ACTA ARITHMETICA
XXII (1972)

On the maximum modulus of cyclotomic integers

by

J. H. Loxton (Cambridge)

1. Introduction. Let β be a cyclotomic integer, i.e. an algebraic integer in a cyclotomic field. Then β can be represented as the sum of roots of unity. We denote by $N(\beta)$ the least number of roots of unity in any such sum representing β. Also, as usual, $\overline{|\beta|}$ denotes the maximum of the absolute values $|\beta'|$ of the conjugates β' of β. Following Robinson [4], we shall say that two cyclotomic integers β and β^* are equivalent if $\beta^* = \varrho\beta'$ for some conjugate β' of β and some root of unity ϱ. Clearly $\overline{|\beta^*|} = \overline{|\beta|}$ for equivalent β, β^*. The object of this paper is the following

Theorem 1. *Suppose that $k > \log 2$. Then there is a positive number c depending only on k such that*

$$\overline{|\beta|}^2 \geqslant cn\exp(-k\log n/\log\log n) \tag{1.1}$$

for all cyclotomic integers β with $N(\beta) = n$ [1].

The statement of Theorem 1 fails when $k = \log 2$. In fact, we shall prove

Theorem 2. *Suppose that $c > 0$. Then there are infinitely many positive integers n with the following property: There are infinitely many inequivalent cyclotomic integers β with $N(\beta) = n$ and*

$$\overline{|\beta|}^2 < cn\exp(-\log 2\cdot\log n/\log\log n).$$

These theorems give an answer to a conjecture of R. M. Robinson [3], namely, if β is a cyclotomic integer and $\overline{|\beta|} \leqslant n$, then β can be expressed as a sum of at most n roots of unity, except possibly for a finite number of inequivalent cases for each n. That this was rather too optimistic in general was shown by Schinzel [5]; he proves that there are infinitely many inequivalent cyclotomic integers β with $\overline{|\beta|} < 3$ which are not sums of 3 roots of unity. Theorem 1 can be reformulated to apply to this question as follows: If $k > \log 2$, there is a positive number c_0 depending only on k

[1] The function on the right-hand side of the inequality (1.1) is taken to be 0 for $n = 0$ and c for $n = 1$.

such that any cyclotomic integer β with $\overline{|\beta|}^2 \leqslant c_0 n\exp(-k\log n/\log\log n)$ can be expressed as a sum of at most $n-1$ roots of unity. Further, from Theorem 2, this is not true for $k = \log 2$, even if we allow finitely many inequivalent exceptions for each n and finitely many exceptional n. These statements follow from Theorems 1 and 2 at once because, as shown in § 3, the function $n\exp(-k\log n/\log\log n)$ increases with n for all sufficiently large n and tends to ∞ as $n \to \infty$.

The layout of the proof is as follows. Instead of dealing with the maximum $\overline{|\beta|}$ of the absolute values $|\beta'|$ of the conjugates β' of β, it is more convenient to use the mean of $|\beta'|^2$, an idea due to Cassels [1]. This is detailed in § 2. In § 3, we derive some estimates and inequalities for the function $n\exp(-k\log n/\log\log n)$ and also for a closely related function which proves easier to handle. § 4 and § 5 contain intermediate results towards the proof of Theorem 1, which follows in § 6. Finally, Theorem 2 is proved in § 7.

I would like to express my thanks to Professor J. W. S. Cassels, my supervisor, who suggested this problem to me and helped greatly with the presentation of the proof.

2. The function $\mathscr{M}$. For any algebraic number $\varkappa$, we shall denote by $\mathscr{M}(\varkappa)$ the mean of $|\varkappa'|^2$ taken over all the conjugates $\varkappa'$ of $\varkappa$. Trivially

(2.1) $$\overline{|\varkappa|}^2 \geqslant \mathscr{M}(\varkappa).$$

Also, if $\varkappa$ is a non-zero integer, its norm is at least 1 in absolute value, and so

(2.2) $$\mathscr{M}(\varkappa) \geqslant 1,$$

by the inequality of the arithmetic and geometric means applied to the $|\varkappa'|^2$.

We shall need some formulae for $\mathscr{M}(\beta)$ when β is a cyclotomic integer; the statements and their proofs are all from Cassels [1].

For any integer $P \geqslant 1$, we denote by $\boldsymbol{Q}(P)$ the field obtained by adjoining all the Pth roots of unity to the rational field $\boldsymbol{Q}$.

First case. Suppose that $P = pP_1$, where p is a prime and $p \nmid P_1$. Any $\beta \in \boldsymbol{Q}(P)$ may be written in the form

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

where ξ is a primitive pth root of unity and $a_j \in \boldsymbol{Q}(P_1)$ $(0 \leqslant j \leqslant p-1)$. When β is an integer, the a_j can be chosen to be integers. $\mathscr{M}(\beta)$ is given by

(2.4) $$2(p-1)\mathscr{M}(\beta) = \sum_{i,j=0}^{p-1} \mathscr{M}(a_i - a_j).$$

If precisely X of the a_j are non-zero, we may write (2.3) in the form

(2.5) $$\beta = \sum_{j=1}^{X} \gamma_j \xi^{r_j}$$

where $\gamma_j \in \boldsymbol{Q}(P_1)$, $\gamma_j \neq 0$ and the r_j are integers incongruent mod p. From (2.4),

(2.6) $$2(p-1)\mathscr{M}(\beta) = 2(p-X)\sum_{j=1}^{X} \mathscr{M}(\gamma_j) + \sum_{i,j=1}^{X} \mathscr{M}(\gamma_i - \gamma_j).$$

Second case. Suppose that $P = p^N P_2$, where p is a prime, $p \nmid P_2$ and $N \geqslant 2$. Put $P_1 = p^{N-1}P_2$. Every $\beta \in \boldsymbol{Q}(P)$ can be written uniquely in the form

