groupoid (see the paragraph following Definition 1.16). This need is fulfilled by

Procedure LATTICE(QA, QB, L_1F, L_1D, L_1, L_2F, L_2D, L_2, K, L_3F, L_3D, L_3). For $i = 1$ or 2 let L_i' be the lattice in the quaternion algebra $\mathfrak{A} = (QA, QB)$ represented by L_iF, L_iD, L_i in Notation 4.3. K is either 4 or 2. If $K = 4$, we assume L_2' is a lattice on $\mathfrak{A}$, i.e., L_2 is a 4×4 matrix, while if $K = 2$, we assume L_2' is a lattice on some imaginary quadratic number field contained in $\mathfrak{A}$, i.e., we assume L_2 is a 4×2 matrix. We always assume that L_1' is a lattice on $\mathfrak{A}$ and further that L_1 is in lower triangular form. Also we assume that L_2 is in lower triangular form if $K = 4$. The procedure computes the lattice $L_3' = L_1'L_2'$ and represents L_3' by L_3F, L_3D, L_3 in Notation 4.3. L_3 is given in lower triangular form and L_3F, L_3D, L_3 is "reduced" (see Procedure REDUCE). The procedure

goes as follows. First if L is a matrix, denote by $L(j)$ the jth column of L. If $K = 4$, perform the operations:

$$\text{QMULT}(i, j, QA, QB, L_1(i), L_2(j), L_3(4(i-1)+j); \quad \text{for } 1 \leqslant i, \ j \leqslant 4,$$

while if $K = 2$ performs the operations

$$\text{QMULT}(i, 1, QA, QB, L_1(i), L_2(j), L_3(4(i-1)+j); \quad \text{for } 1 \leqslant i \leqslant 4, \ 1 \leqslant j \leqslant 2.$$

Thus $L_3(k)$, $k = 1,\ldots, 4K$ are all elements of Z^4 and viewing them as column vectors we form the $4 \times 4K$ integral matrix $L_3 = (L_3(j))$. Now perform the operations:

$$L_3F = (L_1F)(L_2F);$$
$$L_3D = (L_1D)(L_2D);$$
$$\text{HERMITE}(L_3, 4, 4K);$$
$$\text{REDUCE}(L_3, L_3D, L_3F).$$

This completes the procedure LATTICE. Note that after performing HERMITE(L_3, 4, $4K$), only the first four columns of L_3 are nonzero, so we view L_3 as a 4×4 matrix by discarding the 5th, 6th,..., $4K$th columns.

5. Finding an Order of Level N

In this section we explain Steps 1 and 2 of Section 3. First we find the algebra.

Proposition 5.1. *Let p be a prime. Then the (unique) quaternion algebra $\mathfrak{A}(p)$ over Q ramified precisely at p and ∞ is given by*:

$$\mathfrak{A}(p) = (-1, -1) \quad \text{if } p = 2;$$
$$\mathfrak{A}(p) = (-1, -p) \quad \text{if } p \equiv 3(4);$$
$$\mathfrak{A}(p) = (-2, -p) \quad \text{if } p \equiv 5(8);$$

and

$$\mathfrak{A}(p) = (-p, -q) \quad \text{if } p \equiv 1(8)$$

where q is a prime with $q \equiv 3(4)$ and $(p/q) = -1$.

Proof. This follows from an easy exercise in calculating Hilbert symbols. See [24, p. 157, #10 on p. 186, and Theorem 2.27 on p. 163]. Note that one does not really have to calculate the Hilbert symbol $(QA, QB)_2$ as the number of ramified primes must be even.

PROPOSITION 5.2. *Let p be a prime and let $\mathfrak{A}(p) = (QA, QB)$ be the quaternion algebra (ramified precisely at p and ∞) given by Proposition 5.1 above. Then a maximal order of $\mathfrak{A}(p)$ is given by the Z-basis*:

$$\begin{aligned}
&\tfrac{1}{2}(1 + I + J + K), I, J, K && \text{if } p = 2,\\
&\tfrac{1}{2}(1 + J), \tfrac{1}{2}(I + K), J, K && \text{if } p \equiv 3(4),\\
&\tfrac{1}{2}(1 + J + K), \tfrac{1}{4}(I + 2J + K), J, K && \text{if } p \equiv 5(8),
\end{aligned}$$

and

$$\tfrac{1}{2}(1 + J), \tfrac{1}{2}(I + K), 1/q(J + aK), K \qquad \text{if } p \equiv 1(8),$$

where a is some integer such that $q \mid (a^2p + 1)$. Here $1, I, J, K$ is the canonical basis of $\mathfrak{A}(p) = (QA, QB)$ with relations $I^2 = QA$, $J^2 = QB$, and $IJ = K = -JI$.

Proof. The case $p = 2$ is classical. By Proposition 1.1 we need only check that the discriminant of the lattice given by the above basis is p^2 and that the lattice is in fact a subring $\ni 1$. The explicit calculations necessary to demonstrate this are straightforward and easy (but rather tedious). We leave them to the reader.

According to Step 2 of Section 3 we need a method of finding all suborders of index q or p^2 (q and p primes) in a given order. Assume we are given an order $\mathcal{O}'$ represented by QORFAC, QORDEN, and QOR = (QOR[i, j]) in Notation 4.3. Further suppose a Z-basis of $\mathcal{O}'$ is given by $f_1, \ldots, f_4$, i.e., $(f_1, \ldots, f_4) = (1, I, J, K)$((QORFAC/QORDEN)QOR). Let $\mathcal{O}''$ be a suborder of index q in $\mathcal{O}'$. Assume $\mathcal{O}'' = Zg_1 + \cdots + Zg_4$. Then $g_j = \sum_i b_{ij} f_i$ for some $b_{ij} \in Z$ with $\det((b_{ij})) = q$. Put $B = (b_{ij})$. Then $(g_1, \ldots, g_4) = (1, I, J, K)$((QORFAC/QORDEN)(QOR)($B$)). Multiplying B on the right by a unimodular matrix does not change $\mathcal{O}''$. Thus we can assume B is in Hermite normal form, i.e.,

$$B = \begin{pmatrix} q & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{or} \quad B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ a & q & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{or}$$

$$B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ a & b & q & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{or} \quad B = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ a & b & c & q \end{pmatrix}, \tag{5.1}$$

where $0 \leqslant a, b, c < q$. Thus any suborder (or sublattice for that matter) of index q in $\mathcal{O}'$ must be of the form

$$Zg_1 + \cdots + Zg_4 \tag{5.2}$$

where $(g_1, \ldots, g_4) = (1, I, J, K)$((QORFAC/QORDEN)(QOR)($B$)) where B is allowed to run over the matrices in (5.1).

Now we must give a method for deciding if a lattice given by (5.2) is in fact an order. Thus let L' be a lattice represented by LFAC, LDEN, $L = L[i, j]$ in Notation 4.3. First perform the operations:

HERMITE(L, 4, 4);
REDUCE(L, LDEN, LFAC);

Now first check to see if LFAC = 1. If LFAC $\neq$ 1, then L' is not an order since $1 \notin L'$ if LFAC $\neq$ 1. If LFAC = 1, then next check to see if $1 \in L'$. This is easy to do since L is in lower triangular form. If $1 \in L'$, we finally check to see if L' is a ring, i.e., we see if L' is closed under multiplication. All we need really do is check that $g_i g_j \in L'$ for $1 \leqslant i, j \leqslant 4$ if L' is given by (5.2). A convenient method for doing this is to perform the operations:

LATTICE(QA, QB, LFAC, LDEN, L, LFAC, LDEN,
L, 4, MFAC, MDEN, M);

then L' is an order if and only if MFAC = LFAC, MDEN = LDEN and the 4×4 matrices L and M are identical. Clearly L' defines an order if and only if $1 \in L'$ (which we have already checked above) and $L'L' = L'$. Using the uniqueness of the Hermite normal form one easily checks that $L'L' = L'$ if and only if MFAC = LFAC, MDEN = LDEN, and $M = L$.

The only difference in finding suborders of index p^2 in $\mathcal{O}'$ is that we must let B range over all integer 4×4 matrices in Hermite normal form with $\det(B) = p^2$.

Finally we employ Proposition 1.6 to select an order of level N'' (where $N'' = q$ (level(Q')) or $N'' = p^2$(level(Q')) depending on the case) from among the possibilities given above. Specifically, let $\mathcal{O}''$ be a suborder of index q in $\mathcal{O}'$ and assume q is not the ramified prime of $\mathfrak{A}$. Then by Proposition 1.6, $\mathcal{O}''$ is an order of level N'' if and only if $\mathcal{O}''$ contains a subring isomorphic (over Z_q) to $Z_q \oplus Z_q$. This is true if and only if $\mathcal{O}''_q$ contains an element α (such as $\left(\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right)$) with $\mathrm{Tr}(\alpha) = 1$ and $N(\alpha) = 0$ or, if $q \neq 2$, an element β (such as $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$) with $\mathrm{Tr}(\beta) = 0$ and $N(\alpha) = -1$. On the other hand if p is the finite ramified prime of $\mathfrak{A}$ and $\mathcal{O}''$ is an order of index p^2 in $\mathcal{O}'$, then $\mathcal{O}''$ is an order of level N'' if and only if $\mathcal{O}''_p$ contains an order isomorphic (over Z_p) to R, the ring of integers of L, the unramified quadratic field extension of Q_p. This is true if and only if $\mathcal{O}''_p$ contains an element α (such as $u^{1/2}$) with $\mathrm{Tr}(\alpha) = 0$ and $N(\alpha) = -u$ where $u \in Z$ is a quadratic nonresidue mod p for $p > 2$ or an element β (such as $(1 + 5^{1/2})/2$) with $\mathrm{Tr}(\beta) = 1$ and $N(\beta) = -1$ for $p = 2$. These local calculations are probably best done by hand, or at least I have done them by hand in my computations.

