Commun. Math. Phys.
Digital Object Identifier (DOI) 10.1007/s00220-010-1136-2

Communications in
Mathematical Physics

Cyclotomic Integers, Fusion Categories, and Subfactors

Frank Calegari[1], **Scott Morrison**[2], **Noah Snyder**[3]

[1] Department of Mathematics, Northwestern University, Evanston, IL, 60208-2730, USA
[2] Department of Mathematics, University of California, Berkeley, CA 94720-3840, USA
[3] Department of Mathematics, Columbia University, New York, NY 10027, USA.
E-mail: nsnyder@math.columbia.edu

Received: 3 May 2010 / Accepted: 31 May 2010

Abstract: Dimensions of objects in fusion categories are cyclotomic integers, hence number theoretic results have implications in the study of fusion categories and finite depth subfactors. We give two such applications. The first application is determining a complete list of numbers in the interval $(2, 76/33)$ which can occur as the Frobenius-Perron dimension of an object in a fusion category. The smallest number on this list is realized in a new fusion category which is constructed in the Appendix written by V. Ostrik, while the others are all realized by known examples. The second application proves that in any family of graphs obtained by adding a 2-valent tree to a fixed graph, either only finitely many graphs are principal graphs of subfactors or the family consists of the A_n or D_n Dynkin diagrams. This result is effective, and we apply it to several families arising in the classification of subfactors of index less than 5.

1. Introduction

Let C be a fusion category and f any ring map from the Grothendieck ring $K(C)$ to $\mathbf{C}$. If X is an object in C, then Etingof–Nikshych–Ostrik proved in [13] that $f([X])$ is a cyclotomic integer. This result allows for applications of algebraic number theory to fusion categories and subfactors. The first such application was given by Asaeda and Yasuda [1,3] who excluded a certain infinite family of graphs as possible principal graphs of subfactors. We prove two main results, one a classification of small Frobenius–Perron dimensions of objects in fusion categories, and the other a generalization of Asaeda–Yasuda's result to arbitrary families of the same form.

Theorem 1.0.1. *Let X be an object in a fusion category whose Frobenius–Perron dimension satisfying $2 < FP(X) \leq 76/33 = 2.303030\ldots$ then $FP(X)$ is equal to one of the following algebraic integers*:

Published online: 26 September 2010

$$\begin{aligned}
\frac{\sqrt{7}+\sqrt{3}}{2} &= 2.188901059\ldots,\\
\sqrt{5} &= 2.236067977\ldots,\\
1+2\cos(2\pi/7) &= 2.246979603\ldots,\\
\frac{1+\sqrt{5}}{\sqrt{2}} &= 2\cos(\pi/20)+2\cos(9\pi/20) = 2.288245611\ldots,\\
\frac{1+\sqrt{13}}{2} &= 2.302775637\ldots.
\end{aligned}$$

Remark 1.0.2. Each of the numbers in Theorem 1.0.1 can be realized as the Frobenius–Perron dimension of an object in a fusion category. See §3.1 and Appendix A (written by Ostrik).

Theorem 1.0.3. *Let Γ be a connected graph with $|\Gamma|$ vertices. Fix a vertex v of Γ, and let Γ_n denote the sequence of graphs obtained by adding a 2-valent tree of length $n-|\Gamma|$ to Γ at v (see Fig. 1). For any fixed Γ, there exists an effective constant N such that for all $n \geq N$, either*:

(1) Γ_n is the Dynkin diagram A_n or D_n.
(2) Γ_n is not the principal graph of a subfactor.

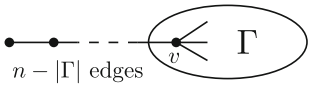

Fig. 1. The family of graphs Γ_n

Remark 1.0.4. The main theorem of Asaeda–Yasuda [3] is the particular case where Γ is the Dynkin diagram A_7 and v is the central vertex. See Example 10.1.9 to see our results applied to this case and two others arising in the classification of subfactors of small index.

Perhaps surprisingly, both Theorem 1.0.1 and Theorem 1.0.3 can be deduced purely from arithmetic considerations.

The first main result follows immediately from the following theorem.

Theorem 1.0.5. *Let $\beta \in \mathbf{Q}(\zeta)$ be a real algebraic integer in some cyclotomic extension of the rationals. Let $\boxed{\beta}$ denote the largest absolute value of all conjugates of β. If $\boxed{\beta} \leq 2$ then $\boxed{\beta} = 2\cos(\pi/n)$ for some integer n. If $2 < \boxed{\beta} < 76/33$, then $\boxed{\beta}$ is one of the five numbers occurring in Theorem 1.0.1.*

The second main result is a consequence of the following theorem, combined with the fact that the even part of a finite depth subfactor is a fusion category.

Theorem 1.0.6. *For any Γ, there exists an effective constant N such that for all $n \geq N$, either*:

(1) All the eigenvalues of the adjacency matrix M_n are of the form $\zeta + \zeta^{-1}$ for some root of unity ζ, and the graphs Γ_n are the Dynkin diagrams A_n or D_n.

(2) The largest eigenvalue λ of the adjacency matrix M_n is greater than 2, and the field $\mathbf{Q}(\lambda^2)$ is not abelian.

Although Theorem 1.0.6 is, in principle, effective, it is difficult to apply in practice. We also give a logically weaker but more effective version of Theorem 1.0.6 which is sufficient to prove Theorem 1.0.3 and is practical for many examples.

We briefly summarize the main ideas in the proofs of these arithmetic theorems. A key idea of Cassels [7] is to study elements with small normalized trace $\mathscr{M}(\beta) = \frac{1}{\deg \beta}\mathrm{Tr}(\beta \cdot \overline{\beta}) \in \mathbf{Q}$ rather than work directly with bounds on $\boxed{\beta}$. A key principle, made rigorous by Loxton [25], says that if β is a cyclotomic integer and $\mathscr{M}(\beta)$ is small, then β can be written as a sum of a small number of roots of unity. This principle was first applied by Cassels to study cyclotomic integers of small norm [7]. In fact, Theorem 1.0.5 (at least for $\boxed{\beta} \leq \sqrt{5}$) is a consequence of the main theorem of Cassels *with finitely many exceptions*.

A careful study of Cassels' analysis shows that any exceptions must lie in the field $\mathbf{Q}(\zeta_N)$ with

$$\begin{aligned} N &= 4692838820715366441120 \\ &= 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 47 \cdot 53. \end{aligned}$$

Given that the problem of finding small vectors inside a lattice (say, of algebraic integers) is NP-complete, this is not immediately useful. We improve on Cassels argument in three main ways. First, we show that $\boxed{\beta} < 76/33$ implies that $\mathscr{M}(\beta) < 23/6$ (which improves substantially on the obvious bound of $(76/33)^2$). Second, we systematically exploit the condition that β is real (an assumption that Cassels did not make). In particular, we adapt techniques of A. J. Jones [20] and Conway and A. J. Jones [8] for classifying small sums of three roots of unity to understand *real* sums of five roots of unity. Finally, we engage in a detailed case-by-case analysis to complete the argument and remove all exceptions.

We now sketch the ideas of the proof of Theorem 1.0.6. Let λ_n be the Frobenius-Perron eigenvalue of the graph Γ_n. The average $\frac{1}{n}\sum_{\mu} |\mu^2 - 2|^2$ over all eigenvalues μ of the adjacency matrix of Γ_n can be shown to converge to 2 as n increases without bound. Since all Galois conjugates of λ_n are eigenvalues of the adjacency matrix, this suggests that $\mathscr{M}(\lambda_n^2 - 2)$ should also be small. By the Cassels-Loxton principle, if λ_n^2 is cyclotomic, one would expect that $\lambda_n^2 - 2$ should be a sum of a small number of roots of unity. Explicitly, we deduce for all n greater than some explicit bound (depending on Γ) that either λ_n^2 is *not* cyclotomic or $\lambda_n^2 - 2$ is the sum of at most two roots of unity. The latter case can only occur if $|\lambda_n| \leq 2$, in which case the characteristic polynomial of Γ_n is a Chebyshev polynomial, and Γ_n is necessarily an extended Dynkin diagram. In order to make this argument rigorous, one needs to understand the relationship between all eigenvalues and the subset of eigenvalues conjugate to λ_n. We do this in two different ways. First, we use the result of Etingof-Nikshych-Ostrik to show that all non-repeating eigenvalues are cyclotomic integers. In light of this result, we need only control the repeated eigenvalues and the eigenvalues of the form $\zeta + \zeta^{-1}$ for roots of unity ζ. This can be done using techniques of Gross-Hironaka-McMullen [15]. To finish the argument, we use a much easier version of Theorem 1.0.5 to get a contradiction. For the second proof, we use some height inequalities to show that the degree of λ_n grows linearly in n. Again this is enough to get a bound on $\mathscr{M}(\lambda_n^2 - 2)$, as well as bounds on $\mathscr{M}(P(\lambda_n^2))$ for other polynomials in λ_n^2. The desired contradiction then follows from Loxton's result applied to a particular polynomial in λ_n^2.

Remark 1.0.7. The methods used in our proof of Theorem 1.0.1 can certainly be extended further than 76/33, at the cost of a certain amount of combinatorial explosion. However, there do exist limit points of the set of possible $\boxed{\beta}$, including at $2\sqrt{2} = \varinjlim 2\sqrt{2}\cos(\pi/n)$ and $3 = \varinjlim 1 + 2\cos(2\pi/n)$. The best general "sparseness" result we have is Theorem 9.1.1 which states that the set of values of $\mathscr{M}(\beta)$ for β a cyclotomic integer is a closed subset of $\mathbf{Q}$.

Theorem 1.0.1 is similar in spirit to Haagerup's classification of all subfactors of index less than $3 + \sqrt{3} = 4.73205...$ [16]. In fact, a version of Theorem 1.0.1 follows from Haagerup's classification, for example, "if X is an object in a *unitary* tensor category with duals then the dimension of X does not lie in the interval $(2, \sqrt{\frac{5+\sqrt{13}}{2}}) = (2, 2.074313\ldots)$." Our result is weaker in that we assume finiteness, but stronger in that it does not assume unitarity and applies to larger dimensions.

In the other direction, one might wonder if purely arithmetic considerations have implications for finite depth subfactors of small index larger than 4. Indeed, using only arithmetic we can prove the following result.

Theorem 1.0.8. *Suppose that* $4 < \alpha < 4 + 10/33 = 4.303030\ldots$ *is the index of a finite depth subfactor. Then either* $\alpha = 3 + 2\cos(2\pi/7)$, *or* $\alpha = \frac{5+\sqrt{13}}{2}$.

1.1. Detailed summary. The proof of Theorem 1.0.5 proceeds in several steps. We first prove the theorem for those β which can be written as the sum of at most 5 roots of unity (Theorem 4.2.10). This argument requires some preliminary analysis of vanishing sums of roots of unity, which we undertake in §4. Having done this, we prove Theorem 5.0.13, which shows that any exception to Theorem 1.0.5 lies in $\mathbf{Q}(\zeta_N)$ with $N = 420$. A useful technical tool is provided by Lemma 5.1.1, which allows us to reduce our search to β satisfying $\mathscr{M}(\beta) < 23/6$ rather than $\mathscr{M}(\beta) < 5$ as in Cassels. In Lemma 7.0.8 and Corollary 7.0.10, we prove Theorem 1.0.5 for $\beta \in \mathbf{Q}(\zeta_{84})$. In §8 we make the final step of showing that any counterexample $\beta \in \mathbf{Q}(\zeta_{420})$ must actually lie in $\mathbf{Q}(\zeta_{84})$. There is a certain amount of combinatorial explosion in this section which we control as much as possible with various tricks. Although our paper is written to be independent, it would probably be useful to the reader to consult A. J. Jones [20] when reading §4.2, and Cassels [7] when reading §§5.2–8.

In §9, we prove an easier version of Theorem 1.0.5 which will be used to prove the effective version of Theorem 1.0.3. In this section, we also prove that the values of $\mathscr{M}(\beta)$ for β a cyclotomic integer are a closed subset of $\mathbf{Q}$. We then prove an effective version of Theorem 1.0.3 in §10 and give applications to several families which appear in the classification of small index subfactors. In §11, we prove Theorem 1.0.6 which is logically stronger but less effective than the result in the previous section. A reader mainly interested in the applications to subfactors may wish to skip directly to §10 & §11.

2. Definitions and Preliminaries

If N is an integer, let ζ_N denote $\exp(2\pi i/N)$. Having fixed this choice for all N, there is no ambiguity when writing expressions such as $\zeta_{12} + \zeta_{20}$—*a priori*, such an expression is not even well defined up to conjugation.

Suppose that $\mathbf{Q}(\beta)$ is an abelian extension. By the Kronecker–Weber theorem, β is contained inside some minimal cyclotomic field $\mathbf{Q}(\zeta_N)$. (N is the *conductor* of $\mathbf{Q}(\beta)$.) If $\beta \in \mathbf{Q}(\zeta_N)$ is an algebraic integer, we shall consider several invariants attached to β:

Definition 2.0.1. *For a cyclotomic integer β, we denote by $\mathcal{N}(\beta)$ the size of the smallest set S such that $\beta = \sum_S \xi_i$ for ξ_i a root of unity.*

Definition 2.0.2. *If β is any algebraic integer, we let $\boxed{\beta}$ denote the maximum of the absolute values of all the conjugates of β, and let $\mathcal{M}(\beta)$ denote the average value of the real numbers $|\sigma\beta|^2$, where $\sigma\beta$ runs over all conjugates of β.*

Remark 2.0.3. If $\beta \in K$, where K is Galois and $G = \mathrm{Gal}(K/\mathbf{Q})$, then $\mathcal{M}(\beta)$ is well behaved whenever complex conjugation is central in G, since then $|\sigma\beta|^2 = \sigma|\beta|^2$, and $[K : \mathbf{Q}]\mathcal{M}(\beta) = \mathrm{Tr}(|\beta^2|)$. This is the case, for example, whenever K is totally real or abelian. In particular, in these cases, $\mathcal{M}(\beta) \in \mathbf{Q}$.

There are inequalities $\mathcal{N}(\beta) \geq \boxed{\beta}$, which follows from the triangle inequality, and $\boxed{\beta}^2 \geq \mathcal{M}(\beta) \geq |N_{K/\mathbf{Q}}(\beta)|^{1/[K:\mathbf{Q}]}$, which is ≥ 1 if β is non-zero. Note that $\boxed{\alpha+\beta} \neq \boxed{\alpha}+\boxed{\beta}$ in general.

Example 2.0.4. Suppose that β is a totally real algebraic integer and that $\boxed{\beta} \leq 2$. If $\alpha + \alpha^{-1} = \beta$, then all the conjugates of α have absolute value 1. A theorem of Kronecker [24] implies that α is a root of unity, and then an easy computation shows that $\boxed{\beta} = 2\cos(\pi/n)$ for some integer n.

This example shows that the values $\boxed{\beta}$ are discrete in $[0, \theta]$ for any $\theta < 2$. On the other hand, it follows from Theorem 1 of [31] that the values of $\boxed{\beta}$ for totally real algebraic integers β are dense in $[2, \infty)$. Thus, the discreteness implicit in Theorem 1.0.5 reflects a special property of cyclotomic integers. It also follows from Theorem 1 of [31] that the values $\mathcal{M}(\beta)$ (for totally real β) are dense in $[2, \infty)$. On the other hand, a classical theorem of Siegel [29] says that $\mathcal{M}(\beta) \geq 3/2$ for any totally real algebraic integer β of degree ≥ 2, the minimum value occurring for $\beta = \frac{1+\sqrt{5}}{2}$, and, furthermore, the values of $\mathcal{M}(\beta)$ are discrete in $[0, \theta]$ for any $\theta < \lambda = 1.733610\ldots$. In the cyclotomic case, we once more see a limit point of $\mathcal{M}(\beta)$ at 2 followed by a region beyond 2 where $\mathcal{M}(\beta)$ is discrete (Theorem 9.0.1). Moreover, the closure of $\mathcal{M}(\beta)$ on $[0, \infty)$ is, in fact, a closed subset of $\mathbf{Q}$ (Theorem 9.1.1).

3. Background on Fusion Categories and Subfactors

In this section, we rapidly review some notions about fusion categories and subfactors, and collect a few remarks and examples. Although the applications of our main results are to fusion categories and subfactors, their proofs are purely arithmetic and can be read independently from this section.

A *fusion category* C over a field k is an abelian, k-linear, semisimple, rigid, monoidal category with finitely many isomorphism classes of simple objects. In this paper, all fusion categories are over the complex numbers.

A *subfactor* is an inclusion $A < B$ of von Neumann algebras with trivial centers. We will only consider subfactors in this paper which are irreducible (B is an irreducible A-B bimodule) and type II_1 (there exists a unique normalized trace). A subfactor is called

finite depth if only finitely many isomorphism classes of simple bimodules appear as summands of tensor powers of ${}_A B_A$. In particular, to every finite depth subfactor there is an associated fusion category C, called the *principal even part* which is the full subcategory of the category of A-A bimodules whose objects are summands of tensor powers of ${}_A B_A$.

The *principal graph* of a subfactor is a bipartite graph whose even vertices are the simple A-A bimodules which occur as summands of tensor powers of ${}_A B_A$, whose odd vertices are the simple A-B bimodules which occur as summands of tensor powers of ${}_A B_A$ tensored with ${}_A B_B$, and where X and Y are connected by $\dim(X \otimes {}_A B_B, Y)$ edges.

