VALUES OF CYCLOTOMIC POLYNOMIALS AT ROOTS OF UNITY

R. P. KURSHAN and A. M. ODLYZKO

Abstract.

If $C_N(z)$ is the Nth cyclotomic polynomial and ζ_m a primitive mth root of unity, then $C_N(\zeta_m)$ is an algebraic integer in the mth cyclotomic field. This paper investigates the degree of $C_N(\zeta_m)$ over the rationals. A complete answer is obtained when $N=p^\alpha m$ for a prime p, $p \nmid m$, and $\alpha \geqq 1$; the degree is variously 1, $\varphi(m_1)$, $\varphi(m_1)/2$, or $2m_1/(m_1,\varphi(m_1))$ depending upon the values of p and $\varphi(pm_1)$ modulo m_1, where m_1 is the largest odd, square-free factor of m. Partial results are presented for the other cases.

The case $N=pm$ solves a problem of determining the power distributions of certain recursive linear digital filters.

1. Introduction.

This paper is devoted to a study of the arithmetic nature of the values of cyclotomic polynomials at roots of unity. Our terminology follows that in [1]. Let

$$\zeta_m = \exp\{2\pi i/m\} .$$

Then every primitive mth root of unity may be expressed as ζ_m^a for some a, $(a,m)=1$. Let

$$C_N(z) = \prod_{a (\bmod N)}' (z-\zeta_N^a)$$

denote the Nth cyclotomic polynomial, where $\prod'$ means that we take the product over any reduced residue system modulo N. Various properties of cyclotomic polynomials have been studied for a long time (see the bibliography in [9] or at the end of [2], for example). We will study the values $C_N(\mu)$, μ a root of unity — say a primitive mth rooth. Since $C_N(z) \in \mathbf{Z}[z]$, $C_N(\mu)$ is an algebraic integer in the field $\mathbf{Q}(\zeta_m)$. Up to units of the field, it is quite easy to determine which algebraic integer it is.

Received June 6, 1980.

PROPOSITION 1. *If N and m are positive integers, $N \neq m$, and μ is a primitive* mth *root of unity, then there is a unit $u \in \mathbf{Z}[\zeta_m]$ dependent upon N, m, and μ such that*

$$C_N(\mu) = \begin{cases} pu & \text{if } N/m = p^{\alpha}, \quad p \text{ a prime}, \quad \alpha > 0; \\ (1-\zeta_{p^{\alpha}})\mu & \text{if } N/m = p^{-\alpha}, \quad p \text{ a prime}, \quad \alpha > 0, \quad \text{and } p \nmid N; \\ (1-\zeta_{p^{\alpha+1}})^{p-1}u & \text{if } N/m = p^{-\alpha}, \quad p \text{ a prime}, \quad \alpha > 0, \quad \text{and } p \mid N; \\ u & \text{otherwise.} \end{cases}$$

Relative to the second and third cases, $(1-\zeta_{p^{\alpha}})^{\varphi(p^{\alpha})} = pu'$ for a unit u' (see Section 2). These characterizations of $C_N(\mu)$ appear in part in Diederichsen [5] (see also Magurn [10; Lemma 9.3] and Bass [4; Corollary 5.4]). The preceding determines completely the ideal generated by $C_N(\mu)$ in $\mathbf{Z}[\zeta_m]$, but leaves open the question of the nature of the algebraic integer $C_N(\mu)$ itself. Most of this paper is devoted to an investigation of that question. The principal results are stated in this section, while the proofs appear in subsequent sections.

Notice that if μ and ν are primitive mth roots of unity, then $C_N(\mu)$ and $C_N(\nu)$ are conjugates. An investigation of $C_N(\mu)$ is thus accomplished through an investigation for the particular case that $\mu = \zeta_m$. Let $u(N,m)$ be the unit u of Proposition 1 in this case.

We were led to this investigation by a question arising in the design of recursive linear digital filters [8]. As will be demonstrated in Section 5, this question can be reduced to a determination for a given m of those primes p for which $u(pm,m) = 1$ or $|u(pm,m)| = 1$. In fact, in the somewhat more general case that N/m is a (positive) prime power, we have obtained a complete characterization of the units u in terms of their degrees over the rationals and their relative moduli; this is given in Theorem 1.

For any integer $m > 1$, let m_0 be the largest square-free factor of m (i.e., m_0 is the product of one each of the prime factors of m), and let m_1 be the largest odd divisor of m_0 (i.e., $m_1 = m_0$ if m is odd, and $m_1 = m_0/2$ if m is even); set $1_0 = 1_1 = 1$.

THEOREM 1. *Let p be a prime, $p \nmid m$, and let $\alpha > \beta \geqq 0$ be integers. If $m_1 = 1$, then $u(p^{\alpha}m, p^{\beta}m) = 1$. If $m_1 > 1$, then*

i) $p \equiv 1 \pmod{m_1} \Leftrightarrow u(p^{\alpha}m, p^{\beta}m) = 1$;

ii) $p \equiv -1 \pmod{m_1} \Leftrightarrow |u(p^{\alpha}m, p^{\beta}m)| = 1$, $u(p^{\alpha}m, p^{\beta}m) \neq 1$; *in this case $u(p^{\alpha}m, p^{\beta}m)$ is a primitive* kth *root of unity, where $k = 2m_1/(m_1, \varphi(m_1))$.*

iii) $p \not\equiv \pm 1 \pmod{m_1} \Leftrightarrow |u(p^{\alpha}m, p^{\beta}m)| \neq 1$; *in this case the conjugates of $u(p^{\alpha}m, p^{\beta}m)$ have $\varphi(m_1)/2$ distinct absolute values, none equal to 1, and if $m_1 \mid \varphi(pm_1)$ then $u(p^{\alpha}m, p^{\beta}m) \in \mathbf{R}$ and has degree $\varphi(m_1)/2$ over $\mathbf{Q}$, whereas if $m_1 \nmid \varphi(pm_1)$, then $u(p^{\alpha}m, p^{\beta}m) \notin \mathbf{R}$ and has degree $\varphi(m_1)$ over $\mathbf{Q}$.*

The theorem remains true if in the three congruences we replace m_1 by m_0.

In the general situation our results are much less complete. If N is divisible by a prime p which is congruent to ± 1 modulo a certain divisor of m, then we can prove the result below. (Note that if the conditions of i) or ii) hold, then $C_N(\zeta_m) = pu(N,m)$ if $N = p^\alpha m$ for $\alpha \geqq 1$ and p a prime, and $C_N(\zeta_m) = u(N,m)$ otherwise.)

Proposition 2. *Let m, N be distinct positive integers and let p be a prime divisor of N. Set $N' = N_1$ if the highest powers of 2 dividing m and N are equal, $N' = N_0$ otherwise, and set $\hat{m} = m/(m, N/N')$. Then*

i) $p \equiv 1 \pmod{\hat{m}} \Rightarrow u(N,m) = 1$;

ii) $p \equiv -1 \pmod{\hat{m}} \Rightarrow u(N,m) = (-1)^\beta \mu$, *where μ is a primitive k-th root of unity, $k = \hat{m}/(\hat{m}, \varphi(N'/p))$, and $\beta = 1$ if $N' = p$ or $p\hat{m}$ and 0 otherwise.*

Note that if $N = rm$, $(r,m) = 1$, then $\hat{m} = m_1$, while if $N = N_1$, then $\hat{m} = m$.

Unfortunately, Proposition 2 does not cover all cases in which $|u(N,m)| = 1$. For example, for $N = 47 \cdot 73 \cdot 79 \cdot 151 \cdot 229$, $C_N(\zeta_{65}) = 1$ while none of the prime divisors of N are congruent to ± 1 modulo $\hat{m} = 65$. This evaluation can be easily checked by using the formula

$$C_N(z) = \prod_{d \mid N} (z^{N/d} - 1)^{\mu(d)} .$$

(Here $\mu(d)$ denotes the Möbius function.) Later we will say a few words about how this pair N, m was found. Another example where the degree of $C_N(\zeta_m)$ is less than $\varphi(m)$ is given by $C_{105}(\zeta_{24}) = -(2+\sqrt{\ })$, a unit of degree 2. Nonetheless, it is true that if m is sufficiently large, the degree of $C_N(\zeta_m)$ can be less than $\varphi(m)$ only because of the reduction below.