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

where ξ is a primitive p^N-th root of unity and $a_j \in \boldsymbol{Q}(P_1)$ $(0 \leqslant j \leqslant p-1)$. The a_j are integers if β is. In this case

(2.8) $$\mathscr{M}(\beta) = \sum_{j=0}^{p-1} \mathscr{M}(a_j).$$

3. The functions f and g. Let $k > 0$. To prove Theorem 1, we have to investigate the function defined by

$$f(t) = f(t, k) = t\exp(-k\log t/\log\log t) \quad (t > 0;\ t \neq 1, e)$$

and

$$f(0) = 0, \quad f(1) = 1.$$

Since f behaves rather irregularly for small values of t, we shall prefer to consider the function

$$g(t) = t\exp(-k\log t'/\log\log t') \quad (t \geqslant 0)$$

where $t' = t + c_1$ and c_1 is a positive constant, possibly depending on k, which is to be chosen later. Now

$$g'(t) = \exp\left(-\frac{k\log t'}{\log\log t'}\right)\left\{1 - \frac{kt}{t'\log\log t'} + \frac{kt}{t'(\log\log t')^2}\right\}$$

and

$$g''(t) = -\frac{k}{t'\log\log t'}\exp\left(-\frac{k\log t'}{\log\log t'}\right)\left\{1 + O\left(\frac{1}{\log\log t'}\right)\right\},$$

the constant implied by the O-notation depending only on k. So we can choose $c_1 = c_1(k)$ such that

(3.1) $$g'(t) \geqslant 0 \quad \text{and} \quad g''(t) \leqslant 0 \quad \text{for all } t \geqslant 0,$$

and also

$$\log\log c_1 \geqslant 2. \tag{3.2}$$

This makes g increasing and concave on $[0, \infty)$, so by [2], § 94, we have at once

LEMMA 1. *If $a_1, a_2, \ldots, a_\nu$ are non-negative real numbers, then*

$$\frac{1}{\nu}\sum_{r=1}^{\nu} g(a_r) \leqslant g\left(\frac{1}{\nu}\sum_{r=1}^{\nu} a_r\right).$$

The next lemma is also a consequence of concavity; it must be notorious, but I cannot provide a precise reference.

LEMMA 2. *Let $0 \leqslant \lambda, \mu < \infty$ and $a > 0$ be given. For any numbers $a_1, a_2, \ldots, a_\nu$ satisfying*

$$\lambda \leqslant a_r \leqslant \mu \quad (1 \leqslant r \leqslant \nu) \quad \text{and} \quad \sum_{r=1}^{\nu} a_r \geqslant a,$$

we have

$$\sum_{r=1}^{\nu} g(a_r) \geqslant ug(\lambda) + (\nu - u - 1)g(\mu) + g(\sigma)$$

where

$$u = [(\mu\nu - a)/(\mu - \lambda)]$$

and

$$\sigma = a - u\lambda - (\nu - u - 1)\mu.$$

Proof. Suppose that some two of the a_r do not equal λ or μ, say $\lambda < a_1 \leqslant a_2 < \mu$. Put $\delta = \min\{a_1 - \lambda, \mu - a_2\}$ and $a_r^* = a_r$ $(r \neq 1, 2)$, $a_1^* = a_1 - \delta$ and $a_2^* = a_2 + \delta$. Using the mean value theorem and the concavity of g, we find that replacing $\{a_r\}$ by $\{a_r^*\}$ decreases $\sum g(a_r)$ and increases the number of a_r equal to λ or μ. So we may suppose that all but one a_r equals λ or μ, say

$$\lambda = a_1 = \ldots = a_v < a_{v+1} \leqslant a_{v+2} = \ldots = a_\nu = \mu.$$

Let $\sum a_r = a^*$ and define u and σ as in the statement of the lemma. By an easy calculation, we get

$$v = [(\mu\nu - a^*)/(\mu - \lambda)] \leqslant u$$

and

$$\lambda \leqslant \sigma \leqslant \mu.$$

Hence

$$\begin{aligned}\sum g(a_r) &= vg(\lambda) + g(a_{v+1}) + (\nu - v - 1)g(\mu)\\ &\geqslant ug(\lambda) + g(\sigma) + (\nu - u - 1)g(\mu).\end{aligned}$$

LEMMA 3. *If $t \geqslant c_1$, then*

$$0 < \log f(t) - \log g(t) < \frac{c_1 k}{t\log\log t}.$$

Proof. Write $\varphi(t) = \log t/\log\log t$ and let $t \geqslant c_1$. By the mean value theorem,

$$\begin{aligned}\log f(t) - \log g(t) &= k\{\varphi(t') - \varphi(t)\}\\ &= c_1 k\varphi'(s) \qquad (t < s < t')\\ &= \frac{c_1 k}{s\log\log s}\left(1 - \frac{1}{\log\log s}\right),\end{aligned}$$

and the lemma follows at once.

LEMMA 4. *$g(s) + g(t) \geqslant g(s+t)$ if $s, t \geqslant 0$; further*

$$g(s) + g(t) \geqslant g(s+t) + \frac{c_2 g(t)}{\log\log t'} \quad \text{if} \quad 1 \leqslant t \leqslant s,$$

where

$$c_2 = \frac{k}{2(1 + c_1)}.$$

Proof. By the mean value theorem,

$$\begin{aligned}g(s) + g(t) - g(s+t) &= g(t) - tg'(s + \theta t) \qquad (0 < \theta < 1)\\ &\geqslant g(t) - tg'(t), \quad \text{by (3.1)},\\ &= \frac{ktg(t)}{t'\log\log t'}\left(1 - \frac{1}{\log\log t'}\right),\end{aligned}$$

and the lemma follows using (3.2).

