# VANISHING SUMS OF ROOTS OF UNITY

H W Lenstra, Jr

## INTRODUCTION

This paper is a survey of what is known about the magnitude of coefficients appearing in linear relations between roots of unity. The special case of the cyclotomic polynomial is considered in section 1; section 2 is devoted to more general relations. Various open problems will be indicated.

By n and m we shall always mean positive integers, and by p a prime number; n is called *squarefree* if n is a product of distinct primes. By $m|n$ we mean that m divides n. An *n-th root of unity*, or simply an *n-th root*, is a complex number $\alpha$ for which $\alpha^n = 1$. It is called *primitive* if there exists no $m < n$ with $\alpha^m = 1$. The ring of integers is denoted by $\mathbb{Z}$, and $\mathbb{Q}$ denotes the field of rational numbers.

Research for this paper was supported by the Netherlands Organization for the Advancement of Pure Research (Z.W.O). Acknowledgements are due to the I.H.E.S. for its hospitality and to C.L. Stewart for providing ref. [10].

## 1. Coefficients of the cyclotomic polynomial

The n-th cyclotomic polynomial $\Phi_n$ is defined by

$$\Phi_n = \prod_{\zeta} (X - \zeta), \tag{1.1}$$

where $\zeta$ ranges over the primitive n-th roots of unity. We have

$$\prod_{d|n} \Phi_d = X^n - 1 \tag{1.2}$$

since both sides are equal to $\prod_{\zeta, \zeta^n=1} (X - \zeta)$. From (1.2) one deduces, by induction on n, that $\Phi_n$ has coefficients in $\mathbb{Z}$. Its degree is $\phi(n)$, where $\phi$ is Euler's function.

$$\phi(n) = \left|\{j:\ 0 \le j < n,\ (j,n) = 1\}\right|.$$

The cyclotomic polynomials are known to be irreducible in the polynomial ring $\mathbb{Q}[X]$.

By Moebius inversion it follows from (1.2) that

$$\Phi_n = \prod_{d|n} (X^d - 1)^{\mu(n/d)}. \tag{1.3}$$

Here $\mu$ denotes the Moebius-function:

$$\mu(m) = (-1)^r \quad \text{if } m \text{ is the product of } r \text{ distinct primes, } r \ge 0,$$
$$\mu(m) = 0 \quad \text{otherwise.}$$

The polynomials $\Phi_n$ can be determined inductively, using the formulae

$$\Phi_1 = X - 1$$

$$\Phi_{np} = \Phi_n(X^p) \quad \text{if } p \text{ divides } n, \tag{1.4}$$

$$\Phi_{np} = \Phi_n(X^p)/\Phi_n \quad \text{if } p \text{ does not divide } n. \tag{1.5}$$

To prove these relations, use (1.3), or check that both sides have the same zeros. In a similar way one proves that

$$\Phi_{2n} = (-1)^{\phi(n)} \cdot \Phi_n(-X) \quad \text{if } n \text{ is odd.} \tag{1.6}$$

For small $n$, no coefficient of $\Phi_n$ exceeds 1 in absolute value. In fact, this is true for $n = p$:

$$\Phi_p = (X^p - 1)/(X - 1) = 1 + X + X^2 + \ldots + X^{p-1},$$

and also for $n = pq$, where $p$ and $q$ are different primes:

$$\Phi_{pq} = \frac{(1-X)(1-X^{pq})}{(1-X^p)(1-X^q)} = \qquad \text{(by (1.3))}$$

$$= (1-X) \cdot \sum_{j=0}^{\infty} X^{jp} \cdot \sum_{k=0}^{p-1} X^{kq} = (1-X) \cdot \sum X^{\alpha}$$

where $\alpha$ ranges over the numbers of the form $jp+kq$, with $j \geq 0$, $0 \leq k < p$, it is easily proved that no integer has more than one such representation. Multiplying $\Sigma X^{\alpha}$ by $(1-X)$ we see that the non-zero coefficients of $\Phi_{pq}$ are alternately $+1$ and $-1$. For a different formula for $\Phi_{pq}$, see (2.16).

From what we just proved and the formulae (1.4) and (1.6) it follows immediately that no coefficient of $\Phi_n$ exceeds 1 in absolute value if n has at most two distinct odd prime factors. The smallest number n not satisfying this condition is $3.5.7 = 105$, and in fact in $\Phi_{105}$ a coefficient $-2$ appears:

$$\begin{aligned}\Phi_{105} = {} & 1 + X + X^2 - X^5 - X^6 - 2X^7 - X^8 - X^9 \\ & + X^{12} + X^{13} + X^{14} + X^{15} + X^{16} + X^{17} \\ & - X^{20} - X^{22} - X^{24} - X^{26} - X^{28} \\ & + X^{31} + X^{32} + X^{33} + X^{34} + X^{35} + X^{36} \\ & - X^{39} - X^{40} - 2X^{41} - X^{42} - X^{43} + X^{46} + X^{47} + X^{48}.\end{aligned}$$

It was first proved by Schur (see [13]) that the coefficients of the cyclotomic polynomials are arbitrarily large in absolute value. In order to present his argument it is convenient to rearrange formula (1.3) as follows.

$$\Phi_n = \Pi^{I}(1-X^d).\Pi^{II}(1+X^d+X^{2d}+\ldots) \tag{1.7}$$

$(n > 1)$, where in $\Pi^{I}$ the product is over the divisors d of n with $\mu(n/d) = 1$, and in $\Pi^{II}$ over those for which $\mu(n/d) = -1$.

