Die Zahl $\mathrm{card}\{H_2 \subseteq G_{\mathfrak{m}}/H_1 \colon H_2 \cong G_2\}$ unterscheidet sich von $\varrho(G_2, x)$ nur um einen beschränkten Faktor, denn

$$\mathrm{card}\{H_2 \subseteq G_{\mathfrak{m}}/H_1 \colon H_2 \cong G_2\} = \frac{1}{\varphi(p^n)} \cdot p^{\sum_{j=1}^{n} j h_j'(p)} \left(p^{n\bar{h}_n'(p)} - p^{(n-1)\bar{h}_n'(p)}\right).$$

$h_j'(p)$ sind die Invarianten von $G_{\mathfrak{m}}/H_1$. Aber $h_j(p) = h_j'(p) + O(1)$ wo $h_j(p)$ die Invarianten von $G_{\mathfrak{m}}$ sind, also

$$\mathrm{card}\{H_2 \subseteq G_{\mathfrak{m}}/H_1 \colon H_2 \cong G_2\} \geqslant C_2\varrho(G_2, x),$$

wobei C_2 nicht von H_1 abhängt, sondern bloß von G_1. Demnach ist

$$\varrho(G_1 \oplus G_2, x) \geqslant C_3\varrho(G_1, x)\varrho(G_2, x),$$

also

$$\log\varrho(G_1 \oplus G_2, x) \sim \log\varrho(G_1, x) + \log\varrho(G_2, x).$$

Wir haben damit für jede endliche abelsche Gruppe G eine asymptotische Formel für $\log\varrho(G, x)$ gewonnen: Man zerlege G in zyklische Gruppen von Primpotenzordnung G_i und summiere die entsprechenden Formeln für $\log\varrho(G_i, x)$ aus dem Satz.

3. Beispiele. Sei k ein Körper, wo $d(p^j) = \varphi(p^j)$ ist für alle j. Das gilt zum Beispiel für $k = \boldsymbol{Q}$ und jede Primzahl oder $k = \boldsymbol{Q}(\zeta_m)$ und $(p, m) = 1$. Dann ist

$$C(p) = \frac{1}{p-1}\log p,$$

$$C(p^2) = \frac{p+1}{p(p-1)}\log p, \qquad C(p, p) = \frac{2}{p-1}\log p,$$

$$C(p^3) = \frac{p^2+p+1}{p^2(p-1)}\log p, \qquad C(p^2, p) = \frac{2p+1}{p(p-1)}\log p,$$

$$C(p, p, p) = \frac{3}{p-1}\log p.$$

Literatur

[1] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, London and New York 1967.

[2] S. Lang, *Algebraic Number Theory*, Reading–London 1971.

Eingegangen 6. 7. 1973 (432)

ACTA ARITHMETICA
XXVI (1974)

On two problems of R. M. Robinson about sums of roots of unity

by

J. H. Loxton (Cambridge)

1. Introduction. Let β be a cyclotomic integer, that is an algebraic integer in a cyclotomic field. As usual, we define the maximum modulus of β, denoted by $\overline{|\beta|}$, to be the maximum of the absolute values of the conjugates of β. It is well-known that β can be represented as a sum of roots of unity. The aim of this paper is to investigate how these representations depend on the properties of β, such as its degree and maximum modulus. In particular, we consider two problems proposed by R. M. Robinson [4].

First, how can we tell whether a given cyclotomic integer can be expressed as a sum of a prescribed number of roots of unity? This problem was solved by A. Schinzel [6] who proved that a cyclotomic integer of degree d is a sum of n roots of unity only if it is a sum of n roots of unity of common degree less than

$$d(2\log d + 200\, n^2 \log 2n)^{20n^2}. \tag{1.1}$$

We shall show, by quite different methods, that this upper bound can be replaced by

$$10^{n+1} d \log\log 20d,$$

which is the main result of § 4. On the way, in § 3, we shall see that an integer in a given cyclotomic field, K say, is a sum of n roots of unity only if it is a sum of at most n roots of unity lying in the field K.

Second, how can we tell whether there is any cyclotomic integer with a given maximum modulus? For this problem, we consider two cyclotomic integers β and β^* to be equivalent if $\beta^* = \varrho\beta'$ for some conjugate β' of β and some root ϱ of unity. Clearly, equivalent cyclotomic integers have the same maximum modulus. In § 5, we shall show that there are only finitely many inequivalent cyclotomic integers with a given maximum modulus and give a method for finding them.

I would like to thank Professor J. W. S. Cassels for criticising the earlier versions of this paper, and Professors A. Schinzel and V. Ennola for stimulating discussions and correspondence.

2. Notation and preliminary lemmas. For any integer $P \geqslant 1$, we denote by $Q(P)$ the field obtained by adjoining the P-th roots of unity to the rational field Q; these are the so-called "cyclotomic fields". If β is a cyclotomic integer, we denote by $P(\beta)$ the least positive integer P such that β is in the cyclotomic field $Q(P)$ and by $N(\beta)$ the least integer n for which there is a representation of β as a sum of n roots of unity. Note that $P(\beta)$ is the highest common factor of the integers P for which β is in $Q(P)$. Finally, we call β a minimal cyclotomic integer if there is no root ϱ of unity such that $P(\varrho\beta) < P(\beta)$. Every cyclotomic integer is the product of a root of unity and a minimal cyclotomic integer, that is, is equivalent to a minimal cyclotomic integer.

The remainder of this section contains various elementary facts about cyclotomic fields.