Remark 3.0.5. Usually included in the data of a principal graph is the choice of a fixed leaf which corresponds to the monoidal unit ${}_A A_A$. All the techniques in our paper which eliminate a graph Γ as a possible principal graph eliminate the graph for any choice of leaf. Nonetheless, techniques in other papers often depend on the choice of fixed leaf.

In particular, the families in Haagerup's list of potential principal graphs of small index [16] have modularity restrictions on the length of the degree 2 tree which depend on the choice of leaf. Strictly speaking, our main result when applied to $\Gamma = A_7$ with v the middle vertex is stronger than the result in [3] where they only check noncyclotomicity after assuming Haagerup's modularity conditions. Nonetheless, we will often elide this issue, and when we say a paper eliminated a family of potential principal graphs we will mean that they eliminated the principal graphs in that family which had not already been eliminated by Haagerup.

A *dimension function* on a fusion category C is a ring map $f : K(C) \to \mathbf{C}$, where $K(C)$ is the Grothendieck group thought of as a ring with the product induced by the tensor product. We often abuse notation by applying f directly to objects in C. There exists a unique dimension function FP called the *Frobenius–Perron dimension* which assigns a *positive* real number to each simple object [13, §8]. The Frobenius–Perron dimension of $X \in C$ is given by the unique largest eigenvalue of left multiplication by $[X]$ in $K(C) \otimes \mathbf{C}$. The Frobenius–Perron dimension of ${}_A B_A$ in C is the index of $A < B$ which is denoted $[B : A]$. The index of $A < B$ is the square of the largest eigenvalue of the adjacency matrix of the principal graph.

For the applications in our paper, we need the following strong arithmetic condition on dimensions.

Theorem 3.0.6 [13, Corollary 8.53]. *If C is a fusion category, X is an object in C, and f is a dimension function, then $\mathbf{Q}(f(X))$ is abelian.*

We will also want a version of this result that more easily applies to principal graphs:

Lemma 3.0.7. *If Γ is the principal graph of a finite depth subfactor $A < B$ and λ is an eigenvalue of $M(\Gamma)$ of multiplicity one, then $\mathbf{Q}(\lambda^2)$ is abelian.*

Proof. Let C be the fusion category which is the principal even part of the subfactor. Let X be the object ${}_A B_A$ inside C. From the definition of the principal graph it follows that λ^2 is a multiplicity 1 eigenvalue for left multiplication by $[X]$ in the base extended Grothendieck group $K(C) \otimes \mathbf{C}$. Decompose $K(C) \otimes \mathbf{C}$ as a product of matrix algebras $\prod \mathrm{End}(V_i)$. An element of $\mathrm{End}(V_i)$ can be thought of as acting by left multiplication on itself or as acting on V_i. The eigenvalues of the former action are exactly the eigenvalues of the latter action but each repeated $\dim V_i$ times. In particular, if x is an element of a multi-matrix algebra then any multiplicity one eigenvalue of x acting on the algebra

by left multiplication must be a component of x in one of the 1-dimensional matrix summands. In particular, we see that there is a map of rings $f : K(C) \otimes \mathbf{C} \to \mathbf{C}$ such that $\lambda^2 = f(X)$. Our result now follows immediately from Theorem 3.0.6. □

The following well-known arithmetic arguments proving two versions of the V. Jones index restriction [21] are baby examples of the main idea of this paper:

Lemma 3.0.8. *If X is an object in a fusion category with $FP(X) \leq 2$, then $FP(X) = 2\cos(\pi/n)$ for some integer n.*

Lemma 3.0.9. *If $A < B$ is a finite depth subfactor with index $[B : A] \leq 4$, then $[B : A] = 4\cos(\pi/n)^2 = 2 + 2\cos(2\pi/n)$.*

Proofs. In light of Theorem 3.0.6, Lemma 3.0.8 follows directly from Example 2.0.4. In light of Lemma 3.0.7, Lemma 3.0.9 follows either from applying Example 2.0.4 to λ, where $\lambda^2 = [B : A]$, or to $\lambda^2 - 2$. □

Remark 3.0.10. This is weaker than the V. Jones index restriction since we are making a finite depth assumption. Indeed, all our results in this paper about subfactors and monoidal categories depend crucially on finiteness assumptions.

3.1. Realizing the possible dimensions. As mentioned in the Introduction, each of the numbers in Theorem 1.0.5 can in fact be realized as the dimension of an object in a fusion category. Nonetheless, we do not necessarily expect that every number of the form $\boxed{x}$ for x a real cyclotomic integer can be realized as a dimension of an object in a fusion category. We quickly summarize how each of these numbers can be realized. The dimension $(\sqrt{3} + \sqrt{7})/2$ occurs in a fusion category constructed by Ostrik in the Appendix based on an unpublished construction via a conformal inclusion (due to Xu [33]) of a subfactor originally constructed by Izumi [18]. The dimension $\sqrt{5}$ can be achieved by a Tambara–Yamigami category associated to $\mathbb{Z}/5\mathbb{Z}$ [32]. The dimension $1 + 2\cos(2\pi/7)$ occurs as a dimension of an object in quantum SU(2) at a 14^{th} root of unity. The dimension $(1 + \sqrt{5})/\sqrt{2}$ occurs in the Deligne tensor product of quantum SU(2) at a 10^{th} root of unity and quantum SU(2) at an 8^{th} root of unity. Finally, $(1 + \sqrt{13})/2$ occurs as the dimension of an object in the dual even part of the Haagerup subfactor [2].

3.2. Deduction of Theorem 1.0.8 from Lemma 3.0.7. Suppose that α is the index of a finite depth subfactor and $4 < \alpha < 4 + 10/33 = 4.303030\ldots$ Then α is a cyclotomic integer by Lemma 3.0.7, and $\alpha = \lambda^2$ for a totally real algebraic integer λ which is the Perron–Frobenius eigenvalue of the principal graph. Thus

$$-2 \leq (\sigma\lambda)^2 - 2 \leq 76/33$$

for every conjugate $\sigma\lambda$ of λ. In particular, if $\beta = \alpha - 2$, then $2 < \boxed{\beta} < 76/33$, and by Theorem 1.0.5, we deduce that β is one of the five numbers occurring in Theorem 1.0.1. On the other hand, for three of these five numbers β has a conjugate smaller than -2, and hence the corresponding field $\mathbf{Q}(\lambda)$ is not totally real. Thus, either $\alpha = 3 + 2\cos(2\pi/7)$ or $\alpha = \frac{5+\sqrt{13}}{2}$. □

4. The Case when β is a Sum of at most 5 Roots of Unity

The goal of this section is to prove Theorem 1.0.5 in the case that $\mathcal{N}(\beta) \leq 5$ (see Theorem 4.2.6). The outline of this argument is that we first use the Conway–A. J. Jones classification of small vanishing sums of roots of unity in order to show that, outside a few exceptional cases, any real sum of five roots of unity is of the obvious form (with pairs of complex conjugate terms). We then make a more in depth analysis of small sums of the form $\zeta_N^a + \zeta_N^{-a} + \zeta_N^b + \zeta_N^{-b}$.

4.1. Vanishing Sums. Consider a vanishing sum:

$$\sum_S \xi_i = 0,$$

where the ξ_i are roots of unity. Such a sum is called *primitive* if no proper subsum vanishes. We say that such a sum has $|S|$ terms. We may normalize any such sum up to a finite ambiguity by insisting that one of the summands be 1.

Theorem 4.1.1 (Conway–A. J. Jones [8]). *For every $|S|$, there are only finitely many primitive normalized vanishing sums $\sum_{i\in S} \xi_i = 0$.*

The Conway and A. J. Jones result is more precise, in that they give explicit bounds on the conductor of the cyclotomic field generated by the ξ_i in a vanishing sum with a fixed number of terms. For our purposes, it will be useful to have a more explicit description of the primitive normalized vanishing sums for small $|S|$. The following result is a small extension of Theorem 6 of [8] which can be found in Table 1 of [28].

Theorem 4.1.2 (Conway–A. J. Jones, Poonen–Rubinstein). *The primitive vanishing sums with $|S|$ even and $|S| \leq 10$ are as follows:*

- $|S| = 2$*:*

$$1 + (-1) = 0.$$

- $|S| = 6$*:*

$$\zeta_6 + \zeta_6^5 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4 = 0.$$

- $|S| = 8$*:*

$$\begin{aligned}
\zeta_6 + \zeta_6^5 + \zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 + \zeta_7^6 &= 0.\\
\zeta_6 + \zeta_6^5 + \zeta_{30}^4 + \zeta_{30}^{10} + \zeta_{30}^{11} + \zeta_{30}^{17} + \zeta_{30}^{23} + \zeta_{30}^{24} &= 0.\\
\zeta_6 + \zeta_6^5 + \zeta_{30} + \zeta_{30}^2 + \zeta_{30}^{12} + \zeta_{30}^{13} + \zeta_{30}^{19} + \zeta_{30}^{20} &= 0.
\end{aligned}$$

- $|S| = 10$*:*

$$\begin{aligned}
\zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 + \zeta_7^6 + \zeta_{10} + \zeta_{10}^3 + \zeta_{10}^7 + \zeta_{10}^9 &= 0.\\
1 + \zeta_3 + \zeta_7 + \zeta_7^2 + \zeta_{21}^{10} + \zeta_{21}^{13} + \zeta_{42} + \zeta_{42}^{25} + \zeta_{42}^{31} + \zeta_{42}^{37} &= 0.\\
1 + \zeta_3 + \zeta_7 + \zeta_7^3 + \zeta_{21}^{10} + \zeta_{21}^{16} + \zeta_{42} + \zeta_{42}^{19} + \zeta_{42}^{31} + \zeta_{42}^{37} &= 0.\\
1 + \zeta_3 + \zeta_7 + \zeta_7^4 + \zeta_{21}^{10} + \zeta_{21}^{19} + \zeta_{42} + \zeta_{42}^{19} + \zeta_{42}^{25} + \zeta_{42}^{37} &= 0.\\
1 + \zeta_3 + \zeta_7 + \zeta_7^5 + \zeta_{21} + \zeta_{21}^{10} + \zeta_{42} + \zeta_{42}^{19} + \zeta_{42}^{25} + \zeta_{42}^{31} &= 0.\\
1 + \zeta_3 + \zeta_7^2 + \zeta_7^4 + \zeta_{21}^{13} + \zeta_{21}^{19} + \zeta_{42} + \zeta_{42}^{13} + \zeta_{42}^{25} + \zeta_{42}^{37} &= 0.
\end{aligned}$$

In particular, there does not exist any vanishing sum with $|S| = 4$.

Note that any vanishing sum of roots of unity with $|S|$ terms decomposes as a sum of primitive vanishing sums each with $|S_i|$ terms, where $|S| = \sum |S_i|$ is a partition of $|S|$.

We are interested in cyclotomic integers β that are totally real.

Lemma 4.1.3. *Suppose that $\mathcal{N}(\beta) \leq 5$, and that $\beta \neq 0$ is real. Then there exists integers a, b, and a root of unity ζ such that, up to sign, one of the following holds:*

(1) $\mathcal{N}(\beta) = 1$, *and* $\beta = 1$.
(2) $\mathcal{N}(\beta) = 2$ *and* $\beta = \zeta^a + \zeta^{-a}$.
(3) $\mathcal{N}(\beta) = 3$, *and* $\beta = \zeta^a + \zeta^{-a} + 1$.
(4) $\mathcal{N}(\beta) = 4$, *and* $\beta = \zeta^a + \zeta^{-a} + \zeta^b + \zeta^{-b}$.
(5) $\mathcal{N}(\beta) = 5$, *and* $\beta = \zeta^a + \zeta^{-a} + \zeta^b + \zeta^{-b} + 1$.
(6) $\mathcal{N}(\beta) = 3$, *and β is Galois conjugate to* $\zeta_{12} + \zeta_{20} + \zeta_{20}^{17}$.
(7) $\mathcal{N}(\beta) = 4$, *and β is Galois conjugate to one of*
  (a) $\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^{3} + \zeta_{84}^{15}$,
  (b) $\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^{3} + \zeta_{84}^{27}$,
  (c) $1 + \zeta_{12} + \zeta_{20} + \zeta_{20}^{17}$.
(8) $\mathcal{N}(\beta) = 5$, *and β is Galois conjugate to one of*
  (a) $\zeta_{12} + \zeta_{20} + \zeta_{20}^{17} + \zeta^a + \zeta^{-a}$ *for some root of unity* ζ,
  (b) $1 + \zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^{3} + \zeta_{84}^{15}$,
  (c) $1 + \zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^{3} + \zeta_{84}^{27}$,
  (d) $\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84} + \zeta_{84}^{3} + \zeta_{84}^{13}$
  (e) $\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^{15} + \zeta_{84}^{25} + \zeta_{84}^{73}$.

Proof. Let I denote a set of size $\mathcal{N}(\beta)$ such that $\beta = \sum_I \xi_i$. Note that -1 is a root of unity. If β is real, then we have a vanishing sum

$$\beta - \overline{\beta} = \sum_I \xi_i + \sum_I -\xi_i^{-1} = 0$$

with $2\mathcal{N}(\beta) \leq 10$ terms. This sum can be decomposed into primitive sums whose number of terms sum to $2\mathcal{N}(\beta)$. Write such a primitive vanishing sum as

$$\sum_A \xi_i + \sum_B -\xi_i^{-1} = 0,$$

where A and B are disjoint subsets of I. Suppose that $|A| + |B|$ is odd. Since the sum is invariant under complex conjugation, we may assume that $|A| > |B|$. It follows that

$$\beta = \sum_I \xi_i = \sum_{I \setminus A} \xi_i + \sum_A \xi_i = \sum_{I \setminus A} \xi_i + \sum_B \xi_i^{-1},$$

and hence $\mathcal{N}(\beta) \leq |I| - |A| + |B| < |I|$, a contradiction. Thus, every such vanishing subsum must have an even number of terms.

Suppose that there is a vanishing subsum with 2 terms. Then we have the following options:

(1) If $\xi_i + \xi_j = 0$, then $\beta = \sum_{I - \{i,j\}} \xi_i$, and hence $\mathcal{N}(\beta) \leq |I| - 2$, a contradiction.
(2) If $\xi_i - \xi_i^{-1} = 0$, then $\xi_i = \pm 1$. Let $\gamma = \beta - \xi_i$. Then γ real and satisfies $\mathcal{N}(\gamma) = \mathcal{N}(\beta) - 1$.
(3) If $\xi_i - \xi_j^{-1} = 0$, let $\gamma = \beta - \xi_i - \xi_i^{-1}$. Then γ is real and $\mathcal{N}(\gamma) = \mathcal{N}(\beta) - 2$.

In all these cases, the result follows by induction on $\mathscr{N}(\beta)$. So we may assume that there are no vanishing subsums with 2 terms.

Since there exists no primitive vanishing sum with 4 terms, and since $10 < 6+6$, it follows that $\sum_I \xi_i + \sum_I -\xi_i^{-1}$ is itself primitive.

Suppose that $2|I| = 6$ and our sum is proportional to a primitive vanishing sum with 6 terms. Hence our sum is proportional to $\zeta_6 + \zeta_6^5 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4$. By construction, there exists a decomposition of the sum $\sum_I \xi_i + \sum_I -\xi_i^{-1}$ into pairs with product -1. Rescaling, we have a decomposition of the sum $\zeta_6 + \zeta_6^5 + \zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4$ into pairs with constant product. Since the product of all of these numbers is 1, this constant product must be a third root of unity. But at least one pair consists only of fifth roots of unity, so the product of this pair is a fifth root of unity. Hence the product of each pair must be 1. It follows that the constant of proportionality is $\zeta_4^{\pm 1}$. Hence, up to sign and Galois conjugation, $\beta = \zeta_4\zeta_6 + \zeta_4\zeta_5 + \zeta_4\zeta_5^2$, which is Galois conjugate to $\eta := \zeta_{12} + \zeta_{20} + \zeta_{20}^{17}$. The minimal polynomial of this number is $x^8 - 8x^6 + 14x^4 - 7x^2 + 1$, and its largest Galois conjugate is $2.40487\ldots$. We note in passing that

$$\eta = 2\cos(\pi/30) + 2\cos(13\pi/30), \quad \text{and} \quad \eta^2 = \frac{4 + \sqrt{5} + \sqrt{15 + 6\sqrt{5}}}{2}.$$

Suppose that $2|I| = 8$ and our sum is proportional to a primitive vanishing sum with 8 terms. First suppose that the vanishing sum is proportional to $\zeta_6 + \zeta_6^5 + \zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 + \zeta_7^6$. Again, we look for a way of decomposing this sum into four pairs with a fixed constant product. Since the product of all the terms is 1, the constant must be a fourth root of unity. However, at least one pair has product which is a seventh root of unity. Hence, the constant product must be 1. Hence, β must be a sum of four elements, each consisting of one term from each of the pairs (ζ_6, ζ_6^{-1}), (ζ_7, ζ_7^{-1}), $(\zeta_7^2, \zeta_7^{-2})$, $(\zeta_7^3, \zeta_7^{-3})$ all scaled by a fixed primitive 4^{th} root of unity. This leads to sixteen possibilities, which fall under two Galois orbits. One Galois orbit consists of the twelve Galois conjugates of $\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^3 + \zeta_{84}^{15}$, which has minimal polynomial

$$x^{12} - 15x^{10} + 64x^8 - 113x^6 + 85x^4 - 22x^2 + 1,$$

and largest root $\beta = 3.056668\ldots$. The other orbit consists of the four conjugates of $\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^3 + \zeta_{84}^{27}$, which has minimal polynomial $x^4 - 5x^2 + 1$. We have

$$\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^3 + \zeta_{84}^{27} = \frac{\sqrt{3} + \sqrt{7}}{2} = 2.188901\ldots.$$

Now suppose that the vanishing sum is proportional to a sum of the form

$$\zeta_5^{a_1} + \zeta_5^{a_2} - \zeta_5^{a_3}(\zeta_3 + \zeta_3^2) - \zeta_5^{a_4}(\zeta_3 + \zeta_3^2) - \zeta_5^{a_5}(\zeta_3 + \zeta_3^2),$$

where the a_i are some permutation of $\{0, 1, 2, 3, 4\}$. This includes the last two vanishing sums with 8 terms. Here the product of all the terms is $\zeta_5^{a_3+a_4+a_5}$. Rescaling the sum by a fifth root of unity, we may assume that the product of all the terms is 1. So the product of each pair must be a fourth root of unity. Furthermore, at least one pair consists of two 30^{th} roots of unity, hence the product of each pair must be a 30^{th} root of unity. Hence the product of each pair must be ± 1. Since the fifth roots of unity must then pair with each other the product must be 1. However, at most one other pair multiplies to 1 (if $a_i = 0$ for $i = 3, 4, 5$). Hence there are no β that yield this vanishing sum.

