TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 217, 1976

GENERALIZED KLOOSTERMAN SUMS AND THE FOURIER COEFFICIENTS OF CUSP FORMS[1]

BY

L. ALAYNE PARSON

ABSTRACT. Certain generalized Kloosterman sums connected with congruence subgroups of the modular group and suitably restricted multiplier systems of half-integral degree are studied. Then a Fourier coefficient estimate is obtained for cusp forms of half-integral degree on congruence subgroups of the modular group and the Hecke groups $G(\sqrt{2})$ and $G(\sqrt{3})$.

1

1.1. *Generalized Kloosterman sums.* In [18] H. Petersson studied certain generalized Kloosterman sums connected with congruence characters on congruence subgroups of the modular group. In [8] M. I. Knopp and J. R. Smart examined the same sums except now connected with multiplier systems of half-integral degree on the full modular group. In this section we extend the results of H. Petersson, M. I. Knopp, and J. R. Smart to Kloosterman sums $W(c, n, \mu, v, \Gamma)$ connected with suitably restricted multiplier systems of half-integral degree on congruence subgroups of the modular group and obtain

$$W(c, n, \mu, v, \Gamma) = O(c^{1/2+\epsilon}) \tag{1.1}$$

for each $\epsilon > 0$ where the constant involved is independent of μ.

Let $\Gamma(1)$ denote the homogeneous modular group, that is, the group of all 2×2 matrices with rational integer entries and determinant one. For a positive integer N, the principal congruence subgroup of level N is defined by

$$\Gamma(N) = \{M \in \Gamma(1)\colon M \equiv \pm I \pmod N\}$$

where the congruence is elementwise. $\Gamma(N)$ is normal and of finite index in $\Gamma(1)$. A subgroup Γ of $\Gamma(1)$ is called a congruence subgroup of level N if $\Gamma(N) \subset \Gamma$ and N is minimal with respect to this property.

Let Γ be a subgroup of finite index with $-I \in \Gamma$. A mapping v from Γ into

Received by the editors December 13, 1974.

AMS (MOS) subject classifications (1970). Primary 10D05, 10D15, 10G05; Secondary 20H05.

Key words and phrases. Kloosterman sums, Hecke groups, cusp forms.

[1] This research is part of the author's doctoral dissertation, completed at the University of Illinois, Chicago, under the direction of Professor Marvin I. Knopp, whose help and encouragement are gratefully acknowledged.

the complex numbers of absolute value one which satisfies $v(-I) = (-1)^r$ and the "consistency condition" (1.2) is called a multiplier system for Γ of degree $-r$, r a real number.

$$v(M_1M_2)(c_3z + d_3)^r = v(M_1)v(M_2)(c_1M_2z + d_1)^r(c_2z + d_2)^r \tag{1.2}$$

for z in the upper half plane H, M_1, $M_2 \in \Gamma$ with

$$M_i = \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix}, \quad i = 1, 2, \quad \text{and} \quad M_1M_2 = \begin{pmatrix} * & * \\ c_3 & d_3 \end{pmatrix}.$$

Here $M_2z = (a_2z + b_2)/(c_2z + d_2)$. In order to fix the branch of $(cz + d)^r$ for r nonintegral, for any complex number τ and real s we set $\tau^s = |\tau|^s \exp(is \arg \tau)$ with $-\pi \leqslant \arg \tau < \pi$. When r is an integer, (1.2) reduces to $v(M_1M_2) = v(M_1)v(M_2)$; and v is a character on Γ.

Set $S = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. For Γ of finite index, there exists a smallest positive integer λ such that $S^\lambda = \left(\begin{smallmatrix} 1 & \lambda \\ 0 & 1 \end{smallmatrix}\right)$ is in Γ. Given a multiplier system v on Γ, κ is defined by $v(S^\lambda) = e(\kappa), 0 \leqslant \kappa < 1$, where we are using the notation $e(z) = e^{2\pi iz}$. Also, from (1.2) we have

$$v(S^\lambda M) = v(S^\lambda)v(M) \quad \text{and} \quad v(MS^\lambda) = v(M)v(S^\lambda) \tag{1.3}$$

for any $M \in \Gamma$.

Now let v be a multiplier system of half-integral degree $-r = -s/2$, s an integer. Set $u = 4(-r/2 - [\![-r/2]\!])$ where $[\![x]\!]$ is the greatest integer less than or equal to x. Then $u = 0, 1, 2,$ or 3 according as $-s \equiv 0, 1, 2,$ or $3 \pmod 4$. Let v_2 denote the multiplier system for $\eta^{-1}(z)$, a modular form of degree ½. Then, for any $M \in \Gamma$, we may write

$$v(M) = v_1(M)v_2^u(M) \tag{1.4}$$

where v_1 is a character on Γ of degree $2[\![-r/2]\!]$. If κ_1 and κ_2 are given by $v_i(S^\lambda) = e(\kappa_i)$, $0 \leqslant \kappa_i < 1$, $i = 1, 2$, we have $\kappa \equiv \kappa_1 + u\kappa_2 \pmod 1$. Since it is well known that $e(\kappa_2) = e(-\lambda/24)$,

$$24\kappa \equiv 24\kappa_1 \pmod 1. \tag{1.5}$$

We come now to the definition of the generalized Kloosterman sums $W(c, n, \mu, v, \Gamma)$. Let v be any multiplier system for Γ. Let c be a positive integer such that $\left(\begin{smallmatrix} * & * \\ c & * \end{smallmatrix}\right) \in \Gamma$ and $D(c) = \{d\colon \left(\begin{smallmatrix} * & * \\ c & d \end{smallmatrix}\right) \in \Gamma \text{ and } 0 < d \leqslant c\lambda\}$. For any integers μ and n and any $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ with lower row (c, d),

$$W(c, n, \mu, v, \Gamma) = \sum_{d \in D(c)} \bar{v}(M)e\left(\frac{1}{c\lambda}[(n + \kappa)a + (\mu + \kappa)d]\right). \tag{1.6}$$

When $\Gamma = \Gamma(N)$ and $v = 1$, (1.6) becomes the original sum introduced by H. D. Kloosterman in [5]. Let

$$g(a, b, c, d) = \bar{v}(M)e\left(\frac{1}{c\lambda}[(n + \kappa)a + (\mu + \kappa)d]\right).$$

It follows easily from (1.3) that

$$g(a + c\lambda, b + d\lambda, c, d) = g(a, b, c, d), \tag{1.7}$$

and

$$g(a, a\lambda + b, c, c\lambda + d) = g(a, b, c, d). \tag{1.8}$$

(1.7) implies that $W(c, n, \mu, v, \Gamma)$ does not depend on the specific choice of a and b for M in Γ with lower row (c, d).

For later use we record here an estimate on certain related sums which were studied by Malyshev [11]. Let

$$K_r(u, v; l, L; q) = \sum_{x \ (\mathrm{mod}\ q); x \equiv l \ (\mathrm{mod}\ L); (x,q)=1} \left(\frac{x}{r}\right) e\left(\frac{ux + vx'}{q}\right)$$

where u, v, and l are integers; q is a positive integer; r is an odd positive integer dividing q; L is a positive integer dividing q; and x' is any integer for which $xx' = 1 \pmod{q}$. Also, (x/r) is the Jacobi symbol. Then

$$|K_r(u, v; l, L; q)| < A(\epsilon)q^{1/2+\epsilon} \min\{\sqrt{(u, q)}, \sqrt{(v, q)}\} \tag{1.9}$$

for each $\epsilon > 0$ where $A(\epsilon)$ is a constant depending only on ϵ.

1.2. *Congruence characters.* To obtain a nontrivial estimate for $W(c, n, \mu, v, \Gamma)$ we take Γ to be a congruence subgroup and v a multiplier system of half-integral degree. In addition, given the decomposition of v in (1.4), we assume that v_1 is a congruence character, that is, that the kernel of v_1 is a congruence subgroup. It is well known that there are only twelve characters on $\Gamma(1)$. The six with $v(-I) = 1$ are identically one on $\Gamma(6)$ and are thus congruence characters. The question of the existence of congruence characters on proper congruence subgroups is examined in

THEOREM 1.1. *All congruence characters on a congruence subgroup Γ of level N, $N > 1$, are identically one on $\Gamma(R)$ where*

$$R = \begin{cases} 12N^2/(N, 12) & \textit{if } N \textit{ is odd,} \\ 24N^2/(N, 12) & \textit{if } N \textit{ is even.} \end{cases} \tag{1.10}$$

Therefore, the number of congruence characters on Γ is $l = |\Gamma/\Gamma(R)/(\Gamma/\Gamma(R))'|$ where $(\Gamma/\Gamma(R))'$ denotes the commutator subgroup of $\Gamma/\Gamma(R)$; and for each of these characters v, $v^l \equiv 1$.

PROOF. Let v be a congruence character with kernel K. Then since $\Gamma' \subset K \subset \Gamma$, in R. A. Rankin's terminology, K is a lattice congruence subgroup of Γ. A. W. Mason [13] has shown that the level of K divides R where R is given by (1.10) so that $K \supset \Gamma(R)$. Since v was arbitrary, all congruence characters are identically one on $\Gamma(R)$. It is now clear that the group of congruence characters is isomorphic to the group of characters of $\Gamma/\Gamma(R)$; and since the number of characters on $\Gamma/\Gamma(R)$ is l, the proof is complete.