COROLLARY. *If $a_1, a_2, \ldots, a_\nu$ are non-negative numbers, then*

$$\sum_{r=1}^{\nu} g(a_r) \geqslant g\left(\sum_{r=1}^{\nu} a_r\right).$$

Proof. Use induction on ν, and the lemma.

LEMMA 5. *Let k and δ be given positive numbers, with $k > \log 2$. Let $0 \leqslant t \leqslant s$ and put $u = s + t$. Then there is a positive number $c_3 = c_3(k, \delta)$, depending only on k and δ, such that*

$$g\left(\frac{t}{(\log t)^\delta}\right) \leqslant \frac{c_2 g(t)}{2\log\log t'} \quad \text{whenever } t \geqslant c_3,$$

and

$$g(s) + g(t) \geqslant g(u) + 2g\left(\frac{u}{\log u}\right)$$

whenever

$$t \geqslant \max\{c_3, u(\log u)^{\delta-1}\}.$$

If, in addition, $\delta < 1-k^{-1}\log 2$, then there is a positive number $c_4 = c_4(k, \delta)$, depending only on k and δ, such that

$$tg\left(\frac{s}{t}\right) \geqslant 2g(s)$$

whenever

$$s \geqslant c_4 \quad \textit{and} \quad \tfrac{1}{4}(\log s)^{1-\delta} \leqslant t \leqslant s^{1/2}.$$

Proof. As before, write $\varphi(t) = \log t/\log\log t$. In the proof, the constants implied by the O-notation depend only on k and δ. We divide the proof into 5 steps. To begin with, we are given k and δ with $k > \log 2$ and $\delta > 0$.

(i) Suppose that $c_1 \leqslant t \leqslant s^{1/2}$. Then

$$\log\frac{s}{t} = \log s - \log t,$$

so

$$\log\log\frac{s}{t} = \log\log s + \log\left(1-\frac{\log t}{\log s}\right) = \log\log s + O\left(\frac{\log t}{\log s}\right), \quad \text{as } s \to \infty,$$

and so

$$\varphi\left(\frac{s}{t}\right) = \frac{\log s}{\log\log s}\left(1-\frac{\log t}{\log s}\right)\left\{1+O\left(\frac{\log t}{\log s\log\log s}\right)\right\}$$

whence

$$\varphi(s)-\varphi\left(\frac{s}{t}\right) = \frac{\log t}{\log\log s}\left\{1+O\left(\frac{1}{\log\log s}\right)\right\}, \quad \text{as } s \to \infty.$$

(ii) Putting $t = (\log s)^\delta$ in (i) gives

$$\varphi(s)-\varphi\left(\frac{s}{(\log s)^\delta}\right) = O(1), \quad \text{as } s \to \infty.$$

(iii) Let $s \geqslant c_1$. From Lemma 3 and (ii),

$$\begin{aligned}\log g(s)-\log g\left(\frac{s}{(\log s)^\delta}\right) &= \log f(s) - \log f\left(\frac{s}{(\log s)^\delta}\right) + O(1)\\ &= \delta\log\log s + O(1)\\ &\geqslant \log(2c_2^{-1}\log\log s') \quad \text{if } s \geqslant c_3, \text{ say,}\end{aligned}$$

where $c_3 = c_3(k, \delta) > c_1$. So

$$g\left(\frac{s}{(\log s)^\delta}\right) \leqslant \frac{c_2 g(s)}{2\log\log s'} \quad \text{whenever } s \geqslant c_3.$$

(iv) Suppose that $t \geqslant \max\{c_3, u(\log u)^{\delta-1}\}$. By Lemma 4 and (iii),

$$\begin{aligned}g(s)+g(t)-g(u) &\geqslant \frac{c_2 g(t)}{\log\log t'}\\ &\geqslant 2g\left(\frac{t}{(\log t)^\delta}\right)\\ &\geqslant 2g\left(\frac{u}{(\log u)^{1-\delta}}\,\frac{1}{(\log t)^\delta}\left(\frac{\log t}{\log u}\right)^\delta\right), \text{ by (3.1)},\\ &= 2g\left(\frac{u}{\log u}\right).\end{aligned}$$

(v) Now suppose that $0 < \delta < 1-k^{-1}\log 2$ and $\frac{1}{4}(\log s)^{1-\delta} \leqslant t \leqslant s^{1/2}$. By Lemma 3 and (i),

$$\begin{aligned}\log\left\{tg\left(\frac{s}{t}\right)g(s)^{-1}\right\} &= \log\left\{tf\left(\frac{s}{t}\right)f(s)^{-1}\right\} + O(s^{-1/2}), \text{ as } s \to \infty,\\ &= k\left\{\varphi(s)-\varphi\left(\frac{s}{t}\right)\right\} + O(s^{-1/2})\\ &= \frac{k\log t}{\log\log s}\left\{1+O\left(\frac{1}{\log\log s}\right)\right\}\\ &\geqslant k(1-\delta) + O\left(\frac{1}{\log\log s}\right)\\ &> \log 2,\end{aligned}$$

providing s is large enough, say $s \geqslant c_4 = c_4(k, \delta)$. So

$$tg\left(\frac{s}{t}\right) \geqslant 2g(s) \quad \text{whenever } s \geqslant c_4.$$

4. The basic inequality. Throughout this section, β denotes a cyclotomic integer in a fixed cyclotomic field $\boldsymbol{Q}(P)$. We consider only the first case of § 2, i.e. $P = pP_1$, where p is a prime and $p \nmid P_1$. As in § 2, ξ denotes a primitive pth root of unity. As a step towards the proof of Theorem 1, we have