Now let t be an odd integer $\geq 3$, and let $p_1, p_2, \ldots, p_t$ be prime numbers with

$$2 < p_1 < p_2 < \ldots < p_t < p_1 + p_2;$$

such primes can be found for every t. We put $n = p_1 p_2 \ldots p_t$ and we calculate $\Phi_n$ modulo terms of degree $\geq p_t + 1$ using formula (1.7). The only divisors of n which are $< p_t + 1$ are $1, p_1, p_2, \ldots, p_t$, and since t is odd we obtain

$$\Phi_n \equiv (1-X^{p_1})(1-X^{p_2})\ldots(1-X^{p_t})(1+X+X^2+\ldots+X^{p_t})$$
$$\equiv (1-X^{p_1}-X^{p_2}-\ldots-X^{p_t})\ (1+X+X^2+\ldots X^{p_t})$$

modulo terms of degree $\geq p_t + 1$. Multiplying out we find that the coefficient at $X^{p_t}$ equals $1 - t$, thus finishing the proof.

From (1.7) and the fact that $\Phi_n$ has degree less than n, for $n > 1$, it is clear that any coefficient of $\Phi_n$ is in absolute value less than or equal to the corresponding coefficient of

$$\prod_{d|n} (1 + X^d + X^{2d} + \ldots + X^{n-d}).$$

Since the coefficients of this polynomial are positive, they are bounded from above by the value of the polynomial in 1, which equals

$$\prod_{d|n} \frac{n}{d} = n^{\tau(n)/2}.$$

Here $\tau(n)$ denotes the number of divisors of n. Using the fact that

$$\tau(n) < 2^{(1+\varepsilon)\log n/\log\log n}$$

for all $\varepsilon > 0$ and all $n > n_0(\varepsilon)$ (see [9, theorem 317]) we find, after an easy manipulation:

THEOREM (1.8) *For every real number* $\varepsilon > 0$ *there exists an integer* $n_0(\varepsilon)$ *such that for all* $n > n_0(\varepsilon)$ *the absolute value of any coefficient of* $\Phi_n$ *is less than*

$$\exp(n^{(1+\varepsilon)\log 2/\log\log n}).$$

Notice that this estimate, which is due to BATEMAN [2], is much better than the trivial upper bound

$$2^{\phi(n)}$$

for the sum of the absolute values of the coefficients of $\Phi_n$, which one obtains from (1.1) by using $|\zeta| = 1$.

Bateman's estimate is in a sense best possible, since VAUGHAN [19] has

shown that there are infinitely many n for which $\Phi_n$ has a coefficient exceeding

$$\exp(n^{\log 2 / \log \log n})$$

in absolute value.

Using Bateman's argument and [9, theorem 432] one finds that for every $\varepsilon > 0$ the sum of the absolute values of the coefficients of $\Phi_n$ is less than

$$\exp((\log n)^{1+\log 2+\varepsilon})$$

for almost all n. Non-trivial lower bounds valid for almost all n are not known.

Bounds of a different nature have been obtained for numbers n having only a few odd prime factors. Using (1.4) and (1.6) we again restrict to the case n is odd and squarefree.

For $n = p$ and $n = pq$ we have already seen that $\Phi_n$ has no coefficient exceeding 1 in absolute value. For $n = pqr$, with p, q and r primes, $2 < p < q < r$, it was proved by BANG (see [4]) that all coefficients of $\Phi_n$ are at most

$$p - 1$$

in absolute value. This bound was improved to

$$p - k \quad \text{if } p = 4k \pm 1, \quad k \in \mathbb{Z},$$

by BEITER [3], and she conjectured that it may further be lowered to

$$\frac{p+1}{2}.$$

This result, if true, would be best possible, since MOLLER [17] proved that for every odd prime p there exist infinitely many prime pairs q, r with $p < q < r$, for which $\Phi_{pqr}$ has a coefficient $\frac{1}{2}(p+1)$.

For $n = pqrs$, with p,q,r,s primes, $2 < p < q < r < s$, the coefficients of $\Phi_n$ are bounded by

$$p(p - 1)(pq - 1)$$

in absolute value. This was proved by BLOOM [4]. He conjectured that, generally, for

$$n = p_1 p_2 \cdots p_t$$

with $p_1, p_2, \ldots, p_t$ primes, $2 < p_1 < p_2 < \ldots < p_t$, $t \geq 2$, the coefficients of $\Phi_n$ are bounded in absolute value by a number depending only on $p_1, p_2, \ldots, p_{t-2}$. This conjecture was proved by FELSCH and SCHMIDT [8] and JUSTIN [11]:

THEOREM (1.9) *There is a function* f *on the positive integers, such that for all* m, *and all primes* p,q *with*

$$p \neq q, \quad (pq,m) = 1,$$

*the coefficients of* $\Phi_{mpq}$ *are less than* f(m) *in absolute value.*

We present Justin's elegant proof of this theorem.
Define the polynomials $\Psi_n$ by

$$\Psi_n \cdot \Phi_n = 1 - X^n.$$

Let m,p,q be as in the theorem. Applying (1.5) twice we get

$$\Phi_{mpq} = \frac{\Phi_m(X^{pq}) \cdot \Phi_m}{\Phi_m(X^p) \cdot \Phi_m(X^q)}$$

$$= \Phi_m(X^{pq}) \cdot \Phi_m \cdot \Psi_m(X^p) \cdot \Psi_m(X^q) \cdot (1 - X^{mp})^{-1} \cdot (1 - X^{mq})^{-1} \tag{1.10}$$

$$= A \cdot B$$

where A is the product of the first four factors in (1.10), and B is the power series

$$\sum_{j,k \geq 0} X^{jmp + kmq}.$$

If $\Phi_m = \sum_i a_i X^i$, $\Psi_m = \sum_i b_i X^i$, then the sum of the absolute values of the coefficients of A is clearly bounded by

$$\Big(\sum_i |a_i|\Big)^2 \cdot \Big(\sum_i |b_i|\Big)^2. \tag{1.11}$$

Further, if $B = \sum_i c_i X^i$ then $c_i \in \{0,1\}$ for all $i < mpq$, since no number less than $mpq$ has more than one representation $jmp + kmq$, $j \geq 0$, $k < 0$. Multiplying A and B, and observing that the product $\Phi_{mpq}$ has degree $< mpq$, we conclude that all coefficients of $\Phi_{mpq}$ are bounded in absolute value by (1.11). Since this number depends only on m the theorem follows.

An explicit function f for which the conclusion of the theorem holds has been given by MÖLLER [17].

In the next section we shall see that there exists a positive constant $C_1$ such that for all squarefree $n > 1$ the number of non-zero coefficients of $\Phi_n$ exceeds

$$C_1 (\log n)^2 / \log \log n,$$

see (2.8). Schinzel has posed the problem to improve this estimate. It is known that for every $\varepsilon > 0$ there exist infinitely many squarefree n for which $\Phi_n$ has less than

$$n^{\frac{8}{13}+\varepsilon}$$

non-zero coefficients (see (2.18)). This could be improved to $(8n)^{1/2}$ if it were known that for infinitely many primes p, one of $2p + 1$ and $2p - 1$ is prime. It is an interesting problem to construct squarefree integers n for which $\Phi_n$ has substantially fewer non-zero coefficients. A question which may be related is the following: do there exist numbers n, divisible by arbitrarily many distinct primes, for which $\Phi_n$ has only coefficients -1, 0,1?

Finally we mention some results on the behaviour of the i-th coefficient - i.e., the coefficient at $X^i$ - of the cyclotomic polynomials, for fixed i. For squarefree n, it is clear from (1.7) that the i-th coefficient of $\Phi_n$ only depends on those primes $p \leq i$ which divide n, and on the parity of the total number of primes dividing n. In particular, the i-th coefficient can assume only finitely many values, and it is easily seen that this assertion remains valid if we drop the restriction that n should be squarefree.

LEHMER [12] has given a table of the i-th coefficient of $\Phi_n$ for $i \leq 10$ and n odd and squarefree, distinguishing 16 cases according to the value of $\mu(n)$ and the greatest common divisor of n and 105. His table implies that

for $i \leq 10$ the $i$-th coefficient is one of 1, 0, -1, except if $n = 105\,p_1p_2\cdots p_{2h}$ ($p_i$ distinct primes $> 7$), in which case the 7-th coefficient equals -2. Compare also MOLLER [16].

ERDOS and VAUGHAN [7] proved that for all $i$ the $i$-th coefficient of $\Phi_n$ is bounded in absolute value by

$$\exp(C_0 \cdot i^{1/2} + C_2 i^{3/8});$$

here $C_2$ is some constant, and $C_0 = 2 \cdot \prod_p (1 - \frac{2}{p(p+1)})^{\frac{1}{2}} \approx 1.373580$. On the other hand, they proved that for some constant $C_3 > 0$ and all sufficiently large $i$ there exists $n$ for which the $i$-th coefficient of $\Phi_n$ exceeds

$$\exp(C_3 (i/\log i)^{\frac{1}{2}})$$

in absolute value. VAUGHAN [19] proved that for infinitely many $i$ this can be improved to

$$\exp(C_4 \cdot i^{1/2}/(\log i)^{1/4}).$$

Here $C_4$ denotes a positive constant.

## 2. Primitive relations between roots of unity.

Let $\{\zeta_1, \zeta_2, \ldots, \zeta_k\}$ be a set of $k$ distinct roots of unity, $k > 0$, which is linearly dependent over $\mathbb{Q}$, while no proper subset is; *proper* means: not empty, and not the whole set. Then there is a relation

$$\sum_{i=1}^{k} \lambda_i \zeta_i = 0$$

($\lambda_i$ rational, not all zero), and this relation is uniquely determined up to a rational multiple. Multiplying by a common denominator we can make the $\lambda_i$ into integers, and dividing by their greatest common divisor we arrive at a relation

$$\sum_{i=1}^{k} a_i \zeta_i = 0$$

in which the coefficients $a_i$ are non-zero integers with greatest common

divisor 1. A linear relation which arises in this way is called a *primitive* relation. It is clear that if $\Sigma_{i=1}^{k} a_i'\zeta_i = 0$ is another primitive relation between the same $\zeta_i$, then we have either $a_i' = a_i$ for all i, or $a_i' = -a_i$ for all i.