REMARKS. 1. Using the results of M. Newman and J. R. Smart [15], [16] on modulary groups and McQuillan's classification [14] of normal congruence subgroups, it is possible to calculate the number of characters on $\Gamma(N)$ which are 1 on $\Gamma(kN)$, k a positive integer. It then follows that $\Gamma(R)$ is the largest principal congruence subgroup on which all congruence characters of $\Gamma(N)$ are 1 and that the number of such characters is $12N^3/(N, 12)$ if N is odd, $48N^3/(N, 12)$ if $N = 2$ or $N \equiv 0 \pmod 4$, and $96N^3/(N, 12)$ if $N \equiv 2 \pmod 4$, $N > 2$.

2. It is also interesting to note that although there are infinitely many characters on $\Gamma(N)$, $N \geqslant 2$, which take values that are roots of unity, only finitely many of these are congruence characters.

1.3. *Reduction of* $W(c, n, \mu, v, \Gamma)$. $W(c, n, \mu, v, \Gamma)$ is now reduced to a finite sum of sums which can be estimated by (1.9). The method of reduction is due to H. Petersson [18] who used it while studying $W(c, n, \mu, v, \Gamma)$ when v was a congruence character.

Let Γ be of level N. Then, since $S^N \in \Gamma$, there exists a positive integer h such that $N = h\lambda$. Also, since v_1 is a congruence character, $v_1 \equiv 1$ on $\Gamma(12N^2)$. Therefore, $1 = v_1(S^{12N^2}) = v_1(S^\lambda)^{12Nh} = e(12Nh\kappa_1)$; and $12Nh\kappa_1$ is an integer. It now follows from (1.5) that $24Nh\kappa$ is an integer. From (1.8) we have

$$(1.11) \qquad 24NhW(c, n, \mu, v, \Gamma) = \sum_{d \in D(24Nhc)} \bar{v}(M) e\left(\frac{ma + wd}{24cN^2}\right)$$

where $m = 24Nhn + 24Nh\kappa$ and $w = 24Nh\mu + 24Nh\kappa$ are integers.

We next note that Γ has the coset decomposition

$$(1.12) \qquad \Gamma = \sum_{s=1}^{l/24Nh} \sum_{t=1}^{24Nh} S^{\lambda t} K_s \bar{\Gamma}(24N^2)$$

where $\bar{\Gamma}(24N^2) = \{M \in \Gamma(1) : M \equiv I \pmod{24N^2}\}$, $l = |\Gamma : \bar{\Gamma}(24N^2)|$, and the K_s, $s = 1, \ldots, l/24Nh$, are elements of Γ which have distinct lower rows modulo $24N^2$. Set

$$K_s = \begin{pmatrix} \alpha_s & \beta_s \\ \gamma_s & \delta_s \end{pmatrix}.$$

It then follows from (1.12) that the pair (c, d) is a lower row for an element in

Γ if and only if $(c, d) = 1$ and $c \equiv \gamma_s$, $d \equiv \delta_s \pmod{24N^2}$ for some s. This fact together with (1.7) and (1.12) allows us to rewrite (1.11) as

$$24NhW(c, n, \mu, v, \Gamma) = \sum_{s=1}^{l/24Nh}{}' \sum_{d=1}^{24cN^2}{}^* \bar{v}(M) e\left(\frac{ma + wd}{24cN^2}\right)$$

where the prime on the outer sum indicates that we are summing over only those s for which $\gamma_s \equiv c \pmod{24N^2}$ and the inner sum is restricted by the conditions $M \equiv K_s \pmod{24N^2}$, $(c, d) = 1$, and $d \equiv \delta_s \pmod{24N^2}$. For notational convenience set

$$p = \begin{cases} 0 & \text{if } u \text{ is even,} \\ 1 & \text{if } u \text{ is odd.} \end{cases}$$

By (1.4) v may be written as $v = v_1 v_2^{u-p} v_2^p$. Since v_2^{u-p} is a character of $\Gamma(1)$ and since $\Gamma(1)' \supset \bar{\Gamma}(12)$ [9], $v_1 v_2^{u-p} \equiv 1$ on $\bar{\Gamma}(24N^2)$. We then have

$$\begin{aligned} 24NhW &= \sum_{s=1}^{l/24Nh}{}' \bar{v}_1(K_s) \bar{v}_2^{u-p}(K_s) \sum_{d=1}^{24cN^2}{}^* \bar{v}_2^p(M) e\left(\frac{ma + wd}{24cN^2}\right) \\ &= \sum_{s=1}^{l/24Nh}{}' \bar{v}_1(K_s) \bar{v}_2^{u-p} W(K_s). \end{aligned} \tag{1.13}$$

We next note that if

$$K_s' = S^t K_s S^r = \begin{pmatrix} \alpha_s' & \beta_s' \\ \gamma_s & \delta_s' \end{pmatrix}$$

where t and r are integers and $\beta_s' = \beta_s + t\delta_s + r(\alpha_s + t\gamma_s)$, then by (1.3)

$$W(K_s') = \bar{v}_2^p(S^t) \bar{v}_2^p(S^r) e\left(\frac{mt + wr}{24cN^2}\right) W(K_s). \tag{1.14}$$

The summation conditions on $W(K_s')$ are equivalent to $(c, d) = 1$, $\alpha \equiv \alpha_s'$, $d \equiv \delta_s' \pmod{24N^2}$, and $ad \equiv 1 + \beta_s' c \pmod{24cN^2}$. Since $(\alpha_s, \gamma_s) = 1$, we may choose integers t_s and r_s so that $r_s(\alpha_s + t_s\gamma_s) \equiv -\beta_s - t_s\gamma_s \pmod{24N^2}$, that is, so that $\beta_s' \equiv 0 \pmod{24N^2}$. For this choice of t and r the summation conditions on $W(K_s')$ become $(d, 24cN^2) = 1$, $d \equiv \delta_s' \pmod{24N^2}$, and $ad \equiv 1 \pmod{24cN^2}$. Setting

$$e(q_s) = \bar{v}_1(K_s) \bar{v}_2^{u-p}(K_s) v_2^p(S^{t_s}) v_2^p(S^{r_s}) e\left(\frac{-mt_s - wr_s}{24cN^2}\right),$$

we find from (1.13) and (1.14) that

$$24NhW = \sum_{s=1}^{l/24Nh}{}' e(q_s) W(K_s') \tag{1.15}$$

where

$$W(K_s') = \sum_{d=1}^{24cN^2} \bar{v}_2^p(M) e\left(\frac{ma + wd}{24cN^2}\right) \tag{1.16}$$

with the summation conditions $(d, 24cN^2) = 1, ad \equiv 1 \pmod{24cN^2}$, and $d \equiv \delta_s' \pmod{24N^2}$.

1.4. *Proof of* (1.1).

THEOREM 1.2. *Let Γ be a congruence subgroup of level N with multiplier system $v = v_1 v_2^u$, $u = 4(-r/2 - [\![-r/2]\!])$, of half-integral degree $-r$. If v_1 is a congruence character, then*

$$W(c, n, \mu, v, \Gamma) = O(c^{1/2+\epsilon}) \tag{1.1}$$

for each $\epsilon > 0$ where the constant involved is independent of μ.

PROOF. When u is even, $p = 0$ and $W(K_s')$ is a classical Kloosterman sum which carries the famous estimate of H. Salié [22] and A. Weil [27].

$$W(K_s') = O((24cN^2)^{1/2+\epsilon} \min\{\sqrt{(m, 24cN^2)}, \sqrt{(w, 24cN^2)}\}) = O(c^{1/2+\epsilon}).$$

For a recent elementary proof of this estimate see S. A. Stepanov [26]. Since the constant here depends on Γ, ϵ, and $m = 24Nh(n + \kappa)$, (1.1) follows from (1.15).

When u is odd, $p = 1$; and we make use of the following explicit expression for v_2 (see, for instance, [7, p. 51]). For $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1)$, $c, d > 0$,

$$\bar{v}_2(M) = \begin{cases} \left(\dfrac{d}{c}\right) e\left(\dfrac{1}{24}[(a + d)c - bd(c^2 - 1) - 3c]\right) & \text{if } c \text{ is odd,} \\ \left(\dfrac{c}{d}\right) e\left(\dfrac{1}{24}[(a + d)c - bd(c^2 - 1) + 3(d - 1) - 3cd]\right) & \\ & \text{if } c \text{ is even.} \end{cases} \tag{1.17}$$

If c is odd, substituting (1.17) into (1.16) gives

$$W(K_s') = e(-c/8) K_c(w + c^2N^2, m + c^2N^2; \delta_s', 24N^2; 24cN^2)$$

in A. V. Malyshev's notation. By (1.9) we conclude that

$$\begin{aligned} W(K_s') &= O((24cN^2)^{1/2+\epsilon} \min\{(w + c^2N^2, 24cN^2)^{1/2}, (m + c^2N^2, 24cN^2)^{1/2}\}) \\ &= O(c^{1/2+\epsilon}) \end{aligned}$$

where, as before, the constant is independent of μ.