Let $m^* = 2\hat{m}$ ($\hat{m}$ as in Proposition 2) when the highest power of 2 dividing N is greater than that dividing m and let $m^* = \hat{m}$ otherwise. In Section 2 we observe that for some h, $(h, m^*) = 1$,

$$C_N(\zeta_m) = C_{N_1}(\zeta_{m^*}^h) .$$

Thus we can always reduce to the case where N is odd and square-free. In this situation, however, the next result states that no further reduction are possible if m is sufficiently large.

Theorem 2. *For any odd, square-free positive integer N there is an integer $m(N)$ such that if $m > m(N)$ then $C_N(\zeta_m) \notin \mathsf{R}$, $C_N(\zeta_m)$ is of degree $\varphi(m)$ over* Q *and the moduli of its conjugates constitute $\varphi(m)/2$ distinct values, none equal to* 1.

Our proofs of parts of theorems 1 and 2 are quite complicated, involving

Gaussian and Ramanujan sums, the non-vanishing of Dirichlet L-series at 1, and the construction of Dirichlet characters with special properties. It would be very desirable if we could find simpler proofs. Very general results about multiplicative relations among numbers of the form $1-\zeta_m$ have been proved by Ennola [6] (who corrected a mistake in [3]) and Ramachandra [12], but they do not appear to be applicable to our situation.

It is possible to give easy proofs of rather weak results about the $C_N(z)$. For example, suppose that $f(z)$ is the minimal polynomial of $C_N(\zeta_m)$ over $\mathbf{Q}$. Then $f(C_N(z))$ has ζ_m as a zero, and since its degree is $(\deg f)\cdot\varphi(N)$, we conclude that $\deg(C_N(\zeta_m))\geqq\varphi(m)/\varphi(N)$.

The engineering design problem described in Section 5 relates to a question of equalities among Fourier coefficients and among their moduli. The Fourier coefficients are of the form

$$b(\mu) = \prod_{\substack{h(\operatorname{mod} m)\\ h\not\equiv 1}}{}' \; (1-\mu^{h-1})^{-1}$$

where μ ranges over the primitive mth roots of unity. Propoisitions 3 and 4 are proved in Section 5. They provide relationships which together with Theorem 1 enable one to count the number of equalities as required. Each proposition concerns a primitive mth root of unity μ, a positive integer h, $(h,m)=1$ and any of the (infinite number of) primes p satisfying $p\equiv h \pmod m$.

Proposition 3. *The following are equivalent.*

1) $b(\mu)=b(\mu^h)$;

1′) $b(\mu^f)=b(\mu^g)$ *whenever* $(f,m)=1, fh\equiv g \pmod m$;

2) $C_{pm}(\mu)=p$;

2′) $\mu(pm,m)=1$.

Proposition 4. *The following are equivalent*:

1) $|b(\mu)|=|b(\mu^h)|$;

1′) $|b(\mu^f)=|b(\mu^g)|$ *whenever* $(f,m)=1,\ fh\equiv g \pmod m$;

2) $|C_{pm}(\mu)|=p$;

2′) $|u(pm,m)|=1$.

From these propositions and Theorem 1 one readily deduces that for a given m there are exactly $\varphi(m_1)$ distinct values for $b(\mu)$ and (when $m_1>1$) $\varphi(m_1)/2$ distinct values for $|b(\mu)|$. Indeed, using Theorem 1, Proposition 3 shows that $b(\mu^f)=b(\mu^g)$ if and only if $f\equiv g \pmod{m_1}$. Thus, there are as many distinct values for $b(\mu^h)$, $(h,m)=1$, as there are residue classes modulo m_1 of integers relatively prime to m, namely $\varphi(m_1)$. Similarly, Proposition 4 shows that (when $m_1>1$), there are one half as many values for $|b(\mu^h)|$, $(h,m)=1$, as there are such residue classes. In particular, all of the values of $b(\mu)$ are equal if and only if $m=2^\alpha$ and all of the values of $|b(\mu)|$ are equal and only if $m=2^\alpha 3^\beta$, for nonnegative integers α, β.

2. Preliminaries; Proofs of propositions 1 and 2 and parts of the theorems.

We start by recalling some elementary facts about roots of unity. First of all, if μ is a primitive mth root of unity and $(a,m)=1$ then there is an integer h satisfying $ah \equiv 1 \pmod m$ so

$$(1+\mu+\ldots+\mu^{a-1})(1+\mu^a+\ldots+\mu^{a(h-1)}) = (\mu^{ah}-1)/(\mu-1) = 1$$

whence $1+\mu+\ldots+\mu^{a-1}$ is a unit. If also v is a primitive mth root of unity then $v=\mu^a$ for some a, $(a,m)=1$. Thus

$$1-v = 1-\mu^a = (1-\mu)(1+\mu+\ldots+\mu^{a-1})$$

and consequently $1-v$ and $1-\mu$ are associates. From these simple facts it follows that p and $(1-\zeta_{p^\alpha})^{\varphi(p^\alpha)}$ are associates, as $p=C_{p^\alpha}(1)=\prod'_\alpha(1-\zeta^\alpha_{p^\alpha})$. On the other hand, if m is composite, then $1-\mu$ is a factor of $C_m(1)=1$ and thus is a unit.

The next observation is used to reduce the propositions and theorems to the square-free case $N=N_0$. (Recall that N_0 is the largest square-free factor of N and N_1 is the largest odd factor of N_0). As $C_N(z)=C_{N_0}(z^{N/N_0})$, it follows that

$$C_N(\zeta_m) = C_{N_0}(\zeta^b_k), \quad k = \frac{m}{(m, N/N_0)}, \tag{2.1a}$$

for some b, $(b,k)=1$. Since ζ_k and ζ^b_k are conjugates, so are $C_{N_0}(\zeta_k)$ and $C_{N_0}(\zeta^b_k)$. Thus, for any mth root of unity μ, $C_N(\mu)$ and $C_{N_0}(\zeta_k)$ are conjugates.

Furthermore, as $C_{2n}(z)=C_n(-z)$ when $2 \nmid n$, we can make the further reduction

$$C_{N_0}(\zeta_k) = C_{N_1}(-\zeta_k) \tag{2.1b}$$

if $2 \mid N_0$, where $-\zeta_k$ is a conjugate of ζ_{2k} if $2 \nmid k$, of ζ_k if $4 \mid k$ and of $\zeta_{k/2}$ if $k \equiv 2$ (mod 4).

The following lemma will be of general use.

LEMMA 2.2. *For $z \in \mathbf{C}$, $|z|=1$, $C_N(z) \neq 0$,*

$$2\operatorname{Arg} C_N(z) \equiv \varphi(N)\operatorname{Arg} z \pmod{2\pi}$$

when $N>1$ and $2\operatorname{Arg} C_1(z) \equiv \operatorname{Arg} z + \pi \pmod{2\pi}$.

PROOF. Write $C_N(z)=\sum_{i=0}^k a_i z^i$, $k=\varphi(N)$. The result is trivial for $N \leqq 2$, so assume $N>2$, whence $2 \mid \varphi(N)$. Let $H=k/2$. Since $a_i=a_{k-i}$,

$$\begin{aligned} C_N(z) &= z^H\left(a_H+\sum_{i=1}^{H} a_{H-i}(z^i+z^{-i})\right) \\ &= z^H\left(a_H+2\sum_{i=1}^{H} a_{H-i}\cos(i \operatorname{Arg} z)\right) \end{aligned}$$

and the result follows.

COROLLARY 2.3. *Suppose N and m are distinct positive integers, $N>1$. Then $C_N(\zeta_m) \in \mathbf{R}$ if and only if $m \mid \varphi(N)$.*

This yields our claim of Theorem 2 that $C_N(\zeta_m) \notin \mathbf{R}$ if m is sufficiently large.