If we have $\Sigma_{i=1}^{k} a_i\zeta_i = 0$, and $\rho$ is a root of unity, then we have also $\Sigma_{i=1}^{k} a_i(\rho\zeta_i) = 0$; two such relations are said to be *similar*. Clearly, any relation is similar to one with $\zeta_1 = 1$.

The *exponent* of a relation $\Sigma_{i=1}^{k} a_i\zeta_i = 0$ is the smallest integer $n > 0$ for which $\zeta_i^n = 1$ for all i, and the *reduced exponent* is the smallest n for which $(\zeta_i\zeta_j^{-1})^n = 1$ for all i,j. Notice that two similar relations have the same reduced exponent, and that in the case where $\zeta_1 = 1$ the reduced exponent coincides with the exponent.

If $\Phi_n = \Sigma\, c_i X^i$ is the n-th cyclotomic polynomial, and $\zeta$ is a primitive n-th root, then we have

$$(2.1) \qquad \sum_{i,\, c_i \neq 0} c_i \zeta^i = 0.$$

This is a primitive relation, since $\Phi_n$ has leading coefficient 1 and is irreducible over $\mathbb{Q}$. The reduced exponent of (2.1) is the product of the distinct primes dividing n, this follows from (1.4) and the fact that $c_0 \neq 0 \neq c_1$ if n is squarefree (use (1.7)).

In this section we are interested in the number of terms k and the magnitudes of the coefficients $a_i$ in a primitive relation of reduced exponent n. The results are much less complete than those known in the special case of the cyclotomic polynomial.

In (2.2) and (2.3) we describe the general technique for dealing with vanishing sums of roots of unity, cf. [15, 6].

THEOREM (2.2) *Let* m *be the product of the different primes dividing* n, *and let* $\varepsilon,\zeta$ *denote primitive* m*-th and* n*-th roots, respectively. Then* $\{\varepsilon^i\zeta^j$. $0 \le i < m,\ 0 \le j < n/m\}$ *is the set of* n*-th roots, and*

$$\sum_{i=0}^{m-1} \sum_{j=0}^{(n/m)-1} a_{ij}\varepsilon^i\zeta^j = 0 \qquad (a_{ij} \in \mathbb{Z})$$

*if and only if*

$$\sum_{i=0}^{m-1} a_{ij}\varepsilon^i = 0$$

*for every* j, $0 \le j < n/m$.

This theorem readily follows from the irreducibility of $X^{n/m} - \zeta^{n/m}$ over the field $\mathbb{Q}(\varepsilon)$; to prove this irreducibility, just notice that $[\mathbb{Q}(\zeta):\mathbb{Q}(\varepsilon)] = \phi(n)/\phi(m) = n/m$. For details we refer to [15, 6].

Theorem (2.2) reduces the analysis of vanishing sums of n-th roots to the case that n is squarefree. It follows in particular, that the reduced exponent of a primitive relation is necessarily squarefree.

Relations of squarefree exponent n can be treated by induction on the number of primes dividing n, using the following theorem.

THEOREM (2.3) *Let* $n = pm$, *where* p *is prime and* p *does not divide* m, *and let* $\varepsilon,\zeta$ *denote primitive* m*-th and* p*-th roots, respectively. Then* $\{\varepsilon^i\zeta^j: 0 \le i < m,\ 0 \le j < p\}$ *is the set of* n*-th roots, and*

$$\sum_{i=0}^{m-1}\sum_{j=0}^{p-1} a_{ij}\varepsilon^i\zeta^j = 0 \qquad (a_{ij} \in \mathbb{Z}) \tag{2.4}$$

*if and only if*

$$\sum_{i=0}^{m-1} a_{ij}\varepsilon^i - \sum_{i=0}^{m-1} a_{i0}\varepsilon^i = 0 \tag{2.5}$$

*for all* j, $1 \le j < p$.

The proof of this theorem depends on the irreducibility of $X^{p-1} + \ldots + X^2 + X + 1$ over $\mathbb{Q}(\varepsilon)$, which is a consequence of $[\mathbb{Q}(\varepsilon,\zeta):\mathbb{Q}(\varepsilon)] = \phi(n)/\phi(m) = p - 1$. Compare with [15, 6].

If, in (2.4), there exists j' with $a_{ij'} = 0$ for all i, then (2.5) clearly yields

$$\sum_{i=0}^{m-1} a_{ij}\varepsilon^i = 0$$

for all j, $0 \le j < p$, which means that the vanishing sum (2.4) of n-th roots decomposes in vanishing sums of m-th roots. On the other hand, if for every j there exists i with $a_{ij} \neq 0$, then (2.4) has at least p non-zero terms. In particular, it follows that if $\sum_{i=1}^{k} a_i\zeta_i = 0$ is a primitive relation of reduced exponent n, then $k \ge p$, where p is the largest prime divid-

ing n. A more precise result is given by the following theorem, due to CONWAY and JONES [6]. In this theorem, we call a relation $\sum_{i=1}^{k} a_i\zeta_i = 0$ *minimal* if there is no proper subset $I \subset \{1,2,\ldots,k\}$ with $\sum_{i\in I} a_i\zeta_i = 0$; clearly, any primitive relation is minimal.