If c is even, substituting (1.17) into (1.16) gives

$$W(K_s') = e(-1/8) \sum_{d=1}^{24cN^2} \left(\frac{c}{d}\right) e\left(\frac{1}{24cN^2}[(m + c^2N^2)a + (w + 3cN^2 - 2c^2N^2)d]\right)$$

with the summation conditions $(d, 24cN^2) = 1, ad \equiv 1 \pmod{24cN^2}, d \equiv \delta'_s \pmod{24N^2}$. Now write $c = 2^t c_1, (c_1, 2) = 1, t \geqslant 1$. By quadratic reciprocity

$$(c/d) = (-1)^{(d^2-1)t/8}(-1)^{(c_1-1)(d-1)/4}(d/c_1).$$

Since $d \equiv \delta'_s \pmod 8$ and $(\delta'_s, 8) = 1$, we have

$$W(K'_s) = E(s, c)K_{c_1}(w + 6cN^2 - 2c^2N^2 - 3cc_1N^2, m + c^2N^2; \\ \delta'_s, 24N^2; 24cN^2)$$

where

$$E(s, c) = \begin{cases} e((c_1 - 2)/8) & \text{if } \delta'_s \equiv \pm 1 \pmod 8, \\ e((c_1 - 2 - 4t)/8) & \text{if } \delta'_s \equiv \pm 3 \pmod 8. \end{cases}$$

By (1.9) $W(K'_s) = O(c^{1/2+\epsilon})$ where, as usual, the constant is independent of μ. For u odd, the estimate on W now follows from (1.15); and the proof of the theorem is complete.

REMARKS. By Theorem 1.1 only finitely many multiplier systems of a fixed degree $-r$ satisfy the conditions of Theorem 1.2. As special cases of Theorem 1.2 we have the estimates of M. I. Knopp, J. R. Smart, and H. Petersson.

1.5. *Cusp form Fourier coefficient estimate.* Since $W(c, n, \mu, v, \Gamma)$ does arise naturally in the theory of modular forms, we conclude this section with an application of Theorem 1.2 to the estimation of the Fourier coefficients of modular cusp forms. For Γ of finite index in $\Gamma(1)$, a function F, regular in H, satisfying

$$F(Mz) = v(M)(cz + d)^r F(z) \tag{1.18}$$

for all $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$, where v is a multiplier system of real degree $-r$, is called a cusp form if $y^{r/2}|F(x + yi)|$ is bounded in H. It then follows that F has a Fourier expansion of the form

$$F(z) = \sum_{n+\kappa>0} a_n e\left(\frac{(n+\kappa)z}{\lambda}\right), \quad \operatorname{Im} z > 0. \tag{1.19}$$

It is the coefficients a_n which are estimated in

THEOREM 1.3. *Let F be a cusp form with Fourier expansion* (1.19) *on a congruence subgroup Γ with multiplier system v of half-integral degree $-r$, $r \geqslant 5/2$. As usual, write $v = v_1 v_2^u$, $u = 4(-r/2 - [\![-r/2]\!])$. Then, if v_1 is a congruence character,*

$$a_n = O(n^{r/2-1/4+\epsilon}) \quad \text{as } n \longrightarrow \infty,$$

for any $\epsilon > 0$.

Proof. It is well known that, since $r > 2$, F can be expressed as a finite linear combination of Poincaré series $G_m(z, -r, v, \Gamma)$, m an integer, $m + \kappa > 0$. The nth Fourier coefficient of $G_m(z, -r, v, \Gamma)$ is [10, p. 298]

$$c_n = 2\delta_{m,n} + \frac{4\pi i^{-r}}{\lambda}\left(\frac{n+\kappa}{m+\kappa}\right)^{(r-1)/2} \sum_{c>0}{}' c^{-1} W(c, m, n, v, \Gamma) \cdot J_{r-1}\left(\frac{4\pi\sqrt{(m+\kappa)(n+\kappa)}}{c\lambda}\right)$$

where $J_{r-1}(x)$ is a Bessel function and $\Sigma'_{c>0}$ indicates that the sum is over all positive c such that $\begin{pmatrix} * & * \\ c & * \end{pmatrix} \in \Gamma$. From Theorem 1.2 we have $|W(c, m, n, v, \Gamma)| < A_1 c^{1/2+\epsilon}$ where A_1 is a constant independent of n. For $J_{r-1}(x)$, $x > 0$, we have [17] $J_{r-1}(x) < A_2 \min\{x^{r-1}, x^{-1/2}\}$ where A_2 is a constant depending only on r. Together these estimates give $c_n = O(n^{r/2-1/4+\epsilon})$; and the theorem is proved.

Remark. For an excellent summary of other methods of obtaining Fourier coefficient estimates for modular cusp forms, known results, and conjectures, see A. Selberg [24].

2

2.1. *The Hecke groups* $G(\sqrt{2})$ *and* $G(\sqrt{3})$. In [3] E. Hecke introduced an infinite class of discrete groups $\hat{G}(\lambda_q)$ of linear fractional transformations preserving $\mathcal{H}$. $\hat{G}(\lambda_q)$ is the group generated by $S^{\lambda_q} z = z + \lambda_q$ and $Tz = -1/z$ where $\lambda_q = 2\cos(\pi/q)$, q an integer, $q \geqslant 3$. When $q = 3$, we have the modular group. When $q = 4$ or 6, the resulting groups are $\hat{G}(\sqrt{2})$ and $\hat{G}(\sqrt{3})$. These two groups are of particular interest since they are the only Hecke groups, aside from the modular group, whose elements are completely known. For this reason, many of the classical results on the modular group have been generalized to $\hat{G}(\sqrt{2})$ and $\hat{G}(\sqrt{3})$. (See, for instance, J. R. Smart [25] and J. Raleigh [20].) In §3 we shall extend the circle method for estimating the Fourier coefficients of modular cusp forms to the groups $\hat{G}(\sqrt{2})$ and $\hat{G}(\sqrt{3})$.

For notational convenience, let m stand for 2 or 3. To each linear fractional transformation $z' = (\alpha z + \beta)/(\gamma z + \delta)$ in $\hat{G}(\sqrt{m})$ we associate the two matrices $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ and $\begin{pmatrix} -\alpha & -\beta \\ -\gamma & -\delta \end{pmatrix}$ and denote the resulting matrix group by $G(\sqrt{m})$. We then have that $G(\sqrt{m})$ is generated by $S^{\sqrt{m}} = \begin{pmatrix} 1 & \sqrt{m} \\ 0 & 1 \end{pmatrix}$ and $T = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. In addition, it is known [4], [28] that $G(\sqrt{m})$ consists of the set of all elements of the following two types:

(i) $\begin{pmatrix} a & b\sqrt{m} \\ c\sqrt{m} & d \end{pmatrix}$, $a, b, c, d \in Z$, $ad - mbc = 1$, and

(ii) $\begin{pmatrix} a\sqrt{m} & c \\ b & d\sqrt{m} \end{pmatrix}$, $a, b, c, d \in Z$, $mad - bc = 1$.

Those of type (i) are called even whereas those of type (ii) are called odd. Since

$G(\sqrt{m})$ is a subgroup of $SL(2, Z[\sqrt{m}])$, it is natural to define its principal congruence subgroups by

$$\Gamma_m(N + R\sqrt{m}) = \{M \in G(\sqrt{m}): M \equiv \pm I \pmod{N + R\sqrt{m}}\}$$

where $N + R\sqrt{m}$ is a nonzero element of $Z[\sqrt{m}]$ and the congruence is elementwise. It is clear that $\Gamma_m(N + R\sqrt{m})$ is normal in $G(\sqrt{m})$ and of finite index.

THEOREM 2.1. *Let* $M = \begin{pmatrix} a & b\sqrt{m} \\ c\sqrt{m} & d \end{pmatrix}$ *be in* $G(\sqrt{m})$. *Then* $M \in \Gamma_m(N + R\sqrt{m})$ *if and only if*

$$a \equiv d \equiv \pm 1 \pmod{|N^2 - R^2m|/(N, R)},$$
$$b \equiv c \equiv 0 \pmod{|N^2 - R^2m|/(N, Rm)}.$$

PROOF. The result is immediate once we note that the smallest positive integer in the ideal generated by $N + R\sqrt{m}$ in $Z[\sqrt{m}]$ is $|N^2 - R^2m|/(N, R)$ and that if ρ is the smallest positive integer such that $\rho\sqrt{m}$ is in the ideal generated by $N + R\sqrt{m}$, then $\rho = |N^2 - R^2m|/(N, Rm)$.

This simple theorem has a remarkable number of corollaries which are collected in

COROLLARY 2.1. (i) *The group of even elements in* $G(\sqrt{m})$ *is* $\Gamma_m(\sqrt{m})$.

(ii) *If* $N + R\sqrt{m}$ *is a nonunit with* $(N, Rm) = 1$, *then the group of even elements in* $\Gamma_m(N + R\sqrt{m})$ *is* $\Gamma_m(|N^2 - R^2m|)$.