Suppose that $2|I| = 10$ and our sum is proportional to a primitive vanishing sum with 10 terms. First suppose our vanishing sum is proportional to the first 10-term vanishing sum: $\zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 + \zeta_7^6 - (\zeta_5 + \zeta_5^2 + \zeta_5^3 + \zeta_5^4)$. The product of all of the terms in this sum is 1, hence the product of each pair must be a 5^{th} root of unity. However, at least one pair consists only of 7^{th} roots of unity, hence the product of each pair must be 1. Hence, $\beta = \zeta_4^{\pm 1}(\zeta_7^{\pm 1} + \zeta_7^{\pm 2} + \zeta_7^{\pm 3} - \zeta_5^{\pm 1} - \zeta_5^{\pm 2})$. Up to Galois conjugation there are two numbers of this form. Their minimal polynomials are

$$x^{24} - 36x^{22} + 506x^{20} - 3713x^{18} + 15825x^{16} - 40916x^{14} + 64917x^{12} - 62642x^{10} + 35684x^8 - 11253x^6 + 1717x^4 - 90x^2 + 1$$

and $x^8 - 12x^6 + 34x^4 - 23x^2 + 1$. The largest roots of these are $3.7294849\ldots$ and $2.861717\ldots$ respectively.

Now suppose our vanishing sum is proportional to a sum of the form

$$\zeta_7^{a_1} + \zeta_7^{a_2} + \zeta_7^{a_3} + \zeta_7^{a_4} - \zeta_7^{a_5}(\zeta_3 + \zeta_3^2) - \zeta_7^{a_6}(\zeta_3 + \zeta_3^2) - \zeta_7^{a_7}(\zeta_3 + \zeta_3^2),$$

where the a_i are a permutation of the numbers $\{0, \ldots, 6\}$. This form includes the remaining 5 vanishing sums. After possibly rescaling by a 7^{th} root of unity, the product of all the terms is 1, and hence the product of each pair is a 5^{th} root of unity. Since the only fifth root of unity that appears as a product of two terms is 1, the product of each pair must be 1. Hence, without loss of generality the pairs must be

$$\{\zeta_7^{a_1}, \zeta_7^{-a_1}\}, \{\zeta_7^{a_3}, \zeta_7^{-a_3}\}, \{-\zeta_3, -\zeta_3^2\}, \{-\zeta_7^{a_6}\zeta_3, -\zeta_7^{-a_6}\zeta_3^2\}, \{-\zeta_7^{-a_6}\zeta_3, -\zeta_7^{a_6}\zeta_3^2\}.$$

Thus β is Galois conjugate to something of the form $\zeta_4(\zeta_7 + \zeta_7^x - \zeta_3^{\pm 1} - \zeta_7^y\zeta_3 - (\zeta_7^y\zeta_3^2)^{\pm 1})$. If the last sign is positive then β can be rewritten, using $\zeta_3 + \zeta_3^2 = -1$, as a sum of 4 terms. Hence the last sign is negative. Now, if the first sign is positive we can also rewrite β as a sum of four roots of unity. Namely, we see that

$$\begin{aligned}\zeta_4(\zeta_7 + \zeta_7^x - \zeta_3 - \zeta_7^y\zeta_3 - \zeta_7^{-y}\zeta_3) &= -\zeta_4\zeta_3(-\zeta_3^{-1}\zeta_7 - \zeta_3^{-1}\zeta_7^x + 1 + \zeta_7^y + \zeta_7^{-y}) \\ &= -\zeta_4\zeta_3(-\zeta_7^a - \zeta_7^b + \zeta_3\zeta_7 + \zeta_3\zeta_7^x),\end{aligned}$$

where $a, b, x, \pm y$ are a permutation of $2, \ldots, 6$. The relation that we used is $\zeta_7^{a_1} + \zeta_7^{a_2} + \zeta_7^{a_3} + \zeta_7^{a_4} + \zeta_7^{a_5} - (\zeta_3 - \zeta_3^{-1})\zeta_7^{a_6} - (\zeta_3 - \zeta_3^{-1})\zeta_7^{a_7}$, where the a_i are a premutation of $0, \ldots, 6$.

Hence β is Galois conjugate to

$$\zeta_4(\zeta_7 + \zeta_7^x - \zeta_3^2 - \zeta_7^y\zeta_3 - \zeta_7^{-y}\zeta_3),$$

where x and y are each one of $\{2, 3, 4, 5\}$ such that x is not congruent to $\pm y$ modulo 7.

There are two different Galois orbits of that form. The roots of $x^{12} - 16x^{10} + 60x^8 - 78x^6 + 44x^4 - 11x^2 + 1$, the largest of which is approximately $3.354753\ldots$; and the roots of $x^{12} - 22x^{10} + 85x^8 - 113x^6 + 64x^4 - 15x^2 + 1$, the largest of which is approximately $4.183308\ldots$. These correspond to Galois conjugates of the roots occurring in $(8d)$ and $(8e)$ in the statement of the theorem. Note the curious identities (of sums of real numbers):

$$(\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84} + \zeta_{84}^3 + \zeta_{84}^{13}) = (\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^3 + \zeta_{84}^{15}) + (\zeta_{84} + \zeta_{84}^{13} - \zeta_{84}^{15}),$$
$$(\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^{15} + \zeta_{84}^{25} + \zeta_{84}^{73}) = (\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^3 + \zeta_{84}^{15}) + (\zeta_{84}^{25} + \zeta_{84}^{73} - \zeta_{84}^3).$$

Here the "exotic" real numbers $\zeta_{84} + \zeta_{84}^{13} - \zeta_{84}^{15}$ and $\zeta_{84}^{25} + \zeta_{84}^{73} - \zeta_{84}^3$ are equal to $2\cos(13\pi/84)$ and $2\cos(25\pi/84)$ respectively, and so can actually be written as the sum of two roots of unity. □

4.2. Estimates. In this section, we analyze in more detail sums of the form $\beta = \zeta_N^a + \zeta_N^{-a} + \zeta_N^b + \zeta_N^{-b}$. We wish to find all such sums which have $\boxed{\beta} < 4\cos(2\pi/7)$. Our argument in this section closely follows the paper of A. J. Jones [20], who studies expressions of the form $\beta = 1 + \zeta_N^a + \zeta_N^b$ with $\boxed{\beta}$ small. In outline, this argument uses the geometry of numbers, as follows. The Galois conjugates of $\zeta_N^a + \zeta_N^{-a} + \zeta_N^b + \zeta_N^{-b}$ are all of the form $\zeta_N^{ak} + \zeta_N^{-ak} + \zeta_N^{bk} + \zeta_N^{-bk}$ for $(k, N) = 1$. Using Minkowski's theorem, we can find a k such that all four roots of unity are all "close" to one, and thus the expression above is large. However, it is not immediately apparent that one can choose such a k co-prime to N. Instead, using certain estimates involving the Jacobsthal function, we show that *either* there exists a suitable k co-prime to N *or* the integers (a, b) satisfy a linear relation $ax - by = 0 \mod N$ with (x, y) one of a small explicit finite set of integers ((2, 2), (3, 3), or (2, 4)). In the latter case, we may study β directly. A much simpler 1-dimensional argument, also using estimates on the Jacobsthal function, gives a description of all $\beta = \zeta_{12} + \zeta_{20} + \zeta_{20}^{17} + \zeta_N^a + \zeta_N^{-a}$ such that $\boxed{\beta} < 4\cos(2\pi/7)$.

Definition 4.2.1. *The Jacobsthal function $j(N)$ is defined to be the smallest m with the following property: In every arithmetic progression with at least one integer co-prime to N, every m consecutive terms contains an element co-prime to N.*

Lemma 4.2.2. *Suppose that $M|N$ has one fewer distinct prime factors than N. Then there is an inequality $j(M)^2 \leq N/11$ for $N > 210$ and $N \neq 330, 390$.*

Proof. A result of Kanold [22] shows that $j(N) \leq 2^{\omega(N)}$, where $\omega(N)$ is the number of distinct primes dividing N. Note that $j(N)$ only depends on the square-free part of N. Suppose that N has at least $d \geq 7$ prime factors. Then $j(M) \leq 2^{d-1}$, whereas

$$N/11 \geq (11)^{-1} \prod_{n=1}^{d} p_n \geq 2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 4^{d-6} = \frac{1365}{512} \cdot 4^{d-1} \geq j(M)^2.$$

For smaller d, we note the following bounds on $j(M)$, noting that M has one less distinct prime divisor than N. These bounds were computed by Jacobsthal [19]:

$$\begin{aligned} &\text{if } d = 2, \quad \text{then } j(M) \leq 2, \\ &\text{if } d = 3, \quad \text{then } j(M) \leq 4, \\ &\text{if } d = 4, \quad \text{then } j(M) \leq 6 \text{ and} \\ &\text{if } d = 5, \quad \text{then } j(M) \leq 10. \end{aligned}$$

Thus, if N has 5 prime factors, we are done if $N \geq 1100$, if N has 4 prime factors, we are done if $N \geq 396$, and if N has less than three prime factors, we are done if $N \geq 176$. Yet if N has 5 prime factors, then $N \geq 2310$, and if N has 4 prime factors, then $N \geq 396$ unless $N = 210, 330$, or 390. □

Lemma 4.2.3. *$j(M) \leq 2M/5 - 1$ for all M except $M \in \{1, 2, 3, 4, 5, 6, 7, 10, 12\}$.*

Proof. As in Lemma 4.2.2 we use the result of Kanold to see that this theorem is true for all M which is divisible by 3 or more primes. If M is a product of two primes, then $j(M) \leq 4$, so the inequality follows so long as $M > 12$. If M is prime then $j(M) \leq 2$, so the inequality follows so long as $M > 7$. □

Remark 4.2.4. The known asymptotic bounds for $j(N)$ are much better, see, for example, Iwaniec [17].

Now we apply these bounds on Jacobsthal functions to finding small sums of roots of unity.

Lemma 4.2.5. *If* $\beta = \zeta_{12} + \zeta_{20} + \zeta_{20}^{17} + \zeta_N^a + \zeta_N^{-a}$, *then* $\boxed{\beta} = 2\cos(2\pi/60)$, *or* $\boxed{\beta} = \zeta_{12} + \zeta_{20} + \zeta_{20}^{17}$, *or* $\boxed{\beta} \geq 4\cos(2\pi/7)$.

Proof. Let $\eta = \zeta_{12} + \zeta_{20} + \zeta_{20}^{17}$. Write $N = AM$, where $A = (N, 60)$. We see that β is conjugate to $\eta + \zeta_N^b + \zeta_N^{-b}$ for any $(b, N) = 1$ such that $b \equiv a \mod A$. If there exists such a b satisfying $b/N \in [-1/5, 1/5]$, then

$$\boxed{\beta} \geq \eta + 2\cos(2\pi/5) = 3.022901\ldots,$$

which is certainly greater than $4\cos(2\pi/7)$. To guarantee the existence of such a b, we need to ensure that at least one term of the arithmetic progression of integers congruent to $a \mod A$ in the range $[-N/5, N/5]$ is co-prime to M (it is automatically co-prime to A). The length of this arithmetic progression is at least $2N/5A - 1 = 2M/5 - 1$. Such a b always exists provided that $j(M) \leq 2M/5 - 1$, where $j(M)$ denotes the Jacobsthal function. By Lemma 4.2.3, this inequality holds for all M except $M \in \{1, 2, 3, 4, 5, 6, 7, 10, 12\}$. This leaves a finite number of possible N and β to consider, which we can explicitly compute. In particular, we look at

$$\begin{aligned} N \in \{&1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 24, 25, 28, 30, 35, 36, 40,\\ &42, 45, 48, 50, 60, 70, 72, 75, 80, 84, 90, 100, 105, 120, 140, 144, 150, 180, 200,\\ &210, 240, 300, 360, 420, 600, 720\}. \end{aligned}$$

Indeed, in this range, the smallest largest conjugate of β is $2\cos(2\pi/60)$ (with, e.g., $N = 60, a = 17$), the second smallest is $\eta = 2.40487\ldots$ (with, e.g., $N = 4, a = 1$), and the next smallest is

$$\eta + 2\cos\left(2\pi\frac{19}{60}\right) = 2.71559\ldots > 4\cos(2\pi/7).$$

□

Theorem 4.2.6. *Suppose that* $N > 230$ (*we will need a slightly higher bound than the* 210 *of the Lemma* 4.2.2), *and* $N \neq 330$, *or* 390. *Let* β *be a number of the form* $\zeta_N^a + \zeta_N^{-a} + \zeta_N^b + \zeta_N^{-b}$, *where* a *and* b *are relatively prime, then either*:

(1) β *is the sum of at most two roots of unity, and thus* $\boxed{\beta} \leq 2$,
(2) β *is conjugate to* $(1 + \sqrt{5})/\sqrt{2}$ *or* $\sqrt{6}$,
(3) β *has a positive conjugate whose absolute value is bigger than* $4\cos(2\pi/7)$, *in particular,* $\boxed{\beta} \geq 4\cos(2\pi/7)$.

Before proving this theorem we prove several lemmas. Let us fix once and for all the constant $K = 2/49$.

Lemma 4.2.7. *Let* $x, y \in \mathbf{R}$. *Suppose that* $x^2 + y^2 < K$. *Then* $2\cos(2\pi x) + 2\cos(2\pi y) > 4\cos(2\pi/7)$.

Proof. The minimum value of $2\cos(2\pi x) + 2\cos(2\pi y)$ occurs when $x = y = 1/7$. □

Definition 4.2.8. *Denote by* $\Lambda_{a,b,N} \subset \mathbf{Z}^2$ *the set of integer vectors* x *such that* $x.(a, -b) \equiv 0 \mod N$.

The determinant of the lattice $\Lambda_{a,b,N}$ is N. We may describe it explicitly as follows. Let $u = (b, a)$, and fix a vector v such that $v.(a, -b) = 1$. Then $\mathbf{Z}^2$ is generated by u and v, and $\Lambda_{a,b,N}$ is generated by u and Nv. Up to scalar, there is a canonical map $\phi : \Lambda_{a,b,N} \to \mathbf{Z}/N\mathbf{Z}$ obtained by reduction modulo N. We say that a vector $\lambda \in \Lambda_{a,b,N}$ is co-prime to N if and only if the image $\phi(\lambda)$ of λ in $\mathbf{Z}/N\mathbf{Z}$ lands in $(\mathbf{Z}/N\mathbf{Z})^\times$. Denote by Q the quadratic form $Q(x, y) = x^2 + y^2$ on $\mathbf{Z}^2$ restricted to $\Lambda_{a,b,N}$; it has discriminant $-4N^2$.

Lemma 4.2.9. *If* λ *is co-prime to* N, *and* $Q(\lambda) \leq K \cdot N^2$, *then* $\beta = \zeta_N^a + \zeta_N^{-a} + \zeta_N^b + \zeta_N^{-b}$ *has* $\boxed{\beta} \geq 4\cos(2\pi/7)$.

Proof. We may write $(r, s) = \lambda = k(b, a) \mod N$, for some k co-prime to N. Replacing ζ by ζ^k is thus an automorphism of $\mathbf{Q}(\zeta)$, which has the effect of replacing β by

$$\zeta^{ka} + \zeta^{-ka} + \zeta^{kb} + \zeta^{-kb} = 2\cos(2\pi r/N) + 2\cos(2\pi s/N) \leq 4\cos(2\pi/7).$$

Hence, from Lemma 4.2.7, we deduce the result. □

Proof of Theorem 4.2.6. It suffices to assume that $\boxed{\beta} < 4\cos(2\pi/7)$ and derive a contradiction. Note that the Galois conjugates of β can be obtained by replacing ζ_N by ζ_N^k for some integer k such that $(k, N) = 1$. Hence the Galois conjugates are exactly the numbers of the form $\zeta_N^{a'} + \zeta_N^{-a'} + \zeta_N^{b'} + \zeta_N^{-b'}$ for $(a', b') \in \Lambda_{a,b,N}$ which is relatively prime to N.