LEMMA 1. *Suppose $P = pP_1$, where p is a prime and $p \nmid P_1$. Let ξ be a primitive p-th root of unity. Then every β in $Q(P)$ has the shape*

$$\beta = \sum_{j=0}^{p-1} a_j \xi^j \tag{2.1}$$

with the a_j in $Q(P_1)$. The representation (2.1) is not unique, but any other such representation has the form

$$\beta = \sum_{j=0}^{p-1} (a_j + a)\xi^j$$

for some a in $Q(P_1)$. The conjugates of β given by (2.1) over $Q(P_1)$ are the

$$\beta' = \sum_{j=0}^{p-1} a_j \xi^{ij} \quad (1 \leqslant i \leqslant p-1). \tag{2.2}$$

Finally, if β in (2.1) is an integer, then the a_j can all be chosen to be integers (for example, by taking $a_{p-1} = 0$).

LEMMA 2. *Suppose $P = p^N P_2$, where p is a prime, $p \nmid P_2$ and $N > 1$. Let L be a positive integer with $L < N$ and put $P = p^L P_1$. Let ξ be a primitive p^N-th root of unity. Then every β in $Q(P)$ is uniquely of the shape*

$$\beta = \sum_{j=0}^{p^L-1} a_j \xi^j \tag{2.3}$$

with the a_j in $Q(P_1)$. The a_j are integers if β is. The conjugates of β given by (2.3) over $Q(P_1)$ are the

$$\beta' = \sum_{j=0}^{p^L-1} a_j \varrho^j \xi^j \tag{2.4}$$

where ϱ runs through all the p^L-th roots of unity.

Note that in either of the situations described in Lemmas 1 and 2, if ϱ is a root of unity in $Q(P)$, then we can write

$$\varrho = a\xi^j \tag{2.5}$$

where a is a root of unity in $Q(P_1)$ and j is a rational integer.

LEMMA 3. *Suppose β lies in a cyclotomic field. Then the conjugates of $|\beta|^2$ are just the $|\beta'|^2$, where β' runs through the conjugates of β, and each conjugate of $|\beta|^2$ occurs the same number of times.*

This is a simple consequence of the fact that the cyclotomic fields are abelian (see [4], p. 211).

3. Cyclotomic integers in a given field. Let P be a positive integer and let β be an integer in the cyclotomic field $Q(P)$. We seek to describe, as far as possible, all the representations

$$\beta = \sum_{j=1}^{n} \varrho_j \tag{3.1}$$

where the ϱ_j are roots of unity. The argument is based on a method apparently first noted by H. B. Mann [3].

THEOREM 1. *Let β be a cyclotomic integer and suppose (3.1) is a representation of β as a sum of n roots of unity. Let $Q(P)$ be the smallest cyclotomic field containing β and $Q(P^*)$ the smallest cyclotomic field containing $\varrho_1, \ldots, \varrho_n$.*

(i) *If $n = N(\beta)$, then $P^* = P$.*

(ii) *If $n = N(\beta)+1$, then $P^* = P$ or $3P$, but the latter case can only occur if $3 \nmid P$.*

(iii) *If $n \geqslant N(\beta)+2$, then P^* may be any integer divisible by both P and 3.*

COROLLARY. *A cyclotomic integer is a sum of n roots of unity in infinitely many ways if and only if it is a sum of m roots of unity for some $m \leqslant n-2$.*

The above corollary was proved by Schinzel [6] as a consequence of the estimate (1.1), but it also follows at once from Theorem 1.

Proof of Theorem 1. The proof falls into two parts. We begin by proving (i) and (ii). Suppose that $n \leqslant N(\beta)+1$ in (3.1) and define P

and P^* as in the statement of the theorem. Clearly $P|P^*$. If $P\nmid P^*$, then one of the following two cases arises.

First case. Suppose there is a prime p and an integer $N>1$ such that $p^N\|P^*$ but $p^N\nmid P$. Put $P^*=pP_1$ and let ξ be a primitive p^N-th root of unity. As in (2.5), we can express each ϱ_j in the form

$$\varrho_j=\gamma_j\xi^{r_j}, \tag{3.2}$$

where γ_j is a root of unity in $Q(P_1)$ and $0\leqslant r_j\leqslant p-1$. Collecting terms with the same value of r_j in (3.1), we obtain

$$\beta=\sum_{j=0}^{p-1}a_j\xi^j \tag{3.3}$$

where

$$a_j=\sum_{r_i=j}\gamma_i\quad(0\leqslant j\leqslant p-1). \tag{3.4}$$

But now β and each a_j are in $Q(P_1)$, so by Lemma 2,

$$\beta=a_0\quad\text{and}\quad a_1=a_2=\ldots=a_{p-1}=0. \tag{3.5}$$

Since $p^N\|P^*$, there is an integer j $(1\leqslant j\leqslant p-1)$ for which the set $\{i: r_i=j\}$ is not empty and so, by (3.5), contains at least two elements. But now the first equation in (3.5) expresses β as a sum of at most $n-2$ roots of unity, contradicting the hypothesis that $n\leqslant N(\beta)+1$.

Second case. Suppose there is a prime p such that $p\|P^*$ but $p\nmid P$. Note that $p=2$ cannot occur here, because if $2\nmid N$, we have $Q(2N)=Q(N)$. Put $P^*=pP_1$ and let ξ be a primitive p-th root of unity. Again, we have the equations (3.2), (3.3) and (3.4), with β and each a_j in $Q(P_1)$. So by Lemma 1,

$$a_0-\beta=a_1=\ldots=a_{p-1}=a\ \text{(say)}. \tag{3.6}$$

If $a=0$, we reach a contradiction as in the first case. So suppose $a\neq 0$. From (3.6), the equation $\beta=a_0-a$ expresses β as a sum of at most $n-(p-2)N(a)$ roots of unity. But $p\geqslant 3$ and $N(a)\geqslant 1$, so the only way to escape a contradiction to the hypothesis $n\leqslant N(\beta)+1$ is to have $p=3$ and $n=N(\beta)+1$.

