PACIFIC JOURNAL OF MATHEMATICS
Vol. 112, No 2, 1984

MINIMAL POLYNOMIALS FOR CIRCULAR NUMBERS

S. GURAK

In a recent paper I gave polynomial expressions to compute the beginning coefficients of the minimal polynomials for the Gauss periods and cyclotomic units lying in the cyclotomic field $Q(\xi_m)$, where ξ_m is a fixed m-root of unity for a prime m. Here I extend these results for circular numbers lying in $Q(\xi_m)$ for m composite. My methods explain the linear recursion relations found among the beginning coefficients of the minimal polynomials for certain such circular numbers.

1. Introduction. For any positive integer m set $\xi_m = \exp(2\pi i/m)$ and let $G(m)$ denote the group of reduced residues modulo m. For any congruence subgroup A defined modulo m, let $\overline{A}$ be the canonical set of least non-negative integral representatives for the elements of A. Now fix a congruence subgroup H defined modulo m and of order f. Choose integers $t_1 = 1, t_2, \ldots, t_e$ to represent the $e = \phi(m)/f$ cosets of H in $G(m)$. The circular numbers

$$\sum_{x \in \overline{H}} \xi_m^{t_i x} \qquad (1 \leq i \leq e) \tag{1}$$

are conjugate over Q and, if they are distinct, have minimal polynomial

$$g(x) = x^e + a_1 x^{e-1} + \cdots + a_{e-1}x + a_e. \tag{2}$$

I consider the general question of determining the coefficients of the minimal polynomial for a sum of circular numbers of the form (1). Specifically let C denote a finite set of k positive integers (repetitions allowed), and consider the sum

$$\theta = \sum_{c \in C} \left(\sum_{x \in \overline{H}} \xi_m^{cx} \right), \quad \text{of circular numbers (1).} \tag{3}$$

If θ has degree e over the rational field Q then its minimal polynomial has the form (2) and equals $g(x) = \prod_{i=1}^{e}(x - \theta^{(i)})$, where for $1 \leq i \leq e$,

$$\theta^{(i)} = \sum_{c \in C} \left(\sum_{x \in \overline{H}} \xi_m^{ct_i x} \right). \tag{4}$$

It is well known from the theory of equations [2] that the coefficients a_r of $g(x)$ can be computed in terms of the symmetric power sums $S_n = \Sigma(\theta^{(i)})^n$

using Newton's identities

$$(5)\quad S_r + a_1 S_{r-1} + a_2 S_{r-2} + \cdots + a_{r-1} S_1 + r a_r = 0 \qquad (1 \le r \le e)$$
$$S_n + a_1 S_{n-1} + a_2 S_{n-2} + \cdots + a_{e-1} S_{n-e+1} + a_e S_{n-e} = 0 \qquad (n > e).$$

To compute the power sums I must introduce certain functions $T_n(m, d)$. Specifically for each positive $d|m$, let $T_n(m, d)$ equal the number of times a relation

$$(6)\qquad \mathrm{GCD}(c_1 x_1 + c_2 x_2 + \cdots + c_n x_n, m) = m/d$$

is satisfied by a choice of tuples $(c_1, c_2, \ldots, c_n)$ in C^n and $(x_1, x_2, \ldots, x_n)$ in $\overline{H}^n$.

In the next section I shall explicitly determine the power sums S_n in terms of the $T_n(m, d)$; namely,

$$(7)\qquad S_n = \frac{1}{f} \sum_{d|m} \left(\frac{\phi(m)}{\phi(d)} \right) T_n(m, d) \mu(d).$$

(Here ϕ and μ are the usual Euler phi and Mobius functions.) This result suggests that the functions $T_n(m, d)$ can be expressed in terms of certain appropriately defined power sums $S_n(d)$ for $d|m$. I treat this in §3, and then proceed to investigate certain multiplicative properties of the $T_n(m, d)$ and $S_n(d)$.

D. H. and E. Lehmer [5] have recently found curious linear recursion relations among the beginning coefficients of the minimal polynomials for certain circular numbers of the form (1) with H cyclic of order $f \le 4$, where m is a product of two distinct primes. For instance, if $m = 35$ and H is the cyclic congruence group of order $f = 2$ generated by 29 modulo 35, then the circular number $\xi_{35} + \xi_{35}^{29}$ has minimal polynomial

$$g(x) = x^{12} - x^{11} + 2x^{10} - 3x^9 + 5x^8 - 8x^7 + 13x^6 + 8x^5$$
$$+ 5x^4 + 3x^3 + 2x^2 + x + 1.$$

Its initial coefficients 1, −1, 2, −3, 5, −8, 13 are the first seven terms of the alternating Fibonacci sequence. The theory I describe in §§2–4 can be applied to study the presence of such linear recursion relations. In the concluding section of the paper I explain in broad generality this curious phenomenon detected by the Lehmers.

2. Minimal polynomials for circular numbers. Before explicitly determining the power sums used in (5) to compute the coefficients of the minimal polynomial for the circular numbers given in (1) and (3), I first wish to give conditions that ensure that the circular numbers in (1) are all

distinct, and thus of algebraic degree e over Q. This entails describing the notion of a conductor for congruence groups.

As before, $G(m)$ denotes the group of reduced residues modulo m. From duality theory there is a one-to-one correspondence between congruence subgroups of $G(m)$ and groups of numerical characters realizable modulo m. If Ω is any group of numerical characters that can be realized modulo m, I shall denote its realization modulo m by $\Omega(m)$. The smallest modulus $f = f(\Omega)$ for which Ω can be realized is, of course, the conductor of Ω. In view of the duality just mentioned a congruence group A is said to be realizable modulo m if its corresponding group Ω of numerical characters is realizable modulo m. In this case I shall denote that congruence group which corresponds to $\Omega(m)$ by $A(m)$. The group $A(m)$ is called the realization of A modulo m. The conductor of A is then the smallest modulus $f = f(A)$ for which A can be realized, and is, of course, equal to the conductor of the corresponding group of numerical characters. For instance if $A = A(12)$ with $\overline{A} = \{1, 5\}$, then the corresponding group $\Omega = \Omega(12)$ of numerical characters is generated by the numerical character χ given by

$$\chi(t) = \begin{cases} 1 & \text{if } t \equiv 1, 5 \pmod{12}, \\ -1 & \text{if } t \equiv 7, 11 \pmod{12}, \\ 0 & \text{otherwise.} \end{cases}$$

Hence both A and Ω have conductor $f = 4$ with $\overline{A(4)} = \{1\}$ and $\Omega(4) = \langle \chi \rangle$, where $\chi(t)$ coincides with the Jacobi symbol $(-1/t)$ for t odd.

