Kontakt / Contact

DigiZeitschriften e.V.
Papendiek 14
37073 Goettingen
Email: info@digizeitschriften.de

Math. Ann. 185, 134—160 (1970)

Hecke Operators on $\Gamma_0(m)$

A. O. L. ATKIN and J. LEHNER

1. Introduction

We first summarize briefly the relevant classical properties of modular forms; for a fuller account we refer the reader to [3] or [7]. Let $\Gamma = LF(2, Z)$ be the modular group of linear fractional transformations

$$\tau' = V\tau = (a\tau + b)/(c\tau + d), \tag{1.1}$$

where a, b, c, and d, are rational integers and $ad - bc = 1$. We shall in the sequel freely use 2×2 matrices to represent transformations, so that V is represented by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, or, as we shall write, $(a, b; c, d)$. The matrices $(a, b; c, d)$ and $(ka, kb; kc, kd)$ with $k \neq 0$ represent the same transformation, and we shall write these matrices as equal where convenient in matrix calculations. The transformations

$$S = (1, 1; 0, 1) \quad \text{and} \quad T = (0, -1; 1, 0)$$

generate Γ, and we have

$$T^2 = (ST)^3 = I,$$

where I is the identical transformation. We define the principal congruence subgroup $\Gamma(m)$ by

$$\Gamma(m) = \{V; V \in \Gamma \quad \text{and} \quad b \equiv c \equiv 0, a \equiv d \equiv \pm 1 (\text{mod}\, m) \quad \text{in} \quad (1.1)\}.$$

A subgroup G of Γ containing some $\Gamma(m)$ is called a *congruence* subgroup; if m is the least m_0 such that $G \supset \Gamma(m_0)$ we say that G has *level* m. We are particularly concerned in this paper with the subgroup $\Gamma_0(m)$ of level m defined by

$$\Gamma_0(m) = \{V; V \in \Gamma \text{ and } c \equiv 0 (\text{mod}\, m) \quad \text{in } (1.1)\}.$$

We also define

$$\Gamma_0(m, m') = \{V; V \in \Gamma \quad \text{and } c \equiv 0 (\text{mod}\, m),\ b \equiv 0 (\text{mod}\, m') \quad \text{in } (1.1)\}.$$

Thus $\Gamma_0(m, 1) = \Gamma_0(m)$, and $\Gamma_0(1, m) = \Gamma^0(m)$, $\Gamma_0(m, m) = \Gamma_0^0(m)$ in the usual notation; $\Gamma_0(m, m')$ has level $\{m, m'\}$, the least common multiple of m and m'. It is also clear that $\Gamma_0(m, m') \supset \Gamma_0(mn, m'n')$ for any integers n, n'.

The groups we consider in this paper are those above, and various conjugates of them by elements of $GL^+(2, Z)$, the set of integral 2×2 matrices with positive determinant, which are thus all in $LF(2, R)$. Any element of $LF(2, R)$ maps H, the upper half-plane $\text{Im}\,\tau > 0$, into itself, and all our groups are discontinuous

groups acting on H. Any such group G has a connected fundamental domain D, and the points of compactification of D on the boundary of H are called *cusps*. In our cases, these cusps may be taken as ∞ (often written $i\infty$, to show that u is bounded and $v \to \infty$ as $\tau = u + iv$ approaches the cusp in D) and various rational points P on the real axis. If $V \in G$ fixes P, and $U \in \Gamma$ is such that $P = U\infty$, then $U^{-1}VU$ fixes ∞, and is thus a translation $\tau' = \tau + \mu_1$. If μ is the least positive such μ_1, we call μ the *width* of the cusp P, and the local uniformizing variable at P is $\xi = e^{2\pi i U^{-1}\tau/\mu}$; μ and ξ are independent of the choice of U.

We now fix, once for all, an even positive integer $2k$, and define for a complex-valued function $f(\tau)$ and a transformation $L = (a, b; c, d) \in LF(2, R)$ the operator*

$$f|L = (ad - bc)^k (c\tau + d)^{-2k} f(L\tau),$$

so that $f|L$ depends only on the transformation and not on the matrix, and we have

$$f|L_1 L_2 = (f|L_1)|L_2.$$

We also define, for complex constants α_1 and α_2,

$$f|(\alpha_1 L_1 + \alpha_2 L_2) = \alpha_1 f|L_1 + \alpha_2 f|L_2.$$

We say that $f(\tau)$ is a *cuspform of weight k on G*, or for brevity "$f(\tau)$ is on G", if

(i) $f(\tau)$ is analytic in the interior of H,
(ii) $f(\tau)$ is zero at each cusp of G,
(iii) $f|V = f(\tau)$ for all $V \in G$. (1.2)

Thus "weight" k is "dimension" $-2k$ in another notation.

It follows from (ii) and (iii) that if ξ is the local uniformizing variable at any cusp $P = U\infty$ of G, then there is an expansion $f|U = \sum_{n=1}^{\infty} a(n)\xi^n$ in positive integral powers of ξ. The expansion of $f|I = f(\tau)$ at the cusp ∞ in powers of $\xi = e^{2\pi i\tau/\mu}$ is of particular importance in what follows, and we call this expansion the *Fourier series* of $f(\tau)$, and the coefficients of ξ^n the *Fourier coefficients*. Many of our lemmas have the form: "if $f(\tau)$ is on G then $f|L$ is on G^*" for some $G \subset \Gamma$ and some operator $L = \sum \alpha_i L_i$ with $L_i \in GL^+(2, Z)$. The only difficulty is in proving (iii) for $f|L$ and G^*, since (i) is immediate, and (ii) follows since $f(\tau)$ is zero at every rational cusp; in the proofs we therefore confine ourselves to establishing (iii).

If $f(\tau)$ and $g(\tau)$ are on G, we define a scalar product (f, g) by

$$(f, g) = (f, g; G) = \iint_D f(\tau)\,\overline{g(\tau)}\, v^{2k-2}\, du\, dv, \tag{1.3}$$

where $\tau = u + iv$ and D is a fundamental domain of G. If $\tau = L\tau'$ where $\tau' = u' + iv'$ and $L = (a, b; c, d) \in LF(2, R)$, then $v = v'(ad - bc)/|c\tau' + d|^2$, and the element

* This "stroke" operator should not be confused with the symbol for "divides", which is printed somewhat smaller.

of hyperbolic area $v^{-2}\,du\,dv = v'^{-2}\,du'\,dv'$. Thus for any region Δ in H we have

$$\iint_{\tau\in\Delta} f(\tau)\,\overline{g(\tau)}\,v^{2k-2}\,du\,dv = \iint_{\tau'\in L^{-1}\Delta} f(L\tau')\,\overline{g(L\tau')}\cdot(ad-bc)^{2k}$$
$$\cdot\,|c\tau'+d|^{-4k}\cdot(v')^{2k-2}\cdot du'\,dv' = \iint_{\tau\in L^{-1}\Delta} f\,|L\cdot\overline{g\,|L}\,v^{2k-2}\,du\,dv\,. \tag{1.4}$$

This shows that the definition (1.3) is independent of the choice of fundamental domain D. For the convergence of the double integral at the cusps, we may transform any cusp to ∞ by some L using (1.4), and now $f(\tau)$ and $g(\tau)$ are $O(e^{-2\pi v/\mu})$ as $v\to\infty$. The definition of (f, g) depends on the group G. If G_1 is a subgroup of index r in G, we clearly have

$$(f, g; G_1) = r(f, g; G)\,. \tag{1.5}$$

We now denote by $\langle G, k\rangle_0$ the set of all cuspforms of weight k on G. It is clear that $\langle G, k\rangle_0$ is a vector space, which can be made a Hilbert space with the scalar product $(f, g; G)$, and it is also finite-dimensional. When G is a suitable congruence subgroup of level m, in particular when G is $\Gamma(m)$, $\Gamma_0^0(m)$, or $\Gamma_0(m)$, then the theory of Hecke operators developed by Hecke and Petersson [4, 5, 10] shows that there exists a basis of $\langle G, k\rangle_0$ of which each member $f_i(\tau)$ is an eigenfunction of certain operators T_r for $(r, m) = 1$. This property also translates into a multiplicative number-theoretic property of the Fourier coefficients of $f_i(\tau)$, which in the case of $\Gamma_0(m)$ where the local uniformizing variable at ∞ is $x = e^{2\pi i\tau}$ and $f_i(\tau) = \sum_{n=1}^{\infty} a_i(n)x^n$, can be written

$$a_i(np) + p^{2k-1}a_i(n/p) = \lambda_i(p)a_i(n)\,,$$

for all integral n and prime p with $(p, m) = 1$, where $a_i(\alpha) = 0$ if α is not a positive integer.

The main object of this paper is to provide a satisfactory account of operators analogous to the T_r with $(r, m) > 1$ for $\Gamma_0(m)$, and to deduce the corresponding multiplicative properties of the Fourier coefficients. Our results are expressed in Theorems 2, 3, and 5 below. They are of course limited by our definition (1.2) which implies "multiplier system unity" and our choice of integral weight k. The limitation to $\Gamma_0(m)$ rather than $\Gamma(m)$ is not so serious, since $f(\tau)$ on $\Gamma_0(m^2)$ is equivalent to $f(\tau/m)$ on $\Gamma_0^0(m)$, which is not far removed from $\Gamma(m)$ insofar as the number theory of the Fourier coefficients is concerned. In any event, $\Gamma_0(m)$ is an important group in its own right, being the group whose function field is defined by $j(\tau)$ and $j(m\tau)$, and the group which arises naturally in the relation of modular forms to algebraic geometry.

Our methods consist both of formal transformations of functions of τ on groups, and detailed examination of Fourier series in powers of $x = e^{2\pi i\tau}$. We develop the classical Hecke operators ab initio (assuming the results stated in this introduction), though not precisely in the original manner of Hecke.

2. Group-theoretic Lemmas

We remind the reader that "$f(\tau)$ is on G" means $f(\tau) \in \langle G, k\rangle_0$, and that all transformations implied are represented by matrices in $GL^+(2, Z)$.

Lemma 1. *If $f(\tau)$ is on G and V is a transformation, then $f|V$ is on $V^{-1}GV$.*

For if $U \in V^{-1}GV$ then $VUV^{-1} \in G$ and $(f|V)|U = f|VU = f|V$.

Corollary. If V lies in the normalizer of G in $GL^+(2, Z)$ and $f(\tau)$ is on G, then $f|V$ is on G.

We now define the transformation A_n by

$$A_n = (n, 0;\ 0, 1)\,. \tag{2.1}$$

Lemma 2. *If $f(\tau)$ is on $\Gamma_0(m, m')$ then $f|A_n$ is on $\Gamma_0(mn, m'/(m', n))$ and $f|A_n^{-1}$ is on $\Gamma_0(m/(m, n), m'n)$.*

For the subgroups given are just the intersections of $A_n^{-1}\Gamma_0(m, m')A_n$ and $A_n\Gamma_0(m, m')A_n^{-1}$ with Γ.

Lemma 3. *Suppose that G_1 is a subgroup of index μ in G, and that R_i ($i = 1$ to μ) is a set of right coset representatives for G_1 in G. If $f_1(\tau)$ is on G_1 then $f(\tau) = \sum_{i=1}^{\mu} f_1|R_i$ is on G.*

For if $V \in G$, we have $R_iV = g_iR_j$ with $g_i \in G_1$, and distinct i give rise to distinct j. Hence

$$f|V = \sum_{i=1}^{\mu} f_1|R_iV = \sum_{j=1}^{\mu} f_1|R_j = f(\tau)\,.$$

Lemma 4. *Suppose that G_1 is a subgroup of Γ of level m, and that $G_1 \subset G \subset \Gamma$. Then if $(m, m') = 1$, a set of right coset representatives R_i for G_1 in G can be chosen so that $R_i \in \Gamma(m')$.*

If R_i' is some set of coset representatives, we may replace each R_i' by any $R_i \in \Gamma$ such that R_i is congruent to R_i' modulo m. By the Chinese remainder theorem this can be done with $R_i \in \Gamma(m')$.

Lemma 5. *If p is prime, then a set of right coset representatives for $\Gamma_0(m, p)$ in $\Gamma_0(m)$ is given by*

$$S^j (0 \leqq j \leqq p-1) \quad \text{if} \quad p|m\,,$$

and

$$S^j (0 \leqq j \leqq p-1) \text{ and } U \quad \text{if} \quad (p, m) = 1\,,$$

where U is any transformation $(p\beta, 1; m\gamma, 1) \in \Gamma$.

