TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 277, Number 2, June 1983

GAUSS SUMS AND FOURIER ANALYSIS ON MULTIPLICATIVE SUBGROUPS OF $\mathbf{Z}_q$

BY

HAROLD G. DIAMOND, FRANK GERTH III AND JEFFREY D. VAALER[1]

ABSTRACT. Let $G(q)$ denote the multiplicative group of invertible elements in $\mathbf{Z}_q$, the ring of integers modulo q. Let $H \subseteq G(q)$ be a multiplicative subgroup with cosets aH and bH. If f: $\mathbf{Z}_q \to \mathbf{C}$ is supported in aH we show that f can be recovered from the values of $\hat{f}$ restricted to bH if and only if Gauss sums for H are nonvanishing. Here $\hat{f}$ is the (finite) Fourier transform of f with respect to the additive group $\mathbf{Z}_q$. The main result is a simple criterion for deciding when these Gauss sums are nonvanishing. If $H = G(q)$ then f can be recovered from $\hat{f}$ restricted to $G(q)$ by a particularly elementary formula. This formula provides some inequalities and extremal functions.

1. Introduction. Let $\mathbf{Z}_q$ denote the ring of residue classes of integers modulo q and let $G(q) \subseteq \mathbf{Z}_q$ be the multiplicative group of residue classes which are relatively prime to q. Here $q \geqslant 2$ is an integer and $|G(q)| = \varphi(q)$, where φ is Euler's function. If f: $\mathbf{Z}_q \to \mathbf{C}$ we define the (finite) Fourier transform of f to be the function $\hat{f}$: $\mathbf{Z}_q \to \mathbf{C}$ determined by

$$\hat{f}(n) = q^{-1/2} \sum_{m=1}^{q} f(m) e\left(\frac{-nm}{q}\right), \tag{1.1}$$

where $e(x) = e^{2\pi i x}$. As is well known, the function f can be recovered from $\hat{f}$ by the inversion formula

$$f(m) = q^{-1/2} \sum_{n=1}^{q} \hat{f}(n) e\left(\frac{nm}{q}\right). \tag{1.2}$$

Alternatively, a function f: $\mathbf{Z}_q \to \mathbf{C}$ can be identified in an obvious way with a point in the finite-dimensional vector space $\mathbf{C}^q$. Thus the Fourier transform can be viewed as a linear transformation from $\mathbf{C}^q$ to $\mathbf{C}^q$ determined by the matrix $\mathfrak{F}_q = \{q^{-1/2} e(-nm/q)\}$, where $1 \leqslant n \leqslant q$ and $1 \leqslant m \leqslant q$. The inversion formula is then equivalent to the observation that $\mathfrak{F}_q^{-1} = \{q^{-1/2} e(nm/q)\}$.

In the present paper we investigate some questions concerning the inverse of certain submatrices of $\mathfrak{F}_q$. Let f: $\mathbf{Z}_q \to \mathbf{C}$ be a function with support contained in the multiplicative group $G(q)$, that is, $f(m) = 0$ if $(m, q) > 1$. Is it possible to recover f

Received by the editors May 21, 1982.
1980 *Mathematics Subject Classification.* Primary 12C25; Secondary 12C20, 15A24.
Key words and phrases. Gauss sums, finite Fourier transforms.
[1]Research of the three authors was supported in part by grants from the National Science Foundation.

0002-9947/82/0000-0884/$04.50

from the values of $\hat{f}$ restricted to $G(q)$? If we write

$$\mathcal{F}_{G(q)} = \left\{ q^{-1/2} e\left(\frac{-nm}{q} \right) \right\} \tag{1.3}$$

for the $\varphi(q) \times \varphi(q)$ matrix where $1 \leqslant n \leqslant q$, $1 \leqslant m \leqslant q$, $(n, q) = (m, q) = 1$, then this question is clearly equivalent to asking if $\mathcal{F}_{G(q)}$ is an invertible matrix. More generally let $H \subseteq G(q)$ be a multiplicative subgroup and let aH and bH be cosets of H in $G(q)$. If f: $\mathbf{Z}_q \to \mathbf{C}$ is supported in the coset aH, can f be recovered from the values of $\hat{f}$ restricted to bH? Now the corresponding matrix question involves the $|H| \times |H|$ matrix

$$\mathcal{F}_H^{(s)} = \left\{ q^{-1/2} e\left(\frac{-snm}{q} \right) \right\} \tag{1.4}$$

where $n \in H$, $m \in H$ and $s = ab$, and asks if the matrix $\mathcal{F}_H^{(s)}$ is invertible. We give a complete solution to this problem by determining those subgroups $H \subseteq G(q)$ for which $\mathcal{F}_H^{(s)}$ has an inverse. Our solution allows us to give inversion formulas analogous to (1.2). When $H = G(q)$ these formulas are particularly elementary and lead to some interesting inequalities and extremal functions.

In order to determine those matrices $\mathcal{F}_H^{(s)}$ which are invertible we solve an equivalent problem on the nonvanishing of Gauss sums associated with an arbitrary subgroup $H \subseteq G(q)$. Specifically, let γ: $H \to T$ be a homomorphism, where $T = \{z \in \mathbf{C}: |z| = 1\}$ denotes the circle group. As usual we call such a homomorphism γ a character of H. We shall always assume that the domain of γ is extended to $\mathbf{Z}_q$ by setting $\gamma(m) = 0$ if $m \notin H$. We write Γ_H for the set of all distinct characters γ and note that $|\Gamma_H| = |H|$. It is easy to show that every $\gamma \in \Gamma_H$ has the form

$$\gamma(m) = \begin{cases} \chi(m) & \text{if } m \in H, \\ 0 & \text{if } m \notin H \end{cases}$$

for some Dirichlet character χ.

In our notation the Fourier transform of $\gamma \in \Gamma_H$ is the function

$$\hat{\gamma}(n) = q^{-1/2} \sum_{m=1}^{q} \gamma(m) e\left(\frac{-nm}{q} \right). \tag{1.5}$$

Aside from the factor $q^{-1/2}$, the right-hand side of (1.5) is a Gauss sum associated with characters on the subgroup H. The connection between these sums and the matrices $\mathcal{F}_H^{(s)}$ is provided by the following simple result, which is proved in §3.

THEOREM 1. *Let $H \subseteq G(q)$ be a multiplicative subgroup. Then for each integer s, $(s, q) = 1$,*

$$\pm \det\left(\mathcal{F}_H^{(s)} \right) = \prod_{\gamma \in \Gamma_H} \hat{\gamma}(s), \tag{1.6}$$

where the $+$ or $-$ sign depends only on H. Moreover, if (1.6) *is not zero for some integer s, $(s, q) = 1$, then* (1.6) *is not zero for every integer s, $(s, q) = 1$.*

For certain special subgroups H the value of $\hat{\gamma}(s)$ can, of course, be explicitly determined. For results in this direction we note the recent survey of Berndt and

Evans [1]. In view of Theorem 1, our problem here is to determine those subgroups H for which $\prod_{\gamma\in\Gamma_H}\hat{\gamma}(s)\neq 0$ whenever $(s,q)=1$. Some special cases of this problem have already been considered. Weber [7, §19] gives a complete solution when q is a prime power. For arbitrary q, Fuchs [3] has determined the cyclic subgroups H such that (in our notation) $\hat{\gamma}_0(1)\neq 0$, where γ_0 is the principal character in Γ_H (see also Kummer [6]). More recently, Evans [2] has given a generalization of Weber's result for certain cyclic subgroups H and arbitrary q.

