

Some Conjectures About Cyclotomic Integers

By Raphael M. Robinson

1. Introduction. Kronecker [2] proved in 1857 that the only algebraic integers which lie with their conjugates on the unit circle $|z| = 1$ are the roots of unity. If we consider instead the closed interior of the unit circle, $|z| \leq 1$, then we allow only one additional algebraic integer, namely 0. But if we consider the set $|z| \leq R$, where $R > 1$, then infinitely many other algebraic integers appear. Indeed, by a theorem of Fekete and Szegő [1], there are infinitely many algebraic integers which lie with their conjugates in $r \leq |z| \leq R$, provided that $1 \leq r < R$.

What happens if we restrict our attention to cyclotomic integers, that is, to algebraic integers which lie in the field generated by all the roots of unity? Here the situation is quite different. If $R < \sqrt{2}$, then no additional numbers appear; that is, the only cyclotomic integers which lie with their conjugates in $|z| < \sqrt{2}$ are 0 and the roots of unity. (This is proved in §2.) We wish to study what happens for larger values of R . Now if α lies with its conjugates in $|z| \leq R$, then the same is true of any conjugate of α multiplied by any root of unity. Hence, for this problem, we can consider two numbers as equivalent if one is a root of unity times a conjugate of the other. Denoting by $\|\alpha\|$ the maximum absolute value of the conjugates of α , what we said above was that any cyclotomic integer α with $\|\alpha\| < \sqrt{2}$ is either 0 or a root of unity; in the latter case, α is equivalent to 1.

I have made a numerical study of cyclotomic integers α with $\|\alpha\| \leq 3$, as described in §3. This study has suggested a number of problems and conjectures, several of which are stated below. Some evidence for the conjectures appears in §§4, 5.

Problem 1. How can we tell whether there is any cyclotomic integer with a given absolute value? More generally, how can we find all the cyclotomic integers with this absolute value? Does it ever happen that there are infinitely many inequivalent cyclotomic integers with the same absolute value?

Problem 2. How can we tell whether a given cyclotomic integer can be expressed as a sum of a prescribed number of roots of unity?

Conjecture 1. Any cyclotomic integer α with $\|\alpha\| < 2$ is either the sum of two roots of unity, is equivalent to a number of the form $(\sqrt{a} + i\sqrt{b})/2$, where a and b are positive integers, or is equivalent to one of the following three numbers:

$$\frac{3 + \sqrt{13} + i\sqrt{(26 - 6\sqrt{13})}}{4}, \quad 1 + i\frac{\sqrt{5} + 1}{2}, \quad 2\cos\frac{2\pi}{7} + \frac{1 + i\sqrt{3}}{2}.$$

Conjecture 2. There are only a finite number of inequivalent cyclotomic integers with $\|\alpha\| \leq \sqrt{5}$ which are not equivalent to a number of one of the following forms, where N is a positive integer:

$$2\cos\pi/N, \quad 1 + 2i\cos\pi/N, \quad \sqrt{5}\cos\pi/N + i\sin\pi/N.$$

Received September 8, 1964. This work was supported in part by the Miller Institute for Basic Research in Science.

Conjecture 3. The numbers $1 + 2i \cos \pi/N$ and $\sqrt{5} \cos \pi/N + i \sin \pi/N$ are equivalent only for $N = 2, 10, 30$.

Conjecture 4. If α is a cyclotomic integer with $\|\alpha\| \leq \sqrt{5}$, then either $\|\alpha\|$ has one of the forms

$$2 \cos \pi/N, \quad \sqrt{(1 + 4 \cos^2 \pi/N)},$$

where N is a positive integer, or else is equal to one of the two numbers

$$\sqrt{\frac{5 + \sqrt{13}}{2}}, \quad \frac{\sqrt{7} + \sqrt{3}}{2}.$$

Conjecture 5. The only cyclotomic integers satisfying $\|\alpha\| \leq \sqrt{5}$ which are expressible as sums of three roots of unity are those equivalent to numbers of the forms

$$2 \cos \pi/N, \quad 1 + 2i \cos \pi/N,$$

where N is a positive integer, or to one of the five numbers

$$\frac{1 + i\sqrt{7}}{2}, \quad \frac{\sqrt{5} + i\sqrt{3}}{2}, \quad 2 \cos \frac{2\pi}{7} + \frac{1 + i\sqrt{3}}{2}, \\ 1 + e^{2\pi i/13} + e^{8\pi i/13}, \quad 1 + e^{2\pi i/24} + e^{14\pi i/24}.$$