(iii) *If* $N + R\sqrt{m}$ *is such that* $(N, Rm) > 1$, *then* $\Gamma_m(N + R\sqrt{m})$ *contains only even elements and*

$$\Gamma_m(N + R\sqrt{m}) = \begin{cases} \Gamma_m\left(\dfrac{|N^2 - R^2m|}{(N, R)}\right) & \textit{when } (N, Rm) = (N, R), \\ \Gamma_m\left(\dfrac{|N^2 - R^2m|}{m(N, R)}\sqrt{m}\right) & \textit{when } (N, Rm) = m(N, R). \end{cases}$$

REMARKS. It is clear from Corollary 2.1 that the principal congruence subgroups reduce to three basic types; $\Gamma_m(N)$, $\Gamma_m(R\sqrt{m})$, where N and R are positive integers, and $\Gamma_m(N + R\sqrt{m})$ where $(N, Rm) = 1$. Since both $\Gamma_m(N)$, $N > 1$, and $\Gamma_m(R\sqrt{m})$ contain only even elements, Theorem 2.1 gives an alternate definition of these groups.

THEOREM 2.2. *Let* $M = \begin{pmatrix} a\sqrt{m} & b \\ c & d\sqrt{m} \end{pmatrix}$ *be in* $G(\sqrt{m})$. *Then* $M \in \Gamma_m(N + R\sqrt{m})$ *where* $(N, Rm) = 1$ *if and only if*

$$(2.1) \qquad b \equiv c \equiv 0 \quad \textit{and} \quad a \equiv d \equiv \pm d_0 \pmod{|N^2 - R^2m|}$$

where $d_0 = v_0N + u_0R$ *and* (u_0, v_0) *is a fixed solution to* $uN + vmR = -1$.

PROOF. If $M \in \Gamma_m(N + R\sqrt{m})$, it is clear that b and c are multiples of $|N^2 - R^2 m|$. In addition, there exist integers u and v such that $d\sqrt{m} \mp 1 = (u + v\sqrt{m})(N + R\sqrt{m})$ or $d = uR + vN$ and $\mp 1 = uN + vmR$. Since all solutions (u, v) of $uN + vmR = -1$ are of the form $u = u_0 - tmR$ and $v = v_0 + tN$ where t is an integer, $d \equiv \pm d_0 \pmod{|N^2 - R^2 m|}$; Similarly,

$$a \equiv d \equiv \pm d_0 \pmod{|N^2 - R^2 m|};$$

and (2.1) is verified.

Now let M be an odd element of $G(\sqrt{m})$ satisfying (2.1). Without loss of generality, we may assume that $a \equiv d \equiv d_0 \pmod{|N^2 - R^2 m|}$. It is clear that $b \equiv c \equiv 0 \pmod{N + R\sqrt{m}}$. Also, there exists an integer t such that $d = d_0 + t(N^2 - R^2 m) = (v_0 + tN)N + (u_0 - tmR)R$. If we set $v = v_0 + tN$ and $u = u_0 - tmR$, then $uN + vmR = -1$ and $d\sqrt{m} - 1 = (u + v\sqrt{m})(N + R\sqrt{m})$. The same argument then shows that $a\sqrt{m} \equiv 1 \pmod{N + R\sqrt{m}}$ so that $M \equiv I \pmod{N + R\sqrt{m}}$; and $M \in \Gamma_m(N + R\sqrt{m})$.

REMARKS. 1. $\Gamma_m(N + R\sqrt{m})$, $(N, Rm) = 1$, does contain odd elements. Since $md_0^2 = 1 + (v_0^2 m - u_0^2)(N^2 - R^2 m)$, if we set $t = v_0^2 m - u_0^2$, then

$$\begin{pmatrix} d_0\sqrt{m} - td_0(N^2 - R^2 m)\sqrt{m} & t - tmd_0^2 \\ N^2 - R^2 m & d_0\sqrt{m} \end{pmatrix}$$

belongs to $\Gamma_m(N + R\sqrt{m})$.

2. From Theorems 2.1 and 2.2 we have that $\Gamma_2(R\sqrt{2}) = \Gamma_2(R)$ whenever R is odd, $\Gamma_m(2\sqrt{m}) = \Gamma_m(2)$, and $\Gamma_m(N + R\sqrt{m}) = \Gamma_m(N' + R'\sqrt{m})$ whenever $(N, Rm) = (N', R'm) = 1$ and $|N^2 - R^2 m| = |N'^2 - R'^2 m|$.

2.2. *The index of the principal congruence subgroups.*

THEOREM 2.3. $|G(\sqrt{m}) : \Gamma_m(2)| = 4m$. *For* $N > 2$,

$$|G(\sqrt{m}) : \Gamma_m(N)| = \begin{cases} N^3 \prod\limits_{p|N} \left(1 - \dfrac{1}{p^2}\right) & \textit{if } (N, m) = 1, \\ \left(1 - \dfrac{1}{m}\right) N^3 \prod\limits_{p|N; p \neq m} \left(1 - \dfrac{1}{p^2}\right) & \textit{if } (N, m) = m. \end{cases}$$

PROOF. For convenience we introduce the group

$$\bar{\Gamma}_m(N) = \{M \in G(\sqrt{m}) \colon M \equiv I \pmod{N}\}.$$

Since $\bar{\Gamma}_m(2) = \Gamma_m(2)$ and $|\Gamma_m^{\cdot}(N) : \bar{\Gamma}_m(N)| = 2$ when $N > 2$, it suffices to determine $|G(\sqrt{m}) : \bar{\Gamma}_m(N)|$. Our calculation of the index of $\bar{\Gamma}_m(N)$ is a modification of the method usually used in calculating the index of $\bar{\Gamma}(N)$ in the modular group (see, for instance, R. C. Gunning [2, p. 8]).

We begin by considering $\Gamma_m(\sqrt{m})$. Let ψ be the natural homomorphism from Z to Z_N, the integers mod N. Then ψ induces a homomorphism from $\Gamma_m(\sqrt{m})$ onto

$$H = \left\{ \begin{pmatrix} a & b\sqrt{m} \\ c\sqrt{m} & d \end{pmatrix} : ad - mbc \equiv 1 \pmod{N}, a, b, c, d \in Z_N \right\}$$

such that $\Gamma_m(\sqrt{m})/\bar{\Gamma}_m(N) \cong H$. To see that ψ actually maps onto H, let $M = \left(\begin{smallmatrix} a & b\sqrt{m} \\ c\sqrt{m} & d \end{smallmatrix}\right)$ be in H. Since $ad - mbc \equiv 1 \pmod{N}$, there exists an integer k such that $ad - mbc - kN = 1$. In particular, $(mc, d, N) = 1$. Thus there exists an integer n such that $(mc, d + nN) = 1$; and we may assume that $(mc, d) = 1$. Now consider the matrix $\left(\begin{smallmatrix} a+eN & (b+fN)\sqrt{m} \\ c\sqrt{m} & d \end{smallmatrix}\right)$ where e and f are integers yet to be determined. This matrix has determinant $1 + N(de - mcf + k)$. Since $(mc, d) = 1$, we may choose e and f so that $mcf - de = k$. Then, for this choice of e and f, we have an element of $\Gamma_m(\sqrt{m})$ which is mapped to M under ψ.

Since we now have $|G(\sqrt{m}) : \bar{\Gamma}_m(N)| = 2|H|$, it remains to calculate the order of H. We note that a pair (c, d) of integers mod N determines a lower row of an element in H if and only if $(mc, d, N) = 1$. It is then elementary to show that for each such fixed pair (c, d) there are N incongruent pairs (a, b) of integers mod N such that $ad - mbc \equiv 1 \pmod{N}$. In other words, to each lower row in H there correspond N distinct elements. Therefore, $|H| = N \cdot \lambda(N)$ where $\lambda(N)$ is defined to be the number of incongruent pairs (c, d) of integers mod N with $(mc, d, N) = 1$.

Since it is easily verified that $\lambda(N)$ is multiplicative, that is, that $\lambda(N_1N_2) = \lambda(N_1)\lambda(N_2)$ for $(N_1, N_2) = 1$, it now suffices to find $\lambda(p^k)$, p prime. For $p \neq m$, there are $\varphi(p^k) = p^k(1 - 1/p)$ integers c mod p^k with $(mc, p) = 1$. For each of these, there are p^k choices for d mod p^k such that $(mc, d, p^k) = 1$. This gives $p^{2k}(1 - 1/p)$ incongruent pairs. Also for $p \neq m$, there are p^{k-1} values for c mod p^k with $(mc, p) = p$. To each of these there correspond $\varphi(p^k) = p^k(1 - 1/p)$ choices for d mod p^k such that $(mc, d, p^k) = 1$. This gives $p^{2k-1}(1 - 1/p)$ additional incongruent pairs. Therefore, for $p \neq m$, $\lambda(p^k) = p^{2k}(1 - 1/p^2)$. Similarly, $\lambda(m^k) = m^{2k}(1 - 1/m)$; and, finally,

$$|H| = \begin{cases} N^3 \prod\limits_{p/N} \left(1 - \dfrac{1}{p^2}\right) & \text{if } (N, m) = 1, \\ \left(1 - \dfrac{1}{m}\right) N^3 \prod\limits_{p/N; p \neq m} \left(1 - \dfrac{1}{p^2}\right) & \text{if } (N, m) = m. \end{cases}$$

The proof of the theorem is now complete.