Of course we do not have to find all suborders of index q or p^2 in a given order in Step 2. One should just find a few (there are not too many possibilities in any case) and test them for an order of level N'' (at this point, it would be very convenient to rename orders of "level N" so that the explicit "N" does not occur in the name and thus we could do away with the annoying N'').

6. Calculating the Representation Numbers

Let $Q(x)$ be a positive definite integral quadratic form in r variables. We want a procedure for calculating the number of times $Q(x)$ represents 0, 1, 2,..., T (for some given T) as x varies over Z^r, i.e., for calculating the so-called representation numbers of $Q(x)$.

First let us consider the easiest nontrivial example $Q(x) = x_1^2 + x_2^2$. The obvious way to find the number of times $Q(x)$ represents the integers 0, 1,..., T as x varies over Z^2 is as follows: let x_1 vary over the integers $-T^{1/2} \leqslant x_1 \leqslant T^{1/2}$ and let x_2 vary over the integers $-(T - x_1^2)^{1/2} \leqslant x_2 \leqslant (T - x_1^2)^{1/2}$ and evaluate $Q(x_1, x_2)$ and count the number of times each integer from 0 to T occurs. We could shorten this a little by making use of the fact that $Q(-x) = Q(x)$. Also in the present example we could use the fact that $Q(-x_1, x_2) = Q(x_1, x_2)$, etc., but in general the isometry $x \to -x$ is the only isometry we will have available. It is difficult to imagine a more efficient elementary method for calculating the representation numbers of $Q(x) = x_1^2 + x_2^2$ since each (x_1, x_2) considered by the above method actually contributes a $Q(x_1, x_2)$ in the desired range. Let us now reinterpret the above method.

Again consider $Q(x) = x_1^2 + x_2^2$. We present an iterative method, essentially identical to that above, for calculating the representation numbers of $Q(x)$. The graph of $Q(x)$ with $x \in \mathbb{R}^2$ is a two-dimensional paraboloid with its minimum point (0, 0) having $Q(0, 0) = 0$. This is of course true for all positive definite quadratic forms except that in general the dimension of their paraboloid graph equals the number of variables of the form. Let $C[i]$ denote the number of times $Q(x)$ represents i. Our method is:

Rep 0. Let $C[0] = C[1] = \cdots = C[T] = 0$.

Rep 1. Let $x_1 = 0$.

Rep 2. Calculate the minimum point m_2 of the one-dimensional paraboloid $Q(x_1, x_2) = x_1^2 + x_2^2$ with x_1 fixed and $x_2 \in \mathbb{R}$.

Rep 3. If $Q(x_1, m_2) > T$, then go to Rep 11.

Rep 4. Let x_2 be the least integer $> m_2$.

Rep 5. While $Q(x_1, x_2) \leqslant T$ iterate the steps:

(a) replace $C[Q(x_1, x_2)]$ by $C[Q(x_1, x_2)] + 1$;

(b) replace x_2 by $x_2 + 1$;

(c) go to Rep 5.

Rep 6. Let x_2 be the greatest integer $\leqslant m_2$.

Rep 7. While $Q(x_1, x_2) \leqslant T$ iterate the steps:

(a) replace $C[Q(x_1, x_2)]$ by $C[Q(x_1x_2)] + 1$;

(b) replace x_2 by $x_2 - 1$;

(c) Go to Rep 7.

Rep 8. If $x_1 = 0$, then replace $C[i]$ by $C[i]/2$ for $i = 1,..., T$.

Rep 9. Replace x_1 by $x_1 + 1$.

Rep 10. Go to Rep 2.

Rep 11. Replace $C[i]$ by $2C[i]$ for $i = 1,..., T$.

Rep 12. End.

Remark 6.1. We use the fact that $Q(x) = Q(-x)$ so that we consider only $x_1 \geqslant 0$. As Rep 8 shows, we do not attempt to make use of the fact that $Q(-x_1, x_2) = Q(x_1, x_2)$, etc., as such phenomena do not occur in general.

Remark 6.2. The major point on which this method is based is that a paraboloid has a unique minimum point and as we move away from it in any direction, the surface always rises. In the case $Q(x) = x_1^2 + x_2^2$, the minima of the associated prabolas (see Rep 2) are always trivial to calculate ($m_2 = 0$ always) and this is what makes the computation of the representation numbers of $Q(x) = x_1^2 + x_2^2$ very easy. But in general calculating the minimum point of a paraboloid is quite easy. One just has to solve (since we know calculus) some simultaneous linear equations. In our case we set things up so that the coefficient matrix of these simultaneous linear equations will be lower triangular and thus solving them is very easy.

The generalization of our method to an arbitrary integral positive definite quadratic form is (or should be) obvious. As this is the critical step in our algorithm, we give below an explicit procedure written in ALGOL60 that covers the cases we require. According to (3.1), we need to calculate the representation numbers $C[n]$ of quadratic forms of the type $N(x)/N(L')$ for $x \in L'$ where L' is some lattice in a quaternion algebra over Q. Let L' be represented by LFAC, LDEN, $L = (L[i, j])$ in Notation 4.3. We can and do assume L is in lower triangular form. Then $x \in L' \Leftrightarrow x = (\text{LFAC/LDEN})y$ with $y \in Zf_1 + \cdots + Zf_4$ where $(f_1,..., f_4) = (1, I, J, K)L$. Then $N(x)/N(L') = n \Leftrightarrow ((\text{LFAC})^2/(\text{LDEN})^2\, N(L'))\, N(y) = n$. Thus we are led to consider quadratic forms of the type $(F/K)\, N(x)$ where x varies over some lattice $Zf_1 + \cdots + Zf_4$

with $(f_1,\ldots,f_4) = (1, I, J, K)A$ where A is a 4×4 lower triangular integer matrix. The explicit procedure is (note that for typographical reasons we use a double asterisk to denote exponentiation):

```
PROCEDURE REPRESENTATION. NO(A, P, Q, C, K, F, R);
VALUE F, K, R, P, Q;
INTEGER ARRAY A, C;
INTEGER K, F, R, P, Q;
        COMMENT: THIS PROCEDURE REPRESENTATION. NO
                 CALCULATES THE REPRESENTATION
                 NUMBERS
                 C[N] FOR N <= R FOR THE QUADRATIC
                 FORM F/K(NORM(X1 + X2I + X3J + X4K)) =
                 F/K[(X1)**2 + P(X2)**2 + Q(X3)**2 +
                 + PQ(X4)**2] EVALUATED ON (I. E.
                 WHERE X1 + X2I + X3J + X4K VARIES OVER
                 THE POINTS OF) THE LATTICE WITH Z BASIS
                 A11 + A21I + A31J + A41K, A22I + A32J +
                 + A42K, A33J + A43K, AND A44K IN THE
                 QUATERNION ALGEBRA (-P, -Q) WHERE
                 1, I, J, K DENOTES THE CANONICAL BASIS
                 OF (-P, -Q) (NOTE THAT WE ARE
                 ASSUMING THAT THE MATRIX A IS LOWER
                 TRIANGULAR). THE RESULTS ARE STORED
                 IN C[0],..., C[R].;
  BEGIN
  INTEGER X1, X2, X3, X4, I1, I2, I3, I4, J, S3, S4, T3, T4, U3, V, W, L,
          L1, L2, L3, K1, K2, K3, J1, J2, J3, Q1, Q2, Q3, Q4,
          P2, P3, P4, R3, R4;
  LONG REAL M2, M3, M4;
  V := P*Q; W := (R*K) DIV F; K3 := A[4, 4]*A[4, 4]*V;
  FOR J := 0 UNTIL R DO C[J] := 0;
  X1 := 0;
  I1 := 1;                    COMMENT : BEGIN X1 BLOCK;
    BEGIN
B200 :  BEGIN                 COMMENT : BEGIN X2 BLOCK;
      Q1 := X1*A[1, 1];
      Q2 := X1*A[2, 1];
      Q3 := X1*A[3, 1];
      Q4 := X1*A[4, 1];
      M2 := -Q2/A[2, 2];
      M3 := -(Q3 + M2*A[3, 2])/A[3, 3];
      M4 := -(Q4 + M2*A[4, 2] + M3*A[4, 3])/A[4, 4];
```

```
                BEGIN
    COMMENT : THE ABOVE CALCULATES THE MIN. OF THE
              3 DIM. PARABALOID WITH X1 FIXED;
    IF Q1*Q1 + P*(Q2 + M2*A[2, 2])**2 +
    Q*(Q3 + M2*A[3, 2] + M3*A[3, 3])**2 +
    V*(Q4 + M2*A[4, 2] + M3*A[4, 3] + M4*A[4, 4])**2 > W + 1
    THEN GOTO R300;
    X2 := ENTIER(M2) + 1;
    FOR I2 := 1 STEP -2 UNTIL -1 DO
      BEGIN
        BEGIN
B300 :    BEGIN          COMMENT : BEGIN X3 BLOCK;
          P2 := X2*A[2, 2];
          P3 := X2*A[3, 2];
          P4 := X2*A[4, 2];
          M3 := -(Q3 + P3)/A[3, 3];
          M4 := -(Q4 + P4 + M3*A[4, 3])/A[4, 4];
          COMMENT : THE ABOVE CALCULATES THE MIN. OF
                    THE 2 DIM. PARABALOID WITH X1, X2
                    FIXED;
          S3 := Q1*Q1 + P*(Q2 + P2)**2;
          T3 := Q3 + P3;
          U3 := Q4 + P4;
          IF S3 + Q*(T3 + M3*A[3, 3])**2 + V*(U3 + M3*A[4, 3] +
          + M4*A[4, 4])**2 > W + 1 THEN GOTO R200;
          X3 := ENTIER(M3) + 1;
          FOR I3 := 1 STEP -2 UNTIL -1 DO
            BEGIN
              BEGIN
B400 :          BEGIN        COMMENT : BEGIN X4 BLOCK;
                R3 := X3*A[3, 3];
                R4 := X3*A[4, 3];
                M4 := -(U3 + R4)/A[4, 4];
                COMMENT : THE ABOVE CALCULATES THE
                          MIN. OF THE 1 DIM. PARABALOID
                          WITH X1, X2, X3 FIXED;
                S4 := S3 + Q*(T3 + R3)**2;
                T4 := U3 + R4;
                IF S4 + V*(T4 + A[4, 4]*M4]**2 > W + 1
                THEN GOTO R100;
                X4 := ENTIER(M4) + 1;
                FOR I4 := 1 STEP -2 UNTIL -1 DO
```

```
                    BEGIN
                    L := 0;
                    K1 := T4 + X4*A[4, 4];
                    K2 := V*2*A[4, 4]*K1;
                    J2 := J := S4 + V*K1*K1;
                    WHILE J <= W DO
                      BEGIN
                      J1 := (J*F) DIV K;
                      C[J1] := C[J1] + 1;
                      L := L + I4;
                      J := J2 + L*K2 + L*L*K3;
                      END;
                    X4 := ENTIER(M4);
                    END;
                  END;                    COMMENT : END X4 BLOCK;
                X3 := X3 + I3;      GOTO B400;
R100 :          END;
              X3 := ENTIER(M3);
              END;
            END;                          COMMENT : END X3 BLOCK;
          X2 := X2 + I2;      GOTO B300;
R200 :    END;
        X2 := ENTIER(M2);
        END;
      END;                                COMMENT : END X2 BLOCK;
    IF X1 = 0 THEN
      BEGIN
      FOR J3 := 0 UNTIL R DO C[J3] := C[J3] DIV 2;
      END;
    X1 := X1 + I1;      GOTO B200;
R300 : END;
  FOR J := 1 UNTIL R DO C[J] := C[J]*2;
  END;
      COMMENT : END OF X1 BLOCK AND END OF PROCEDURE;
```