Now if the congruence subgroup H in (1) has conductor m, then it corresponds through elementary classfield theory to the subfield K of $Q(\xi_m)$ left fixed by the group of Galois actions σ_x: $\xi_m \to \xi_m^x$ (x in $\overline{H}$). Indeed $\eta = \sum_{x \in \overline{H}} \xi_m^x = \mathrm{Tr}_{Q(\xi_m)/K}(\xi_m)$. It can be shown that η generates the subfield K and hence has degree e over Q. (See the appendix for details of the proof of this fact.)

I am now ready to verify that the power sums S_n in (5) satisfy (7). I shall *always* assume that the congruence group H has conductor m, and that the set C has been chosen so that θ in (3) has algebraic degree e over the rationals Q.

Fix a positive integer n. For any $d \mid m$ the number of primitive d-roots of unity in the multinomial expansion of any $(\theta^{(i)})^n$ is $T_n(m, d)$. Since the terms $(\theta^{(i)})^n$ in S_n are permuted by the action $\xi_m \to \xi_m^t$ for any $(t, m) = 1$, each primitive d-root of unity must occur an equal number of times in S_n when taking into account the total contribution of each term $(\theta^{(i)})^n$. Thus one finds a total of $eT_n(m, d)$ primitive d-roots of unity, explicitly

$eT_n(m, d)/\phi(d)$ occurrences of each of the $\phi(d)$ primitive d-roots of unity. Since the Mobius function $\mu(d)$ equals the sum of the primitive d-roots of unity, the value S_n must be $\Sigma_{d|m} eT_n(m, d)\mu(d)/\phi(d)$. This yields formula (7).

Utilizing (7) for the example cited in the introduction (where $m = 35$ with $\bar{H} = \{1, 29\}$, $f = 2$ and $C = \{1\}$) one finds the following values $T_n(35, d)$, S_n, a_n $(1 \leq n \leq 12, d|35)$:

n	$T_n(35,1)$	$T_n(35,5)$	$T_n(35,7)$	$T_n(35,35)$	S_n	a_n
1	0	0	0	2	1	−1
2	0	0	2	2	−3	2
3	0	0	0	8	4	−3
4	0	0	6	10	−7	5
5	0	0	2	30	11	−8
6	0	0	20	44	−18	13
7	14	114	0	0	−174	8
8	0	0	70	186	−47	5
9	0	0	72	440	76	3
10	0	0	254	770	−123	2
11	0	0	330	1718	199	1
12	0	0	948	3148	−322	1

3. Inversion formulae for the $T_n(m, d)$. Fix a congruence group H as before of conductor m and of order f. For each positive divisor $d|m$ set $\mathcal{H}_d = \{x \in Z | x \equiv x' \pmod{d}$ for some $x' \in \bar{H}\}$. The set $\mathcal{H}_d$ determines a congruence subgroup H_d of $G(d)$ having order $f(d)$. Using the $e(d) = \phi(d)/f(d)$ cosets of H_d in $G(d)$ one obtains sums $\eta_1, \eta_2, \ldots, \eta_{e(d)}$ of circular numbers as in (4) which are conjugates of $\eta = \Sigma_{c \in C}(\Sigma_{x \in \bar{H}_d} \xi_d^{cx})$. Define the symmetric power sums

$$S_n(d) = \sum \eta_i^n. \tag{8}$$

Note though that the polynomial $\prod_{i=1}^{e(d)}(x - \eta_i)$, which is determined from the values $S_n(d)$, need not be the minimal polynomial of η, but perhaps some power of it. Indeed, the stipulation that H have conductor m and the choice of the set C in (3) does not guarantee that η will have algebraic degree $e(d)$ over Q. Since the group H_d need not be of conductor d, it is even possible that $\eta = 0$.

In any case, the power sums $S_n(d)$ can be evaluated from an analog of (7):

$$S_n(d) = \frac{1}{f(d)} \sum_{\delta|d} \left(\frac{\phi(d)}{\phi(\delta)} \right) T_n(d, \delta)\mu(\delta), \tag{9}$$

where for any $\delta \mid d$, $T_n(d, \delta)$ equals the number of times a relation

$$\text{GCD}(c_1x_1 + c_2x_2 + \cdots + c_nx_n, d) = d/\delta \tag{10}$$

is satisfied by a choice of tuples $(c_1, c_2, \ldots, c_n)$ in C^n and $(x_1, x_2, \ldots, x_n)$ in $\overline{H}_d^n$. Setting $T_n(d) = T_n(d, 1)$ it follows from (10) that $T_n(d)$ equals the number of times a congruence

$$c_1x_1 + c_2x_2 + \cdots + c_nx_n \equiv 0 \pmod{d} \tag{11}$$

is satisfied by a choice of tuples $(c_1, c_2, \ldots, c_n)$ in C^n and $(x_1, x_2, \ldots, x_n)$ in $\overline{H}_d^n$. The following lemma gives an expression for $T_n(d, \delta)$ in terms of the $T_n(d')$ for $d' \mid d$.

LEMMA 1. *For any* $\delta \mid d$,

$$T_n(d, d/\delta) = \sum_{\delta \mid d' \mid d} \mu\left(\frac{d'}{\delta}\right) T_n(d') \left(\frac{f(d)}{f(d')}\right)^n, \tag{12}$$

where the sum is over the d'.

Proof. For a fixed tuple $\bar{c} = (c_1, c_2, \ldots, c_n)$ in C^n and any divisor $d' \mid d$, let $N(\bar{c})$ denote the number of tuples $(x_1, x_2, \ldots, x_n)$ in $\overline{H}_d^n$ satisfying $\text{GCD}(c_1x_1 + \cdots + c_nx_n, d) = \delta$, and let $N(\bar{c}, d')$ be the number of solutions $c_1x_1 + \cdots + c_nx_n \equiv 0 \pmod{d'}$ with x_i in $\overline{H}_d$. By the principle of inclusion-exclusion,

$$N(\bar{c}) = \sum_{\delta \mid d' \mid d} \mu(d'/\delta) N(\bar{c}, d'), \tag{13}$$

where the sum is over d'.Since $N(\bar{c}, d')$ is $(|\overline{H}_d|/|\overline{H}_{d'}|)^n = (f(d)/f(d'))^n$ times the number of solutions of $c_1x_1 + \cdots + c_nx_n \equiv 0 \pmod{d'}$ with x_i in $\overline{H}_{d'}$ one has

$$\sum_{\bar{c} \in C^n} N(\bar{c}, d') = T_n(d') \left(\frac{f(d)}{f(d')}\right)^n. \tag{14}$$

Summing in equation (13) over each of the tuples $\bar{c}$ of C^n, the result (12) follows from (14).

