On the magnitudes of some small cyclotomic integers

by

FREDERICK ROBINSON (Los Angeles, CA) and
MICHAEL WURTZ (Redmond, WA)

1. Introduction. In [Rob65], Raphael Robinson made a study of small cyclotomic integers, namely, cyclotomic integers α all of whose conjugates lie in $|z| \leq R$ for $R = 2$ and $R = \sqrt{5}$. Robinson made a sequence of five conjectures concerning these numbers, four of which were proved by Schinzel [Sch66], Cassels [Cas69], and Jones [Jon68, Jon69]. In this paper, we resolve the final outstanding conjecture. First, we recall the following definition:

DEFINITION 1.1 (House). For a cyclotomic integer β, let the *house* of β, denoted $\overline{|\beta|}$, be the largest absolute value of all conjugates of β.

Our main result is as follows:

THEOREM 1.2 (Robinson's Conjecture 4 [Rob65]). *If β is a cyclotomic integer with $\overline{|\beta|}^2 \leq 5$, then $\overline{|\beta|}$ 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

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

Note that these values do actually occur as $\overline{|\beta|}$ for some cyclotomic integers (with the exception of $N = 1$ in the first equation), specifically, for β as follows: $\zeta_N + \zeta_N^{-1}$, $\zeta_4 + \zeta_N + \zeta_N^{-1}$, $1 + \zeta_{13} + \zeta_{13}^4$, and $\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^3 + \zeta_{84}^{27}$. The first and last numbers on this list are totally real, so $\overline{|\beta|} = \beta$ in these cases. In studying this problem, we follow the approach of Cassels [Cas69], as well as the recent paper of Calegari, Morrison, and Snyder [CMS11], where a version of this theorem is proven for totally real β.

We actually prove the following stronger statement:

THEOREM 1.3. *If β is a cyclotomic integer with $\overline{|\beta|}^2 \leq 5 + 1/25$, then either $\overline{|\beta|}$ is a number on the list above, or*

$$\overline{|\beta|} = |1 + \zeta_{70} + \zeta_{70}^{10} + \zeta_{70}^{29}|, \quad where \quad \zeta_{70} = e^{2\pi i/70}.$$

The main result of Cassels [Cas69] implies Theorem 1.2 with *at most finitely many exceptions*. The methods of Cassels, however, do not lead to a practical algorithm for determining what those exceptions might be. Indeed, it is noted in [CMS11] that any exception must lie in $\mathbb{Z}[\zeta_N]$ for

$$N = 4692838820715366441120 = 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 47 \cdot 53.$$

The motivation for this project is twofold. Most naturally, it was desirable to answer Robinson's conjecture. Robinson was motivated in part by understanding the relationship between the house of a cyclotomic integer α and the "complexity" of such an integer, as for example measured by the number of roots of unity required to represent α. Although this problem was qualitatively answered by Loxton [Lox72], those arguments are not effective. Another motivation is to the interaction between the algebraic number theory of cyclotomic fields and the numerology of subfactors of small index, as occurring (for example) in [Jon83] and more recently in [IJMS]. This was also the motivation for the recent paper [CMS11]. Although there is no direct application of our result to the indices of subfactors, it is intriguing that the square of the "exotic" case $\sqrt{(5 + \sqrt{13})/2}$ of Theorem 1.2 is also the index of the first exotic subfactor constructed by Aseada and Haagerup [AH99].

1.1. Some notation. The following is well known:

LEMMA 1.4 (Cyclotomic integer). *A number $\beta \in \mathbb{Q}(\zeta_N)$ is a cyclotomic integer if and only if $\beta \in \mathbb{Z}(\zeta_N)$ for some N, i.e. if β can be written as a finite sum of roots of unity.*

In light of this, the following definition makes sense:

DEFINITION 1.5 ($\mathscr{N}$). *For a given cyclotomic integer β, $\mathscr{N}(\beta)$ is the minimal number of roots of unity whose sum is β.*

Note that given α and β, we have $\mathscr{N}(\alpha) - \mathscr{N}(\beta) \leq \mathscr{N}(\alpha \pm \beta) \leq \mathscr{N}(\alpha) + \mathscr{N}(\beta)$.

Following Cassels, we also make the following definition:

DEFINITION 1.6 ($\mathscr{M}$). *For a given cyclotomic integer β, $\mathscr{M}(\beta)$ is the arithmetic mean of $|\beta'|^2$ for all conjugates β' of β.*

Note that $|\beta|^2 = \beta\overline{\beta}$ is a cyclotomic integer. Since the Galois group of a cyclotomic extension is abelian, complex conjugation commutes with any automorphism. In particular, $\mathscr{M}(\beta) = \mathscr{M}(\beta')$ for any conjugate β' of β, and moreover $\mathscr{M}(\beta)$ is the (normalized) trace of $|\beta|^2$, and hence lies in $\mathbb{Q}$.

DEFINITION 1.7 (Equivalence). Two cyclotomic integers α and β are *equivalent* if $\alpha = \zeta\beta'$ for some ζ a root of unity and β' a conjugate of β. We write $\alpha \equiv \beta$.

Since every root of unity has absolute value one, it follows that $\mathscr{M}(\zeta\gamma) = \mathscr{M}(\gamma)$ for any root of unity ζ. In particular, if $\alpha \equiv \beta$, then $\mathscr{M}(\alpha) = \mathscr{M}(\zeta\beta') = \mathscr{M}(\beta') = \mathscr{M}(\beta)$.

DEFINITION 1.8 (Minimal cyclotomic integer). A cyclotomic integer β is *minimal* if $\beta \in \mathbb{Q}(\zeta_N)$, and there is no equivalent $\beta' \in \mathbb{Q}(\zeta_{N'})$ with $N' < N$.

Since $\overline{|\beta|} = \overline{|\beta'|}$, to prove the theorem it suffices to consider all minimal cyclotomic integers.

DEFINITION 1.9 (ζ_N). We always mean by ζ_N a primitive Nth root of unity, not any Nth root of unity.

2. Some preliminary results

2.1. Properties of $\mathscr{M}$

REMARK 2.1. $\mathscr{N}(\beta) = 1$ if and only if $\mathscr{M}(\beta) = 1$. This follows from [Kro37].

LEMMA 2.2. *If* $\mathscr{N}(\beta) = 2$, *then either* $\mathscr{M}(\beta) \geq 15/8$, *or* $\mathscr{M}(\beta) = 3/2, 5/3, 7/4, 9/5$, *or* $11/6$. *The first four values occur only when β is equivalent to $1 + \zeta_N$ for $N = 5$, 7, 30, or 11 respectively, and $11/6$ occurs only for $N = 13$ or 42.*

Proof. The sum of two roots of unity is equivalent to $1 + \zeta_N$ for some N. One computes directly that $\mathscr{M}(1 + \zeta_N) = 2(1 + \mu(N)/\varphi(N))$, where μ is the Möbius μ-function and φ is Euler's totient function, from which the result follows (cf. [CMS11, Remark 9.0.2]). ■

REMARK 2.3 ([Cas69, Lemma 3]). If $\mathscr{N}(\beta) \geq 3$, then $\mathscr{M}(\beta) \geq 2$.