To describe our solution to this problem we define $v=v(q)$ to be the divisor of q determined by

$$v(q)=\begin{cases}\prod_{p|q}p & \text{if } 8\nmid q,\\ 2\prod_{p|q}p & \text{if } 8\mid q,\end{cases}$$

where the products extend over distinct primes p which divide q. We then define $U(q)=\{m\in\mathbf{Z}_q\colon m\equiv 1 \bmod v\}$. It is clear that $U(q)\subseteq G(q)$. Since $U(q)$ is closed under multiplication it is in fact a multiplicative subgroup of $G(q)$. We also note that the set $U(q)$ has an additive structure. The set $\{m\in\mathbf{Z}_q\colon m\equiv 0 \bmod v\}$ is obviously an additive subgroup of $\mathbf{Z}_q$and $U(q)$ is one of its cosets.

THEOREM 2. *Let $H\subseteq G(q)$ be a multiplicative subgroup. Then the following four conditions are equivalent*:

(i) $\prod_{\gamma\in\Gamma_H}\hat{\gamma}(s)\neq 0$ *for each* s, $(s,q)=1$,

(ii) $\hat{\gamma}_0(1)\neq 0$, *where* γ_0 *is the principal character in* Γ_H,

(iii) H *does not contain a coset of a nontrivial additive subgroup of* $\mathbf{Z}_q$,

(iv) $H\cap U(q)=\{1\}$.

By combining Theorems 1 and 2 we find that the matrices $\mathcal{F}_H^{(s)}$, $(s,q)=1$, are invertible if and only if $H\cap U(q)=\{1\}$. The last condition is simple to check. Cases in which (iii) does not hold are sometimes clear by inspection, e.g. $\{1,19\}\subset G(36)$. Whenever q is square free the subgroup $U(q)$ is trivial, and so $\mathcal{F}_H^{(s)}$ is invertible for all subgroups $H\subset G(q)$ and all s with $(s,q)=1$. A proof of Theorem 2 is given in §4.

We now consider the problem of determining the inverse of $\mathcal{F}_H^{(s)}$ whenever it exists. Let $H\subseteq G(q)$ be a subgroup satisfying $H\cap U(q)=\{1\}$ and let s be an integer, $(s,q)=1$. For each coset sH we define $W_{sH}\colon \mathbf{Z}_q\to\mathbf{C}$ by

$$W_{sH}(m)=q^{1/2}|H|^{-1}\sum_{\gamma\in\Gamma_H}\hat{\gamma}(s)^{-1}\gamma(m\tilde{s}) \tag{1.7}$$

where $s\tilde{s}\equiv 1 \bmod q$. If $sH=tH$ then $s\equiv th \bmod q$ for some $h\in H$. Using Lemma 5 in §2 we find that

$$\sum_{\gamma\in\Gamma_H}\hat{\gamma}(s)^{-1}\gamma(m\tilde{s})=\sum_{\gamma\in\Gamma_H}\hat{\gamma}(th)^{-1}\gamma(m\tilde{t})\overline{\gamma(h)}=\sum_{\gamma\in\Gamma_H}\hat{\gamma}(t)^{-1}\gamma(m\tilde{t}).$$

This identity shows that W_{sH} depends only on the coset sH and not on the coset representative s. In §5 we show that W_{sH} is the unique function for which the following three conditions hold:

(1.8) the support of W_{sH} is contained in the coset sH,

(1.9) $\hat{W}_{sH}(1) = q^{1/2}$,

(1.10) if $n \in H$ but $n \not\equiv 1 \bmod q$, then $\hat{W}_{sH}(n) = 0$.

From these properties of W_{sH} we can easily deduce the inversion formulas analogous to (1.2).

THEOREM 3. *Let $H \cap U(q) = \{1\}$ and let $s = ab$ where $(a, q) = (b, q) = 1$. Suppose that f: $\mathbf{Z}_q \to \mathbf{C}$ is supported in the coset aH and its Fourier transform $\hat{f}$ is defined by* (1.1). *Let W_{sH}: $\mathbf{Z}_q \to \mathbf{C}$ be defined by* (1.7). *Then for all integers m we have*

$$f(m) = q^{-1/2} \sum_{n \in bH} \hat{f}(n) W_{sH}(mn) \tag{1.11}$$

and for all integers l

$$\hat{f}(l) = q^{-1/2} \sum_{n \in bH} \hat{f}(n) \hat{W}_{sH}(l\tilde{n}), \tag{1.12}$$

where $n\tilde{n} \equiv 1 \bmod q$. Moreover, the inverse of the matrix $\mathcal{F}_H^{(s)}$ is $\{q^{-1/2} W_{sH}(smn)\}$, $m \in H$, $n \in H$.

The identity (1.12) shows that if the values of $\hat{f}$ on bH are given then $\hat{f}$ can be extended to all of $\mathbf{Z}_q$ in such a way that f is supported in aH.

If f: $\mathbf{Z}_q \to \mathbf{C}$ is supported in the coset aH then Theorem 3 can, at least in principle, be used to bound $|f(m)|$ by an expression depending on $|\hat{f}(n)|$ only for values of n in bH. For example, if $|\hat{f}(n)| \leqslant A$ for all n in bH then

$$|f(m)| \leqslant q^{-1/2} A \sum_{n \in bH} |W_{sH}(mn)| \tag{1.13}$$

for all m in aH. If m is fixed then an obvious choice of $\hat{f}$ shows that this inequality is sharp. Another bound of the same type is

$$|f(m)|^2 \leqslant |H|^{-1} \sum_{\gamma \in \Gamma_H} |\hat{\gamma}(s)|^{-2} \sum_{n \in bH} |\hat{f}(n)|^2 \tag{1.14}$$

where $m \in aH$ and $s = ab$. This is easily obtained from (1.7), (1.11), the Cauchy-Schwarz inequality and the orthogonality relations for the characters in Γ_H. In the special case $H = G(q)$ these bounds can be put in a much more satisfactory form. In fact if $H = G(q)$ it is possible to give an elementary representation of $W_{G(q)}$ as a finite Fourier series which does not involve multiplicative characters. We carry this out in §6, and also give some resulting upper bound estimates.

2. Preliminary lemmas. In this section we collect together several results which will be used to prove the main theorems.

LEMMA 4. *Let p be an odd prime, $(m, p) = 1$, ζ a primitive p^αth root of unity for some fixed $\alpha \geqslant 1$, and ω a primitive mth root of unity. Suppose that*

$$1 \leqslant l_1 < l_2 < \cdots < l_J \leqslant p^\alpha$$

are integers with $J \leqslant p - 1$. Then the numbers $\{\zeta^{l_j}: j = 1, 2, \ldots, J\}$ are linearly independent over $\mathbf{Q}(\omega)$.