Remark 6.3. In the procedure REPRESENTATION. NO we have attempted to be reasonably efficient and not do the same computation again and again. Thus, for example, knowing x^2, we compute $(x + 1)^2$ by using the fact that $(x + 1)^2 = x^2 + 2x + 1$. Also note that an easy modification of the above procedure allows us to explicitly find all $\alpha \in L'$, instead of just the number of such α, with $N(\alpha) = nN(L')$. In the case of weight 2, we just have to count the number of such α, but for modular forms of weight $k > 2$, we would need these α to be determined explicitly (see Step 4 in Section 3 and also Example 5 in Section 9).

7. Finding Representatives of the Ideal Classes

In this section we explain Step 3 in Section 3. Step 2 of the algorithm provides us with an order $\mathcal{O}$ of level N. Assume $\mathcal{O}$ is represented by QORFAC, QORDEN, QOR = (QOR[i, j]) in Notation 4.3.

We can further assume that QORFAC = 1 and that QOR is in Hermite normal form (see Section 5). Let $(f_1, \ldots, f_4) = (1, I, J, K)$ QOR. Thus $\{f_i / \text{QORDEN} \mid i = 1, \ldots, 4\}$ is a basis for $\mathcal{O}$.

Step 3a. Compute (using Theorem 1.12) the class number of (left) ideals for orders of level $N = p^{2r+1}M$, $p \nmid M$ and denote this number by H ($=H(p^{2r+1}M)$). Consider the arrays IDFAC[k], IDDEN[k], ID[i, j, k], and IDNORM[k], where $1 \leqslant k \leqslant H$ and $1 \leqslant i, j \leqslant 4$. Fixing k, IDFAC[k], IDDEN[k], ID[i, j, k] will represent in Notation 4.3 the kth ideal L_k in the set of H-ideals representing all the left $\mathcal{O}$-ideal classes. IDNORM[k] is of course the norm of the kth ideal L_k (it will always be an integer).

Step 3b. Let IDFAC[1] = QORFAC, IDDEN[1] = QORDEN, ID[i, j, 1] = QOR[i, j] for $1 \leqslant i, j \leqslant 4$, and IDNORM[1] = 1.

Step 3c. Suppose at this point we have obtained IDFAC[k], IDDEN[k], ID[i, j, k], and IDNORM[k] for $1 \leqslant k \leqslant t$ and $1 \leqslant i, j \leqslant 4$.

Step 3d. Choose some element $S = (S[1], \ldots, S[4]) \in Z^4$ and let $\alpha = (1/\text{QORDEN})(\sum_j S[j] f_j)$, i.e., $\alpha = (1/\text{QORDEN})(1, I, J, K)(\text{QOR})(S^t) = (1/\text{QORDEN})(1, I, J, K)(D^t)$ where $D = (D[j]) = ((\text{QOR})(S^t)^t \in Z^4$. If $\alpha \in Q$, choose another S. Let DISC = $(\text{Tr}(\alpha)^2 - 4N(\alpha)) = \{(\text{QTRACE}(D))^2 - 4(\text{QNORM}(QA, QB, D))\}/(\text{QORDEN})^2$, the discriminent of the order $Z + Z\alpha$.

Step 3e. Preform the operations:

GAUSS(DISC, A, B, CLASS. NO),

Note that $[2(D[2]I + D[3]J + D[4]K)]^2 = (\text{DISC})(\text{QORDEN})^2$ and thus $Q((\text{DISC})^{1/2})$ has a natural imbedding in $\mathfrak{A} = (QA, QB)$. Consider the array $T'[i, j, k]$ with $1 \leqslant i \leqslant 4$, $1 \leqslant j \leqslant 2$, and $1 \leqslant k \leqslant$ CLASS. NO, where $T'[1, 1, k] = 2A[k](\text{QORDEN})$ for $1 \leqslant k \leqslant$ CLASS. NO; $T'[i, 1, k] = 0$ for $2 \leqslant i \leqslant 4$, $1 \leqslant k \leqslant$ CLASS. NO; $T'[1, 2, k] = -B[k]$ QORDEN for $1 \leqslant k \leqslant$ CLASS. NO; and $T'[i, 2, k] = 2D[i]$ for $2 \leqslant i \leqslant 4$, $1 \leqslant k \leqslant$ CLASS. NO. Also let TNORM[k] = $4A[k](\text{QORDEN})^2$. Then according to Procedure GAUSS, $L'_k = Z(T'[1, 1, k]) + Z(T'[1, 2, k] + T'[2, 2, k]I + T'[3, 2, k]J + T'[4, 2, k]K)$ for $1 \leqslant k \leqslant$ CLASS. NO are representatives of all the distinct ideal classes in the order of discriminant DISC generated by α. By Remark 4.2, TNORM[k] is the norm of the kth ideal.

Step 3f. Let $\nu = 1$.

Step 3g. We "push up" the ideal represented by $T'[i, j, \nu]$, $1 \leqslant i \leqslant 4$, $1 \leqslant j \leqslant 2$, to a left $\mathcal{O}$-ideal. We do this by performing the following operations:

Let $F[i, j] = T'[i, j, \nu]$ for $1 \leqslant i \leqslant 4$, $1 \leqslant j \leqslant 2$;

LATTICE(QA, QB, QORFAC, QORDEN, QOR, 1, 1, F, 2, TF, TD, T);

Now TF, TD, T represents, in Notation 4.3, the left $\mathcal{O}$-ideal $L_\nu = \mathcal{O}L'_\nu$ generated by the ideal L'_ν.

Step 3h. Using REPRESENTATION. NO (T, $-QA$, $-QB$, C, $(TD)^2 \times$ (TNORM[ν]), $(TF)^2$, LIMIT2) we compute the first LIMIT2 Fourier coefficients of the theta series $\theta_{L_\nu}(t)$. We then proceed to compare theta series as in Step 3h in Section 3.

The remainder of Step 3h is self-explanatory with the possible exception of testing whether or not $\overline{T}_\nu L_\gamma$ contains an element of norm $N(T_\nu)\, N(L_\gamma)$. Before we explain this we set

Notation 7.1. If $L = (L[i, j])$ is any 4×4 integer matrix, we denote by $\bar{L}$ the matrix $(\bar{L}[i, j])$ given by $\bar{L}[1, j] = L[1, j]$ for $1 \leqslant j \leqslant 4$ and $\bar{L}[i, j] = -L[i, j]$ for $2 \leqslant i \leqslant 4$, $1 \leqslant j \leqslant 4$. Thus if $L' = Zq_1 + \cdots + Zq_4$ is the lattice represented by LFAC, LDEN, L in Notation 4.3, $\bar{L}' = Z\bar{q}_1 + \cdots + Z\bar{q}_4$ is the lattice represented by LFAC, LDEN, $\bar{L}$ in Notation 4.3.

We can test whether or not $\overline{T}_\nu L_\gamma$ contains an element of norm $N(T_\nu)\, N(L_\gamma)$ as follows:

suppose T_ν is represented by TF, TD, T and L_γ is represented by LF, LD, L in Notation 4.1. Let $N(T)$ and $N(L)$ denote the norms of T_ν and L_γ respectively. Perform the procedures:

LATTICE(QA, QB, TF, TD, $\overline{T}$, LF, LD, L, 4, XF, XD, X);

REPRESENTATION. NO($X, -QA, -QB, C, (XD)^2(N(T))(N(L)), (XF)^2, 1$); If $C[1] = 0$, then $\overline{T}_\nu L_\gamma$ does not contain any elements of norm $N(T_\nu)\, N(L_\gamma)$, while if $C[1] \neq 0$, then $T_\nu L_\gamma$ does contain an element of norm $N(T_\nu)\, N(L_\gamma)$.

We now explain Option 1.

Option 1a. Select an integer μ, $2 \leqslant \mu \leqslant t$.