Another useful observation is that if $\alpha, \beta \in \mathbf{Q}(\zeta_m)$, then for any automorphism σ,

$$|\alpha| = |\beta| \Rightarrow |\sigma(\alpha)| = |\sigma(\beta)| . \tag{2.4}$$

Indeed, if $|\alpha|=|\beta|$ then $\alpha\bar{\alpha}=\beta\bar{\beta}$, so $\sigma(\alpha)\sigma(\bar{\alpha})=\sigma(\alpha\bar{\alpha})=\sigma(\beta\bar{\beta})=\sigma(\beta)\sigma(\bar{\beta})$. Since $\sigma(\zeta_m)=\zeta_m^a$ for some a, $(a,m)=1$, σ commutes with complex conjugation, so $\sigma(\alpha)\overline{\sigma(\alpha)}=\sigma(\beta)\overline{\sigma(\beta)}$, proving (2.4). A consequence of this observation is the fact that if $\alpha \in \mathbf{Q}(\zeta_m)$ and $|\alpha|=1$ then each conjugate of α has modulus 1; thus, if α is integral over $\mathbf{Q}$, α must be a root of unity by Kronecker's theorem [11].

We now prove the first two propositions.

PROOF OF PROPOSITION 1. Writing

$$C_N(\zeta_m) = \prod_{a(\bmod N)}' (\zeta_m-\zeta_N^a) = \zeta_m^{\varphi(N)} \prod{}' (1-\zeta_N^a\zeta_m^{-1})$$

we see from the preliminary remarks that $C_N(\zeta_m)$ is determined up to a unit by the number of factors in this product for which $\zeta_N^a\zeta_m^{-1}$ has prime power order. In other .words, it suffices to determine for which a, $(a,N)=1$, $1 \leqq a<N$,

$$\frac{a}{N}-\frac{1}{m} = \frac{b}{p^\alpha} \tag{2.5}$$

for a prime p, $\alpha>0$ and $(b,p)=1$. It is then easy to see that (2.5) does not hold if N/m is not a positive or negative power of the prime p, and that if N/m is such a power, then (2.5) occurs just the right number of times to yield the assertion of Proposition 1.

Proof of Proposition 2. From (2.1) and the remarks which follow it, we see that $u(N,m)$ is a conjugate of $u(N',\hat{m})$. Let $N^*=N'/p$. Then

$$C_{N'}(z) = \prod_{d\mid N'} (z^{N'/d}-1)^{\mu(d)} = \prod_{d\mid N^*} \left(\frac{z^{N'/d}-1}{z^{N^*/d}-1}\right)^{\mu(d)} \tag{2.7}$$

If $p\equiv 1 \pmod{\hat{m}}$, then

$$\zeta_{\hat{m}}^{N'/d}-1 = \zeta_{\hat{m}}^{N^*/d}-1\,,$$

and so each of the terms in the last product above is 1 when we set $z=\zeta_{\hat{m}}$, except when $\zeta_{\hat{m}}^{N^*/d}=1$ for some value of d, in which case

$$\lim_{z\to\zeta_{\hat{m}}} \frac{z^{N'/d}-1}{z^{N^*/d}-1} = p\,. \tag{2.8}$$

Thus

$$C_{N'}(\zeta_{\hat{m}}) = \prod_{\substack{d\mid N^*\\ \hat{m}\mid N^*/d}} p^{\mu(d)} = \begin{cases} p & \text{if } N^*=\hat{m}\,,\\ 1 & \text{otherwise}\,,\end{cases}$$

which proves the first part of the proposition.

If $p\equiv -1 \pmod{\hat{m}}$, then

$$\zeta_{\hat{m}}^{N'/d}-1 = -\zeta_{\hat{m}}^{-N^*/d}(\zeta_{\hat{m}}^{N^*/d}-1)\,,$$

while (2.8) still holds for those d for which $\zeta_{\hat{m}}^{N^*/d}=1$. Hence (2.7) yields

$$\begin{aligned} C_{N'}(\zeta_{\hat{m}}) &= \prod_{d\mid N^*} (-\zeta_{\hat{m}}^{-N^*\mu(d)/d})\cdot \prod_{\substack{d\mid N^*\\ \hat{m}\mid N^*/d}} (-p)^{\mu(d)}\\ &= (-1)^{\alpha}\zeta_{\hat{m}}^{b}(-p)^{c}\,,\end{aligned}$$

where

$$a = \sum_{d\mid N^*} \mu(d) = \begin{cases} 1 & \text{if } N^*=1\,,\\ 0 & \text{otherwise}\,,\end{cases}$$

$$b = -N^* \sum_{d\mid N^*} \frac{\mu(d)}{d} = -\varphi(N^*)\,,$$

$$c = \sum_{\substack{d\mid N^*\\ \hat{m}\mid N^*/d}} \mu(d) = \begin{cases} 1 & \text{if } N^*=\hat{m}\,,\\ 0 & \text{otherwise}\,.\end{cases}$$

We now apply Proposition 2 to prove part of Theorem 1. Since $C_{p^{\alpha}m}(\zeta_{p^{\beta}m})$

$=C_{p^{\alpha-\beta}m}(\zeta_m)$, we may assume $\beta=0$. By the reductions (2.1), if $N=p^\alpha m$, $p \nmid m$, then

$$C_N(\zeta_m) \;=\; C_{pm_1}(\zeta_{m_1}^a), \qquad (a,m)=1\ ,$$

which is a conjugate of $C_{pm_1}(\zeta_{m_1})$. If we now apply Proposition 2, we obtain the forward implications of i) and ii).

The remainder of Theorem 1 will follow from the forward implication and second part of iii). In the next two sections it will be shown that if $p \not\equiv \pm 1$ $(\mathrm{mod}\, m_1)$, then the conjugates of $u(pm_1, m_1)$ have $\varphi(m_1)/2$ distinct absolute values which by (2.4) are then necessarily different from 1. Since by Lemma 2.2 $u(pm_1,m_1) \in \mathsf{R}$ if and only if $m_1 \mid \varphi(pm_1)$ (which happens, for example, for $m_1=21$, $p=29$), the remainder of the theorem follows from the fact that when $u=u(pm_1,m_1) \in \mathsf{R}$, then $u=\bar{u}$.

Note that in the special case that $m=2^\alpha 3^\beta q^\gamma$ for a prime q it is an easy computation to prove the converse of i). Indeed, by (2.2), when $m_1=q$, $q \mid \varphi(pq)$ so $m_1 \mid (p-1)$. Similarly for $m_1=3$. Otherwise, $m_1=3q$ so

$$3q \mid (p-1)(q-1) \;\Rightarrow\; q \mid (p-1) \;\Rightarrow\; 3p \;\equiv\; 3 \;\; (\mathrm{mod}\, m_1)\ .$$

Also, $3 \mid (p+1)$ or $3 \mid (p-1)$ so $pq \equiv \pm q$ $(\mathrm{mod}\, m_1)$ and $|1-\zeta_{m_1}^q| = |1-\zeta_{m_1}^{pq}|$. This implies that if $p=C_{pm_1}(\zeta_{m_1})$ then

$$|1-\zeta_{m_1}^p| \;=\; |1-\zeta_{m_1}| \;\Rightarrow\; p \;\equiv\; \pm 1 \;\; (\mathrm{mod}\, m_1)\ .$$

If $p \equiv -1$ $(\mathrm{mod}\, m_1)$ then $q \mid (p+1)$ so $q=2$, a contradiction.

3. Analytic expansions.

In this section we will start the proof of the remaining parts of theorems 1 and 2, which will then be proved completely in Section 4. We will show that if

$$|C_N(\zeta_m| \;=\; |C_N(\zeta_m^h)| \tag{3.1}$$

holds for some h, $(h,m)=1$, then some very stringent conditions must be satisfied. The basic fact we will use was already noted in Section 2, namely if (3.1) holds for some h, then

$$|C_N(\zeta_m^b)| \;=\; |C_N(\zeta_m^{hb})| \tag{3.2}$$

for any $b \in \mathsf{Z}$, $(b,m)=1$. But then if χ is any character modulo m, we obtain from (3.2) the fact that

$$\sum_{b (\mathrm{mod}\, m)}{}' \chi(b) \log |C_N(\zeta_m^b)| \;=\; \sum_{b (\mathrm{mod}\, m)}{}' \chi(b) \log |C_N(\zeta_m^{hb})|\ . \tag{3.3}$$

(Conversely, if (3.3) holds for all characters χ modulo m, then (3.2) holds for all

b with $(b,m)=1$.) In order to obtain a contradiction from (3.3), we need to evaluate the sums on the two sides of (3.3). By the reductions of Section 2, we can assume $N=N_0$.