PROOF. Suppose, contrary to the statement of the lemma, that there are numbers a_j in $\mathbf{Q}(\omega)$ which are not all zero and such that

$$\sum_{j=1}^{J} a_j \zeta^{l_j} = 0. \tag{2.1}$$

Obviously we may assume that each $a_j \neq 0$, for otherwise the corresponding l_j can be discarded. Let $l_{J+1} = p^\alpha + l_1$ so that $\Sigma_{j=1}^{J}(l_{j+1} - l_j) = p^\alpha$. It follows that for some integer k we have $1 \leqslant k \leqslant J$ and

$$(l_{k+1} - l_k) \geqslant p^\alpha J^{-1} \geqslant p^\alpha (p-1)^{-1} > p^{\alpha-1}.$$

With this choice of k we define the polynomial $P(X)$ in $\mathbf{Q}(\omega)[X]$ by

$$P(X) = \sum_{j=1}^{k} a_j X^{p^\alpha + l_j - l_{k+1}} + \sum_{j=k+1}^{J} a_j X^{l_j - l_{k+1}}. \tag{2.2}$$

In (2.2) the second sum on the right does not occur if $k = J$. Now if $1 \leqslant j \leqslant k$ we have

$$\begin{aligned} 0 = l_1 - l_1 &\leqslant p^\alpha + l_1 - l_{k+1} \leqslant p^\alpha + l_j - l_{k+1} \\ &\leqslant p^\alpha + l_k - l_{k+1} < p^\alpha - p^{\alpha-1} = \varphi(p^\alpha). \end{aligned}$$

If $k+1 \leqslant j \leqslant J$ we find that

$$\begin{aligned} 0 = l_{k+1} - l_{k+1} &\leqslant l_j - l_{k+1} \leqslant p^\alpha - l_{k+1} \\ &< p^\alpha - (l_{k+1} - l_k) < p^\alpha - p^{\alpha-1} = \varphi(p^\alpha). \end{aligned}$$

Thus $P(X)$ is a polynomial of degree strictly less than $\varphi(p^\alpha)$. Also the coefficients of $P(X)$ are not all zero. If $k = J$ this is obvious. If $k < J$ it follows that $1 \leqslant p^\alpha + l_j - l_{k+1}$ for $1 \leqslant j \leqslant k$, and so the constant term of $P(X)$ is $a_{k+1} \neq 0$.

Next we observe that if (2.1) holds then

$$\begin{aligned} 0 &= \zeta^{l_{k+1}} \sum_{j=1}^{J} a_j \zeta^{l_j - l_{k+1}} \\ &= \zeta^{l_{k+1}} \left\{ \sum_{j=1}^{k} a_j \zeta^{p^\alpha + l_j - l_{k+1}} + \sum_{j=k+1}^{J} a_j \zeta^{l_j - l_{k+1}} \right\} \\ &= \zeta^{l_{k+1}} P(\zeta). \end{aligned} \tag{2.3}$$

To obtain a contradiction to (2.3) we argue as follows. The field $\mathbf{Q}(\omega)$ has degree $\varphi(m)$ over $\mathbf{Q}$. Since $(p^\alpha, m) = 1$ it follows that $\mathbf{Q}(\omega, \zeta)$ has degree $\varphi(p^\alpha)\varphi(m)$ over $\mathbf{Q}$ and hence $\mathbf{Q}(\omega, \zeta)$ has degree $\varphi(p^\alpha)$ over $\mathbf{Q}(\omega)$. Thus a nonzero polyomial in $\mathbf{Q}(\omega)[X]$ which vanishes at ζ must have degree at least $\varphi(p^\alpha)$. Since $P(\zeta) = 0$ and P has degree less than $\varphi(p^\alpha)$, the contradiction proves the lemma.

Throughout the remainder of this section we assume that $H \subseteq G(q)$ is a multiplicative subgroup.

LEMMA 5. *If $h \in H$ and n is an integer then for each $\gamma \in \Gamma_H$ we have $\hat{\gamma}(nh) = \hat{\gamma}(n)\overline{\gamma(h)}$ where $\bar{z}$ is the complex conjugate of z.*

PROOF. Let $\tilde{h}$ denote the inverse of h in H. Since γ is a homomorphism on H we have

$$\hat{\gamma}(nh) = q^{-1/2} \sum_{m \in H} \gamma(m) e\left(\frac{-nhm}{q}\right) = q^{-1/2} \sum_{m \in H} \gamma(m\tilde{h}) e\left(\frac{-nm}{q}\right)$$

$$= \overline{\gamma(h)}\, q^{-1/2} \sum_{m \in H} \gamma(m) e\left(\frac{-nm}{q}\right) = \overline{\gamma(h)}\, \hat{\gamma}(n).$$

LEMMA 6. *For each integer $q \geqslant 2$ the subgroup $U(q)$ is cyclic of order q/v.*

PROOF. Let $q = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ where $p_1 < p_2 < \cdots < p_r$ are distinct primes. If $m \in G(q)$ and $m \equiv n_j \bmod p_j^{\alpha_j}$ for $j = 1, 2, \ldots, r$ then

$$m \to (n_1, n_2, \ldots, n_r) \tag{2.4}$$

is an isomorphism from $G(q)$ onto $G(p_1^{\alpha_1}) \times \cdots \times G(p_r^{\alpha_r})$. If $u \in U(q)$ then $u \equiv 1 \bmod v(q)$ and so $u \equiv 1 \bmod v(p_j^{\alpha_j})$ for each j. It follows that (2.4) induces an isomorphism from $U(q)$ onto $U(p_1^{\alpha_1}) \times \cdots \times U(p_r^{\alpha_r})$. Since the order of $U(p_j^{\alpha_j})$ is $p_j^{\alpha_j}\{v(p_j^{\alpha_j})\}^{-1}$ and the primes p_j are distinct, it suffices to prove that each group $U(p_j^{\alpha_j})$ is cyclic. This is in fact well known and is proved in Hasse [5, p. 59].

Our next result was first obtained by Weber [7, §19]. We give a shorter proof here by appealing to Lemma 4.