REMARK 2.4 ([Cas69, Section 3]). If $\beta \in \mathbb{Z}(\zeta_N)$, and p^n exactly divides N, then we can write β as a sum of products of p^nth roots of unity with $\eta_j \in \mathbb{Z}(\zeta_{N/p})$. Write $\beta = \sum_{j=0}^{p-1} \zeta_{p^n}^j \eta_j$, and let X be the number of non-zero terms in the summation. Let α_i, $1 \leq i \leq X$, refer to the X non-zero η_j.

If p exactly divides N, note that this representation is unique up to adding a constant to all η_i. We have the equality

$$(2.1) \qquad (p-1)\mathscr{M}(\beta) = (p - X)\sum_{i=1}^{X}\mathscr{M}(\alpha_i) + \sum_{1 \leq i < j \leq X}\mathscr{M}(\alpha_i - \alpha_j).$$

On the other hand, if $n > 1$, then this representation is unique. In this case,

we have the equality

$$(2.2) \qquad \mathscr{M}(\beta) = \sum_{i=1}^{X} \mathscr{M}(\alpha_i).$$

2.2. Conjugation. Throughout the paper, in many cases we will need to show, for β the sum of two given cyclotomic integers, that $\overline{|\beta|}^2 > 5 + 1/25$, and thus β is not an exception to the theorem. One common method of proving this is as follows:

LEMMA 2.5. *Suppose β is equivalent to $\alpha + \zeta_{p^n}\gamma$, where $\alpha \in \mathbb{Q}(\zeta_{M'})$ and $\gamma \in \mathbb{Q}(\zeta_{M''})$. Let m be the largest integer such that $\zeta_{p^m} \in \mathbb{Q}(\zeta_{M'})$ or $\mathbb{Q}(\zeta_{M''})$. Then if $m < n$,*

$$(2.3) \qquad \overline{|\beta|}^2 \geq |\alpha|^2 + |\gamma|^2 + 2|\alpha| \cdot |\gamma| \cdot \cos(\theta)$$

where

$$\theta = \begin{cases} 2\pi/p^n & \text{if } m = 0, \\ \pi/p^{n-m} & \text{if } m > 0. \end{cases}$$

Moreover, if $(M', M'') = 1$, then

$$(2.4) \qquad \overline{|\beta|}^2 \geq \overline{|\alpha|}^2 + \overline{|\gamma|}^2 + 2\overline{|\alpha|} \cdot \overline{|\gamma|} \cdot \cos(\theta).$$

Proof. By assumption on m and n, there exists a Galois automorphism sending ζ_{p^n} to $\zeta_{p^n}^i$ and fixing α and γ as long as $(i, p) = 1$ and $\zeta_{p^m} = \zeta_{p^m}^i$, i.e. when $i \equiv 1 \bmod p^m$. If $m = 0$, we may conjugate ζ_{p^n} to any other *primitive* p^nth root of unity. The largest angle between two adjacent primitive p^nth roots of unity is $2 \cdot 2\pi/p^n$, so we can place the argument of $\zeta_{p^n}^i\gamma$ to within $2\pi/p^n$ of the argument of α. If $m > 0$, then there are p^{n-m} equally spaced primitive p^nth roots of unity that are congruent to 1 mod p^m. We can then guarantee that some conjugate of β is $\alpha + \zeta_{p^n}^i\gamma$, where the difference in arguments between α and $\zeta_{p^n}^i\gamma$ is at most π/p^{n-m}.

For the second claim, if $(M', M'') = 1$, then we may *simultaneously* conjugate α and γ to their largest conjugate, and then apply the first part of the lemma. ∎

2.3. A note on computational accuracy. In several places we have verified results through the use of a computer. For example, given β, we wish to know if $\overline{|\beta|}$ is equal to some γ from the list of Theorem 1.3. We show that by computing $\overline{|\beta|}$ to a necessary degree of accuracy, we can claim that $\overline{|\beta|}$ is equal to γ, and not just very near to it.

LEMMA 2.6. *Suppose β is a cyclotomic integer, γ is on the list of Theorem 1.3, and $k = [\mathbb{Q}(\zeta_N) : \mathbb{Q}] = \varphi(N)$, where $\beta, \gamma \in \mathbb{Q}(\zeta_N)$. If $|\,\overline{|\beta|} - \gamma| < (10 + 1/25)^{-k}$, then $\overline{|\beta|} = \gamma$.*

Proof. Let $\delta = |\,\overline{|\beta|} - \gamma|$. Then δ is also a cyclotomic integer in $\mathbb{Q}(\zeta_N)$ and δ has at most k conjugates. Denote the conjugates by $\delta_1, \ldots, \delta_i$ with $\delta_1 = \delta$. As all conjugates of $\overline{|\beta|}$ and γ have magnitude at most $5 + 1/25$, all conjugates of δ have magnitude at most $10 + 2/25$. Then $|\mathrm{Norm}(\delta)| = |\delta_1 \cdots \delta_i| \leq \delta(10 + 2/25)^{k-1} < 1$. We have $|\mathrm{Norm}(\delta)| < 1$ if and only if $\mathrm{Norm}(\delta) = 0 = \delta$, so $\overline{|\beta|} = \gamma$. ∎

2.4. Theorem 1.3 when $\mathscr{N}(\beta) \leq 3$. In this section, we recall known results that allow us to deduce Theorem 1.3 in the special case when $\mathscr{N}(\beta) \leq 3$:

1. If $\mathscr{N}(\beta) = 1$, then $\overline{|\beta|} = 1 = 2\cos(\pi/3)$.
2. If $\mathscr{N}(\beta) = 2$, then $\beta \equiv 1 + \zeta_n$ for some n and $\overline{|\beta|} = 2|\cos(\pi/n)|$.
3. If $\mathscr{N}(\beta) = 3$, Jones' [Jon69, Theorem 2] states that if $\overline{|\beta|} \leq 1 + \sqrt{2}$, then β is equivalent to (a) $1 + \zeta_n - \zeta_n^{-1}$, (b) $1 \pm i + \zeta_n$, or (c) one of 15 numbers that he lists.

In case (a), $\overline{|\beta|}$ is equal to $\sqrt{1 + 4\cos^2(\pi/M)}$ where the value of M depends on n in a slightly subtle way. In particular,

$$
M(n) = \begin{cases} 2n & \text{if } n \text{ is odd,} \\ n & \text{if } n/2 \text{ is odd,} \\ n/4 & \text{if } n/4 \text{ is odd,} \\ n/2 & \text{if } n/4 \text{ is even.} \end{cases}
$$

In case (b) Lemma 2.5 proves that if n does not divide $2^4 \cdot 3 \cdot 5 \cdot 7$, then $\overline{|\beta|} > \sqrt{5 + 1/25}$ (by letting $\alpha = 1 + i$). There are then 40 divisors of $2^4 \cdot 3 \cdot 5 \cdot 7$ that were checked computationally.

We checked each number in case (c), and all were equal to a form from Robinson.