Option 1b. Perform the operations:

Let $S[i, j] =$ ID$[i, j, \mu]$ for $1 \leqslant i, j \leqslant 4$;

LATTICE(QA, QB, IDFAC[μ], (IDDEN[μ])(NORM[μ]), $\bar{S}$, IDFAC[μ], IDDEN[μ], S, 4, FAC, DEN, TEST2);

REPRESENTATION. NO(TEST2, $-QA$, $-QB$, REP, $(\text{DEN})^2$, $(\text{FAC})^2$, LIMIT2).

If the Fourier coefficients REP[1],..., REP[LIMIT2] are not identical to the corresponding Fourier coefficient in $\theta_{L_1}(\tau)$ ($L_1 = \mathcal{O}$ remember), then the order $L_\mu^{-1}L_\mu$ (which is represented by FAC, DEN, TEST2—see Proposition 1.17) is not isomorphic to $\mathcal{O}$ and we go to Option 1c. Otherwise go to Option 1a, selecting a different μ. If we use up all μ, $2 \leqslant \mu \leqslant t$, Option 1 fails.

Option 1c. Perform the operations:

Replace QORFAC, QORDEN, QOR by FAC, DEN, TEST2.

Replace ID$[i, j, \mu]$ by $\overline{\text{ID}}[i, j, \mu] = \bar{S}[i, j]$, for $1 \leqslant i, j \leqslant 4$.

(Note that IDFAC$[\mu]$, IDDEN$[\mu]$, $\bar{S}$ represents the ideal $\bar{I}_\mu = N(I_\mu)\, I_\mu^{-1} = N(I_\mu)\, I_\mu^{-1} I_1$ as I_1 is the left order of I_μ.)

Replace IDFAC[1], IDDEN[1], (ID$[i, j,)1]$), $1 \leqslant i, j \leqslant 4$ by FAC, DEN, TEST2;

For $k = 2, 3,..., t$, $k \neq \mu$ preform the operations (i) through (v):

(i) Let $Y[i, j] = \text{ID}[i, j, k]$ for $1 \leqslant i, j \leqslant 4$.

(ii) LATTICE(QA, QB, IDFAC$[\mu]$, IDDEN$[\mu]$, $\bar{S}$, IDFACK$[k]$, IDDEN$[k]$, Y, 4, XF, XD, X);

(Note that XF, XD, X represents the ideal $\bar{I}_\mu I_k = N(I_\mu)\, I_\mu^{-1} I_k$).

(iii) Replace NORM$[k]$ by (NORM$[\mu]$)(NORM$[k]$).

(iv) If $(XF)^2 \mid$ NORM$[k]$, then replace NORM$[k]$ by NORM$[k]/(XF)^2$ and replace XF by 1; (Note that NORM$[k] = ((XF)^2/(XD)^2)W$ for some integer W and so $(XF)^2 \mid$ NORM$[k]$. We use the "if" statement because we are very cautions.)

(v) Replace IDFAC$[k]$, IDDEN$[k]$, ID$[i, j, k]$ for $1 \leqslant i, j \leqslant 4$ by XF, XD, X;

Option 1d. Go to Step 3d (in Section 3).

This completes our discussion of Option 1 and also our explanation of how to find representations of the left-ideal classes for some order of level N in $\mathfrak{A}$.

8. Calculating the Theta Series and the Brandt Matrices

This section explains Step 4 of the algorithm. First we consider the case of cusp forms of weight 2 on $\Gamma_0(N)$. The modified Brandt matrices $B_0'(n)$, $(n, N) = 1$ give a representation of the Hecke operators $T_2(n)$, $(n, N) = 1$ on the vector space of cusp forms $\langle\theta_1(t)\rangle \oplus \cdots \oplus \langle\theta_d(t)\rangle$ in the notation of Theorem 2.28. Further if $B_0'(n) = (b_{ij}'(n))$, then the theta series $\sum_{n=1}^{\infty} b_{ij}'(n) \exp(n)$ (for $1 \leqslant i, j \leqslant H - 1$) are the theta series we are interested in computing. Thus we need only compute the $B_0'(n)$ to obtain all the relevant information. By Lemma 2.19,

once we have computed the Brandt matrices $B_0(n)$, obtaining the modified Brandt matrices $B_0'(n)$ is trivial. Hence we compute $B_0(n)$ for $n = 0, 1, \ldots,$ LIMIT1. As is noted in Step 4 in Section 3, $\sum_{n=0}^{\infty} B_0(n) \exp(n\tau) = (1/e_j\theta_{L_jL_i}(\tau))$ and $\theta_{L_jL_i}(\tau) = \theta_{L_iL_j}(\tau)$ where e_j is the first (not the zeroth) Fourier coefficient of $\theta_{L_jL_j}(\tau)$. Thus we need only calculate the 0th, 1st,..., LIMIT1th Fourier coefficients of $\theta_{L_iL_k}(\tau)$ for $1 \leqslant l \leqslant k \leqslant H$. But the Fourier coefficients of $\theta_{L_iL_k}(\tau)$ are given by the operations:

Let $F[i, j] = \mathrm{ID}[i, j, l]$ for $1 \leqslant i, j \leqslant 4$;

Let $G[i, j] = \mathrm{ID}[i, j, k]$ for $1 \leqslant i, j \leqslant 4$;

LATTICE(QA, QB, IDFAC[l], IDDEN[l], $\bar{F}$, IDFAC[k], IDDEN[k], G, 4, XF, XD, X).

REPRESENTATION. NO(X, $-QA$, $-QB$, REP, $(XD)^2 \cdot$ IDNORM[l] $\cdot$ IDNORM[k], $(XF)^2$, LIMIT1).

9. Examples

In this section we give numerical examples computed using the algorithm. They have been chosen to illustrate various aspects of the theory of Brandt Matrices, theta series, and the basis problem.

Example 1. Our first example $S_2(37)$ is of historical interest. 37 is the first prime for which Hecke's original conjecture—which began the basis problem—fails (see Remark 2.16 above, [12, p. 169; 38, 40]). By Propositions 5.1 and 5.2 the quaternion algebra $\mathfrak{A}(37)$ equals $(-2, -37)$ and a (maximal) order $\mathcal{O}$ of level 37 has Z-basis $\frac{1}{2}(1 + J + K)$, $\frac{1}{4}(I + 2J + K)$, J, and K. The class number (Theorem 1.12) is 3. Using Step 3 of Section 3 (see also Section 7) we find $I_1 = \mathcal{O}$, $I_2 = Z(2 + 6J + 10K) + Z(I + 2J + 9K) + Z(12J + Z(12K)$, and $I_3 = Z(2 + 26J + 26K) + Z(I + 2J + 13K) + Z(28J) + Z(28K)$ are representatives of the left $\mathcal{O}$-ideal classes. Their norms are $N(I_1) = 1$, $N(I_2) = 48$, $N(I_3) = 112$. The corresponding Brandt matrices $B(n) = B_0(n; 37, 1)$ for $n \leqslant 19$ are

$$B(0) \quad \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \qquad B(1) \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad B(2) \quad \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 2 \\ 1 & 2 & 0 \end{pmatrix} \qquad B(3) \quad \begin{pmatrix} 2 & 1 & 1 \\ 1 & 0 & 3 \\ 1 & 3 & 0 \end{pmatrix} \qquad B(4) \quad \begin{pmatrix} 1 & 3 & 3 \\ 3 & 3 & 1 \\ 3 & 1 & 3 \end{pmatrix}$$

$$B(5) \quad \begin{pmatrix} 2 & 2 & 2 \\ 2 & 1 & 3 \\ 2 & 3 & 1 \end{pmatrix} \qquad B(6) \quad \begin{pmatrix} 4 & 4 & 4 \\ 4 & 7 & 1 \\ 4 & 1 & 7 \end{pmatrix} \qquad B(7) \quad \begin{pmatrix} 2 & 3 & 3 \\ 3 & 2 & 3 \\ 3 & 3 & 2 \end{pmatrix} \qquad B(8) \quad \begin{pmatrix} 5 & 5 & 5 \\ 5 & 5 & 5 \\ 5 & 5 & 5 \end{pmatrix} \qquad B(9) \quad \begin{pmatrix} 3 & 5 & 5 \\ 5 & 7 & 1 \\ 5 & 1 & 7 \end{pmatrix}$$

$$B(10)\quad \begin{pmatrix} 6 & 6 & 6 \\ 6 & 8 & 4 \\ 6 & 4 & 8 \end{pmatrix} \qquad B(11)\quad \begin{pmatrix} 6 & 3 & 3 \\ 3 & 2 & 7 \\ 3 & 7 & 2 \end{pmatrix} \qquad B(12)\quad \begin{pmatrix} 8 & 10 & 10 \\ 10 & 6 & 12 \\ 10 & 12 & 6 \end{pmatrix} \qquad B(13)\quad \begin{pmatrix} 2 & 6 & 6 \\ 6 & 3 & 5 \\ 6 & 5 & 3 \end{pmatrix} \qquad B(14)\quad \begin{pmatrix} 8 & 8 & 8 \\ 8 & 9 & 7 \\ 8 & 7 & 9 \end{pmatrix}$$

$$B(15)\quad \begin{pmatrix} 8 & 8 & 8 \\ 8 & 11 & 5 \\ 8 & 5 & 11 \end{pmatrix} \qquad B(16)\quad \begin{pmatrix} 13 & 9 & 9 \\ 9 & 9 & 13 \\ 9 & 13 & 9 \end{pmatrix} \qquad B(17)\quad \begin{pmatrix} 10 & 4 & 4 \\ 4 & 7 & 7 \\ 4 & 7 & 7 \end{pmatrix} \qquad B(18)\quad \begin{pmatrix} 13 & 13 & 13 \\ 13 & 7 & 19 \\ 13 & 19 & 7 \end{pmatrix} \qquad B(19)\quad \begin{pmatrix} 8 & 6 & 6 \\ 6 & 7 & 7 \\ 6 & 7 & 7 \end{pmatrix}.$$

Note that in the notation of (2.5), $\theta_{21}(\tau) = \theta_{31}(\tau)$, so that the cusp forms $\theta_{21}(\tau) - \theta_{11}(\tau)$ and $\theta_{31}(\tau) - \theta_{11}(\tau)$ are equal and hence do not span the two-dimensional space $S_2(37)$. This gives a counterexample to Hecke's conjecture. Note that Hecke himself checked his conjecture for all primes $\leqslant 37$ (see [18, p. 884]) so he probably realized 37 was an inportant example but not having computers he must have erred. As the type number is 2 in this case, one can check that the case $p = 37$ satisfies the modified version of Hecke's conjecture given in [38]. We note that dimensions of $S_2(N)$ and $S_2^0(N)$ for $N \leqslant 300$ can be found in [3].