2. Some Useful Formulas. Before describing the computation which was made, we prove a theorem and derive some useful formulas. In the first place, if α is a cyclotomic integer, then the conjugates of $|\alpha|^2$ are $|\alpha^{(j)}|^2$, where $\alpha^{(j)}$ runs through the conjugates of α . (However, distinct conjugates of α may not produce distinct conjugates of $|\alpha|^2$.) Indeed, choose m so that α lies in the field $R(\zeta)$ obtained by adjoining $\zeta = e^{2\pi i/m}$ to the field of rationals. The automorphisms of this field are defined by $\sigma_j(\zeta) = \zeta^j$, where j runs through a reduced residue system mod m . Notice that $\sigma_j \sigma_k = \sigma_{jk} = \sigma_k \sigma_j$. Also, $\sigma_{-1}(\zeta) = \zeta^{-1} = \bar{\zeta}$, hence $\sigma_{-1}(z) = \bar{z}$ for any z in $R(\zeta)$. Thus

$$\sigma_j(\bar{\alpha}) = \sigma_j(\sigma_{-1}(\alpha)) = \sigma_{-1}(\sigma_j(\alpha)) = \overline{\sigma_j(\alpha)},$$

and so

$$\sigma_j(|\alpha|^2) = \sigma_j(\alpha \bar{\alpha}) = \sigma_j(\alpha) \sigma_j(\bar{\alpha}) = \sigma_j(\alpha) \overline{\sigma_j(\alpha)} = |\sigma_j(\alpha)|^2.$$

The proof of this result depends on the fact that the automorphisms of the cyclotomic field $R(\zeta)$ commute.

In particular, if α is a cyclotomic integer with $\|\alpha\| \leq 2$, then the conjugates of $|\alpha|^2$ all lie in $[0, 4]$, and hence have the form

$$2 + 2 \cos 2k\pi/N \quad [0 \leq k \leq N/2, (k, N) = 1],$$

as shown by Kronecker [2]; see also [3]. It follows that

$$\|\alpha\| = \sqrt{(2 + 2 \cos 2\pi/N)} = \begin{cases} 2 & \text{if } N = 1, \\ 2 \cos \pi/N & \text{if } N \geq 2. \end{cases}$$

Thus the smallest possible value of $\|\alpha\|$ which is greater than 1 is $\sqrt{2}$. This proves the statement made in §1 that if α is a cyclotomic integer with $\|\alpha\| < \sqrt{2}$, then α is 0 or a root of unity.

Are all these values of $\|\alpha\|$ possible? Yes, we can take

$$\alpha = 2 \cos \pi/N = e^{i\pi/N} + e^{-i\pi/N}.$$

As we shall see in §4, there are some values of N for which there are also other essentially different possibilities. But it is easily seen that if α is a sum of two roots of unity, then α must be equivalent to this number.

Similarly, if α is a cyclotomic integer which lies with all of its conjugates in $1 \leq |z| \leq \sqrt{5}$, then the conjugates of $|\alpha|^2$ lie in $[1, 5]$, and hence have the form

$$3 + 2 \cos 2k\pi/N \quad [0 \leq k \leq N/2, (k, N) = 1].$$

It follows that

$$\|\alpha\| = \sqrt{3 + 2 \cos 2\pi/N} = \sqrt{1 + 4 \cos^2 \pi/N}.$$

Are all these values possible? Yes, for either of the following choices of α :

$$\alpha = 1 + 2i \cos \pi/N, \quad \alpha = \sqrt{5} \cos \pi/N + i \sin \pi/N.$$

For some cases in which there are still other possibilities, see §4. For discussion of a method of showing that these two choices are usually not equivalent, see §5.