PROPOSITION 3.4. *Let N be square-free, $m \in \mathbf{Z}^+$, $k \in \mathbf{Z}$, $(k,m)=1$, and let χ be a character modulo m which is induced by a character χ' which is primitive modulo m', $m' \neq 1$. Set $m''=m/m'$and assume that m'' is square-free and that $(m',m'')=1$. Then*

$$\sum_{b \pmod m}{}' \chi(b)\log|C_N(\zeta_m^{kb})| = \bar{\chi}(k)\,d(\chi)\,,$$

where

$$d(\chi) = -\tfrac{1}{2}\{1+\chi(-1)\}\cdot L(1,\bar{\chi}')\cdot\chi'(m'')\cdot G(1,\chi')\mu(m'')\mu(N)\cdot$$
$$\cdot\prod_{p\mid Nm''}(1-\bar{\chi}'(p)p^{-1})$$

(3.5)
$$\cdot\prod_{\substack{p\mid N\\ p\mid m''}}\left\{1+\frac{\bar{\chi}'(p)(p-1)^2}{p-\bar{\chi}'(p)}\right\}\cdot\prod_{\substack{p\mid N\\ p\nmid m''}}\left\{1-\frac{\bar{\chi}'(p)(p-1)}{p-\bar{\chi}'(p)}\right\}\cdot\prod_{\substack{p\mid m''\\ p\nmid N}}\left\{1-\frac{\bar{\chi}'(p)(p-1}{p-\bar{\chi}'(p)}\right\},$$

where $G(1,\chi')$ is the Gaussian sum of χ' and $L(s,\bar{\chi}')$ the Dirichlet L-series of $\bar{\chi}'$.

The most important fact about the expansion (3.5) is that only one term depends on k, and most of the terms are clearly nonzero. In particular, if (3.1) holds, then (3.3) and the above proposition imply that

$$\{\bar{\chi}(h)-1\}d(\chi) = 0\,.$$

Now $L(1,\bar{\chi}')$ is a finite nonzero number by Dirichlet's theorem, $G(1,\chi')$ is of absolute value $(m')^{1/2}$ [1, Chapter 8], $\chi'(m'')\neq 0$ since $(m',m'')=1$, and $\mu(m'')\mu(N)\neq 0$ since N and m'' are squarefree. Further, $1-\bar{\chi}'(p)p^{-1}\neq 0$ for any p, while

$$1+\frac{\bar{\chi}'(p)(p-1)^2}{p-\bar{\chi}'(p)} = 0$$

if and only if $p=3$ and $\chi'(3)=-1$. Finally,

$$1-\frac{\bar{\chi}'(p)(p-1)}{p-\bar{\chi}'(p)} = 0$$

if and only if $\chi'(p)=1$. Therefore if (3.1) holds for some h with $(h,m)=1$, and χ is any character modulo m that satisfies the hypotheses of Proposition 3.4, then one of the following must hold:

$$(3.6)\quad\begin{array}{ll}\text{a)} & \chi(-1)=-1\ ,\\ \text{b)} & \chi(h)=1\ ,\\ \text{c)} & 3\,|\,N,\ 3\,|\,m'',\ \text{and}\ \chi'(3)=-1\ ,\\ \text{d)} & \text{There is a prime } p\,|\,N,\ p\nmid m'', \text{ or else a prime } p\,|\,m'',\ p\nmid N, \text{ such that}\\ & \chi'(p)=1\ .\end{array}$$

In the next section we will show that under appropriate assumptions on N and m there is a character χ modulo m such that none of the conditions (3.6) hold for $h\not\equiv\pm 1 \pmod m$, which will complete the proofs of theorems 1 and 2. At this point let us note that the conditions (3.6) yield a procedure for constructing examples of N and m such that the degree of $C_N(\zeta_m)$ is small. This, in fact, was how the examples quoted in the introduction were discovered.

The hypotheses that m'' is square-free and that $(m',m'')=1$ were imposed in order to obtain simple evaluations of Gaussian and Ramanujan sums. These sums can also be evaluated explicitly without these requirements, but the resulting formulas are quite complicated and unwieldy. Since these general formulas are not needed for our results, we will not prove them there.

Proof of Proposition 3.4. We have

$$\begin{aligned}\sum_{b(\operatorname{mod} m')}{}' \chi(b)\log|C_N(\zeta_m^{kb})| &= \bar\chi(k) \sum_{b(\operatorname{mod} m)}{}' \chi(kb)\log|C_N(\zeta_m^{kb})|\\ &= \bar\chi(k) \sum_{b(\operatorname{mod} m)}{}' \chi(b)\log|C_N(\zeta_m^{b})|\ .\end{aligned}$$

This proves that the sum in the proposition is of the form $\bar\chi(k)d(\chi)$ for some $d(\chi)$. To evaluate $d(\chi)$ it will therefore suffice to evaluate the sum for $k=1$. Since

$$\log(1-z) = -\sum_{n=1}^{\infty} n^{-1}z^n$$

is (conditionally) convergent for $|z|=1$, $z\neq 1$, we have, for $(b,m)=1$,

$$\begin{aligned}\log|C_N(\zeta_m^b)| &= \log\left|\prod_{a(\operatorname{mod} N)}{}' (1-\zeta_N^a\zeta_m^{-b})\right|\\ &= -\sum_{a(\operatorname{mod} N)}{}' \operatorname{Re}\sum_{n=1}^{\infty}\frac{1}{n}\zeta_N^{an}\zeta_m^{-bn}\\ &= -\operatorname{Re}\sum_{n=1}^{\infty}\frac{1}{n}\zeta_m^{-bn}c_N(n)\ ,\end{aligned}$$

where

$$c_N(n) = \sum_{a(\mathrm{mod}\, N)}' \zeta_N^{an}$$

is a Ramanujan sum [1, Chapter 8], [7, Chapter 16], which is real. Hence

$$\log|C_N(\zeta_m^b)| = -\tfrac{1}{2} \sum_{n=1}^{\infty} n^{-1} c_N(n)\{\zeta_m^{bn} + \zeta_m^{-bn}\} ,$$

and therefore

$$\begin{aligned} S &= \sum_{b(\mathrm{mod}\, m)}' \chi(b) \log|C_N(\zeta_m^b)| \\ &= -\tfrac{1}{2} \sum_{n=1}^{\infty} n^{-1} c_N(n)\{G(n,\chi) + G(-n,\chi)\} , \qquad (3.7) \end{aligned}$$

where

$$G(r,\chi) = \sum_{b(\mathrm{mod}\, m)} \chi(b) \zeta_m^{br}$$

is a Gaussian sum [1, Chapter 8]. To proceed further, we need to evaluate $G(r,\chi)$.

LEMMA 3.8. *Let χ be a character modulo m which is induced by a primitive character χ' modulo m'. Let $m'' = m/m'$, and assume that $(m', m'') = 1$. Then*

$$G(r,\chi) = \chi'(m'')\bar{\chi}'(r) G(1,\chi') c_{m''}(r) .$$

PROOF. Since every b, $1 \leqq b \leqq m$, $(b,m) = 1$, can be written uniquely as

$$b = m'x + m''y, \quad \begin{array}{ll} 1 \leqq x \leqq m'', & (x, m'') = 1 , \\ 1 \leqq y \leqq m', & (y, m') = 1 , \end{array}$$

we have

$$\begin{aligned} G(r,\chi) &= \sum_{x(\mathrm{mod}\, m'')}' \sum_{y(\mathrm{mod}\, m')}' \chi(m'x + m''y) \exp\{2\pi i r(m'x + m''y)/m\} \\ &= \sum_{x(\mathrm{mod}\, m'')}' \sum_{y(\mathrm{mod}\, m')}' \chi'(m''y) \zeta_{m''}^{rx} \zeta_{m'}^{ry} \\ &= \chi'(m'') \sum_{y(\mathrm{mod}\, m')}' \chi'(y) \zeta_{m'}^{ry} \sum_{x(\mathrm{mod}\, m'')} \zeta_{m''}^{rx} \\ &= \chi'(m'') G(r,\chi') c_{m''}(r) . \end{aligned}$$

Since χ' is primitive modulo m', $G(r,\chi') = \bar{\chi}'(r) G(1,\chi')$ [1, Chapter 8], and this completes the proof of the lemma.