LEMMA 7. *Let $q = p^{\alpha}$ be a prime power and suppose that $H \cap U(p^{\alpha}) = \{1\}$. Then for each integer s, $(s, p^{\alpha}) = 1$, we have $\prod_{\gamma \in \Gamma_H} \hat{\gamma}(s) \neq 0$.*

PROOF. First we consider the case $p = 2$. If $\alpha = 1$ or $\alpha = 2$ it is easy to check that H must be the trivial subgroup. The conclusion of the lemma is then obvious. Thus we suppose that $p = 2$ and $\alpha \geqslant 3$. In this case $U(2^{\alpha})$ is a cyclic subgroup of order $2^{\alpha-2}$ and we have the isomorphism (Hasse [5, p. 59]) $G(2^{\alpha}) \cong \{1, -1\} \times U(2^{\alpha})$. If H is trivial the result is obvious, as before. If H is not trivial but $H \cap U(2^{\alpha})$ is trivial then either $H = \{1, -1\}$ or $H = \{1, 2^{\alpha-1} - 1\}$. In both of these cases we can compute $\hat{\gamma}(s)$ directly. If $H = \{1, -1\}$ we have

$$\hat{\gamma}(s) = 2^{-\alpha/2}\left\{e\left(\frac{-s}{2^{\alpha}}\right) \pm e\left(\frac{s}{2^{\alpha}}\right)\right\} \neq 0.$$

If $H = \{1, 2^{\alpha-1} - 1\}$ we have

$$\hat{\gamma}(s) = 2^{-\alpha/2}\left\{e\left(\frac{-s}{2^{\alpha}}\right) \pm e\left(\frac{-s}{2} + \frac{s}{2^{\alpha}}\right)\right\}$$

$$= 2^{-\alpha/2}\left\{e\left(\frac{-s}{2^{\alpha}}\right) \mp e\left(\frac{s}{2^{\alpha}}\right)\right\} \neq 0.$$

This completes the proof if $p = 2$.

Next we suppose that p is an odd prime and $\alpha \geqslant 1$. In this case we have the isomorphism (Hasse [5, p. 59]) $G(p^{\alpha}) \cong L(p^{\alpha}) \times U(p^{\alpha})$ where $L(p^{\alpha})$ is a cyclic subgroup of order $p - 1$. Since $|U(p^{\alpha})| = p^{\alpha-1}$ is prime to $p - 1$ and $H \cap U(p^{\alpha}) = \{1\}$ it follows that $H \subseteq L(p^{\alpha})$.

Now let $\gamma \in \Gamma_H$. Since $H \subseteq L(p^{\alpha})$ we have $h^{p-1} \equiv 1 \bmod p^{\alpha}$ for all $h \in H$. Therefore $\gamma(h) \in \mathbf{Q}(\omega)$ where ω is a primitive $(p - 1)$th root of unity. Also, if

$1 \leqslant h_1 < h_2 < \cdots < h_J < p^\alpha$ are the distinct elements of H then $J = |H| \leqslant |L(p^\alpha)| = p - 1$. If we apply Lemma 4 with $m = p - 1$ and $\zeta = e(-s/p^\alpha)$ we find that

$$\sum_{j=1}^{J} \gamma(h_j) e\left(\frac{-sh_j}{p^\alpha}\right) \neq 0.$$

This proves the lemma for odd primes.

3. Proof of Theorem 1. Let $K = \{k_{mn}\}$, $m \in H$, $n \in H$ be the $|H| \times |H|$ matrix

$$k_{mn} = \begin{cases} 1 & \text{if } n \equiv \tilde{m} \bmod q, \\ 0 & \text{if } n \not\equiv \tilde{m} \bmod q, \end{cases}$$

where $\tilde{m}$ is the inverse of m in H. It follows that $\det(K) = \pm 1$ since K is a permutation matrix. A simple calculation shows that $K\mathcal{F}_H^{(s)} = \{q^{-1/2} e(-s\tilde{n}m/q)\}$. If $\gamma \in \Gamma_H$ and $n \in H$ then

$$q^{-1/2} \sum_{m \in H} \gamma(m) e\left(\frac{-s\tilde{n}m}{q}\right) = \hat{\gamma}(s\tilde{n}) = \hat{\gamma}(s)\overline{\gamma(\tilde{n})} = \hat{\gamma}(s)\gamma(n)$$

by Lemma 5. Thus γ is an eigenvector for the matrix $K\mathcal{F}_H^{(s)}$ with eigenvalue $\hat{\gamma}(s)$. Since Γ_H provides $|H|$ linearly independent eigenvectors we have

$$\pm \det\left(\mathcal{F}_H^{(s)}\right) = \det\left(K\mathcal{F}_H^{(s)}\right) = \prod_{\gamma \in \Gamma_H} \hat{\gamma}(s). \tag{3.1}$$

This proves (1.6).

To establish the last part of the theorem we observe that

$$\det\left(\mathcal{F}_H^{(s)}\right) = q^{-|H|/2} \sum_{\pi} \operatorname{sgn}(\pi) e\left(-\frac{s}{q} \sum_{h \in H} h\pi(h)\right) \tag{3.2}$$

where the sum on the right side of (3.2) extends over all permutations π of the elements in H. Ignoring the factor $q^{-|H|/2}$, the right-hand side of (3.2) is a polynomial with integer coefficients evaluated at $e(-s/q)$. Obviously this polynomial vanishes at one primitive qth root of unity if and only if it vanishes at every primitive qth root of unity.

The matrix $K\mathcal{F}_H^{(s)}$ which occurs in the preceding argument is an example of a circulant matrix with respect to the group H. Identity (3.1) is a special case of a general formula for the determinant of a circulant matrix as a product over characters of a group.

4. Proof of Theorem 2. We show that (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i). Since the first implication is obvious, we begin by proving that (ii) $\Rightarrow$ (iii). Suppose that there exists a coset of a nontrivial additive subgroup in H,

$$\mathcal{C} = \{a, a + d, a + 2d, \ldots, a + (r - 1)d\} \subset H,$$

where $rd = q$ and $r > 1$. By deleting elements of $\mathcal{C}$ if necessary, we can assume that $r = p$, a prime. Let $K = \tilde{a}\mathcal{C}$, where $a\tilde{a} \equiv 1 \bmod q$. Thus $K \subseteq H$. It is easy to verify that $K = \{m \in \mathbf{Z}_q : m \equiv 1 \bmod q/p\}$ is also a multiplicative subgroup of H.

Let $h_1, h_2, \dots, h_J$ denote distinct representatives of the cosets of K in H. We then have

$$q^{1/2}\hat{\gamma}_0(1) = \sum_{m\in H} e(-m/q) = \sum_{j=1}^{J} \sum_{k\in K} e\left(\frac{-h_j k}{q}\right)$$
$$= \sum_{j=1}^{J} \sum_{t=0}^{p-1} e\left(\frac{-h_j}{q}\left(\frac{tq}{p}+1\right)\right) = \sum_{j=1}^{J} e\left(\frac{-h_j}{q}\right) \sum_{t=0}^{p-1} e\left(\frac{-h_j t}{p}\right) = 0.$$

Thus (ii) does not hold if (iii) does not hold.

Next, we show that (iii) implies (iv). Suppose that (iv) does not hold, so $H \cap U(q)$ is not the one element subgroup. Let p be a prime number such that $H \cap U(q)$ contains a subgroup of order p. By Lemma 6 the group $U(q)$ is cyclic and so contains exactly one subgroup of order p, namely $K = \{m \in \mathbf{Z}_q : m \equiv 1 \bmod q/p\}$. The set $K \subseteq H \cap U(q) \subseteq H$ and K is a coset of an additive subgroup. Thus (iii) does not hold if (iv) does not hold.