Proof. Let $V = (a, b; mc, d)$ be any element of $\Gamma_0(m)$. Then $VS^{-j} = (., b - aj; ., .)$ and if $a \not\equiv 0 \pmod p$ we can choose j with $0 \leqq j \leqq p-1$ so that $b - aj \equiv 0 \pmod p$. If $p|m$ then p cannot divide a. If $p|a$ and $(p, m) = 1$ then $VU^{-1} = (., -a + p\beta b; ., .) \in \Gamma_0(m, p)$. Also it is clear that no two distinct S^j are equivalent modulo $\Gamma_0(m, p)$, and $S^jU^{-1} = (., -1 + p\beta j; ., .) \notin \Gamma_0(m, p)$. This completes the proof.

We now make the convention that, in relation to a given m, the letter p (possibly with a subscript) refers to primes with $(p, m)=1$ and q to primes with $q|m$. We then define[1] Hecke operators T_p^* and U_q^* for $f(\tau)$ by

$$f|T_p^* = \sum_{j=0}^{p-1} f|A_p^{-1}S^j + f|A_p,$$
$$f|U_q^* = \sum_{j=0}^{q-1} f|A_q^{-1}S^j. \tag{2.2}$$

We observe that m does not appear in the right hand sides directly, so that $f|T_p^*$ and $f|U_q^*$ are independent of m considered as formal operators. We now prove

Lemma 6. *If $f(\tau)$ is on $\Gamma_0(m)$ then $f|T_p^*$ is on $\Gamma_0(m)$ if $(p, m)=1$, and $f|U_q^*$ is on $\Gamma_0(m)$ if $q|m$.*

Proof. We have $f|A_p^{-1}$ on $\Gamma_0(m, p)$ by Lemma 2. Thus by Lemmas 3 and 5, when $(p, m)=1$, we have

$$\sum_{j=0}^{p-1} f|A_p^{-1}S^j + f|A_p^{-1}|(p\beta, 1; m\gamma, 1) \quad \text{on} \quad \Gamma_0(m).$$

Now $A_p^{-1}(p\beta, 1; m\gamma, 1) = (\beta, 1; m\gamma, p)A_p$, and hence the last term in the sum above is just $f|A_p$. The proof for $q|m$ is the same, without this last complication.

Lemma 7. *If $f(\tau)$ is on $\Gamma_0(m)$ and $q^2|m$, then $f|U_q^*$ is on $\Gamma_0(m/q)$. If $f(\tau)$ is on $\Gamma_0(m)$ and $q|m$, $q^2 \nmid m$, then*

$$f|U_q^* + f|W_q \quad \text{is on} \quad \Gamma_0(m/q),$$

where W_q is any transformation $(q\beta, 1; m\gamma, q)$ with $q^2\beta - m\gamma = q$.

Proof. Since $f|A_q^{-1}$ is on $\Gamma_0(m/q, q)$ we have $\sum f|A_q^{-1}|R_i$ on $\Gamma_0(m/q)$, where R_i runs over a set of right coset representatives for $\Gamma_0(m/q, q)$ in $\Gamma_0(m/q)$. Lemma 5 now gives the desired result, since

$$W_q = A_q^{-1}(q\beta, 1; m\gamma/q, 1).$$

We now require some information about the normalizer N_m of $\Gamma_0(m)$ in $GL^+(2, Z)$. We denote by W_Q, W_Q', etc., *any* matrices in $GL^+(2, Z)$ such that

$$W_Q = (Qx, y; mz, Qw) \quad \text{and} \quad \det(W_Q) = Q,\ Q|m,\ (Q, m/Q) = 1.$$

The condition $(Q, m/Q)=1$ can of course be deduced from $\det(W_Q)=Q$.

Lemma 8. *If $V \in \Gamma_0(m)$ then $W_Q V W_Q' \in \Gamma_0(m)$.*

For $W_Q V W_Q'$ is a matrix of determinant Q^2, and it is easily verified that all the entries are divisible by Q, and the third entry by mQ.

Since W_Q^{-1} is equivalent as a transformation to $(Qw, -y; -mz, Qx) = W_Q'$, we see that W_Q is in N_m. Also with $V=I$ in Lemma 8, we have W_Q^2 in $\Gamma_0(m)$.

[1] Our approach to the Hecke operators here is that of Wohlfahrt [16].

It is finally easily verified that $W_{Q_1} \cdot W_{Q_2} =$ some W''_Q, where $Q = \{Q_1, Q_2\}$, the least common multiple of Q_1 and Q_2. Applying Lemma 8 with Q, we see that W_{Q_1} and W_{Q_2} commute modulo $\Gamma_0(m)$. Also if $Q_1 \neq Q_2$, then $W_{Q_1} \cdot \Gamma_0(m) \neq W_{Q_2} \cdot \Gamma_0(m)$. Hence

Lemma 9. *Let $m = q_1^{\alpha_1} \cdot q_2^{\alpha_2} \ldots q_i^{\alpha_i}$, where the q_j are distinct primes. Write*[2]

$$W_{q_j} = (q_j^{\alpha_j} x, y; mz, q_j^{\alpha_j} w), \qquad (\det W_{q_j} = q_j^{\alpha_j}) \tag{2.3}$$

where x, y, z, and w, are any integers satisfying (2.3). *Then N_m, the normalizer of $\Gamma_0(m)$ in $GL^+(2, Z)$, contains any product of the W_{q_j}. If $N_m^* \subset N_m$ is the group generated by $\Gamma_0(m)$ and the W_{q_j}, then $N_m^*/\Gamma_0(m)$ is abelian of type* (2, 2, 2, ..., 2) *and order 2^i.*

Note in particular that $\prod_{j=1}^{i} W_{q_j}$ is equivalent to $(0, -1; m, 0)$ modulo $\Gamma_0(m)$, and that when $\alpha_j = 1$, the W_{q_j} is equivalent to that which occurs as W_q in Lemma 7. We have also by Lemma 1

Lemma 10. *If $f(\tau)$ is on $\Gamma_0(m)$, and $q \mid m$, then $f \mid W_q$ is on $\Gamma_0(m)$, and is independent of the choice in* (2.3).

We prove next

Lemma 11. *If $(p, m) = 1$ and $q \mid m$ and $f(\tau)$ is on $\Gamma_0(m)$, then*

$$(f \mid T_p^*) \mid W_q = (f \mid W_q) \mid T_p^* .$$

Since, by Lemma 6, $f \mid T_p^*$ is on $\Gamma_0(m)$, both sides are independent of the choice of W_q. We choose W_q subject to (2.3) with $W_q \equiv (1, 0; 0, 1) \pmod{p}$, which is possible since $(p, m) = (p, q) = 1$. Then for any matrix $M = (1, j; 0, p)$ or $(p, 0; 0, 1)$ we have that $M W_q M^{-1}$ is a matrix with integral entries and is some W'_q, so that $f \mid M W_q M^{-1} W_q^{-1} = f(\tau)$. Hence each separate term in the sum defining T_p^* in (2.2) satisfies $f \mid M W_q = f \mid W_q M$, and Lemma 11 follows on addition.

Lemma 12. *Let G_1 be a subgroup of index μ in G, and R_i ($i = 1$ to μ) be a set of right coset representatives for G_1 in G, as in Lemma 3. If $f_1(\tau)$ is on G_1, and $g(\tau)$ is on G, and $f(\tau) = \sum_{i=1}^{\mu} f_1 \mid R_i$, then*

$$(f, g; G) = (f_1, g; G_1) .$$

Proof. We know from Lemma 3 that $f(\tau)$ is on G. If D is a fundamental domain for G, and D_1 is defined by

$$D_1 = \sum_{i=1}^{\mu} R_i D , \tag{2.4}$$

[2] So that W_{q_j} is W_Q with $Q = q_j^{\alpha_j}$ in the former notation above.

then D_1 is a fundamental domain for G_1. Thus

$$(f, g; G) = \sum_{i=1}^{\mu} \iint_D (f_1 | R_i) \cdot \bar{g} v^{k-2} \, du \, dv$$

$$= \sum_{i=1}^{\mu} \iint_{R_i D} (f_1 | R_i | R_i^{-1}) \cdot \overline{g | R_i^{-1}} \cdot v^{k-2} \, du \, dv$$

$$= \sum_{i=1}^{\mu} \iint_{R_i D} f_1 \cdot \bar{g} v^{k-2} \, du \, dv = (f_1, g; G_1)$$

by (2.4) and (1.4).

We conclude this section by proving

Lemma 13. *T_p^* is an hermitian operator with regard to the scalar product (f, g) on $\Gamma_0(m)$; that is, if $f(\tau)$ and $g(\tau)$ are on $\Gamma_0(m)$ and $(m, p) = 1$ then*

$$(f | T_p^*, g; \Gamma_0(m)) = (f, g | T_p^*; \Gamma_0(m)) .$$

Proof. From the definition (2.2) and Lemma 5 we see that $f | T_p^* = \sum_i (f | A_p^{-1}) | R_i$ taken over right coset representatives R_i for $\Gamma_0(m, p)$ in $\Gamma_0(m)$. Thus by the last lemma

$$(f | T_p^*, g; \Gamma_0(m)) = (f | A_p^{-1}, g; \Gamma_0(m, p)) .$$

Now let $W = (\alpha p, \beta p; m\gamma, \delta p)$ with $p\alpha\delta - m\beta\gamma = 1$. Then $W^{-1} \Gamma_0(m, p) W = \Gamma_0(m, p)$, and $A_p^{-1} W \in \Gamma_0(m)$, $W A_p \in \Gamma_0(m)$. Thus, by (1.4),

$$(f | A_p^{-1}, g; \Gamma_0(m, p)) = (f | A_p^{-1} | W, g | W; \Gamma_0(m, p)) = (f, g | A_p^{-1}; \Gamma_0(m, p)) ,$$

as desired. Note that since W is in the normalizer of $\Gamma_0(m, p)$ with fundamental domain Δ, we may replace $\iint_{W^{-1}\Delta}$ by $\iint_{\Delta}$ in (1.4).

3. Number-theoretic Lemmas

In this section we establish further properties by direct examination of Fourier series. Some of these lemmas can also be proved by group-theoretical methods only, but we have chosen to include these here for simplicity of proof. We have, for any $f(\tau) \in \langle \Gamma_0(m), k \rangle_0$, a Fourier series expansion

$$f(\tau) = \sum_{n=1}^{\infty} a(n) x^n, \qquad (x = e^{2\pi i \tau}) .$$

With $a(\alpha)=0$ when α is non-integral, we now define in terms of the $a(n)$ the operators T_p, U_q, B_d by

$$f|T_p=\sum_{n=1}^{\infty}\{a(np)+p^{2k-1}a(n/p)\}\cdot x^n,$$
$$f|U_q=\sum_{n=1}^{\infty}a(nq)x^n,$$
$$f|B_d=\sum_{n=1}^{\infty}a(n)x^{nd}. \tag{3.1}$$

We now relate these to our operators defined in § 2.

Lemma 14. *We have*

$$f|T_p=p^{k-1}f|T_p^*,$$
$$f|U_q=q^{k-1}f|U_q^*,$$
$$f|B_d=d^{-k}f|A_d=f(d\tau).$$

Proof. Let $\omega=e^{2\pi i/p}$. Then

$$f|T_p^*=p^kf(p\tau)+p^{-k}\sum_{j=0}^{p-1}f\left(\frac{\tau+j}{p}\right).$$

With $\xi=e^{2\pi i\tau/p}$ the sum is

$$\sum_{j=0}^{p-1}\sum_{n=1}^{\infty}\omega^{jn}a(n)\xi^n=\sum_{n=1}^{\infty}\sum_{j=0}^{p-1}\omega^{jn}a(n)\xi^n=\sum_{m=1}^{\infty}pa(mp)\xi^{mp}=\sum_{n=1}^{\infty}pa(np)x^n,$$

while $f(p\tau)=\sum_{n=1}^{\infty}a(n)x^{pn}=\sum_{n=1}^{\infty}a(n/p)x^n$. Thus $p^{k-1}f|T_p^*=f|T_p$. The proof for U_q is similar, and for B_d obvious.