THEOREM (2.6) *If* $\sum_{i=1}^{k} a_i\zeta_i = 0$ *is a minimal relation of reduced exponent* n, *then* n *is squarefree, and*

$$(2.7) \qquad k \geq \sum_{p\mid n} (p-2) + 2,$$

*the sum ranging over the primes* p *dividing* n. *Conversely, for every squarefree integer* n *there exists a minimal relation of reduced exponent* n *for which equality holds in* (2.7).

For the proof of this theorem we refer to [6]. Conway and Jones used (2.6) to classify all linear relations between roots of unity of less than 10 terms.

As is remarked in [6], one can deduce from (2.6) that for every $C > 1$ there exists $C'$ such that

$$n \leq C'.\exp(C(k \log k)^{\frac{1}{2}})$$

for all n, k as in (2.6). It follows that

$$(2.8) \qquad k \geq C_1 \cdot (\log n)^2/\log\log n \qquad (n > 1)$$

for some positive constant $C_1$.

Various interesting theorems in elementary geometry have been proved by the use of the technique described in (2.2) and (2.3). An appropriate one to mention at this occasion is a result appearing in G. Bol's "Beantwoording van prijsvraag no. 17" [5]:

if n is odd, $n \geq 3$, then no three diagonals of a regular n-gon pass through one point, unless they have the same endpoint.

Let the n-gon have as its vertices the n-th roots of unity in the complex plane, and suppose that the diagonals $\alpha\beta$, $\gamma\delta$, $\varepsilon\zeta$ intersect in one point. For a complex number x to be on the line through $\alpha$ and $\beta$ it is necessary and sufficient that

$$\frac{x-\alpha}{\beta-\alpha} = \frac{\bar{x}-\bar{\alpha}}{\bar{\beta}-\bar{\alpha}}$$

which by $\bar{\alpha} = \alpha^{-1}$, $\bar{\beta} = \beta^{-1}$ simplifies to

$$x + \alpha\beta\bar{x} = \alpha + \beta.$$

Hence, if x is on all three diagonals $\alpha\beta$, $\gamma\delta$, $\varepsilon\zeta$ we must have

$$(2.9) \qquad \begin{vmatrix} 1 & \alpha\beta & \alpha+\beta \\ 1 & \gamma\delta & \gamma+\delta \\ 1 & \varepsilon\zeta & \varepsilon+\zeta \end{vmatrix} = 0.$$

Working out the determinant we see that (2.9) is a vanishing sum of twelve roots of unity. This observation makes (2.2), (2.3) applicable, and after some work we arrive at Bol's result. For more applications of (2.2), (2.3) we refer to [6].

The following theorem gives a bound for the coefficients appearing in a primitive relation.

THEOREM (2.10) *Let* $\sum_{i=1}^{k} a_i \zeta_i = 0$ *be a primitive relation between* k *roots of unity. Then*

$$|a_i| \leq 2^{1-k} \cdot k^{k/2}$$

*for* $i = 1,2,\ldots,k$.

In the proof of this theorem we denote by n the reduced exponent of the relation. We know that n is squarefree, and we may assume that the $\zeta_i$ are n-th roots.

LEMMA (2.11) [cf. 18]. *Let* n *be squarefree. Then for every* n*-th root* $\zeta$ *either* $\zeta$ *or* $-\zeta$ *is a sum of distinct primitive* n*-th roots. Further, the primitive* n*-th roots are linearly independent over* $\mathbb{Q}$.

PROOF OF (2.11) We first prove by induction on the number of primes dividing n that every n-th root $\zeta$ is plus or minus a sum of primitive ones. For $n = 1$ this is obvious. For $n = p$, the case $\zeta = 1$ is dealt with by

$$1 = -\sum_{\zeta} \alpha$$

($\alpha$ ranging over the primitive p-th roots), and in the case $\zeta \neq 1$ the representation

$$\zeta = \zeta$$

works. If $n \neq 1$, p then we can write $n = \ell \cdot m$, with $\ell, m < n$, $(\ell, m) = 1$. Every n-th root $\zeta$ has a unique representation $\zeta = \eta\theta$, where $\eta, \theta$ are $\ell$-th and m-th roots, respectively. By the induction hypothesis, we can write

$$\eta = \pm \sum \beta, \qquad \theta = \pm \sum \gamma,$$

where $\beta$ ranges over a certain set of primitive $\ell$-th roots and $\gamma$ over a certain set of primitive m-th roots. Multiplying we find

$$\zeta = \pm \sum \beta\gamma .$$

Each term $\beta\gamma$ is a primitive n-th root, and no primitive n-th root occurs twice. This proves our assertion that every n-th root is $\pm$ a sum of primitive ones.