THEOREM 3. *Let $k > \log 2$. There is a positive number $c_5 = c_5(k)$, depending only on k, with the following property. Suppose that, as in (2.3), $\beta = \sum a_j\xi^j$, where the $a_j \in \boldsymbol{Q}(P_1)$ are integers, that $\log N(\beta) \leqslant p-1$ and that $p \geqslant c_5$. Then*

$$\sum_{i,j=0}^{p-1} g[N(a_i-a_j)] \geqslant 2(p-1)g[N(\beta)]. \tag{4.1}$$

This result is useful in relating the functions $\mathscr{M}$ and g, as we shall eventually do, because (4.1) has the same shape as (2.4). Before proving Theorem 3, we need some lemmas. To shorten the notation, when dealing with the representations (2.3) and (2.5) for β, we shall write

$$N(\beta) = n,$$

$$N(a_j) = n_j, \quad N(a_i - a_j) = n_{ij} \quad (0 \leqslant i, j \leqslant p-1),$$

and

$$N(\gamma_i) = m_i, \quad N(\gamma_i - \gamma_j) = m_{ij} \quad (1 \leqslant i, j \leqslant X).$$

Lemma 6. *If* $\beta = \sum_{i=1}^{X} \gamma_i \xi^{r_i}$ *and* $X \leqslant \frac{1}{2}(p-1)$, *then* $n = \sum_{i=1}^{X} m_i$.

Proof. Clearly $n \leqslant \sum m_i$. Suppose that $n < \sum m_i$. Choose a representation $\beta = \sum a_j \xi^j$ of the form (2.3) with $\sum n_j = n$, and let $S = \{r_i\colon 1 \leqslant i \leqslant X\}$. Now

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

so there is an a such that

$$\text{(4.2)} \qquad a_j = \begin{cases} \gamma_i + a & \text{if} \quad j = r_i \in S, \\ a & \text{if} \quad j \notin S. \end{cases}$$

Now, $a \neq 0$ because $\sum n_j = n < \sum m_i$, and from (4.2)

$$\beta = \sum_{j \in S} a_j \xi^j + \sum_{j \notin S} a_j \xi^j = \sum_{j \in S} a_j \xi^j - \sum_{j \in S} a \xi^j.$$

So $\sum_{j \in S} n_j + XN(a) \geqslant n = \sum_{j=0}^{p-1} n_j = \sum_{j \in S} n_j + (p-X)N(a)$, by (4.2), and since $N(a) \neq 0$, this contradicts the data $X \leqslant \frac{1}{2}(p-1)$. So $n = \sum m_i$, as required.

Lemma 7. *Let* $k > \log 2$ *and* $\beta = \sum_{i=1}^{X} \gamma_i \xi^{r_i}$. *If*

$$\text{(4.3)} \qquad X \leqslant \tfrac{1}{2}(p-1)\min\{1, c_2/\log\log n'\}$$

then

$$\text{(4.4)} \qquad (p-X)\sum_{i=1}^{X} g(m_i) + \tfrac{1}{2}\sum_{i,j=1}^{X} g(m_{ij}) \geqslant (p-1)g(n).$$

Proof. Clearly (4.4) holds if $X = 1$; suppose it holds if $X = Y \geqslant 1$. Let $X = Y+1$ satisfy (4.3) and consider

$$\beta = \sum_{i=1}^{Y+1} \gamma_i \xi^{r_i} \quad \text{and} \quad \beta_1 = \sum_{i=1}^{Y} \gamma_i \xi^{r_i}.$$

Without loss of generality, we may suppose $m_1 \geqslant m_2 \geqslant \ldots \geqslant m_{Y+1}$. By Lemma 6, $N(\beta) = \sum_{i=1}^{Y+1} m_i = n$, $N(\beta_1) = \sum_{i=1}^{Y} m_i = m$, say, so in particular, $m_{Y+1} \leqslant m \leqslant n$. Also note that $m_{i,Y+1} \geqslant m_i - m_{Y+1}$, so by Lemma 4, $g(m_{i,Y+1}) \geqslant g(m_i) - g(m_{Y+1})$. On writing $T(X)$ for the left-hand side of (4.4), we have

$$\begin{aligned} T(Y+1) &= T(Y) + (p-Y-1)g(m_{Y+1}) + \sum_{i=1}^{Y}\{g(m_{i,Y+1}) - g(m_i)\} \\ &\geqslant (p-1)g(m) + (p-2Y-1)g(m_{Y+1}), \text{ by hypothesis,} \\ &\geqslant (p-1)\left\{g(n) + \frac{c_2 g(m_{Y+1})}{\log\log m'_{Y+1}}\right\} - 2Yg(m_{Y+1}), \text{ by Lemma 4,} \\ &\geqslant (p-1)g(n), \text{ since } X = Y+1 \text{ satisfies (4.3).} \end{aligned}$$

The lemma now follows by induction.

Lemma 8. *Let* $\beta = \sum a_j \xi^j$. *Suppose that for each fixed* i $(0 \leqslant i \leqslant p-1)$, *at least* $2g(n)/g(1)$ *of the numbers* $a_i - a_j$ $(0 \leqslant j \leqslant p-1)$ *are non-zero. Then*

$$\sum_{i,j=0}^{p-1} g(n_{ij}) \geqslant 2(p-1)g(n).$$

Proof. Since g is increasing, we have

$$\sum_{i,j=0}^{p-1} g(n_{ij}) \geqslant \sum_{i=0}^{p-1} \frac{2g(n)}{g(1)} g(1) = 2pg(n) \geqslant 2(p-1)g(n).$$