This proves (i) and (ii) and it remains to establish (iii). Suppose β is non-zero and $n\geqslant N(\beta)+2$. Let

$$\beta=\sum_{j=1}^{N(\beta)}\sigma_j \tag{3.7}$$

be a representation of β as a sum of $N(\beta)$ roots of unity. By the first part of the proof, each σ_j is in $Q(P)$. Let ω be a primitive cube root of unity. Since $1+\omega+\omega^2=0$ and $1+(-1)=0$, there is a relation

$$\sum_{j=1}^{n-N(\beta)-1}\nu_j=1\quad\text{with }\nu_j=1,\,-1,\,-\omega,\text{ or }-\omega^2.$$

Now, if ϱ is any root of unity, the expression

$$\beta=\sum_{j=1}^{n-N(\beta)-1}\nu_j\sigma_1+\sum_{j=2}^{N(\beta)}\sigma_j+\varrho-\varrho$$

is a representation of β as a sum of n roots of unity and this gives (iii). A similar argument applies if $\beta=0$.

Note that all the possibilities allowed in the theorem can occur. Suppose, for example, that β is a non-zero cyclotomic integer and $3\nmid P(\beta)$. Let ω be a primitive cube root of unity and let (3.7) again be a representation of β as a sum of $N(\beta)$ roots of unity. Then the expression

$$\beta=-\omega\sigma_1-\omega^2\sigma_1+\sum_{j=2}^{N(\beta)}\sigma_j$$

is a representation of β as a sum of $N(\beta)+1$ roots of unity and the smallest cyclotomic field containing all the terms on the right-hand side is $Q(3P(\beta))$.

The following result, which is also a corollary of Theorem 1, will be useful later.

THEOREM 2. *Let β be an integer in the cyclotomic field $Q(P)$ and let p be a prime divisor of P. Let*

$$\beta=\sum_j a_j\xi^j \tag{3.8}$$

be a representation for β of the shape (2.1) if $p\|P$, or (2.3) if $p^2|P$. In the former case, suppose in addition that at most $\frac{1}{2}(p-1)$ of the a_j are non-zero. Then

$$N(\beta)=\sum_j N(a_j).$$

Proof. Clearly, $N(\beta)\leqslant\sum N(a_j)$. Suppose, if possible, that

$$N(\beta)<\sum_j N(a_j). \tag{3.9}$$

From Theorem 1 and (2.5), there is a representation

$$\beta=\sum_j a_j^*\xi^j \tag{3.10}$$

of the form (2.1) if $p\|P$, or (2.3) if $p^2|P$, such that

$$N(\beta) = \sum_j N(a_j^*). \tag{3.11}$$

We now subdivide the argument into two cases.

First case. Suppose $p^2|P$. From Lemma 2, the two representations (3.8) and (3.10) for β are the same, in contradiction to (3.9) and (3.11).

Second case. Suppose $p\|P$ and set $P = pP_1$. On applying Lemma 1 to the representations (3.8) and (3.10), we have $a_j^* = a_j + a$ for some a in $Q(P_1)$. If $a = 0$, we have a contradiction as in the first case. Otherwise

$$\beta = \sum_{a_j\neq 0} a_j^* \xi^j + \sum_{a_j=0} a_j^* \xi^j = \sum_{a_j\neq 0} a_j^* \xi^j - \sum_{a_j\neq 0} a\xi^j,$$

so, if X denotes the number of non-zero a_j,

$$\sum_{a_j\neq 0} N(a_j^*) + (p-X)N(a) = \sum_{j=0}^{p-1} N(a_j^*) = N(\beta) \leqslant \sum_{a_j\neq 0} N(a_j^*) + XN(a),$$

a contradiction, since $X \leqslant \frac{1}{2}(p-1)$ and $N(a) \neq 0$.

This proves the theorem.

4. Cyclotomic integers of given degree. Let β be a cyclotomic integer of degree d which can be expressed as a sum of n roots of unity. To complete the story begun in § 3, we now find an estimate for $P(\beta)$ in terms of n and d.

THEOREM 3. *Suppose β is a non-zero cyclotomic integer of degree d and let $N(\beta) = n$. Then*

$$P(\beta) < 10^n d\log\log 20d.$$

COROLLARY. *A cyclotomic integer of degree d is a sum of n roots of unity only if it is a sum of n roots of unity of common degree less than*

$$10^{n+1} d\log\log 20d.$$

The corollary follows at once from Theorems 1 and 3. To prove Theorem 3 itself, we need two lemmas.

LEMMA 4. *Let P_0 be a positive integer and β a non-zero cyclotomic integer and set $N(\beta) = n$. Let $Q(P)$ be the smallest cyclotomic field containing both $Q(P_0)$ and β, and let d be the degree of β over $Q(P_0)$. Then*

$$\varphi(P) \leqslant dc_1^{n-1}\varphi(P_0), \tag{4.1}$$

where φ is Euler's function and $c_1 = e^{2.03248} = 7.63299\ldots$

Proof. The lemma is clearly true if $P = 1$, since then $P_0 = 1$ and β is a rational integer. The proof proceeds by induction on P.

Let P_0 be a positive integer and β a non-zero cyclotomic integer with degree d over $Q(P_0)$ and set $N(\beta) = n$. Let $Q(P)$ be the smallest cyclotomic field containing both $Q(P_0)$ and β. We note first that it suffices to consider the case $P_0 = 1$. For, if $Q(P^*)$ is the smallest cyclotomic field containing β, then

$$[Q(P):Q(P_0)(\beta)] \leqslant [Q(P^*):Q(\beta)]$$

since both the field extensions here may be obtained by the adjunction of a generating root of unity for $Q(P^*)$. Let d^* denote the degree of β over Q and suppose the lemma is known for β when $P_0 = 1$. Then

$$\varphi(P)/d\varphi(P_0) = [Q(P):Q(P_0)(\beta)] \leqslant [Q(P^*):Q(\beta)] = \varphi(P^*)/d^* \leqslant c_1^{n-1},$$

so that the lemma is true for β and all integers P_0.