It follows that the $\phi(n)$ primitive n-th roots span the $\mathbb{Q}$-vector space generated by all n-th roots. But by the irreducibility of $\Phi_n$ this vector space has dimension $\phi(n)$. We conclude that the primitive n-th roots are linearly independent over $\mathbb{Q}$. In particular, for no n-th root $\zeta$ can both $\zeta$ and $-\zeta$ be written as a sum of distinct primitive n-th roots. This proves lemma (2.11).

Continuing the proof of the theorem, we write, using the lemma

$$\pm\zeta_i = \sum_{\alpha} e_{i\alpha}\alpha, \qquad 1 \leq i \leq k,$$

with $\alpha$ ranging over the primitive n-th roots and $e_{i\alpha} = 0$ or 1 for all $i,\alpha$. By the primitivity of the relation $\Sigma\, a_i\zeta_i = 0$, the $k \times \phi(n)$-matrix $(e_{i\alpha})_{i,\alpha}$ has rank $k-1$. Choose a $k \times (k-1)$-submatrix of rank $k-1$. If $b_1, b_2, \ldots, b_k$ denote the $(k-1) \times (k-1)$ determinants of this submatrix in a suitable order, and provided with suitable signs, then

$$\sum_{i=1}^{k} b_i e_{i\alpha} = 0$$

for all $\alpha$, so

$$\sum_{i=1}^{k} (\pm b_i)\zeta_i = 0.$$

Here the coefficients $\pm b_i$ are in $\mathbb{Z}$, and they do not all vanish. Since the relation $\sum_{i=1}^{k} a_i\zeta_i = 0$ is primitive it follows that $\pm b_i = ca_i$ for some non-zero integer c and all i, so

$$|a_i| \le |b_i|.$$

Thus, to finish the proof of the theorem it suffices to prove the following lemma.

LEMMA (2.12) *Let* $B = (\beta_{ij})$ *be a* $(k-1) \times (k-1)$*-matrix with* $\beta_{ij} = 0$ *or* $1$ *for all* $i,j$, $1 \le i,j \le k-1$. *Then* $|\det B| \le 2^{1-k} \cdot k^{k/2}$.

PROOF. Define the $k \times k$-matrix $C = (\gamma_{ij})$ by

$$\gamma_{ij} = 2\beta_{ij} - 1 \qquad 1 \le i,j \le k-1,$$

$$\gamma_{kj} = -1 \qquad 1 \le j \le k-1,$$

$$\gamma_{ik} = 1 \qquad 1 \le i \le k.$$

By elementary column operations, $\det C = 2^{k-1} \cdot \det B$. Further $\gamma_{ij} = \pm 1$ for all i,j, so from Hadamard's inequality

$$|\det(\gamma_{ij})| \le \prod_{i=1}^{k} \left( \sum_{j=1}^{k} \gamma_{ij}^2 \right)^{1/2}$$

we get

$$|\det C| \le k^{k/2},$$

$$|\det B| = |2^{1-k} \cdot \det C| \le 2^{1-k} \cdot k^{k/2}.$$

This proves (2.12) and (2.10).

It is not known whether theorem (2.10) is best possible.

If n = p is prime, then the only primitive relation of exponent n is

$$\pm\sum \zeta = 0,$$

$\zeta$ ranging over all n-th roots. In the case $n = pq$, p and q distinct primes, all primitive relations have been determined by MANN [15]:

THEOREM (2.13) *Let* p *and* q *be primes,* $p \neq q$, *and let* $A,A',B,B'$ *be non-empty sets of roots of unity such that*

$$A \cup A' = \{\textit{all p-th roots}\}, \qquad A \cap A' = \emptyset,$$

$$B \cup B' = \{\textit{all q-th roots}\}, \qquad B \cap B' = \emptyset.$$

*Then*

$$\sum_{\alpha\in A}\sum_{\beta\in B}\alpha\beta - \sum_{\alpha\in A'}\sum_{\beta\in B'}\alpha\beta = 0.$$

*This is a primitive relation of reduced exponent* pq, *and every primitive relation of reduced exponent* pq *is similar to one of this form.*

For the proof, which is a direct application of (2.3), we refer to [15].

Theorem (2.13) suggests a representation for $\Phi_{pq}$ which is different from the one we have seen in section 1. Let $\Phi_{pq} = \sum c_i X^i$, and let $\zeta$ be a primitive pq-th root. Then $\sum_{i,c_i\neq 0} c_i\zeta^i = 0$ is a primitive relation of reduced exponent pq, and one may wonder which sets $A,A',B,B'$ correspond to this relation. A few trials suggest that one should take

(2.14) $$A = \{\zeta^{jq}: 0 \le j < \mu\}, \qquad A' = \{\zeta^{jq}: \mu \le j < p\},$$

(2.15) $$B = \{\zeta^{ip}: 0 \le i < \lambda\}, \qquad B' = \{\zeta^{iq}: \lambda \le i < q\},$$

where the integers $\lambda,\mu$ are determined by

$$\lambda p \equiv 1 \bmod q, \qquad 0 < \lambda < q,$$

$$\mu q \equiv 1 \bmod p, \qquad 0 < \mu < p.$$

Notice that $\lambda p + \mu q = 1 + pq$, since $\lambda p + \mu q \equiv 1 \bmod pq$, $1 < \lambda p + \mu q < 2pq$. Thus, the choice (2.14), (2.15) for $A,A',B,B'$ is correct if and only if

$$\Phi_{pq} = \sum_{i=0}^{\lambda-1} \sum_{j=0}^{\mu-1} X^{ip+jq} - \sum_{i=\lambda}^{q-1} \sum_{j=\mu}^{p-1} X^{ip+jq-pq}. \tag{2.16}$$