Proof of Theorem 3. First, we may choose any representation of the form (2.3) for β. For, if $\beta = \sum a_j \xi^j = \sum a_j^* \xi^j$ are two such representations, then $a_i - a_i^* = a_j - a_j^*$, whence

$$N(a_i - a_j) = N(a_i^* - a_j^*) \quad (0 \leqslant i, j \leqslant p-1).$$

So we may suppose

$$\text{(4.5)} \qquad \sum_{j=0}^{p-1} n_j = n.$$

Next, a permutation of the a_j in $\sum a_j \xi^j$ does not change $N(\beta)$. For let σ be a permutation of $\{0, 1, \ldots, p-1\}$ and τ be its inverse. Let $\beta^* = \sum a_{\sigma(j)} \xi^j$ and choose a representation $\beta^* = \sum a_j^* \xi^j$ with $\sum N(a_j^*) = N(\beta^*)$. Comparing the two expressions for β^*, we see that there is an a such that

$$a_j^* = a_{\sigma(j)} + a \quad (0 \leqslant j \leqslant p-1).$$

Now

$$\beta = \sum a_j \xi^j = \sum (a_j + a)\xi^j = \sum a_{\tau(j)}^* \xi^j.$$

So

$$N(\beta) \leqslant \sum N(a_j^*) = N(\beta^*) \leqslant \sum N(a_j) = N(\beta),$$

whence $N(\beta^*) = N(\beta)$, as required. So we may suppose that

$$n_0 \geqslant n_1 \geqslant \ldots \geqslant n_{X-1} > n_X = \ldots = n_{p-1} = 0. \tag{4.6}$$

As a final piece of notation, choose $\delta = \delta(k)$, depending only on k, such that

$$0 < \delta < 1 - k^{-1}\log 2. \tag{4.7}$$

The proof now proceeds by induction on n. If $n = 0$, (4.1) is trivially true. So we make the following induction hypothesis: If $\beta^* = \sum a_j^* \xi^j \in \boldsymbol{Q}(P)$, the $a_j^* \in \boldsymbol{Q}(P_1)$ being integers, and $N(\beta^*) < n$, then

$$\sum_{i,j=0}^{p-1} g[N(a_i^* - a_j^*)] \geqslant 2(p-1)g[N(\beta^*)].$$

Now, to prove (4.1) for n (> 0), we distinguish 3 cases.

First case. $\dfrac{4g(n)}{(p-1)g(1)} \leqslant \min\left\{1, \dfrac{c_2}{\log\log n'}\right\}$. If any of the representations $\beta = \sum_j (a_j - a_i)\xi^j$ $(0 \leqslant i \leqslant p-1)$ has less than $\frac{1}{2}(p-1) \times \times \sum_j (a_j - a_i) \min\{1, c_2/\log\log n'\}$ non-zero terms, then (4.1) follows from Lemma 7. Otherwise, all such representations have at least $2g(n)/g(1)$ non-zero terms, and (4.1) follows from Lemma 8. This proves the first case.

From now on, we therefore suppose that

$$\frac{4g(n)}{(p-1)g(1)} > \min\left\{1, \frac{c_2}{\log\log n'}\right\}.$$

Consequently, there is a positive number $c_6 = c_6(k)$, depending only on k, such that

$$p \leqslant \min\{n, n/\log n\} \quad \text{whenever } p \geqslant c_6. \tag{4.8}$$

Second case. $n_j \leqslant n(\log n)^{\delta-1}$ $(0 \leqslant j \leqslant p-1)$. Set $t = [\frac{1}{2}(\log n)^{1-\delta}]$ and consider a fixed i $(0 \leqslant i \leqslant p-1)$. Let $a_1, \ldots, a_\nu$ be the non-zero numbers among the n_{ij} $(0 \leqslant j \leqslant p-1)$. Then

$$\lambda = 1 \leqslant a_r \leqslant \mu = nt^{-1} \quad (1 \leqslant r \leqslant \nu)$$

and

$$\sum_{r=1}^{\nu} a_r \geqslant n,$$

because $\beta = \sum_j (a_j - a_i)\xi^j$. From this, $n \leqslant \sum a_r \leqslant \nu \max a_r \leqslant \nu n t^{-1}$, so

$$\nu \geqslant t. \tag{4.9}$$

Now by (4.8), there is a number $c_7 = c_7(k) \geqslant c_6$ such that

$$p \leqslant nt^{-1} \quad \text{and} \quad t \geqslant 2 \quad \text{whenever } p \geqslant c_7. \tag{4.10}$$

So, if $p \geqslant c_7$,

$$\left[\frac{\mu\nu - n}{\mu - \lambda}\right] = \left[\nu - t + \frac{\nu - t}{n/t - 1}\right] = \nu - t$$

because, by (4.9) and (4.10),

$$0 \leqslant \frac{\nu - t}{n/t - 1} \leqslant \frac{p - t}{n/t - 1} \leqslant \frac{n/t - t}{n/t - 1} < 1.$$

Hence by Lemma 2,

$$\begin{aligned}\sum_{j=0}^{p-1} g(n_{ij}) &= \sum_{r=1}^{\nu} g(a_r)\\ &\geqslant (\nu - t)g(1) + (t-1)g(nt^{-1}) + g(nt^{-1} - \nu + t)\\ &\geqslant (t-1)g(nt^{-1}) + g(nt^{-1}) \text{ by Lemma 4, Corollary,}\\ &= tg(nt^{-1})\\ &\geqslant 2g(n), \text{ by Lemma 5,}\end{aligned}$$

providing $n \geqslant c_4$ and $\frac{1}{4}(\log n)^{1-\delta} \leqslant t \leqslant n^{1/2}$. The last of these conditions is satisfied if $p \geqslant c_7$, by (4.10). Then, we also have $n \geqslant p$, by (4.8). So

$$\sum_{j=0}^{p-1} g(n_{ij}) \geqslant 2g(n) \quad \text{whenever } p \geqslant \max\{c_4, c_7\}.$$

From this

$$\sum_{i,j=0}^{p-1} g(n_{ij}) \geqslant 2pg(n) \geqslant 2(p-1)g(n) \quad \text{whenever } p \geqslant \max\{c_4, c_7\}.$$