The index of the other piincipal congruence subgroups is easily derived from Theorem 2.3.

THEOREM 2.4. *If $N + R\sqrt{m}$ is a nonunit, $(N, Rm) = 1$, then*

$$(2.2)\qquad |G(\sqrt{m}:\Gamma_m(N+R\sqrt{m})| = \begin{cases} 6 \quad \textit{when } |N^2-3R^2| = 2, \\ \tfrac{1}{2}|N^2-R^2m|^3 \displaystyle\prod_{p\,/\,|N^2-R^2m|}\left(1-\frac{1}{p^2}\right) \\ \qquad\qquad\qquad\qquad\qquad\qquad \textit{otherwise.} \end{cases}$$

If $R > 1$,

$$(2.3)\qquad |G(\sqrt{m}):\Gamma_m(R\sqrt{m})| = (m-1)R^3 \prod_{p\,/\,R\,;\,p\neq m}\left(1-\frac{1}{p^2}\right).$$

Proof. Since $|\Gamma_m(N+R\sqrt{m}):\Gamma_m(|N^2-R^2m|)| = 2$, (2.2) follows immediately from Theorem 2.3. Also, since $\Gamma_m(2\sqrt{m}) = \Gamma_m(2)$, (2.3) needs verifying only when $R > 2$; and, by Theorem 2.3, it suffices to prove that

$$(2.4)\qquad |\Gamma_m(R):\Gamma_m(R\sqrt{m})| = \begin{cases} m-1 & \text{if } (R, m) = 1, \\ m & \text{if } (R, m) = m. \end{cases}$$

If $m = 2$ and R is odd, (2.4) is immediate since $\Gamma_2(R) = \Gamma_2(R\sqrt{2})$. If $m = 2$ and R is even, $R > 2$,

$$V = \begin{pmatrix} R^2-R+1 & R^2\sqrt{2}/2 \\ R\sqrt{2} & R+1 \end{pmatrix}$$

is in $\Gamma_2(R)$ but not in $\Gamma_2(R\sqrt{2})$; and we claim that

$$\Gamma_2(R) = \Gamma_2(R\sqrt{2}) \cup \Gamma_2(R\sqrt{2}) \cdot V.$$

Since the two cosets are disjoint, we need only show that $M = \begin{pmatrix} a & b\sqrt{2} \\ c\sqrt{2} & d \end{pmatrix}$ in $\Gamma_2(R)$ lies in one of them. Since $1 = ad - 2bc \equiv ad \pmod{2R}$, either $a \equiv d \equiv \pm 1 \pmod{2R}$ or $a \equiv d \equiv R \pm 1 \pmod{2R}$. In the first case, $M \in \Gamma_2(R\sqrt{2})$; and in the second case, $MV^{-1} \in \Gamma_2(R\sqrt{2})$. The verification of (2.4) for $m = 3$ is similar and is thus omitted.

2.3. *Congruence characters.* A multiplier system v of degree $-r$ for a subgroup of $G(\sqrt{m})$ is again a map from the matrix group into the unit circle which satisfies (1.2) and $v(-I) = (-1)^r$. A multiplier system of even integral degree is called a congruence character if its kernel is a congruence subgroup where Γ is a congruence subgroup of level N if N is the smallest positive integer such that $\Gamma \supset \Gamma_m(N)$. M. I. Knopp [6] has determined all characters of even degree on the full group $G(\sqrt{m})$. It is easily verified that all $2m$ of these characters are identically one on $\Gamma_m(2m)$ and are thus congruence characters. For proper congruence subgroups we have the following result.

Theorem 2.5. *If* Γ *is a congruence subgroup of level* N, $N > 1$, *then all congruence characters on* Γ *are identically one on* $\Gamma_m(R)$ *where*

$$R = \begin{cases} 24m^2N^2/(12, mN) & \textit{if } mN \textit{ is even}, \\ 12m^2N^2/(12, mN) & \textit{if } mN \textit{ is odd}, \end{cases}$$

and the number of such characters is $|(\Gamma/\Gamma_m(R))/(\Gamma/\Gamma_m(R))'|$.

PROOF. Let v be a congruence character with kernel K. Set $H = K \cap \Gamma_m(N)$. Since $K \supset \Gamma'$, $\Gamma_m(N)' \subset H \subset \Gamma_m(N)$. Let f be the isomorphism from $\Gamma_m(\sqrt{m})$ onto $\Gamma_0(m) = \{\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma(1)\colon c \equiv 0 \pmod{m}\}$ defined by $f(\left(\begin{smallmatrix} a & b\sqrt{m} \\ c\sqrt{m} & d \end{smallmatrix}\right)) = \left(\begin{smallmatrix} a & b \\ cm & d \end{smallmatrix}\right)$. Then $f(H)$ is a lattice congruence subgroup of $f(\Gamma_m(N))$. Since $f(\Gamma_m(N))$ is of level mN, by A. W. Mason's results [13] the level of $f(H)$ divides R. Therefore, $f(H) \supset \Gamma(R)$ and $K \supset \Gamma_m(R)$. Since v was arbitrary, all congruence characters on Γ are identically one on $\Gamma_m(R)$; and, as in the case of the modular group, the number of such characters is $|(\Gamma/\Gamma_m(R))/(\Gamma/\Gamma_m(R))'|$.

3

3.1. *A cusp form Fourier coefficient estimate using the circle method.* In this final section we improve upon the Fourier coefficient estimate of §1.5 and simultaneously obtain a Fourier coefficient estimate for cusp forms on congruence subgroups of $G(\sqrt{2})$ and $G(\sqrt{3})$. This is accomplished by modifying the classical Kloosterman version of the circle method [5].

From this point on let m stand for 1, 2, or 3 so that the modular group, $G(\sqrt{2})$, and $G(\sqrt{3})$ may be collectively referred to as $G(\sqrt{m})$ with principal congruence subgroups $\Gamma_m(N)$. For r real and Γ of finite index in $G(\sqrt{m})$ with $-I \in \Gamma$, F is in the space of cusp forms $C^0(\Gamma, -r, v)$ if F is analytic in H; satisfies $F(Vz) = v(V)(\gamma z + \delta)^r F(z)$ for all $V = \left(\begin{smallmatrix} * & * \\ \gamma & \delta \end{smallmatrix}\right)$ in Γ and z in H, and has expansions of the form (3.1) at all parabolic points q of Γ. For $\Gamma \subset \Gamma(1)$ it is well known that q is a parabolic point if and only if q is rational (where $\infty = 1/0$ is called rational). The corresponding result for the Hecke groups is that q is a parabolic point for Γ of finite index if and only if $q = a\sqrt{m}/b$ where a and b are integers.

$$F(z) = \sigma_q(z) \sum_{n+\kappa_q>0} a_n(q) e((n + \kappa_q)V_q z/\lambda_q) \tag{3.1}$$

where

$$\sigma_q(z) = \begin{cases} (z-q)^{-r} & \text{if } q < \infty, \\ 1 & \text{if } q = \infty, \end{cases}$$

and V_q is any element of $G(\sqrt{m})$ for which $V_q(q) = \infty$. In particular, we set $V_\infty = I$. λ_q is the smallest positive real number such that $S^{\lambda_q} \in V_q \Gamma V_q^{-1}$; and κ_q is defined by $v(V_q^{-1} S^{\lambda_q} V_q) = e(\kappa_q)$, $0 \leqslant \kappa_q < 1$. As the notation indicates, $a_n(q)$, λ_q, and κ_q are independent of the choice of V_q.

As in §1 we restrict ourselves to multiplier systems v of half-integral degree $-r$ and write $v = v_1 v_2^u$, $u = 4(-r/2 - [\![-r/2]\!])$, with a fixed multipler system v_2 of degree 1/2. For the modular group we again take v_2 to be the multiplier system for $\eta^{-1}(z)$. For the Hecke groups $G(\sqrt{2})$ and $G(\sqrt{3})$ we take v_2 to be the multiplier system for $\eta(z, \sqrt{2})^{1/2}$ and $\eta(z, \sqrt{3})^{1/2}$ respectively. An explicit expression for these multiplier systems is given by J. R. Smart in [25].

3.2. *Preliminary lemmas.* The multiplier system v_2 takes a particularly simple form on certain principal congruence subgroups as seen in

LEMMA 3.1. *Let N be a positive integer such that $N \equiv 0 \pmod{24}$ when m is 1 or 3 and $N \equiv 0 \pmod{16}$ when $m = 2$. Then, for $M = \left(\begin{smallmatrix} * & * \\ c\sqrt{m} & d \end{smallmatrix}\right) \in \Gamma_m(N)$,*

$$v_2(M) = \begin{cases} (c/d)_* & \text{if } M \equiv I \pmod{N}, \\ i(c/d)_* & \text{if } M \equiv -I \pmod{N}, \end{cases}$$

where

$$\left(\frac{c}{d}\right)_* = \left(\frac{c}{|d|}\right)(-1)^{\frac{\operatorname{sgn} c - 1}{2} \cdot \frac{\operatorname{sgn} d - 1}{2}}$$

$$\text{if } c \neq 0 \quad \text{and} \quad \left(\frac{0}{1}\right)_* = 1, \ \left(\frac{0}{-1}\right)_* = -1.$$

As usual, if x is a nonzero real number, then $\operatorname{sgn} x = x/|x|$.