From $B(0)$ we see $e_1 = e_2 = e_3 = 2$. One can check that the $B(n)$ above satisfy the conclusions of Propositions 2.18 and 2.22, i.e., they are (in this case since all e_i are equal) symmetric, the row sums are independent of the row (and are equal to deg $T_2(n)$ if $(n, 37) = 1$, in particular equal to $n + 1$ for primes $n \neq 37$), $B(n)\,B(m) = B(nm)$ if $(n, m) = 1$, $B(l^r)\,B(l^s) = \sum_{\sigma=0}^{t} l^\sigma B(l^{r+s-2\sigma})$, where $t = \min(r, s)$ for primes $l \neq 37$, and the $B(n)$, $(n, 37) = 1$ are simultaneously diagonalizable. Note that these are a rather stingent set of conditions for a set of matrices to satisfy and the fact that the $B(n)$ do satisfy them gives one confidence in the algorithm.

The matrix A of Lemma 2.19 is

$$A = \begin{pmatrix} 1 & 1 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & -1 \end{pmatrix} \quad \text{so} \quad A^{-1} = \frac{1}{3}\begin{pmatrix} 1 & 1 & 1 \\ 1 & -2 & 1 \\ 1 & 1 & -2 \end{pmatrix}$$

and the first few $AB(n)\,A^{-1}$ for $0 \leqslant n \leqslant 4$ are

$$\frac{1}{2}\begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 3 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 1 & -1 \end{pmatrix} \quad \begin{pmatrix} 4 & 0 & 0 \\ 0 & -1 & 2 \\ 0 & 2 & -1 \end{pmatrix} \quad \begin{pmatrix} 7 & 0 & 0 \\ 0 & 0 & -2 \\ 0 & -2 & 0 \end{pmatrix}.$$

We see that conjugating by A behaves according to Lemma 2.19. In particular the entries in the lower right-hand block of the $AB(n)\,A^{-1}$ give Fourier Coefficients of cusp forms.

The $B(n)$ can be simultaneously diagonalized by conjugation by

$$C = \begin{pmatrix} 2 & 2 & 2 \\ 2 & -1 & -1 \\ 0 & 3 & -3 \end{pmatrix}, \qquad C^{-1} = \frac{1}{6}\begin{pmatrix} 1 & 2 & 0 \\ 1 & -1 & 1 \\ 1 & -1 & -1 \end{pmatrix}.$$

Letting $x = e^{2\pi i\tau}$ we have

$$\sum_{n=0}^{\infty} CB(n)\, C^{-1}x^n = \begin{pmatrix} f(\tau) & 0 & 0 \\ 0 & \theta_1(\tau) & 0 \\ 0 & 0 & \theta_2(\tau) \end{pmatrix},$$

where $f(\tau) = \frac{3}{2} + x + 3x^2 + 4x^3 + 7x^4 + 6x^5 + 12x^6 + 8x^7 + 15x^8 + 13x^9 + 18x^{10} + 12x^{11} + \cdots$, $\theta_1(\tau) = x + x^3 - 2x^4 - x^7 - 2x^9 + 3x^{11} - 2x^{12} - 4x^{13} + 4x^{16} + 6x^{17} + 2x^{19} - x^{21} + \cdots$, $\theta_2(\tau) = x - 2x^2 - 3x^3 + 2x^4 - 2x^5 + 6x^6 - x^7 + 6x^9 + 4x^{10} - 5x^{11} - 6x^{12} - 2x^{13} + 2x^{14} + \cdots$.

Here $f(\tau)$ is an Eisenstein series on $\Gamma_0(37)$ (the transform of the zeta function of $\mathcal{O}$) and $\theta_1(\tau)$ and $\theta_2(\tau)$ are by Corollary 2.29 the newforms in $S_2{}^0(37) = S_2(37)$.

We now explain how to determine the action of the canonical involution E on the $\theta_i(\tau)$. First we explain how to determine the action of E on $S_2(p)$ for any prime. The canonical involution E for modular forms $M_k(p)$ on $\Gamma_0(p)$ is given by the matrix $\left(\begin{smallmatrix} 0 & -1 \\ p & 0 \end{smallmatrix}\right)$ and as we are considering the case of prime level $E = W_p$, the W-operator of Atkin and Lehner (see [2]). For $q(\tau) \in M_2(p)$, we have

$$q \mid E(\tau) = p^{-1}\tau^{-2}q(-1/p\tau).$$

THEOREM 9.1. *Let p be a prime and consider modular forms of weight 2 on $\Gamma_0(p)$. Let $\theta_{ij}(\tau)$ be the entries of the Brandt matrix series, $(\theta_{ij}(\tau)) = \sum_{n=0}^{\infty} B_0(n; p, 1)x^n$. Then the action of E on the $\theta_{ij}(\tau)$ is given by the matrix $-B(p) = -B_0(p; p, 1)$, i.e., $\Theta_{ij} \mid E$ is equal to the i, jth entry of $\sum_{n=0}^{\infty} ((-B(p))(B(n))\, x^n$ where the product $(-B(p))(B(n))$ is a matrix product.*

COROLLARY 9.2. *If we diagonalize the Brandt Matrix series so as to obtain the newforms $\theta_1(\tau), \ldots, \theta_d(\tau)$ of $S_2(p)$ in the notation of Corollary 2.29, the corresponding diagonalization of $-B(p)$ will give the action of E on the $\theta_i(\tau)$.*

Proof of Theorem 9.1. Let $\mathcal{O}$ be a (maximal) order of level p. Then $\mathcal{O}$ contains a unique ideal, say P, of norm p and P is a two-sided ideal (see [14, Chap. II]. By Theorem 3.2 of [37], the action of E on a theta series $\theta_I(\tau)$ attached to a left Q-ideal I is as follows: $\theta_I \mid E(\tau) = -\theta_{PI}(\tau)$ in the notation of Proposition 2.17 above. By Theorem 9.20 and Remarks 9.22 and 9.25 of [39], this translates to: $\theta_{ij} \mid E$ is equal to the i, jth entry of $\sum_{n=0}^{\infty} ((-\tilde{W}_0(P))\, B(n))\, x^n$, where $\tilde{W}_0(P)$ is given by Definition 9.1 of [39]. Hence we need only show that $B(p)$ equals $\tilde{W}_0(P)$. Let $I_1, \ldots, I_H$ be the representatives of the left $\mathcal{O}$-ideal classes in terms of which the $B(n)$ are defined and let $\mathcal{O}_i$ be the right order of I_i. There exists

idèles $\tilde{\gamma}_i \in J_{\mathfrak{A}}$ such that $I_i = \mathcal{O}\tilde{\gamma}_i$ and $\mathcal{O}_i = \tilde{\gamma}_i^{-1}\mathcal{O}\tilde{\gamma}_i$ for $i = 1,\ldots, H$. For an explanation of the idèlic language used in this proof see [37]. Let $B(p) = (b_{ij}(p))$. As we saw in the proof of Lemma 2.18 above, $b_{ij}(p)$ is equal to the number of integral left $\mathcal{O}_i$-idelas in the same class as $I_i^{-1}I_j$ having norm p. But $\mathcal{O}_i$ has a unique ideal of norm p, namely, $P_i = \tilde{\gamma}_i^{-1}P\tilde{\gamma}_i$. Hence, precisely one entry of the row $b_{i1}(p)$, $b_{i2}(p),\ldots, b_{iH}(p)$ is one and the rest are zero. Further $b_{ij}(p) = 1$ if and only if there exists $\alpha \in \mathfrak{A}^x$ such that $I_i^{-1}I_j\alpha = P_i$ if and only if $I_j\alpha = I_iP_i = \mathcal{O}\tilde{\gamma}_i\tilde{\gamma}_i^{-1}P\tilde{\gamma}_i = P\tilde{\gamma}_i = PI_i$. This is precisely how the matrix $\tilde{W}_0(P)$ is defined (see Definition 9.1 of [39]).

Remark 9.3. If the Conjecture 9.24 of [39] concerning the action of the W-operators is true, the above argument would show that for the case of level $N = pM$, $(p, M) = 1$ the W-operator W_p would correspond to the matrix $-B_0(p; p, M)$.

Now let us return to our example $S_2(37)$.

$$B(37) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \quad \text{and} \quad CB(37)C^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Thus $\theta_1 \mid E = -\theta_1$ and $\theta_2 \mid E = \theta_2$. Note that this is in agreement with [3] which indicates that the two newforms in $S_2^0(37)$ have distinct eigenvalues under E.

EXAMPLE 2. Our next example, $S_2^0(15)$ shows that newforms for composite levels can be computed in several ways. This has the by-product of producing nontrivial linear relations among theta series attached to quaternary quadratic forms. For other ways of obtaining linear relations among theta series, see the paper of Kneser ([23]).