Before deriving the formulas for the $T_n(m, d)$, I need two additional results.

LEMMA 2. *If* $d \mid m$ *then* $\Sigma_{d' \mid d} \mu^2(m/d')/\phi(m/d') = d \mid \mu(m/d) \mid /\phi(m)$.

LEMMA 3. *If* $d \mid m$ *then* $\Sigma_{d \mid d' \mid m} \mu(d')/d' = \mu(d)\phi(m)/(m\phi(d))$, *where the sum is over* d'.

Since the above lemmas are proved in a straightforward manner, exploiting the multiplicativity of the functions μ and ϕ, I shall omit their proofs.

Denoting the greatest common divisor and least common multiple functions by $(,)$ and $[,]$ respectively, I now prove

THEOREM 1. *The functions $T_n(m, d)$ for $d \mid m$ are expressed by*

$$T_n(m, d) = \frac{1}{m} \sum_{\delta \mid m} \mu\left(\frac{[m, d\delta]}{m}\right) \phi(d) f(\delta) \times S_n(\delta) \left(\frac{f(m)}{f(\delta)}\right)^n \Big/ \phi\left(\frac{[m, d\delta]}{m}\right). \tag{15}$$

In particular,

$$T_n(m) = \frac{1}{m} \sum_{d \mid m} f(d) S_n(d) \left(\frac{f(m)}{f(d)}\right)^n, \tag{16}$$

and

$$T_n(m, m) = \frac{1}{m} \sum_{d \mid m} \mu(d) \phi(m) f(d) S_n(d) \left(\frac{f(m)}{f(d)}\right)^n \Big/ \phi(d). \tag{17}$$

Proof. Using (12) I first derive an alternate form of (9) which can be inverted to yield (16). Explicitly

$$\begin{aligned} S_n(d) &= \frac{1}{f(d)} \sum_{\delta \mid d} \frac{\phi(d) T_n(d, d/\delta) \mu(d/\delta)}{\phi(d/\delta)} \\ &= \frac{1}{f(d)} \sum_{\delta \mid d} \frac{\phi(d) \mu(d/\delta)}{\phi(d/\delta)} \sum_{\delta \mid d' \mid d} \mu\left(\frac{d'}{\delta}\right) T_n(d') \left(\frac{f(d)}{f(d')}\right)^n \end{aligned}$$

from (12) or equivalently upon interchanging the order of summation,

$$S_n(d) = \frac{1}{f(d)} \sum_{d' \mid d} T_n(d') \left(\frac{f(d)}{f(d')}\right)^n \phi(d) \sum_{\delta \mid d'} \frac{\mu(d/\delta) \mu(d'/\delta)}{\phi(d/\delta)}. \tag{18}$$

Now

$$\sum_{\delta \mid d'} \frac{\mu(d/\delta) \mu(d'/\delta)}{\phi(d/\delta)} = 0 \quad \text{if } \mu(d/d') = 0,$$

otherwise equals

$$\mu\left(\frac{d}{d'}\right)\sum_{\delta|d'}\frac{\mu^2(d/\delta)}{\phi(d/\delta)}=\frac{d'\mu(d/d')}{\phi(d)}$$

using the multiplicativity of the Mobius function and the result of Lemma 2. Thus (18) becomes

$$S_n(d)=\frac{1}{f(d)}\sum_{d'|d}\mu\left(\frac{d}{d'}\right)d'T_n(d')\left(\frac{f(d)}{f(d')}\right)^n. \tag{19}$$

Substituting this expression for $S_n(d)$ in the sum

$$\left(\frac{1}{m}\right)\sum_{d|m}f(d)S_n(d)\left(\frac{f(m)}{f(d)}\right)^n,$$

a straightforward manipulation gives (16).

To obtain the general expression (15) for the $T_n(m, d)$, it is convenient to use $T_n(m, m/d)$. From (12) and (16) I find that

$$\begin{aligned}T_n\left(m,\frac{m}{d}\right)&=\sum_{d|d'|m}\mu\left(\frac{d'}{d}\right)T_n(d')\left(\frac{f(m)}{f(d')}\right)^n\\&=\sum_{d|d'|m}\mu\left(\frac{d'}{d}\right)\left(\frac{f(m)}{f(d')}\right)^n\sum_{\delta|d'}\frac{f(\delta)S_n(\delta)(f(d')/f(\delta))^n}{d'},\end{aligned}$$

where the initial sum is over d' with m and d fixed. Upon replacing d' by dd' this last expression becomes

$$\frac{1}{d}\sum_{dd'|m}\frac{\mu(d')}{d'}\sum_{\delta|dd'}f(\delta)S_n(\delta)\left(\frac{f(m)}{f(\delta)}\right)^n \tag{20}$$

or, equivalently,

$$\frac{1}{d}\sum_{\delta|m}f(\delta)S_n(\delta)\left(\frac{f(m)}{f(\delta)}\right)^n\sum_{\delta|dd'|m}\frac{\mu(d')}{d'} \tag{21}$$

upon interchanging the order of summation. The final sum $\Sigma_{\delta|dd'|m}\,\mu(d')/d'$ of (21) is over d' and is the same as

$$\sum_{\delta/(d,\delta)|d'|m/d}\frac{\mu(d')}{d'},$$

which equals

$$\frac{d}{m}\phi(m/d)\mu\left(\frac{\delta}{(d,\delta)}\right)\Big/\phi\left(\frac{\delta}{(d,\delta)}\right)$$

by the result of Lemma 3. Thus

$$T_n\left(m, \frac{m}{d}\right) = \frac{1}{m}\sum_{\delta|m}\mu\left(\frac{\delta}{(d,\delta)}\right)\phi\left(\frac{m}{d}\right)f(\delta)S_n(\delta)\left(\frac{f(m)}{f(\delta)}\right)^n \Big/ \phi\left(\frac{\delta}{(d,\delta)}\right),$$

which, upon replacing d by m/d, gives (15). Since the last formula (17) is immediate from (15) the proof of the theorem is complete.