Lemmas 6, 7, 11, and 13 clearly remain valid with T_p, U_q replacing T_p^*, U_q^*, with the sole change that from Lemma 7 we derive

$$f|U_q+q^{k-1}f|W_q \text{ is on } \Gamma_0(m/q) \text{ if } f(\tau) \text{ is on } \Gamma_0(m) \text{ and } q|m,\ q^2\nmid m. \tag{3.2}$$

We now prove

Lemma 15.

$$(f|T_p)|T_{p'}=(f|T_{p'})|T_p, \qquad (p\neq p')$$
$$(f|T_p)|U_q=(f|U_q)|T_p, \qquad (p\neq q)$$
$$(f|T_p)|B_d=(f|B_d)|T_p \quad \text{if} \quad (p,d)=1,$$
$$(f|U_q)|B_d=(f|B_d)|U_q \quad \text{if} \quad (q,d)=1.$$

First,

$$(f|T_p)|T_{p'}=\sum_{n=1}^{\infty}\{a(np'p)+p^{2k-1}a(np'/p)+(p')^{2k-1}(a(np/p')+p^{2k-1}a(n/pp'))\}\cdot x^n,$$

and this is clearly symmetrical in p and p'. Next,

$$(f|T_p)|U_q=\sum_{n=1}^{\infty}\{a(nqp)+p^{2k-1}a(nq/p)\}x^n=(f|U_q)|T_p.$$

We note here that, with our conventions, $a\left(\frac{n}{p}\cdot p'\right)=a\left(\frac{np'}{p}\right)$, since $p|np'$ if and only if $p|n$. Finally

$$(f|T_p)|B_d=(f|B_d)|T_p=\sum_{n=1}^{\infty}\{a(pn)+p^{2k-1}a(n/p)\}x^{nd}.$$

While Lemma 15 expresses only a formal aspect of power series which is universally valid, we shall of course only apply it when $f(\tau)$ is on some $\Gamma_0(m)$. We prove next

Lemma 16. *Suppose that $f(\tau)$ is any formal power series in positive integral powers of $x=e^{2\pi i\tau}$, and that $f|A_d$ is on $\Gamma_0(m)$. Then, if $d|m$, $f(\tau)$ is in fact a form on $\Gamma_0(m/d)$, while if $d\nmid m$ we have $f(\tau)=0$.*

Proof. By Lemma 2, $f(\tau)=f|A_d|A_d^{-1}$ is on $\Gamma_0(m',d)$, where we write $m'=m/(m,d)$, $d'=d/(m,d)$. But $f|S=f(\tau)$, and so $f(\tau)$ is on the group generated by S and $\Gamma_0(m',d)$, which is $\Gamma_0(m')$. If $d|m$, then $(m,d)=d$, and we have our result. If $d\nmid m$, let p be a prime dividing d', so that $(p,m')=1$. With $g(\tau)=f|A_p$, we have $g|A_{d/p}$ on $\Gamma_0(m)$, so that repeating the above argument with d replaced by d/p we find $g(\tau)$ on $\Gamma_0(m/(m,d/p))=\Gamma_0(m')$ since $(m,d/p)=(m,d)$. But by (3.1)

$$(f|A_p^{\alpha})|T_p=f|A_p^{\alpha-1}+p^{2k-1}f|A_p^{\alpha+1},$$

and thus $f(\tau)$, $f|A_p$ on $\Gamma_0(m')$ implies $f|A_p^{\alpha}$ on $\Gamma_0(m')$ for all α. Since $\langle\Gamma_0(m'),k\rangle_0$ is finite-dimensional this is impossible unless $f(\tau)\equiv 0$.

Our next result is the basis of our arguments in §§ 4 and 5.

Theorem 1. *Let $f(\tau)=\sum_{n=1}^{\infty}a(n)x^n$ be on $\Gamma_0(m)$, and suppose that $a(n)=0$ whenever $(n,N)=1$, where N is a fixed integer greater than 1. Then*

$$f(\tau)=\sum_i f_i|B_{q_i},$$

where the q_i are primes dividing m, and $f_i(\tau)$ is on $\Gamma_0(m/q_i)$.

We define first an "annihilator" operator K_p for prime p by

$$f|K_p=f(\tau)-(f|U_p)|B_p. \tag{3.3}$$

If $f(\tau)$ is on $\Gamma_0(m)$, then $f|K_p$ is certainly on $\Gamma_0(mp^2)$, and $f|K_p$ is on $\Gamma_0(mp)$ if $p|m$, and on $\Gamma_0(m)$ if $p^2|m$. This follows readily from Lemmas 2, 7, and 14, if we observe that formally $f|T_p=f|U_p+p^{2k-1}f|B_p$. The effect of K_p on the Fourier series of $f(\tau)$ is to remove precisely those terms $a(n)x^n$ with $p|n$.

Given now the $f(\tau)$ of Theorem 1, we may write

$$f(\tau)=\sum_{i=1}^{\lambda}\phi_i|B_{q_i}+\sum_{j=1}^{\mu}\phi_j|B_{p_j}, \tag{3.4}$$

where any $\phi_i(\tau)$ or $\phi_j(\tau)$ is a formal power series in positive integral powers of x, not necessarily a form, and q_i are the primes dividing N with $q_i|m$, and p_j the primes dividing N with $(p_j, m)=1$. Let $K=\prod_{i=1}^{\lambda} K_{q_i}\cdot\prod_{j=1}^{\mu-1} K_{p_j}$. Then $f|K=(\phi_\mu|B_{p_\mu})|K=(\phi_\mu|K)|B_{p_\mu}$, since B_p commutes with $K_{p'}$ for $p'\neq p$, and we have $f|K$ on $\Gamma_0\left(m\cdot\prod_{i=1}^{\lambda} q_i\cdot\prod_{j=1}^{\mu-1} p_j^2\right)$. Hence, by Lemma 16, $\phi_\mu|K=0$. Thus $\phi_\mu|B_{p_\mu}$ has in its Fourier series only terms $a(n)\cdot x^n$ with some q_i or $p_j (1\leqq j\leqq \mu-1)$ dividing n. We may therefore absorb the $\phi_\mu|B_{p_\mu}$ by changing the other $\phi_i|B_{q_i}$ and $\phi_j|B_{p_j}$ in (3.4), and repeat the argument with μ replaced by $\mu-1$. Proceeding in this way we obtain

$$f(\tau)=\sum_{i=1}^{\lambda}\phi_i|B_{q_i},\quad \text{where}\quad q_i|m. \tag{3.5}$$

If $\lambda=1$ in (3.5) then by Lemma 16 we have $\phi_1(\tau)$ on $\Gamma_0(m/q_1)$ and Theorem 1 is proved. We shall prove Theorem 1 in general by induction on λ. We suppose that Theorem 1 has been established for any set of $(l-1)$ distinct primes dividing m, with $\lambda=l-1$ in (3.5), and deduce it for $\lambda=l$.

Suppose first that $q_1^2|m$. We may suppose that the terms $a(n)x^n$ with $q_1|n$ in $\phi_i|B_{q_i}$ for $i\geqq 2$ absorbed in $\phi_1|B_{q_1}$, so that $\phi_i|B_{q_i}|U_{q_1}=0$ for $2\leqq i\leqq l$. Then $f|U_{q_1}$ is on $\Gamma_0(m/q_1)$, by Lemma 7, and since trivially $f|U_{q_1}=\phi_1|B_{q_1}|U_{q_1}=\phi_1(\tau)$, we have $\phi_1|B_{q_1}$ on $\Gamma_0(m)$, and so $f(\tau)-\phi_1|B_{q_1}=\sum_{i=2}^{l}\phi_i|B_{q_i}$ is on $\Gamma_0(m)$. By the induction hypothesis this last sum is equal to $\sum_{i=2}^{l} f_i|B_{q_i}$, where $f_i(\tau)$ is on $\Gamma_0(m/q_i)$, and Theorem 1 for $\lambda=l$ is established in this case.

If now $q_1|m$, $q_1^2\nmid m$, we first rewrite (3.5) with new $\phi_i(\tau)$ so that

$$\phi_i|U_{q_j}=0\quad\text{if}\quad j>i,$$

as is clearly possible. Then $f|U_{q_l}=\phi_l(\tau)$ is on $\Gamma_0(m)$. We now prove

$$\phi_i(\tau)\quad\text{is a form on}\quad \Gamma_0(m\cdot q_{i+1}\cdot q_{i+2}\cdots q_l),\qquad (i<l). \tag{3.6}$$

For suppose (3.6) established for $j>i$. Then $f|U_{q_i}=\phi_i(\tau)+\sum_{j>i}\phi_j|B_{q_j}|U_{q_i}$ is on $\Gamma_0(m)$, and $\phi_j|B_{q_j}|U_{q_i}$ is on $\Gamma_0(m\cdot q_{j+1}\cdots q_l\cdot q_j)\supset\Gamma_0(m\cdot q_{i+1}\cdot q_{i+2}\cdots q_l)$. Thus (3.6) is established by reverse induction on i. In particular all the $\phi_i|B_{q_i}$ are on $\Gamma_0(m^2/q_1)$, so that $\phi_1(\tau)$ is on $\Gamma_0(m^2/q_1^2)$ by Lemma 16, since q_1 divides m^2/q_1.

We now write $W=(\alpha q_1, \beta; m^2\gamma/q_1, \delta q_1)$ with $\alpha\delta q_1-\beta\gamma m^2/q_1^2=1$, so that W is a suitable W_{q_1} for $\Gamma_0(m^2/q_1)$ and for $\Gamma_0(m)$. For $i\geqq 2$ we have

$$A_{q_i}WA_{q_i}^{-1}=(\alpha q_1, \beta q_i; m^2\gamma/q_1 q_i, \delta q_1)=W'$$

which is a suitable W_{q_1} for $\Gamma_0(m^2/q_1 q_i)$, on which group $\phi_i(\tau)$ is a form. Thus

$$(\phi_i|A_{q_i})|W=(\phi_i|W')|A_{q_i},$$

and since $\phi_i|W'$ has an expansion in integral powers of x, $(\phi_i|A_{q_i})|W$, and thus $(\phi_i|B_{q_i})|W$, has an expansion in integral powers of x^{q_i}. Further

$$(\phi_1|A_{q_1})|W=\phi_1|(\alpha q_1,\beta;m^2\gamma/q_1^2,\delta)=\phi_1$$

since $\phi_1(\tau)$ is on $\Gamma_0(m^2/q_1^2)$.

We now operate on (3.5) with $U_{q_1}+q_1^{k-1}W_{q_1}$. By (3.2) we have that $f^*(\tau)=f|(U_{q_1}+q_1^{k-1}W_{q_1})$ is on $\Gamma_0(m/q_1)$. Also

$$(\phi_1|B_{q_1})|(U_{q_1}+q_1^{k-1}W_{q_1})=\phi_1(\tau)+q_1^{-1}(\phi_1|A_{q_1})|W=(1+q_1^{-1})\phi_1(\tau).$$

Further, for $i\geqq 2$, $(\phi_i|B_{q_i})|U_{q_1}$ clearly has an expansion in integral powers of x^{q_i}, and so does $(\phi_i|B_{q_i})|W$ as we have already shown. Hence finally

$$\phi_1(\tau)=f_1(\tau)+\sum_{i=2}^{l}\psi_i|B_{q_i}, \tag{3.7}$$

where $f_1(\tau)=(1+q_1^{-1})^{-1}f^*(\tau)$ is on $\Gamma_0(m/q_1)$, and the $\psi_i(\tau)$ have expansions in integral powers of x (and are in fact forms). Hence we may rewrite (3.5) as

$$f(\tau)=f_1|B_{q_1}+\sum_{i=2}^{l}\chi_i|B_{q_i},$$

where the $\chi_i(\tau)$ have expansions in integral powers of x, and this last sum is, by the induction hypothesis, equal to $\sum_{i=2}^{l}f_i|B_{q_i}$, with $f_i(\tau)$ on $\Gamma_0(m/q_i)$. This completes the proof of Theorem 1.

4. Newforms on $\Gamma_0(m)$

We first summarize in Lemma 17 the results of Lemmas 6, 7, 11, 12, 13, and 15.

Lemma 17. *Let p be any prime with $(p,m)=1$, and let q be a prime dividing m such that $q^\alpha \| m$. Let $f(\tau)$ be on $\Gamma_0(m)$, that is, $f(\tau)$ is a cuspform of weight k on $\Gamma_0(m)$. Then*

(i) *$f|T_p$, $f|U_q$, $f|W_q$, are on $\Gamma_0(m)$.*

(ii) $(f|T_p)|T_{p'}=(f|T_{p'})\,T_p$,
$(f|T_p)|U_q=(f|U_q)|T_p$,
$(f|T_p)|W_q=(f|W_q)|T_p$.

(iii) *if $\alpha=1$, then $f|U_q+q^{k-1}f|W_q$ is on $\Gamma_0(m/q)$.*

(iv) *if $\alpha>1$, then $f|U_q$ is on $\Gamma_0(m/q)$.*

(v) *if $g(\tau)$ is on $\Gamma_0(m)$ then*

$$(f|T_p,g;\Gamma_0(m))=(f,g|T_p;\Gamma_0(m)).$$

We now establish

Theorem 2. *(Hecke-Petersson). There exists a basis $f_i(\tau)$ $(i=1$ to $v)$ for $\langle\Gamma_0(m),k\rangle_0$ of dimension v such that each $f_i(\tau)$ is an eigenfunction of all the*

operators T_p, i.e.,

$$f_i | T_p = \lambda_i(p) \cdot f_i(\tau) \qquad ((p, m) = 1).$$

Further the forms $f_i(\tau)$ fall into equivalence classes defined by $f_i(\tau) \sim f_j(\tau)$ if $\lambda_i(p) = \lambda_j(p)$ for all p. Any form $f(\tau)$ in $\langle \Gamma_0(m), k \rangle_0$ which is an eigenfunction of all the T_p with $(p, m) = 1$ lies in the vector space spanned by some equivalence class.