First let $p = 3$ and $M = 5$. An order of level 15 in $\mathfrak{A}(3) = (-1, -3)$ is given by $\mathcal{O} = Z(\frac{1}{2}(1 + J + 2K)) + Z(\frac{1}{2}(I + 5K)) + Z(J + 2K) + Z(5K)$. The class number is 2 and ideal class representatives are $I_1 = \mathcal{O}$ and $I_2 = Z(3 + J + 2K) + Z(3I + 5K) + Z(2J + 4K) + Z(10K)$. Further $N(I_1) = 1$ and $N(I_2) = 12$. The first few Brandt matrices are

$$\begin{array}{ccccccc} B(0) & B(1) & B(2) & B(3) & B(4) & B(5) & B(6) \\ \frac{1}{4}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} & \begin{pmatrix} 3 & 4 \\ 4 & 3 \end{pmatrix} & \begin{pmatrix} 6 & 5 \\ 5 & 6 \end{pmatrix} & \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}. \end{array}$$

Conjugating by $A = \left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$ we have

$$\sum_{n=0}^{\infty} AB(n)\, A^{-1}x^n = \begin{pmatrix} f(\tau) & 0 \\ 0 & \theta(\tau) \end{pmatrix}.$$

By Corollary 2.29 $\langle\theta(\tau)\rangle \cong 2S_2^0(3) \oplus S_2^0(15) = S_2^0(15)$ so

$$\theta(\tau) = x - x^2 - x^3 - x^4 + x^5 + x^6 + 3x^8 + x^9 - x^{10} - 4x^{11} + x^{12} - 2x^{13} - x^{15} - x^{16} + \cdots \tag{9.1}$$

is the newform in $S_2^0(15)$. Note that $N(x_1 + x_2I + x_3J + x_4K) = x_1^2 + x_2^2 + 3x_3^2 + 3x_4^2$. Let $q_i(\tau) = \theta_{I_i}(\tau) = \sum_{\alpha\in I_i} \exp(N(\alpha)\tau/N(I_i))$ for $i = 1, 2$ be the theta series attached to the quadratic form $N(x)/N(I_i)$ on the lattice I_i. Then $q_i(\tau) = 4\theta_{i1}(\tau)$ in the notation of (2.5):

$$q_1(\tau) = 1 + 4x + 4x^2 + 12x^4 + 24x^5 + 8x^6 + 16x^7 + 36x^8 + \cdots,$$
$$q_2(\tau) = 1 + 8x^2 + 4x^3 + 16x^4 + 20x^5 + 4x^6 + 16x^7 + 24x^8 + \cdots.$$

We see that $q_1(\tau) - q_2(\tau) = 4\theta(\tau)$.

On the other hand we can let $p = 5$ and $M = 3$. An order of level 15 in $\mathfrak{A}(5) = (-2, -5)$ is $\mathcal{O}' = Z(\frac{1}{2}(1 + J + 3K)) + Z(\frac{1}{4}(I + 2J + K)) + Z(J) + Z(3K)$. The class number is again 2 and ideal class representatives are $J_1 = \mathcal{O}'$ and $J_2 = Z(1 + 3J + 3K) + Z(I + 2J + K) + Z(4J) + Z(6K)$. $N(J_1) = 1$ and $N(J_2) = 8$. The first few Brandt matrices are

$$\begin{array}{ccccccc} B(0) & B(1) & B(2) & B(3) & B(4) & B(5) & B(6) \\ \frac{1}{6}\begin{pmatrix}3 & 1\\ 3 & 1\end{pmatrix} & \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} & \begin{pmatrix}2 & 1\\ 3 & 0\end{pmatrix} & \begin{pmatrix}5 & 2\\ 6 & 1\end{pmatrix} & \begin{pmatrix}5 & 2\\ 6 & 1\end{pmatrix} & \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} & \begin{pmatrix}16 & 5\\ 15 & 6\end{pmatrix}. \end{array}$$

Conjugating by $A = \frac{1}{3}\left(\begin{smallmatrix}3 & 1\\ 3 & -3\end{smallmatrix}\right)$ we have

$$\sum_{n=0}^{\infty} AB(n)\, A^{-1} = \begin{pmatrix} f'(\tau) & 0 \\ 0 & \theta'(\tau)\end{pmatrix}.$$

By Corollary 2.29, $\langle\theta'(\tau)\rangle \cong 2S_2^0(5) \oplus S_2^0(15) = S_2^0(15)$ so $\theta'(\tau)$ is the newform in $S_2^0(15)$, i.e., $\theta'(\tau) = \theta(\tau)$ and the Fourier coefficients of $\theta'(\tau)$ are given by (9.1). Now $N(x_1 + x_2I + x_3J + x_4K) = x_1^2 + 2x_2^2 + 5x_3^2 + 10x_4^2$. Let $q_i'(\tau) = \theta_{J_i}(\tau) = \sum_{\alpha\in J_i} \exp(N(\alpha)\tau/N(J_i))$ for $i = 1, 2$. Then $q_1'(\tau) = 1 + 2x + 4x^2 + 10x^3 + 10x^4 + 2x^5 + 32x^6 + 12x^7 + 24x^8 + 38x^9 + \cdots$ and $q_2'(\tau) = 1 + 6x^2 + 12x^3 + 12x^4 + 30x^6 + 12x^7 + 18x^8 + 36x^9 + 6x^{10} + \cdots$. We see $q_1'(\tau) - q_2'(\tau) = 2\theta'(\tau)$. Hence we obtain the nontrivial relation

$$q_1(\tau) - q_2(\tau) = 2q_1'(\tau) - 2q_2'(\tau) = 4x - 4x^2 - 4x^3 - 4x^4 + \cdots. \tag{9.2}$$

This same procedure can be applied with any composite N as the level and shows that there are infinitely many nontrivial relations among theta series attached to quaternary quadratic forms

EXAMPLE 3. Let $N = 54$ and set $p = 3$, $r = 1$, and $M = 2$. $\mathfrak{A}(3) = (-1, -3)$ and an order $\mathcal{O}$ of level 54 in $\mathfrak{A}(3)$ is given by $\mathcal{O} = Z(\frac{1}{2}(1 + I + 3J +$

$K)) + Z(I + K) + Z(3J) + Z(3K)$. The class number is 5 and the first few Brandt matrices $B_0(n)$ are

$$B(0) \quad \frac{1}{4}\begin{pmatrix} 2 & 2 & 2 & 1 & 2 \\ 2 & 2 & 2 & 1 & 2 \\ 2 & 2 & 2 & 1 & 2 \\ 2 & 2 & 2 & 1 & 2 \\ 2 & 2 & 2 & 1 & 2 \end{pmatrix} \qquad B(1) \quad \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \qquad B(2) \quad \begin{pmatrix} 0 & 1 & 1 & 1 & 2 \\ 1 & 2 & 1 & 0 & 1 \\ 1 & 1 & 2 & 0 & 1 \\ 2 & 0 & 0 & 1 & 2 \\ 2 & 1 & 1 & 1 & 0 \end{pmatrix}$$

$$B(4) \quad \begin{pmatrix} 2 & 3 & 3 & 1 & 4 \\ 3 & 3 & 2 & 2 & 3 \\ 3 & 2 & 3 & 2 & 3 \\ 2 & 4 & 4 & 1 & 2 \\ 4 & 3 & 3 & 1 & 2 \end{pmatrix} \qquad B(5) \quad \begin{pmatrix} 2 & 1 & 1 & 0 & 2 \\ 1 & 0 & 3 & 1 & 1 \\ 1 & 3 & 0 & 1 & 1 \\ 0 & 2 & 2 & 2 & 0 \\ 2 & 1 & 1 & 0 & 2 \end{pmatrix} \qquad B(7) \quad \begin{pmatrix} 1 & 2 & 2 & 1 & 2 \\ 2 & 1 & 2 & 1 & 2 \\ 2 & 2 & 1 & 1 & 2 \\ 2 & 2 & 2 & 0 & 2 \\ 2 & 2 & 2 & 1 & 1 \end{pmatrix};$$

$B(3)$ and $B(6)$ are identically zero. Letting

$$C = \begin{pmatrix} 4 & 4 & 4 & 2 & 4 \\ -9 & 0 & 0 & 0 & 9 \\ 1 & -2 & -2 & 2 & 1 \\ 2 & -1 & -1 & -2 & 2 \\ 0 & -9 & 9 & 0 & 0 \end{pmatrix}, \qquad C^{-1} = \frac{1}{18}\begin{pmatrix} 1 & -1 & 1 & 2 & 0 \\ 1 & 0 & -2 & -1 & -1 \\ 1 & 0 & -2 & -1 & 1 \\ 1 & 0 & 4 & -4 & 0 \\ 1 & 1 & 1 & 2 & 0 \end{pmatrix},$$

we find

$$\sum_{n=0}^{\infty} CB_0(n)\, C^{-1}x^n = \begin{pmatrix} f(\tau) & & & & \\ & \theta_1(\tau) & & 0 & \\ & & \theta_2(\tau) & & \\ & 0 & & \theta_3(\tau) & \\ & & & & \theta_4(\tau) \end{pmatrix},$$

where

$$\theta_1(\tau) = x - 2x^2 - 2x^4 - x^7 + 4x^8 + 5x^{13} + 2x^{14} + 4x^{16} - 7x^{19} - 5x^{25} - 10^{26} + \cdots,$$

$$\theta_2(\tau) = x + 2x^2 - 2x^4 - x^7 - 4x^8 + 5x^{13} - 2x^{14} + 4x^{16} - 7x^{19} - 5x^{25} + 10x^{26} + \cdots,$$

$$\theta_3(\tau) = x - x^2 + x^4 + 3x^5 - x^7 - x^8 - 3x^{10} - 3x^{11} - 4x^{13} + x^{14} + x^{16} + 2x^{19} + 3x^{20} + \cdots,$$

$$\theta_4(\tau) = x + x^2 + x^4 - 3x^5 - x^7 + x^8 - 3x^{10} + 3x^{11} - 4x^{13} - x^{14} + x^{16} + 2x^{19} - 3x^{20} + \cdots.$$