Since the computations are straightforward, the verification of the lemma is omitted.

LEMMA 3.2. *Let N be as in Lemma 3.1. Then $v_2(M^{-1}S^{N\sqrt{m}}M) = 1$ for any $M \in G(\sqrt{m})$. In particular, $\kappa_q = 0$ for any parabolic point of $\Gamma_m(N)$.*

PROOF. If M is even with lower row $(c\sqrt{m}, d)$, then by Lemma 3.1 $v_2(M^{-1}S^{N\sqrt{m}}M) = (-c^2Nm/(1 - dcNm))_*$. If M is odd with lower row $(c, d\sqrt{m})$, then $v_2(M^{-1}S^{N\sqrt{m}}M) = (-c^2N/(1 - dcNm))_*$. If $c = 0$, the result is immediate. If $c \neq 0$, both of the preceding expressions are of the form $(-k^2n/(1 - sn))_*$, $k \neq 0, n > 0, n \equiv 0 \pmod{8}$. However,

$$\left(\frac{-k^2n}{1-sn}\right)_* = \left(\frac{-k^2n}{|1-sn|}\right)(-1)^{\frac{1-\operatorname{sgn}(1-sn)}{2}} = \left(\frac{n}{|1-sn|}\right)$$
$$= \left(\frac{n_1}{|1-sn|}\right) = 1$$

where n_1 is the largest odd integer dividing n; and the proof of the lemma is complete.

In the circle method the cusp form expansions at parabolic points are not used as given by (3.1) but rather in the equivalent formulation given in

Lemma 3.3. *Let F be in $C^0(\Gamma_m(N), -r, v_2^u)$ where N is as in Lemma 3.1, r is a half-integer, and $u = 4(r/2 - [\![-r/2]\!])$. Then to each $M = \left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right) \in G(\sqrt{m})$ there corresponds an expansion of F, valid for* $\operatorname{Im} z > 0$, *of the following form*:

$$F(z) = \frac{1}{(\gamma z + \delta)^r} \sum_{n=1}^{\infty} a_n(M) e(nMz/N\sqrt{m}).$$

In addition, if $M' = \left(\begin{smallmatrix}\alpha' & \beta' \\ \gamma' & \delta'\end{smallmatrix}\right) \equiv M \pmod N$ with $V = M'^{-1}M = \left(\begin{smallmatrix}* & * \\ c\sqrt{m} & d\end{smallmatrix}\right)$, then

$$a_n(M') = (c/d)_*^u e(rk) a_n(M) \tag{3.2}$$

where k is the integer, independent of z in H, defined by

$$k(M, M') = (1/2\pi)(\arg(\gamma' Vz + \delta') - \arg(\gamma z + \delta) + \arg(c\sqrt{m}z + d)).$$

Proof. Given $M = \left(\begin{smallmatrix}\alpha & \beta \\ \gamma & \delta\end{smallmatrix}\right) \in G(\sqrt{m})$ with $\gamma \neq 0$, $q = -\delta/\gamma$ is a finite parabolic point of $\Gamma_m(N)$. Since $M(q) = \infty$, the expansion (3.1) of F at q becomes

$$F(z) = \frac{1}{(z + \delta/\gamma)^r} \sum_{n=1}^{\infty} a_n(q) e(nMz/N\sqrt{m}).$$

Note that $\kappa_q = 0$ by Lemma 3.2. Then, since $(z + \delta/\gamma)^r = \gamma^{-r}(\gamma z + \delta)^r K$ where K is a constant of absolute value one, independent of z,

$$F(z) = \frac{1}{(\gamma z + \delta)^r} \sum_{n=1}^{\infty} \frac{\gamma^r}{K} a_n(q) e(nMz/N\sqrt{m});$$

and $a_n(M) = \gamma^r a_n(q)/K$. Similarly, if $M \in G(\sqrt{m})$ has $\gamma = 0$, $M = \pm\left(\begin{smallmatrix}1 & t\sqrt{m} \\ 0 & 1\end{smallmatrix}\right)$; and $a_n(M) = (\pm 1)^r e(-t/N) a_n(\infty)$.

To prove (3.2) consider first the expansion

$$F(z) = \frac{1}{(\gamma' z + \delta')^r} \sum_{n=1}^{\infty} a_n(M') e(nM'z/N\sqrt{m}).$$

Replacing z by Vz and using the equation $F(Vz) = v_2^u(V)(c\sqrt{m}z + d)^r F(z)$, we have

$$F(z) = \frac{1}{v_2^u(V)(c\sqrt{m}z + d)^r(\gamma' Vz + \delta')^r} \sum_{n=1}^{\infty} a_n(M') e(nMz/N\sqrt{m}).$$

Since $\gamma' Vz + \delta' = (\gamma z + \delta)/(c\sqrt{m}z + d)$,

$$F(z) = \frac{1}{(\gamma z + \delta)^r} \sum_{n=1}^{\infty} \overline{v}_2^u(V) e(-rk(M, M')) a_n(M') e(nMz/N\sqrt{m}).$$

By the uniqueness of the expansion, $a_n(M') = v_2^u(V) e(rk(M, M')) a_n(M)$. Since $V \equiv I \pmod N$, $v_2^u(V) = (c/d)_*^u$ by Lemma 3.1; and the proof of (3.2) is complete.

LEMMA 3.4. *Let M, M', V and $k(M, M')$ be defined as in Lemma* 3.3. *If* $\gamma \neq 0$ *and* $\gamma' = \gamma$, *then* $k(M', V) = 0$.

PROOF.

$$2\pi k(M, M') = \arg(\gamma Vz + \delta') - \arg(\gamma z + \delta) + \arg(c\sqrt{m}z + d)$$

$$= \arg(Vz + \delta'/\gamma) - \arg(z + \delta/\gamma) + \arg(c\sqrt{m}z + d).$$

Since $Vz + \delta'/\gamma$ and $z + \delta/\gamma$ lie in H, $-\pi + \arg(c\sqrt{m}z + d) < 2\pi k(M, M') < \pi + \arg(c\sqrt{m}z + d)$. Then, since $0 \leqslant \arg(c\sqrt{m}z + d) < \pi$ when $c \geqslant 0$ and $-\pi < \arg(c\sqrt{m}z + d) < 0$ when $c < 0$, $k(M', M) = 0$.

The last in this series of lemmas is used to reduce the problem of estimating the Fourier coefficients of cusp forms on congruence subgroups to that of estimating the Fourier coefficients of cusp forms on the principal congruence subgroups.

LEMMA 3.5. *Let Γ be a congruence subgroup with $\Gamma_m(N) \subset \Gamma$. Let $F \in C^0(\Gamma, -r, v)$ have Fourier expansion at ∞*

$$F(z) = \sum_{k+\kappa>0} a_k e((k+\kappa)z/\lambda). \tag{3.3}$$

Let

$$F(z) = \sum_{n+\kappa'>0} b_n e((n+\kappa')z/N\sqrt{m})$$

be the Fourier expansion at ∞ of F considered as a cusp form on $\Gamma_m(N)$ where κ' is defined by $v(S^{N\sqrt{m}}) = e(\kappa')$, $0 \leqslant \kappa' < 1$. Then

$$b_n = \begin{cases} a_k & \text{if } n = kt + [\![\kappa t]\!], \\ 0 & \text{otherwise,} \end{cases} \tag{3.4}$$

where $t = N\sqrt{m}/\lambda$.

PROOF. Since $\Gamma_m(N) \subset \Gamma$, there does exist a positive integer t such that $S^{N\sqrt{m}} = S^{\lambda t}$. Then $e(\kappa') = v(S^\lambda)^t = e(\kappa t)$ so that $\kappa t = [\![\kappa t]\!] + \kappa'$. Using these facts in (3.3), we have

$$F(z) = \sum_{kt+[\![\kappa t]\!]+\kappa'>0} a_k e((kt + [\![\kappa t]\!] + \kappa')/N\sqrt{m}).$$

(3.4) now follows from the uniqueness of the Fourier expansion.

3.3. *The Fourier coefficient estimate.* The main result of this section is contained in

THEOREM 3.1. *Let Γ be a congruence subgroup of $G(\sqrt{m})$ of level N and let $F \in C^0(\Gamma, -r, v)$ have the Fourier expansion at ∞*

$$F(z) = \sum_{n+\kappa>0} a_n e((n+\kappa)z/\lambda).$$

If r is a positive half-integer, $r \geqslant 1/2$, and v_1 is a congruence character where $v = v_1 v_2^u$, then

$$a_n = O(n^{r/2-1/4} \ln^{3/2} n \sigma_{-1/2}(nt + \kappa t)) \quad \text{as } n \to \infty \tag{3.5}$$

where $t = 24m^2N^2\sqrt{m}/\lambda(mN, 12)$.

REMARKS. 1. By Theorems 1.1 and 2.5 only finitely many multiplier systems of a fixed degree $-r$ satisfy the conditions of Theorem 3.1. However, (3.5) is valid for all multiplier systems of positive half-integral degree on $\Gamma(1)$, $G(\sqrt{2})$, or $G(\sqrt{3})$.