Once discovered, this formula is easily verified the right hand side equals

$$\frac{(1-X^{\lambda p})(1-X^{\mu q})}{(1-X^{p})(1-X^{q})} - \frac{(X^{\lambda p}-X^{pq})(X^{\mu q} X^{pq})X^{-pq}}{(1-X^{p})(1-X^{q})}$$

and this simplifies to

$$\frac{(1-X)(1-X^{pq})}{(1-X^{p})(1-X^{q})},$$

which is $\Phi_{pq}$, by (1.3).

From (2.16) one sees that the number of non-zero coefficients of $\Phi_{pq}$ equals $2\lambda\mu - 1$. In the case $q \equiv 1 \bmod p$ we have $\mu = 1$, $\lambda = ((p-1)q+1)/p$, so

$$2\lambda\mu - 1 = \frac{2(p-1)(q-1)}{p} + 1. \tag{2.17}$$

HOOLEY [10] has shown that for every $\varepsilon > 0$ there exist infinitely many primes $q$ for which $q-1$ has a prime divisor $p$ with $p > q^{(5/8)-\varepsilon}$. Putting $n = pq$ and using (2.17) we find that for every $\varepsilon > 0$ there are infinitely many squarefree $n$ for which $\Phi_n$ has less than

$$n^{(8/13)+\varepsilon} \tag{2.18}$$

non-zero coefficients. This confirms a remark made in section 1. If $q = 2p\pm1$, then one obtains in the same way less than $(8n)^{\frac{1}{2}}$ non-zero coefficients, with $n = pq$. It is unknown, however, whether for infinitely many primes $p$ one of $2p+1$ and $2p-1$ is prime.

Theorem (2.13) implies that primitive relations of reduced exponent $pq$ have *no coefficients other than* $\pm 1$. *Combining this observation with theorem* (1.9) one is led to the following question:

> does there exist a function $f$ on the positive integers, such that for all $m$, and all primes $p,q$ with $p \neq q$, $(pq,m) = 1$, and all primitive relations $\sum_{i=1}^{k} a_i \zeta_i = 0$ of reduced exponent $mpq$, the coefficients $a_i$ are bounded in absolute value by $f(m)$?

I do not know the answer to this question. Theorem (2.19) gives a partial

result.

THEOREM (2.19) *There exists a function* f *on the positive integers such that for all* m, *all primes* p *not dividing* m, *and all primitive relations* $\Sigma_{i=1}^{k} a_i\zeta_i = 0$ *of reduced exponent* mp, *the coefficients* $a_i$ *are less than* f(m) *in absolute value.*

PROOF. Let p be an odd prime not dividing m, let R be the set of p-th roots, and let B be the set of m-th roots. Any mp-th root $\alpha$ has a unique expression as $\alpha = \beta\rho$, with $\beta \in B$, $\rho \in R$, so the given primitive relation is similar to one of the form

$$\sum_{\rho\in R} \sum_{\beta\in B(\rho)} a_{\beta\rho}\beta\rho = 0 \tag{2.20}$$

where $B(\rho) \subset B$ for each $\rho \in R$, and all $a_{\beta\rho} \neq 0$. Using (2.3) we find that

$$\sum_{\beta\in B(\rho)} a_{\beta\rho}\beta = \sum_{\beta\in B(\rho')} a_{\beta\rho'}\beta \tag{2.21}$$

for any two $\rho,\rho' \in R$. Thus, if some $B(\rho')$ were empty, then all these sums would vanish, contradicting that (2.20) is a primitive relation of reduced exponent mp. We conclude that the $B(\rho)$ are non-empty. Next we claim that

$$B(\sigma) = B(\sigma') \Rightarrow a_{\beta\sigma} = a_{\beta\sigma'} \quad \text{for all } \beta \in B(\sigma) \tag{2.22}$$

$(\sigma,\sigma' \in R)$. In fact, if this would not be true, then by putting

$$c_{\beta\rho} = a_{\beta\rho} \quad \text{if } \rho \in R,\ \rho \neq \sigma,\sigma',\ \beta \in B(\rho),$$

$$c_{\beta\sigma} = a_{\beta\sigma'} \quad \text{if } \beta \in B(\sigma)$$

$$c_{\beta\sigma'} = a_{\beta\sigma} \quad \text{if } \beta \subset B(\sigma)$$

we would get a relation

$$\sum_{\rho\in R} \sum_{\beta\in B(\rho)} c_{\beta\rho}\beta\rho = 0,$$

which is not plus or minus the original relation (2.20) (here we use $p \geq 3$), contradicting the primitivity.