Finally we prove that (iv) implies (i). If this implication is false, then there exists a counterexample consisting of an integer q, a subgroup $H \subseteq G(q)$ such that $H \cap U(q) = \{1\}$, and a character $\gamma \in \Gamma_H$ such that $\hat{\gamma}(s) = 0$ for some s, $(s, q) = 1$. We may assume that q is the smallest positive integer for which such a counterexample exists. In view of Lemma 7 q cannot be a prime power. Thus we may suppose that $q = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ where $p_1 < p_2 < \cdots < p_r$ are distinct primes, $r \geqslant 2$ and so p_r is odd.

Let $q_1 = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_{r-1}^{\alpha_{r-1}}$ and $q_2 = p_r^{\alpha_r}$. Next we let x and y be integers such that $xq_1 + yq_2 = 1$. We then have

$$q^{1/2}\hat{\gamma}(s) = \sum_{h\in H} \gamma(h) e\left(\frac{-sh}{q}(xq_1 + yq_2)\right)$$
$$= \sum_{h\in H} \gamma(h) e\left(\frac{-syh}{q_1}\right) e\left(\frac{-sxh}{q_2}\right)$$
$$= \sum_{t\in G(q_2)} \left\{ \sum_{\substack{h\in H \\ h\equiv t \bmod q_2}} \gamma(h) e\left(\frac{-syh}{q_1}\right)\right\} e\left(\frac{-sxt}{q_2}\right)$$
$$= \sum_{t\in G(q_2)} a(t)\zeta^t \tag{4.1}$$

where $\zeta = e(-sx/q_2)$ is a primitive $p_r^{\alpha_r}$th root of unity and

$$a(t) = \sum_{\substack{h\in H \\ h\equiv t \bmod q_2}} \gamma(h) e\left(\frac{-syh}{q_1}\right). \tag{4.2}$$

In order to apply Lemma 4 to the right-hand side of (4.1) we will show that $a(t) \neq 0$ for at most $p_r - 1$ values of t, the coefficients $a(t)$ are elements of a suitable field $\mathbf{Q}(\omega)$, and $a(1) \neq 0$.

By Euler's theorem $h^{\varphi(v)} \equiv 1 \bmod v$ for each $h \in H$. Since $h^{\varphi(v)} \in H$ and $H \cap U(q) = \{1\}$ it follows that

$$h^{\varphi(v)} \equiv 1 \mod q \tag{4.3}$$

whenever $h \in H$. As in our proof of Lemma 7 we have the isomorphism

$$G(q_2) \cong L(q_2) \times U(q_2) \tag{4.4}$$

where $L(q_2)$ has order $p_r - 1$ and $U(q_2)$ has order $p_r^{\alpha_r - 1}$. From (4.3) we see that the order of $h \bmod q$ divides $\varphi(v)$ and so the order of $h \bmod q_2$ must divide $\varphi(v)$. But $(\varphi(v), p_r^{\alpha_r - 1}) = 1$ since p_r is the largest prime divisor of q. Hence we find that $h \equiv t \bmod q_2$ implies that $t \in L(q_2)$. In other words, the canonical homomorphism of $G(q)$ onto $G(q_2)$ maps H onto a subgroup of $L(q_2)$. Applying these observations to the coefficients $a(t)$ defined by (4.2) we conclude that $a(t) = 0$ if $t \notin L(q_2)$. Thus (4.1) can be written as

$$q^{1/2}\hat{\gamma}(s) = \sum_{t \in L(q_2)} a(t)\zeta^t. \tag{4.5}$$

From (4.3) it follows that $\gamma(h)$ is a $\varphi(v)$th root of unity for all $h \in H$. Therefore the coefficients $a(t)$ defined by (4.2) are elements of the field $\mathbf{Q}(\omega)$ where ω is a primitive $\varphi(v)q_1$th root of unity. We note that $(\varphi(v)q_1, q_2) = 1$ as is required in the hypotheses of Lemma 4.

Finally, we need to show that $a(t) \neq 0$ for some $t \in L(q_2)$. In fact we will show that $a(1) \neq 0$. Let $K \subseteq H$ be the subgroup defined by $K = \{h \in H: h \equiv 1 \bmod q_2\}$. Then let σ: $K \to G(q_1)$ be the canonical homomorphism. If $K' \subseteq G(q_1)$ is determined by $\sigma(K) = K'$ then σ: $K \to K'$ is an isomorphism since its kernel is clearly trivial. We claim that $K' \cap U(q_1) = \{1\}$. If not there exists a nontrivial element $k \in K$ such that $k \equiv \sigma(k) \equiv 1 \bmod v(q_1)$ and (by the definition of K) $k \equiv 1 \bmod q_2$. Since $v(q_2) \mid q_2$ it follows that $k \equiv 1 \bmod v(q)$. This contradicts our assumption that $H \cap U(q) = \{1\}$ and so establishes that $K' \cap U(q_1) = \{1\}$. Next we observe that

$$a(1) = \sum_{k \in K} \gamma(k) e\left(\frac{-syk}{q_1}\right) = \sum_{k' \in K'} \gamma(\sigma^{-1}(k')) e\left(\frac{-syk'}{q_1}\right). \tag{4.6}$$

Now $\gamma \circ \sigma^{-1}$ is clearly a character in $\Gamma_{K'}$. Since $q_1 < q$ and q is the *smallest* modulus for which a counterexample to the result can be constructed, it follows that the right-hand side of (4.6) cannot be zero.

To complete the proof we apply Lemma 4 to conclude that the right-hand side of (4.5) is not zero. This proves that (iv) implies (i).

5. Proof of Theorem 3. We begin by showing that the function W_{sH} defined by (1.7) satisfies the three conditions (1.8), (1.9), and (1.10). Of course, it is trivial that W_{sH} satisfies (1.8), since the functions $\gamma(m\tilde{s})$ in (1.7) are supported in the coset sH. If we apply the Fourier transform to both sides of (1.7) we find that

$$\hat{W}_{sH}(n) = q^{1/2} |H|^{-1} \sum_{\gamma \in \Gamma_H} \hat{\gamma}(s)^{-1} \hat{\gamma}(ns) \tag{5.1}$$

for all n. Now for $h \in H$ we have $\hat{\gamma}(hs) = \hat{\gamma}(s)\overline{\gamma(h)}$ by Lemma 5. Using this observation in (5.1) we obtain

$$\hat{W}_{sH}(h) = q^{1/2}|H|^{-1} \sum_{\gamma \in \Gamma_H} \overline{\gamma(h)} \tag{5.2}$$

for all $h \in H$. By the orthogonality of the characters of H, the right-hand side of (5.2) is $q^{1/2}$ if h is the identity element in the group H and zero otherwise. This establishes (1.9) and (1.10).