Proof. Let $\boldsymbol{u} = (u_1, u_2, \ldots, u_\nu)$, with $u_i = u_i(\tau)$, be a basis of $\langle \Gamma_0(m), k \rangle_0$ which is orthonormal under the scalar product already defined. Then for each p the operator T_p can be represented by a matrix Λ_p in terms of $\boldsymbol{u}$. The commutativity and hermitian property of the T_p are carried over to the Λ_p. Thus by a theorem of algebra [3] the Λ_p can be simultaneously diagonalised by an unitary matrix $\boldsymbol{A}$. Each element of the new basis $\boldsymbol{f} = \boldsymbol{A}\boldsymbol{u}$ is an eigenfunction of all the operators T_p. Moreover any form $F(\tau)$ in $\langle \Gamma_0(m), k \rangle_0$ is a linear combination of basis forms f_i, and if $F(\tau)$ is an eigenfunction of all the T_p, the f_i involved must be equivalent. We may extend the equivalence relation $F(\tau) \sim G(\tau)$ to any pair of forms which are eigenfunctions of all the T_p with the same eigenvalues. We shall in fact call the $f_i(\tau)$ *eigenforms* to avoid any possible confusion with *functions* on $\Gamma_0(m)$ which have $k = 0$.

We now consider the vector space $\langle \Gamma_0(m'), k \rangle_0$ where m' is any proper divisor of m. The application of Theorem 2 gives rise to a basis of eigenforms $g_j(\tau)$. If d is any divisor of m/m', then by Lemma 2 $g_j | B_d$ is on $\Gamma_0(m)$, and by Lemma 15 we have

$$(g_j | B_d) | T_p = (g_j | T_p) | B_d = \lambda_j(p) \cdot g_j | B_d .$$

[Note that T_p is the *same* operator on both $\Gamma_0(m)$ and $\Gamma_0(m')$.] We denote by $C^-(m)$ the subspace of $\langle \Gamma_0(m), k \rangle_0$ spanned by all such $g_j | B_d$, for any m' and any d. The above equation shows that every T_p maps $C^-(m)$ into itself. If now $C^+(m)$ is defined as the orthogonal complement of $C^-(m)$ in $\langle \Gamma_0(m), k \rangle_0$, then the hermitian property shows that every T_p must also map $C^+(m)$ into itself, and the proof of Theorem 2 gives

Lemma 18. *There exists a basis $F_i(\tau)$ of $C^+(m)$ with the property that each $F_i(\tau)$ is an eigenform of all operators T_p with $(p, m) = 1$.*

We define a *newform* on $\Gamma_0(m)$ as any one of the forms $F_i(\tau)$. We shall conventionally agree that the form which is identically zero belongs both to $C^+(m)$ and to $C^-(m)$.

Lemma 19. *In the Fourier series of a newform $F_i(\tau) = \sum_{n=1}^{\infty} a_i(n) x^n$, we have $a_i(1) \neq 0$.*

Proof. Suppose that $a_i(1) = 0$. We show first that in this case $a_i(n) = 0$ for $(n, m) = 1$. If not, let n_1 be the smallest n with $(n, m) = 1$ such that $a_i(n) \neq 0$, and

[3] See, for example, Gantmacher [2], page 291 (Vol. 1).

let p be a prime dividing n_1. Then $F_i|T_p = a_i(n_1)\cdot x^{n_1/p}+\cdots = \lambda_i(p)\cdot F_i(\tau)$ $= \lambda_i(p)\cdot\left\{\sum_{(n,m)>1} a_i(n)x^n + a_i(n_1)\cdot x^{n_1}+\cdots\right\}$, a contradiction. But now $F_i(\tau)$ is a sum of forms $g|B_q$ with $g(\tau)$ on $\Gamma_0(m/q)$, by Theorem 1, and so $F_i(\tau)\in C^-(m)$. Thus $F_i(\tau)\in C^-(m)\cap C^+(m)$ and so $F_i(\tau)=0$. Hence finally $a_i(1)\neq 0$.

In view of Lemma 19 we may normalize[4] the newforms to have $a_i(1)=1$, so that

$$F_i(\tau) = x+\cdots . \tag{4.1}$$

Now for any p with $(p,m)=1$ we have for all n

$$a_i(np)+p^{2k-1}a_i(n/p)=\lambda_i(p)a_i(n),$$

and setting $n=1$ we obtain

$$\lambda_i(p)=a_i(p), \tag{4.2}$$

giving

$$a_i(np)-a_i(n)a_i(p)+p^{2k-1}a_i(n/p)=0. \tag{4.3}$$

Lemma 20. *If $F_1(\tau)$ and $F_2(\tau)$ are newforms on $\Gamma_0(m)$, and $F_1(\tau)\sim F_2(\tau)$, then $F_1(\tau)=F_2(\tau)$.*

By (4.3), the value of $a_1(n)$ for $(n,m)=1$ depends only on the values of $a_1(p)$. Hence $a_1(n)=a_2(n)$ for $(n,m)=1$. But now $F_1(\tau)-F_2(\tau)$ is in $C^-(m)$ by Theorem 1, and is thus zero. We have also

Lemma 21. *Any form in $C^+(m)$ which is an eigenform of all the T_p with $(p,m)=1$ is a constant multiple of some newform $F_i(\tau)$.*

We now consider a form $g_j(\tau)$ which is a newform on $\Gamma_0(m')$, for any *proper* divisor m' of m, and the class of forms $\{g_j|B_d\}$ where d runs over all divisors of m/m'. Such a class of forms for fixed g_j and varying d we call an *oldclass* on $\Gamma_0(m)$, and its members we call *oldforms*.

Lemma 22. *$C^-(m)$ is spanned by the oldforms. All the members of an oldclass belong to the span of the same equivalence class prescribed by Theorem 2. Any form on $\Gamma_0(m)$ which is an eigenform of all the T_p with $(p,m)=1$ is equivalent to a form $g_j(\tau)$ which was a newform on $\Gamma_0(m')$ for some $m'|m$.*

We prove the first sentence by induction on the factors of m. Suppose it is true for all proper divisors m' of m. Then any $g_j|B_d$ on $\Gamma_0(m)$ with $g_j(\tau)$ on $\Gamma_0(m')$ for $m'<m$ is a linear combination of forms $h_i|B_{d'}|B_d$ with $h_i(\tau)$ a newform on some $\Gamma_0(m_i)$ with $m_i<m'$ (by the induction hypothesis) and forms $n_k|B_d$ with $n_k(\tau)$ a newform on $\Gamma_0(m')$, all of which forms belong to the oldclasses of $\Gamma_0(m)$.

The second sentence of Lemma 22 is clear since T_p and B_d commute. For the third sentence, such a form is either equivalent to a newform on $\Gamma_0(m)$ (and so $m'=m$), or lies in the span of some equivalence class, which must contain an oldclass and so a newform on $\Gamma_0(m')$ with $m'|m$ equivalent to the given form.

[4] So that the basis ceases to be orthonormal, as in the proof of Theorem 2.

We shall in fact prove later in Theorem 5 that the oldforms are a *basis* for $C^-(m)$, by showing that the forms in two distinct oldclasses are not equivalent.

We now prove

Lemma 23. *If $F(\tau)$ is a newform on $\Gamma_0(m)$, and $F(\tau) \sim g(\tau) \not\equiv 0$ where $g(\tau) \in C^-(m)$, then $F(\tau) \equiv 0$.*

Proof. By Lemma 22, $g(\tau) \sim h(\tau)$ for some $h(\tau)$ which is a newform on $\Gamma_0(m')$ for $m' < m$. Thus (since $h(\tau) = x + \cdots$) the Fourier coefficients $a(n)$ of $F(\tau)$ and $h(\tau)$ are the same if $(n, m) = 1$. Hence $F(\tau) - h(\tau) \in C^-(m)$, whence $F(\tau) \in C^-(m)$ and $F(\tau) = 0$. We are now in a position to establish the basic properties of newforms on $\Gamma_0(m)$.

Theorem 3. *Suppose that $F(\tau)$ is a newform on $\Gamma_0(m)$, and that p is any prime with $(p, m) = 1$, and q is any prime dividing m such that $q^\alpha \| m$.*

Then if $F(\tau) = x + \sum_{n=2}^{\infty} a(n)x^n$ we have

(i) $F \mid T_p = a(p) \cdot F(\tau)$,

(ii) $F \mid U_q = a(q) \cdot F(\tau)$,

(iii) $F \mid W_q = \lambda(q) \cdot F(\tau)$, *where* $\lambda(q) = \pm 1$.

Further[5], *if* $\alpha \geqq 2$, *then* $a(q) = 0$, *while if* $\alpha = 1$ *we have* $a(q) = -q^{k-1}\lambda(q)$.

In terms of the Fourier coefficients, (i) *and* (ii) *become*

(i)′ $a(np) - a(n)a(p) + p^{2k-1}a(n/p) = 0 \quad (n \geqq 1)$,

(ii)′ $a(nq) - a(n)a(q) = 0 \quad (n \geqq 1)$.

Proof. Since for any p we have

$$(F \mid U_q) \mid T_p = (F \mid T_p) \mid U_q = a(p) \cdot F \mid U_q ,$$

it follows that $F \mid U_q \sim F(\tau)$. If $\alpha \geqq 2$, then $F \mid U_q$ is on $\Gamma_0(m/q)$ and so belongs to $C^-(m)$, whence by Lemma 23 we have $F \mid U_q = 0$. Similarly $F \mid W_q \sim F$. If $F \mid W_q \in C^-(m)$, then $F \mid W_q = 0$, and so $F(\tau) = (F \mid W_q) \mid W_q = 0$. Thus $F \mid W_q \in C^+(m)$, and, by Lemmas 20 and 21, $F \mid W_q = \lambda(q) \cdot F(\tau)$. Since $(F \mid W_q) \mid W_q = F(\tau)$, we have $\lambda^2(q) = 1$, $\lambda(q) = \pm 1$. Now if $\alpha = 1$, then by Lemma 17 (iii) we have $F(\tau) \sim F \mid (U_q + q^{k-1} W_q) \in C^-(m)$, so that $F \mid U_q + q^{k-1} F \mid W_q = 0$, or $F \mid U_q = -\lambda(q) \cdot q^{k-1} F(\tau)$. The translation to Fourier series is immediate, and this completes the proof of Theorem 3.

Theorem 3 gives a complete description of the newforms on $\Gamma_0(m)$; if the eigenvalues $a(p)$ and $\lambda(q)$ are given, then every Fourier coefficient is determined. It would have been possible, following Hecke, to define operators T_n for all n with the ultimate effect that, for a newform, $F \mid T_n = a(n) \cdot F(\tau)$, but the increase in complexity would have been great, and no new number-theoretic information arises. One may interpret $\lambda(q)$ as follows: if $F(\tau)$ is also on the group $\{\Gamma_0(m), W_q\}$, then $\lambda(q) = +1$; otherwise $\lambda(q) = -1$. The values of $a(p)$ are not in general given by any simple formula. It is known (Shimura [13]) that they are algebraic integers. There is also Petersson's generalization of the Ramanujan

[5] Since this paper was written, Ogg has obtained in Math. Ann. **179**, 101—108 (1969) the values of $a(q)$ on the assumption of (ii).

conjecture, that $|a(p)| \leqq 2p^{k-\frac{1}{2}}$, which would imply by Theorem 3 that $a(n) = O(n^{k-\frac{1}{2}+\varepsilon})$ as $n \to \infty$, but the best known result in this direction is

$$a(n) = O(n^{k-\frac{1}{2}+\varepsilon}) \quad \text{as} \quad n \to \infty \quad \text{for any} \quad \varepsilon > 0. \tag{4.4}$$

The estimate in (4.4) depends on Weil's work on exponential sums in [14]; for a discussion of the problem see Selberg [12]. For the special case $k=1$ corresponding to differentials on $H/\Gamma_0(m)$, the Ramanujan conjecture was proved for almost all p by Eichler [1] and for all p by Igusa [6].