**3. An upper bound for $\mathscr{M}(\beta)$.** Many of our arguments are based on the following lemma:

LEMMA 3.1. *If β is a cyclotomic integer with $\overline{|\beta|}^2 \leq 5 + 1/25$, then $\mathscr{M}(\beta) < 13/4$ or $\overline{|\beta|} = \sqrt{1 + 4\cos^2(\pi/N)}$ for some N.*

REMARK 3.2. One should compare this with Lemma 5.1.1 of [CMS11], where, assuming the slightly weaker condition $\overline{|\beta|} \leq 76/33$, it is shown that $\mathscr{M}(\beta) < 23/6$. The significant improvement $(23/6 = 13/4 + 7/12)$ in our upper bound for $\mathscr{M}(\beta)$ (at the cost of a stronger bound on $\overline{|\beta|}$) is what allows us to push the methods of Cassels and [CMS11] to prove Robinson's conjecture.

Proof of Lemma 3.1. Let P_i and α_i be as below (note that all P_i are irreducible over $\mathbb{Z}$, and their roots are real and positive):

i	P_i	$1000\alpha_i$	N
1	$x - 3$	110	4
2	$x - 4$	530	6
3	$x - 5$	620	1
4	$x^2 - 6x + 6$	18	12
5	$x^2 - 6x + 7$	28	8
6	$x^2 - 7x + 11$	194	10
7	$x^3 - 10x^2 + 31x - 29$	130	14
8	$x^4 - 13x^3 + 58x^2 - 98x + 41$	45	–
9	$x^4 - 13x^3 + 59x^2 - 107x + 61$	40	15

Let $f(x) = 13/4 - x - \sum \alpha_i \log |P_i(x)|$. We claim that $f(x)$ is positive for all values of x in $[0, 5 + 1/25]$ where it is defined (there are many asymptotes where $f(x) \to +\infty$). Note that f is defined everywhere that is not a root of some P_i.
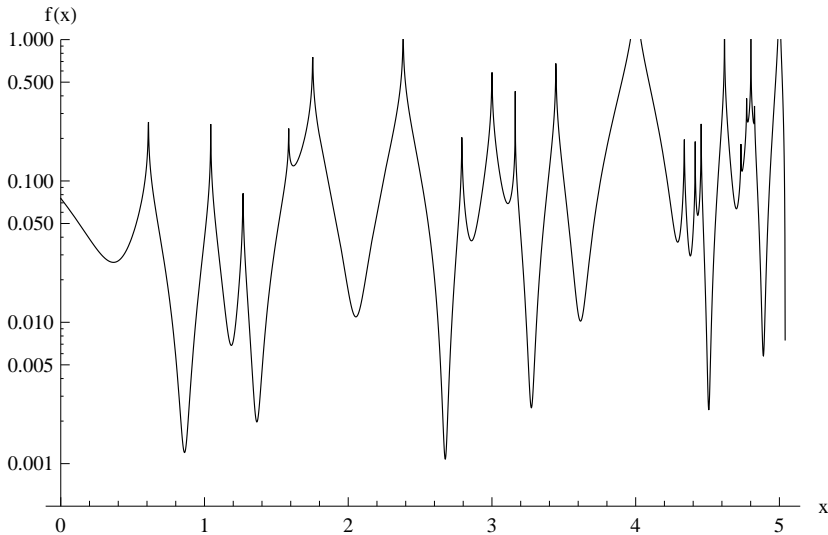
The derivative of $f(x)$ has 20 real zeroes in $[0, 5 + 1/25]$, at which all of f is positive. Also, f is positive at 0 and $5 + 1/25$. So f is positive everywhere on $[0, 5 + 1/25]$ where it is defined.

Now take any non-zero cyclotomic integer β with $\beta\bar{\beta} = \overline{|\beta|}^2 \le 5 + 1/25$.

If $\overline{|\beta|}^2$ is equivalent to a root of some P_i, note two things: it cannot be P_8, as that has a non-abelian Galois group D_8 which would imply that β is not a cyclotomic integer. Furthermore $\overline{|\beta|}^2$ is the largest root of P_i. All largest roots of P_i, $i \ne 8$, are squares of $\sqrt{1 + 4\cos^2(\pi/N)}$ for N as shown in the above table.

If $\beta\bar{\beta}$ is not equivalent to a root of any P_i, let x_j, $1 \le j \le n$, be the conjugates of $\beta\bar{\beta}$. Note that the conjugates of $\beta\bar{\beta}$ are $\beta'\bar{\beta}'$ for β' the conjugates

of β. Then $0 < x_j \le 5 + 1/25$ and $P_i(x_j) \ne 0$ for any i, j, so we have

$$\sum_{j=1}^{n} f(x_j) > 0,$$

$$\sum_{j=1}^{n} \left(\tfrac{13}{4} - x_j - \sum_i \alpha_i \log |P_i(x_j)| \right) > 0,$$

$$\tfrac{13}{4} n - \sum_{j=1}^{n} x_j - \sum_i \left(a_i \sum_{j=1}^{n} \log |P_i(x_j)| \right) > 0,$$

$$\tfrac{13}{4} n - n \mathcal{M}(\beta) - \sum_i a_i \log \left| \prod_{j=1}^{n} P_i(x_j) \right| > 0,$$

$$\tfrac{13}{4} n - n \mathcal{M}(\beta) > \sum_i a_i \log \left| \prod_{j=1}^{n} P_i(x_j) \right|,$$

$$\tfrac{13}{4} n - n \mathcal{M}(\beta) > \sum_i a_i \log |\mathrm{Norm}(P_i(\beta \bar\beta))|,$$

$$\tfrac{13}{4} n - n \mathcal{M}(\beta) > 0,$$

$$\tfrac{13}{4} > \mathcal{M}(\beta). \quad \blacksquare$$

4. If $\beta \in \mathbb{Q}(\zeta_N)$, then N or $N/2$ is squarefree

LEMMA 4.1. *Suppose $\beta \in \mathbb{Q}(\zeta_N)$ is an exception to Theorem* 1.3 *and is minimal in the sense of Definition* 1.8. *If p^2 divides N, then $p = 2$ and 4 exactly divides N.*

Suppose towards a contradiction that p^n exactly divides N, with $n \ge 2$ and $p^n \ne 4$. Write $\beta = \sum_{j=0}^{p-1} \zeta_{p^n}^{j} \eta_j$, with $\eta_j \in \mathbb{Q}(\zeta_{N/p})$. We refer to this as the *p-decomposition* of β. Let α_i be the X non-zero η_j. We know by Cassels [Cas69] that $\mathcal{M}(\beta) = \sum \mathcal{M}(\alpha_i)$, so by Lemma 3.1, $\sum \mathcal{M}(\alpha_i) < 13/4$. Moreover, X must be 2: indeed, $X = 1$ would mean N is not minimal, $X = 3$ would mean $\mathcal{N}(\beta) = 3$, and $X > 3$ would mean $\mathcal{M}(\beta) \ge 4$.

Let $\beta = \alpha + \zeta_{p^n} \gamma$, and assume without loss of generality that $\mathcal{M}(\alpha) \le \mathcal{M}(\gamma)$. Then $\mathcal{M}(\alpha) \le 13/8$, so $\mathcal{M}(\alpha) = 1$ or $3/2$.