We shall therefore now assume that β is a non-zero cyclotomic integer of degree d and set $N(\beta) = n$ and $P(\beta) = P$. We divide the subsequent argument into three cases.

First case. Suppose there is a prime p such that $p\|P$ and $p > 2n$. Set $P = pP_1$ and let ξ be a primitive p-th root of unity. By Theorem 1 and (2.5), we can write

$$\beta = \sum_{j=0}^{p-1} a_j \xi^j, \tag{4.2}$$

where the a_j are integers in $Q(P_1)$ and at most n of them are non-zero. Moreover, the representation (4.2) is unique, for by Lemma 1, any other such representation has the shape

$$\beta = \sum_{j=0}^{p-1} (a_j + a)\xi^j$$

for some non-zero a in $Q(P_1)$ and so has at least $p-n$ ($> n$) non-zero terms. Group the non-zero a_j ($1 \leqslant j \leqslant p-1$) in (4.2) into sets of mutually conjugate ones and choose one number from each of these sets, say $\gamma_1, \gamma_2, \ldots, \gamma_k$. Let m_i be the number of a_j ($1 \leqslant j \leqslant p-1$) conjugate to γ_i and set $m = \min\{m_1, \ldots, m_k\}$ and $\gamma_0 = a_0$.

Let d' denote the degree of β over $Q(P_1)$. The conjugates of β over $Q(P_1)$ are the

$$\beta_i = \sum_{j=0}^{p-1} a_j \xi^{ij} \quad (1 \leqslant i \leqslant p-1).$$

There are d' distinct numbers among them and each occurs just $(p-1)/d'$ times. But, from the uniqueness of the representation (4.2), we have $\beta_i = \beta$ say, if and only if $a_{ij} = a_j$ ($1 \leqslant j \leqslant p-1$), where the subscripts are interpreted mod p. Hence

$$p-1 \leqslant md'. \tag{4.3}$$

Next, the Galois group of $Q(P)/Q$ is isomorphic in the obvious way to the direct product of the Galois groups of $Q(P)/Q(P_1)$ and $Q(P_1)/Q$. So the conjugates of β over Q are the numbers $\sigma\tau(\beta)$ where σ is an automorphism of $Q(P)/Q(P_1)$ and τ is an automorphism of $Q(\gamma_0, \ldots, \gamma_k)/Q$ extended to $Q(\gamma_0, \ldots, \gamma_k, \xi)$ by the definition $\tau(\xi) = \xi$. This prescription gives each of the d distinct conjugates of β the same number of times, say X times. Hence

$$(p-1)[Q(\gamma_0, \ldots, \gamma_k):Q] = dX. \tag{4.4}$$

We need an estimate for X. So suppose, in the above notation, that

$$\sigma\tau(\beta) = \beta. \tag{4.5}$$

If τ is assigned, there are either $(p-1)/d'$ choices of σ for which (4.5) holds, or no such choices. Also, by Lemma 1, the equation (4.5) means that

$$\sum_{j=0}^{p-1} \tau(a_j)\xi^{lj} = \sum_{j=0}^{p-1} a_j \xi^j$$

for some integer l with $1 \leqslant l \leqslant p-1$. So by the uniqueness of the representation (4.2), we see that $\tau(\gamma_0) = \gamma_0$ and that there are at most m_i choices for the number $\tau(\gamma_i)$ for $1 \leqslant i \leqslant k$. Hence

$$X \leqslant m_1 \ldots m_k(p-1)/d'. \tag{4.6}$$

It follows from (4.3), (4.4) and (4.6) that

$$(p-1)[Q(\gamma_0, \ldots, \gamma_k):Q] \leqslant dmm_1 \ldots m_k. \tag{4.7}$$

Now, by Theorem 2,

$$n = \sum_{j=0}^{p-1} N(a_j) = N(\gamma_0) + \sum_{i=1}^{k} m_i N(\gamma_i). \tag{4.8}$$

Let $Q(N_i)$ denote the smallest cyclotomic field containing $\gamma_0, \gamma_1, \ldots, \gamma_i$ $(0 \leqslant i \leqslant k)$. Each $Q(N_i)$ is a subfield of $Q(P_1)$ and, since $P_1 < P$, we can apply the induction hypothesis to $\gamma_0, \gamma_1, \ldots, \gamma_k$ in turn, giving

$$\varphi(N_0) \leqslant [Q(\gamma_0):Q]c_1^{N(\gamma_0)-1} \tag{4.9}$$

and, for $1 \leqslant i \leqslant k$,

$$\begin{aligned} \varphi(N_i) &\leqslant [Q(N_{i-1})(\gamma_i):Q(N_{i-1})]c_1^{N(\gamma_i)-1}\varphi(N_{i-1}) \\ &\leqslant [Q(\gamma_0, \ldots, \gamma_i):Q(\gamma_0, \ldots, \gamma_{i-1})]c_1^{N(\gamma_i)-1}\varphi(N_{i-1}). \end{aligned} \tag{4.10}$$

On putting these inequalities together, we get

$$\begin{aligned} \varphi(P) &= (p-1)\varphi(P_1) = (p-1)\varphi(N_k) \\ &\leqslant (p-1)[Q(\gamma_0, \ldots, \gamma_k):Q]c_1^{N(\gamma_0)+\ldots+N(\gamma_k)-1} \\ &\leqslant dmm_1 \ldots m_k c_1^{N(\gamma_0)+\ldots+N(\gamma_k)-1}, \text{ by (4.7)}, \\ &\leqslant dc_1^{n-1}, \end{aligned}$$

by (4.8) and rather crude estimation which requires $c_1 \geqslant 4$.