That the sequence $\{T_n(m, d)\}$ satisfies a linear recurrence relation for any $d|m$ is an immediate consequence of Theorem 1. Indeed it follows from the theory of linear recurrence sequences that

COROLLARY 1. *For any $d|m$ the sequence $\{T_n(m, d)\}$ satisfies a linear recursion relation over Z of order at most $\Sigma_{\delta|m}|\mu([m, d\delta]/m)|e(\delta)$.*

EXAMPLE. For the example given in §2, one finds from (16) that

$$T_n(35) = \tfrac{1}{35}[S_n(1)2^n + 2S_n(5) + S_n(7)2^n + 2S_n(35)]$$

where

$$S_n(1) = 1, \qquad S_n(7) = \sum_{i=1}^{6}\xi_7^{in},$$

$$S_n(5) = \left(\xi_5 + \xi_5^{-1}\right)^n + \left(\xi_5^2 + \xi_5^{-2}\right)^n \quad \text{and} \quad S_n(35) = \sum_{i=1}^{12}\left(\xi_{35}^{i} + \xi_{35}^{29i}\right)^n$$

from (8) with $f(1) = 1$, $f(5) = 2$, $f(7) = 1$ and $f(35) = 2$. The product of the minimal polynomials associated to the power sums in the expression for $T_n(35)$ is

$$(x-2)(x^6 + 2x^5 + 4x^4 + 8x^3 + 16x^2 + 32x + 64)(x^2 + x - 1)$$
$$\cdot (x^{12} - x^{11} + 2x^{10} - 3x^9 + 5x^8 - 8x^7 + 13x^6$$
$$+8x^5 + 5x^4 + 3x^3 + 2x^2 + x + 1)$$

or

$$(x^7 - 128)(x^{14} + 29x^7 - 1) = x^{21} - 99x^{14} - 3713x^7 + 128.$$

Thus the $\{T_n(35)\}$ satisfy the recursion $T_{n+21} = 99T_{n+14} + 3713T_{n+7} - 128T_n$. Alternatively one finds that $T_n(35) = \frac{1}{5}(2^n + 2L_n)$ if $7|n$, otherwise 0, where $\{L_n|n > 0\}$ is the alternating Lucas sequence $-1, 3, -4, 7, -11, 18, -29, \ldots$.

4. Multiplicative properties of $S_n(d)$ and $T_n(d, \delta)$. Here I investigate certain multiplicative properties of the functions $S_n(d)$ and $T_n(d, \delta)$ discussed in the previous section and give some explicit computations. I

assume the congruence subgroup H of conductor m and the set C is fixed throughout as before. For any tuple $\bar{c} = (c_1, c_2, \ldots, c_n)$ in C^n and any divisors $\delta \mid d \mid m$ let $T_n(\bar{c}, d, \delta)$ denote the number of tuples $\bar{x} = (x_1, x_2, \ldots, x_n)$ in $\bar{H}_d^n$ satisfying $(c_1x_1 + \cdots + c_nx_n, d) = d/\delta$. Then clearly

$$T_n(d, \delta) = \sum_{C^n} T_n(\bar{c}, d, \delta). \tag{22}$$

The components $T_n(\bar{c}, d, \delta)$ are bimultiplicative in the following sense.

PROPOSITION 1. *If $d, d' \mid m$ with $(d, d') = 1$ and if $\mathcal{H}_{dd'} = \mathcal{H}_d \cap \mathcal{H}_{d'}$ then*

$$T_n(\bar{c}, dd', \delta\delta') = T_n(\bar{c}, d, \delta)T_n(\bar{c}, d', \delta') \tag{23}$$

for any tuple $\bar{c}$ in C^n and choice $\delta \mid d$, $\delta' \mid d'$.

Proof. I first note that from the definition of the congruence subgroups H_d for $d \mid m$ the inclusion $\mathcal{H}_{dd'} \subset \mathcal{H}_d \cap \mathcal{H}_{d'}$ always holds. If $\mathcal{H}_{dd'} = \mathcal{H}_d \cap \mathcal{H}_{d'}$ then the canonical set $\bar{H}_{dd'}$ is just that obtained from the Chinese Remainder Theorem for finding the least nonnegative solutions $\bar{x}$ of each of the systems of congruences given by

$$\bar{x} \equiv x \pmod{d}, \qquad \bar{x} \equiv x' \pmod{d'} \qquad \left(x \in \bar{H}_d, x' \in \bar{H}_{d'}\right). \tag{24}$$

Consequently the relations $e(dd') = e(d)e(d')$ and $f(dd') = f(d)f(d')$ hold. From these remarks it follows that each pair of tuples $(x_1, x_2, \ldots, x_n)$ and $(x_1', x_2', \ldots, x_n')$ satisfying $(c_1x_1 + \cdots + c_nx_n, d) = d/\delta$ and $(c_1x_1' + \cdots + c_nx_n', d') = d'/\delta'$ with $x_i \in \bar{H}_d$ and $x_i' \in \bar{H}_{d'}$ corresponds to a unique tuple $(\bar{x}_1, \bar{x}_2, \ldots, \bar{x}_n)$ with $\bar{x}_i \in \bar{H}_{dd'}$ satisfying $(c_1\bar{x}_1 + \cdots + c_n\bar{x}_n, dd') = dd'/\delta\delta'$ and conversely. Thus (23) is proved.

If $C = \{1\}$ then the power sums $S_n(d)$ are multiplicative in the following sense.

PROPOSITION 2. *If $d, d' \mid m$ with $(d, d') = 1$ and $\mathcal{H}_{dd'} = \mathcal{H}_d \cap \mathcal{H}_{d'}$, then, if $C = \{1\}$,*

$$T_n(dd', \delta\delta') = T_n(d, \delta)T_n(d', \delta') \quad \textit{for any } \delta \mid d, \delta' \mid d', \tag{25}$$

$$S_n(dd') = S_n(d)S_n(d'). \tag{26}$$

Proof. Statement (25) is clear from Proposition 1. In view of (8) and the fact that $\eta = \sum_{x \in \bar{H}_d} \xi_d^x$ and $\eta' = \sum_{x' \in \bar{H}_{d'}} \xi_{d'}^{x'}$ are linearly disjoint over Q (since $(d, d') = 1$), together with the remarks I made at the beginning of

the proof of Proposition 1, to deduce (26) it suffices to show that the circular number $\bar{\eta} = \Sigma_{\bar{x} \in \bar{H}_{dd'}} \xi_{dd'}^{\bar{x}}$ is conjugate to the product $\eta\eta' = \Sigma_{x \in \bar{H}_d, x' \in \bar{H}_{d'}} \xi_{dd'}^{d'x + dx'}$. Since $(d + d', dd') = 1$ one can find an integer a such that $a(d + d') \equiv 1 \pmod{dd'}$. I claim that

$$\bar{\eta} = \sum_{x \in \bar{H}_d,\, x' \in \bar{H}_{d'}} \xi_{dd'}^{a(d'x + dx')}, \tag{27}$$

the conjugate of $\eta\eta'$ under the action $\xi_{dd'} \to \xi_{dd'}^{a}$. To verify this assertion I must show that the residues $ad'x + adx'$ run through the elements of $\bar{H}_{dd'}$ modulo dd' as the x and x' run through $\bar{H}_d$ and $\bar{H}_{d'}$ respectively. Since $(d, d') = 1$ and $(a, dd') = 1$ the $f(d)f(d') = f(dd')$ residues $ad'x + adx'$ are all distinct modulo dd'. Also each lies in both H_d and $H_{d'}$ since $ad'x + adx'$ is congruent to x modulo d and to x' modulo d' by the choice of a. But $\mathcal{H}_{dd'} = \mathcal{H}_d \cap \mathcal{H}_{d'}$, so my assertion will follow, thus completing the proof of (26).