By Corollary 2.29

$$\langle\theta_1(\tau)\rangle \oplus \cdots \oplus \langle\theta_4(\tau)\rangle \cong 2S_2^0(3) \oplus 2S_2^0(27) \oplus S_2^0(6) \oplus S_2^0(54). \quad (9.3)$$

As $S_2^0(3) = S_2^0(6) = 0$ (see [3]) we have

$$\langle\theta_1(\tau)\rangle \oplus \cdots \oplus \langle\theta_4(\tau)\rangle \cong 2S_2^0(27) \oplus S_2^0(54). \tag{9.4}$$

We see immediately that $\theta_1(\tau) \sim \theta_2(\tau)$, that is, they have the same eigenvalues for the Hecke operators $T_2(n)$, $(n, 54) = 1$ (the eigenvalue for $T_2(n)$ is given by the nth Fourier coefficient). Thus $\langle\theta_1(\tau)\rangle \cong \langle\theta_2(\tau)\rangle \cong S_2^0(27)$. Since $\theta_1(\tau)$ and $\theta_2(\tau)$ are eigenforms in $S_2(54)$, they must be oldforms (see [2]). If $q(\tau)$ is the newform in $S_2^0(27)$, then by the main Theorem 5 of Atkin–Lehner ([2]) $\theta_1(\tau)$ and $\theta_2(\tau)$ must be a linear combination of $q(\tau)$ and $q(2\tau)$. In fact

$$q(\tau) = x - 2x^4 - x^7 + 5x^{13} + 4x^{16} - 7x^{19} - 5x^{25} + \cdots$$

(which we found using our algorithm) and $\theta_1(\tau) = q(\tau) - 2q(2\tau)$ and $\theta_2(\tau) = q(\tau) + 2q(2\tau)$. Since $\theta_3(\tau)$ and $\theta_4(\tau)$ are not equivalent to any other $\theta_i(\tau)$ (i.e., they occur with multiplicity one) by (9.4) they must be the newforms in $S_2^0(54)$. Note that $\dim S_2^0(54) = 2$ by [3]. This illustrates the algorithm for finding all newforms on $\Gamma_0(N)$ if N is not a perfect square given by Corollary 7 of [36]. Note that if in (9.3) $S_2^0(6)$ were nonzero, we would first have had to consider the case $N = 6$ to be able to distinguish $S_2^0(6)$ from $S_2^0(54)$—checking the $\theta_i(\tau)$ for multiplicity one would not have been sufficient. Note also that if $\phi(n) = (n/3)$ and $\theta_3(\tau) = \sum_{n-1}^{\infty} a(n)\, x^n$, then $\theta_4(\tau) = \sum_{n-1}^{\infty} \phi(n)\, a(n)\, x^n$. This is explained by Theorem 3.1 of Atkin and Li ([4], also see [22]). Finally note that if we were just interested in $S_2^0(54)$, it would have been easier but less interesting to let $p = 2$ and $M = 27$.

EXAMPLE 4. In this example we consider the case of square level (specifically $N = 49$) briefly alluded to in Remark 2.32. The algorithm works without change. $\mathfrak{A}(7) = (-1, -7)$. By Theorem 1.5 of [39] any order of index 7 in a maximal order of $\mathfrak{A}(7)$ is an order of "level" 49. One such is $\mathcal{O} = Z(\frac{1}{2}(1 + J)) + Z(\frac{1}{2}(7I + K)) + Z(J) + Z(K)$. The class number (see Theorem 4.18 of [39]) is 4 and the first few Brandt matrices are

$$\begin{array}{cccc} B(0) & B(1) & B(2) & B(3) \\ \frac{1}{2}\begin{pmatrix} 1&1&1&1\\1&1&1&1\\1&1&1&1\\1&1&1&1 \end{pmatrix} & \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix} & \begin{pmatrix} 2&1&0&0\\1&2&0&0\\0&0&2&1\\0&0&1&2 \end{pmatrix} & \begin{pmatrix} 0&0&2&2\\0&0&2&2\\2&2&0&0\\2&2&0&0 \end{pmatrix} \\ B(4) & B(5) & B(6) & B(7) \\ \begin{pmatrix} 3&4&0&0\\4&3&0&0\\0&0&3&4\\0&0&4&3 \end{pmatrix} & \begin{pmatrix} 0&0&3&3\\0&0&3&3\\3&3&0&0\\3&3&0&0 \end{pmatrix} & \begin{pmatrix} 0&0&6&6\\0&0&6&6\\6&6&0&0\\6&6&0&0 \end{pmatrix} & \begin{pmatrix} 2&2&2&2\\2&2&2&2\\2&2&2&2\\2&2&2&2 \end{pmatrix}. \end{array}$$

Letting

$$C = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 2 & -2 & 0 & 0 \\ 0 & 0 & 2 & -2 \end{pmatrix}, \qquad C^{-1} = \frac{1}{4}\begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 1 & -1 & 0 \\ 1 & -1 & 0 & 1 \\ 1 & -1 & 0 & -1 \end{pmatrix}$$

we have

$$\sum_{n=0}^{\infty} CB(n)\, C^{-1}x^n = \begin{pmatrix} f_1(\tau) & & 0 & \\ & f_2(\tau) & & \\ & 0 & \theta_1(\tau) & \\ & & & \theta_2(\tau) \end{pmatrix}.$$

If $q(\tau) = \sum_{n=0}^{\infty} a(n)\, x^n$ and χ is a Direchlet character, we let $q^{\chi} = \sum_{n=0}^{\infty} \chi(n) \times a(n)\, x^n$. By Theorem 5.34 of [39], $f_1(\tau)$ should be the transform of the zeta function of $\mathcal{O}$ and $f_2 - f_1^{\phi} = \sum_{n=0}^{\infty} a(n)\, x^n$ with $a(n) = 0$ if $p \nmid n$ where $\phi(n) = (n/7)$. In fact we find $f_1(\tau) = 2 + x + 3x^2 + 4x^3 + 7x^4 + 6x^5 + 12x^6 + 8x^7 + 15x^8 + 13x^9 + 18x^{10} + \cdots$ and $f_2(\tau) = f_1^{\phi}(\tau)$. By Proposition 10.1 of [39],

$$2S_2^0(49) \oplus S_2^0(7) \cong \langle\theta_1(\tau)\rangle \oplus \langle\theta_2(\tau)\rangle \oplus S_2^0(7)^{\phi} \oplus 2 \sum_{\substack{\{\psi\} \\ \{\psi^2 \neq 1\}}} S_2(7, \psi^2)^{\bar{\psi}},$$

where $S_2(p, \psi^2)$ denotes the space of cusp forms of weight 2 on $\Gamma_0(p)$ with character ψ^2, $S_2(p, \psi^2)^{\bar{\psi}} = \{f^{\bar{\psi}} \mid f \in S_2(p, \psi^2)\}$, $\phi = (n/7)$, and the sum $\sum_{\{\psi\},\{\psi^2\neq 1\}}$ is over a set of representatives of the pairs $\{\psi, \bar{\psi}\}$ of the characters of $(Z/7Z)^x$ with $\psi^2 \neq 1$. In our case $\dim S_2^0(49) = 1$, $S_2^0(7) = 0$ so $S_2^0(7, \psi^2) = 0$ for all ψ and $2S_2^0(49) \cong \langle\theta_1(\tau)\rangle \oplus \langle\theta_2(\tau)\rangle$. Thus $\theta_1(\tau) = \theta_2(\tau)$ is the newform in $S_2^0(49)$. In fact we have

$$\theta_1(\tau) = \theta_2(\tau) = x + x^2 - x^4 - 3x^8 - 3x^9 + 4x^{11} - x^{16} - 3x^{18} + 4x^{22} + 8x^{23} - 5x^{25} + \cdots.$$

By Theorem 5.34 of [39], since $\theta_i(\tau)$ are newforms, $\theta_1^{\phi} = \theta_2 = \theta_1$ so for all $n \equiv 0, 3, 5$ or $6 \pmod 7$, the nth Fourier coefficient of $\theta_1(\tau)$ must be zero. Note also that 13 is the first prime p for which $S_2(p, \psi^2) \neq 0$ for some character $\psi^2 \neq 1$ of $(Z/pZ)^x$. This is the reason 13^2 is the first level $N > 1$ for which $S_2^0(N)$ is not generated by theta series attached to quaternion algebras (see [31, 39]).

EXAMPLE 5. Our last example, $S_2^0(16, \phi)$, was computed by Shemanske using a slightly modified version of the algorithm to construct the newform in $S_3^0(16, \phi)$ where ϕ is the nontrivial Dirichlet character mod 4 ($\phi(n) = (-1)^{n-1/2}$ if n is odd and $\phi(n) = 0$ if n is even). By $S_3^0(16, \phi)$ we mean the subspace of $S_3(16, \phi)$ generated by newforms (see [26] or [27]). The basis problem for cusp

forms with character will be considered in [22]. Let $\mathfrak{A}(2) = (-1, -1)$ and let $\mathcal{O}$ be an order of $\mathfrak{A}(2)$ having index 8 in the maximal order and such that $\mathcal{O}_2 = \mathcal{O} \otimes_Z Z_2$ contains a subring isomorphic to $Z_2 + Z_2\sqrt{-1}$, i.e., let $\mathcal{O}$ be a "$\sqrt{-1}$-order of level 16"—see Shemanske [45]. Such an order is $\mathcal{O} = Z + Z(I) + Z(2J) + Z(2K)$. In a manner similar to Eichler [14, pp. 109–110] one can define a character (which we still call ϕ) on $\mathcal{O}$ such that $\phi \mid Z = \phi$ and then again in analogy with Eichler ([14, p. 110]) one defines Brandt matrices $B_1(n; \phi)$ with character ϕ. In order to explicitly compute the $B_1(n; \phi)$, one needs to modify the Procedure REPRESENTATION. NO of Section 6 so that instead of computing the number of representatives α such that $F/KN(\alpha) = n$, one computes the representatives themselves. (So that one can evaluate $\phi(\alpha)\, X_1(\alpha)$, see Step 4 of Section 3 and also [14, p. 110].) This is easy since at the 25th line from the end of the procedure ($C[J1] := C[J1] + 1$), the 4-tuple ($X1$, $X2$, $X3$, $X4 + L$) gives the coefficients in terms of the basis of the lattice of an element α with $F/KN(\alpha) = J1$. Note that only ($X1$, $X2$, $X3$, $X4 + L$) with $X1 \geqslant 0$ are computed, so if $X1 > 0$, one also has to add the representative $(-X1, -X2, -X3, -(X4 + L))$.