By reduction theory for quadratic forms, there exists a basis μ, ν of $\Lambda_{a,b,N}$ for which

$$Q(x \cdot \mu + y \cdot \nu) = Ax^2 + Bxy + Cy^2, \qquad |B| \leq A \leq C, \quad \Delta := B^2 - 4AC = -4N^2.$$

Now $A^2 \leq AC \leq AC + \frac{1}{3}(AC - B^2) = -\frac{4}{3}\Delta = 3N^2 \leq K^2 \cdot N^4$, providing that $N > 43$. Hence $Q(\mu) < K \cdot N^2$, and thus, by Lemma 4.2.9, μ is not co-prime to N. Since $\phi : \Lambda_{a,b,N} \to \mathbf{Z}/N\mathbf{Z}$ is surjective, there exists an integer k such that $k\mu + \nu$ is co-prime to N. By assumption, N has a prime factor q that divides μ. The terms in this sequence must all be automatically co-prime to q. Let M be N divided by the highest power of q dividing N. In order to find something of the form $k\mu + \nu$ is co-prime to N, it suffices to find one that is co-prime to M. By definition of the Jacobsthal function, it follows that we may take a

$$k \in \left[\frac{-j(M)}{2} + \frac{B}{2A}, \frac{j(M)}{2} + \frac{B}{2A}\right]$$

such that $k\mu + \nu$ is co-prime to N, and hence $Q(k\mu + \nu) > K \cdot N^2$. Yet

$$Q(k\mu+\nu) = Ak^2+Bk+C = A(k - B/2A)^2 + (4AC - B^2)/4A \leq j(M)^2A/4 + N^2/A,$$

and thus

$$j(M)^2A^2/4 + N^2 \geq KN^2A.$$

Since this inequality holds for $A = 0$, and since $j(M)^2 > 0$, we see that the inequality holds exactly on the complement of some (possibly empty) interval. Using the assumption that $N \geq 230$ and Lemma 4.2.2, we see that the inequality does not hold for $A = \sqrt{3}N$. Namely,

$$\frac{3}{4} j(M)^2 N^2 + N^2 \leq \frac{3}{44} N^3 + N^2 < K N^2 A.$$

Similarly, using that $N \geq 28$, we also see that the inequality does not hold for $A = 25$. Namely,

$$\left(\frac{25}{4} j(M)^2 + N^2/25 \leq \frac{N}{44} + \frac{N^2}{25} \right) A < K \cdot N^2 \cdot A.$$

Hence the inequality does not hold for any A in the interval $[25, \sqrt{3}N]$. Since A is positive and $A^2 \leq 3N^2$ it follows that $A \leq 24$, and hence $Q(\mu) \leq 24$.

Write $\mu = (x, y)$. Then $x^2 + y^2 \leq 24$, and $ax - by \equiv 0 \mod N$. Recall that μ is not co-prime to N, and thus x must not be co-prime to y. It follows that (x, y), up to sign and ordering, is one of the pairs $(2, 2)$, $(3, 3)$ or $(2, 4)$. We consider each of these in turn.

(1) $(x, y) = (2, 2)$. It follows that $(a, b) = (a, a)$ or $(a, a + N/2)$. In the first case, the maximum absolute value of any conjugate of β is of the form $4\cos(\pi/M)$ for some M. In the second case, $\zeta^a = -\zeta^b$, so $\beta = 0$.

(2) $(x, y) = (3, 3)$, either $(a, b) = (a, a)$, or, after making an appropriate permutation, $(a, b) = (a, a + N/3)$. In this case, with $\omega^3 = 1$,

$$\beta = \zeta^a + \zeta^{-a} + \zeta^a \omega + \zeta^{-a} \omega^{-1} = -\omega^{-1} \zeta^a - \omega \zeta^a$$

is a sum of two roots of unity.

(3) $(x, y) = (2, 4)$. The only new possibility is $(a, b) = (a, a + N/4)$. Letting $i^4 = 1$, we find that

$$\beta = \zeta^a (1 + i) + \zeta^{-a} (1 - i) = \sqrt{2}(\zeta^a \zeta_8 + \zeta^{-a} \zeta_8^{-1}) = \sqrt{2}(\zeta' + \zeta'^{-1}),$$

and hence $\boxed{\beta} = 2\sqrt{2}\cos(\pi/M)$ for some M. The only numbers of this kind between 2 and $4\cos(\pi/7)$ occur for $M = 5$ and 6, for which we obtain the values $(1 + \sqrt{5})/\sqrt{2}$ and $\sqrt{6}$.

This completes the proof of the theorem. □

Theorem 4.2.10. *Let β be totally real, and suppose that $\mathcal{N}(\beta) \leq 5$. Then either*

(1) β is a sum of at most two roots of unity.
(2) $\boxed{\beta} \geq 4\cos(2\pi/7)$.
(3) A conjugate of β is one of the following numbers, listed in increasing order:

$$\begin{aligned}
\frac{\sqrt{3}+\sqrt{7}}{2} &= 2.18890105931673\ldots,\\
\sqrt{5} &= 2.23606797749978\ldots,\\
1+2\cos(2\pi/7) = 2\cos(\pi/7)+2\cos(3\pi/7) &= 2.24697960371746\ldots,\\
\frac{1+\sqrt{5}}{\sqrt{2}} = 2\cos(\pi/20)+2\cos(9\pi/20) &= 2.28824561127073\ldots,\\
1+2\cos(4\pi/13)+2\cos(6\pi/13) &= 2.37720285397295\ldots,\\
1+2\cos(2\pi/11)+2\cos(6\pi/11) &= 2.39787738911579\ldots,\\
2\cos(\pi/30)+2\cos(13\pi/30) &= 2.40486717237206\ldots,\\
1+\sqrt{2} &= 2.41421356237309\ldots,\\
\sqrt{6} = 2\cos(\pi/12)+2\cos(5\pi/12) &= 2.44948974278317\ldots,\\
2\cos(11\pi/42)+2\cos(13\pi/42) &= 2.48698559166908\ldots.
\end{aligned}$$

Proof. We split into cases using the classification of Lemma 4.1.3. If $\mathscr{N}(\beta) = 3$ and $\beta = 1+\zeta^a+\zeta^{-a}$, then the largest conjugate of β is $1+2\cos(2\pi/N)$. For N less than 7 we could rewrite this as a sum of fewer than three terms. If $N = 7$, then $\beta = 1+2\cos(2\pi/7)$. If $N = 8$, then $\beta = 1+\sqrt{2}$. If $N \geq 9$, then $\beta > 4\cos(2\pi/7)$.

If $\mathscr{N}(\beta) = 4$, and $\beta = \zeta^a+\zeta^{-a}+\zeta^b+\zeta^{-b}$, then the previous theorem applies if $N > 230$ and $N \neq 330$ or 390.

If $\mathscr{N}(\beta) = 5$, and $\beta = 1+\zeta^a+\zeta^{-a}+\zeta^b+\zeta^{-b}$, then the previous theorem applies to $\beta - 1$ if $N > 230$ and $N \neq 330$ or 390. If $\beta - 1$ has a positive conjugate whose absolute value is larger than $4\cos(2\pi/7)$, it follows that $\boxed{\beta} > 1+4\cos(2\pi/7)$

If $\mathscr{N}(\beta) = 5$ and $\beta = \zeta_{12}+\zeta_{20}+\zeta_{20}^{17}+\zeta_N^a+\zeta_N^{-a}$, then we apply Lemma 4.2.5.

Hence we need only consider finitely many remaining numbers. First, we may have that $N \leq 230$ or $N = 330$ or $N = 390$. Second, we may be in one of the finitely many exceptional cases in Lemma 4.1.3. In the former case, we compute directly that the largest conjugates all have absolute value at least $4\cos(2\pi/7)$, except for the exceptions listed above. For the latter case, only one of the exception numbers, $(\sqrt{3}+\sqrt{7})/2$, has $\boxed{\beta}$ small enough. □

Remark 4.2.11. It is a consequence of this computation and Theorem 1.0.5 that the smallest largest conjugate of a real cyclotomic integer which is *not* a sum of 5 or fewer roots of unity is

$$\frac{1+\sqrt{13}}{2} = -\left(\zeta^2+\zeta^{-2}+\zeta^6+\zeta^{-6}+\zeta^8+\zeta^{-8}\right) = 2.30277\ldots,$$

where ζ is a 13^{th} root of unity.

We shall use the following result, which follows directly from Theorem 4.2.10.

Corollary 4.2.12. *Let β be a real cyclotomic integer such that $3 \leq \mathscr{N}(\beta) \leq 5$. Then either β is conjugate to $\frac{1}{2}(\sqrt{3}+\sqrt{7})$, $\sqrt{5}$, $1+2\cos(2\pi/7)$, $(1+\sqrt{5})/\sqrt{2}$, or $\boxed{\beta} \geq 76/33$.*

5. The Normalized Trace

The goal of the next two sections is to prove that

Theorem 5.0.13. *If β is a cyclotomic integer such that β is real, $\boxed{\beta} < 76/33$, and $\mathscr{N}(\beta) \geq 3$, then either $\boxed{\beta} = (1+\sqrt{13})/2$, or $\beta \in \mathbf{Q}(\zeta_N)$, where*

$$N = 4 \cdot 3 \cdot 5 \cdot 7 = 420.$$

So suppose that β is real, that $\beta \in \mathbf{Q}(\zeta_N)$ with N minimal, that $\mathscr{N}(\beta) \geq 3$, and $\boxed{\beta} < 76/33$. First we prove a lemma which allows us to reduce to studying β with $\mathscr{M}(\beta) < 23/6$. Second, we show that if $p^k \mid N$ with $k > 1$ then $p^k = 4$, this argument uses techniques developed by Cassels [7]. In the next section, we will show that if $p > 7$ then either $p \nmid N$ or $p = 13$ and $\beta = (1+\sqrt{13})/2$. Again this argument will use techniques generalizing those of Cassels.

5.1. Relationship between $\boxed{\beta}$ and $\mathscr{M}(\beta)$. The following lemma allows us to reduce to considering β with $\mathscr{M}(\beta)$ small.

Lemma 5.1.1. *Let $\beta \in \overline{\mathbf{Q}}$ be a totally real algebraic integer, and suppose that $\boxed{\beta} < 76/33 = 2.303030\ldots$ Then either $\beta^2 = 4$ or 5, or $\mathscr{M}(\beta) < 23/6 = 3.833333\ldots$.*

Proof. Let $\kappa = 23/6$, and let $\alpha = \frac{1+\sqrt{13}}{2}$. Since

$$\mathscr{M}(\alpha) = \frac{1}{2}\left(\frac{7+\sqrt{13}}{2} + \frac{7-\sqrt{13}}{2}\right) = \frac{7}{2} < \frac{23}{6},$$

we may assume that β is not a conjugate of α. Similarly $\mathscr{M}(\sqrt{3}) = 3$, and so we may assume that $\beta^2 \neq 3$.

The inequality

$$\Theta(x) = 120(\kappa - x) - \Big(36\log|x-4| + 160\log|x-5| + 9\log|x-3| + 2\log|x^2 - 7x + 9|\Big) > 0$$

for $x \in [0, (76/33)^2] = [0, 5.303948\ldots]$ is an easy calculus exercise. (Note that the roots of the polynomial $x^2 - 7x + 9$ are the conjugates of α^2.) The critical points are the roots of $-40200 + 68381x - 44376x^2 + 13814x^3 - 2071x^4 + 120x^5$. The absolute minimum value in this range occurs at approximately $x = 3.320758\ldots$, where Θ obtains its minimum of roughly $0.394415\ldots$ (Fig. 2).

Let $S = \{x_i\}$ be a finite set of real numbers in $[0, (76/33)^2]$ whose average is greater than $\kappa = 23/6$. Then the average of $\kappa - x_i$ is less than zero, and hence

$$0 > 120\sum(\kappa - x_i) \geq 36\sum\log|x_i - 4| + 160\sum\log|x_i - 5| + 9\sum\log|x_i - 3| + 2\sum\log|x_i^2 - 7x_i + 9|.$$

Suppose that S consists of the squares of the conjugates of $\beta \in K = \mathbf{Q}(\beta)$. Since $\boxed{\beta} < 76/33$, it follows that all the x_i lie in $[0, (76/33)^2]$. Since we are assuming that $\beta^2 \neq 3, 4, 5$, nor a conjugate of α^2 (which is a root of $x^2 - 7x + 9$), it follows that the norms of $\beta^2 - 3$, $\beta^2 - 4$, and $\beta^2 - 5$, as well as $\beta^4 - 7\beta^2 + 9$, are non-zero algebraic integers. Hence the absolute value of their norms are at least one. Taking logarithms, we deduce that every sum occurring on the right-hand side of the inequality above is non-negative, which is a contradiction, and the lemma is established. □

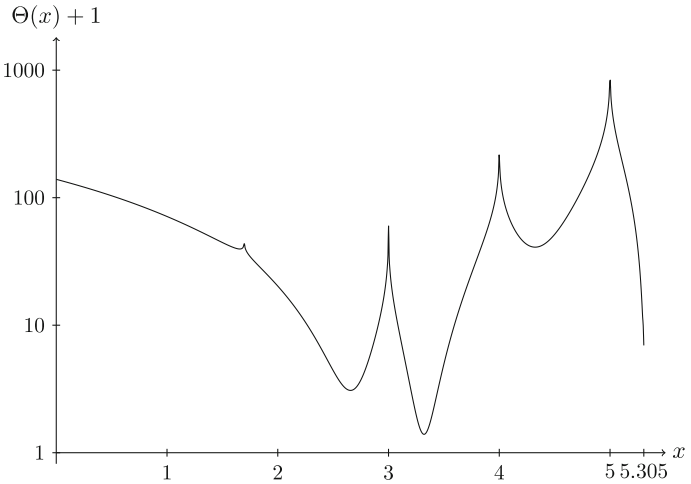

Fig. 2. The function $\Theta(x)+1$, on a log scale. The four visible peaks, and one that is not apparent on the graph, near $x = 5.30278$, are actually asymptotes

Remark 5.1.2. The constants (120, 36, 160, 9, 2) chosen in this proof are somewhat arbitrary and mysterious, and fine tuning would certainly lead to an improved result. However, to increase 76/33 substantially one would need to allow $\mathscr{M}(\beta)$ to increase, which would increase the combinatorial difficulty of our later arguments.

It follows that in order to prove Theorem 5.0.13, we may assume that $\mathscr{M}(\beta) < 23/6$. We shall also frequently use the following lemmas:

Lemma 5.1.3. (Cassels' Lemma 2 [7]) *If* $\mathscr{N}(\alpha) \geq 2$, *then* $\mathscr{M}(\alpha) \geq 3/2$.

Lemma 5.1.4. (Cassels' Lemma 3 [7]) *If* $\mathscr{N}(\alpha) \geq 3$, *then* $\mathscr{M}(\alpha) \geq 2$.

5.2. The case when $p^2|N$. Suppose that $\beta \in \mathbf{Q}(\zeta_N)$, and suppose that N is minimal with respect to this property. We start with what Cassels calls the *second case*, that is, the case when N admits a prime p such that $p^2|N$. Explicitly, assume that $p^m \| N$ for an integer $m \geq 2$. Let $N = p^{m-1}M$, so $p \| M$. Let ζ be a $p^{m\text{th}}$ root of unity. We may write

$$\beta = \sum_S \zeta^i \alpha_i,$$

where $\alpha_i \in \mathbf{Q}(\zeta_M)$. Here S denotes any set of p^{m-1} integers that are distinct modulo p^{m-1}. After having chosen an S, the α_i are determined uniquely by β. Since β is real, it is invariant under complex conjugation. It follows that

$$\sum_S \zeta^i \alpha_i = \sum_S \zeta^{-i} \overline{\alpha_i}.$$

If p is odd, let S denote the set $\{-\frac{(p^{m-1}-1)}{2}, -\frac{(p^{m-1}-3)}{2}, \ldots, -1, 0, 1, 2, \ldots \frac{(p^{m-1}-1)}{2}\}$. If $p = 2$, let $S = \{-(2^{m-2}-1), \ldots, -1, 0, 1, 2, \ldots, 2^{m-2}\}$. From the uniqueness of this expansion we deduce, if p is odd, that $\overline{\alpha_i} = \alpha_{-i}$ for all $i \in S$. If $p = 2$, we deduce that $\overline{\alpha_i} = \alpha_{-i}$ if $i < 2^{m-2}$, and that $\overline{\zeta^{2^{m-2}}\alpha_{2^{m-2}}} = \zeta^{2^{m-2}}\alpha_{2^{m-2}}$.

Lemma 5.2.1. *There is an equality* $\mathscr{M}(\beta) = \sum \mathscr{M}(\alpha_i)$.

Proof. Our proof is essentially that of Cassels (who proves it under extra hypotheses that are not required for the proof of this particular statement). We reproduce the proof here. The conjugates of ζ over $\mathbf{Q}(\zeta_M)$ are $\zeta \cdot \zeta^{pn}$ for $n = 0$ to $p^{m-1} - 1$. Let $\mathscr{M}'(\theta)$ denote the average of the conjugates of $|\theta|^2$ over $\mathbf{Q}(\zeta_M)$. Then

$$\begin{aligned} p^{m-1}\mathscr{M}'(\beta) &= \sum_n \sum_i \zeta^i \alpha_i \zeta^{pni} \sum_j \zeta^{-j} \overline{\alpha_j} \zeta^{-pnj} \\ &= \sum_n \sum_{i,j} \zeta^{i-j} \zeta^{pn(i-j)} \alpha_i \overline{\alpha_j} \\ &= \sum_{i,j} \zeta^{i-j} \alpha_i \overline{\alpha_j} \sum_n \zeta^{pn(i-j)}. \end{aligned}$$

Now $i \equiv j \mod p^{m-1}$ if and only if $i = j$, and thus $\zeta^{p(i-j)} = 1$ if and only if $i = j$. For all other pairs (i, j), the final sum is a power sum of a non-trivial root of unity over a complete set of congruence classes, and is thus 0. Hence, as in Cassels, we find that

$$\mathscr{M}'(\beta) = \sum |\alpha_i|^2,$$

and the result follows upon taking the sum over the conjugates of $\mathbf{Q}(\zeta_M)$ over $\mathbf{Q}$. □

Let X denote the number of α_i which are non-zero. In order to prove Theorem 5.0.13 in this case, we must show that if $p^2 \mid N$, then $p = 2$ and $4 \| N$.