We now return to the proof of Proposition 3.4. Combining Lemma 3.8, (3.7) and the facts that $c_s(\gamma) = c_s(-\gamma)$ and that $c_s(rt) = c_s(r)$ for $(t,s) = 1$ yields

$$S = -\tfrac{1}{2} \sum_{n=1}^{\infty} n^{-1} c_N(n) \chi'(m'') G(1,\chi') c_{m''}(n) \{\bar{\chi}'(n) + \bar{\chi}'(-n)\}$$

$$= -\tfrac{1}{2} \chi'(m'') G(1,\chi') \{1 + \chi'(-1)\} \sum_{n=1}^{\infty} n^{-1} \bar{\chi}'(n) c_N(n) c_{m''}(n) .$$

If s is square-free, then [1, Chapter 8], [7, Chapter 16]

$$c_s(r) = \mu(s)\mu((r,s))\varphi((r,s)) ,$$

and so, since N and m'' are squarefree, we obtain

$$S = -\tfrac{1}{2}\chi'(m'')G(1,\chi')\{1+\chi'(-1)\}\mu(m'')\mu(N)H , \tag{3.9}$$

where

$$H = \sum_{n=1}^{\infty} n^{-1}\bar{\chi}'(n)\mu((N,n))\mu((m'',n))\varphi((N,n))\varphi((m'',n)) .$$

To evaluate H, we consider the Dirichlet series

$$H(s) = \sum_{n=1}^{\infty} n^{-s}\bar{\chi}'(n)\mu((N,n))\mu((m'',n))\varphi((N,n))\varphi((m'',n)) . \tag{3.10}$$

Since the series (3.10) for $H(s)$ is absolutely convergent for $s > 1$, and the coefficient of n^{-s} is a multiplicative function of n, $H(s)$ has the Euler product

$$H(s) = \prod_{\substack{p \mid N \\ p \mid m''}} P_1(p,s) \prod_{\substack{p \mid N \\ p \nmid m''}} P_2(p,s) \prod_{\substack{p \mid m'' \\ p \nmid N}} P_2(p,s) \prod_{\substack{p \nmid N \\ p \nmid m''}} [1 - \bar{\chi}'(p)p^{-s}]^{-1} , \tag{3.11}$$

where

$$P_1(p,s) = 1 + \bar{\chi}'(p)(p-1)^2[p^s - \bar{\chi}'(p)]^{-1}$$

and

$$P_2(p,s) = 1 - \bar{\chi}'(p)(p-1)[p^s - \bar{\chi}'(p)]^{-1} .$$

Since

$$\prod_{\substack{p \nmid N \\ p \nmid m''}} (1 - \bar{\chi}'(p)p^{-s})^{-1} = L(s,\bar{\chi}') \prod_{p \mid Nm''} (1 - \bar{\chi}'(p)p^{-s}) ,$$

and $L(1,\bar{\chi}')$ is analytic at $s=1$ for $m' \neq 1$ (if $m'=1$, $L(s,\bar{\chi}')$ is the Riemann zeta function, and its pole at $s=1$ is cancelled by one of the other factors in the product for $H(s)$) we can let $s \to 1$ in (3.10) to obtain

(3.12)
$$H = L(1,\bar{\chi}') \prod_{p \mid Nm''} (1 - \bar{\chi}'(p)p^{-1}) \prod_{\substack{p \mid n \\ p \mid m''}} P_1(p,1) \prod_{\substack{p \mid N \\ p \nmid m''}} P_2(p,1) \prod_{\substack{p \mid m'' \\ p \nmid N}} P_2(p,1) .$$

Proposition 3.4 then follows from (3.12) and (3.9).

4. Construction of special Dirichlet characters.

In this section we will demonstrate the existence of some special Dirichlet characters, which together with Proposition 3.4 will prove theorems 1 and 2. We consider the slightly easier Theorem 2 first.

A. Proof of Theorem 2. N is odd and squarefree by hypothesis. We wish to show that if m is large,

$$(4.1) \qquad |C_N(\zeta_m)| = |C_N(\zeta_m^h)|, \quad (h,m) = 1$$

implies that $h \equiv \pm 1 \pmod m$. Suppose therefore that (4.1) holds for some h, $h \not\equiv \pm 1 \pmod m$. Then, as we pointed out in Section 3, Proposition 3.4 implies that if χ is any character modulo m which is induced by a primitive character χ' modulo m', and $m' \neq 1$, $m'' = m/m'$, m'' is squarefree, $(m', m'') = 1$, then at least one of the conditions (3.6) holds. We will show that one can find a character χ such that none of the conditions (3.6) holds. We will choose χ such that $m' = m$, $m/2$, or $m/3$. Our proof will use the following auxiliary results:

Lemma 4.2. *Let $k_1, \ldots, k_r$ be any r distinct integers, with $k_j \geqq 2$ for all j. Then there is a $B = B(k_1, \ldots, k_r)$ such that for any nonzero complex numbers $c_1, \ldots, c_r$ and for any $p^\alpha > B$, $(k,p) = 1$, $k \not\equiv \pm 1 \pmod{p^\alpha}$, $\varepsilon = \pm 1$, and $c \in \mathbf{C} - \{-1\}$, there is a primitive character χ modulo p^α such that $\chi(k_j) \neq c_j$ for $1 \leqq j \leqq r$, $\chi(-1) = \varepsilon$, and $\chi(k) \neq c$. Unless $p = 2$ and $k \equiv 2^{\alpha-1} + 1 \pmod{2^\alpha}$, the conclusions of the lemma hold also if $c = -1$.*

Lemma 4.3. *If p is a prime, $\alpha \in \mathbf{Z}^+$, $p^\alpha \neq 2$, $(k,p) = 1$, $k \not\equiv 1 \pmod{p^\alpha}$, then $\chi(k)$ takes on at least two distinct values as χ varies over the primitive characters modulo p^α, unless* i) *$p^\alpha = 3$ and $k \equiv -1 \pmod 3$*, or ii) *$p = 2$, $\alpha \geqq 2$, and $k \equiv 2^{\alpha-1} + 1 \pmod{2^\alpha}$*.

Lemmas 4.2 and 4.3 will be proved later; we now use them to complete the proof of Theorem 2. Suppose that

$$\{k_1, \ldots, k_r\} = \{p : p \mid N\} \cup \{2,3\}.$$

Let $B = B(k_1, \ldots, k_r)$ be given by Lemma 4.2. There is a $B_1 = B_1(B)$ such that if $n \geqq B_1$, then there is a prime power $p^\alpha > B^\alpha$, $p^\alpha \mid n$.

Let us suppose that $m \geqq 100B_1$, and let p^α be a prime power such that $p^\alpha \mid m$, $p^{\alpha+1} \nmid m$, $p^\alpha > B$. Suppose that (4.1) holds for some h, $(h,m) = 1$, $h \not\equiv \pm 1 \pmod m$. We distinguish 3 cases.

a) $h \not\equiv \pm 1 \pmod{p^\alpha}$. If p is odd, we set $m' = m/2$ if $m \equiv 2 \pmod 4$ and $m' = m$ otherwise, and $m^* = m' p^{-\alpha}$. Let ψ be any primitive character modulo m^*. By

Lemma 4.2 applied with $k=h$, there is a primitive character ξ modulo p^α such that

$$\xi(h)\psi(h) \neq 1 ,$$

$$\xi(-1)\psi(-1) = 1 ,$$

$$\psi(q)\xi(q) \neq 1 \quad \text{for } q=2 \text{ and for primes } q \mid N .$$

But then $\chi'=\xi\psi$ is a primitive character modulo m' which satisfies none of the conditions (3.6), and thus gives the desired contradiction.