Conversely, if $\|\alpha\| = \sqrt{3 + 2 \cos 2\pi/N}$, then the conjugates of $|\alpha|^2$ have the form $3 + 2 \cos 2k\pi/N$, and hence lie in $[1, 5]$. Thus if a cyclotomic integer α satisfies $\|\alpha\| \leq \sqrt{5}$, then $\|\alpha\|$ will fail to have the form mentioned if and only if some conjugate of α lies in $|z| < 1$. There are two cases given in §4 where this happens, and in which $2 < \|\alpha\| < \sqrt{5}$.

When can all the conjugates of a cyclotomic integer lie on a circle $|z| = R$? Only if R^2 has no other conjugates, that is, R^2 is a rational integer q . Furthermore, these values are all possible, since we may take $\alpha = \sqrt{q}$. Indeed, \sqrt{q} is a cyclotomic integer, since the Gauss sum

$$\sum_{k=0}^{q-1} e^{2\pi i k^2/q} = \begin{cases} \sqrt{q} & \text{if } q \equiv 1 \pmod{4}, \\ i\sqrt{q} & \text{if } q \equiv 3 \pmod{4}, \end{cases}$$

and $e^{2\pi i/8} + e^{-2\pi i/8} = \sqrt{2}$, which enables us to handle the case when q is even.

More generally, we can take $\alpha = (\sqrt{a} + i\sqrt{b})/2$, where $a + b = 4q$. The latter condition makes $|\alpha|^2 = q$, and also insures that α is an algebraic integer, namely, a root of the equation $(\alpha^2 + q)^2 = a\alpha^2$. In this way, we find a number of cyclotomic integers which lie with their conjugates on the circle $|z| = \sqrt{q}$. If $q = q_1 q_2$, then we may also choose α_1 and α_2 with $|\alpha_1| = \sqrt{q_1}$ and $|\alpha_2| = \sqrt{q_2}$, and put $\alpha = \alpha_1 \alpha_2$.

3. The Computation. It is known that every cyclotomic integer α is a sum of roots of unity. (See, for example, Weiss [4, p. 264].) If α is a sum of n roots of unity, then of course $\|\alpha\| \leq n$. Conversely, it appears likely that if $\|\alpha\|$ is small, then α can be expressed as a sum of a small number of roots of unity. Although I do not know any precise result in this direction, this assumption suggested the computation described below.

Using the IBM 7090 at the Computer Center of the University of California, Berkeley, during the period January–June 1964, I made a survey of cyclotomic integers expressed as sums of n m th roots of unity, which covered the following cases:

$$n = 3, m \leq 240; \quad n = 4, m \leq 90; \quad n = 5, m \leq 50; \quad n = 6, m \leq 30.$$

(However, certain sums of six 27th roots were lost by being "reduced" to sums of five 54th roots, as explained at the end of this section.) In each case, the value of $\|\alpha\|$ was computed, and those cases with $\|\alpha\| \leq 3$ were determined. We shall consider in this paper only the cases in which $\|\alpha\| \leq \sqrt{5}$.

If α is a sum of n m th roots of unity, then we may put

$$\alpha = \zeta^{l_1} + \zeta^{l_2} + \cdots + \zeta^{l_n},$$

where $\zeta = e^{2\pi i/m}$. To cover all sums of n m th roots, it is sufficient to allow l_1, l_2, \dots, l_n to vary independently over complete residue systems mod m . However, this is redundant. How much can we restrict the number of cases? We may use the fact that α is equivalent to any conjugate

$$\alpha^{(j)} = \zeta^{jl_1} + \zeta^{jl_2} + \cdots + \zeta^{jl_n},$$

where $(j, m) = 1$, and also to $\alpha^{(j)}$ multiplied by any root of unity.