5.3. The case when $X = 1$. If p is odd, then $\beta = \alpha = \overline{\alpha}$. In this case we find that $\beta \in \mathbf{Q}(\zeta_M)$, contradicting the minimality assumption on N. If $p = 2$, then either $\beta = \alpha = \overline{\alpha}$, or

$$\beta = \zeta^{2^{m-2}} \alpha_{2^{m-2}} = \overline{\zeta^{2^{m-2}} \alpha_{2^{m-2}}}.$$

By minimality, we deduce that $2^{m-2} = 1$, and hence $2^m = 4$. (The number $\frac{\sqrt{3}+\sqrt{7}}{2}$ is, in fact, of this form.)

5.4. The case when $X = 2$. If p is odd, we deduce that $\beta = \zeta\alpha + \zeta^{-1}\overline{\alpha}$. If $\mathscr{N}(\alpha) \leq 2$, then we are done, by Corollary 4.2.12. If $\mathscr{N}(\alpha) > 2$, then by Lemma 3 of Cassels, $\mathscr{M}(\alpha) \geq 2$, and $\mathscr{M}(\beta) \geq 4$.

If $p = 2$, the same argument applies, except in this case it could be that

$$\beta = \alpha_0 + \zeta^{2^{m-2}} \alpha_{2^{m-2}}.$$

Once more, since N is minimal with respect to β, it must be the case that $2^{m-2} = 1$ and $2^m = 4$.

5.5. The case when $X = 3$. If p is odd, then, for some primitive $p^{m\text{th}}$ root of unity ζ, we have $\beta = \zeta\alpha + \gamma + \zeta^{-1}\overline{\alpha}$. If α is a root of unity, then, by Corollary 4.2.12, we may assume that $\mathscr{N}(\gamma) \geq 3$ and hence (by Lemma 3 of Cassels) that $\mathscr{M}(\gamma) \geq 2$, and thus $\mathscr{M}(\beta) \geq 1 + 1 + 2 = 4$. If $\mathscr{N}(\alpha) = 2$, then by Lemma 2 of Cassels, $\mathscr{M}(\alpha) \geq 3/2$, and hence $\mathscr{M}(\beta) \geq 3/2 + 3/2 + 1 = 4$.

If $p = 2$, there is at least one i such that $\alpha_i \neq 0$ and $i \neq 0, 2^{m-2}$. It follows that $\beta = \zeta\alpha + \gamma + \zeta^{-1}\overline{\alpha}$ for some γ such that $\overline{\gamma} = \gamma$, and the proof proceeds as above.

5.6. The case when $X \geq 4$ It is immediate that $\mathscr{M}(\beta) \geq 4$. .

6. The Case when p Exactly Divides N

We now consider what Cassels calls the *first case*, where $p \mid\mid N$. So suppose that β is real, that $\beta \in \mathbf{Q}(\zeta_N)$ with N minimal, that $\mathscr{N}(\beta) \geq 3$, and $\boxed{\beta} < 76/33$. We will show in this section that if $p \mid N$ then $p \leq 7$ or $p = 13$ and $\beta = (1 + \sqrt{13})/2$. (In particular, we may assume that p is odd.) This will complete the proof of Theorem 5.0.13.

Write $N = pM$ once again, and let ζ be a primitive p^{th} root of unity. The conjugates of ζ are now $\zeta \cdot \zeta^k$ for any k *except* $k \equiv -1 \mod p$.

We write

$$\beta = \sum_S \zeta^i \alpha_i,$$

where $\alpha_i \in \mathbf{Q}(\zeta_M)$ and S denotes $\{-(p-1)/2, \ldots, 0, 1, \ldots, (p-1)/2\}$. This expansion is no longer unique; there is ambiguity given by a fixed constant for each element. Since β is real, it is invariant under complex conjugation. It follows that there exists a fixed $\lambda \in \mathbf{Q}(\zeta_M)$ such that

$$\overline{\alpha_i} = \alpha_{-i} + \lambda.$$

The element λ itself must satisfy $\overline{\lambda} = -\lambda$, or equivalently, that $\lambda \cdot \sqrt{-1}$ is real.

Let X denote the number of terms occurring in S such that $\alpha_i \neq 0$.

Lemma 6.0.1. *If $\lambda \neq 0$, then $X \geq (p+1)/2$. If λ is a root of unity, then $\lambda = \pm\sqrt{-1}$.*

Proof. If $\lambda \neq 0$, then since $\alpha_{-i} - \overline{\alpha_i} = \lambda$, at least one of $\{\alpha_i, \alpha_{-i}\}$ must be non-zero. Since there are $(p+1)/2$ such pairs not containing any common element, the result follows. The second claim follows from the fact that $\lambda \cdot \sqrt{-1}$ is real. □

6.1. The case when $X = 1$. We deduce that $\beta = \alpha = \overline{\alpha}$, contradicting the minimality of N.

6.2. The case when $X = 2$. If $p \geq 7$, by Lemma 6.0.1, we may assume that $\lambda = 0$, and hence

$$\beta = \zeta\alpha + \zeta^{-1}\overline{\alpha}.$$

If α is a root of unity, then $\mathscr{N}(\beta) \leq 2$. Hence, we may assume (replacing α by a conjugate) that $|\alpha| \geq \sqrt{2}$. Note that we may choose ζ to be primitive, since N was chosen

to be minimal with respect to β. Write $\zeta\alpha = |\alpha|e^{2\pi i\theta}$. The conjugates of ζ are $\zeta \cdot \zeta^k$, where k is any integer such that $k \not\equiv -1 \mod p$. We replace ζ by a conjugate to make θ as close to 0 or $1/2$ as possible. By Dirichlet's box principle, with no constraint on k we could insist that $\|\theta\| \leq 1/2p$, or, if we liked, that $\|\theta - 1/2\| \geq 1/2p$. Given our single constraint, we may *at least* find a conjugate of ζ such that θ satisfies one of these inequalities. In either case, we deduce that

$$|\beta| > 2|\alpha|\cos(\pi/7) \geq 2\sqrt{2}\cos(\pi/7) = 2.548324\ldots > 2.303030\ldots = 76/33.$$

6.3. The case when $X = 3$. Suppose that $X = 3$, and suppose that $p \geq 11$. By Lemma 6.0.1, we may assume that $\lambda = 0$. We may therefore assume that

$$\beta = \zeta\alpha + \gamma + \zeta^{-1}\overline{\alpha},$$

where $\overline{\gamma} = \gamma$. After conjugating, we may assume that $|\alpha\gamma| \geq 1$. After possibly negating β, we may assume that γ is positive. Write $\zeta\alpha = |\alpha|e^{2\pi i\theta}$. Now we must insist that $\|\theta\|$ is small rather than $\|\theta - 1/2\|$, and thus may only deduce that $\|\theta\| \leq 1/p$. It follows that

$$\beta \geq 2|\alpha|\cos(2\pi/11) + \frac{1}{|\alpha|} \geq 2 \cdot \sqrt{\frac{2|\alpha|\cos(2\pi/11)}{|\alpha|}} = 2.594229\ldots > 76/33.$$

6.4. An interlude. We recall some facts that will be used heavily in the sequel. There is always a formula:

$$(p-1)\mathscr{M}(\beta) = (p-X)\sum \mathscr{M}(\alpha_i) + \sum \mathscr{M}(\alpha_i - \alpha_j), \tag{1}$$

(This is Eq. 3.9 of Cassels, his argument is similar to that in Lemma 5.2.1.) We often use this equation in the following way. Suppose that the X non-zero terms break up into sets of size X_j consisting of equal terms. Then, since $\mathscr{M}(\alpha_i - \alpha_j) \geq 1$ if $\alpha_i \neq \alpha_j$, we deduce that

$$\begin{aligned}(p-1)\mathscr{M}(\beta) &\geq (p-X)\sum \mathscr{M}(\alpha_i) + \frac{1}{2}\sum X_j(X - X_j)\\ &= (p-X)\sum \mathscr{M}(\alpha_i) + \frac{1}{2}\left(X^2 - \sum X_j^2\right).\end{aligned} \tag{2}$$

We also note the following lemma, whose proof is obvious.

Lemma 6.4.1. *Suppose that at least Y of the α_i are equal to α. Then we may — after subtracting α from each α_i — assume that $X \leq p - Y$.*

Finally, we note the following.

Lemma 6.4.2. *Suppose that $p \geq 13$. Then we may assume that $X \leq \frac{p-1}{2}$ and $\lambda = 0$.*

Proof. The Corollary to Lemma 1 of Cassels states that if $\mathscr{M}(\beta) < \frac{1}{4}(p+3)$ then at least $\frac{p+1}{2}$ of the α_i are equal to each other. By Lemma 6.4.1 it follows that we can assume that $X \leq \frac{p-1}{2}$. Hence, we need only compute that

$$\frac{(p+3)}{4} \geq 4 > 23/6 > \mathscr{M}(\beta).$$

□

6.5. The case when $X = 4$, and $p \geq 11$. By Lemma 6.0.1, we may write

$$\beta = \zeta\alpha + \zeta^{-1}\overline{\alpha} + \zeta^i\gamma + \zeta^{-i}\overline{\gamma}.$$

If α and γ are roots of unity, then we are done by Corollary 4.2.12. Thus, we may assume that $\mathscr{N}(\alpha) \geq 2$, and hence that $\mathscr{M}(\alpha) = \mathscr{M}(\overline{\alpha}) \geq 3/2$. If γ is not equal to α or $\overline{\alpha}$, then $\{\alpha, \overline{\alpha}\}$ are certainly both distinct from $\{\gamma, \overline{\gamma}\}$. Hence evaluating $\mathscr{M}$ on the corresponding differences is at least one. Using Eq. 1, we deduce that

$$(p-1)\mathscr{M}(\beta) \geq (p-4)(3/2 \cdot 2 + 2) + 4,$$

and hence, if $p \geq 11$, that $\mathscr{M}(\beta) \geq 3.9 > 23/6$. This contradicts Lemma 5.1.1. Suppose that $\gamma = \alpha$. If α is not real, then α and γ are distinct from $\overline{\alpha}$ and $\overline{\gamma}$, and hence

$$(p-1)\mathscr{M}(\beta) \geq (p-4)(3/2 \cdot 4) + 4,$$

from which we deduce a contradiction as above. If $\gamma = \alpha$ *is* real, then

$$\beta = \alpha\left(\zeta + \zeta^{-1} + \zeta^i + \zeta^{-i}\right).$$

Since α and $\left(\zeta + \zeta^{-1} + \zeta^i + \zeta^{-i}\right)$ lie in disjoint Galois extensions, the maximal conjugate of β is the product of the maximal conjugate of α and the maximal conjugate of the second factor. Since $p > 5$, the latter factor cannot be written as a sum of a smaller number of roots of unity, and hence its maximum is at least $(\sqrt{3} + \sqrt{7})/2$, by Corollary 4.2.12. Yet, since $\mathscr{M}(\alpha) \geq 3/2$, at least one conjugate of α has absolute value $\geq \sqrt{2}$, and hence

$$\boxed{\beta} \geq \frac{\sqrt{14} + \sqrt{6}}{2} = 3.095573\ldots > 76/33.$$

6.6. The case when $X = 5$, and $p \geq 11$. Once more by Lemma 6.0.1, we may write that

$$\beta = \zeta\alpha + \zeta^i\gamma + \delta + \zeta^{-i}\overline{\gamma} + \zeta^{-1}\overline{\alpha}.$$

If α, δ, and γ are roots of unity, then we are done by Corollary 4.2.12. We break up our argument into various subcases.

6.6.1. $X = 5$ and $\mathscr{M}(\alpha) = \mathscr{M}(\gamma) = 1$, $\mathscr{M}(\delta) \geq 3/2$ If $\alpha = \gamma$ are both real, then, after replacing β by $-\beta$ if necessary, they are both one, and

$$\beta = \delta + \left(\zeta + \zeta^{-1} + \zeta^i + \zeta^{-i}\right).$$

We deduce that

$$(p-1)\mathscr{M}(\beta) \geq (p-5)(3/2 + 4) + 4.$$

This implies that $\mathscr{M}(\beta) \geq 4$ if $p \geq 13$. By computation, if $p = 11$, there exist two conjugates of the right-hand side, one positive and one negative, both of which have absolute value at least

$$2\cos(2\pi/11) + 6\cos(3\pi/11) = 1.397877\ldots.$$

On the other hand, there exists a conjugate of δ with absolute value at least $\sqrt{2}$, and hence there exists a conjugate of β with absolute value at least

$$\sqrt{2} + 2\cos(2\pi/11) + 6\cos(3\pi/11) = 2.812090\ldots > 2.303030\ldots = 76/33.$$

Thus we may assume that either α is real and γ is not, or that they are both not real. Thus δ is distinct from the four terms $\{\alpha, \overline{\alpha}, \gamma, \overline{\gamma}\}$ and either $\{\alpha, \overline{\alpha}\}$ has no intersection with $\{\gamma, \overline{\gamma}\}$ or $\{\alpha, \gamma\}$ has no intersection with $\{\overline{\alpha}, \overline{\gamma}\}$. In either case, we deduce that

$$(p-1)\mathscr{M}(\beta) \geq (p-5)(3/2+4) + 8,$$

which implies that $\mathscr{M}(\beta) \geq 4.1 > 23/6$.

6.6.2. $X = 5$ and $\mathscr{M}(\alpha) \geq 3/2$. We break this case up into further subcases.

(1) $\mathscr{M}(\gamma) = \mathscr{M}(\delta) = 1$: Clearly the terms involving α are distinct from the other terms, and hence

$$(p-1)\mathscr{M}(\beta) \geq 6(p-5) + 6,$$

and thus $\mathscr{M}(\beta) \geq 4.2 > 23/6$.

(2) $\mathscr{M}(\delta) \geq 3/2$, and $\mathscr{M}(\gamma) = 1$: In this case,

$$(p-1)\mathscr{M}(\beta) \geq (p-5)(3/2 \cdot 3 + 2) + 6,$$

which implies that $\mathscr{M}(\beta) \geq 4.5 > 23/6$.

(3) $\mathscr{M}(\gamma) \geq 3/2$, $\mathscr{M}(\delta) = 1$: In this case,

$$(p-1)\mathscr{M}(\beta) \geq (p-5)(3/2 \cdot 4 + 1) + 4,$$

and thus $\mathscr{M}(\beta) \geq 4.6 > 23/6$.

(4) $\mathscr{M}(\alpha_i) \geq 3/2$ for all i: In this case,

$$(p-1)\mathscr{M}(\beta) \geq (p-5)(3/2 \cdot 5),$$

and hence $\mathscr{M}(\beta) \geq 4.5 > 23/6$.

6.7. The case when $X = 6$, $p \geq 11$, and $\lambda = 0$. If $X = 6$, then Lemma 5.1.1 no longer applies when $p = 11$. We consider this possibility at the end of this subsection. Thus, we assume that

$$\beta = \alpha_i\zeta^i + \alpha_j\zeta^j + \alpha_k\zeta^k + \overline{\alpha_i}\zeta^{-i} + \overline{\alpha_j}\zeta^{-j} + \overline{\alpha_k}\zeta^{-k}.$$

Again, we break up into subcases.

6.7.1. $X = 6$, all the α_i are roots of unity. If all the α_i are the same, they must be (after changing the sign of β if necessary) equal to 1. We compute in this case that

$$(p-1)\mathscr{M}(\beta) = (p-6)6.$$

If $p \neq 11, 13$, then $\mathscr{M}(\beta) \geq 4.125 > 23/6$. Otherwise, we may write

$$\beta = 2\cos(2\pi i/p) + 2\cos(2\pi j/p) + 2\cos(2\pi k/p).$$

Note that $(i, p) = (j, p) = (k, p) = 1$. Without loss of generality, we may assume that $i = 1$. The smallest value of $\boxed{\beta}$ for $p = 11$ or $p = 13$ of this kind may easily be computed to be

$$-2(\cos(4\pi/11) + \cos(8\pi/11) + \cos(12\pi/11)) = 2.397877\ldots,$$
$$\frac{1+\sqrt{13}}{2} = -2(\cos(4\pi/13) + \cos(12\pi/13) + \cos(16\pi/13)) = 2.302775\ldots,$$

the former of which is larger than $76/33$, the latter which is on our list. The second smallest number for $p = 13$ is $3.148114\ldots > 76/33$.

Suppose that one of the α_i is not real. Then α_i is certainly distinct from $\overline{\alpha_i}$, and either $\alpha_j \neq \overline{\alpha_j}$ or α_j and $\overline{\alpha_j}$ are both distinct from α_i and $\overline{\alpha_i}$, and similarly with k. It follows that there are at least 9 pairs of numbers which are distinct, the minimum occurring when $\alpha_i = \alpha_j = \alpha_k$ or when $\alpha_j = \alpha_k = \pm 1$. In either case, we find that

$$(p-1)\mathscr{M}(\beta) \geq (p-6)6 + 9,$$

and hence $\mathscr{M}(\beta) \geq 3.9 > 23/6$.