2. When $\Gamma = \Gamma_1(N)$, $v \equiv 1$, and r is an even integer, (3.5) reduces to A. V. Malyshev's estimate in [12]. This estimate has been improved recently by R. A. Rankin [21] who has shown that if $F \in C^0(\Gamma(1), -r, 1)$, r an even integer, is an eigenform, then

$$|a_n| \leqslant n^{r/2-1/4}\sigma_{-1/2}(n).$$

However, P. Deligne's recent proof of the Ramanujan conjecture should now lead to the estimate $a_n = O(n^{r/2-1/2+\epsilon})$.

3. The cusp forms $\eta(z)$ and $\eta^3(z)$ of degrees $-1/2$ and $-3/2$ respectively both satisfy the conditions of Theorem 3.1. Since their expansions at ∞ are

$$\eta(z) = \sum_{m=-\infty}^{\infty} (-1)^m e((m(3m+1)/2 + 1/24)z)$$

and

$$\eta^3(z) = \sum_{m=0}^{\infty} (-1)^m (2m+1) e((m(m+1)/2 + 1/8)z),$$

the best exponent for n in (3.5) is $r/2 - 1/4$ when r is half of an odd integer.

PROOF. The Kloosterman-Esterman version of the Hardy-Littlewood circle method is used to prove (3.5). Since the details of this method are well known (see [1], [5], [12], or [23]), only the modification necessary to handle cusp forms on the Hecke groups and nontrivial multiplier systems of nonintegral degree are emphasized.

Let $N' = 24m^2N^2/(mN, 12)$. By Theorems 1.1 and 2.5, $v \equiv v_2^u$ on $\Gamma_m(N')$. Also note that N' satisfies the conditions of Lemma 3.1. By Lemma 3.5 it suffices to prove $c_n = O(n^{r/2-1/4}\ln^{3/2} n\sigma_{-1/2}(n))$ for $F \in C^0(\Gamma_m(N'), -r, v_2^u)$ with Fourier expansion

$$F(z) = \sum_{n=1}^{\infty} c_n e(nz/N'\sqrt{m}). \tag{3.6}$$

From (3.6) it follows that

$$c_n = \frac{1}{N'\sqrt{m}} \int_{z_0}^{z_0 + N'\sqrt{m}} F(z) e(-nz/N'\sqrt{m})\, dz$$

for any fixed z_0 in $\mathcal{H}$. We take $z_0 = \sqrt{m}/(\mu + 1) + i\eta$ where $\eta = \sqrt{m}/n$ and $\mu = [\![\sqrt{n}]\!]$ and then divide up the path of integration by means of the mediants of the Farey sequence of order μ multiplied by $\sqrt{m}$. This gives

$$\begin{aligned} c_n = \frac{e(n\eta/N'\sqrt{m})}{N'\sqrt{m}} \sum_{q=1}^{\mu} \sum_{0<h\leqslant N'q} e(-nh) \\ \cdot \int_{-\sqrt{m}/q(q+q_2)}^{\sqrt{m}/q(q+q_1)} F\left(\frac{h}{q}\sqrt{m} + \theta + i\eta\right) e(-n\theta/N'\sqrt{m})\, d\theta \end{aligned} \tag{3.7}$$

where q_1 and q_2 are uniquely defined by $q_1 h \equiv -1 \pmod{q}$, $\mu - q < q_1 \leqslant \mu$, and $q_2 h \equiv 1 \pmod{q}$, $\mu - q < q_2 \leqslant \mu$. The sum on h and the integral in (3.7) are now interchanged using the auxiliary function

$$g_{\mu,q}(\theta, h) = \begin{cases} 1, & -\sqrt{m}/q(q + q_2) \leqslant \theta \leqslant \sqrt{m}/q(q + q_1), \\ 0 & \text{otherwise,} \end{cases}$$

which was first introduced by H. D. Kloosterman. This gives

$$c_n = \frac{e(n\eta/N'\sqrt{m})}{N'\sqrt{m}} \sum_{q=1}^{\mu} \int_{-\sqrt{m}/q(\mu+1)}^{\sqrt{m}/q(\mu+1)} e(-n\theta/N'\sqrt{m}) \sum_{0<l\leqslant N;(l,q,N')=1} d^{(l)}(\theta)$$

where

$$\begin{aligned} d^{(l)}(\theta) = \sum_{0<h'\leqslant qN'';(h',qN'')=1;h'\equiv l'(\mathrm{mod}\, N'')} g_{\mu,q}(\theta, h) e\left(\frac{-nh'}{N''q}\right) \\ \cdot F\left(\frac{h\sqrt{m}}{q} + \theta + i\eta\right) \end{aligned} \tag{3.8}$$

with, for fixed l, $\delta = (l, N')$, $l = \delta l'$, $N' = \delta N''$, and $h = \delta h'$.

It is at this point that we use the fact that F is a cusp form. For each h in the sum (3.8) we choose $M_h \in G(\sqrt{m})$ so that $M_h(h\sqrt{m})/q) = \infty$ and then replace $F(h\sqrt{m}/q + \theta + i\eta)$ in (3.8) by the expansion of Lemma 3.3 corresponding to M_h evaluated at $z = h\sqrt{m}/q + \theta + i\eta$. If $q \equiv 0 \pmod{m}$, define $M_h = \begin{pmatrix} a & b\sqrt{m} \\ c\sqrt{m} & d \end{pmatrix}$ as follows:

$$a = -\delta(\delta')^2 h'', \qquad c\sqrt{m} = q\sqrt{m}/m,$$

$$d = -h, \qquad b\sqrt{m} = \frac{ad-1}{c\sqrt{m}} = \frac{\delta^2(\delta')^2 h'h'' - 1}{q}\sqrt{m},$$

where $\delta\delta' \equiv 1 \pmod{q}$ with $0 < \delta' \leqslant q$, $h'h'' \equiv 1 \pmod{qN''}$ with $0 < l'' \leqslant qN''$, and, for $h' \neq l'$, $qN'' < h'' \leqslant 2qN''$. If $q \not\equiv 0 \pmod{m}$, $(q, m) = 1$. Write $N'' = m^s N^*$ where $(N^*, m) = 1$ and define $M_h = \begin{pmatrix} a\sqrt{m} & b \\ c & d\sqrt{m} \end{pmatrix}$ by

$$a\sqrt{m} = -\delta(\delta')^2 m^{s+1}(m')^{s+1}h'^*\sqrt{m}, \qquad c = q,$$

$$d\sqrt{m} = -h\sqrt{m}, \qquad b = \frac{mad-1}{c} = \frac{\delta^2(\delta')^2(m')^{s+1}m^{s+1}mh'h'^* - 1}{q},$$

where h'^* is uniquely determined by $mh'h'^* \equiv 1 \pmod{qN^*}$, $0 < l'^* \leqslant qN^*$ and, for $h' \neq l'$, $qN^* < h'^* \leqslant 2qN^*$. Also, $mm' \equiv 1 \pmod{q}$ with $0 < m' \leqslant q$.

Since $M_h \equiv M_l \pmod{N'}$ whenever $h' \equiv l' \pmod{N''}$, the coefficients $a_v^{(l)}$ and $a_v^{(h)}$ in the expansions of F corresponding to M_l and M_h respectively are related by

$$a_v^{(h)} = (C/D)_*^u e(rk(M_l, M_h))a_v^{(l)}$$

where $M_h^{-1}M_l = \left(\begin{smallmatrix} * & * \\ C\sqrt{m} & D \end{smallmatrix}\right)$. By Lemma 3.4, $k(M_l, M_h) = 0$. Also

$$(C/D)_* = \begin{cases} (l'/q')(h'/q') & \text{when } q \equiv 0 \pmod{m}, \\ (l'/q'')(h'/q'') & \text{when } q \not\equiv 0 \pmod{m}, \end{cases} \tag{3.9}$$

where q' is the largest odd integer dividing q/m and q'' is the largest odd integer dividing q. The verification of (3.9) is left until the end of the proof of the theorem. For notational convenience set

$$p = p(q, u) = \begin{cases} 1 & \text{if } u \text{ is even}, \\ q' & \text{if } u \text{ is odd and } q \equiv 0 \pmod{m}, \\ q'' & \text{if } u \text{ is odd and } q \not\equiv 0 \pmod{m}. \end{cases}$$

Then, for fixed l, whenever $h' \equiv l' \pmod{N''}$,

$$a_v^{(h)} = (l'/p)(h'/p)a_v^{(l)}.$$

Now set $\omega = \theta + i\eta$ and

$$Q = \begin{cases} q/\sqrt{m} & \text{if } q \equiv 0 \pmod{m}, \\ q & \text{if } q \not\equiv 0 \pmod{m}. \end{cases}$$

Replacing $F(h\sqrt{m}/q + \omega)$ in (3.8) by the corresponding series and using the fact that $g_{\mu,q}(\theta) = \Sigma_{k=1}^{q} b_k e(kh^{-1}/q)$, where h^{-1} is any integer such that $hh^{-1} \equiv 1 \pmod{q}$, we have

$$d^{(l)}(\theta) = \frac{1}{(Q\omega)^r} \sum_{v=1}^{\infty} \left(\frac{l'}{p}\right) a_v^{(l)} e(-v/Q^2\omega N\sqrt{m})\sigma_v^{(l)}(N'', \mu, q; \theta, h)$$

where, in A. V. Malyshev's notation,

$$\sigma_v^{(l)}(N'', \mu, q; \theta, h) = \sum_{k=1}^{q} b_k K_p(-n, -v(\delta')^2 M + kN''\delta'; l', N''; qN'')$$

with

$$M = \begin{cases} 1 & \text{if } q \equiv 0 \pmod{m}, \\ (m')^{s+1} m^s & \text{if } q \not\equiv 0 \pmod{m}. \end{cases}$$

Note that the generalized Kloosterman sums are introduced here.