Second case. Suppose there is a prime p such that $p^N \| P$ with $N > 1$. Set $P = pP_1$ and let ξ be a primitive p^N-th root of unity. By Lemma 2, we can write β uniquely in the form (4.2), where the a_j are integers in $Q(P_1)$. We shall temporarily call two cyclotomic integers, α and α^*, p-equivalent if $\alpha^* = \varrho\alpha'$ for some conjugate α' of α and some p^{N-1}-th root ϱ of unity. Now group the non-zero a_j $(1 \leqslant j \leqslant p-1)$ into sets of mutually p-equivalent ones and choose one number from each of these sets, say $\gamma_1, \ldots, \gamma_k$, such that the smallest cyclotomic field containing γ_i contains all the a_j $(1 \leqslant j \leqslant p-1)$ which are p-equivalent to γ_i $(1 \leqslant i \leqslant k)$. Also, let m_i be the number of a_j $(1 \leqslant j \leqslant p-1)$ which are p-equivalent to γ_i and set $m = \min\{m_1, \ldots, m_k\}$ and $\gamma_0 = a_0$.

By the minimality of P, we have $Q(P_1)(\beta) = Q(P)$, whence the degree of β over $Q(P_1)$ is p. As in the first case, the conjugates of β over Q are the $\sigma\tau(\beta)$ where σ is an automorphism of $Q(P)/Q(P_1)$ and τ is an automorphism of $Q(a_0, \ldots, a_{p-1})/Q$ extended to $Q(a_0, \ldots, a_{p-1}, \xi)$ by $\tau(\xi) = \xi^l$, with $1 \leqslant l < p^{N-1}$. We get each of the d distinct conjugates of β the same number of times, say X times. Hence

$$p[Q(a_0, \ldots, a_{p-1}):Q] = dX. \tag{4.11}$$

To estimate X, consider again the equation (4.5): $\sigma\tau(\beta) = \beta$. If τ is assigned, this determines σ uniquely because the degree of β over $Q(P_1)$ is p. By Lemma 2, the equation (4.5) means that

$$\sum_{j=0}^{p-1} \tau(a_j)\varrho^{lj}\xi^{lj} = \sum_{j=0}^{p-1} a_j \xi^j$$

for some p-th root ϱ of unity which is determined by σ and some integer l with $1 \leqslant l < p^{N-1}$. By the uniqueness of the representation (4.2), there are at most m choices for l and at most m_i choices for the number $\tau(\gamma_i)$ for $1 \leqslant i \leqslant k$ and $\tau(\gamma_0) = \gamma_0$. Hence

$$X \leqslant mm_1 \ldots m_k[Q(a_0, \ldots, a_{p-1}):Q(\gamma_0, \ldots, \gamma_k)].$$

Combining this with (4.11), we get

$$p[Q(\gamma_0, \ldots, \gamma_k):Q] \leqslant dmm_1 \ldots m_k. \tag{4.12}$$

We again have the equations (4.8), (4.9) and (4.10) so

$$\begin{aligned}\varphi(P) &= p\varphi(P_1) \leqslant p[Q(\gamma_0, \dots, \gamma_k):Q]c_1^{N(\gamma_0)+\dots+N(\gamma_k)-1}\\ &\leqslant dmm_1 \dots m_k c_1^{N(\gamma_0)+\dots+N(\gamma_k)-1}, \text{ by (4.12)},\\ &\leqslant dc_1^{n-1},\end{aligned}$$

by (4.8), giving (4.1) in this case.

Third case. Suppose neither of the two preceding cases arises. Then P divides the product of the primes less than $2n$, so by [5], Theorem 9,

$$\varphi(P) \leqslant \prod_{p\leqslant 2n-1}(p-1) \leqslant \tfrac{1}{3}\prod_{p\leqslant 2n-1} p < \tfrac{1}{3}e^{1.01624(2n-1)} < c_1^{n-1}.$$

Hence the inequality (4.1) holds for β in all cases and the lemma follows by induction.

Lemma 5. *For* $n \geqslant 3$,

$$\frac{n}{\varphi(n)} \leqslant e^{\gamma}\log\log\varphi(n) + c_2,$$

where $\gamma = 0.57721\dots$ *is Euler's constant and* $c_2 = 3 - e^{\gamma}\log\log 2 = 3.65278\dots$

Proof. Suppose first that $n \geqslant 30$. From [5], Theorem 15,

$$\frac{n}{\varphi(n)} < e^{\gamma}\log\log n + \frac{2.50637}{\log\log n}. \tag{4.13}$$

So, if we write

$$\log\varphi(n) = \log n\{1-\lambda(n)\},$$

then we have

$$\lambda(n) < \frac{1}{\log n}\left\{\log\log\log n + \gamma + \frac{2.50637}{e^{\gamma}(\log\log n)^2}\right\} < 0.51$$

and consequently

$$\log\log\varphi(n) = \log\log n + \log\{1-\lambda(n)\} > \log\log n - 0.72.$$

So from (4.13),

$$\frac{n}{\varphi(n)} < e^{\gamma}\{\log\log\varphi(n) + 0.72\} + \frac{2.50637}{\log\log 30} < e^{\gamma}\log\log\varphi(n) + 3.4.$$

To complete the proof, we now compute

$$\frac{n}{\varphi(n)} - e^{\gamma}\log\log\varphi(n)$$

for $3 \leqslant n \leqslant 30$; its maximum on this range turns out to be c_2 when $n = 6$.