Now let q be the smallest prime larger than $2^m$, and let T be the set of q-th roots. The number of different sets $B(\rho)$, $\rho \in R$, is clearly less than q, so we are able to choose, for every $\tau \in T$, a subset $C(\tau) \subset B$ such that

$$\{C(\tau): \tau \in T\} = \{B(\rho): \rho \in R\}.$$

Define $b_{\beta\tau}$ for $\tau \in T$, $\beta \in C(\tau)$ by

$$b_{\beta\tau} = a_{\beta\sigma}$$

where $\sigma \in R$ is chosen such that $B(\sigma) = C(\tau)$; by (2.22) this definition does not depend on the choice of $\sigma$. By (2.21) we have

$$\sum_{\beta \in C(\tau)} b_{\beta\tau}\beta = \sum_{\beta \in C(\tau')} b_{\beta\tau'}\beta$$

for all $\tau, \tau' \in T$, so

$$\sum_{\tau \in T} \sum_{\beta \in C(\tau)} b_{\beta\tau}\beta\tau = 0. \tag{2.23}$$

We claim that this is a primitive relation between mq-th roots of unity. Obviously the coefficients $b_{\beta\tau}$ have greatest common divisor 1, so if (2.23) is not primitive than there exist subsets $D(\tau) \subset C(\tau)$, not all empty, and not all $D(\tau) = C(\tau)$, such that $\{\beta\tau: \tau \in T, \beta \in D(\tau)\}$ is linearly dependent over $\mathbb{Q}$. Reversal of the above procedure would then, as the reader readily checks, give rise to subsets $E(\rho) \subset B(\rho)$, not all empty, and not all $E(\rho) = B(\rho)$, such that also $\{\beta\rho: \rho \in R, \beta \subset E(\rho)\}$ is linearly dependent over $\mathbb{Q}$, and this would contradict that (2.20) is primitive.

Thus we have proved that any coefficient appearing in a primitive relation of reduced exponent mp, with p an odd prime not dividing m, appears in a primitive relation between mq-th roots. But q depends only on m, and there are only finitely many primitive relations of given exponent. Hence there are only finitely many coefficients, and this conclusion remains unaffected if we also allow p = 2. This proves theorem (2.19).

REFERENCES

[1] APOSTOL, T.M., *The resultant of the cyclotomic polynomials* $F_m(ax)$ *and* $F_n(bx)$, Math. Comp. 29 (1975), p. 1-6.

[2] BATEMAN, P.T., *Note on the coefficients of the cyclotomic polynomial*, Bull. Amer. Math. Soc. 55 (1949), p. 1180-1181.

[3] BEITER, M., *Magnitude of the coefficients of the cyclotomic polynomial* $F_{pqr}$, II, Duke Math. J. 38 (1971), p. 591-594.

[4] BLOOM, D.M., *On the coefficients of the cyclotomic polynomials*, Amer. Math. Monthly 75 (1968), p. 372-377.

[5] BOL, G., *Beantwoording van prijsvraag no.* 17, Nieuw Archief voor Wiskunde (2), 18 (1936), p. 14-66, cf. Zentralblatt 237 # 50008, 244 # 50009.

[6] CONWAY, J.H. & A.J. JONES, *Trigonometric diophantine equations (On vanishing sums of roots of unity)*, Acta. Arith. 30 (1976), p. 229-240.

[7] ERDOS, P. & R.C. VAUGHAN, *Bounds for the r-th coefficients of cyclotomic polynomials*, J. London Math. Soc. (2), 8 (1974), p. 393-401.

[8] FELSCH, V. & E. SCHMIDT, *Uber Perioden in den Koeffizienten der Kreisteilungspolynome* $F_{np}(x)$, Math. Z. 106 (1968), p. 267-272.

[9] HARDY, G.H. & E.M. WRIGHT, *An introduction to the theory of numbers*, fourth edition, Oxford University Press 1960.

[10] HOOLEY, C., *On the largest prime factor of* $p+a$ Mathematika 20 (1973), p. 135-143.

[11] JUSTIN, J., *Bornes des coefficients du polynôme cyclotomique et de certains autres polynômes*, C.R. Acad. Sci. Paris 268 (1969), Sér. A, p. 995-997.

[12] LEHMER, D.H., *Some properties of the cyclotomic polynomial*, J. Math. Anal. Appl. 15 (1966), p. 105-117.

[13] LEHMER, E., *On the magnitude of the coefficients of the cyclotomic polynomial*, Bull. Amer. Math Soc. 42 (1936), 389-392.

[14] LeVEQUE, W.J., *Reviews in number theory*, vol. I, Amer. Math. Soc., 1974 .

[15] MANN, H.B., *On linear relations between roots of unity,* Mathematika 12 (1965), p. 107-117.

[16] MÖLLER, H., *Über die i-ten Koeffizienten der Kreisteilungspolynome,* Math. Ann. 188 (1970), p. 26-38.

[17] MÖLLER, H., *Über die Koeffizienten des n-ten Kreisteilungspolynoms,* Math. Z. 119 (1971), p. 33-40.

[18] RÉDEI, L., *Natürliche Basen des Kreisteilungskörpers,* I, Abh. Math. Sem. Univ. Hamburg 23 (1959), p. 180-200; id., II, ibid., 24 (1960), p. 12-40.

[19] VAUGHAN, R.C., *Bounds for the coefficients of cyclotomic polynomials,* Michigan Math. J. 21 (1975), p. 289-295.

For more references to the literature about cyclotomic polynomials, one should consult [1] and [14, pp. 404-411].