Next we prove the inversion formula (1.11). If $m \notin aH$ and $n \in bH$ then $mn \notin sH$. Thus both sides of (1.11) are zero. If $m \in aH$ then the right-hand side of (1.11) is

$$\begin{aligned} &q^{-1} \sum_{n \in bH} \sum_{k \in aH} f(k) e\left(\frac{-nk}{q}\right) W_{sH}(mn) \\ &\qquad = q^{-1} \sum_{k \in aH} f(k) \left\{ \sum_{n \in bH} W_{sH}(mn) e\left(\frac{-nk}{q}\right) \right\}. \end{aligned} \tag{5.3}$$

Using (1.8) we see that the inner sum on the right-hand side of (5.3) can be extended to a sum over all $n \in \mathbf{Z}_q$. Thus (5.3) equals

$$q^{-1/2} \sum_{k \in aH} f(k) \hat{W}_{sH}(k\tilde{m}) = f(m)$$

by (1.9) and (1.10). To obtain formula (1.12) we take the Fourier transform of both sides of (1.11). It follows immediately from (1.11) and the definition of the inverse of a matrix that the inverse of $\mathcal{F}_H^{(s)}$ is given by $\{q^{-1/2} W_{sH}(smn)\}$, $m \in H$, $n \in H$. This completes the proof of Theorem 3.

It is easy to show that W_{sH} is the unique function which satisfies the three conditions (1.8), (1.9) and (1.10), for if g: $\mathbf{Z}_q \to \mathbf{C}$ also satisfies these conditions then we may apply Theorem 3 with $a = s$ and $b = 1$. We obtain

$$g(m) = q^{-1/2} \sum_{n \in H} \hat{g}(n) W_{sH}(mn) = W_{sH}(m)$$

since g satisfies (1.11) and $\hat{g}(n) = 0$ if $n \in H$ but $n \not\equiv 1 \bmod q$.

6. The special case $H = G(q)$. Throughout this section *we assume that q is square free* and so $U(q)$ is trivial. We have seen that the matrices $\mathcal{F}_{G(q)}^{(s)}$ are all invertible, but now there is only one coset so we take $s = 1$ and write simply $\mathcal{F}_{G(q)}$. The characters γ used to define $W_{G(q)}$ in (1.7) are now the ordinary Dirichlet characters so we write

$$W_{G(q)}(m) = q^{1/2} \varphi(q)^{-1} \sum_{\chi} \hat{\chi}(1)^{-1} \chi(m), \tag{6.1}$$

where the sum is over all Dirichlet characters to the modulus q. We also simplify our notation by writing $W_{G(q)}(m) = W(m)$.

If d is a positive divisor of q we define $\bar{d}$ to be the unique integer, $1 \leqslant \bar{d} \leqslant q/d$, which satisfies $d\bar{d} \equiv 1 \bmod (q/d)$. It is easy to check that $\{d\bar{d}\colon d \mid q\}$ is precisely the set of idempotent elements in the ring $\mathbf{Z}_q$. In particular the residue classes $d\bar{d} \bmod q$ are distinct since $(d\bar{d}, q) = d$.

LEMMA 8. *If $d \mid q$ then*

$$\sum_{p \mid d} (q/p)\overline{(q/p)} \equiv (q/d)\overline{(q/d)} \mod q, \tag{6.2}$$

where the summation is over primes p which divide d.

PROOF. Let p_0 be a prime divisor of q. If $p_0 \mid d$ then

$$\begin{aligned}\sum_{p \mid d} (q/p)\overline{(q/p)} &\equiv (q/p_0)\overline{(q/p_0)} \mod p_0 \\ &\equiv 1 \mod p_0\end{aligned}$$

and

$$\begin{aligned}(q/d)\overline{(q/d)} &\equiv 1 \mod d \\ &\equiv 1 \mod p_0.\end{aligned}$$

If $p_0 \nmid d$ then both sides of (6.2) are congruent to zero mod p_0. Thus (6.2) holds mod p_0 for each p_0 dividing q and therefore holds mod q.

We now give an elementary representation for the function $W(m)$ which does not involve the Dirichlet characters.

THEOREM 9. *For square free q the function W defined by* (1.7) *has the finite Fourier series representation*

$$W(m) = \sum_{d \mid q} \mu(d) e\left(\frac{d\bar{d}m}{q}\right), \tag{6.3}$$

where μ denotes the Möbius function, and the product representation

$$W(m) = \prod_{p \mid q} \left\{ e\left(\frac{m}{p}\overline{(q/p)}\right) - 1 \right\}. \tag{6.4}$$

PROOF. From Lemma 8 we have

$$\begin{aligned}\prod_{p \mid q} \left\{ e\left(\frac{m}{p}\overline{(q/p)}\right) - 1 \right\} &= \sum_{d \mid q} \mu(d) e\left(\sum_{p \mid (q/d)} \frac{m}{p}\overline{(q/p)} \right) \\ &= \sum_{d \mid q} \mu(d) e\left(\frac{m}{q} \sum_{p \mid (q/d)} (q/p)\overline{(q/p)} \right) \\ &= \sum_{d \mid q} \mu(d) e\left(\frac{d\bar{d}m}{q} \right).\end{aligned}$$

Thus the function $f(m) = \Sigma_{d \mid q} \mu(d) e(d\bar{d}m/q)$ has the product representation (6.4). Now (6.4) shows that $f(m)$ is supported in $G(q)$ and therefore satisfies the condition (1.8). From the finite Fourier series for f we see that

$$\hat{f}(n) = \begin{cases} q^{1/2}\mu(d) & \text{if } n \equiv d\bar{d} \bmod q, \text{ some } d \mid q, \\ 0 & \text{otherwise.} \end{cases}$$

Since the only idempotent element in $G(q)$ is 1 it follows that $f(m)$ satisfies the conditions (1.9) and (1.10). In §5 we proved that $W(m)$ is the unique function satisfying these three conditions and so $f(m) = W(m)$ for all m.

COROLLARY 10. *If* $\alpha > 0$ *then*

$$\left\{ \sum_{m=1}^{q} |W(m)|^{\alpha} \right\}^{1/\alpha} = 2^{\omega(q)} \prod_{p|q} \left\{ \sum_{l=1}^{p-1} \left(\sin \frac{\pi l}{p} \right)^{\alpha} \right\}^{1/\alpha} \tag{6.5}$$

where $\omega(q)$ *is the number of prime divisors of* q. *In particular we have*

$$\sum_{m=1}^{q} |W(m)| = 2^{\omega(q)} \prod_{p|q} \cot \frac{\pi}{2p}, \tag{6.6}$$

$$\sum_{m=1}^{q} |W(m)|^2 = 2^{\omega(q)} q, \tag{6.7}$$

$$\max_{m} |W(m)| = 2^{\omega(q)} \prod_{\substack{p|q \\ p>2}} \cos \frac{\pi}{2p}. \tag{6.8}$$

PROOF. Using the product representation (6.4) we obtain

$$\sum_{m=1}^{q} |W(m)|^{\alpha} = \sum_{m \in G(q)} \prod_{p|q} \left| 2i \sin \left\{ \frac{\pi m}{p} \overline{(q/p)} \right\} \right|^{\alpha}. \tag{6.9}$$

Now let $q = p_1 p_2 \cdots p_r$ be written as a product of distinct primes. Since $G(q) \cong G(p_1) \times G(p_2) \times \cdots \times G(p_r)$, we may write the right-hand side of (6.9) as

$$2^{\alpha\omega(q)} \prod_{p|q} \sum_{l \in G(p)} \left| \sin \left\{ \frac{\pi l}{p} \overline{(q/p)} \right\} \right|^{\alpha}. \tag{6.10}$$

Of course $\overline{(q/p)}$ is relatively prime to p, so the identity (6.5) follows immediately. The identities (6.6) and (6.7) follow from easy calculations, while (6.8) follows from (6.5) by letting $\alpha \to +\infty$. Alternatively, (6.8) can be obtained directly from (6.4) by an easy calculation.