Applying (26) for special choices of the congruence group H, I next obtain some explicit computational results.

COROLLARY 2. *Let H be the group of e-powers modulo a prime p so that θ in* (1) *is a Gauss period of degree $f = (p - 1)/e$ for p. Then*

$$S_n(p) = pT_n(p)/f - f^{n-1}, \tag{28}$$

where, if $p > n^{\phi(f)}$, the $T_n(p)$ are determined for prime $f = l$ by

$$T_n(p) = \left(\frac{n!}{((n/l)!)^l} \right) \quad \text{if } l \mid n, \quad \text{otherwise } 0, \tag{29}$$

and for $f = 4$ by

$$T_n(p) = \binom{n}{n/2}^2 \quad \text{if } 2 \mid n, \quad \text{otherwise } 0. \tag{30}$$

D. H. Lehmer [5] attributes the case $f = 2$ in the above corollary to Sylvester, and he has found the cases $f = 3$ and 4. In the general case, formula (28) follows easily from (7) or (19) and is my result (10) in [3]. Only equation (29) needs to be proved but, in view of the comments made at the beginning of the proof of Theorem 1 in [3], this is achieved by a straightforward counting argument involving multinomial coefficients.

COROLLARY 3. *For distinct odd primes p and q let H be the congruence group determined from the set*

$$\mathcal{H} = \{x \in Z | x \equiv \pm 1 \pmod{p};\ x \equiv 1 \pmod{q}\}$$

of conductor pq. The functions $T_n(pq)$ *and* $S_n(pq)$ *associated to the circular number* (1) *corresponding to H for* $n < p$ *satisfy*

$$T_n(pq) = \binom{n}{n/2} \quad \text{or} \quad 0 \qquad \text{as } (n,2q) = 2 \text{ or not}; \tag{31}$$

$$S_n(pq) = \begin{cases} 2^{n-1} & \text{if } (n,2q) = 1, \\ 2^{n-1} - \dfrac{p}{2}\binom{n}{n/2} & \text{if } (n,2q) = 2, \\ -(q-1)2^{n-1} & \text{if } (n,2q) = q, \\ -(q-1)2^{n-1} + \dfrac{p(q-1)}{2}\binom{n}{n/2} & \text{if } (n,2q) = 2q. \end{cases} \tag{32}$$

COROLLARY 4. *For distinct odd primes p and q let H be the intersection of the groups* ± 1 *modulo p and q. The functions* $T_n(pq)$ *and* $S_n(pq)$ *associated to the circular number* θ *in* (1) *corresponding to H satisfy for* $n < p$ *and q,*

$$T_n(pq) = \binom{n}{n/2}^2 \quad \text{or} \quad 0 \qquad \text{as } 2 \mid n \text{ or not}; \tag{33}$$

(34)

$$S_n(pq) = \begin{cases} \dfrac{1}{4}\left(pq\binom{n}{n/2}^2 - 2^n q\binom{n}{n/2} - 2^n p\binom{n}{n/2} + 2^{2n} \right) & \text{if } 2 \mid n, \\ 2^{2n-2} \quad \text{otherwise.} \end{cases}$$

Moreover, the coefficients a_r *of the minimal polynomial* (2) *for* θ *satisfy* $a_r = P_r(p,q)$, *where for each r,* P_r *is a polynomial of degree* $2[r/2]$, *which is of degree* $[r/2]$ *in both p and q and whose leading term has sign* $(-1)^{[(r+1)/2]}$ (*Here* [ ] *denotes the greatest integer function.*)

The expressions for T_n and S_n in Corollaries 3 and 4 are easily obtained from Corollary 2 and Proposition 2. The last statement of Corollary 4 is proved by an argument similar to the one I employed to deduce Theorem 1 in [**3**]. In fact, the same techniques readily give the following generalization of Corollary 4.

PROPOSITION 3. *For prescribed positive integers* $f_1, f_2, \ldots, f_s$ *choose distinct odd primes* $l_1, l_2, \ldots, l_s$ *with* $l_i \equiv 1 \pmod{f_i}$, *and for* $1 \leq i \leq s$, *let* H_{l_i} *be the group of* $(l_i - 1)/f_i$ *powers modulo* l_i. *Let* p_i *denote the smallest prime factor of* f_i $(1 \leq i \leq s)$. *Let* H *be the intersection of the congruence groups* H_{l_i} *with* θ *its corresponding circular number* (1). *If each* $l_i > r^{\Phi(f_i)}$ $(1 \leq i \leq s)$ *then the coefficient* a_r *for the minimal polynomial* (2) *of* θ *satisfies* $a_r = P_r(l_1, l_2, \ldots, l_s)$ *where for each* r, P_r *is a polynomial of degree* $[r/p_i]$ *in* l_i $(1 \leq i \leq s)$.

5. Recursive relations among the beginning coefficients. Using explicit formulas similar to (31) and (33) to compute the power sums S_n for a circular number θ of form (1) for which m is a product of two distinct primes and H is cyclic of order $f \leq 4$, the Lehmers [**5**] have shown that the beginning coefficients of its minimal polynomial are the initial part of a linear recurrence sequence $B = \{b_n \mid n \geq 0\}$ which is readily determined from H. Moreover, for any positive integer s they construct circular numbers of similar type for which the first $s + 1$ coefficients of their minimal polynomials are identically $b_0, b_1, \ldots, b_s$ in the sequence B. These results can be deduced from formula (7) using the results of the previous section and completely generalized to treat sums of circular numbers in (3) without such restriction on the modulus m and choice of congruence subgroup H. I shall give this generalization next, but first I need an important lemma.