The class number of $\mathcal{O}$ is 2 so the $B_1(n; \phi)$ are $H(s+1) \times H(s+1) = 4 \times 4$ matrices. We find $B_1(n; \phi) = 0$ if $2 \mid n$ or $n \equiv 3 \pmod 4$. The first four nonzero $B_1(n; \phi)$ are

$$B(1) \qquad B(5)$$

$$\frac{1}{3}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 2 & 1-i \\ 0 & 0 & 1+i & 1 \end{pmatrix} \qquad \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & -6 & 0 & 0 \\ 0 & 0 & -4 & -2+i \\ 0 & 0 & -2-i & -2 \end{pmatrix}$$

$$B(9) \qquad B(13)$$

$$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 9 & 0 & 0 \\ 0 & 0 & 6 & 3-3i \\ 0 & 0 & 3+3i & 3 \end{pmatrix} \qquad \frac{1}{3}\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 30 & 0 & 0 \\ 0 & 0 & 20 & 10-10i \\ 0 & 0 & 10+10i & 10 \end{pmatrix}.$$

Letting

$$C = \begin{pmatrix} 0 & 3i & 1+i & 1 \\ 0 & -3i & 1+i & 1 \\ 6+6i & 0 & -2i & 2+2i \\ -6i & 0 & 2i & -2-2i \end{pmatrix},$$

$$C^{-1} = \frac{1}{6}\begin{pmatrix} 0 & 0 & 1 & 1 \\ -i & i & 0 & 0 \\ 1-i & 1-i & 1 & 1-i \\ 1 & 1 & -1-i & -2 \end{pmatrix},$$

we have

$$\sum_{n=1}^{\infty} CB(n;\phi)C^{-1} = \begin{pmatrix} \theta(\tau) & & & 0 \\ & \theta(\tau) & & \\ & & 0 & \\ 0 & & & 0 \end{pmatrix},$$

where $\theta(\tau) = x - 6x^5 + 9x^9 + 10x^{13} - 30x^{17} + 11x^{25} + 42x^{29} - 70x^{37} + \cdots$. $\theta(\tau)$ is the newform in $S_3^0(16, \phi)$ and this is in agreement with the theory presented in [22]. Atkin has informed us that $\theta(\tau) = \zeta^6(4\tau)$, where $\zeta(\tau)$ is the Dedekind eta function $\zeta(\tau) = x^{1/24}\prod_{n=1}^{\infty}(1 - x^n)$.

Acknowledgments

The author would like to express his appreciation to the Brandeis Computer Center and also the University of Rochester for providing computer support for this work.

References

1. E. Artin, Zur Arithmetik hyperkomplexer Zahlen, *Hamb. Abh.* **5** (1928), 261–289.
2. A. O. L. Atkin and J. Lehner, Hecke operators on $\Gamma_0(m)$, *Math. Ann.* **185** (1970), 134–160.
3. A. O. L. Atkin and D. J. Tingley, Lecture Notes in Mathematics No. 476, pp. 135–141, Springer–Verlag, Berlin/New York, Table 5.
4. A. O. L. Atkin and W.-C. W. Li, Twists of newforms and pseudo-eigenvalues of W-operators, *Invent. Math.* **48**((1978), 221–243.
5. W. A. Blankinship, Algorithm 287, matrix triangulation with integer arithmetic, *Comm. A.C.M.* **9** (1966), 513.
6. Z. Borevich and I. Shafarevich, "Number Theory," Academic Press, New York, 1966.
7. N. Bourbaki, "Elements de Mathématique, Algebra," Chap. 8, Herman, Paris, 1958.
8. J. W. Cassels and A. Frohlich, "Algebraic Number Theory, Proceedings of the Brighton Conference," Academic Press, New York, 1968.
9. M. Deuring, Die Anzahl der Typen von Maximalordnungen einer definiten Quaternionenalgebra mit primer Grundzahl, *Über. Deutsch. Mat. Verein.* **54** (1950), 24–41.
10. M. Eichler, Über die Idealklassenzahl total difiniter Quaternionen-Algebren, *Math. Z.* **43** (1937), 102–109.
11. M. Eichler, Zur Zahlentheorie der Quaternionen-Algebren, *J. Reine Angew. Math.* **195** (1956), 127–151.
12. M. Eichler, Über die Darstellbarkeit von Modulformen durch Thetareihen *J. Reine Angew. Math.* **195** (1956), 156–171.
13. M. Eichler, Quadratische Formen und Modulfunctionen, *Acta Arith.* **4** (1958), 217–239.
14. M. Eichler, "The Basis Problem for Modular Forms and the traces of the Hecke Operators," pp. 75–151, Lecture Notes in Mathematics No. 320, Springer–Verlag, Berlin/New York.
15. S. Gelbart, "Automorphic Forms on Adele Groups," Annals of Mathematics Studies No. 83, Princeton Univ. Press, Princeton, N.J., 1975.

16. R. GUNNING, "Lectures on Modular Forms," Annals of Mathematics Studies No. 48, Princeton Univ. Press, Princeton, N.J., 1962.
17. R. GUNNING AND H. ROSSI, "Analytic Functions of Several Complex Variables," Prentice–Hall, Englewood Cliffs, N.J., 1965.
18. E. HECKE, Analytische Arithmetik der positiven quadratischen Formen, *Math. Werke*, 789–918.
19. H. HIJIKATA, Explicit formula of the traces of the Hecke operators for $\Gamma_0(N)$, *J. Math. Soc. Japan*, **26** (1974), 56–82.
20. H. HIJIKATA, On the theta series obtained from certain orders of quaternion algebras, Proceedings U.S.-Japan Seminar on applications of automorphic forms to number theory, Mimeographed Notes, Ann Arbor, 1975, pp. 27–34.
21. H. HIJIKATA AND H. SAITO, On the representability of modular forms by theta series, *in* "Number Theory, Algebraic Geometry, and Commutative Algebra in honor of Y. Akizuki," pp. 13–21, Kinokuniya, Tokyo, 1973.
22. H. HIJIKATA, A. PIZER, AND T. SHEMANSKE, Theta series, newforms, and the basis problem (?), to appear.
23. M. KNESER, Lineare Relationen zwischen Darstellungsanzahlen quatratischer Formen, *Math. Ann.* **168** (1967), 31–39.
24. T. LAM, "The Algebraic Theory of Quadratic Forms," Benjamin, New York, 1973.
25. S. LANG, "Algebra," Addison–Wesley, Reading, Mass., 1971.
26. W.-C. W. LI, Newforms and functional equations, *Math. Ann.* **212** (1975), 285–315.
27. T. MIYAKE, On automorphic forms on GL_2 and Hecke operators, *Ann. of Math.* **94** (1971), 174–189.
28. M. NEWMANN, "Integral Matrices," Academic Press, New York, 1972.
29. A. OGG, "Modular Forms and Dirichlet Series," Benjamin, New York, 1969.
30. O. O'MEARA, "Introduction to Quadratic Forms," Springer–Verlag, Berlin/New York, 1971.
31. W. PARRY, "Theta series of quadratic forms and modular forms on $\Gamma_0(N)$," Dissertation, University of California at Berkeley, 1975.
32. M, PETERS, Ternäre and quaternäre quadratic Formen und Quaternionenalgebren, *Acta Arith.* **15** (1969), 329–365.
33. A. PIZER, Type numbers of Eichler orders, *J. Reine Angew. Math.* **264** (1973), 76–102.
34. A. PIZER, On the arithmetic of quaternion algebras, *Acta Arith.* **31** (1976), 61–89.
35. A. PIZER, On the arithmetic of quaternion algebras, II, *J. Math. Soc. Japan* **28** (1976), 676–688.
36. A. PIZER, The representability of modular forms by theta series, *J. Math. Soc. Japan* **28** (1976), 689–698.
37. A. PIZER, The action of the canonical involution on modular forms of weight 2 on $\Gamma_0(M)$, *Math. Ann.* **226** (1977), 99–116.
38. A. PIZER, A note on a conjecture of Hecke, *Pacific J. Math.* **79** (1978), 541–547.
39. A. PIZER, Theta series and modular forms of level p^2M, *Compositio Math.* **40** (1980), 177–241.
40. P. PONOMAREV, A correspondence between quaternary quadratic forms, *Nagoya Math. J.* **62** (1976), 125–140.
41. I. REINER, "Maximal Orders," Academic Press, New York, 1975.
42. B. SCHOENEBERG, Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen, *Math. Ann.* **166** (1939).
43. B. SCHOENEBERG, "Elliptic Modular Functions: An Introduction," Springer–Verlag, Berlin/New York, 1974.
44. J. P. SERRE, "A Course in Arithmetic," Springer–Verlag, Berlin/New York, 1973.

45. T. SHEMANSKE, "The Basis problem for modular forms on $\Gamma_0(2^{2r}M)$, Dissertation, University of Rochester, 1979.
46. G. SHIMURA, "Introduction to the Arithmetic Theory of Automorphic Functions," Princeton Univ. Press, Princeton, N.J., 1971.
47. C. SIEGEL, "Über die analytische Theory der quadratic Formen, Gesammelte Abhandlungen," Band I, Springer–Verlag, Berlin/New York, 1966.
48. A. WEIL, "Basic Number Theory," Springer–Verlag, Berlin/New York, 1967.