Third case. $n_0 > n(\log n)^{\delta-1}$. Put

$$\beta_1 = \sum_{j=1}^{p-1} a_j \xi^j = \beta - a_0.$$

From (4.5) and the two representations of β_1, we see that $N(\beta_1) = n - n_0 = m$, say. Thus the induction hypothesis applies to β_1 giving

$$\sum_{i,j=1}^{p-1} g(n_{ij}) + 2\sum_{j=1}^{p-1} g(n_j) \geqslant 2(p-1)g(m). \tag{4.11}$$

Just as in the proof of Lemma 7, we have $g(n_{0j}) \geqslant g(n_0) - g(n_j)$. Using this and (4.11),

$$\sum_{i,j=0}^{p-1} g(n_{ij}) \geqslant 2(p-1)g(m) + 2\sum_{j=1}^{p-1}\{g(n_{0j}) - g(n_j)\} \tag{4.12}$$

$$\geqslant 2(p-1)\{g(m)+g(n_0)\} - 4\sum_{j=1}^{p-1} g(n_j)$$

$$\geqslant 2(p-1)\left\{g(m)+g(n_0) - 2g\left(\frac{m}{p-1}\right)\right\}, \text{ by Lemma 1.}$$

First subcase. $n_0 \leqslant \frac{1}{2}n$. By data, $\log n \leqslant p-1$. Also g is increasing, so from (4.12),

$$\sum_{i,j=0}^{p-1} g(n_{ij}) \geqslant 2(p-1)\left\{g(m)+g(n_0) - 2g\left(\frac{n}{\log n}\right)\right\}$$

$$\geqslant 2(p-1)g(n), \text{ by Lemma 5, providing } n_0 \geqslant c_3.$$

But by (4.10), $n_0 > \dfrac{n}{(\log n)^{1-\delta}} > \dfrac{n}{\log n} \geqslant p$ whenever $p \geqslant c_7$ $(\geqslant c_0)$. So

$$\sum_{i,j=1}^{p-1} g(n_{ij}) \geqslant 2(p-1)g(n) \quad \text{whenever } p \geqslant \max\{c_3, c_7\}.$$

Second subcase. $n_0 > \frac{1}{2}n$. If X satisfies the hypotheses of Lemma 7, then (4.1) is immediate. So we can suppose that

$$X > \tfrac{1}{2}(p-1)\min\{1, c_2/\log\log n'\} \geqslant \tfrac{1}{2}\log n \min\{1, c_2/\log\log n'\}.$$

Now, $m \geqslant X-1$, so there is a number $c_8 = c_8(k)$ such that

$$m \geqslant c_3(k,1) \quad \text{whenever } n \geqslant c_8. \tag{4.13}$$

Next, $p-1 \geqslant \log n \geqslant \log m$, so by (4.12) and Lemma 4,

$$\sum_{i,j=0}^{p-1} g(n_{ij}) \geqslant 2(p-1)\left\{g(n) + \frac{c_2 g(m)}{\log\log m'} - 2g\left(\frac{m}{\log m}\right)\right\}$$

$$\geqslant 2(p-1)g(n) \text{ if } n \geqslant c_8, \text{ by (4.13) and Lemma 5.}$$

So by (4.8)

$$\sum_{i,j=0}^{p-1} g(n_{ij}) \geqslant 2(p-1)g(n) \quad \text{whenever } p \geqslant \max\{c_6, c_8\}.$$

Finally, combining the three cases,

$$\sum_{i,j=0}^{p-1} g(n_{ij}) \geqslant 2(p-1)g(n) \quad \text{whenever } p \geqslant \max\{c_3, c_4, c_7, c_8\}.$$

So the theorem follows by induction with $c_5 = \max\{c_3, c_4, c_7, c_8\}$.

5. Small values of p.

The next lemma enables us to deal with the case when P is the product of distinct small primes. Denote the sequence of odd primes by $\{p_r\}$ and put $p_0 = 1$.

LEMMA 9. *Suppose that $P = p_1 p_2 \ldots p_\nu$ and let β be a cyclotomic integer in $\boldsymbol{Q}(P)$. Then*

$$\mathscr{M}(\beta) \geqslant 2^{-\nu} N(\beta).$$

Proof. The statement is true for $\nu = 0$, because then $P = 1$ and β is a rational integer, so $|\beta| = N(\beta)$ and $\mathscr{M}(\beta) = N(\beta)^2 \geqslant N(\beta)$. Suppose that the statement is true when $\nu = \mu - 1$ $(\mu \geqslant 1)$. Let $P = p_1 p_2 \ldots p_\mu$ and $\beta \in \boldsymbol{Q}(P)$. Set $p = p_\mu$, and let ξ be a primitive pth root of unity. Then we can write

$$\beta = \sum_{j=0}^{p-1} a_j \xi^j = \sum_{j=0}^{p-1} (a_j - a_i)\xi^j \quad (0 \leqslant i \leqslant p-1),$$

where $a_j \in \boldsymbol{Q}(P/p)$ are integers. So

$$N(\beta) \leqslant \sum_{j=0}^{p-1} N(a_j - a_i) \quad (0 \leqslant i \leqslant p-1). \tag{5.1}$$

Now

$$2(p-1)\mathscr{M}(\beta) = \sum_{i,j=0}^{p-1} \mathscr{M}(a_i - a_j), \text{ by (2.4)},$$

$$\geqslant \sum_{i,j=0}^{p-1} 2^{-\mu+1} N(a_i - a_j), \text{ by hypothesis},$$

$$\geqslant 2^{-\mu+1} p N(\beta), \text{ by (5.1)},$$

so

$$\mathscr{M}(\beta) \geqslant 2^{-\mu} N(\beta).$$

Hence the statement is true for $\nu = \mu$ and so for all ν, by induction.