4.1. $\mathcal{M}(\alpha) = 1$. Recall that $\mathcal{N}(\beta) > 3$, so $\mathcal{N}(\gamma) \ge 3$.

Assume without loss of generality (by multiplying β by a root of unity) that $\alpha = 1$. We know that $2 \le \mathcal{M}(\gamma) < 9/4$.

- First assume that $\overline{|\gamma|}^2 > 2$, then by [Cas69, corollary to Lemma 5], we have $\overline{|\gamma|}^2 \ge 3$. If $p \ge 3$, then by Lemma 2.5, $\overline{|\beta|}^2 \ge 4 + \sqrt{3}$.

In the case of 2^n, $n > 2$, write $\gamma = \gamma' + \zeta_{2^{n-1}} \gamma''$, with $\gamma', \gamma'' \in \mathbb{Q}(\zeta_{N/4})$. Since $\mathcal{M}(\gamma') + \mathcal{M}(\gamma'') = \mathcal{M}(\gamma) < 21/4$, either both γ' and γ'' are roots of

unity and β is 3 roots of unity, or one of γ' or γ'' is 0. The latter case implies $\beta \equiv 1 + \zeta_{2^n}^i (\gamma' + \gamma'')$, and by Lemma 2.5, $\overline{|\beta|}^2 \geq 4 + \sqrt{6}$.

• The other case is if $\mathscr{M}(\gamma) = \overline{|\gamma|}^2 = 2$. By [Cas69, Lemma 6], γ is equivalent to one of $(-1 + \sqrt{-7})/2 \equiv 1 + \zeta_7 + \zeta_7^3$ or $(\sqrt{5} + \sqrt{-3})/2 \equiv \zeta_3 - \zeta_5 - \zeta_5^{-1}$. We break down into cases as follows:

(a) $p^n = 3^2$ and $\gamma \equiv 1 + \zeta_7 + \zeta_7^3$. Then $\theta \leq 2\pi/9$ and $\overline{|\beta|}^2 > 5.1667$.

(b) $p^n = 3^2$ and $\gamma \equiv \zeta_3 - \zeta_5 - \zeta_5^{-1}$. Here, we have $\gamma = \zeta_m \cdot (\zeta_3^j - \zeta_5^k - \zeta_5^{-k})$, and so, after multiplying β by some root of unity, we may assume β is of the form $1 + \zeta_{3^2}^i \cdot \zeta_m^l \cdot (\zeta_3^j - \zeta_5^k - \zeta_5^{-k})$ for some values of i, j, k, l. If 2^4, 5^2, or any prime greater than 5 divides m, we may conjugate β by Lemma 2.5. We may also assume (by changing i) that 3 does not divide m. This limits m to eight possible values. We may conjugate ζ_m so that $l = 1$. There are then $384 = 2 \cdot 4 \cdot 6 \cdot 8$ possibilities for β. Computation reveals that all of these have $\overline{|\beta|}^2 > 5.094$.

(c) $p^n = 2^3$ and $\gamma \equiv \zeta_3 - \zeta_5 - \zeta_5^{-1}$ or $\gamma \equiv 1 + \zeta_7 + \zeta_7^3$. Then β is of the form $1 + \zeta_{2^3}^i \cdot \zeta_m^l \cdot \gamma'$ for some i, l, and γ' a conjugate of $\zeta_3 - \zeta_5 - \zeta_5^{-1}$ or $1 + \zeta_7 + \zeta_7^3$. Reasoning as above, m divides $3^2 \cdot 5 \cdot 7$. There are then 12 possible values for m. There are $672 = 4 \cdot 12 \cdot (8 + 6)$ possibilities for β. Computation reveals that all of these have $\overline{|\beta|}^2 > 5.0489$.

(d) In all other cases, $\theta \leq \pi/5$. Hence $\overline{|\beta|}^2 \geq 3 + 2\sqrt{2}\cos(\pi/5) \approx 5.28825$.

4.2. $\mathscr{M}(\alpha) = 3/2$. Note that $\mathscr{M}(\gamma) < 13/4 - 3/2 = 7/4$.

• $\mathscr{M}(\gamma) = 3/2$. Then α and γ are both equivalent to $1 + \zeta_5$. Let $\zeta_5 = e^{2\pi i/5}$. Then by conjugating and multiplication by a root of unity, assume without loss of generality that $\beta = (1 + \zeta_5) + \varrho(\zeta_5^i + \zeta_5^j)$ for some root of unity ϱ. If the difference between i and j (mod 5) is 2 or 3, then β is equivalent to $(\zeta_5 + \zeta_5^4) + \varrho'(\zeta_5^2 + \zeta_5^3)$. If $(i - j) \bmod 5$ is 1 or 4, then β is equivalent to $\alpha + \zeta_{p^n}\gamma$ with $|\alpha| = |\gamma| = (1 + \sqrt{5})/2$. Then by Lemma 2.5, regardless of p^n we have $\theta \leq \pi/4$, and $\overline{|\beta|}^2 \geq (2 + \sqrt{2})(3 + \sqrt{5})/2 \approx 8.93853$.

• $\mathscr{M}(\gamma) = 5/3$. Then α is equivalent to $1 + \zeta_5$, and γ is equivalent to $1 + \zeta_7$. Again by Lemma 2.5, regardless of p^n we have $\theta \leq \pi/4$, and $\overline{|\beta|}^2$ is even larger than in the preceding case.

5. If $\beta \in \mathbb{Q}(\zeta_N)$, then N divides 420

LEMMA 5.1. *If $\overline{|\beta|}^2 < 5.3$, then either β is on the list of Theorem 1.3, or $\beta \in \mathbb{Q}(\zeta_{420})$.*

First we establish some facts that we use throughout. Recall that X refers to the number of non-zero terms in the p-decomposition of β.

From [Cas69, (3.5)] and Lemma 3.1 we have

(5.1) $$p \geq 11 \implies X \leq (p-1)/2.$$

By (2.1), and since $\mathscr{M}(\beta) < 13/4$ by Lemma 3.1, we have

$$(5.2) \qquad \tfrac{13}{4}(p-1) > (p-X)\sum_{i=1}^{X}\mathscr{M}(\alpha_i) + \sum_{1 \le i < j \le X}\mathscr{M}(\alpha_i - \alpha_j).$$

Now let $\beta \in \mathbb{Q}(\zeta_N)$ be a minimal cyclotomic integer that is an exception to Theorem 1.3. Let p be the largest prime dividing N, and suppose $p > 7$. By Lemma 4.1, p exactly divides N. We proceed by considering different combinations of p and X.

5.1. $p = 11$. Note that by (5.1), $X \le 5$.