Finally, suppose that all the α_i are real, but that they are not all equal. Then, up to sign,

$$\beta = 2\cos(2\pi i/p) + 2\cos(2\pi j/p) - 2\cos(2\pi k/p).$$

In this case, we compute that $(p-1)\mathscr{M}(\beta) \geq (p-6)6 + 8$, which is larger than $23/6$ if $p \neq 11$. If $p = 11$, we enumerate the possibilities directly, and find that the smallest value of $\boxed{\beta}$ is

$$2\cos(2\pi/11) - 2\cos(8\pi/11) - 2\cos(16\pi/11) = 3.276858\ldots > 76/33.$$

6.7.2. $X = 6$, and $\mathscr{M}(\alpha_i) \geq 3/2$. If $\mathscr{M}(\alpha_j) \geq 3/2$ also then

$$(p-1)\mathscr{M}(\beta) \geq (p-6)8,$$

and hence $\mathscr{M}(\beta) \geq 4$. Thus we may assume that $\mathscr{M}(\alpha_j) = \mathscr{M}(\alpha_k) = 1$. In this case, there are clearly at least 8 distinct pairs, and thus

$$(p-1)\mathscr{M}(\beta) \geq (p-6)7 + 8,$$

and hence $\mathscr{M}(\beta) \geq 4.3 > 23/6$.

6.8. The case when $X \geq 7$, and $p \geq 11$. Note that we make no assumptions on λ in this case. Write $\beta = \sum_S \alpha_i \zeta^i$. From Eq. 2, we deduce that

$$(p-1)\mathscr{M}(\beta) \geq X(p-X) + \frac{1}{2}\left(X^2 - \sum X_j^2\right).$$

If $p \geq 13$, then by Lemma 6.4.2, we may assume that $X \leq (p-1)/2$. In particular, this implies that $p \geq 17$. In this case, the inequality

$$(p-1)\mathscr{M}(\beta) \geq X(p-X)$$

already implies that $\mathscr{M}(\beta) \geq 4.375 > 23/6$. Hence we may reduce to the case when $p = 11$. By Lemma 6.4.1, we may assume that $X_j \leq 11 - X$. We consider the various possibilities:

(1) Suppose that $X = 7$. Then $X_j \leq 4$, and hence $\sum X_j^2 \leq 25$, and

$$10\mathscr{M}(\beta) \geq 7(11-7) + \frac{1}{2}(49-25) = 40,$$

and $\mathscr{M}(\beta) \geq 4 > 23/6$.

(2) Suppose that $X = 8$. Then $X_j \leq 3$, and hence $\sum X_j^2 \leq 22$, and

$$10\mathscr{M}(\beta) \geq 8(11-8) + \frac{1}{2}(64-22) = 45,$$

and $\mathscr{M}(\beta) \geq 4.5 > 23/6$.

(3) Suppose that $X = 9$. Then $X_j \leq 2$, and hence $\sum X_j^2 \leq 17$, and

$$10\mathscr{M}(\beta) \geq 9(11-9) + \frac{1}{2}(81-17) = 50,$$

and $\mathscr{M}(\beta) \geq 5 > 23/6$.

(4) Suppose that $X = 10$. Then $X_j \leq 1$, and hence $\sum X_j^2 \leq 10$, and

$$10\mathscr{M}(\beta) \geq 10(11-10) + \frac{1}{2}(100-10) = 55,$$

and $\mathscr{M}(\beta) \geq 5.5 > 23/6$.

6.9. The case when $X = 6$, $p = 11$, and $\lambda \neq 0$. Write $\beta = \sum_S \alpha_i \zeta^i$. Since $\lambda \neq 0$, it must be the case that either α_i or α_{-i} is non-zero. Moreover, by cardinality reasons, at least one of these must be zero, and hence $\lambda = \alpha_i - \overline{\alpha_{-i}} = \alpha_i$. Thus, in this case, it must be the case that

$$\beta = \alpha + \lambda \sum_T \zeta^i,$$

where T is a subset of S of cardinality 5 such that $T \cup \{-T\} \cup \{0\} = S$. Moreover, $\alpha - \overline{\alpha} = \lambda$, and $\lambda \cdot \sqrt{-1}$ is real. If λ is not a root of unity, then

$$10\mathscr{M}(\beta) \geq (11-6)(3/2 \cdot 5 + 1),$$

and hence $\mathscr{M}(\beta) \geq 4.25 \geq 23/6$. Hence λ is a root of unity, which must be equal (after changing the sign of β) to $\sqrt{-1}$. Clearly α is not equal to $\sqrt{-1}$. Hence

$$\mathscr{M}(\beta) \geq (11-6)(5+\mathscr{M}(\alpha))+5 = 30+5\mathscr{M}(\alpha).$$

It follows that $\mathscr{M}(\alpha) < 8/5 < 2$, and thus α is the sum of at most two roots of unity. If α is a root of unity, then $\overline{\alpha} = \alpha^{-1}$, and hence

$$\alpha - \alpha^{-1} = \lambda = \sqrt{-1}.$$

This implies that $\alpha = \zeta_{12}$ or ζ_{12}^5. In this case we may check every possibility for β (the set of possible T has cardinality 2^5 since it requires a choice of one of $\{i, -i\}$ for each non-zero $i \mod 11$), and the smallest such (largest conjugate) is:

$$\zeta_{12} + \zeta_4\left(\zeta_{11}^{-1} + \zeta_{11}^2 + \zeta_{11}^{-3} + \zeta_{11}^{-4} + \zeta_{11}^{-5}\right) = 2.524337\ldots > 2.303030\ldots = 76/33.$$

Suppose that $\mathscr{N}(\alpha) = 2$. Then either $\mathscr{M}(\alpha) = 3/2$ and α is a root of unity times $(1+\sqrt{5})/2$, or $\mathscr{M}(\alpha) \geq 5/3 > 8/5$. Hence we may now assume that $\alpha = (1+\sqrt{5})/2 \cdot \xi$ for a root of unity ξ. We now obtain the equation

$$\left(\frac{1+\sqrt{5}}{2}\right)(\xi - \xi^{-1}) = \sqrt{-1}.$$

From this equation we deduce that $\xi = \zeta_{20}$ or ζ_{20}^9. Again, we check the possibilities for β, the smallest being:

$$\left(\frac{1+\sqrt{5}}{2}\right)\zeta_{20} + \zeta_4\left(\zeta_{11}^{-1} + \zeta_{11}^2 + \zeta_{11}^{-3} + \zeta_{11}^{-4} + \zeta_{11}^{-5}\right) = 3.197154\ldots > 76/33.$$

This completes the proof of Theorem 5.0.13.

7. An Analysis of the Field $\mathbf{Q}(\zeta_{84})$

In order to progress further, we require some more precise analysis of certain elements α in the field $\mathbf{Q}(\zeta_{84})$ with $\mathscr{M}(\alpha)$ small.

Lemma 7.0.1. *Suppose that $\alpha \in \mathbf{Q}(\zeta_7)$ satisfies $\mathscr{M}(\alpha) \leq 4$. Then, up to sign and rescaling by a 7^{th} root of unity, either*:

(1) $\alpha = 0$ *or* $\alpha = 1$, *and* $\mathscr{M}(\alpha) = 0$ *or* 1.
(2) $\alpha = 1 + \zeta_7^i$ *with* $i \neq 0$, *and* $\mathscr{M}(\alpha) = 5/3$.
(3) $\alpha = 1 - \zeta_7^i$ *with* $i \neq 0$, *and* $\mathscr{M}(\alpha) = 7/3$.
(4) $\alpha = 1 + \zeta_7^i + \zeta_7^j$ *with* (i, j) *distinct and non-zero, and* $\mathscr{M}(\alpha) = 2$.
(5) $\alpha = 1 + \zeta_7^i - \zeta_7^j$ *with* (i, j) *distinct and non-zero, and* $\mathscr{M}(\alpha) = 10/3$.
(6) $\alpha = 2$ *and* $\mathscr{M}(\alpha) = 4$.
(7) $\alpha = \zeta_7^i + \zeta_7^j + \zeta_7^k - 1$ *with* (i, j, k) *distinct and non-zero, and* $\mathscr{M}(\alpha) = 4$.

Proof. Write $\alpha = \sum a_i \zeta_7^i$, where $a_i \in \mathbf{Z}$. We may assume that all the a_i are non-negative, and that at least one a_i is equal to 0. Suppose that A_i of the a_i are equal to i. Then

$$6\mathscr{M}(\alpha) = \sum (a_i - a_j)^2 = \sum (i-j)^2 A_i A_j.$$

Suppose that $\mathscr{M}(\alpha) \leq 4$. From the inequality $48 \geq 12\mathscr{M}(\alpha) \geq n^2 A_n A_0$, we deduce that $A_n = 0$ if $n \geq 7$. It is easy to enumerate the partitions of $7 = \sum A_i$ satisfying the inequality $24 \geq \sum (i-j)^2 A_i A_j$. We write A as $(A_0, A_1, \ldots)$, showing only up until the last nonzero value, and find a strict inequality for

$$A \in \{(7), (1,6), (2,5), (3,4), (4,3), (5,2), (6,1), (2,4,1), (1,5,1), (1,4,2)\}$$

(giving cases (1), (1), (2), (4), (4), (2), (1), (5), (3) and (5) of the statement, respectively) and equality for $A \in \{(6,0,1), (3,3,1), (1,3,3), (1,0,6)\}$ (giving cases (6),(7),(7) and (6) of the statement, respectively). The result follows. □

Corollary 7.0.2. *Suppose that $\alpha \in \mathbf{Q}(\zeta_7)$ satisfies $\mathscr{N}(\alpha) \geq 4$, then $\mathscr{M}(\alpha) \geq 4$.*

Lemma 7.0.3. *Suppose that $\alpha \in \mathbf{Q}(\zeta_{21})$ satisfies $\mathscr{M}(\alpha) < 17/6$. Then, up to sign and a 21^{st} root of unity, either*:

(1) α is a sum of at most three roots of unity.
(2) α lies in the field $\mathbf{Q}(\zeta_7)$.
(3) $\alpha = \zeta_7^i + \zeta_7^j + \zeta_7^k - \zeta_3$, where (i, j, k) are distinct and non-zero, and $\mathscr{M}(\alpha) = 5/2$.
(4) $\alpha = 1 + \zeta_7^i - (\zeta_7^j + \zeta_7^k)\zeta_3$, where (i, j, k) are distinct and non-zero, and $\mathscr{M}(\alpha) = 8/3$.
(5) $\alpha = \zeta_7^i + \zeta_7^j + (\zeta_7^j + \zeta_7^k)\zeta_3$, where (i, j, k) are distinct, and $\mathscr{M}(\alpha) = 8/3$.

Proof. We may write $\alpha = \gamma + \delta\zeta_3$, where

$$\mathscr{M}(\alpha) = \frac{1}{2}(\mathscr{M}(\gamma) + \mathscr{M}(\delta) + \mathscr{M}(\gamma - \delta)).$$

We may assume that $\gamma \neq \delta$, since otherwise $\alpha = -\zeta_3^2\gamma$ is, up to a root of unity, in $\mathbf{Q}(\zeta_7)$, giving case (2). In general, we note that $\alpha = (\gamma - \delta) - \delta\zeta_3^2 = (\delta - \gamma)\zeta_3 - \gamma\zeta_3^2$, Hence, after re-ordering if necessary, we may assume that

$$\mathscr{N}(\gamma - \delta) \geq \mathscr{N}(\gamma) \geq \mathscr{N}(\delta).$$

Assume that $\mathscr{M}(\alpha) \leq 17/6$. If $\mathscr{N}(\delta) \geq 3$, then $\mathscr{M}(\gamma - \delta)$, $\mathscr{M}(\gamma)$, and $\mathscr{M}(\delta)$ are all ≥ 2, and thus $\mathscr{M}(\alpha) \geq 3$, a contradiction. We consider various other cases.

(i) $\mathscr{N}(\delta) = 1$ and $\mathscr{N}(\gamma) \leq 2$: In this case, $\mathscr{N}(\alpha) \leq 3$, giving case (1).
(ii) $\mathscr{N}(\delta) = 1$ and $\mathscr{N}(\gamma) = 3$: If $\mathscr{N}(\gamma - \delta) \geq 4$, then $\mathscr{M}(\alpha) \geq (1 + 2 + 10/3)/2 \geq 19/6$. Thus $\mathscr{N}(\gamma - \delta) = 3$. In particular,

$$(\delta - \gamma) + (\gamma) - (\delta) = 0$$

is a vanishing sum of length $3 + 1 + 3$. The only primitive vanishing sums in $\mathbf{Q}(\zeta_7)$ have length 7 or 2. Thus, the expression above must be a multiple of the vanishing sum

$$1 + \zeta_7 + \zeta_7^2 + \zeta_7^3 + \zeta_7^4 + \zeta_7^5 + \zeta_7^6 + \zeta_7^7 = 0.$$

After scaling, we may assume that $\delta = -1$, and thus $\gamma = \zeta_7^i + \zeta_7^j + \zeta_7^k$ for some triple (i, j, k) that are all distinct and non-zero. Since $\delta - \gamma$ is sum of 3 distinct 7^{th} roots of unity in this case, we deduce that $\mathscr{M}(\gamma) = \mathscr{M}(\delta - \gamma) = 2$, and hence $\mathscr{M}(\alpha) = 5/2$. We are thus in case (3).

(iii) $\mathscr{N}(\delta) = 1$ and $\mathscr{N}(\gamma) \geq 4$: It follows immediately that $\mathscr{M}(\alpha) \geq (1 + 10/3 + 10/3)/2 = 23/6$, a contradiction.

(iv) $\mathscr{N}(\delta) = 2$ and $\mathscr{N}(\gamma) = 2$: If $\mathscr{N}(\delta - \gamma) \geq 4$, then $\mathscr{M}(\alpha) \geq (5/3+5/3+10/3) = 20/6$. If $\mathscr{N}(\delta - \gamma) = 3$, we obtain a vanishing sum

$$(\delta - \gamma) + (\gamma) - (\delta) = 0$$

of length 7, and hence $\gamma = \zeta_7^i + \zeta_7^j$ and $\delta = -(\zeta_7^k + \zeta_7^l)$, where (i, j, k, l) are all distinct. In this case, $\mathscr{M}(\gamma) = \mathscr{M}(\delta) = 5/3$, and $\gamma - \delta$ is minus a sum of three distinct 7^{th} roots of unity, and so $\mathscr{M}(\gamma - \delta) = 2$. It follows that $\mathscr{M}(\alpha) = 8/3$ and we are in case (4). If $\mathscr{N}(\delta - \gamma) = 2$, then the above sum is a vanishing sum of length 6. It follows that it is composed of vanishing subsums of length 2, from which it easily follows that $\delta = \zeta_7^j + \zeta_7^k$ and $\gamma = \zeta_7^i + \zeta_7^j$. In this case, $\mathscr{M}(\delta) = \mathscr{M}(\gamma) = 5/3$, and $\mathscr{M}(\delta - \gamma) = 2$, and thus $\mathscr{M}(\alpha) = 8/3$, giving case (5).

(v) $\mathscr{N}(\delta) = 2$ and $\mathscr{N}(\gamma) \geq 3$: It follows immediately that $\mathscr{M}(\alpha) \geq (5/3+2+2)/2 = 17/6$, a contradiction. □

Corollary 7.0.4. *Suppose that $\alpha \in \mathbf{Q}(\zeta_{21})$ satisfies $\mathscr{M}(\alpha) < 9/4$ and $\mathscr{N}(\alpha) \geq 3$, then $\alpha = 1 + \zeta_7^i + \zeta_7^j$ where (i, j) are distinct and non-zero and $\mathscr{M}(\alpha) = 2$.*

Lemma 7.0.5. *Suppose that $\alpha \in \mathbf{Q}(\zeta_{21})$ satisfies $\mathscr{M}(\alpha) < 23/6$, then $\mathscr{N}(\alpha) \leq 5$.*

Proof. As before we may write $\alpha = \gamma + \delta\zeta_3$ and we may assume that $\mathscr{N}(\gamma - \delta) \geq \mathscr{N}(\gamma) \geq \mathscr{N}(\delta)$. If $\mathscr{N}(\delta) \leq 2$, then we are done unless $\mathscr{N}(\gamma - \delta) \geq \mathscr{N}(\gamma) \geq 4$. In this case, we deduce from Corollary 7.0.2 that $\mathscr{M}(\gamma - \delta) \geq 4$ and $\mathscr{M}(\gamma) \geq 4$, from which it follows directly that $\mathscr{M}(\alpha) \geq (4 + 4 + 1)/2 > 23/6$. Suppose that $\mathscr{N}(\delta) \geq 3$. If $\mathscr{N}(\delta - \gamma) \geq 4$, then $\mathscr{M}(\alpha) \geq (2 + 2 + 4)/2 = 4 > 23/6$. Thus, we may assume that

$$\mathscr{N}(\delta) = \mathscr{N}(\gamma) = \mathscr{N}(\delta - \gamma) = 3.$$

Let us consider the resulting vanishing sum

$$(\delta - \gamma) + (\gamma) - (\delta) = 0.$$

It has length $9 = 7 + 2$. After scaling α by a root of unity, we may assume that this sum is (having re-arranged the order of the roots of unity):

$$(1 + \zeta_7 + \zeta_7^2 + \cdots + \zeta_7^6) + (1 - 1) = 0.$$

At least one of the three terms must be contained within the first sum. Furthermore, the $(1 - 1)$ sum cannot be contained within a single term. Hence, we obtain the following two possibilities (up to symmetry):

$$\begin{aligned} \gamma &= 1 + \zeta_7^i + \zeta_7^j, \quad \delta = 1 - \zeta_7^k - \zeta_7^l, \quad \delta - \gamma = 1 + \zeta_7^m + \zeta_7^n, \\ \gamma &= 2 + \zeta_7^i, \qquad \delta = 1 - \zeta_7^j - \zeta_7^k, \quad \delta - \gamma = \zeta_7^l + \zeta_7^m + \zeta_7^n, \end{aligned}$$

where (i, j, k, l, m, n) are distinct and non-zero. In the first case, we notice that since $1 + \zeta_3 = -\zeta_3^2$, in fact $\mathscr{N}(\alpha) \leq 5$. In the second case, we compute that $\mathscr{M}(\alpha) = (13/3 + 10/3 + 2)/2 = 29/6 > 23/6$. □

Lemma 7.0.6. *Suppose that* $\alpha \in \mathbf{Q}(\zeta_{21})$ *satisfies* $\mathcal{N}(\alpha) = 2$, *then* $\mathcal{M}(\alpha) \geq 2$, *or* $\mathcal{M}(\alpha) = 5/3$.