Let f: $\mathbf{Z}_q \to \mathbf{C}$ be supported in the subgroup $G(q)$ of invertible elements. Taking $H = G(q)$ and $s = 1$ in (1.11) we have

$$f(m) = q^{-1/2} \sum_{n \in G(q)} \hat{f}(n) W(mn)$$

for all integers m. We may now use Corollary 10 to obtain sharp bounds on $|f(m)|$ which depend only on the values of $|\hat{f}(n)|$ for $n \in G(q)$. From (6.5) and Hölder's inequality we find that

$$\begin{aligned} |f(m)| &\leq q^{-1/2} \left\{ \sum_{n \in G(q)} |W(mn)|^{\alpha} \right\}^{1/\alpha} \left\{ \sum_{n \in G(q)} |\hat{f}(n)|^{\beta} \right\}^{1/\beta} \\ &= q^{-1/2} 2^{\omega(q)} \prod_{p|q} \left\{ \sum_{l=1}^{p-1} \left(\sin \frac{\pi l}{p} \right)^{\alpha} \right\}^{1/\alpha} \left\{ \sum_{n \in G(q)} |\hat{f}(n)|^{\beta} \right\}^{1/\beta}, \end{aligned} \tag{6.11}$$

where $m \in G(q)$, $\alpha^{-1} + \beta^{-1} = 1$ and $\alpha > 1$. If we define f_k: $\mathbf{Z}_q \to \mathbf{C}$ for each $k \in G(q)$ by

$$f_k(m) = q^{-1/2} \sum_{n \in G(q)} \overline{W(kn)}\, |W(kn)|^{\alpha-2} W(mn), \tag{6.12}$$

then an easy computation shows that f_k is supported on $G(q)$, $\hat{f}_k(n) = \overline{W(kn)}\, |W(kn)|^{\alpha-2}$ for $n \in G(q)$, and there is equality in (6.11) when $m = k$. The limiting cases $\alpha = 1$ and $\alpha = +\infty$ can be dealt with in a similar manner. In these cases we may use (6.6) and (6.8) to obtain

$$|f(m)| \leqslant q^{-1/2} 2^{\omega(q)} \left\{ \prod_{p|q} \cot \frac{\pi}{2p} \right\} \left\{ \max_{(n,q)=1} |\hat{f}(n)| \right\} \tag{6.13}$$

and

$$|f(m)| \leqslant q^{-1/2} 2^{\omega(q)} \left\{ \prod_{\substack{p|q \\ p>2}} \cos \frac{\pi}{2p} \right\} \left\{ \sum_{n \in G(q)} |\hat{f}(n)| \right\}. \tag{6.14}$$

We consider one other class of extremal problems for functions f: $\mathbf{Z}_q \to \mathbf{C}$ which have support contained in $G(q)$, the invertible elements. The Fourier coefficients of f can be determined from the values of $\hat{f}$ on $G(q)$ with the aid of the W function. This fact and our additive representation of W enable us to give sharp upper estimates for

$$\|\hat{f}\|_\alpha = \left\{ \sum_{1 \leqslant k \leqslant q} |\hat{f}(k)|^\alpha \right\}^{1/\alpha}, \qquad \alpha \geqslant 1,$$

in terms of $\max\{|\hat{f}(k)| : k \in G(q)\}$.

We have from (1.12)

$$\hat{f}(n) = q^{-1/2} \sum_{k \in G(q)} \hat{f}(k) \hat{W}(n\tilde{k})$$

and from the proof of Theorem 9

$$\hat{W}(l) = \begin{cases} q^{1/2}\mu(d) & \text{if } l \equiv d\bar{d} \bmod q, \text{ some } d \mid q, \\ 0 & \text{otherwise.} \end{cases}$$

It follows that

$$\hat{f}(n) = \sum_{d|q} \mu(d) \sum_{\substack{k \in G(q) \\ n\tilde{k} \equiv d\bar{d} \bmod q}} \hat{f}(k).$$

Now $n \equiv kd\bar{d} \bmod q$ if and only if $n \equiv k \bmod q/d$ and $d = (n, q)$, and so we obtain the alternative formula

$$\hat{f}(n) = \mu((n,q)) \sum_{\substack{k \in G(q) \\ k \equiv n \bmod q/(n,q)}} \hat{f}(k). \tag{6.15}$$

If $|\hat{f}(k)| \leqslant 1$ for all $k \in G(q)$, then

$$|\hat{f}(n)| \leqslant \sum_{\substack{k \in G(q) \\ k \equiv n \bmod q/(n,q)}} 1.$$

The last sum extends over integers k relatively prime to (n, q) and congruent to n mod $q/(n, q)$. By the Chinese remainder theorem, there are $\varphi((n, q))$ such numbers in $[1, q]$, so we obtain $|\hat{f}(n)| \leq \varphi((n, q))$, $1 \leq n \leq q$.

Now

$$\sum_{n=1}^{q} |\hat{f}(n)|^{\alpha} \leq \sum_{n=1}^{q} \varphi((n, q))^{\alpha} = \sum_{d|q} \varphi(d)^{\alpha} \sum_{\substack{1 \leq n \leq q \\ (n,q)=d}} 1$$

$$= \sum_{d|q} \varphi(d)^{\alpha} \varphi(q/d) = \prod_{p|q} \{(p-1)^{\alpha} + p - 1\},$$

and so

$$\|\hat{f}\|_{\alpha} \leq \prod_{p|q} \{(p-1)^{\alpha} + p - 1\}^{1/\alpha}, \qquad \alpha \geq 1, \tag{6.16}$$

$$\|\hat{f}\|_{\infty} \leq \varphi(q), \tag{6.17}$$

provided that $|\hat{f}(k)| \leq 1$ for all $k \in G(q)$. In particular we have $\|f\|_2 = \|\hat{f}\|_2 = \{q\varphi(q)\}^{1/2}$. The example $f = \sqrt{q}\chi_0$, where χ_0 is the principal character on $G(q)$, shows these bounds to be sharp. We have $\hat{f}(n) = \mu((n, q))\mu(q)\varphi((n, q))$ by a familiar formula for Ramanujan sums [**4**, §16.6].

7. Concluding remarks. We close by mentioning some questions that we have not settled and some interesting relations that we have observed but not put to good use.