5.1.1. $X = 2$. By (5.2),

$$\tfrac{65}{2} > 9(\mathscr{M}(\gamma) + \mathscr{M}(\alpha)) + \mathscr{M}(\gamma - \alpha).$$

Assume without loss of generality that $\mathscr{M}(\alpha) \le \mathscr{M}(\gamma)$. We have

$$\mathscr{M}(\alpha) \le \tfrac{65}{36} \;\Rightarrow\; \mathscr{M}(\alpha) = 1, \tfrac{3}{2}, \tfrac{5}{3}, \tfrac{7}{4} \text{ or } \tfrac{9}{5}.$$

We consider each possible value of $\mathscr{M}(\alpha)$ below:

• $\mathscr{M}(\alpha) = 1$. As $\mathscr{N}(\beta) > 3$, $\mathscr{N}(\gamma) > 2$ and thus $\mathscr{M}(\gamma) \ge 2$. By conjugating we can assume $|\gamma| \ge \sqrt{2}$; then by Lemma 2.5 we have $\overline{|\beta|}^2 \ge 3 + 2\sqrt{2}\cos(2\pi/11) \approx 5.37942$.

• $\mathscr{M}(\alpha) = 3/2$. If $\mathscr{N}(\gamma) > 2$ the inequality is false, since $\mathscr{M}(\gamma - \alpha) \ge 1$ and $M(\gamma) \ge 2$. If $\mathscr{N}(\gamma) = 1$ then $\mathscr{N}(\beta) = 3$. So let γ be equivalent to $1 + \zeta_n$.

If $n = 5$ then $\alpha \equiv \gamma \equiv 1 + \zeta_5$. As we have previously argued, either $\beta \equiv (\zeta_5 + \zeta_5^4) + \varrho(\zeta_5^2 + \zeta_5^3)$ for some root of unity ϱ, or we can conjugate to assume that $|\alpha| = |\gamma| = (1 + \sqrt{5})/2$. Then $\overline{|\beta|}^2 \ge (3 + \sqrt{5})(1 + \cos(2\pi/11)) \approx 9.64093$.

If n is coprime to 5 then $n \ge 4$, and by Lemma 2.5 with $\theta = 2\pi/11$, $\overline{|1 + \zeta_5|} = (1 + \sqrt{5})/2$, and $\overline{|1 + \zeta_n|} \ge \sqrt{2}$, we have $\overline{|\beta|}^2 \ge 8.46802$.

If n is divisible by 5 it must be at least 10. Conjugate β so $|1 + \zeta_n| = \overline{|1 + \zeta_n|} \ge \overline{|1 + \zeta_{10}|} = \sqrt{(5 + \sqrt{5})/2}$. The smallest conjugate of $1 + \zeta_5$ is $(\sqrt{5} - 1)/2$. Thus by Lemma 2.5 with $\theta = 2\pi/11$, $\overline{|\beta|}^2 > 5.9779$.

• $\mathscr{M}(\alpha) = 5/3$. Again we have $\mathscr{N}(\gamma) = 2$. Let γ be equivalent to $1 + \zeta_n$.

If $n = 7$ then both α and γ are equivalent to $1 + \zeta_7$. We may conjugate them simultaneously so neither is the smallest conjugate as follows. Let ζ_7 be $e^{2\pi i/7}$. Assume without loss of generality that $\alpha = 1 + \zeta_7$, and $\gamma = \varrho(1 + \zeta_7^i)$ for ϱ a root of unity. Then $\beta = (1 + \zeta_7) + \zeta_{11}\varrho(1 + \zeta_7^i)$. If $i \ne 3, 4$ we are done, otherwise, β under the conjugation $\zeta_7 \to \zeta_7^2$ is $(1 + \zeta_7^2) + \zeta_{11}\varrho'(1 + \zeta_7^{2i})$, which satisfies our requirement. We now have $|\alpha|, |\gamma| \ge |e^{2\pi i 2/7}|$, and then by Lemma 2.5, $\overline{|\beta|}^2 > 6.09385$.

The case of n coprime to 7 easily follows from the previous case with $\mathscr{M}(\alpha) = 3/2$, since $\overline{|1 + \zeta_7|} > \overline{|1 + \zeta_5|}$.

If n is divisible by 7, then similarly to before, conjugate γ to its largest conjugate and then $|\gamma| = \overline{|\gamma|} \geq |e^{2\pi i/14}|$ and $|\alpha| \geq |e^{2\pi i 3/7}|$. We then have $\overline{|\beta|}^2 > 5.66523$.

- $\mathscr{M}(\alpha) = 9/5$. Then $\alpha \equiv 1 + \zeta_{11}$, but this is impossible as $\zeta_{11} \notin \mathbb{Q}(\zeta_{N/11})$.

- $\mathscr{M}(\alpha) = 7/4$. Then $\mathscr{M}(\gamma) = 7/4$ or $11/6$. However, $11/6$ makes the inequality false with $\mathscr{M}(\alpha - \gamma) \geq 1$, so $\mathscr{M}(\gamma) = 7/4$.

Recall that $\mathscr{M}(\rho) = 7/4 \Rightarrow \rho \equiv 1 + \zeta_{30}$. Conjugate α to $1 + e^{2\pi i/30}$. This will fix γ to be some other conjugate, of which the smallest is $1 + e^{2\pi i 13/30}$. By Lemma 2.5, $\overline{|\beta|}^2 > 5.71638$.

5.1.2. $X = 3$. By (5.2),

$$\tfrac{65}{2} > 8 \sum_{i=1}^{3} \mathscr{M}(\alpha_i) + \sum_{1 \leq i < j \leq 3} \mathscr{M}(\alpha_i - \alpha_j).$$

If more than one α_i is not a root of unity, the inequality is false. We may assume that not all three α_i are roots of unity, as the case $\mathscr{N}(\beta) = 3$ is done. Then notice that $\mathscr{N}(\alpha_i) > 2$ again makes the inequality false. So we may assume without loss of generality that $\mathscr{N}(\alpha_1) = \mathscr{N}(\alpha_2) = 1$, and $\mathscr{N}(\alpha_3) = 2$.

The respective $\mathscr{M}$-values are either $(1, 1, 3/2)$, $(1, 1, 5/3)$, or $(1, 1, 7/4)$.

We must calculate $\overline{|\beta|}$ with β of the form $1 + \zeta_{11}\zeta_{420}^i + \zeta_{11}^j\zeta_{420}^k(1 + \zeta_n)$ for all i, j, k where $n = 5, 7$, or 30. Some computation shows that the smallest such β is $1 + \zeta_{77} + \zeta_{77}^{11} + \zeta_{77}^{55}$ and $\overline{|\beta|} > 5.761$.

5.1.3. $X = 4$. By (5.2),

$$\tfrac{65}{2} > 7 \sum_{i=1}^{4} \mathscr{M}(\alpha_i) + \sum_{1 \leq i < j \leq 4} \mathscr{M}(\alpha_i - \alpha_j).$$

If any α_i is not a root of unity, this inequality is false.

Therefore each α_i is a root of unity and

$$\tfrac{9}{2} > \sum_{1 \leq i < j \leq 4} \mathscr{M}(\alpha_i - \alpha_j),$$

which implies there are at most two distinct roots of unity.

There remain three cases after conjugation, with $(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$ equivalent to one of the following, for ζ some root of unity:

$$(1, 1, \zeta, \zeta) \quad \text{or} \quad (1, 1, 1, \zeta) \quad \text{or} \quad (1, 1, 1, 1).$$

In both cases with ζ, we must have $\mathscr{M}(1 - \zeta) = 1$ or else the inequality is false. Thus $\zeta = \zeta_6$.