5. We now investigate further the equivalence classes of Theorem 2. We prove first

Lemma 24. *Let $F_1(\tau)$ be a newform on $\Gamma_0(m)$, and $F_2(\tau) \neq F_1(\tau)$ a newform on $\Gamma_0(m')$, where $m' | m$ (and possibly $m' = m$). Then if $(p, m) = 1$ and the eigenvalues of $F_1(\tau)$ and $F_2(\tau)$ for T_p are $a_1(p)$ and $a_2(p)$, we have*

$$a_1(p) \neq a_2(p) \quad \textit{for infinitely many } p.$$

Proof. Suppose not, so that $a_1(p) = a_2(p)$ except for $p = p_j$ ($j = 1$ to μ). Let q_i ($i = 1$ to λ) be the primes dividing m, and let $N = \prod_{j=1}^{\mu} p_j \prod_{i=1}^{\lambda} q_i$. Then $F_1(\tau) - F_2(\tau) = f(\tau)$ satisfies the hypothesis of Theorem 1, so that $f(\tau)$ is an oldform on $\Gamma_0(m)$, and thus $F_1(\tau) = 0$ when $m' < m$, and $F_1(\tau) = F_2(\tau)$ when $m' = m$, both of which are impossible.

Lemma 25. *If $q | m$ then W_q is hermitian with respect to the scalar product on $\Gamma_0(m)$, i.e.,*

$$(f | W_q, g; \Gamma_0(m)) = (f, g | W_q; \Gamma_0(m)).$$

The proof is immediate from (1.4) since $f | W_q^2 = f$, and Δ and $W_q^{-1}\Delta$ are both fundamental domains of $\Gamma_0(m)$ since $W_q^{-1}\Gamma_0(m) W_q = \Gamma_0(m)$. We could have introduced Lemma 25 earlier, and slightly simplified that part of Theorem 3 relating to W_q. On the other hand, the discussion of oldforms would have been more complicated, since while the T_p remain the same operators on all the overgroups of $\Gamma_0(m)$, the W_q do not.

Lemma 26. *Let $g(\tau)$ be a form on $\Gamma_0(m')$, where $m' | m$, and let $d | (m/m')$. For any prime $q | m$, let $q^\alpha \| m$, $q^{\alpha-\beta} \| m'$, $q^\gamma \| d$, so that $\gamma \leqq \beta \leqq \alpha$. For $\gamma \leqq \beta/2$ let $d' = q^{\beta-2\gamma} d$, so that $q^{\beta-\gamma} \| d'$ and $d' | (m/m')$. Let W_q be the operator on $\Gamma_0(m)$ and W_q' that on $\Gamma_0(m')$ as defined by (2.3) in Lemma 9. Then*

$$(g | A_d) | W_q = (g | W_q') | A_{d'}.$$

For $A_d W_q A_{d'}^{-1} = (xq^\alpha d, ydd'; mz, wq^\alpha d')$, a matrix of determinant $dd'q^\alpha$, and dividing each entry by $q^{\beta-\gamma} d$ we obtain a suitable W_q' of determinant $q^{\alpha-\beta}$.

We now consider the effect of W_q on the oldclasses. If $g(\tau)$ is a newform on $\Gamma_0(m')$, then $g | W_q' = \lambda'(q) \cdot g(\tau)$, where $\lambda'(q) = \pm 1$ (if $(q, m') = 1$ we take conventionally $W_q' = I$ and $\lambda'(q) = 1$). In terms of B_d Lemma 26 becomes

$$(g | B_d) | W_q = q^{k(\beta-2\gamma)} (g | W_q') | B_{d'},$$

so that $(g|B_d)|W_q = \lambda'(q)\cdot q^{k(\beta-2\gamma)}\cdot g|B_{d'}$, and since W_q is of period 2, $(g|B_{d'})|W_q = \lambda'(q)\cdot q^{k(2\gamma-\beta)}\cdot g|B_d$. Thus the d dividing m/m' split into pairs (d, d') with $d'>d$ such that

$$g|B_d \pm q^{k(\beta-2\gamma)} g|B_{d'} \quad \text{is an eigenform of } W_q \text{ with eigenvalue } \pm\lambda'(q), \tag{5.1}$$

and if $\beta = 2\gamma$ when β is even then

$$g|B_d \quad \text{is an eigenform of } W_q \text{ with eigenvalue } \lambda'(q). \tag{5.2}$$

We may now, either by repeated application of (5.1) and (5.2), or directly using Lemma 25 and the commutativity of W_q and T_p, establish

Lemma 27. *There exists a basis $f_i(\tau)$ $(i=1$ to $\nu)$ for $\langle\Gamma_0(m), k\rangle_0$ such that each $f_i(\tau)$ is an eigenform of all the operators T_p and W_q, where $(p, m)=1$ and $q|m$.*

It is not possible to make the $f_i(\tau)$ also eigenforms of all the operators U_q. We now define, for a newform

$$F(\tau) = x + \sum_{n=2}^{\infty} a(n)x^n$$

on $\Gamma_0(m)$, the associated ζ-function by

$$\zeta(s) = 1 + \sum_{n=2}^{\infty} a(n)\cdot n^{-s}. \tag{5.3}$$

By the estimate (4.3) it is clear that the series in (5.3) converges for $\mathrm{Re}\, s > k+1$. Now by Theorem 3 and the remark after Lemma 9 we have

$$F|(0, -1; m, 0) = F|\prod_q W_q = \gamma F(\tau),$$

where $\gamma = \pm 1$, so that

$$F(-1/m\tau) = \gamma m^k \tau^{2k} F(\tau). \tag{5.4}$$

Now if

$$R(s) = \int_0^{\infty} F(iy) y^{s-1}\, dy, \tag{5.5}$$

where $y^{s-1} = \exp[(s-1)\log y]$, we have formally

$$\begin{aligned} R(s) = -\int_0^{\infty} F\left(\frac{i}{my}\right)(my)^{1-s} d(m^{-1}y^{-1}) &= \int_0^{\infty} \gamma m^k (iy)^{2k} F(iy)\cdot m^{-s} y^{-s-1}\, dy \\ &= \gamma\cdot(-1)^k m^{k-s} R(2k-s), \end{aligned} \tag{5.6}$$

and the convergence is assured for all s by the estimate $F(iy) = O(e^{-2\pi y})$ as $y\to\infty$ and $F(iy) = O(y^{-2k}e^{-2\pi/my})$ as $y\to 0+$, the latter obtained from (5.4). These estimates show that $R(s)$ is an entire function. Further we may for $\mathrm{Re}\, s > k+1$ integrate term-by-term in (5.5) to give

$$R(s) = (2\pi)^{-s}\Gamma(s)\zeta(s), \tag{5.7}$$

and $\zeta(s)$ can be continued over the whole s-plane by means of (5.7). We now have

Lemma 28. *For* $\mathrm{Re}\, s > k+1$ we have

$$\zeta(s) = \prod_q (1 - a(q) \cdot q^{-s})^{-1} \prod_p (1 - a(p) \cdot p^{-s} + p^{2k-1-2s})^{-1},$$

where the products are over primes p *with* $(p, m) = 1$ *and primes* q *with* $q | m$.

The proof is immediate from (i)′ and (ii)′ of Theorem 3. For brevity in the discussion which follows we shall write

$$\zeta_q(s) = (1 - a(q) \cdot q^{-s})^{-1}, \quad \zeta_p(s) = (1 - a(p) \cdot p^{-s} + p^{2k-1-2s})^{-1}.$$

Theorem 4. *If* $g_1(\tau)$ *is a newform on* $\Gamma_0(m_1)$, *and* $g_2(\tau)$ *is a newform on* $\Gamma_0(m_2)$, *then* $g_1(\tau)$ *and* $g_2(\tau)$ *have distinct eigenvalues with respect to an infinity of the operators* T_p *for* $(p, m_1 m_2) = 1$, *or else* $g_1(\tau) \equiv g_2(\tau)$ *and* $m_1 = m_2$.

Let $\zeta^1(s)$, $R^1(s)$ and $\zeta^2(s)$, $R^2(s)$ be the functions associated with $g_1(\tau)$ and $g_2(\tau)$ by (5.3) and (5.5). If Theorem 4 is false, let r denote any prime dividing m_1 or m_2, or any of the finite set of primes p with $(p, m_1 m_2) = 1$ for which the eigenvalues of $g_1(\tau)$ and $g_2(\tau)$ differ. Then $R^1(s)/R^2(s) = \zeta^1(s)/\zeta^2(s) = \prod_r \zeta_r^1(s)/\zeta_r^2(s)$. Now $R^1(2k-s)/R^2(2k-s) = (m_1/m_2)^{s-k} \gamma_1 \gamma_2 R^1(s)/R^2(s)$, and since the finite product over r can clearly be continued over the whole s-plane we have an identity

$$(m_1/m_2)^{k-s} \gamma_1 \gamma_2 = \prod_r \zeta_r^1(s) \zeta_r^2(2k-s) / (\zeta_r^2(s) \zeta_r^1(2k-s)). \tag{5.8}$$

As s varies, (5.8) is an identity involving rational functions of r^{-s}. Since there can be no non-trivial algebraic relation between the r^{-s} for different r and all s, it follows that every separate factor on the right-hand side of (5.8) must be a constant (with respect to s) multiple of the power of r^{-s} (if any) occurring in the left-hand side. Let $\mu_1 = 0$ or 1 according as $r | m_1$ or $(r, m_1) = 1$, and define μ_2 similarly. Then with $z = r^{-s}$, $a_1 = a_1(r)$, $a_2 = a_2(r)$ we may write

$$\begin{aligned} &(1 - a_2 z + \mu_2 r^{2k-1} z^2)(1 - a_1 \cdot r^{-2k} z^{-1} + \mu_1 r^{-2k-1} z^{-2}) \\ &\quad = K z^e (1 - a_1 z + \mu_1 r^{2k-1} z^2)(1 - a_2 r^{-2k} z^{-1} + \mu_2 r^{-2k-1} z^{-2}), \end{aligned} \tag{5.9}$$

where K is independent of z and e is integral, and (5.9) is an identical relation in z. We now consider three cases.

Case 1. $\mu_1 = \mu_2 = 1$. Then $a_1 \neq a_2$ by hypothesis. The four zeros $z = z_j$ of each side of (5.9) with $z \neq 0, \infty$ must be the same. Now $(1 - a_1 z + r^{2k-1} z^2)$ and $(1 - a_2 z + r^{2k-1} z^2)$ have no common zero, so that we must have $1 - a_1 z + r^{2k-1} z^2 \equiv 1 - a_1 r z + r^{2k+1} z^2$, which is clearly false.

Case 2. $\mu_1 = 1, \mu_2 = 0$. If $r^2 | m_2$ then $a_2 = 0$, which is impossible. If $r \| m_2$, then $a_2 = -\lambda_2(r) \cdot r^{k-1}$ by Theorem 3, so that $a_2^{-1} \neq a_2 r^{-2k}$, and thus a_2^{-1} is a zero of $(1 - a_1 z + r^{2k-1} z^2)$, giving $a_1 = -\lambda_2(r) \cdot (r^{k-1} + r^k)$, and this makes (5.9) consistent with $K z^e = \lambda_2(r) \cdot r^{-k} z^{-1}$. However in this case we have, by Theorem 3, (i)′,

$$|a_1(r^n)| = \frac{(r^{n+1})^k - (r^{n+1})^{k-1}}{r^k - r^{k-1}},$$

and thus $|a_1(r^n)| \geqq C \cdot (r^n)^k$ for some fixed C, and all n, which is impossible by (4.3). The case $\mu_1 = 0$, $\mu_2 = 1$ is similarly impossible.

Case 3. $\mu_1 = \mu_2 = 0$. Then (5.9) becomes $(1 - a_2 z)(1 - a_1 r^{-2k} z^{-1}) = K z^e (1 - a_1 z)(1 - a_2 r^{-2k} z^{-1})$. If $r \| m_2$, then $a_2 = \pm r^{k-1}$ so that a_2^{-1} is not a zero of $(1 - a_2 r^{-2k} z^{-1})$ and hence $a_1 = a_2$, and the equation holds with $K z^e = 1$. Similarly for $r \| m_1$. If $r^2 | m_1$ and $r^2 | m_2$, then both $a_1 = a_2 = 0$, and the equation is trivial with $K z^e = 1$. In either event we have $\zeta_r^1(s) = \zeta_r^2(s)$.

Thus finally we have $\prod_r \zeta_r^1(s) = \prod_r \zeta_r^2(s)$ over all the possible primes r, and the remaining primes π involved in $\zeta^1(s)$ and $\zeta^2(s)$ have $\zeta_\pi^1(s) = \zeta_\pi^2(s)$ by hypothesis, so that $\zeta^1(s) = \zeta^2(s)$ and hence $g_1(\tau) = g_2(\tau)$. This completes the proof of Theorem 4.