We have found an explicit representation of the W function, independent of characters, for groups $G(q)$ with square free q, which enabled us to make certain estimates. What is an analogous representation of W for a more general group H (for which $H \cap U(q) = \{1\}$)? There is a recipe for composing W functions in the case that $q = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ and H has a direct product representation $H_1 \times \cdots \times H_r$, where each H_i is a multiplicative subgroup of $\mathbf{Z}_{p_i^{\alpha_i}}$. In this case $H \cap U(q) = \{1\}$ if and only if $H_i \cap U(p_i^{\alpha_i}) = \{1\}$ for $1 \leq i \leq r$, and for cH any coset, W_{cH} is given by the formula

$$W_{cH}(n) = \prod_{1 \leq j \leq r} W_{b_j c H_j}(n b_j), \tag{7.1}$$

where $b_j q/p_j^{\alpha_j} \equiv 1 \bmod p_j^{\alpha_j}$.

Suppose that H is a multiplicative group for which W_H exists. Upper estimates for W_{cH} can be deduced from lower bounds for $\{|\hat{\gamma}(c)| : \gamma \in \Gamma_H\}$. What are reasonable estimates for these numbers? Some of them will be rather small, as the following argument shows. Suppose that H is a subgroup that has r distinct cosets in $G(q)$, with $\{a_1, \ldots, a_r\}$ a system of distinct coset representatives. Let γ be a character of H. We have

$$|H| = \sum_{n \in H} |\gamma(n)|^2 = \sum_{1 \leq m \leq q} |\hat{\gamma}(m)|^2$$

$$\geq \sum_{i=1}^{r} \sum_{n \in H} |\hat{\gamma}(n a_i)|^2 = \sum_{i=1}^{r} |\hat{\gamma}(a_i)|^2 \sum_{n \in H} |\overline{\gamma(n)}|^2$$

$$= |H| \sum_{i=1}^{r} |\hat{\gamma}(a_i)|^2.$$

It follows that $\Sigma_{1\leqslant i\leqslant r}|\hat{\gamma}(a_i)|^2 \leqslant 1$, and hence, for each γ there is some integer c with $|\hat{\gamma}(c)| \leqslant r^{-1/2}$.

The argument of the W_G function is of interest, for example, in the construction of extremal functions in §6. We record the identity (for $W(n) \neq 0$)

$$W(n)/|W(n)| = e\left\{n\left(\frac{1}{2q} + \frac{\varepsilon(q)}{2}\right) + \frac{\omega(q)}{4} + \frac{1}{2}\sum_{p|q}\left[\frac{n}{p}\overline{\left(\frac{q}{p}\right)}\right]\right\},$$

where $\omega(q)$ denotes the number of prime divisors of q and $\varepsilon(q) = 0$ or 1 is a solution of the congruence

$$\sum_{p|q}\left(\frac{q}{p}\right)\overline{\left(\frac{q}{p}\right)} \equiv q\varepsilon(q) + 1 \mod 2q.$$

Another identity involving the argument is

$$W(n)e(-n/(2q)) = \mu(q)e(n/(2q))\,\overline{W(n)}.$$

The set of numbers $\{d\bar{d} \bmod q\colon d \mid q\}$ appeared in the explicit form of $W_{G(q)}$. What can one say about these numbers? Are they, for example, in some sense well distributed in $[1, q]$ as $\omega(q) \to \infty$? The number $q = 30$ satisfies $q/p \equiv 1 \bmod p$ for each $p \mid q$. Are there numbers q with arbitrarily large values of $\omega(q)$ having this property? For such numbers the set $\{d\bar{d} \bmod q\colon d \mid q\}$ will be badly distributed in $[1, q]$.

Suppose that $H \cap U(q) \neq \{1\}$, so that some Gauss sums vanish. Is there a tidy theory in this case? We can make a few observations here. Let

$$\mathfrak{N} = \left\{f\colon \mathbf{Z}_q \to \mathbf{C}\colon \operatorname{supp} f \subseteq H, \hat{f} \equiv 0 \text{ on } H\right\}.$$

The set $\mathfrak{N}$ is an ideal under the operations of pointwise addition and a multiplication defined by $f * g(n) = \Sigma_{k\in H} f(n\tilde{k})g(k)$. Moreover, $\mathfrak{N}$ is spanned by the set of characters $\gamma_1, \ldots, \gamma_r$ that lie in $\mathfrak{N} \cap \Gamma_H$. The function

$$W'_H(m) = \frac{q^{1/2}}{|H|}\sum_{\gamma\notin\mathfrak{N}}\frac{\gamma(m)}{\hat{\gamma}(1)}$$

satisfies $f(n) = q^{-1/2}\Sigma_{k\in H} W'_H(nk)\hat{f}(k)$ for all functions f for which $f(n) = \Sigma_{\gamma\notin\mathfrak{N}} \alpha(\gamma)\gamma(n)$.

We have shown that the operator $\mathcal{F}_H$ is invertible if the principal character satisfies $\hat{\gamma}_0(1) \neq 0$. Is there a more direct proof of this implication than the one we have given? One identity that we have noted connecting $\hat{\gamma}_0$ and W_H (when the latter exists!) is $\hat{W}_H(0)\hat{\gamma}_0(1) = 1$.

We conclude by mentioning a class of identities valid for a function supported in $G(q)$, the invertible elements of $\mathbf{Z}_q$, where q is square free. For any $d \mid q$ we have

$$\mu(d)\sum_{(k,q)=d}\hat{f}(k) = \mu(q)q^{-1/2}\sum_{n\in G(q)} f(n).$$

For $d = 1$ we obtain a Poisson-like relation $\Sigma_{k\in G(q)}\hat{f}(k) = \mu(q)\hat{f}(0)$.

REFERENCES

1. B. C. Berndt and R. Evans, *The determination of Gauss sums*, Bull. Amer. Math. Soc. (N.S.) **5** (1981), 107–129.

2. R. Evans, *Generalized cyclotomic periods*, Proc. Amer. Math. Soc. **81** (1981), 207–212.

3. L. Fuchs, *Ueber die Perioden, welche aus den Wurzeln der Gleichung* $\omega^n = 1$ *gebildet sind, wenn n eine zusammengesetzte Zahl ist*, J. Reine Angew. Math. **61** (1863), 374–386.

4. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 4th ed., Oxford Univ. Press, London, 1960.

5. H. Hasse, *Number theory*, Springer-Verlag, Berlin and New York, 1980.

6. E. Kummer, *Theorie der idealen Primfaktoren der complexen Zahlen, welche aus den Wurzeln der Gleichung* $\omega^n = 1$ *gebildet sind, wenn n eine zusammengesetzte Zahl ist*, Math. Abh. Kon. Akad. Wiss. Berlin (1856), 1–47; *Collected papers*, vol. 1. Springer-Verlag, Berlin and New York, 1975, pp. 583–629.

7. H. Weber, *Lehrbuch der Algebra*, 3rd. ed., vol. 2, Chelsea, New York, 1961.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF ILLINOIS, URBANA, ILLINOIS 61801

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF TEXAS, AUSTIN, TEXAS 78712