The only such β with $\overline{|\beta|}^2 < 6$ of the above form are given below:

$(\alpha_1, \alpha_2, \alpha_3, \alpha_4)$	β	$\overline{|\beta|}$
$(1,1,1,1)$	$1 + \zeta_{11} + \zeta_{11}^2 + \zeta_{11}^5$	$\sqrt{1 + 4\cos^2(\pi/11)}$
$(1,1,1,\zeta_6)$	$\zeta_6 + \zeta_{11} + \zeta_{11}^3 + \zeta_{11}^8$	$\sqrt{1 + 4\cos^2(\pi/33)}$
$(1,1,\zeta_6,\zeta_6)$	$\zeta_6 + \zeta_6\zeta_{11} + \zeta_{11}^3 + \zeta_{11}^9$	$\sqrt{1 + 4\cos^2(\pi/22)}$

5.1.4. $X = 5$. By (5.2),

$$\tfrac{65}{2} > 6\sum_{i=1}^{5} \mathscr{M}(\alpha_i) + \sum_{1 \le i < j \le 5} \mathscr{M}(\alpha_i - \alpha_j).$$

If any α_i is not a root of unity it has $\mathscr{M}(\alpha_i) \ge 3/2$ and this inequality is false. So all α_i are roots of unity, and

$$\tfrac{5}{2} > \sum_{1 \le i < j \le 5} \mathscr{M}(\alpha_i - \alpha_j).$$

However, if there exists $\alpha_i \ne \alpha_j$ then the above inequality is also false, so we may assume without loss of generality that $\alpha_i = 1$ for all i.

One can compute every

$$\beta = 1 + \zeta_{11} + \zeta_{11}^a + \zeta_{11}^b + \zeta_{11}^c$$

with a, b, c distinct and not equal to 0 or 1, and with $\overline{|\beta|} < \sqrt{5} + .1$. They are all equivalent to

$$1 + \zeta_{11} + \zeta_{11}^2 + \zeta_{11}^4 + \zeta_{11}^7,$$

which has

$$\overline{|\beta|} = 2\cos(\pi/6) = \sqrt{1 + 4\cos^2(\pi/4)}.$$

5.2. $X = 2$. Let $\beta = \alpha + \zeta_p\gamma$, with $\alpha, \gamma \in \mathbb{Q}(\zeta_{N/p})$ and $p \ge 13$. By (5.2),

$$\tfrac{13}{4}(p - 1) > (p - 2)(\mathscr{M}(\alpha) + \mathscr{M}(\gamma)) + \mathscr{M}(\alpha - \gamma),$$

$$\frac{13}{4} \cdot \frac{p-1}{p-2} > \mathscr{M}(\alpha) + \mathscr{M}(\gamma) + \frac{\mathscr{M}(\alpha - \gamma)}{p - 2},$$

$$\tfrac{39}{11} > \mathscr{M}(\alpha) + \mathscr{M}(\gamma).$$

From here, the reasoning follows almost exactly as in Section 5.1.1. As $p > 11$, any argument based on Lemma 2.5 is still valid, as θ will be smaller. There are two cases where we need to change the argument: $1 + \zeta_{11}$ can appear, and the difference term $\mathscr{M}(\alpha - \gamma)$ may be larger.

We can still assume $\mathscr{M}(\alpha) \ne 9/5$, now because $\frac{1}{2} \cdot 39/11 < 9/5$.

In the $\mathscr{M}(\alpha) = 7/4$ case, $\mathscr{M}(\gamma) = 11/6$ or $9/5$ is still not possible: now by the restriction on $\mathscr{M}(\alpha) + \mathscr{M}(\gamma)$ instead of the other reasons.

5.3. $p = 13$

5.3.1. $X = 3$. By (5.2),

$$39 > 10 \sum \mathscr{M}(\alpha_i) + \sum \mathscr{M}(\alpha_i - \alpha_j).$$

We may assume that the $\mathscr{N}$-values $(\mathscr{N}(\alpha_1), \mathscr{N}(\alpha_2), \mathscr{N}(\alpha_3))$ are $(1, 1, 2)$. If they are less, then $\mathscr{N}(\beta) = 3$, and if they are more, the inequality is false.

The $\mathscr{M}$-values must be $(1, 1, 3/2)$ or $(1, 1, 5/3)$ for the inequality to hold.

- $(1, 1, 3/2)$. We have $\sum \mathscr{M}(\alpha_i - \alpha_j) < 4$. Neither $\mathscr{N}(\alpha_3 - \alpha_1) = 3$ nor $\mathscr{N}(\alpha_3 - \alpha_2) = 3$. If so, then either $\alpha_2 - \alpha_1 = 0$ and $0 + 2 + 2 \geq 4$, or $\mathscr{N}(\alpha_2 - \alpha_1) = 1$ and $1 + 1 + 2 \geq 4$.

Assume without loss of generality that $\alpha_1 = 1$. Because $\mathscr{N}(\alpha_3 - \alpha_1) \leq 2$, there is some cancellation occurring in the difference $\alpha_3 - \alpha_1$. In particular, α_3 must be equal to $1 + \zeta_5$, $\zeta_5 + \zeta_5^i$, or $\zeta_6 + \zeta_6\zeta_5$. We divide into cases based on $\mathscr{N}(\alpha_3 - \alpha_1)$, and employ a result of Mann [Man65] (see also Poonen and Rubinstein [PR98]). For small n, he classified vanishing sums of n roots of unity. For $n < 6$, these must be sums of groups consisting of equally spaced roots of unity.

If $\mathscr{N}(\alpha_3 - \alpha_1) = 0$, then we have a vanishing sum of three roots of unity, which is impossible when two of them differ by a fifth root of unity.

If $\mathscr{N}(\alpha_3 - \alpha_1) = 1$, then we have a vanishing sum of four roots of unity, and by Poonen, it must consist of two groups of two roots of unity each of whose sum vanishes. Hence, $\alpha_3 = 1 + \zeta_5$.

If $\mathscr{N}(\alpha_3 - \alpha_1) = 2$, then we have a vanishing sum of five roots of unity, and by Poonen, it must be a primitive vanishing sum of five roots of unity, or is two vanishing sums, one of two roots of unity and one of three roots of unity. If we are in the five case and $\alpha_3 = \zeta_5 + \zeta_5^i$ or we are in the 2–3 case and $\alpha_3 = \zeta_6 + \zeta_6\zeta_5$.

So, we may assume without loss of generality that $(\alpha_1, \alpha_2, \alpha_3)$ is one of the following: $(1, \zeta_5, \zeta_5^i + \zeta_5^j)$, $(1, \zeta_5, \zeta_6 + \zeta_5^i\zeta_6^j)$, or $(1, \zeta_6, \zeta_6^i + \zeta_5\zeta_6^j)$ for some i, j.

We compute the house of all β with restrictions from above, and in all cases, $\overline{|\beta|}^2 > 5.66$.