In the first place, we may suppose that not all of the differences $l_s - l_r$ have the same factor in common with m , since otherwise we could reduce the value of m , at least after multiplying α by a suitable root of unity. Now if one of the differences is prime to m , then we may number the l 's so that $(l_2 - l_1, m) = 1$. We then divide α by ζ^{l_1} , making $l_1 = 0$ and $(l_2, m) = 1$ for the new α obtained. Choosing j so that $jl_2 \equiv 1 \pmod{m}$, and replacing ζ by ζ^j , we reduce α to an equivalent form with $l_1 = 0, l_2 = 1$.

Can it happen that none of the differences $l_s - l_r$ is prime to m ? This is clearly impossible if m is a prime power, and we shall show that it is also impossible if m has only two distinct prime factors p and q (without all the differences having the same factor in common with m). Indeed, suppose that each difference $l_s - l_r$ is divisible by p or by q , although not all by q . We shall prove that $l_s \equiv l_r \pmod{p}$. If this is not the case, then $l_s \equiv l_r \pmod{q}$. Choose any $l_u \not\equiv l_r \pmod{q}$. Then also $l_u \not\equiv l_s \pmod{q}$. Hence $l_u \equiv l_r \pmod{p}$ and $l_u \equiv l_s \pmod{p}$, so $l_s \equiv l_r \pmod{p}$. That is, all the differences are divisible by p . Thus when m has at most two distinct prime factors, we may always suppose that $l_1 = 0, l_2 = 1$.

In the most general case, we have $m = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$. By the same argument just used, not all of the differences $l_s - l_r$ can be divisible by p_1 or p_2 . Thus we may number the l 's so that $(l_2 - l_1, m)$ is a divisor k of $p_3^{a_3} \cdots p_t^{a_t}$. We then divide α by ζ^{l_1} , making $l_1 = 0$ and $(l_2, m) = k$ for the new α obtained. Choosing j so that $jl_2 \equiv k \pmod{m}$ and $(j, m) = 1$, and replacing ζ by ζ^j , we reduce α to an equivalent form with $l_1 = 0, l_2 = k$. Thus we need only consider numbers α of the form

$$\alpha = 1 + \zeta^k + \zeta^{l_3} + \cdots + \zeta^{l_n},$$

where $k \mid p_3^{a_3} \cdots p_t^{a_t}$, that is, where k may be restricted to being a divisor of the number obtained from m by deleting any two prime powers from its canonical factorization.

Can we put some restrictions on the other exponents? It is convenient to start by allowing each l_r to vary over the interval $[k/2, m + k/2]$. Then, since the terms may be permuted, we may suppose that $l_3 \leq l_4 \leq \cdots \leq l_n$. Furthermore, since

$$\zeta^k \alpha^{(-1)} = 1 + \zeta^k + \zeta^{m+k-l_3} + \cdots + \zeta^{m+k-l_n},$$

we can replace each l_r by its complement $m + k - l_r$. The complements are, of course, in reverse order. Thus we may suppose that $l_3 + l_n \leq m + k$, since otherwise $l_3 + l_n$ would be reduced by taking complements. In order for this inequality to be possible, we must have $2l_3 \leq m + k$. Thus it is sufficient to consider the cases

$$\frac{k}{2} \leq l_3 \leq \frac{m+k}{2}, \quad l_3 \leq l_4 \leq \cdots \leq l_n \leq m+k-l_3.$$

We may still impose the condition $(k, l_3, \dots, l_n) = 1$, which eliminates some cases if $k > 1$. We may also omit cases where two exponents differ by $m/2$, since, in such a case, two terms will cancel. Finally, if two exponents differ by $m/3$, then we may use the identity $\zeta^l + \zeta^{l+m/3} = -\zeta^{l+2m/3}$ to reduce the number of terms. But to eliminate the minus sign, we need an even m . Thus, in this case, we decrease n by one unit at the possible expense of doubling m .

4. Summary of Results. The cyclotomic integers with $\|\alpha\| \leq \sqrt{5}$ obtained by the calculation described in §3 were combined with those given by the formulas of §2 to obtain as complete a list as possible. Duplicate entries were then eliminated, so that the resulting numbers are inequivalent.