We do not know whether Theorem 4 can be proved without recourse to the zeta function. In any event, it does not seem possible to avoid the appeal to some good estimate such as (4.3); our argument in Case 2 carries through with only $a(n) = o(n^k)$, but the easy $a(n) = O(n^k)$ estimate is insufficient to prove $|a(p)| < p^{k-1} + p^k$. There seems to be no hope of proving Theorem 4 by purely group-theoretic and number-theoretic arguments. The identity

$$f_1(\tau) - q_2 f_1(q_2 \tau) = f_2(\tau) - q_1 f_2(q_1 \tau),$$

with $f_i(\tau)$ new on $\Gamma_0(q_i)$ $(i = 1, 2)$ and q_i prime, is perfectly consistent if $a_1(q_2)$ and $a_2(q_1)$ have the values given in Case 2 above, so that $\Gamma_0(q_1 q_2)$ presents all the essential difficulties.

In one case however we can avoid the appeal to Theorem 4. For $\Gamma_0(q^\alpha)$, with q prime, we can use Lemma 24 with respect to any pair $m_1 | q^\alpha$, $m_2 | q^\alpha$, since then $m_1 | m_2$ or $m_2 | m_1$. We now establish Theorem 5 in which we summarize some previous results and state our main result on the basis of $\Gamma_0(m)$.

Theorem 5. *The vector space $\langle \Gamma_0(m), k \rangle_0$ has a basis which is a direct sum of classes. The classes consist of newclasses and oldclasses. Every form in the same class has the same eigenvalues of T_p for all primes p with $(p, m) = 1$. Two forms in different classes have distinct eigenvalues of T_p for an infinity of p.*

Each newclass consists of a single form $F(\tau)$ which is an eigenform of every W_q and U_q for $q | m$. If $q^2 | m$ then $F | U_q = 0$, and if $q \| m$ then $F | U_q = -q^{k-1} F | W_q = \pm q^{k-1} F(\tau)$.

Each oldclass consists of a set of forms $\{g(d\tau)\}$ where $g(\tau)$ is a newform on $\Gamma_0(m')$ for some proper divisor m' of m, and d runs over all divisors of m/m'. Also any such set $\{g(d\tau)\}$ is an oldclass.

The vector space spanned by any oldclass can be given an alternative basis consisting of forms which are eigenforms of all the W_q for $q | m$.

Any form in $\langle \Gamma_0(m), k \rangle_0$ which is an eigenform of all the T_p, U_q, and W_q is a constant multiple of some newform.

Proof. By Lemma 22 the oldclasses form a basis for the oldforms. By Theorem 4 no two oldclasses are equivalent under the $\sim$ of Theorem 2, nor is a newclass equivalent to an oldclass, so that the vector spaces spanned by the

oldclasses and newclasses are precisely the vector spaces spanned by the equivalence classes of Theorem 2. The forms in an oldclass are independent, since any relation $\sum_{i=1}^{r} \lambda_i g(d_i\tau)=0$ with $d_1<d_2<\cdots$ implies $\lambda_1 x^{d_1}+O(x^{d_1+1})=0$ which is false. Thus the oldclasses and the newclasses form a basis for $\langle \Gamma_0(m), k\rangle_0$.

By Lemma 27 we may define a basis of $\langle \Gamma_0(m), k\rangle_0$ which consists of eigenforms of all the W_q and T_p, and by Lemma 26 any W_q maps an oldclass into itself. Suppose now that $g(\tau)$ is a newform on $\Gamma_0(m')$, and that

$$G(\tau)=\sum_i \lambda_i g|B_{d_i} \qquad (d_i|(m/m')) \tag{5.10}$$

is an eigenform of all the U_q and W_q (necessarily of the T_p), and let q be a prime dividing m/m', with $q^\beta \| (m/m')$. We may rewrite (5.10) as

$$G(\tau)=\sum_j g_j^*|(\mu_{0j}+\mu_{1j}B_q+\cdots+\mu_{\beta j}B_{q^\beta}), \tag{5.11}$$

where $g_j^*=g|B_{d_j}$ and d_j runs over all the divisors of $(m/m'q^\beta)$. Both U_q and W_q map each term in the sum over j into an expression of the same form, and hence each term must be an eigenform of U_q and W_q (since the $g|B_{d_i}$ are linearly independent). Dropping the suffix j, so that $\mu_{\gamma j}=\mu_\gamma$, etc., we have for W_q, by (5.1),

$$\mu_{\beta-\gamma}=\pm q^{k(\beta-2\gamma)}\mu_\gamma \qquad (\gamma\neq\beta/2). \tag{5.12}$$

If also $G|U_q=\varrho G$ we have

$$\mu_1+a\mu_0=\varrho\mu_0,\ \mu_2+b\mu_0=\varrho\mu_1,\ \mu_\gamma=\varrho\mu_{\gamma-1}(\gamma\geqq 3),\ \varrho\mu_\beta=0(\beta\geqq 2), \tag{5.13}$$

since $g^*|B_{q^\gamma}|U_q=g^*|B_{q^{\gamma-1}}$ if $\gamma\geqq 1$, while $g^*|U_q=0$ if $q^2\mid m'$, $\pm q^{k-1}g^*(\tau)$ if $q\| m'$, and $c(q)g^*(\tau)-q^{2k-1}g^*|B_q$ if $(q,m')=1$, by Theorem 3 applied to $g(\tau)$, and $g|B_{d_j}|U_q=g|U_q|B_{d_j}$ for $(q,d_j)=1$. Thus

$$(a,b)=(c(q),-q^{2k-1}),\ (\pm q^{k-1},0),\ (0,0), \quad \text{as} \quad q\nmid m',\ q\| m',\ q^2|m'.$$

Now if $\mu_0=0$, we have $\mu_\gamma=0$ for all γ, by (5.13). If $\mu_0\neq 0$ and $\beta\geqq 2$, then $\mu_\beta\neq 0$ by (5.12) and so $\varrho=0$ by (5.13). Hence $\mu_\gamma=0$ for $\gamma\geqq 3$ by (5.13), and so in fact $\beta=2$ (else $\mu_\beta=0\neq 0$, a contradiction). Thus we need consider only $\mu_0\neq 0$, $\beta=1$ or 2.

Case 1. $\mu_0\neq 0$, $\beta=1$. Then $\mu_1=\pm q^k\mu_0$ by (5.12) and $\mu_1=(\varrho-a)\mu_0$, $\varrho\mu_1=b\mu_0$ by (5.13). So $b=\pm q^k\varrho$, $\varrho=a\pm q^k$, and $(a,b)=(\pm q^{k-1},0)$ or $(0,0)$ are clearly impossible. If $(a,b)=(c(q),-q^{2k-1})$ we obtain $c(q)=\mp(q^{k-1}+q^k)$ which is impossible as in the proof of Theorem 4.

Case 2. $\mu_0\neq 0$, $\beta=2$. Then $\mu_2=\pm q^{2k}\mu_0$, by (5.12), and $\varrho\mu_2=0$ by (5.13), so that $\varrho=0$. Hence $\mu_1=-a\mu_0$, $\mu_2=-b\mu_0$ by (5.13), or $b=\mp q^{2k}$, which is impossible.

We have therefore proved for each j in (5.11) that $\mu_{0j}=\mu_{1j}=\cdots=\mu_{\beta j}=0$, and hence $G(\tau)\equiv 0$. Thus q does not divide m/m', and this is true for each q

dividing m. Hence finally $m = m'$, and any form which is an eigenform of all the T_p, U_q, and W_q, is a newform. This completes the proof of Theorem 5.

Of course, as in Theorem 2, any form $f(\tau)$ on $\Gamma_0(m)$ which is an eigenform of all the T_p lies in the vector space spanned by some class. We could further subdivide the vector space spanned by an oldclass into subclasses every form in one of which was an eigenform of all the W_q, but this is not very convenient in practical application.

The operator U_q is not hermitian with respect to the scalar product on $\Gamma_0(m)$. It does not seem possible to give any satisfactory basis for oldclasses in terms of U_q.

6. Further Results

Theorem 5 shows that newforms with well-defined properties arise naturally on $\Gamma_0(m)$ after "removing" the oldforms. The definition of a newform via the orthogonal complement in a Hilbert space is however not feasible as a method of actually finding newforms. We are not concerned with any abstract concepts of "effective computability"; if one wishes to attempt the study of connexions between modular forms and algebraic geometry, then detailed knowledge of the Fourier coefficients of a newform may be helpful. In general the only feasible method we know is to use the T_p on various known forms (such as $\eta^2(\tau)\eta^2(83\tau)$ on $\langle \Gamma_0(83), 1\rangle_0$) to produce a basis for $\langle \Gamma_0(m), k\rangle_0$ and then diagonalise; knowledge of oldforms on overgroups assists in solving the large polynomial equations which arise.

In some cases, however, we may obtain certain newforms directly given the oldforms. These cases arise when $q^2 | m$, and q is an odd prime, or $q = 4$, or $q = 8$. We shall write

$$S_q = (q, 1; 0, q), \tag{6.1}$$

so that $S_1 = S$ and $S_q^q = S$. If $q^2 | m$ and $V = (a, b; q^2 c, d) \in \Gamma_0(m)$, then we have

$$S_q^\lambda V = V' S_q^\mu \quad (1 \leqq \lambda \leqq q-1, 1 \leqq \mu \leqq q-1), \tag{6.2}$$

where

$$V' = (\alpha, \beta; q^2 c, \delta) \in \Gamma_0(m) \quad \text{and} \quad \alpha = a + qc\lambda, \beta = b - \frac{\alpha\mu - d\lambda}{q}, \ \delta = d - qc\mu,$$

and, for a given λ and V, μ is chosen so that $a\mu \equiv d\lambda \pmod q$. This choice is clearly possible since $ad \equiv 1 \pmod q$, and indeed we have

$$\mu \equiv d^2 \lambda \pmod q. \tag{6.3}$$

Thus to each λ in $1 \leqq \lambda \leqq q-1$ there exists a μ in $1 \leqq \mu \leqq q-1$ such that (6.2) holds. We define, for an odd prime q,

$$f | R_q^* = \sum_{\lambda=1}^{q-1} \left(\frac{\lambda}{q}\right) \cdot f | S_q^\lambda, \tag{6.4}$$

where $\left(\frac{\lambda}{q}\right)$ is the quadratic reciprocity symbol. We then have

Lemma 29. *If $f(\tau)$ is on $\Gamma_0(m)$, where $q^2 \mid m$, then*

(i) *if q is an odd prime, $f \mid R_q^*$ is on $\Gamma_0(m)$,*

(ii) *if $q = 2$ or 4 or 8, or 3, then S_q^λ belongs to the normalizer of $\Gamma_0(m)$, and so $f \mid S_q^\lambda$ is on $\Gamma_0(m)$.*

Proof. If $V \in \Gamma_0(m)$ then by (6.2) and (6.3) we have for odd q,

$$f \mid R_q^* \mid V = \sum_{\lambda=1}^{q-1} \left(\frac{\lambda}{q}\right) f \mid V' \mid S_q^\mu = \sum_{\mu=1}^{q-1} \left(\frac{\mu}{q}\right) f \mid S_q^\mu = f \mid R_q^*,$$

since distinct λ in (6.3) give distinct μ, and $\left(\frac{\lambda}{q}\right) = \left(\frac{\mu}{q}\right)$. If $q = 2, 4, 8$, or 3, then $ad \equiv 1 \pmod q$ implies $d^2 \equiv 1 \pmod q$. Thus we can choose $\mu = \lambda$ in (6.3) and $S_q^\lambda V S_q^{-\lambda} = V' \in \Gamma_0(m)$.

We now consider the action of the operators $W_{q'}$ on $f \mid R_q^*$ and $f \mid S_q^\lambda$. When $q = 4$ or 8 in our statements, we shall mean by W_q an appropriate W_2 of (2.3).

Lemma 30. *Let $q^2 \mid m$, and $Q' = q'^{\alpha'} \parallel m$, where q' is a prime with $(q, q') = 1$. Then if $f(\tau)$ is on $\Gamma_0(m)$ we have*

(i) $(f \mid R_q^*) \mid W_{q'} = \left(\frac{Q'}{q}\right) \cdot (f \mid W_{q'}) \mid R_q^*$,

(ii) $(f \mid S_q^\lambda) \mid W_{q'}^{-1} = (f \mid W_{q'}) \mid S_q^{\lambda'}$ *where* $Q' \lambda \lambda' \equiv 1 \pmod q$.