LEMMA 4. *Suppose* $p(x) = x^e + p_1 x^{e-1} + \cdots + p_e$ *is any polynomial with roots* $\omega_1, \omega_2, \ldots, \omega_e$ (*not necessarily distinct*) *and* $S_n = \sum \omega_i^n$ *for each* $n > 0$. *The sequence* $\{b_n\}$ *given by*

$$b_0 = 1, \quad b_1 = S_1, \quad nb_n = b_{n-1}S_1 + \cdots + b_1 S_{n-1} + S_n \qquad (n > 1) \tag{35}$$

is recursive and satisfies the linear relation $b_{n+e} + p_1 b_{n+e-1} + \cdots + p_e b_n = 0$ *for* $n \geq 0$. *Alternatively, the* $\{b_n\}$ *are determined by the relations*

$$b_n p_0 + b_{n-1} p_1 + \cdots + b_1 p_{n-1} + b_0 p_n = 0 \qquad (n \geq 0) \tag{36}$$

where $p_0 = 1$ *and* $p_n = 0$ *for* $n > e$, *or, equivalently, from the generating function*

$$\frac{1}{1 + p_1 x + \cdots + p_e x^e} = \sum b_t x^t. \tag{37}$$

Proof. Clearly it is enough to show that the b_n given in (35) satisfy (36) for $n > 0$. Consider the square $(n+1)$ by $(n+1)$ matrix

$$A = \begin{bmatrix} S_1 & S_2 & \cdots & S_n & b_n \\ 1 & S_1 & \cdots & S_{n-1} & b_{n-1} \\ 0 & 2 & \cdots & S_{n-2} & b_{n-2} \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \cdots & S_1 & b_1 \\ 0 & 0 & \cdots & n & b_0 \end{bmatrix}$$

Since $[b_{n-1}\ b_{n-2}\ \cdots\ b_1\ b_0\ -n] \cdot A^t = [0\ 0\ \cdots\ 0]$ from the defining relations (35), the matrix A is singular. Then the product

$$\begin{bmatrix} 1 & p_1 & p_2 & \cdots & p_n \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix} A,$$

equal to

$$\begin{bmatrix} 0 & 0 & \cdots & 0 & b_n p_0 + \cdots + b_0 p_n \\ 1 & S_1 & \cdots & S_{n-1} & b_{n-1} \\ 0 & 2 & \cdots & S_{n-2} & b_{n-2} \\ \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & \cdots & n & b_0 \end{bmatrix}$$

from the Newton identities expressing the sums S_n in terms of the coefficients of the polynomial $p(x)$, is singular. But this is so if and only if $b_n p_0 + \cdots + b_0 p_n = 0$.

Now fix a circular number θ_0 of form (3) corresponding to a congruence subgroup H_0 of conductor m_0 and order f for a given set C of positive integers. Denote its minimal polynomial by

$$p(x) = x^{e(m_0)} + p_1 x^{e(m_0)-1} + \cdots + p_{e(m_0)}$$

and let $B = \{b_n\}$ be the associated linear sequence given by (35) in the previous lemma. For a given integer $s > 0$ choose any positive integer m_1 relatively prime to m_0 and to each of the sums

$$c_1 + c_2 + \cdots + c_n \qquad (1 \le n \le s,\ c_i \in C). \tag{38}$$

Let H be the congruence group defined modulo $m = m_0 m_1$ which is determined from the set

$$(39)\quad \mathcal{K} = \{x \in Z | x \equiv x_0 \pmod{m_0},\ x \equiv 1 \pmod{m_1} \text{ for some } x_0 \text{ in } \overline{H}_0\}.$$

The congruence group H is of order f, and has conductor m since $(m_0, m_1) = 1$ and H_0 has conductor m_0. Further, it is easy to show that for any pair of divisors $d \mid m_0$ and $d_1 \mid m_1$,

$$(40)\qquad \mathcal{K}_{dd_1} = \mathcal{K}_d \cap \mathcal{K}_{d_1},$$

and $H_{m_0} = H_0$. If θ is the circular number (3) corresponding to H for the given set C then the beginning coefficients of its minimal polynomial (2) are characterized by

THEOREM 2. *Under the above hypothesis, the coefficients* $a_1, \ldots, a_s$ *depend on the value* $\mu(m_1)$ *as follows*:

(i) *If* $\mu(m_1) = -1$ *then* $a_r = b_r$ $(1 \le r \le s)$.

(ii) *If* $\mu(m_1) = 1$ *then* $a_r = p_r$ $(1 \le r \le s)$ *where* $p_r = 0$ *for* $r > e(m_0)$.

(iii) *If* $\mu(m_1) = 0$ *then* $a_r = 0$ $(1 \le r \le s)$.

Proof. I assert that for any $1 \le n \le s$ the sum $S_n(m) = \mu(m_1) S_n(m_0)$. Then from the Newton identities (5) one determines the coefficients $a_1, \ldots, a_s$ by

$$(41)\quad \mu(m_1)(S_1 + a_1 S_{r-1} + \cdots + a_{r-1} S_1) = -r a_r \qquad (1 \le r \le s),$$

where the $S_n = S_n(m_0)$. The result of the theorem will follow.

To prove my assertion I note that by the choice of m_1 in (38) that for any fixed tuple $\bar{c}$ in C^n the component $T_n(\bar{c}, m_1, d_1)$ for $d_1 \mid m_1$ is 1 or 0 as $d_1 = m_1$ or not, since no $c_1 + c_2 + \cdots + c_n$ may have a factor in common with m_1. Thus for $d \mid m_0$ and $d_1 \mid m_1$ one finds from (22) and (23) that

$$(42)\quad \begin{aligned} T_n(m_0 m_1, dd_1) &= \sum_{C^n} T_n(\bar{c}, m_0 m_1, dd_1) \\ &= \sum_{C^n} T_n(\bar{c}, m_0, d) T_n(\bar{c}, m_1, d_1) = T_n(m_0, d) \end{aligned}$$

or 0 as $d_1 = m_1$ or not. But using (7) to compute $S_n(m)$, I find that

$$\begin{aligned} S_n(m) &= \frac{1}{f}\sum_{d|m}\frac{\phi(m)}{\phi(d)}T_n(m,d)\mu(d) \\ &= \frac{1}{f}\sum_{dm_1|m}\frac{\phi(m_0m_1)T_n(m_0m_1, dm_1)\mu(dm_1)}{\phi(dm_1)} \\ &= \frac{\mu(m_1)}{f}\sum_{d|m_0}\frac{\phi(m_0)T_n(m_0,d)\mu(d)}{\phi(d)} \\ &= \mu(m_1)S_n(m_0) \end{aligned}$$

from (42) and the multiplicity of ϕ and μ.