Proof of Theorem 3. Let β be a non-zero cyclotomic integer with degree d and set $P = P(\beta)$ and $n = N(\beta)$. If $P \leqslant 2$, the conclusion of Theorem 3 is immediate, so we may suppose $P \geqslant 3$. From Lemma 4, we have $\varphi(P) \leqslant dc_1^{n-1}$, whence

$$\begin{aligned}e^{\gamma}\log\log\varphi(P) + c_2 &\leqslant e^{\gamma}(\log\log 20d + \log n + \log\log c_1) + c_2\\ &< e^{\gamma}(\log\log 20d + \log n + 3)\\ &< c_1(1+\tfrac{1}{4}\log n)\log\log 20d\\ &< c_1(1.2)^n\log\log 20d.\end{aligned}$$

The desired result now follows from Lemma 5.

We conclude this section with some further remarks about Theorem 3. The following two examples show that the dependence on d of the bound in Theorem 3 is best possible and, for this dependence on d, the bound also has the right order of magnitude with respect to n.

Example 1. Let P be the product of the odd primes not exceeding some number X, let ξ be a primitive P-th root of unity and let n be a positive integer. Let $\beta = n\xi$. Then $P(\beta) = P$, $N(\beta) = n$ and the degree of β is d (say) $= \varphi(P)$. So, as $X \to \infty$,

$$P(\beta) = d\prod_{3\leqslant p\leqslant X}\left(1-\frac{1}{p}\right)^{-1} \sim \tfrac{1}{2}e^{\gamma}d\log\log d.$$

Example 2. Let

$$\beta = \sum_{5\leqslant p\leqslant X}(\xi_p + \xi_p^{-1})$$

where ξ_p is a primitive p-th root of unity and p runs through the primes with $5 \leqslant p \leqslant X$. Let the degree of β be d. Then

$$P(\beta) = \prod_{5\leqslant p\leqslant X} p, \quad d = \prod_{5\leqslant p\leqslant X}\tfrac{1}{2}(p-1), \quad N(\beta) = \sum_{5\leqslant p\leqslant X} 2$$

and, as $X \to \infty$,

$$P(\beta) = d\prod_{5\leqslant p\leqslant X} 2\left(1-\frac{1}{p}\right)^{-1} \sim \tfrac{1}{3}e^{\gamma}2^{\frac{1}{2}N(\beta)}d\log\log d.$$

There is another result of the same sort as Theorem 3 giving an estimate for the smallest cyclotomic field containing all sums of n roots of unity of degree d.

Theorem 4. *Let β be a cyclotomic integer of degree d with $N(\beta) = n$ and let Δ be the discriminant of $Q(\beta)$ over Q. Define numbers a_p, where p runs through the primes, as follows:*

(i) *if $p \mid \Delta$, $p \nmid d$ and $3 \leqslant p \leqslant 2n$, then $a_p = 1$;*

(ii) *if $p \mid \Delta$, $p \nmid d$, $p \equiv 1 \pmod{d'}$ and $2n < p \leqslant nd'+1$ for some divisor d' of d, then $a_p = 1$;*

(iii) *if* $p \mid \Delta$ *and* $p^a \| d$ *with* $a \geqslant 1$, *then* $a_p = a+1$; *and*

(iv) *in all other cases,* $a_p = 0$.

Also define

$$\eta = \begin{cases} 2 & \text{if } d \text{ and } \Delta \text{ are both even,} \\ 1 & \text{otherwise.} \end{cases}$$

Finally, set $P^* = \eta \prod p^{a_p}$. *Then* β *is in* $Q(P^*)$.

We shall need the following quantitative form of Kronecker's theorem on abelian extensions of the rationals. I have been unable to find the exact statement in the literature, but it is easily deduced from the proofs of Kronecker's theorem given, for example, in [8] or more recently [7].

LEMMA 6. *Let* K *be an abelian extension of* Q *with degree* d *and discriminant* Δ *and define*

$$\eta = \begin{cases} 2 & \text{if } d \text{ and } \Delta \text{ are both even,} \\ 1 & \text{otherwise} \end{cases}$$

and

$$P' = \eta \prod p^{a+1},$$

where the product is taken over all primes p *such that* $p \mid \Delta$ *and* $p^a \| d$. *Then* K *is a subfield of* $Q(P')$.

Proof. By Kronecker's theorem ([8], p. 244), K is a subfield of a cyclotomic field. We let $Q(P)$ be the smallest such field. Suppose, in the first instance, that K is cyclic and that its degree is a prime power, say $d = p^a$. If $p = 2$, then by a remark in [8] (p. 255, end of § 3), we see that P divides $4d = p^{a+2}$. If $p > 2$, then again from [8] (p. 263, end of § 5), P divides $pd = p^{a+1}$. In either case, P is a power of p and so also is Δ, since it divides the discriminant of $Q(P)$. This proves the lemma in this special case. The general case follows since any abelian field can be expressed as the compositum of cyclic fields whose degrees are prime powers.

Proof of Theorem 4. We use the notation of the enunciation and set $P = P(\beta)$. By Lemma 6, P divides $\eta \prod p^{a+1}$, where the product is taken over all the primes p such that $p \mid \Delta$ and $p^a \| d$. It therefore only remains to prove that if p is a simple prime factor of P, $p \nmid d$ and $p > 2n$, then p satisfies the conditions in (ii) of the enunciation.

So let p be a prime such that $p \| P$ and $p > 2n$. Write $P = pP_1$ and let d' be the degree of β over $Q(P_1)$. Then d' divides $[Q(P):Q(P_1)] = p-1$, that is $p \equiv 1 \pmod{d'}$. Moreover, we now have exactly the situation of the first case of the proof of Lemma 4, so by (4.3), $p \leqslant nd'+1$. Finally, the conjugates of β over Q split into sets of conjugates over $Q(P_1)$ each having d' members, so d' divides d. This completes the proof of the theorem.