We next assume that $p=2$. Here we take $m'=m/3$ if $m\equiv 3 \pmod 9$ and $m'=m$ otherwise. We now choose (with the help of Lemma 4.3) a primitive character ψ modulo $m'2^{-\alpha}$ such that $\psi(h)\neq -1$. But then Lemma 4.2 again allows us to choose a primitive character ξ modulo 2^α such that $\chi'=\xi\psi$ does not satisfy any of the conditions (3.6).

b) $h\equiv 1 \pmod{p^\alpha}$. If we try to set $m'=m/2$ if $m\equiv 2 \pmod 4$ and $m'=m$ otherwise, then by Lemma 4.3 we will obtain the desired χ' if we can find a primitive character ψ mod $m'p^{-\alpha}$ such that $\psi(h)\neq 1$. If $m'=m/2$, then $h\equiv \pm 1 \pmod{m'}$ implies that $h\equiv m/2\pm 1 \pmod m$, and so $(h,m)\geqq 2$, which is a contradiction. Hence $h\not\equiv \pm 1 \pmod{m'}$. Therefore, in view of Lemma 4.3, the only way this approach can fail is if for each prime power $q^\beta \mid m'$, $q^{\beta+1} \nmid m'$, there is only a single choice of $\delta(h)$ as δ runs through the primitive characters modulo q^β, and if there are exacly two such prime powers q^β for which $\delta(h)=-1$ is the only possibility. But this means that those two prime powers are $2^\gamma \geqq 4$ and 3, and we must have $m\not\equiv 2 \pmod 4$, $h\equiv 2^{\gamma-1}+1 \pmod{2^\gamma}$, $h\equiv -1 \pmod 3$, while $h\equiv 1 \pmod{q^\beta}$ for all other prime powers $q^\beta \mid m'$. In this case we set $m'=m/3$ to obtain the desired results.

c) $h\equiv -1 \pmod{p^\alpha}$. In this case $-h\equiv 1 \pmod{p^\alpha}$, $-h\not\equiv \pm 1 \pmod m$; so by case b) above we can find a primitive character χ' modulo m', $m'=m$, $m/2$, or $m/3$, for which none of the conditions of (3.6) is satisfied when we replace h by $-h$ in them. But $\chi'(-1)=1$ means that $\chi'(h)=\chi'(-h)$, and so χ' violates all of the conditions (3.6).

Since this covers all of the cases, we have completed the proof of Theorem 2 by showing that (4.1) cannot occur for $h\not\equiv \pm 1 \pmod m$.

Proof of Lemma 4.2. Let us first suppose that p is odd. If $(k_j,p)\neq 1$ for some j, then $\chi(k_j)=0\neq c_j$ for any character χ modulo p^α. We may therefore assume $(k_j,p)=1$ for all j.

Pick a primitive root g modulo p^α. Then any n with $(n,p)=1$ can be written uniquely as

$$n \equiv g^{b(n)} \pmod{p^\alpha}, \qquad 1 \leqq b(n) \leqq \varphi(p^\alpha)\,, \tag{4.4}$$

and characters χ modulo p^α are then given [1, Chapter 10] by

$$\chi^{(t)}(n) = \exp\left\{\frac{2\pi i}{\varphi(p^\alpha)}\,b(n)t\right\}, \qquad 1 \leqq t \leqq \varphi(p^\alpha)\,. \tag{4.5}$$

A character $\chi^{(t)}$ is primitive if and only if $(t,p)=1$. As t varies, $\chi^{(t)}(n)$ takes on exactly $e(n)$ values, where $e(n)=\varphi(p^\alpha)/(b(n),\varphi(p^\alpha))$ is the multiplicative order of n modulo p^α, and each of those values is taken on $\varphi(p^\alpha)/e(n)$ times. Thus the condition that $\chi^{(t)}(n) \neq c'$ for some c' rules out at most $\varphi(p^\alpha)/e(n)$ possible values of t. This number will be small if $e(n)$ is large. However,

$$n^{e(n)} \equiv 1 \pmod{p^\alpha}$$

implies that $|n|^{e(n)} \geqq p^\alpha - 1$. Hence if we choose B_3 such that

$$\log B_3 > 100r \cdot \max_{1 \leqq j \leqq r} \log |k_j|\,,$$

then the total number of characters χ modulo p^α, $p^\alpha > B_3$, for which $\chi(k_j)=c_j$ for some j will be

$$\leqq \sum_{j=1}^{r} \frac{\varphi(p^\alpha)}{e(k_j)} < \frac{1}{40}\varphi(p^\alpha)\,.$$

Since there are $p-2$ primitive characters modulo p and $p^{\alpha-2}(p-1)^2$ modulo p^α for $\alpha \geqq 2$, this means that most of the characters χ have $\chi(k_j) \neq c_j$ for $1 \leqq j \leqq r$.

We next consider the conditions that $\chi(-1)=\varepsilon$ and χ be primitive. We have $\chi(-1)=\varepsilon$ precisely when $t \equiv (1-\varepsilon)/2 \pmod 2$, while χ is primitive when $t \not\equiv 0 \pmod p$ if $\alpha \geqq 2$, and when $t \neq p-1$ for $\alpha = 1$. Since p is odd, this yields $p^{\alpha-2}(p-1)^2/2$ primitive characters χ with $\chi(-1)=\varepsilon$ if $\alpha \geqq 2$, and $(p-1)/2$ or $(p-3)/2$ such characters if $\alpha=1$.

The total number of characters χ modulo p^α for which $\chi(k)=c$ or $\chi(k_j)=c_j$ for some j is

$$\leqq p^{\alpha-1}(p-1)\left[\frac{1}{40}+\frac{1}{e(k)}\right].$$

Note that since p is odd and $k \not\equiv \pm 1 \pmod{p^\alpha}$, $e(k) \geqq 3$. If $\alpha=1$ and $p \geqq B_4$ for some large B_4, then this number is less than $(p-3)/2$, which is a lower bound for the total number of primitive character with $\chi(-1)=\varepsilon$, and so a character with the properties specified in the lemma exists. Suppose now that $\alpha \geqq 2$. Then it will again suffice to prove that

$$p^{\alpha-1}(p-1)\left[\frac{1}{40}+\frac{1}{e(k)}\right] < \frac{1}{2}p^{\alpha-2}(p-1)^2\,.$$

This is clearly true for all odd primes p and all $e(k) \geqq 3$, except for $p=3$ and $e(k)=3$. If $p=3$ and $e(k)=3$, we use a refinement of the earlier argument. The condition that $\chi(k) \neq c$ is equivalent to requiring that $t \neq x \pmod 3$ for some x (depending on c only). Since χ is primitive for $t \neq 0 \pmod 3$, χ will be primitive and satisfy $\chi(k) \neq c$ if $t \equiv y \pmod 3$ for some y. Therefore χ will be primitive and satisfy both $\chi(k) \neq c$ and $\chi(-1) = \varepsilon$ for t lying in precisely one residue class modulo 6. Since for p^α large we have

$$\tfrac{1}{40}\varphi(p^\alpha) < \tfrac{1}{6}\varphi(p^\alpha) - 1 ,$$

the desired character χ exists in this case also.

The above arguments prove Lemma 4.2 for p odd. (We need to note that the requirement that $c \neq 1$ was not used in that case.) If $p=2$ (but α is large, as we shall assume), there are no primitive roots modulo 2^α, but every odd n can be written uniquely as [1, Chapter 10]

$$n \equiv (-1)^{(n-1)/2} 5^{b(n)} \pmod{2^\alpha}, \qquad 1 \leqq b(n) \leqq 2^{\alpha-2} ,$$

and the characters χ modulo 2^α are given by

$$\chi^{(a,t)}(n) = (-1)^{a(n-1)/2} \exp\left\{\frac{2\pi i}{2^{\alpha-2}} b(n)t\right\}, \qquad 0 \leqq a \leqq 1,\ 1 \leqq t \leqq 2^{\alpha-2} .$$

Here $\chi^{(\alpha,t)}$ is primitive precisely when $t \equiv 1 \pmod 2$. The rest of the proof is quite similar to the case of p odd, but easier, and is omitted. We should note, however, that in this case $e(k)=2$ occurs for $k \equiv 2^{\alpha-1} \pm 1 \pmod{2^\alpha}$, and that if $k \equiv 2^{\alpha-1}+1 \pmod{2^\alpha}$, all the primitive characters χ modulo 2^α have $\chi(k) = -1$, which accounts for the requirement that $c \neq -1$.