We first summarize the cyclotomic integers found with $\|\alpha\| < 2$. Those which are the sums of at most two roots of unity are equivalent to terms of the sequence

$$\alpha = 2 \cos \pi/N,$$

with $N = 2, 3, 4, \dots$. Here $\|\alpha\| = \alpha$. In any other cases, $\|\alpha\|$ must have the same form. We list in Table 1 the nine cases found, giving $\|\alpha\|$ to five decimals, the corresponding value of N , the number n of roots of unity added, the order m of the roots involved, and the exponents of $\zeta = e^{2\pi i/m}$ in the various terms of α , in the form (or one of the forms) which would be obtained by the computation described in §3. Finally, in the last column, we give a number equivalent to this α , but chosen so as to be of minimum possible degree over the rationals, and of maximum possible absolute value. All of the entries in Table 1 except the one on the seventh line were actually found among the answers given by the computer. This one, as the sum of five 70th roots, was beyond the range of the program. The same number can also be written as a sum of six 35th roots, but would also not be found in this form. However, after supplying this entry, it seems quite likely that our list is

TABLE 1

$\ \alpha\ $	N	n	m	Exponents	Equivalent Value
1.41421	4	3	7	0, 1, 3	$(1 + i\sqrt{7})/2$
1.41421	4	3	30	0, 1, 12	$(\sqrt{5} + i\sqrt{3})/2$
1.73205	6	3	8	0, 1, 3	$1 + i\sqrt{2}$
1.73205	6	4	13	0, 1, 3, 9	$(3 + \sqrt{13} + i\sqrt{(26 - 6\sqrt{13})})/4$
1.73205	6	4	20	0, 1, 4, 13	$(1 + i\sqrt{5})/\sqrt{2}$
1.73205	6	5	11	0, 1, 2, 4, 7	$(1 + i\sqrt{11})/2$
1.73205	6	5	70	0, 1, 11, 42, 51	$(\sqrt{5} + i\sqrt{7})/2$
1.90211	10	3	20	0, 1, 9	$1 + i(\sqrt{5} + 1)/2$
1.94986	14	3	42	0, 1, 13	$2 \cos 2\pi/7 + (1 + i\sqrt{3})/2$

complete. This has been formulated in §1 as Conjecture 1.

The following cyclotomic integers were found with $\|\alpha\| = 2$:

$$\alpha = \frac{\sqrt{(16-b)} + i\sqrt{b}}{2} \quad (b = 0, 1, 2, 3, 5, 6, 7),$$

$$\alpha = \frac{(1+i\sqrt{7})(\sqrt{5}+i\sqrt{3})}{4}.$$

Next, with $2 < \|\alpha\| < \sqrt{5}$, there are the two sequences

$$\alpha = 1 + 2i \cos \pi/N,$$

$$\alpha = \sqrt{5} \cos \pi/N + i \sin \pi/N,$$

with $N = 7, 8, 9, \dots$. In both cases,

$$\|\alpha\| = \sqrt{(3 + 2 \cos 2\pi/N)} = \sqrt{(1 + 4 \cos^2 \pi/N)}.$$

However, it is easily seen that the two are equivalent for $N = 10$ and for $N = 30$, so that one of them should be deleted for these values of N . Conjecture 3 states that there are no other cases of duplication. For a discussion of this conjecture, see §5. Thirteen other solutions with $2 < \|\alpha\| < \sqrt{5}$ were found, and are listed in Table 2 in order of increasing $\|\alpha\|$. In all but two of the cases, $\|\alpha\|$ has the same form as above, and the corresponding value of N is given. Notice that N has a different meaning than in Table 1. The other columns have the same meaning as in Table 1. In the two cases where $\|\alpha\|$ does not have the usual form, its value is $\sqrt{(5 + \sqrt{13})/2}$ and $(\sqrt{7} + \sqrt{3})/2$, respectively; in the latter case, α is, in fact, equivalent to $(\sqrt{7} + \sqrt{3})/2$. Conjecture 4 states that these are the only possible additional values for $\|\alpha\|$ in this range.