It now remains to estimate $\sigma_v^{(l)}$, $d^{(l)}$, and then c_n. Since A. V. Malyshev [12] has shown that

$$|K_t(x, y; j, L; s)| \leqslant \sqrt{s} \min\left\{\tau\left(\frac{s}{(x, s)}\right)\sqrt{(x, s)}, \tau\left(\frac{s}{(y, s)}\right)\sqrt{(y, s)}\right\}$$

and since $\Sigma_{k=1}^{q} |b_k| < ln(4q)$, we have

$$\begin{aligned} |\sigma_v^{(l)}| &< ln(4q)\sqrt{qN''}\sqrt{(qN'', n)}\tau(qN''/(qN'', n)) \\ &< A_1 ln n \tau(q/(q, n))\sqrt{(q, n)}\sqrt{q}. \end{aligned}$$

Here, and in what follows, A_i denotes a constant independent of n. The estimates from the classical version of the circle method now show that

$$|d^{(l)}(\theta)| < A_2 n^{r/2} ln n \tau(q/(q, n))\sqrt{(q, n)}\sqrt{q}$$

and then that

$$|c_n| < A_3 n^{r/2 - 1/4} ln^{3/2} n \sigma_{-1/2}(n).$$

The proof is complete except for the verification of (3.9) which is given in

LEMMA 3.6. *For $h \equiv l \pmod{N'}$ and $M_h^{-1} M_l = \begin{pmatrix} * & * \\ C\sqrt{m} & D \end{pmatrix}$,*

$$(C/D)_* = \begin{cases} (l'/q')(h'/q') & \text{if } q \equiv 0 \pmod{m}, \\ (l'/q'')(h'/q'') & \text{if } q \not\equiv 0 \pmod{m}, \end{cases} \tag{3.9}$$

where q' and q'' are the largest odd integers dividing q/m and q, respectively.

PROOF. If $h = l$, (3.9) is obvious. For $h \neq l$, when $q \equiv 0 \pmod{m}$ $C = -qE/m$ and $D = 1 + lE$ where $E = \delta(\delta')^2(h'' - l'')$. When $q \not\equiv 0 \pmod{m}$, $C = -qG$ and $D = 1 + lmG$ where $G = \delta(\delta')^2 m^{s+1}(m')^{s+1}(h'^* - l'^*)$. Because of the choice of the residue class in which l'', h'', l'^*, and h'^* lie, E and G are positive integers. Also, since $E \equiv G \equiv 0 \pmod{N'}$, $E \equiv G \equiv 0 \pmod{8}$. Therefore, when $q \equiv 0 \pmod{m}$,

$$\left(\frac{C}{D}\right)_* = \left(\frac{q/m}{1 + lE}\right)\left(\frac{E}{1 + lE}\right) = \left(\frac{q'}{1 + lE}\right) = \left(\frac{1 + lE}{q'}\right).$$

However, since $1 + lE \equiv l'h'' \pmod{q'}$,

$$\left(\frac{1 + lE}{q'}\right) = \left(\frac{l'}{q'}\right)\left(\frac{h''}{q'}\right) = \left(\frac{l'}{q'}\right)\left(\frac{h'}{q'}\right).$$

Similarly, when $q \not\equiv 0 \pmod{m}$,

$$\left(\frac{C}{D}\right)_* = \left(\frac{1+lmG}{q''}\right) = \left(\frac{l'mh'^*}{q''}\right) = \left(\frac{l'}{q''}\right)\left(\frac{h'}{q''}\right).$$

REFERENCES

1. T. Esterman, *Vereinfachter Beweis eines Satzes von Kloosterman*, Abh. Math. Seminar Hamburg Univ. 7 (1929), 82–98.

2. R. C. Gunning, *Lectures on modular forms*, Ann. of Math. Studies, no. 48, Princeton Univ. Press, Princeton, N. J., 1962. MR 24 #A2664.

3. E. Hecke, *Über die Bestimmung Dirichletscher Reihen durch ihre Funktionalgleichung*, Math. Ann. 112 (1936), 664–699.

4. J. I. Hutchinson, *On a class of automorphic functions*, Trans. Amer. Math. Soc. 3 (1902), 1–11.

5. H. D. Kloosterman, *Asymptötische Formeln für die Fourierkoeffizienten ganzer Modulformen*, Abh. Math. Seminar Hamburg Univ. 5 (1927), 337–352.

6. M. I. Knopp, *Determination of certain roots of unity in the theory of automorphic forms of dimension zero*, Duke Math. J. 27 (1960), 497–506. MR 22 #5614.

7. ———, *Modular functions in analytic number theory*, Markham, Chicago, Illinois, 1970. MR 42 #198.

8. M. I. Knopp and J. R. Smart, *On Kloosterman sums connected with modular forms of half-integral dimension*, Illinois J. Math. 8 (1964), 480–487. MR 29 #2231.

9. J. H. van Lint, *On the multiplier system of the Riemann-Dedekind function* η, Nederl. Akad. Wetensch. Proc. Ser. A 61 = Indag. Math. 20 (1958), 522–527. MR 21 #2065.

10. J. Lehner, *Discontinuous groups and automorphic functions*, Math. Surveys, no. 8, Amer. Math. Soc., Providence, R. I., 1964. MR 29 #1332.

11. A. V. Malyšev, *Generalized Kloosterman sums and their estimates*, Vestnik Leningrad Univ. 15 (1960), no. 13, 59–75. (Russian) MR 23 #A2391.

12. ———, *On Fourier coefficients of modular forms*, Studies in Number Theory, Seminars in Math., V. A. Steklov Math. Inst., Leningrad, vol. 1; English transl., Consultants Bureau, New York, 1968. MR 38 #103.

13. A. W. Mason, *Lattice subgroups of free congruence groups*, Glasgow Math. J. 10 (1969), 106–115. MR 43 #2112.

14. D. L. McQuillan, *Classification of normal congruence subgroups of the modular group*, Amer. J. Math. 87 (1965), 285–296. MR 32 #2484.

15. M. Newman, *Modular quotient groups*, Illinois J. Math. 18 (1974), 265–274.

16. M. F. Newman and J. R. Smart, *Modulary groups of t × t matrices*, Duke Math. J. 30 (1963), 253–257. MR 26 #6265.

17. H. Petersson, *Über die Entwicklungskoeffizienten der automorphen Formen*, Acta Math. 58 (1932), 169–215.

18. ———, *Über Modulfunktionen und Partitionenprobleme*, Abh. Deutsch. Akad Wiss. Berlin Kl. Math. Allg. Nat. 1954, no. 2, 59 pp. MR 17, 129.

19. H. Rademacher and H. S. Zuckerman, *On the Fourier coefficients of certain modular forms of positive dimension*, Ann. of Math. 39 (1938), 433–462.

20. J. Raleigh, *The Fourier coefficients of the invariants* $j(2^{1/2}; \tau)$ *and* $j(3^{1/2}; \tau)$, Trans. Amer. Math. Soc. 87 (1958), 90–107. MR 20 #7103.

21. R. A. Rankin, *An* Ω*-result for the coefficients of cusp forms*, Math. Ann. 203 (1973), 239–250. MR 48 #241.

22. H. Salié, *Über die Kloosterman Summen* $S(u, v; q)$, Math. Z. 34 (1931), 91–109.

23. ———, *Zur Abschätzung der Fourierkoeffizienten ganzer Modulformen*, Math. Z. 36 (1932), 263–278.

24. A. Selberg, *On the estimation of Fourier coefficients of modular forms*, Proc. Sympos. Pure Math., vol. 8, Amer. Math. Soc. Providence, R. I., 1965, pp. 1–15. MR 32 #93.

25. J. R. Smart, *Parametrization of automorphic forms for the Hecke groups* $G(\sqrt{2})$ *and* $G(\sqrt{3})$, Duke Math. J. 31 (1964), 395–403. MR 29 #2390.

26. S. A. Stepanov, *Estimation of Kloosterman sums*, Izv. Akad. Nauk SSSR Ser. Mat. 35 (1971), 308–323 = Math. USSR Izv. 5 (1971), 319–336. MR 45 #5097.

27. A. Weil, *On some exponential sums*, Proc. Nat. Acad. Sci. U.S.A. 34 (1948), 204–207. MR 10, 234.

28. J. Young, *On the group belonging to the sign* (0, 3; 2, 4, ∞) *and the functions belonging to it*, Trans. Amer. Math. Soc. 5 (1904), 81–104.

DEPARTMENT OF MATHEMATICS, OHIO STATE UNIVERSITY, COLUMBUS, OHIO 43210