- $(1, 1, 5/3)$. We have $\sum \mathscr{M}(\alpha_i - \alpha_j) < 7/3$. Since $\alpha_1 = \alpha_2$, and $\alpha_3 - \alpha_1$ is a root of unity, we may assume that $\alpha_1 = \alpha_2 = 1$ and $\alpha_3 = 1 + \zeta_7$. The smallest such β is $1 + \zeta_{13} + \zeta_{13}^2(1 + \zeta_5)$ with $\overline{|\beta|}^2 > 10$.

5.3.2. $X = 4$. We proceed as in Section 5.1.4. By (5.2),

$$39 > 9 \sum_{i=1}^{4} \mathscr{M}(\alpha_i)$$

implies that α_i are all roots of unity, and

$$3 > \sum_{1 \leq i < j \leq 4} \mathscr{M}(\alpha_i - \alpha_j)$$

implies that they are all the same root of unity. Thus $\beta \in \mathbb{Q}(\zeta_{13})$ is a sum of four roots of unity.

One can verify that the only such β with $\overline{|\beta|} < \sqrt{5} + .1$ is

$$\beta = 1 + \zeta_{13} + \zeta_{13}^3 + \zeta_{13}^9,$$

with

$$\overline{|\beta|} = 2\cos(\pi/6) = \sqrt{1 + 4\cos^2(\pi/4)}.$$

5.3.3. $X \geq 5$. By (5.1), $p = 13$ implies that $X \leq 6$. Now (5.2) gives us $\frac{13}{4} \cdot 12 > (13 - X)X$, which is false for $X = 5, 6$.

5.4. $X = 3$

5.4.1. $p = 17$. By (5.2),

$$52 > 14 \sum \mathscr{M}(\alpha_j) + \sum \mathscr{M}(\alpha_i - \alpha_j).$$

So we may assume without loss of generality that α_1 and α_2 are both roots of unity. Also, assume α_3 is not a root of unity, since this case has been done already. We may conclude that $\mathscr{M}(\alpha_3) = 3/2$, otherwise the inequality is false.

Now,

$$3 > \mathscr{M}(\alpha_1 - \alpha_2) + \mathscr{M}(\alpha_1 - \alpha_3) + \mathscr{M}(\alpha_2 - \alpha_3).$$

For this to hold, we must have $\alpha_1 = \alpha_2$ and $\alpha_3 - \alpha_1$ a root of unity. We may assume without loss of generality that $(\alpha_1, \alpha_2, \alpha_3) = (1, 1, 1 + \zeta_5)$, and then that β is equivalent to

$$\beta = 1 + \zeta_{17} + \zeta_{17}^j(1 + \zeta_5)$$

for some j. One can verify that the smallest such β is $1 + \zeta_{17} + \zeta_{17}^5(1 + \zeta_5)$ with $\overline{|\beta|}^2 > 9$.

5.4.2. $p = 19$. By (5.2),

$$\tfrac{117}{2} > 16 \sum \mathscr{M}(\alpha_i) + \sum \mathscr{M}(\alpha_i - \alpha_j).$$

As in the previous section, $(\mathscr{M}(\alpha_1), \mathscr{M}(\alpha_2), \mathscr{M}(\alpha_3)) = (1, 1, 3/2)$. Then

$$\tfrac{5}{2} > \mathscr{M}(\alpha_1 - \alpha_2) + \mathscr{M}(\alpha_1 - \alpha_3) + \mathscr{M}(\alpha_2 - \alpha_3)$$

and we may assume without loss of generality that $(\alpha_1, \alpha_2, \alpha_3) = (1, 1, 1 + \zeta_5)$. Then β is equivalent to

$$\beta = 1 + \zeta_{19} + \zeta_{19}^j(1 + \zeta_5)$$

for some j. One can verify that the smallest such β is $1 + \zeta_{19} + \zeta_{19}^5(1 + \zeta_5)$ with $\overline{|\beta|}^2 > 10$.

5.4.3. $p \geq 23$. In this case, all α_i must be roots of unity. Otherwise, this contradicts (5.2). Thus $\mathscr{N}(\beta) = 3$ and there are no exceptions to Theorem 1.3.

5.5. $X \geq 4$ **and** $p \geq 17$. By (5.2),

$$\tfrac{13}{4}(p-1) > (p-X)X,$$

and by (5.1), $X \leq (p-1)/2$. We have

$$\frac{d}{dX}((p-X)X) = p - 2X,$$

so for $x < p/2$, $pX - X^2$ increases with X. Thus the minimal value for $(p-X)X$ in the region is at $X = 4$, but

$$\tfrac{13}{4}(p-1) > (p-4)4$$

is false for $p \geq 17$. Hence (5.2) is false when $X \geq 4$ and $p \geq 17$.

6. There are no exceptions in $\mathbb{Q}(\zeta_{420})$

LEMMA 6.1. *Theorem 1.3 holds for* $\beta \in \mathbb{Q}(\zeta_{420})$.

We have computed all $\beta \in \mathbb{Q}(\zeta_{420})$ with $\mathscr{N}(\beta) \leq 6$ as follows: without loss of generality we assume that the first root is 1, the second root ζ_{420}^i has i dividing 420 (or equal to 0), and the other roots ζ_{420}^j have $(420, j) \geq i$. The results were consistent with Theorem 1.2, and all β with $5 < \overline{|\beta|}^2 \leq 5 + 1/25$ are equivalent to $1 + \zeta_{70} + \zeta_{70}^{10} + \zeta_{70}^{29}$, as mentioned in Theorem 1.3. Thus we know that any exceptions β must have $\mathscr{N}(\beta) > 6$.

Write β as $\sum_{i=0}^{4} \zeta_5^i \eta_i$ with $\eta_i \in \mathbb{Q}(\zeta_{84})$. Let X be the minimal number of non-zero η_i that can represent β in this way, and let α_i be these non-zero η_i.

In the cases below we make use of several facts about $\alpha \in \mathbb{Q}(\zeta_{84})$:

- If $\mathscr{N}(\alpha) = 2$, then $\mathscr{M}(\alpha) \geq 5/3$, as $1 + \zeta_5$ cannot appear.
- If $\mathscr{N}(\alpha) = 4$, then $\mathscr{M}(\alpha) \geq 5/2$, by [CMS11, 7.0.8].
- If $\mathscr{N}(\alpha) \geq 5$, then $\mathscr{M}(\alpha) \geq 17/6$, by [CMS11, 7.0.8].

In each of the following cases, we demonstrate a contradiction to (5.2), which now reads

$$13 > (5-X)\sum_{i=1}^{X} \mathscr{M}(\alpha_i) + \sum_{1 \leq i < j \leq X} \mathscr{M}(\alpha_i - \alpha_j) = S.$$

6.1. $X = 1$. In this case, $\beta \in \mathbb{Q}(\zeta_{84})$. We can write $\beta = \alpha + \zeta_4\gamma$ with $\alpha, \gamma \in \mathbb{Q}(\zeta_{21})$. We know that $\mathscr{M}(\alpha) + \mathscr{M}(\gamma) < 13/4$, so we may assume without loss of generality that $\mathscr{M}(\alpha) \leq 13/8$. Then α is a root of unity. But then $\mathscr{M}(\gamma) < 9/4$ and $\mathscr{N}(\gamma) \geq 6$, a contradiction by [CMS11, 7.0.5].