Finally, we list the cases with $\|\alpha\| = \sqrt{5} \approx 2.23607$:

$$\alpha = \frac{\sqrt{(20-b)} + i\sqrt{b}}{2} \quad (b = 0, 1, 3, 4, 6, 7, 8, 9),$$

$$\alpha = \frac{\sqrt{(10+2\sqrt{5})} + i\sqrt{(10-2\sqrt{5})}}{2}.$$

TABLE 2

$\ \alpha\ $	N	n	m	Exponents
2.06082	7	4	42	0, 1, 6, 19
2.07431	—	3	13	0, 1, 4
2.10100	8	3	24	0, 1, 7
2.14896	10	4	40	0, 1, 9, 30
2.14896	10	4	60	0, 3, 5, 38
2.16391	11	4	11	0, 1, 2, 5
2.17533	12	4	60	0, 3, 5, 27
2.18890	—	4	42	0, 1, 6, 18
2.19133	14	4	28	0, 1, 4, 17
2.21611	21	4	42	0, 1, 5, 18
2.21788	22	4	66	0, 1, 7, 30
2.22483	28	4	28	0, 1, 4, 12
2.22797	33	4	66	0, 1, 7, 43

Because a number of the solutions with $\|\alpha\| = 2$ and $\|\alpha\| = \sqrt{5}$ were beyond the range of the computer calculation, we did not venture the conjecture that our lists are complete for $\|\alpha\| \leq \sqrt{5}$. We did, however, make the weaker Conjecture 2 that only a finite number of inequivalent solutions were missed. Also, according to Conjecture 5, there are no additional values of α expressible as sums of three roots of unity. This conjecture would have as consequences that none of the values of α which are listed in Tables 1 and 2 as sums of more than three roots of unity could be reduced to sums of three roots, that none of the solutions of $\|\alpha\| = 2, \sqrt{5}$, except those equivalent to 2 and $2 + i$ could be so written, and that the number $\sqrt{5} \cos \pi/N + i \sin \pi/N$ is not a sum of three roots of unity except for $N = 2, 3, 5, 10, 30$. Thus, if Conjecture 5 is true, this last sequence would furnish infinitely many inequivalent numbers α with $\|\alpha\| < 3$ which are not expressible as sums of three roots of unity, contrary to a very broad conjecture which I made at the Institute in the Theory of Numbers at Boulder in 1959.

5. Discussion. Besides the question as to whether the results listed in §4 are complete, which I have not been able to answer, there is the question of redundancy. Are some two of these numbers, although appearing in different forms, actually equivalent?

It is possible to answer this question in any specific case. For this purpose, we need to know what roots of unity lie in the field $R(e^{2\pi i/m})$. It is easily proved that only the m th roots lie in the field when m is even, and just the $2m$ th roots when m is odd. (See, for example, Weiss [4, p. 267].) Now let α and β be cyclotomic integers. Choose an even integer m so that α and β both lie in $R(e^{2\pi i/m})$. For β to be equivalent to α , the latter must have a conjugate $\alpha^{(j)}$ for which $\beta/\alpha^{(j)}$ is a root of unity. Since this would have to be an m th root, there are only a finite number of trials to be made, and a decision concerning equivalence can be reached by means of an algebraic calculation. However, if $\beta/\alpha^{(j)}$ is not an m th root of unity, it is much easier to prove this by a numerical calculation.

We tested the equivalence of corresponding terms of the two sequences

$$\begin{aligned}\alpha &= 1 + 2i \cos \pi/N, \\ \beta &= \sqrt{5} \cos \pi/N + i \sin \pi/N.\end{aligned}$$

Both of these are seen to lie in the field of $20N$ th roots of unity. It was only necessary to compare β with those conjugates of α with maximum absolute value, that is, with α and $\bar{\alpha}$. In other words, it was sufficient to compute the two quantities

$$\frac{20N}{2\pi} \arctan \left(2 \cos \frac{\pi}{N} \right), \quad \frac{20N}{2\pi} \arctan \left(\frac{1}{\sqrt{5}} \tan \frac{\pi}{N} \right),$$

and see whether the fractional parts are either the same or complementary. This was found, by a computer calculation, to be false for all N with $3 \leq N \leq 1000$, except for $N = 10, 30$. This provides strong evidence for Conjecture 3.