6. Proof of Theorem 1.

In order to prove Theorem 1 for a given $k > \log 2$, it suffices to show that there is a positive number $c_9 = c_9(k)$ such that, for all cyclotomic integers β,

6.1) $$\mathscr{M}(\beta) \geqslant c_9 g[N(\beta)].$$

For suppose (6.1) holds. Let

$$c = \min\{c_9 e^{-\frac{1}{2}k}, f(1)^{-1}, \ldots, f([c_1])^{-1}\},$$

so that $c = c(k) > 0$. If $N(\beta) \geqslant c_1$ then by Lemma 3,

$$\mathscr{M}(\beta) \geqslant c_9 g[N(\beta)] \geqslant c_9 e^{-\frac{1}{2}k} f[N(\beta)] \geqslant c f[N(\beta)].$$

If $0 \leqslant N(\beta) < c_1$, the same conclusion follows from (2.2) and the definition of c. So by (2.1),

$$\overline{|\beta|}^2 \geqslant \mathscr{M}(\beta) \geqslant cf[N(\beta)]$$

for all β, and this is the statement of Theorem 1.

It now remains to prove (6.1). To do this, we suppose that (6.1) is false for every $c_9 > 0$ and show that for suitable c_9 this leads to a contradiction. Choose c_9 initially with

$$0 < c_9 \leqslant 1. \tag{6.2}$$

Let P be the smallest positive integer such that $\boldsymbol{Q}(P)$ contains an exception to (6.1). Then $P > 2$, since if $\beta \in \boldsymbol{Q}(1) = \boldsymbol{Q}(2)$, then β is a rational integer, $N(\beta) = |\beta|$, and

$$\mathscr{M}(\beta) = N(\beta)^2 \geqslant c_9 g[N(\beta)], \text{ by (6.2).}$$

Let p be the largest prime factor of P and suppose that $p^N \| P$ and let $P = pP_1$. Let ξ be a primitive p^Nth root of unity. Now choose $\beta = \sum \alpha_j \xi^j$ to be an exception to (6.1), the $\alpha_j \in \boldsymbol{Q}(P_1)$ being integers. As before, we abbreviate

$$N(\beta) = n, \quad N(\alpha_j) = n_j \quad \text{and} \quad N(\alpha_i - \alpha_j) = n_{ij} \quad (0 \leqslant i, j \leqslant p-1).$$

Further, we choose the α_j such that $\sum n_j = n$. As a final piece of notation, choose a positive number $c_{10} = c_{10}(k)$ such that

$$\pi(t) < \frac{kt}{\log 2 \log t} \quad \text{whenever } t \geqslant c_{10}, \tag{6.3}$$

$\pi(t)$ being the number of primes less than t. We now have to consider various cases.

First case. $N \geqslant 2$. By (2.8),

$$\begin{aligned}\mathscr{M}(\beta) &= \sum \mathscr{M}(\alpha_j)\\ &\geqslant c_9 \sum g(n_j), \quad \text{since each } \alpha_j \in \boldsymbol{Q}(P_1) \text{ and } P_1 < P,\\ &\geqslant c_9 g(n), \text{ by Lemma 4, Corollary,}\end{aligned}$$

and this contradicts the definition of β.

Second case. $N = 1$ and $p \geqslant \max\{c_5, 1+\log n\}$. By (2.4),

$$\begin{aligned}\mathscr{M}(\beta) &= \frac{1}{2(p-1)} \sum \mathscr{M}(\alpha_i - \alpha_j)\\ &\geqslant \frac{c_9}{2(p-1)} \sum g(n_{ij}), \text{ since each } \alpha_i - \alpha_j \in \boldsymbol{Q}(P_1),\\ &\geqslant c_9 g(n), \text{ by Theorem 3,}\end{aligned}$$

a contradiction.

Third case. $N = 1$ and $\max\{\log c_1, c_5, c_{10}\} \leqslant p-1 \leqslant \log n$. By Lemma 9,

$$\begin{aligned}\log \mathscr{M}(\beta) &\geqslant \log n - \pi(p-1)\log 2\\ &\geqslant \log n - \pi(\log n)\log 2, \text{ since } p-1 \leqslant \log n,\\ &> \log n - \frac{k \log n}{\log\log n} \text{ by (6.3), since } \log n \geqslant c_{10},\\ &= \log f(n)\\ &> \log g(n), \text{ by Lemma 3, since } n \geqslant c_1.\end{aligned}$$

So

$$\mathscr{M}(\beta) \geqslant c_9 g(n) \text{ by (6.2),}$$

a contradiction.

Fourth case. $N = 1$ and $p < \max\{\log c_1, c_5, c_{10}\} + 1 = c_{11}$. Again by Lemma 9,

$$\begin{aligned}\mathscr{M}(\beta) &\geqslant 2^{-\pi(c_{11})} n\\ &\geqslant c_9 g(n) \text{ providing } c_9 \leqslant 2^{-\pi(c_{11})}.\end{aligned}$$

So we have a contradiction in all cases if we choose c_9 with $0 < c_9 < 2^{-\pi(c_{11})}$. By the remarks at the beginning of this section, this proves Theorem 1.

7. Proof of Theorem 2. To prove Theorem 2, we make the following construction. As before, let $\{p_r\}$ be the sequence of odd primes, let ξ_r be a primitive p_rth root of unity and define

$$\chi_r(s) = \begin{cases} 1 & \text{if } s \text{ is a non-zero quadratic residue mod } p_r,\\ 0 & \text{otherwise.}\end{cases}$$

Put

$$\alpha_r = \sum_{s=0}^{p_r-1} \chi_r(s) \xi_r^s \quad \text{and} \quad \beta_\nu = \alpha_1 \alpha_2 \ldots \alpha_\nu.$$

For each $\mu \geqslant \nu$, let ζ_μ be a sum of $\frac{1}{2}(p_\nu - 1)$ distinct primitive p_μth roots of unity and write $\beta_{\nu\mu} = \beta_{\nu-1}\zeta_\mu$. We shall show that the $\beta_{\nu\mu}$ have the properties required in Theorem 2.