6.2. $X = 2$. $\mathscr{M}(\alpha_i) \geq 23/6$ contradicts (5.2). So by [CMS11, 7.0.9], $\mathscr{N}(\alpha_i) \leq 5$.

In the following table and throughout we list lower bounds on the values of $\mathscr{M}$ and S. In all cases, $S \geq 13$, contradicting (5.2).

$\mathscr{N}(\alpha_i)$	$\mathscr{M}(\alpha_i)$			$\mathscr{M}(\alpha_1 - \alpha_2)$	S
≥ 2	5	$5/3$	$17/6$	2	$15 1/2$
≥ 3	4	2	$5/2$	1	$14 1/2$

6.3. $X = 3$. The column $\mathscr{M}(\alpha_i - \alpha_j)$ is listed in the order $\alpha_1 - \alpha_2$, $\alpha_1 - \alpha_3$, $\alpha_2 - \alpha_3$.

$\mathscr{N}(\alpha_i)$			$\mathscr{M}(\alpha_i)$			$\mathscr{M}(\alpha_i - \alpha_j)$			S
1	1	≥ 5	1	1	$17/6$	0	2	2	$13 2/3$
1	2	≥ 4	1	$5/3$	$5/2$	1	2	$5/3$	15
1	≥ 3	≥ 3	1	2	2	$5/3$	$5/3$	0	$13 1/3$
2	2	3	$5/3$	$5/3$	2	0	1	1	$12 2/3^{*}$
2	2	≥ 4	$5/3$	$5/3$	$5/2$	0	$5/3$	$5/3$	15
2	≥ 3	≥ 3	$5/3$	2	2	1	1	0	$13 1/3$
≥ 3	≥ 3	≥ 3	2	2	2	1^{**}	0	0	13

 * See that $\mathscr{M}(\alpha_1 - \alpha_2) = 0$ and $\mathscr{M}(\alpha_3 - \alpha_1) = 1$, or else $S > 13$. But then β can be written as a sum of five roots of unity: take $\eta_i' = \eta_i - \alpha_1$.
 ** This results from assuming at least one pair is different. If all α_i are equal, then β can be represented with $X = 2$ by taking $\eta_j' = \eta_j - \alpha_1$.

6.4. $X = 4$. No two α_i are equal. If $\alpha_j = \alpha_k$, then there is another representation with $X < 4$ given by $\eta_i' = \eta_i - \alpha_j$ for all i.

The column $\mathscr{M}(\alpha_i - \alpha_j)$ is listed in the order $\alpha_1 - \alpha_2$, $\alpha_1 - \alpha_3$, $\alpha_1 - \alpha_4$, $\alpha_2 - \alpha_3$, $\alpha_2 - \alpha_4$, $\alpha_3 - \alpha_4$.

$\mathscr{N}(\alpha_i)$				$\mathscr{M}(\alpha_i)$				$\mathscr{M}(\alpha_i - \alpha_j)$						S
1	1	1	≥ 4	1	1	1	$5/2$	1	1	2	1	2	2	$14 1/2$
1	1	2	≥ 3	1	1	$5/3$	2	1	1	$5/3$	1	$5/3$	1	13
1	1	≥ 3	≥ 3	1	1	2	2	1	$5/3$	$5/3$	$5/3$	$5/3$	1	$14 2/3$
1	2	2	2	1	$5/3$	$5/3$	$5/3$	1	1	1	1	1	1	$12^{\dagger}$
1	≥ 2	≥ 2	≥ 3	1	$5/3$	$5/3$	2	1	1	$5/3$	1	1	1	13
2	2	2	2	$5/3$	$5/3$	$5/3$	$5/3$	$5/3^{\dagger\dagger}$	1	1	1	1	1	$13 1/3$
≥ 2	≥ 2	≥ 2	≥ 3	$5/3$	$5/3$	$5/3$	2	1	1	1	1	1	1	13

 † If any of the differences is more than a single root of unity, it increases S by at least 2/3, so at most one difference is more than a single root of unity. Thus we may assume without loss of generality that $\mathscr{M}(\alpha_2 - \alpha_1) = \mathscr{M}(\alpha_3 - \alpha_1) = 1$. Then $\mathscr{N}(\beta) \leq 6$, as evidenced by $\eta_i' = \eta_i - \alpha_1$ for all i.
 †† If every difference is a single root of unity, then $\mathscr{N}(\beta) = 5$: put $\eta_i' = \eta_i - \alpha_1$ for all i.

6.5. $X = 5$. This is not minimal, there is always a representation with $X < p$: put $\eta_i' = \eta_i - \alpha_1$ for all i.

References

[AH99]   M. Asaeda and U. Haagerup, *Exotic subfactors of finite depth with Jones indices* $(5 + \sqrt{13})/2$ *and* $(5 + \sqrt{17})/2$, Comm. Math. Phys. 202 (1999), 1–63.

[CMS11]   F. Calegari, S. Morrison, and N. Snyder, *Cyclotomic integers, fusion categories, and subfactors*, Comm. Math. Phys. 303 (2011), 845–896.

[Cas69]   J. W. S. Cassels, *On a conjecture of R. M. Robinson about sums of roots of unity*, J. Reine Angew. Math. 238 (1969), 112–131.

[IJMS]   M. Izumi, V. F. R. Jones, S. Morrison, and N. Snyder, *Subfactors of index less than 5, part 3: quadruple points*, Comm. Math. Phys.

[Jon68]   A. J. Jones, *Sums of three roots of unity*, Proc. Cambridge Philos. Soc. 64 (1968), 673–682.

[Jon69]   A. J. Jones, *Sums of three roots of unity. II*, Proc. Cambridge Philos. Soc. 66 (1969), 43–59.

[Jon83]   V. F. R. Jones, *Index for subfactors*, Invent. Math. 72 (1983), 1–25.

[Kro37]   L. Kronecker, *Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten*, J. Reine Angew. Math. 53 (1857), 173–175.

[Lox72]   J. H. Loxton, *On the maximum modulus of cyclotomic integers*, Acta Arith. 22 (1972), 69–85.

[Man65]   H. B. Mann, *On linear relations between roots of unity*, Math. 12 (1965), 107–117.

[PR98]   B. Poonen and M. Rubinstein, *The number of intersection points made by the diagonals of a regular polygon*, SIAM J. Discrete Math. 11 (1998), 135–156.

[Rob65]   R. M. Robinson, *Some conjectures about cyclotomic integers*, Math. Comp. 19 (1965), 210–217.

[Sch66]   A. Schinzel, *On sums of roots of unity. Solution of two problems of R. M. Robinson*, Acta Arith. 11 (1966), 419–432.

Frederick Robinson
Department of Mathematics, UCLA
Box 951555 Los Angeles, CA, U.S.A.
E-mail: frobinson@math.ucla.edu

Michael Wurtz
Microsoft Corporation
1 Microsoft Way miwurtz 36/3511
Redmond, WA 98052, U.S.A.
E-mail: miwurtz@microsoft.com