Clearly (ii) implies (i) for odd prime q since $f \mid R_q^*$ is on $\Gamma_0(m)$ and we may thus after summing replace $W_{q'}^{-1}$ by $W_{q'}$. For (ii) we have

$$W_{q'} = (xQ', y; mz, wQ') = (x, y; mz/Q', wQ') A_{Q'} = A_{Q'}^{-1}(xQ', y; mz/Q', w),$$

so that

$$\begin{aligned} W_{q'} S_q^{\lambda'} W_{q'} &= (x, y; mz/Q', wQ') S_q^{\lambda' Q'} (xQ', y; mz/Q', w) \\ &= (x, y; mz/Q', wQ') \cdot (x'Q', y'; mz/Q', w') \cdot S_q^\lambda, \end{aligned}$$

and the product of the first two transformations, each in Γ, is clearly in $\Gamma_0(m)$. [We have used the *formal* transformation after (6.2) with m/Q' instead of m; since $q^2 \mid (m/Q')$ this remains valid.] Note that in general the two equal sides of (ii) depend on the choice of $W_{q'}$.

Lemma 31. *If $q^2 \mid m$, then*

(i) $W_q S_q^\lambda W_q \in \Gamma_0(m/q)$,

(ii) *if $(m/q^2, q) = 1$ and $(\lambda, q) = 1$ then we can choose λ' so that $S_q^\lambda W_q S_q^{\lambda'} \in \Gamma_0(m/q)$. We have $(\lambda/q) = (\lambda'/q)$ if q is an odd prime, and $\lambda = \lambda'$ if $q = 2, 4, 8$, or 3.*

(iii) *if $q = 2, 4, 8$, or 3, and $(m/q^2, q) = 1$ and $(\lambda, q) = 1$ then $(W_q S_q^\lambda)^3$ and $(S_q^\lambda W_q)^3 \in \Gamma_0(m)$.*

Proof. Let $Q = q^\alpha \parallel m$, or $Q = 2^\alpha \parallel m$ when $q = 4$ or 8, and $m' = m/q$, $Q' = Q/q$. Then $W_q = (xQ, y; mz, wQ) = W_q' A_q = A_q^{-1} W_q''$, where $W_q' = (xQ', y; m'z, wQ)$ and $W_q'' = (xQ, y; m'z, wQ')$ are both of the form (2.3) for q in relation to $\Gamma_0(m')$. Now $W_q S_q^\lambda W_q = W_q' S_q^{\lambda q} W_q''$, and $S_q^{\lambda q} = S^\lambda \in \Gamma_0(m')$, so that by Lemma 8 we have $W_q' S^\lambda W_q'' \in \Gamma_0(m')$. This proves (i).

The conditions of (ii) imply that $W_q=(xq^2, y; mz, wq^2)$ with $xwq^2-yz\cdot m/q^2=1$. We compute

$$S_q^{\lambda}W_qS_q^{\lambda'}=(q^4x+qm\lambda z,\ q^3\lambda' x+q^3\lambda w+q^2(y+\lambda\lambda' z\cdot m/q^2);\ q^2mz,\ qm\lambda' z+q^4w).$$

This is a matrix of determinant q^6, and every term is divisible by q^3 if λ' is chosen so that $y+\lambda\lambda' z\cdot m/q^2\equiv 0(\mathrm{mod}\, q)$. Since $-yz\cdot m/q^2\equiv 1(\mathrm{mod}\, q)$, this implies $\lambda\equiv\lambda'(\mathrm{mod}\, q)$, if $q=2, 4, 8$, or 3, and $(\lambda/q)=(\lambda'/q)$ if q is an odd prime. In this case we obtain a transformation in $\Gamma_0(q^2m/q^3)=\Gamma_0(m/q)$.

By Lemma 29 (ii) the proof of (iii) is reduced to the case of $(W_qS_q^{\lambda})^3$ and for this we need only prove $(W_qS_q^{\lambda})^3\in\Gamma_0(q^2)$, since we know already from (i) and (ii) that $(W_qS_q^{\lambda})^3\in\Gamma_0(m/q)$. Conjugating by A_q, we must prove that $(A_qW_qS_q^{\lambda}A_q^{-1})^3\in\Gamma_0^0(q)$. Now

$$A_qW_qA_q^{-1}=(xq, y; z\cdot m/q^2, wq)\in\Gamma \quad\text{and}\quad A_qS_q^{\lambda}A_q^{-1}=S^{\lambda}\in\Gamma.$$

Thus modulo q we have

$$M=A_qW_qS_q^{\lambda}A_q^{-1}\equiv(0, \alpha; -\alpha^{-1}, 0)\,(1, \lambda; 0, 1)\equiv(0, \alpha; -\alpha^{-1}, -\alpha^{-1}\lambda).$$

This last matrix is unimodular modulo q; if its trace is t we have $M^2-tM+I\equiv 0$, $M^3\equiv(t^2-1)M-tI\equiv -tI(\mathrm{mod}\, q)$ since $t^2\equiv 1(\mathrm{mod}\, q)$ for $t=-\alpha^{-1}\lambda$ prime to q and $q=2, 4, 8, 3$. Thus M^3 is congruent to a matrix in $\Gamma_0^0(q)$ modulo q, and hence $M^3\in\Gamma_0^0(q)$, as desired. This completes the proof of Lemma 31.

We now define, for $f(\tau)=\sum a(n)x^n$, the operators R_q, R_{χ}, R_{ψ}, $R_{\chi\psi}$ by

$$f\,|\,R_q=\sum\left(\frac{n}{q}\right)a(n)x^n \qquad (q \text{ an odd prime}),$$

$$f\,|\,R_{\chi}=\sum\chi(n)\,a(n)x^n,\quad f\,|\,R_{\psi}=\sum\psi(n)\,a(n)x^n,\quad f\,|\,R_{\chi\psi}=\sum\chi(n)\cdot\psi(n)\,a(n)x^n,$$

where

$$\chi(n)=(-1)^{(n-1)/2},\qquad \psi(n)=(-1)^{(n^2-1)/8}\qquad (n \text{ odd})$$

and

$$\chi(n)=\psi(n)=0\qquad (n \text{ even}). \tag{6.5}$$

We shall when convenient denote any of these four operators by R_{ϕ}, where $\phi(n)$ is the appropriate quadratic character $\left(\frac{n}{q}\right)$, $\chi(n)$, $\psi(n)$, or $\chi(n)\,\psi(n)$. We have

Lemma 32. *$f\,|\,R_q^*=k_q\cdot f\,|\,R_q$, ($k_q=\sqrt{q}$ or $i\sqrt{q}$ as $q\equiv 1$ or 3 modulo 4),*

$$f\,|\,(S_4-S_4^3)=2i\,f\,|\,R_{\chi},$$

$$f\,|\,(S_8-S_8^3-S_8^5+S_8^7)=2\sqrt{2}\,f\,|\,R_{\psi},$$

$$f\,|\,(S_8+S_8^3-S_8^5-S_8^7)=2i\sqrt{2}\,f\,|\,R_{\chi\psi}.$$

For with $\omega=e^{2\pi i/q}$ we have

$$f\,|\,R_q^*=\sum_n a(n)\sum_{\lambda=1}^{q-1}\left(\frac{\lambda}{q}\right)\omega^{n\lambda}x^n=\sum_n a(n)\sum_{\lambda=1}^{q-1}\left(\frac{n\lambda}{q}\right)\cdot\omega^{n\lambda}\left(\frac{n}{q}\right)x^n,$$

whether n is zero modulo q or not. Now if $(n, q) = 1$ we have

$$\sum_{\lambda=1}^{q-1} \left(\frac{n\lambda}{q}\right)\omega^{n\lambda} = \sum_{j=1}^{q-1} \left(\frac{j}{q}\right)\omega^{j} = k_q .$$

The proofs of the other statements are analogous. The values of the constants are unimportant, since they occur on both sides of any result we prove by translating the operators (6.5) by Lemma 31.

Lemma 33. *If $f(\tau)$ is on $\Gamma_0(m)$, then $f|R_q$, $f|R_\chi$, $f|R_\psi$, $f|R_{\chi\psi}$ are also on $\Gamma_0(m)$ provided that $q^2|m$, $16|m$, $64|m$, $64|m$ respectively. If $(p, m) = 1$ and $Q' = q'^{\alpha'} \| m$, then for any of these R_ϕ we have*

(i) $(f|R_\phi)|T_p = \phi(p)\cdot(f|T_p)|R_\phi$,

(ii) $(f|R_\phi)|U_{q'} = \phi(q')\cdot(f|U_{q'})|R_\phi$,

(iii) $(f|R_\phi)|W_{q'} = \phi(Q')\cdot(f|W_{q'})|R_\phi$, $\quad(\phi(Q') \neq 0)$.

That $f|R_\phi$ is on $\Gamma_0(m)$ follows from Lemmas 29 and 32. The proofs of (i) and (ii) are immediate from the Fourier series, and (ii) is valid even if $\phi(q') = 0$. Lemma 30 and Lemma 32 give (iii), since $\phi(Q') \neq 0$ implies q' prime to q or to 2 as relevant.

Suppose now that $f(\tau)$ is a newform on $\Gamma_0(m)$, where $q^\alpha \| m$ $(\alpha \geqq 2)$ and q is an odd prime. Then $f^*(\tau) = f|R_q$ is a form on $\Gamma_0(m)$. If $f^*(\tau)$ is *not* a newform, then since by Lemma 33 it is an eigenform of all the T_p, it must lie in the vector space spanned by some oldclass, defined by a form $g(\tau)$ which is a newform on $\Gamma_0(m')$ for $m'|m$. Since also by Lemma 33 $f^*(\tau)$ is an eigenform of all $U_{q'}$ and $W_{q'}$ with $(q', q) = 1$, the argument used at the end of the proof of Theorem 5 shows that $m = m'q^\beta$ $(\beta \geqq 1)$, and since $f^*(\tau) = x + \sum_{n=2}^{\infty} a(n)x^n$ with $f^*|U_q = 0$, we must in fact have

$$f^*(\tau) = g|K_q = g(\tau) - (g|U_q)|B_q ,$$

the annihilator defined by (3.3). Now $f(\tau) = f^*|R_q$ (since $f|U_q = 0$ as $q^2|m$), so that $f(\tau) = g|R_q$, and is certainly on $\Gamma_0(m'q^{\max(\alpha-\beta,2)-(\alpha-\beta)})$ since $q^{\alpha-\beta} \| m'$. Thus we have the inequality

$$\max(\alpha - \beta, 2) \geqq \alpha .$$

If $\alpha - \beta \geqq 2$ this is impossible, and otherwise we have $\beta \geqq \alpha - 1$, $\alpha = 2$, $\beta \leqq \alpha$, giving as the only possibilities $\alpha = 2$ and $\beta = 1$ or 2.

Conversely, let $g(\tau)$ be any newform on $\Gamma_0(m/q)$ or $\Gamma_0(m/q^2)$, where $q^2 \| m$, and define $f(\tau) = g|R_q$, which is certainly a form on $\Gamma_0(m)$, and an eigenform of all $U_{q'}$ and $W_{q'}$ for $q'|m$ and $(q, q') = 1$. Then by Lemma 31 (ii) we have $g|S_q^\lambda W_q = g|S_q^{-\lambda'}$, where $(\lambda/q) = (\lambda'/q)$, so that $(g|R_q)|W_q = (-1/q)g|R_q$. Moreover $f|U_q = 0$, so that $f(\tau)$ is an eigenform of *all* U_q and W_q for $q|m$, and hence $f(\tau)$ is a *newform* on $\Gamma_0(m)$, by Theorem 5.

Finally let $q=3$, and suppose that $f(\tau)$ and $f|R_3$ are *both* newforms on $\Gamma_0(m)$, where $3^2 \| m$. We may write

$$f = X_1 + X_2,\ f|R_3 = X_1 - X_2,$$

where $X_1 = \sum_{n\equiv 1(3)} a(n)x^n$ and $X_2 = \sum_{n\equiv 2(3)} a(n)x^n$. Then X_1, X_2, are on $\Gamma_0(m)$. We have, with $\lambda, \lambda^* = \pm 1$,

$$f|W_3 = \lambda(X_1 + X_2),\ f|R_3|W_3 = \lambda^*(X_1 - X_2),\ X_1|S_3 = \omega X_1,\ X_2|S_3 = \omega^2 X_2$$
$$(\omega = e^{2\pi i/3}).$$

We infer $X_1|W_3 = \pm X_1$ or $\pm X_2$, $X_2|W_3 = \pm X_2$ or $\pm X_1$ (with no implied correspondence in the *signs*). Now $(W_3 S_3)^3 \in \Gamma_0(m)$, by Lemma 31 (iii), and applying this to X_1 and X_2 we deduce $X_1|W_3 = X_1$, $X_2|W_3 = X_2$, so that $\lambda = \lambda^* = 1$.