Proof of Lemma 4.3. Suppose that p is odd. Let $e(k)$ be the multiplicative order of k modulo p^α. If $e(k)=2$, then $k \equiv -1 \pmod{p^\alpha}$, and the assertion of the lemma is clearly true. If $e(k) \geqq 3$, then $\chi(k)$ takes on $e(k)$ different values, each one $p^{\alpha-1}(p-1)/e(k)$ times, as χ runs through all the characters modulo p^α. Since there are $p-2$ primitive characters if $\alpha=1$ and $p^{\alpha-2}(p-1)^2$ if $\alpha \geqq 2$, this again proves the lemma. The proof for $p=2$ is similar.

B. Proof of Theorem 1. It remains to show that for m odd and square-free and $N=pm$, where p is a prime with $(p,m)=1$, $p \neq \pm 1 \pmod m$, if (4.1) holds, then $h \equiv \pm 1 \pmod m$.

If χ is any character modulo m, which is induced by a primitive character χ' modulo m', then (since m is squarefre) $m'' = m/m'$ is squarefree and $(m', m'')=1$. Furthermore, since $m'' \mid N$, there are no primes q with $q \mid m''$, $q \nmid N$, while if $q \mid N$, $q \nmid m''$, then either $q=p$ or else $q \mid m'$, and in the latter case $\chi'(q)=0$. Hence in the present situation condition (3.6.d) is equivalent to $\chi(p)=1$. Thus if (4.1) holds for $h \not\equiv \pm 1 \pmod{m}$, and $m' \neq 1$, then at least one of the following conditions must hold:

a) $\chi'(-1) = -1$,
b) $\chi'(h) = 1$,
c) $3 \mid m''$ and $\chi'(3) = -1$,
d) $\chi'(p) = 1$.

The desired contradiction which proves Theorem 1 now follows from the following result.

Proposition 4.6. *Let m be an odd, squarefree positive integer, and let h_1 and h_2 be two (not necessarily distinct) integers such that $(h_j, m) = 1$ and $h_j \not\equiv \pm 1 \pmod{m}$ for $1 \leqq j \leqq 2$. Then there exists a primitive character χ modulo m', $m' \mid m$, $m' \neq 1$, such that $\chi(-1) = 1$, $\chi(h_1) \neq 1$, $\chi(h_2) \neq 1$, and if $3 \mid (m/m')$, then $\chi(3) \neq -1$.*

Proof of Proposition 4.6. We consider several cases.

i) There is a prime $q \mid m$ such that $h_j \not\equiv \pm 1 \pmod{q}$ for $j = 1$ and 2. Since $h_1 \not\equiv \pm 1 \pmod{q}$, $(h_1, q) = 1$, we must have $q \geqq 5$. We let $m' = q$ and choose χ to be a primitive character modulo q given by

$$\chi(n) = \exp\left\{\frac{4\pi i}{q-1} b(n)\right\}, \qquad (n, q) = 1 ,$$

where

$$n \equiv g^{b(n)} \pmod{q}$$

for some fixed primitive root g modulo q (cf. (4.4)–(4.5)). Since $q \neq 3$, χ is primitive. Moreover, $\chi(k) = 1$ means that $b(k) \equiv 0 \pmod{(q-1)/2}$, which occurs only for $k \equiv \pm 1 \pmod{q}$. If $3 \nmid m$, this completes the proof of this case. Suppose therefore that $3 \mid m$ and that $\chi(3) = -1$ for the character defined above. Then $4b(3)/(q-1)$ must be an odd integer, and therefore the multiplicative order of 3 modulo q must divide 4. Since there is no odd prime dividing $3^2 - 1 = 8$, we conclude that 3 has order 4 modulo q, and hence $q = 5$. In this case we let $m' = 15$ and find that the character χ modulo 15 defined by $\chi(2) = -i$, $\chi(4) = -1$, $\chi(7) = i$, $\chi(-1) = 1$ satisfies all the conditions of the Proposition.

ii) There is a prime $q \mid m$ such that $h_1 \not\equiv \pm 1 \pmod{q}$, but $h_2 \equiv 1 \pmod{q}$. (This case also covers the situation where $h_2 \equiv -1 \pmod{q}$, since the proof to be presented below, when applied to the case of h_2 replaced by $-h_2 \equiv 1 \pmod{q}$, produces a character χ with $\chi(h_2) = \chi(-h_2) \neq 1$.) Since $h_2 \not\equiv 1 \pmod{m}$, there is a prime $q' \mid m$ such that $h_2 \not\equiv 1 \pmod{q'}$. If $3 \mid m$, $h_2 \not\equiv 1 \pmod{3}$, we take $q' = 3$. We now distinguish two subcases.

a) Either $3 \mid m$ and $h_2 \not\equiv 1 \pmod 3$ or else $3 \nmid m$. In this case we take $m' = qq'$. Since $3 \nmid m''$, we only have to ensure that $\chi(-1) = 1$, $\chi(h_1) \neq 1$, $\chi(h_2) \neq 1$. Let ψ be a primitive character modulo q' such that $\psi(h_2) \neq 1$, $\psi(-1) = -1$. Since $q \geqq 5$, and $h_1 \not\equiv \pm 1 \pmod q$, $\delta(h_1)$ takes on at least 2 values as δ runs through those primitive characters δ modulo q for which $\delta(-1) = -1$. Choose that δ for which $\delta(h_1)\psi(h_1) \neq 1$. Then $\chi = \delta\psi$ is a primitive character modulo $m' = qq'$ which satisfies all the required properties.

b) $3 \mid m$ and $h_2 \equiv 1 \pmod 3$. In this case we will take $m' = qq'$ or $m' = 3qq'$. Let ξ denote the only primitive character modulo 3, and let ψ denote a primitive character modulo q'. If $q \geqq 7$, we take $m' = 3qq'$ and we choose ψ so that $\psi(-1) = -1$ and $\psi(h_2) \neq 1$. Since there are at least two choices of $\delta(h_1)$ for a primitive character δ modulo q with $\delta(-1) = 1$, we choose that δ for which $\chi = \delta\psi\xi$ satisfies $\chi(h_1) \neq 1$. The properties $\chi(h_2) \neq 1$ and $\chi(-1) = 1$ will then hold automatically, while $3 \nmid (m/m')$. If $q = 5$, and $h_2 \not\equiv -1 \pmod{q'}$, we select $m' = 3qq'$, and we choose a ψ with $\psi(-1) = 1$ and $\psi(h_2) \neq 1$, and then select one of the two possible choices of δ with $\delta(-1) = -1$ so that $\chi = \delta\psi\xi$ satisfies $\chi(h_1) \neq 1$. This χ then again satisfies the claims of the Proposition. Finally, if $q = 5$ and $h_2 \equiv -1 \pmod{q'}$, we choose $m' = qq'$ and set $\chi = \delta\psi$, where $\psi(-1) = -1$, and choose δ to be one of the two primitive characters modulo 5 with $\delta(-1) = -1$ so that $\chi(h_1) \neq 1$. Then $\chi(h_1) \neq 1$, $\chi(h_2) = -1$, and $\chi(-1) = 1$. This χ will fail to work only if $\chi(3) = -1$. However, $\delta(3) = \varepsilon$ for $\varepsilon = \pm i$ so $\chi(3) = -1$ will occur only if $\psi(3) = \delta(3) = \varepsilon$. We need to show that in fact one can choose ψ with $\psi(-1) = -1$ and $\psi(3) \neq \varepsilon$. This, however, is obvious, since if $\psi(-1) = -1$ and $\psi(3) = \varepsilon$, then $\bar{\psi}(-1) = -1$ and $\bar{\psi}(3) = -\varepsilon$. Thus in this case also we can find a suitable χ by selecting $\chi = \delta\bar{\psi}$.