Let c be a given positive number and, for the moment, consider a fixed $\nu > 1$. Exactly $\frac{1}{2}(p_r - 1)$ of the $\chi_r(s)$ are non-zero, so by Lemma 6 and induction on ν,

$$N(\beta_{\nu\mu}) = N(\beta_\nu) = \prod_{r=1}^{\nu} \tfrac{1}{2}(p_r - 1) = n_\nu, \text{ say.} \tag{7.1}$$

By (2.6)

$$\mathscr{M}(\beta_{\nu\mu}) = \tfrac{1}{2}(p_\nu - 1)\left(1 - \frac{p_\nu - 3}{2(p_\mu - 1)}\right)\mathscr{M}(\beta_{\nu-1}),$$

a strictly increasing function of μ. Now, if a and β are equivalent cyclotomic integers, we clearly have $\mathscr{M}(a) = \mathscr{M}(\beta)$. So this shows that the $\beta_{\nu\mu}$ $(\mu \geqslant \nu)$ are inequivalent. Next, let a_r' be a conjugate of a_r. From the Gauss sum, we have

$$a_r' = \begin{cases} \tfrac{1}{2}(-1 \pm p_r^{1/2}) & \text{if} \quad p_r \equiv 1 \pmod 4, \\ \tfrac{1}{2}(-1 \pm i p_r^{1/2}) & \text{if} \quad p_r \equiv -1 \pmod 4. \end{cases}$$

So

$$\overline{|a_r|}^2 \leqslant \tfrac{1}{4}(p_r^{1/2}+1)^2$$

and

$$\overline{|\beta_{\nu\mu}|}^2 = \overline{|\beta_{\nu-1}|}^2 \, \overline{|\zeta_\mu|}^2 \leqslant \prod_{r=1}^{\nu-1} \tfrac{1}{4}(p_r^{1/2}+1)^2 \{\tfrac{1}{2}(p_\nu - 1)\}^2, \tag{7.2}$$

since $N(\zeta_\mu) = \frac{1}{2}(p_\nu - 1)$.

In what follows, $\theta_1, \ldots, \theta_4$ denote functions of ν alone which tend to 1 as $\nu \to \infty$. From the prime number theorem,

$$\nu = \frac{p_\nu}{\log p_\nu}\left\{1 + \frac{\theta_1}{\log p_\nu}\right\}. \tag{7.3}$$

By (7.1) and well-known estimates,

$$\begin{aligned} \log n_\nu &= \sum_{r=1}^{\nu} \log p_r - \nu \log 2 + \sum_{r=1}^{\nu} \log(1 - p_r^{-1}) \\ &= p_\nu - \nu \log 2 + O\left(\frac{p_\nu}{(\log p_\nu)^2}\right), \quad \text{as } \nu \to \infty, \\ &= p_\nu \left\{1 - \frac{\theta_2 \log 2}{\log p_\nu}\right\}, \text{ by (7.3).} \end{aligned}$$

From this, $\log\log n_\nu \sim \log p_\nu$, so

$$p_\nu = \log n_\nu \left\{1 + \frac{\theta_3 \log 2}{\log\log n_\nu}\right\} \tag{7.4}$$

and

$$\log p_\nu = \log\log n_\nu \left\{1 + O\left(\frac{1}{(\log\log n_\nu)^2}\right)\right\}. \tag{7.5}$$

By (7.1) and (7.2),

$$\begin{aligned} \log \frac{\overline{|\beta_{\nu\mu}|}^2}{n_\nu} &\leqslant \sum_{r=1}^{\nu} \log \frac{(p_r^{1/2}+1)^2}{2(p_r - 1)} + O(\log p_\nu) \\ &= -\nu \log 2 + O\left(\sum_{r=1}^{\nu} p_r^{-1/2}\right) + O(\log p_\nu) \end{aligned}$$

$$\begin{aligned} &= -\frac{p_\nu \log 2}{\log p_\nu}\left\{1 + \frac{\theta_4}{\log p_\nu}\right\}, \text{ by (7.3) and (7.5),} \\ &= -\frac{\log 2 \log n_\nu}{\log\log n_\nu}\left\{1 + \frac{\theta(\nu)}{\log\log n_\nu}\right\}, \text{ by (7.4) and (7.5),} \end{aligned}$$

where $\theta(\nu) \to 1 + \log 2$ as $\nu \to \infty$. So

$$\log \frac{\overline{|\beta_{\nu\mu}|}^2}{n_\nu} < -\frac{\log 2 \log n_\nu}{\log\log n_\nu} + \log c, \quad \text{whenever } \nu \text{ is large enough,}$$

i.e. $\overline{|\beta_{\nu\mu}|}^2 < cf(n_\nu, \log 2)$ whenever ν is large enough $(\mu \geqslant \nu)$. This proves Theorem 2.

References

[1] J. W. S. Cassels, *On a conjecture of R. M. Robinson about sums of roots of unity*, J. Reine Angew. Math. 238 (1969), pp. 112–131.

[2] G. H. Hardy, J. E. Littlewood and G. Polya, *Inequalities*, Cambridge 1934.

[3] R. M. Robinson, *Intervals containing infinitely many sets of conjugate algebraic integers*, Report of the Institute in the Theory of Numbers (University of Colorado, 1959), pp. 200–206.

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

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

TRINITY COLLEGE, Cambridge

Received on 28.8.1971 (211)