All the other solutions listed in §4 have been shown to be inequivalent. What we needed to do was to compute $(m/2\pi) \operatorname{amp} \alpha^{(j)}$ for all of these numbers and their conjugates, with an even value of m chosen so that all of the numbers being compared lie in $R(e^{2\pi i/m})$, and to be sure that there are no two cases in which both the fractional parts of this multiple of the amplitudes and the absolute values agree.

The value of m actually used was $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$ for those α with $\|\alpha\| < \sqrt{5}$, and $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19$ when $\|\alpha\| = \sqrt{5}$.

In this connection, the following may be noted. Suppose that we are given a cyclotomic integer α , and we ask whether it is a sum of two roots of unity. If $\|\alpha\| > 2$, then this is, of course, impossible. If $\|\alpha\| = 2$, then α can be a sum of two roots of unity only by being twice a root of unity. Finally, if $\|\alpha\| < 2$, then $\|\alpha\| = 2 \cos \pi/N$ for some N , and α is a sum of two roots of unity only if α is equivalent to $2 \cos \pi/N$, which we can test as above. It was shown that the cyclotomic integers listed in Table 1 are not sums of two roots of unity.

But what about the question whether a cyclotomic integer α can be expressed as a sum of *three* roots of unity (or of some other prescribed number)? For example, how do we know that the number $\alpha = 1 + \zeta + \zeta^3 + \zeta^9$ with $\zeta = e^{2\pi i/13}$, which appeared in Table 1, is not expressible as a sum of three m th roots of unity for some m ? Again, how do we know that $\sqrt{5}$ cannot be expressed as a sum of three roots of unity? In both cases, this seems most unlikely, since the computer calculation would have found any such representation with $m \leq 240$. Conjecture 5 implies a negative answer in both cases. The general question was formulated in §1 as Problem 2.

Added in proof. Andrzej Schinzel has devised a general method of testing whether a given algebraic integer can be expressed as a sum of three roots of unity. In particular, he has applied this method to show that $\sqrt{5}$ cannot be so expressed. The result in this case can also be obtained by checking that $\|\sqrt{5} - \rho\| > 2$ whenever ρ is a root of unity.

In §2, we determined the possible values of $\|\alpha\| \leq 2$, and also the possible values of $\|\alpha\|$ for cyclotomic integers which lie, with their conjugates, in $1 \leq |z| \leq \sqrt{5}$. What other values $\|\alpha\| \leq \sqrt{5}$ are possible? As stated in §4, we found two other possible values, $\sqrt{((5 + \sqrt{13})/2)}$ and $(\sqrt{7} + \sqrt{3})/2 = \sqrt{((5 + \sqrt{21})/2)}$. If someone were to attempt to disprove Conjecture 4, which states that there are no other possibilities, an obvious value to consider for $\|\alpha\|$ would be $\sqrt{((5 + \sqrt{17})/2)}$. It would be sufficient to find a cyclotomic integer having this absolute value. Is there such a number? This question is a special case of Problem 1.

University of California
Berkeley, California

1. M. FEKETE & G. SZEGÖ, "On algebraic equations with integral coefficients whose roots belong to a given point set," *Math. Z.*, v. 63, 1955, pp. 158-172. MR 17, 355.
2. L. KRONECKER, "Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten," *J. Reine Angew. Math.*, v. 53, 1857, pp. 173-175.
3. R. M. ROBINSON, "Intervals containing infinitely many sets of conjugate algebraic integers," *Studies in Mathematical Analysis and Related Topics: Essays in Honor of George Pólya*, Stanford Univ. Press, Stanford, Calif., 1962, pp. 305-315. MR 26 #2433.
4. EDWIN WEISS, *Algebraic Number Theory*, McGraw-Hill, New York, 1963. MR 28 #3021.