iii) The final case to consider is when there is no prime $q \mid m$ such that $h_1 \not\equiv \pm 1 \pmod q$. Since the roles of h_1 and h_2 are interchangeable, we can also assume that there is no prime $q \mid m$ such that $h_2 \not\equiv \pm 1 \pmod q$; i.e., for every $q \mid m$, $h_j \equiv \pm 1 \pmod q$ for $j = 1$ and 2. We again need to consider subcases.

a) There are primes $q_1 \mid n$ and $q_2 \mid n$ such that

$$h_1 \equiv 1 \pmod{q_1}, \qquad h_2 \equiv -1 \pmod{q_1},$$

$$h_1 \equiv -1 \pmod{q_2}, \qquad h_2 \equiv 1 \pmod{q_2}.$$

We let δ_j for $1 \leqq j \leqq 2$ be a primitive character modulo q_j such that $\delta_j(-1) = -1$. Then $\chi = \delta_1\delta_2$ is a primitive character modulo $m' = q_1q_2$ which satisfies $\chi(h_1) = \chi(h_2) = -1$, $\chi(-1) = 1$. Furthermore, if $3 \neq q_2$ then as δ_2 varies over the primitive characters modulo q_2 which satisfy $\delta_2(-1) = -1$, $\delta_2(3)$ assumes at least two values, so by an appropriate choice of δ_2 we can ensure that $\chi(3) \neq -1$, no matter what the choice of δ_1 is.

b) There is no prime $q \mid m$ such that

$$h_1 h_2 \equiv -1 \pmod{q} .$$

Then for every $q \mid m$ we must have $h_1 \equiv h_2 \equiv \pm 1 \pmod{q}$. Since $h_i \not\equiv \pm 1 \pmod{m}$, this means that there are primes $q_1 \mid m$ and $q_2 \mid m$ such that

$$h_1 \equiv h_2 \equiv 1 \pmod{q_1} ,$$

$$h_1 \equiv h_2 \equiv -1 \pmod{q_2} .$$

We set $m' = q_1 q_2$ and choose $\chi = \delta_1 \delta_2$ as in the preceding case.

5. $C_{pm}(\zeta_m) = p$ and equality among Fourier coefficients.

This section examines the special equalities $C_{pm}(\zeta_m) = p$ (equivalently, $u(pm,m) = 1$) and $|C_{pm}(\zeta_m)| = p$ (equivalently, $|u(pm,m)| = 1$) in terms of their respetive relationships to equalities among certain Fourier coefficients and among their moduli. The Fourier coefficients in question are those of the periodic function $x(n)$ defined recursively by

$$x(n) = \sum_{i=1}^{k} a_i x(n-i) , \tag{5.1}$$

where the a_i's are the coefficients of $C_m(z) = z^k - \sum_{i=1}^k a_i z^{k-i}$. Interest in equalities among these Fourier coefficients and among their moduli derives from an applied problem [8] concerning determination of the phase and power distributions in a class of recursive linear digital filters modelled by (5.1). The fewer the number of values assumed by these coefficients and their moduli, the more uniform are the phase and power distributions.

Let m be a fixed positive integer, let μ be any fixed primitive mth root of unity and set $k = \varphi(m)$. Define

$$b(z) = \prod_{\substack{h \pmod{m} \\ h \neq 1}}' (1 - z^{h-1})^{-1} .$$

(It is shown in [8] that $\{b(\mu^h) \mid (h,m) = 1\}$ is the set of nonzero Fourier coefficients of $x(n)$.) The derivative $C'_m(\mu) = \mu^{k-1} b(\mu)^{-1}$, and it follows that for $(h,m) = 1$,

$$b(\mu) = b(\mu^h) \Leftrightarrow \lim_{z \to \mu} \frac{h\mu^{k(h-1)} C_m(z) - C_m(z^h)}{z - \mu} = 0 . \tag{5.2}$$

Note. As $b(\mu) = b(\mu^h) \Leftrightarrow \mu^{(1-k)} C'_m(\mu) = \mu^{h(1-k)} C'_m(\mu^h)$, this holds if and only if $\mu^{(1-k)} C'_m(\mu)$ is in the fixed field of the cyclic group of automorphisms of $\mathbf{Q}(\mu)/\mathbf{Q}$ generated by σ_h where $\sigma_h(\mu) = \mu^h$. Thus, for $m_1 > 1$, not all of the coefficients

$b(\mu^h)$ can be equal, as that would imply that $\mu^{(1-k)}C'_m(\mu)$ were in the fixed field of $\{\sigma_h \mid (h,m)=1\}$; as this is the full group of automorphisms of $\mathbf{Q}(\mu)/\mathbf{Q}$, the implication is that for some $q \in \mathbf{Q}$, μ is a zero of $f(z)=C'_m(z)-qz^{k-1}$. But $f \not\equiv 0$ since $m_1>1$, contradicting the fact that $\deg \mu \equiv k$.

For $(h,m)=1$, let p be a prime satisfying $p \equiv h \pmod m$ (there exist infinitely many such primes by the Dirichlet Theorem on primes in arithmetic progressions [1]). Using the relation $C_{pm}(z)C_m(z)=C_m(z^p)$, it follows from (5.2) that

$$b(\mu) = b(\mu^h) \Leftrightarrow C_{pm}(\mu) = p\mu^{k(p-1)} .$$

However, by Lemma 2.2, if $C_{pm}(\mu)=p\mu^{k(p-1)}$, when $m>1$,

$$\varphi(pm)\operatorname{Arg}\mu \equiv 2\varphi(pm)\operatorname{Arg}\mu \pmod{2\pi}$$

so $m \mid \varphi(pm)=k(p-1)$ whence $C_{pm}(\mu)=p$. On the other hand, if $C_{pm}(\mu)=p$ $(m>1)$ then

$$\varphi(pm)\operatorname{Arg}\mu \equiv 0 \pmod{2\pi}$$

so $m \mid \varphi(pm)=k(p-1)$ and $C_{pm}(\mu)=p\mu^{k(p-1)}$. We have thus proved Proposition 3.

To prove Proposition 4, note that analogous to the derivation of (5.2),

$$|b(\mu)| = |b(\mu^h)| \Leftrightarrow \lim_{z\to\mu} p\left|\frac{C_m(z)}{z-\mu}\right| = \lim_{z\to\mu}\left|\frac{C_m(z^p)}{z-\mu}\right|$$

$$\Leftrightarrow p|C'_m(\mu)| = |C_{pm}(\mu)||C'_m(\mu)| .$$

REFERENCES

1. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York - Berlin - Heidelberg, 1976.
2. T. M. Apostol, *The resultant of the cyclotomic polynomials $F_m(ax)$ and $F_n(bx)$*, Math. Comp. 29 (1975), 1–6.
3. H. Bass, *Generators and relations for cyclotomic units*, Nagoya Math. J. 27 (1966), 401–407.
4. H. Bass, *The Grothendieck group of the category of abelian group automorphisms of finite order*, preprint, Columbia Univ.
5. F. E. Diederichsen, *Über die Ausreduktion ganzzahliger Gruppendarstellungen bei arithmetischer Äquivalenz*, Abh. Math. Sem. Univ. Hamburg 13 (1940), 357–412.
6. V. Ennola, *On relations between cyclotomic units*, J. Number Theory 4 (1972), 236–247.
7. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 4th ed., Oxford University Press, 1960.
8. R. P. Kurshan and A. M. Odlyzko, *Recursive filters with uniform power distribution*, Electronics Letters 16 (1980), 672–673.

9. W. J. LeVeque (ed.), *Polynomials: Cyclotomic Polynomials and Roots of Unity* in *Reviews in Number Theory*, Section C 15, pp. 404–411, American Mathematical Society, Providence, R.I., 1974.

10. B. Magurn, *SK_1 of dihedral groups*, J. Algebra 51 (1978), 399–415.

11. W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers (PWN), Warszawa, 1974.

12. K. Ramachandra, *On the units of cyclotomic fields*, Acta Arith. 12 (1966), 165–173.

BELL LABORATORIES
MURRAY HILL, NEW JERSEY 07974
U.S.A.