EXAMPLE. Pick $\theta_0 = \xi_7^{-3} + \xi_7^{-1} + \xi_7^1 + \xi_7^3$ the circular number (3) corresponding to $\overline{H}_0 = \{1, 6\}$ modulo 7 and $C = \{1, 3\}$. Associated to its minimal polynomial $p(x) = x^3 + 2x^2 - x - 1$ is the sequence $B = \{1, -2, 5, -11, 25, -56, \ldots\}$ from Lemma 4 satisfying $a_{n+3} = -2a_{n+2} + a_{n+1} + a_n$. With $m_1 = 5$ the congruence group H constructed in (39) has $\overline{H} = \{1, 6\}$ modulo 35 and determines for the given set C the number $\theta = \xi_{35}^{18} + \xi_{35}^{1} + \xi_{35}^{6} + \xi_{35}^{3}$. The computation of the $T_n(35, d)$, $S_n(35)$ and a_n for $d \mid 35$ and $1 \le n \le 6$ yields

n	$T_n(35,1)$	$T_n(35,5)$	$T_n(35,7)$	$T_n(35,35)$	S_n	a_n
1	0	0	0	4	2	−2
2	0	4	0	12	−6	5
3	0	6	24	34	−49	9
4	0	44	64	148	−186	25
5	0	130	64	830	−103	−4
6	180	442	780	2694	621	117

The coefficients a_1 and a_2 agree with the sequence B above as expected from Theorem 2. Since $1 + 1 + 3 = 5$ in (38) one cannot expect a_3 to agree.

For the choice $C = \{1\}$ in Theorem 2 with $m_1 = l$, a prime not dividing m_0, one sees from (26) that $S_n(m) = \mu(m_1)S_n(m_0) = -S_n(m_0)$ for $1 \le n < m_1$. It follows from Theorem 2 and the argument used in the proof of (26) that

COROLLARY 5. *Let θ_0 be a circular number* (1) *corresponding to any given congruence subgroup of conductor m_0. For a fixed prime l not dividing m_0, the first l coefficients of the minimal polynomial of $\xi_l\theta_0$ agree with those of the recurrence sequence* (35) *associated to the minimal polynomial of θ_0.*

This last result explains, of course, the behavior of the initial coefficients for the minimal polynomial of $\xi_{35} + \xi_{35}^{29} = \xi_7^3(\xi_5^2 + \xi_5^{-2})$ in the example cited in the introduction. However, the corollary is true in a much broader context as I will show. The next proposition provides an analog of the factorization formula $(x^l - 1)/(x - 1) = x^{l-1} + x^{l-2} + \cdots + x + 1$ for primes l.

PROPOSITION 4. *Let θ_0 be algebraic of degree e over a field F with minimal polynomial $p(x)$ in $F[x]$, and let l be an odd prime. If the field $F(\theta_0)$ is algebraically independent of $Q(\xi_l)$ then the minimal polynomial of $\xi_l\theta_0$ over F is given by $g(x) = P(x^l)/p(x)$, where $P(x)$ is the minimal polynomial of θ_0^l over F.*

Proof. Denote the conjugates of θ_0 over F by $\theta_1 = \theta_0, \theta_2, \ldots, \theta_e$. Since $F(\theta_0)$ is algebraically independent of $Q(\xi_l)$ a complete set of conjugates of $\xi_l\theta_0$ over F is $\{\xi_l^t\theta_i \mid 1 \le t \le l-1,\ 1 \le i \le e\}$. Thus, since

$$P(x^l) = \prod_{i=1}^{e} (x^l - \theta_i^l) = \prod_{t=1}^{l-1} \prod_{i=1}^{e} (x - \xi_l^t\theta_i)p(x),$$

one finds that the minimal polynomial of $\xi_l\theta_0$ over F is $P(x^l)/p(x)$.

EXAMPLE. Pick $\theta_0 = \xi_7^{-3} + \xi_7^{-1} + \xi_7^1 + \xi_7^3$ and $l = 5$ in Proposition 4 where $p(x) = x^3 + 2x^2 - x - 1$. Since the minimal polynomial of θ_0^5 is $P(x) = x^3 + 57x^2 - 16x - 1$, one finds that $\xi_5\theta_0$ has minimal polynomial

$$\begin{aligned} g(x) &= (x^{15} + 57x^{10} - 16x^5 - 1)/(x^3 + 2x^2 - x - 1) \\ &= x^{12} - 2x^{11} + 5x^{10} - 11x^9 + 25x^8 + x^7 + 12x^6 + 2x^5 \\ &\quad + 9x^4 - 4x^3 + 3x^2 - x + 1. \end{aligned}$$

It readily follows from Proposition 4 that the minimal polynomial $g(x)$ of $\xi_l\theta_0$ given in Proposition 4 for $l \ge e$ is essentially determined by the recursion relation

$$a_{n+e} + p_1 a_{n+e-1} + \cdots + p_e a_n = 0 \tag{43}$$

and the sequence (35) associated to the minimal polynomial $p(x) = x^e + p_1 x^{e-1} + \cdots + p_e$ of θ_0. Indeed its first l coefficients match the terms $b_0, b_1, \ldots, b_{l-1}$ of (35). The remaining coefficients are computed from (43) in sequence, except that for the coefficients a_r where $l \mid r$, one finds that

$$a_{vl} = -p_1 a_{vl-1} - \cdots - p_e a_{vl-e} + q_v \qquad (1 \le v < e), \tag{44}$$

where $P(x) = x^e + q_1 x^{e-1} + \cdots + q_e$ is the minimal polynomial of θ_0^l over F.

This behavior for the coefficients of $g(x)$ is exhibited in the last example.

Appendix. Generating classfields over the rational field Q. The purpose here is to verify the assertion made in §2 that if H is a congruence group of conductor m then the circular period $\eta = \Sigma_{x \in \bar{H}} \xi_m^x$ generates the classfield K/Q corresponding to H. The proof for the case K/Q cyclic of degree prime to m is given by Hasse [**4**, p. 435] using Gauss sums. I treat the general case in similar fashion with the aid of the following technical lemma.

LEMMA. *Let Ω be a group of numerical characters with conductor m and fix an integer t relatively prime to m. The following statements are equivalent*:

(1) $\chi(t) = 1$ *for all* χ *in* Ω.