5. Cyclotomic integers of given maximum modulus. In this section, we turn to the second of Robinson's problems and describe a method for finding all the cyclotomic integers with a given maximum modulus.

THEOREM 5. *Let* $\varkappa$ *be an algebraic number and let* β *be a cyclotomic integer with* $\overline{|\beta|} = \varkappa$. *Then* β *is equivalent to an element of a certain finite set (depending on* $\varkappa$*) and this set can be effectively determined.*

It is most convenient to begin the proof of the theorem by proving the special case contained in the following lemma. The theorem is then a relatively easy deduction.

LEMMA 7. *Let* R *be a positive integer and* β *a cyclotomic integer with* $|\beta|^2 = R$. *Then* β *is equivalent to an element of a certain finite set (depending on* R*) and this set can be effectively determined.*

Proof. By Lemma 3, we have $|\beta'|^2 = R$ for each conjugate β' of β. The hypotheses of the lemma are therefore unaffected if we replace β by any number equivalent to it. In particular, we may assume that β is a minimal cyclotomic integer. Set $P = P(\beta)$ and $n = N(\beta)$ and let p be a prime divisor of P with $p^N \| P$.

Pick $k > \log 2$. By Theorem 1 of [2], there is an effectively determined constant c_3, depending only on k, such that

$$R = \overline{|\beta|}^2 \geqslant c_3 n \exp(-k \log n / \log\log n).$$

Thus n is bounded above by a number depending only on R and to prove the lemma, it suffices to show that P has the same property. This, in its turn, will follow once we show that

$$p \leqslant 4^n, \quad p^{N-1} \leqslant 4^n, \tag{5.1}$$

for any choice of the prime divisor p of P. There are two cases to consider.

First case. Suppose that $N = 1$ and $p > 4^n$. Write $P = pP_1$ and let ξ be a primitive p-th root of unity. As in the first case of the proof of Lemma 4, there is a unique representation

$$\beta = \sum_{j=1}^{X} \gamma_j \xi^{r_j}, \tag{5.2}$$

where the γ_j are non-zero integers in $Q(P_1)$, $X \leqslant n$ $(< \frac{1}{2}p)$ and the r_j are integers incongruent mod p. By Dirichlet's theorem (see, for example, [1], Theorem VI, p. 13), there is an integer u such that

$$\|ur_j/p\| \leqslant p^{-1/X} \quad (1 \leqslant j \leqslant X) \quad \text{and} \quad 1 \leqslant u < p$$

where, as usual, $\|\theta\|$ denotes the distance from θ to the nearest integer. Also, by hypothesis, $p^{-1/X} \leqslant p^{-1/n} < \frac{1}{4}$. So, after replacing β by one of its conjugates over $Q(P_1)$ and multiplying by a suitable p-th root of unity, we may suppose that $r_1 = 0$ and $0 < r_j < \frac{1}{2}p$ $(2 \leqslant j \leqslant X)$. It is now more convenient to rewrite (5.2) as

$$\beta = \sum_{j=0}^{p-1} a_j \xi^j,$$

each a_j being 0 or one of the γ_i. Let l be the largest integer for which $a_l \neq 0$. From our construction and the minimality of β, it follows that $a_0 \neq 0$ and that $1 \leqslant l < \frac{1}{2}p$. Now

$$R = |\beta|^2 = \sum_{k=0}^{p-1} \theta_k \xi^k \tag{5.3}$$

where

$$\theta_k = \sum_{i-j\equiv k (\mathrm{mod}\, p)} a_i \overline{a_j}.$$

The number of non-zero θ_k is at most $n^2 < p-1$, by hypothesis, so on applying Lemma 1 to the relation (5.3), we get

$$\theta_1 = \ldots = \theta_{p-1} = 0.$$

On the other hand, we have $a_j = 0$ for $l+1 \leqslant j \leqslant p-1$ and $a_0, a_l \neq 0$, whence

$$\theta_l = a_l \overline{a_0} \neq 0,$$

a contradiction. Hence $p \leqslant 4^n$.

Second case. Suppose that $N > 1$ and $p^{N-1} > 4^n$. Set $L = N-1$ and $P = p^L P_1$ and let ξ be a primitive p^N-th root of unity. By Lemma 2 and Theorem 2, there is a unique representation of the form (5.2) for β, where the γ_j are non-zero integers in $Q(P_1)$, $X \leqslant n$ and the r_j are integers incongruent mod p^L. By Dirichlet's theorem again, there is an integer u with

$$\|ur_j/p^L\| \leqslant p^{-L/X} \quad (1 \leqslant j \leqslant X) \quad \text{and} \quad 1 \leqslant u < p^L.$$

Write $u = p^r v$, with v an integer prime to p, and put $M = L - r$. Then

$$\|vr_j/p^M\| \leqslant p^{-L/X} \quad (1 \leqslant j \leqslant X).$$

After applying the automorphism $\xi \to \xi^v$ of $Q(P)$ over Q and replacing β by one of its conjugates, we may suppose that in the representation (5.2),

$$\|r_j/p^M\| \leqslant p^{-L/X} \quad (1 \leqslant j \leqslant X). \tag{5.4}$$

Now rewrite (5.2) in the shape

$$\beta = \sum_{j=0}^{p^M-1} a_j \xi^j \tag{5.5}$$

where

$$a_j = \sum_{r_i \equiv j (\mathrm{mod}\, p^M)} \gamma_i \xi^{r_i - j}$$

and set $P = p^M P_3$. Then each a_j is in $Q(P_3)$ and $a_j = 0$ unless the inequality in (5.4) holds with r_j replaced by j on the left-hand side. By hypothesis, $p^{-L/X} \leqslant p^{-L/n} < \frac{1}{4}$, so after multiplying β by an appropriate p^N-th root of unity as in the first case, we may assume that $a_0 \neq 0$ and that the a_j with $j \geqslant \frac{1}{2}p^M$ are all 0. Let l be the largest integer for which $a_l \neq 0$, so that, from the minimality of β, $1 \leqslant l < \frac{1}{2}p^M$. Now

$$R = |\beta|^2 = \sum_{k=0}^{p^M-1} \theta_k \xi^k \tag{5.6}$$

where

$$\theta_k = \sum_{i-j\equiv k (\mathrm{mod}\, p^M)} a_i \overline{a_j} \xi^{i-j-k}.$$