We sum up this discussion in

Theorem 6. *Let q be an odd prime, and $f(\tau)$ a newform on $\Gamma_0(m)$, where $q^2|m$, and write $f^*(\tau) = f|R_q$.*

(i) *If $q^3|m$, then $f^*(\tau)$ is also a newform on $\Gamma_0(m)$. (It is of course possible that $f^*(\tau) = f(\tau)$.)*

(ii) *If $q^2 \| m$, and $f^*(\tau)$ is* not *a newform on $\Gamma_0(m)$, then $f^*(\tau) = g|K_q$, where $g(\tau)$ is a newform on $\Gamma_0(m/q)$ or $\Gamma_0(m/q^2)$. The eigenvalues of $f^*(\tau)$ for all T_p, $U_{q'}$, and $W_{q'}$ with $(q, q') = 1$ are the same as those of $g(\tau)$. In this case $f|W_q = (-1/q)f(\tau)$.*

(iii) *If $q = 3$, $3^2 \| m$, and $f^*(\tau)$ is a newform on $\Gamma_0(m)$, then $f|W_3 = f(\tau)$ and $f^*|W_3 = f^*(\tau)$.*

Conversely, if $g(\tau)$ is any newform on $\Gamma_0(m/q^2)$ or $\Gamma_0(m/q)$, where $q^2 \| m$, then $g|R_q$ is a newform on $\Gamma_0(m)$, with eigenvalues derivable from those of $g(\tau)$ by Lemma 33 for T_p and $U_{q'}$ and $W_{q'}$ with $(q, q') = 1$ and

$$(g|R_q)|U_q = 0,\ (g|R_q)|W_q = \left(\frac{-1}{q}\right)(g|R_q).$$

To simplify the statement of the corresponding theorem for powers of 2, we shall omit in Theorem 7 the references to T_p and $U_{q'}$ and $W_{q'}$, and also the converse statements, which are precisely analogous to those of Theorem 6.

Theorem 7. *Let m' be odd (m may be odd or even).*

(i) *If $f(\tau)$ is a newform on $\Gamma_0(4m')$, then $f|W_2 = -f(\tau)$.*

(ii) *If $f(\tau)$ is a newform on $\Gamma_0(32m)$, so is $f|R_\chi$. If $f(\tau)$ is a newform on $\Gamma_0(16m')$, then $f|R_\chi = g|K_2$, where $g(\tau)$ is a newform on $\Gamma_0(2^\alpha m')$ for some $0 \leqq \alpha \leqq 3$. If $\alpha \leqq 2$, then $f|W_2 = -f(\tau)$.*

(iii) *If $f(\tau)$ is a newform on $\Gamma_0(128m)$, so are $f|R_\psi$ and $f|R_{\chi\psi}$. If $f(\tau)$ is a newform on $\Gamma_0(64m')$, then either*

(a) *$f|R_\psi$ and $f|R_{\chi\psi}$ are both newforms on $\Gamma_0(32m')$; or*

(b) *$f|R_\psi = g|K_2$ where $g(\tau)$ is a newform on $\Gamma_0(2^\alpha m')$ for some $0 \leqq \alpha \leqq 3$, and $f|W_2 = f(\tau)$; or*

(c) $f|R_{\chi\psi}=g|K_2$ *where* $g_2(\tau)$ *is a newform on* $\Gamma_0(2^\alpha m')$ *for some* $0\leqq\alpha\leqq 3$, *and* $f|W_2=-f(\tau)$.

Proof. For (i), we observe that $f|S_2=-f(\tau)$ (since $f|U_2=0$) and $f|(W_2S_2)^3=f(\tau)$ by Lemma 31 (iii). The first part of (ii) is similar to that of Theorem 6 (i). If $f(\tau)=X_1+X_3$ and $f|R_\chi=X_1-X_3$ are *both* newforms on $\Gamma_0(16m')$, then $X_1|W_2=\pm X_1$ or $\pm X_3$, $X_3|W_2=\pm X_3$ or $\pm X_1$, and now $X_1|(W_2S_4)^3=X_1$ is impossible, since $X_1|S_4=iX_1$, $X_3|S_4=-iX_3$. Hence $f|R_\chi$ is an oldform equal to $g|K_2$ where $g(\tau)$ is a newform on $\Gamma_0(2^\alpha m')$, $0\leqq\alpha\leqq 3$. (Of course $g|K_2=g(\tau)$ if $\alpha=2$ or 3.) If $\alpha\leqq 2$, then by Lemma 31 (ii) we have $g|R_\chi|W_2=-g|R_\chi$ or $f|W_2=-f(\tau)$. The proof of (iii) is similar in principle but more tedious. We have to consider three distinct possible types of behaviour for X_1, X_3, X_5, and X_7 under W_2 to show that if $f(\tau)$ is a newform on $\Gamma_0(64m')$ then $f|R_\psi$ and $f|R_{\chi\psi}$ are oldforms. The rest is simple, observing that $f|R_{\chi\psi}=f|R_\chi|R_\psi$.

It is interesting to note that all the newforms on $\Gamma_0(16m')$ and $\Gamma_0(64m')$ can be inferred from a knowledge of the oldforms. This implies certain relations between the dimensions of vector spaces of newforms, which we now calculate directly. Let $\delta(m)$ be the dimension of $\langle\Gamma_0(m),k\rangle_0$ and $\nu(m)$ the number of newforms. Then we have

$$\delta(m)=\sum_{m'|m}\nu(m')\cdot d(m/m'), \tag{6.6}$$

where $d(n)$ is the number of divisors of n. We deduce

$$\nu(m)=\sum_{m'|m}\delta(m')\cdot\beta(m/m'), \tag{6.7}$$

where $\beta(n)=\sum_{d|n}\mu(d)\,\mu(n/d)$ is multiplicative, and $\beta(p)=-2$, $\beta(p^2)=1$, $\beta(p^\alpha)=0$ ($\alpha\geqq 3$), for any prime p. If $(p,m)=1$, write $D_\alpha=\sum_{m'|m}\delta(m'p^\alpha)\cdot\beta(m/m')$. Then (6.7) implies that

$$\sum_{\gamma=0}^{\alpha}(\alpha-\gamma+1)\cdot\nu(mp^\gamma)=D_\alpha. \tag{6.8}$$

Now if $p=2$ then, for $\alpha\geqq 2$, $\Gamma_0(m'p^\alpha)$ has no elliptic elements, so that $\delta(m'p^\alpha)$ is easily calculated ([7], pages 216 and 293), giving $\nu(16m)=\nu(8m)+\nu(4m)+\nu(2m)+\nu(m)$ and $\nu(64m)=\sum_{\alpha=0}^{5}\nu(2^\alpha m)$ as expected.

We take this opportunity of correcting an error in Lehner and Newman [8], and state without proof in Theorem 8 the normalizer of $\Gamma_0(m)$ in $LF(2,C)$. That the group we describe is in the normalizer follows easily from our previous results, but our proof that it is the whole normalizer is tedious, and we omit it since we have not required to use it. To avoid introducing new notation, we use the same symbols R for an element of the factor group $N_m/\Gamma_0(m)$ and the coset representative in the decomposition $N_m=\sum_R\Gamma_0(m)\cdot R$.

Theorem 8[6]. *The normalizer of* $\Gamma_0(m)$ *in* $LF(2, C)$ *is the direct product of the following groups:*

(i) $\{C\}$; $C=(i, 0; 0, -i)$, $C^2=I$,

(ii) $\{W_q\}$; $W_q^2=I$ *(for each* $q \geqq 5$, $q \mid m$*)*,

(iii) (a) *if* $3 \| m$, $\{W_3\}$; $W_3^2=I$,

(b) *if* $9 \| m$, $\{W_3, S_3\}$; $W_3^2=S_3^3=(W_3 S_3)^3=I$ *(order 12)*,

(c) *if* $27 \mid m$, $\{W_3, S_3\}$; $W_3^2=S_3^3=I$; S_3 *and* $W_3 S_3 W_3$ *commute (order 18)*,

(iv) *if* $2^\lambda \| m$ $(\lambda \geqq 1)$ *and* $\mu=\min(3, [\lambda/2])$, $\nu=2^\mu$, *then*

(a) *if* $\lambda=1$, $\{W_2\}$; $W_2^2=I$,

(b) *if* $\lambda=2\mu$, $\{W_2, S_\nu\}$; $W_2^2=S_\nu^\nu=(W_2 S_\nu)^3=I$; *orders 6, 24, and 96 for* $\nu=2, 4,$ *and 8 respectively (for* $\nu=8$ *the relations given do not completely define the group, which is isomorphic to* $\Gamma/\Gamma_0^0(8)$*)*,

(c) *if* $\lambda>2\mu$, $\{W_2, S_\nu\}$; $W_2^2=S_\nu^\nu=I$; S_ν *and* $W_2 S_\nu W_2$ *commute (order* $2\nu^2$*)*.

The normalizer of $\Gamma_0(m)$ *in* $LF(2, R)$ *consists of* (ii) *to* (iv) *above, omitting* (i).

7. Concluding Remarks

As we remarked earlier, the eigenvalues $a(p)$ are algebraic integers, and of course real since T_p is hermitian with respect to the scalar product. Further number-theoretic information about the $a(p)$ must probably await developments in algebraic geometry. In one case, however, there is already a clear conjecture, due to Weil [15], that when $k=1$, every elliptic curve defined over Z corresponds to an eigenform with rational integral Fourier coefficients of all the T_p on some $\Gamma_0(m)$, where m is the "conductor" of the curve. It seems clear that this form must be a newform in our sense, and that our Theorems 3, 6, and 7 define the correct form of the ζ-function of the curve and associated curves with regard to the "bad" primes dividing the conductor.

So far as we know, the full statements of Theorems 3 and 5 are new if m is not prime; the case $m=q$ is discussed by Hecke [4, II] and Petersson [10, II], who effectively defines a newform in this case via orthogonality in the scalar product.

It should be possible to extend the concept of the newform to the case of $\Gamma(m)$. In particular, while Hecke's characters are clearly inherent in the problem, we feel that his "Teiler" and corresponding operators T_m^t are somewhat artificial, and do not help to attack the main problem, which is to determine what "newforms" give rise to "oldforms" on $\Gamma(m)$, and the properties of these newforms relative to the operators appropriate to the group on which they are new.

References

1. Eichler, M.: Quaternäre quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktionen. Arch. der Math. **5**, 355—366 (1954).
2. Gantmacher, F. R.: The theory of matrices. New York: Chelsea 1959.
3. Gunning, R. C.: Lectures on modular forms. Princeton: University Press 1962.

[6] We do not prove this theorem here.

4. Hecke, E.: Über Modulfunktionen und die Dirichletschen Reihen mit Eulerscher Produktentwicklung, I, II. Math. Ann. **114**, 1—28, 316—351 (1937).
5. — Analytische Arithmetik der positiven quadratischen Formen. Kgl. Danske Videnskabernes Selskab. XIII, **12** (1940).
6. Igusa, J.-I.: Kroneckerian model of fields of elliptic modular functions. Amer. J. Math. **81**, 561—577 (1959).
7. Lehner, J.: Discontinuous groups and automorphic functions. Providence, 1964.
8. — Newman, M.: Weierstrass points of $\Gamma_0(n)$. Ann. of Math. **79**, 360—368 (1964).
9. Newman, M.: The normalizer of certain modular subgroups. Canad. J. Math. **8**, 29—31 (1956).
10. Petersson, H.: Konstruktion der sämtlichen Lösungen einer Riemannschen Funktionalgleichung durch Dirichlet-Reihen mit Eulerscher Produktentwicklung, I, II, III. Math. Ann. **116**, 401—412 (1939), **117**, 39—64 (1939), **117**, 277—300 (1940).
11. Rankin, R. A.: Hecke operators on congruence subgroups of the modular group. Math. Ann. **168**, 40—58 (1967).
12. Selberg, A.: On the estimation of Fourier coefficients of modular forms. Proc. Symposium Pure Math. (Amer. Math. Soc.) VIII, 1—15 (1965).
13. Shimura, G.: Sur les intégrales attachées aux formes automorphes. J. Math. Soc. Japan **11**, 291—311 (1959).
14. Weil, A.: On some exponential sums. Proc. Acad. Sci. USA. **34**, 204—207 (1948).
15. — Über die Bestimmung Dirichletscher Reihen durch Funktionalgleichungen. Math. Ann. **168**, 149—156 (1967).
16. Wohlfahrt, K.: Über Operatoren Heckescher Art bei Modulformen reeller Dimension. Math. Nachr. **16**, 233—256 (1957).

Dr. A. O. L. Atkin
The Atlas Computer Laboratory
Chilton, Didcot, Berkshire, England

Prof. J. Lehner
Dept. of Mathematics
The University of Maryland
College Park, Maryland 20742, USA
and The National Bureau of Standards
Washington, D.C. 20234, USA

(Received March 27, 1969)