(2) $\chi(t) = 1$ *for all* χ *in* Ω *of conductor* $f = f(\chi)$ *satisfying* $(m/f, f) = 1$ *with* m/f *square-free.*

Proof. It suffices to show that (2) implies (1) for m not square-free. Suppose $m = \prod_{i=1}^r p_i^{b_i} \cdot \prod_{j=1}^s q_j$ as a product of distinct primes $p_1, \ldots, p_r$, $q_1, \ldots, q_s$ where each $b_i > 1$ $(1 \le i \le r)$. Since each $p_i^{b_i}$ divides the conductor m, it follows, upon analyzing the p-components of each numerical character of Ω, that the exponent of Ω is divisible by $\prod_{i=1}^r p_i^{b_i - 1}$. Thus there are characters χ_{p_i} in Ω $(1 \le i \le r)$ of order $p_i^{a_i}$ with $a_i \ge b_i - 1$ and of conductor $f(\chi_{p_i}) \mid m$ satisfying

$$p_i^{b_i} \| f(\chi_{p_i}) \quad \text{with } f(\chi_{p_i})/p_i^{b_i} \text{ square-free.} \tag{45}$$

Let χ be any character in Ω, say of order k. If $f(\chi)$ is divisible by $\prod_{i=1}^r p_i^{b_i}$ then, assuming (2), one has $\chi(t) = 1$. Otherwise, let S be the set of primes p_i for which $p_i^{b_i} \nmid f(\chi)$. Then the characters $\psi = \chi \cdot \prod_{p \in S} \chi_p$ and $\psi' = \bar{\chi} \cdot \prod_{p \in S} \chi_p$ have conductors divisible by $\prod_{i=1}^r p_i^{b_i}$, hence by (2),

$$\psi(t) = \chi(t) \prod_{p \in S} \chi_p(t) = 1 \quad \text{and} \quad \psi'(t) = \bar{\chi}(t) \prod_{p \in S} \chi_p(t) = 1.$$

Thus $\chi^2(t) = \psi(t)\overline{\psi'(t)} = 1$ so $\chi(t) = \pm 1$. If the order k is odd then $\chi(t) = 1$, else by raising ψ to a sufficiently high odd power one finds $\chi(t) = 1$ if $2 \notin S$ or $\chi(t)\chi_2(t) = 1$ if $2 \in S$ since each χ_p is of order p^a for some integer a. In the last instance where $2 \in S$ the same argument applied to the character $\prod_{i=1}^r \chi_{p_i}$ at t shows $\chi_2(t) = 1$, so in all cases $\chi(t) = 1$. This completes the proof of the lemma.

Now let Ω be the group of numerical characters, say of exponent k, which corresponds to the congruence group H of conductor m through duality theory. For each $\chi \in \Omega$ define the Gauss sum $\tau(\chi)$ by

$$\tau(\chi) = \sum_{x \bmod m} \chi(x)\xi_m^x, \tag{46}$$

considering χ as defined modulo m. If χ has conductor $f(\chi)$, then it is known [**4**, p. 427] that

$$\tau(\chi) \neq 0 \quad \text{iff } (m/f(\chi), f(\chi)) = 1 \text{ with } m/f(\chi) \text{ square-free.} \tag{47}$$

In any case $\tau(\chi)$ lies in the compositum $Q(\xi_m, \xi_k) = Q(\xi_M)$ where $M = \mathrm{LCM}(m, k)$. An integer t prime to M corresponds to an automorphism σ of $Q(\xi_M)$ given by the action $\xi_M \to \xi_M^t$. Conjugating in (46) by σ one finds

$$\tau(\chi)^\sigma = \sum_{x \bmod m} \chi^t(x)\xi_m^{tx} = \bar{\chi}^t(t) \sum_{x \bmod m} \chi^t(tx)\xi_m^{tx} = \bar{\chi}^t(t)\tau(\chi^t). \tag{48}$$

Next, choose coset representatives $t_1 = 1, t_2, \ldots, t_e$ for H in $G(m)$, as in the introduction, to define the conjugate circular numbers $\eta_i = \Sigma_{x \in H} \xi_m^{t_i x}$. The Gauss sums are expressible in terms of the η_i and vice versa, namely:

$$\tau(\chi) = \sum_{i=1}^{e} \chi(t_i)\eta_i, \tag{49}$$

$$\eta_i = \left(|\Omega|^{-1}\right) \sum_{\chi \in \Omega} \bar{\chi}(t_i)\tau(\chi). \tag{50}$$

I assert that the η_i $(1 \leq i \leq e)$ are all distinct. If not then $\eta_1 = \eta_t$ for some $t = t_i$ with $i \neq 1$. Since there is no loss in generality in assuming that t is prime to k, it follows that there is an automorphism σ of $Q(\xi_M)$ given by the action $\xi_M \to \xi_M^t$ which fixes the η_i. Then from (49), for any χ in Ω, $\tau(\chi)^0 = \Sigma_{i=1}^e \chi^t(t_i)\eta_i = \tau(\chi^t)$ so $\tau(\chi^t) = \bar{\chi}^t(t)\tau(\chi^t)$ in (48). Thus if $\tau(\chi^t) \neq 0$ then $\chi(t) = 1$ since $(t, k) = 1$. In view of (47) and the lemma, $\chi(t) = 1$ for all χ in Ω so t represents H. This contradicts the assumption $t \neq t_1$.

To summarize, I have established the following result.

THEOREM. *Let K be the subfield of $Q(\xi_m)$ corresponding through classfield theory to a given congruence group H of conductor m. Then K is generated over Q by $\Sigma_{x \in H} \xi_m^x = \mathrm{Tr}_{Q(\xi_m)/K}\, \xi_m$.*

REFERENCES

[1] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, 1966.
[2] L. E. Dickson, *Elementary Theory of Equations*, Wiley, New York.
[3] S. Gurak, *Minimal polynomials for Gauss circulants and cyclotomic units*, (to appear).
[4] H. Hasse, *Vorlesungen uber Zahlentheorie*, Springer Verlag, Berlin 1950.
[5] D. H. and E. Lehmer, *Cyclotomy with short periods*, (to appear).
[6] H. Leopoldt, *Zur Geschlectertheorie in abelschen Zahlkorpern*, Math. Nachr., **9** (1953), 351–362.
[7] W. J. Le Veque, *Topics in Number Theory* v. 1, Addison-Wesley, Reading, Mass., 1965.
[8] J. Riordan, *Combinatorial Identities*, Wiley, New York, 1968.
[9] M. Ward, *Arithmetical properties of sequences in rings*, Ann. of Math., **39** (1938), 210–219.
[10] A. Weil, *Number of solutions of equations in finite fields*, Bull. Amer. Math. Soc., **55** (1949), 497–508.

Received February 16, 1982 and in revised form October 28, 1982.

UNIVERSITY OF SAN DIEGO
SAN DIEGO, CA 92110