Each θ_k is in $Q(P_3)$, so by Lemma 2 applied to (5.6),

$$\theta_k = 0 \quad (1 \leqslant k \leqslant p^M - 1).$$

However, as before, $\theta_l = a_l \overline{a_0} \neq 0$, a contradiction. Hence $p^{N-1} \leqslant 4^n$.

This proves (5.1) and, by the remarks made at the beginning, establishes the lemma.

Proof of Theorem 5. Let β be a cyclotomic integer with $\overline{|\beta|} = \varkappa$. We may suppose that $|\beta|^2 = \varkappa^2$. Let the degree of $\varkappa^2$ over Q be d. By Lemma 3, the conjugates β' of β lie on d circles about the origin, with the same number on each circle. Pick one conjugate from each circle, say $\beta_1 = \beta, \beta_2, \ldots, \beta_d$ and let θ be their product. Then

$$|\theta|^2 = |\beta_1 \ldots \beta_d|^2 = \mathrm{Norm}(\varkappa^2),$$

a rational integer. So by Lemma 7, θ is equivalent to an element of a certain finite set (depending on $\varkappa$). The same is true for $\theta^* = \beta_1 \overline{\beta_2 \ldots \beta_d}$ and hence for

$$\theta\theta^* = \beta^2 |\beta_2 \ldots \beta_d|^2 = \beta^2 \mathrm{Norm}(\varkappa^2)/\varkappa^2.$$

Hence β^2 is equivalent to an element of a certain finite set and, finally, the same holds for β. This proves the theorem.

It is not hard to give an explicit bound for the finite exceptional set of Theorem 5. Thus, let β be a cyclotomic integer with $\overline{|\beta|} = \varkappa$. By following and simplifying the work of [2], it can be shown that

$$N(\beta) < 10^6 \overline{|\beta|}^2 = 10^6 \varkappa^2.$$

Also, if we use this inequality to make the above proof explicit, we find that $P(\beta^2)$ divides the least common multiple of $P(\varkappa^2)$ and

$$\prod_{p\leqslant\mu} p\cdot\prod_{p^L\leqslant\mu} p^L,$$

where

$$\mu = 4^{10^6\,\mathrm{Norm}(\varkappa^2)}.$$

References

[1] J. W. S. Cassels, *An introduction to Diophantine approximation*, Cambridge Tracts in Mathematics and Mathematical Physics, no. 45, Cambridge 1965.

[2] J. H. Loxton, *On the maximum modulus of cyclotomic integers*, Acta Arith. 22 (1972), pp. 69–85.

[3] H. B. Mann, *On linear relations between roots of unity*, Mathematika 12 (1965), pp. 107–117.

[4] R. M. Robinson, *Some conjectures about cyclotomic integers*, Math. Comp. 19 (1965), pp. 210–217.

[5] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), pp. 64–94.

[6] A. Schinzel, *On sums of roots of unity*, Acta Arith. 11 (1966), pp. 419–432.

[7] И. Р. Шафаревич, *Новое доказательство теоремы Кронекера-Вебера*, Труды Мат. Инст. Стеклова 38 (1951), pp. 382–387.

[8] H. Weber, *Theorie der Abel'schen Zahlkörper. III. Der Kronecker'sche Satz*, Acta Math. 8 (1886), pp. 244–263.

Received on 20. 7. 1973 (438)

ACTA ARITHMETICA
XXVI (1974)

Some distribution problems concerning the divisors of integers

by

P. Erdös (Budapest) and R. R. Hall (Heslington)

Introduction. In this paper we study the distribution (mod1) of $\log d$, where d runs through the divisors of the positive integer n. As usual we denote the number of these divisors by $\tau(n)$.

The sequence $\{\log m,\ m = 1, 2, 3, \ldots\}$ is not uniformly distributed (mod 1), nevertheless if we set

$$f_n(x) = \frac{1}{\tau(n)} \sum_{\log d\leqslant x\ (\mathrm{mod}\ 1)} 1,$$

then on a sequence of integers n of asymptotic density 1, we have that

$$f_n(x)\to x$$

uniformly for

$$0\leqslant x\leqslant 1.$$

Indeed, for each $\lambda<\frac{1}{2}$, there is a sequence of density 1 on which

$$\sup_{0\leqslant\alpha\leqslant\beta\leqslant 1} |f_n(\beta)-f_n(\alpha)-(\beta-\alpha)| \leqslant \frac{1}{(\tau(n))^\lambda}.$$

This result was proved in a recent paper of Hall [2].

It follows from this that for each fixed $\alpha\in[0,1)$, there is a sequence of integers n of density 1 on which

$$\min_{d|n} \|\log d-\alpha\| \to 0,$$

where $\|x\|$ denotes the difference between x and the nearest integer to it, and we consider the following problem. How fast can the left hand side tend to zero on a sequence of density 1, or even on a sequence of positive density? It turns out that this question can be answered very precisely.