Proof. Again we write $\alpha = \gamma + \delta\zeta_3$. If either γ or δ is zero, then up to a root of unity $\alpha \in \mathbf{Q}(\zeta_7)$ and we can apply Lemma 7.0.1. If neither γ nor δ is zero, then they must both be roots of unity, hence, $\mathcal{M}(\alpha) = (2 + \mathcal{M}(\gamma - \delta))/2$. Notice that $\gamma - \delta$ is not a root of unity, because there are no vanishing sums

$$(\gamma - \delta) + (\delta) - (\gamma) = 0$$

of length 3 in $\mathbf{Q}(\zeta_7)$. Since α is not a root of unity, $\gamma \neq \delta$, and hence $\mathcal{M}(\alpha) = (2 + \mathcal{M}(\gamma - \delta))/2 \geq 2$. □

Lemma 7.0.7. *Suppose that* $\alpha \in \mathbf{Q}(\zeta_{84})$, *that* $\mathcal{M}(\alpha) < 9/4$, *and that* $\mathcal{N}(\alpha) \geq 3$, *then* $\alpha = \zeta_{84}^i(1 + \zeta_7^j + \zeta_7^k)$.

Proof. Write $\alpha = \gamma + \zeta_4\delta$. Since $\mathcal{N}(\alpha) \geq 3$ it follows that one of γ or δ is not a root of unity. If γ and δ are both nonzero, then $\mathcal{M}(\beta) \geq 1 + 3/2 > 9/4$, hence γ or δ is zero, and up to a root of unity $\alpha \in \mathbf{Q}(\zeta_{21})$. The result then follows from Corollary 7.0.4. □

Lemma 7.0.8. *The elements* $\alpha \in \mathbf{Q}(\zeta_{84})$ *such that* $\mathcal{M}(\alpha) < 17/6$ *are, up to roots of unity, either a sum of at most* 3 *roots of unity, or are, up to a root of unity, one of the exceptional forms in* $\mathbf{Q}(\zeta_{21})$, *specifically*:

(1) $\alpha = \zeta_7^i + \zeta_7^j + \zeta_7^k - \zeta_3$, *where* (i, j, k) *are distinct and non-zero, and* $\mathcal{M}(\alpha) = 5/2$.
(2) $\alpha = 1 + \zeta_7^i - (\zeta_7^j + \zeta_7^k)\zeta_3$, *where* (i, j, k) *are distinct and non-zero, and* $\mathcal{M}(\alpha) = 8/3$.
(3) $\alpha = \zeta_7^i + \zeta_7^j + (\zeta_7^j + \zeta_7^k)\zeta_3$, *where* (i, j, k) *are distinct and non-zero, and* $\mathcal{M}(\alpha) = 8/3$.

Moreover, if $\mathcal{N}(\alpha) = 2$, *then either* $\mathcal{M}(\alpha) \geq 2$ *or* $\mathcal{M}(\alpha) = 5/3$.

Proof. If $\alpha = \gamma + \delta\zeta_4$ with $\gamma, \delta \in \mathbf{Q}(\zeta_{21})$, then $\mathcal{M}(\alpha) = \mathcal{M}(\gamma) + \mathcal{M}(\delta)$. If $\gamma = 0$ or $\delta = 0$ the problem reduces immediately to Lemma 7.0.3. So we may assume that $\gamma \neq 0$ and $\delta \neq 0$. By symmetry, we may assume that $\mathcal{M}(\gamma) \geq \mathcal{M}(\delta) \geq 1$. It follows that $\mathcal{M}(\gamma) < 11/6 < 2$, and hence $\mathcal{N}(\gamma) \leq 2$. If $\mathcal{N}(\delta) = \mathcal{N}(\gamma) = 2$, then $\mathcal{M}(\alpha) \geq 10/3$. If $\mathcal{N}(\alpha) = 2$, then either γ and δ are non-zero, in which case $\mathcal{M}(\alpha) = 2$, or we may assume that $\alpha \in \mathbf{Q}(\zeta_{21c})$, and apply Lemma 7.0.3. □

Lemma 7.0.9. *Suppose that* $\alpha \in \mathbf{Q}(\zeta_{84})$. *Then either* $\mathcal{M}(\alpha) \geq 23/6$, *or* $\mathcal{N}(\alpha) \leq 5$.

Proof. Assume that $\mathcal{M}(\alpha) < 23/6$. Write $\alpha = \gamma + \delta\zeta_4$. If γ and δ are both non-zero, then we may assume that $17/6 > \mathcal{M}(\gamma) \geq \mathcal{M}(\delta) \geq 1$. Suppose that $\mathcal{N}(\delta) \geq 2$. Then $\mathcal{M}(\delta) \geq 5/3$, and hence $\mathcal{M}(\gamma) \leq 13/6 < 5/2$, from which we deduce from Lemma 7.0.8 that $\mathcal{N}(\gamma) \leq 3$, and hence $\mathcal{N}(\alpha) \leq 5$. Suppose that $\mathcal{N}(\delta) = 1$. Since $\mathcal{M}(\gamma) \leq 17/6$, we see that $\mathcal{N}(\gamma) \leq 4$ and $\mathcal{N}(\alpha) \leq 5$. Thus we may assume that one of γ or δ is zero, and hence, up to a root of unity, $\alpha \in \mathbf{Q}(\zeta_{21})$. The result follows by Lemma 7.0.5. □

Corollary 7.0.10. *Suppose that* $\beta \in \mathbf{Q}(\zeta_{84})$ *is real. Then either* $\boxed{\beta} \geq 76/33$, $\mathcal{N}(\beta) \leq 2$, *or* β *is either a conjugate of* $\frac{1}{2}(\sqrt{3} + \sqrt{7})$ *or* $1 + 2\cos(2\pi/7)$.

Proof. The result is an immediate consequence of Lemma 7.0.9, combined with Corollary 4.2.12 and Lemma 5.1.1. □

8. Final Reductions

In this section, we complete the proof of Theorem 1.0.5 by proving the following.

Theorem 8.0.1. *If β is a real cyclotomic integer such that $\beta \in \mathbf{Q}(\zeta_{420})$, $\mathscr{N}(\beta) \geq 3$, and $\boxed{\beta} < 76/33$, then either $\beta \in \mathbf{Q}(\zeta_{84})$, or $\boxed{\beta} = \sqrt{5}$ or $(1+\sqrt{5})/\sqrt{2}$.*

The technique used in this section is to apply the style of arguments from Cassels "first case" which we used in Sect. 6 applied to the prime 5. The arguments are much more detailed than those in Sect. 6 and we exploit our understanding of small numbers in $\mathbf{Q}(\zeta_{84})$. As in Sect. 6 we will use ζ to denote an arbitrary p^{th} root of unity, and in this section $p = 5$. Recall that, on the other hand, ζ_5 denotes the particular 5^{th} root of unity $e^{2\pi i/5}$.

Note that if $\mathscr{N}(\beta) \leq 5$, the result follows from Corollary 4.2.12. We consider various cases in turn.

8.1. The case when $X = 1$ and $p = 5$. The same proof in §6 holds verbatim.

8.2. The case when $X = 2$ and $p = 5$. Since $p = 5$, we may assume by Lemma 6.0.1 that $\lambda = 0$, and hence $\beta = \zeta\alpha + \zeta^{-1}\overline{\alpha}$. Suppose that $\boxed{\alpha} \geq \sqrt{3}$. Then, as in §6, we deduce that

$$\boxed{\beta} \geq 2\boxed{\alpha}\cos(\pi/5) \geq 2\sqrt{3}\cos(\pi/5) = 2.802517\ldots > 2.303030\ldots = 76/33.$$

It follows immediately from Lemma 6 of Cassels [7] that if $\boxed{\alpha} < \sqrt{3}$, then either $\mathscr{N}(\alpha) \leq 2$, or α is a root of unity times one of

$$\frac{1}{2}\left(1+\sqrt{-7}\right), \qquad \frac{1}{2}\left(\sqrt{-3}+\sqrt{5}\right).$$

If $\mathscr{N}(\alpha) \leq 2$, then $\mathscr{N}(\beta) \leq 4$ and we are done. Suppose that, up to a root of unity, α is one of the two exceptional cases. Since $\alpha \in \mathbf{Q}(\zeta_{84})$, only the first possibility may occur. Writing α as a root of unity times $(1+\sqrt{-7})/2$ and enumerating all possibilities, the smallest possible element thus obtained is

$$\left|\frac{\sqrt{7}+\sqrt{-1}}{2}\cdot\zeta_5^2 + \frac{\sqrt{7}-\sqrt{-1}}{2}\cdot\zeta_5^{-2}\right| = \frac{1}{2}\sqrt{13+3\sqrt{5}+\sqrt{14(5+\sqrt{5})}}$$
$$= 2.728243\ldots > 76/33.$$

8.3. The case when $X = 3$, $p = 5$, and $\lambda = 0$. We have that $\beta = \zeta\alpha + \gamma + \zeta^{-1}\overline{\alpha}$. From Eq. 2, we deduce that

$$\begin{aligned} 4\mathscr{M}(\beta) &= 2\mathscr{M}(\alpha) + 2\mathscr{M}(\overline{\alpha}) + 2\mathscr{M}(\gamma) + \mathscr{M}(\alpha-\overline{\alpha}) + \mathscr{M}(\alpha-\gamma) + \mathscr{M}(\overline{\alpha}-\gamma) \\ &= 4\mathscr{M}(\alpha) + 2\mathscr{M}(\gamma) + 2\mathscr{M}(\alpha-\gamma) + \mathscr{M}(\alpha-\overline{\alpha}). \end{aligned}$$

We consider various subcases.

8.3.1. $X = 3$, $p = 5$, $\lambda = 0$, *and* $\alpha = \gamma$. We deduce that α is real, and hence $\beta = \alpha(\zeta + 1 + \zeta^{-1})$. It follows that

$$\boxed{\beta} = \boxed{\alpha} \cdot \boxed{1 + \zeta + \zeta^{-1}} = 2\cos(\pi/5)\boxed{\alpha} > 76/33$$

if $\boxed{\alpha} \geq 2$. Thus $\boxed{\alpha} = 2\cos(\pi/n)$ for some $n|84$, and we quickly determine that the only $\boxed{\beta}$ in the range $[2, 76/33]$ is $(\sqrt{5}+1)/\sqrt{2}$.

8.3.2. $X = 3$, $p = 5$, $\lambda = 0$, $\alpha \neq \gamma$, $\mathcal{N}(\gamma) \leq 2$, $\mathcal{N}(\alpha) \geq 3$, *and* α *is not real.* Since α is not real, $\mathcal{M}(\alpha - \overline{\alpha}) \geq 1$. Since $\mathcal{N}(\alpha) \geq 3$, if $\mathcal{N}(\gamma) = 1$ then $\mathcal{N}(\alpha - \gamma) \geq 2$, whereas if $\mathcal{N}(\alpha - \gamma) = 1$ then $\mathcal{N}(\gamma) \geq 2$. Thus

$$4\mathcal{M}(\beta) \geq 4\mathcal{M}(\alpha) + 2\left(\frac{5}{3} + 1\right) + 1,$$

and hence $\mathcal{M}(\alpha) < 9/4$. It follows from Lemma 7.0.7 (and the fact that $\alpha \in \mathbf{Q}(\zeta_{84})$) that $\alpha = \zeta_{84}^i(1 + \zeta_7^j + \zeta_7^k)$. Moreover, we may assume that either $\gamma = 1$ or $\gamma = \zeta_{84}^l + \zeta_{84}^{-l}$ for some l. Enumerating all possibilities with $\alpha = \zeta_{84}^i(1 + \zeta_7^j + \zeta_7^k)$ (without the assumption that α is not real), we find that the smallest largest conjugate is:

$$2\cos(\pi/5)(1 + 2\cos(2\pi/7)) - 1 = 2.635689\ldots > 76/33.$$

8.3.3. $X = 3$, $p = 5$, $\lambda = 0$, $\alpha \neq \gamma$, $\mathcal{N}(\gamma) \leq 2$, $\mathcal{N}(\alpha) \geq 3$, *and* α *is real.* Suppose that $\mathcal{N}(\gamma)$ and $\mathcal{N}(\alpha - \gamma)$ are both at least two. It follows from Lemma 7.0.7 that $\alpha = \zeta_{84}^i(1 + \zeta_7^j + \zeta_7^k)$, which was considered above. Thus, we may assume that at least one of $\mathcal{N}(\gamma)$ or $\mathcal{N}(\alpha - \gamma)$ equal to one. We show that $\mathcal{N}(\alpha) \leq 4$. If $\mathcal{N}(\gamma) = 1$, and $\mathcal{N}(\alpha) \geq 5$, then $\mathcal{N}(\alpha - \gamma) \geq 4$, and thus $\mathcal{M}(\alpha)$ and $\mathcal{M}(\alpha - \gamma)$ are $\geq 8/3$ by Lemma 7.0.8. Yet then

$$\mathcal{M}(\beta) \geq 8/3 + (8/3 + 1)/2 = 9/2 > 23/6.$$

Conversely, if $\mathcal{N}(\alpha - \gamma) = 1$, then by assumption, $\mathcal{N}(\gamma) \leq 2$, and so $\mathcal{N}(\alpha) \leq 3$. It follows by Lemma 4.1.3 that we assume that α is one of the following forms, up to sign:

(1) $1 + \zeta_{84}^i + \zeta_{84}^{-i}$,
(2) $\zeta_{84}^i + \zeta_{84}^{-i} + \zeta_{84}^j + \zeta_{84}^{-j}$,
(3) $\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^3 + \zeta_{84}^{15}$,
(4) $\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^3 + \zeta_{84}^{27}$,

whereas we may assume that $\gamma = \zeta_{84}^k + \zeta_{84}^{-k}$. (Here we are using the fact that $\alpha \in \mathbf{Q}(\zeta_{84})$ to eliminate some of the other exceptional possibilities in Lemma 4.1.3.) In cases 3 and 4 every β has a conjugate of absolute value at least 3. In the first two cases, $\sqrt{5}$ occurs as a (degenerate) possibility for β. The second smallest largest conjugate is also degenerate, and occurs with $\alpha = 2$ and $\gamma = 1$, where $\boxed{\beta} = 2+2\cos(2\pi/5) = 2.618033\ldots > 76/33$.

8.3.4. $X = 3$, $p = 5$, $\lambda = 0$, $\alpha \neq \gamma$, $\mathcal{N}(\gamma) \leq 2$, *and* $\mathcal{N}(\alpha) \leq 2$. We may let $\alpha = \zeta_{84}^i + \zeta_{84}^j$ and $\gamma = \zeta_{84}^k + \zeta_{84}^{-k}$. The smallest such largest conjugate (besides a degenerate $\sqrt{5}$) is

$$4\cos(\pi/5)\cos(3\pi/7) + 2\cos(\pi/7) = 2.522030\ldots > 2.303030\ldots = 76/33.$$

8.3.5. $X = 3$, $p = 5$, $\lambda = 0$, *and* $\mathscr{N}(\gamma) \geq 3$. By Corollary 7.0.10, we may assume that either $\gamma = \frac{1}{2}(\sqrt{3}+\sqrt{7})$, $1+2\cos(2\pi/7)$, or $\gamma = \boxed{\gamma} \geq 76/33$. In the latter case, we choose a conjugate of ζ such that $\zeta\alpha + \zeta^{-1}\overline{\alpha} > 0$, and then $\beta > \gamma > 76/33$. Since $\mathscr{M}(\frac{1}{2}(\sqrt{3}+\sqrt{7})) = 5/2$ and $\mathscr{M}(1+2\cos(2\pi/7)) = 2$, we may deduce that $\mathscr{M}(\gamma) \geq 2$. Thus

$$4\mathscr{M}(\beta) \leq 4\mathscr{M}(\alpha) + 4 + 2\mathscr{M}(\alpha - \gamma) + \mathscr{M}(\alpha - \overline{\alpha}).$$

The case $\gamma = \alpha$ has already been considered. Thus $\mathscr{M}(\alpha - \gamma) \geq 1$, and hence, since $\mathscr{M}(\beta) < 23/6$, we deduce that $\mathscr{M}(\alpha) < 7/3$. By Lemma 7.0.8, it follows that $\mathscr{N}(\alpha) \leq 3$. Enumerating over all α with $\mathscr{N}(\alpha) \leq 3$ and $\gamma = \frac{1}{2}(\sqrt{3}+\sqrt{7})$ or $1+2\cos(2\pi/7)$, all the smallest conjugates (with $\alpha \neq 0$) are at least 3, except for

$$1 + 2\cos(2\pi/7) + 2\cos(2\pi/5) = 2.865013\ldots > 76/33.$$

8.4. The case when $X = 3$, $p = 5$, *and* $\lambda \neq 0$. It follows, choosing ζ appropriately, that

$$\beta = \alpha + \lambda(\zeta + \zeta^2),$$

where, as usual, $\alpha - \overline{\alpha} = \lambda$. We do a brute force computation for all α with $\mathscr{N}(\alpha) \leq 3$. Note that if $\mathscr{N}(\alpha) = 3$, we may assume that $\alpha = \zeta_{84}^i + \zeta_{84}^j + \zeta_{84}^k$, where i is a divisor of 84. The smallest resulting largest conjugate that arises is

$$\begin{aligned}\zeta_{84}^7 + (\zeta_{84}^7 - \zeta_{84}^{-7})(\zeta^3 + \zeta^4) &= 2\cos(\pi/30) + 2\cos(13\pi/30)\\ &= 2.404867\ldots \geq 2.303030\ldots = 76/33.\end{aligned}$$

We note that

$$4\mathscr{M}(\beta) = (5-3)(\mathscr{M}(\alpha) + 2\mathscr{M}(\lambda)) + 2\mathscr{M}(\alpha - \lambda).$$

Since $\alpha - \lambda = \overline{\alpha}$, we may write this as

$$\mathscr{M}(\beta) = \mathscr{M}(\alpha) + \mathscr{M}(\lambda).$$

Since $\lambda \neq 0$, it follows that $\mathscr{M}(\beta) < 17/6$. We deduce by Lemma 7.0.8 that either $\mathscr{N}(\alpha) \leq 3$, or α is one of three specific forms given in that lemma, that is, we may assume that α is, up to a root of unity, one of the following:

(1) $\alpha = \zeta_{84}^n(\zeta_7^i + \zeta_7^j + \zeta_7^k - \zeta_3)$, where (i, j, k) are distinct and non-zero modulo 7.
(2) $\alpha = \zeta_{84}^n(1 + \zeta_7^i - (\zeta_7^j + \zeta_7^k)\zeta_3)$, where (i, j, k) are distinct and non-zero modulo 7.
(3) $\alpha = \zeta_{84}^n(\zeta_7^i + \zeta_7^j + (\zeta_7^j + \zeta_7^k)\zeta_3)$, where (i, j, k) are distinct modulo 7.

We compute in all cases that the smallest $\alpha + (\alpha - \overline{\alpha})(\zeta + \zeta^2)$ which occur are all ≥ 3.5, or α real and $\lambda = 0$.

8.5. The case when $X = 4$, $p = 5$, and $\lambda \neq 0$. Since $X = 4$, by Lemma 6.4.1, we may assume that all the α_i are distinct. We are assuming that $\lambda \neq 0$. Then $\alpha - \overline{\alpha} = \lambda$. Write

$$\beta = \alpha + \alpha_1\zeta + \alpha_2\zeta^2 + \alpha_3\zeta^3.$$

Then $\alpha_1 = \lambda$, $\alpha_2 - \overline{\alpha_3} = \lambda$. Hence

$$\beta = \alpha + (\alpha - \overline{\alpha})\zeta + (\overline{\gamma} + \alpha - \overline{\alpha})\zeta^2 + \gamma\zeta^3.$$

There is some symmetry in this expression. If we let $\gamma = \overline{\theta} + \alpha - \overline{\alpha}$, then

$$\overline{\gamma} + \alpha - \overline{\alpha} = \theta.$$

This sends the pair $(\alpha - \gamma, \overline{\gamma} + \alpha - \overline{\alpha}) \mapsto (\overline{\alpha} - \overline{\theta}, \theta)$. It follows that the two terms γ and θ can be interchanged in various arguments. We compute that

$$\begin{aligned} 4\mathscr{M}(\beta) &= \mathscr{M}(\alpha) + \mathscr{M}(\alpha - \overline{\alpha}) + \mathscr{M}(\overline{\gamma} + \alpha - \overline{\alpha}) + \mathscr{M}(\gamma) + \mathscr{M}(\alpha) \\ &\quad + \mathscr{M}(\alpha - \gamma) + \mathscr{M}(\alpha - \gamma) + \mathscr{M}(\gamma) + \mathscr{M}(\overline{\gamma} + \alpha - \overline{\alpha}) + \mathscr{M}(\alpha - \overline{\alpha}) \\ &= 2\mathscr{M}(\alpha) + 2\mathscr{M}(\gamma) + 2\mathscr{M}(\alpha - \overline{\alpha}) + 2\mathscr{M}(\alpha - \gamma) + 2\mathscr{M}(\overline{\gamma} + \alpha - \overline{\alpha}). \end{aligned}$$

If $\alpha = \gamma$ then not every term is distinct, which is a contradiction, and hence all the five terms in the sum above are non-zero.

Lemma 8.5.1. *At least one of $\mathscr{N}(\alpha)$ and $\mathscr{N}(\gamma)$ is ≥ 3.*

Proof. We compute all numbers such that $\mathscr{N}(\alpha) \leq 2$ or $\mathscr{N}(\gamma) \leq 2$. We carry out the calculation as follows. Suppose that $\alpha = \zeta_{84}^i + \zeta_{84}^j$ and $\gamma = \zeta_{84}^k + \zeta_{84}^l$. Then we may assume that $l \geq k$, and that either:

(1) $i = 1$,
(2) $i = 3$ and $3|j$,
(3) $i = 4$ and $2|j$,
(4) $i = 7$ and $7|j$,
(5) $i = 12$ and $6|j$,
(6) $i = 21$ and $21|j$,
(7) $i = 28$ and $14|j$.
(8) $i = 84$ and $42|j$.

We remark that this computation also covers the cases where $\mathscr{N}(\alpha) = 1$ or $\mathscr{N}(\gamma) = 1$, since $\zeta_{84}^k = \zeta_{84}^{k-14} + \zeta_{84}^{k+14}$. The smallest largest conjugate which occurs is $\sqrt{5}$, which occurs in case 7, and the second smallest largest conjugate is $2\cos(\pi/30) + 2\cos(13\pi/30)$, in case 4. Thus we have shown that at least one of $\mathscr{N}(\alpha)$ or $\mathscr{N}(\gamma)$ is ≥ 3. By symmetry, the same argument also proves that at least one of $\mathscr{N}(\alpha)$ or $\mathscr{N}(\theta)$ is ≥ 3. □

Lemma 8.5.2. *Either at least three of the terms $\mathscr{M}(\alpha)$, $\mathscr{M}(\gamma)$, $\mathscr{M}(\alpha - \overline{\alpha})$, $\mathscr{M}(\alpha - \gamma)$ and $\mathscr{M}(\overline{\gamma} + \alpha - \overline{\alpha})$ above are roots of unity, or at least two terms are roots of unity and at least two other terms are the sum of at most two roots of unity.*

Proof. If there is at most one root of unity, then, by Lemma 7.0.8,

$$\mathscr{M}(\beta) \geq 1/2(5/3 \cdot 4 + 1) = 23/6.$$

If there are only two roots of unity, and only one other term which can be expressed as the sum of exactly two roots of unity, then

$$\mathscr{M}(\beta) \geq 1/2(2 \cdot 2 + 5/3 + 1 + 1) = 23/6.$$

□

We now consider possible pairs of terms which are roots of unity.

(1) α and γ: The result follows from Lemma 8.5.1.
(2) α and $\alpha - \overline{\alpha}$: The latter is, up to a sign that we fix, $\sqrt{-1} = \zeta_{84}^{21}$, the former is therefore, up to conjugation, ζ_{84}^{7}. By Lemma 8.5.2, either one of the other terms is a root of unity, or at least two terms are the sum of at most two roots of unity. If γ is a root of unity, we reduce immediately to case 1. If $\theta = \overline{\gamma} + \alpha - \overline{\alpha}$ is a root of unity, we also reduce to case 1, by symmetry. If $\alpha - \gamma$ is a root of unity, then $\mathscr{N}(\gamma) \leq 2$. On the other hand, if at least two terms are the sum of at most two roots of unity, then either $\mathscr{N}(\theta)$ or $\mathscr{N}(\gamma)$ is ≤ 2, and by symmetry, we may assume that $\mathscr{N}(\gamma) \leq 2$, and we are done by Lemma 8.5.1.
(3) α and $\alpha - \gamma$: We deduce immediately that $\mathscr{N}(\gamma) \leq 2$, and hence, we are done by Lemma 8.5.1.
(4) α and $\theta = \overline{\gamma} + \alpha - \overline{\alpha}$: This reduces to case 1 by symmetry.
(5) γ and $\alpha - \overline{\alpha}$: The latter, after changing the sign of β, is $\sqrt{-1} = \zeta_{84}^{21}$. By Lemma 8.5.2, either one of the other terms is a root of unity, or at least two terms are the sum of at most two roots of unity. Note that $\theta = \overline{\gamma} + \alpha - \overline{\alpha}$ is equal to $\overline{\gamma} + \zeta_{84}^{21}$. Suppose there is another root of unity. We consider various subcases:
   (a) θ is a root of unity: From the three term vanishing sum $\theta - \overline{\gamma} - \zeta_{84}^{21} = 0$ we deduce that $\gamma = \zeta_{84}^{49}$ or ζ_{84}^{77}. After conjugating we may assume it is the first. Then

$$\beta = \alpha + \zeta_{84}^{21}\zeta + \zeta_{84}^{35}\zeta^2 + \zeta_{84}^{49}\zeta^3.$$

   Now

$$\mathscr{N}(\beta) = 3/2 + \mathscr{M}(\alpha)/2 + \mathscr{M}(\alpha - \zeta_{84}^{49})/2.$$

   Either $\mathscr{M}(\alpha) \leq 23/10$ or $\mathscr{M}(\alpha - \zeta_{84}^{49}) \leq 23/10$. Since $23/10 < 5/2$, it follows from Lemma 7.0.8 that either $\mathscr{N}(\alpha) \leq 3$ or $\mathscr{N}(\alpha - \zeta_{84}^{49}) \leq 3$. Enumerating over all α with $\mathscr{N}(\alpha) = 3$, we find that the smallest value of the expression above is

$$|(1+\zeta_{84}^{42}+\zeta_{84}^{49})+\zeta_{84}^{21}\zeta_5^3+\zeta_{84}^{35}\zeta_5+\zeta_{84}^{49}\zeta_5^4| = \sqrt{1+4\cos^2(\pi/15)} = 2.1970641\ldots,$$

   however, the β occurring here is not real, since we did not impose the condition (in our computation) that $\alpha - \overline{\alpha} = \zeta_{84}^{21}$. The second smallest value that occurs is

$$|(1+\zeta_{84}^{35}+\zeta_{84}^{42})+\zeta_{84}^{21}\zeta_5^4+\zeta_{84}^{35}\zeta_5^3+\zeta_{84}^{49}\zeta_5^2| = \sqrt{1+4\cos^2(\pi/30)} = 2.226273\ldots$$

which is also not real. The third smallest value that occurs is $2.574706\ldots > 2.303030\cdots = 76/33$. If $\mathcal{N}(\alpha - \zeta_{84}^{49}) = 3$, the smallest value thus obtained is

$$|(\zeta_{84}^{49} + 1 + \zeta_{84}^{28} + \zeta_{84}^{56}) + \zeta_{84}^{21}\zeta_5^3 + \zeta_{84}^{35}\zeta_5 + \zeta_{84}^{49}\zeta_5^4| = \sqrt{1 + 4\cos^2(\pi/15)},$$

the second smallest value is, as above, $\sqrt{1 + 4\cos^2(\pi/30)}$, and the third smallest value is (once more) $2.574706\cdots > 2.303030\cdots = 76/33$.

(b) α is a root of unity: Since α and γ are roots of unity, we are reduced to case 1.

(c) $\alpha - \gamma$ is a root of unity: If γ and $\alpha - \gamma$ are roots of unity, then $\mathcal{N}(\alpha) \leq 2$, and we are done by Lemma 8.5.1.

Hence we may assume that all other terms are not roots of unity, and hence there are at least two terms which are sums of at most 2 roots of unity. We consider various possibilities:

(a) Suppose that $\mathcal{N}(\alpha) = 2$. Then we are done by Lemma 8.5.1.

(b) We may assume that $\gamma - \alpha$ and θ are both at most the sum of two roots of unity. Write $\gamma = \zeta_{84}^i$ and $\alpha = \zeta_{84}^i + \zeta_{84}^j + \zeta_{84}^k$ with $i \leq j \leq k$. After conjugating, we may assume that i divides 84. Enumerating all the possibilities, we find that the smallest number of this form is $2\cos(\pi/30) + 2\cos(13\pi/30) = 2.404867\ldots > 2.303030\ldots = 76/33$.

(6) γ and $\alpha - \gamma$: Since $\mathcal{N}(\alpha) \leq 2$ and $\mathcal{N}(\gamma) = 1$, we are done by Lemma 8.5.1.

(7) γ and $\theta := \overline{\gamma} + (\alpha - \overline{\alpha})$: If $\mathcal{N}(\alpha - \overline{\alpha}) = 1$ then we are back in case 5. If $\mathcal{N}(\alpha) = 1$ we are back in case 1. If $\mathcal{N}(\alpha - \gamma) = 1$ we are back in case 6. Thus, by Lemma 8.5.2 it follows that at least one of $\mathcal{N}(\alpha)$ or $\mathcal{N}(\alpha - \gamma)$ is equal to 2. In the first case, we are done by Lemma 8.5.1. In the second case, we may let $\gamma = \zeta_{84}^i$ with $i|84$ and $\alpha = \zeta_{84}^i + \zeta_{84}^j + \zeta_{84}^k$, and we are reduced to the computation in the final section of part 5.

(8) $\alpha - \overline{\alpha}$ and $\alpha - \gamma$: If either $\mathcal{N}(\alpha) = 1$ or $\mathcal{N}(\gamma) = 1$, then the other is the sum of at most two roots of unity, and we are done by Lemma 8.5.1. If θ is a root of unity, then by symmetry we can reduce to case 5. Thus, by Lemma 8.5.2, we may assume that at least two of γ, α and θ are the sums of at most two roots of unity. By Lemma 8.5.1, we are done unless $\mathcal{N}(\gamma) = \mathcal{N}(\theta) = 2$, and $\mathcal{N}(\alpha) \geq 3$. Since $\alpha - \gamma$ is a root of unity, it must be the case that $\mathcal{N}(\alpha) = 3$. Since $\alpha - \overline{\alpha}$ is a purely imaginary root of unity, it must be $\pm\sqrt{-1}$. Changing the sign of β if neccessary, we may assume that $\alpha - \overline{\alpha} = \zeta_{84}^{21}$. It follows that

$$(\alpha - \zeta_{84}^7) - \overline{(\alpha - \zeta_{84}^7)} = 0,$$

and hence $\alpha - \zeta_{84}^7$ is real. Since $2 \leq \mathcal{M}(\alpha - \zeta_{84}^7) \leq 4$, and α lies in $\mathbf{Q}(\zeta_{84})$, it follows that $\alpha - \zeta_{84}^7$ is of the form:

(a) $\zeta_{84}^i + \zeta_{84}^{-i}$,

(b) $\zeta_{84}^i + \zeta_{84}^{-i} + 1$,

(c) $\zeta_{84}^i + \zeta_{84}^{-i} - 1$,

(d) $\zeta_{84}^i + \zeta_{84}^{-i} + \zeta_{84}^j + \zeta_{84}^{-j}$,

(e) Galois conjugate to $\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^3 + \zeta_{84}^{15}$ or $\zeta_{84}^{-9} + \zeta_{84}^{-7} + \zeta_{84}^3 + \zeta_{84}^{27}$.

In all five cases, we let $\gamma = \zeta_{84}^j$ and enumerate all possibilities. The smallest largest conjugate is a relatively gargantuan $2.989043\ldots$.

(9) $\alpha - \overline{\alpha}$ and θ: By symmetry, we are reduced to case 5.
(10) $\alpha - \gamma$ and θ: By symmetry, we are reduced to case 6.

8.6. The case when $X = 4$, $p = 5$, and $\lambda = 0$. We have

$$\beta = \zeta\alpha + \zeta^{-1}\overline{\alpha} + \zeta^2\gamma + \zeta^{-2}\overline{\gamma}.$$

Note that every term is distinct. We have

$$4\mathscr{M}(\beta) = 2\mathscr{M}(\alpha) + 2\mathscr{M}(\gamma) + 2\mathscr{M}(\alpha - \gamma) + 2\mathscr{M}(\alpha - \overline{\gamma}) + \mathscr{M}(\alpha - \overline{\alpha}) + \mathscr{M}(\gamma - \overline{\gamma}).$$

Lemma 8.6.1. *At least one of $\mathscr{N}(\alpha)$ or $\mathscr{N}(\gamma)$ is at least* 3.

Proof. We compute all numbers such that $\mathscr{N}(\alpha) \leq 2$ or $\mathscr{N}(\gamma) \leq 2$. We carry out the calculation as follows. Suppose that $\alpha = \zeta_{84}^i + \zeta_{84}^j$ and $\gamma = \zeta_{84}^k + \zeta_{84}^l$. Then we may assume that $l \geq k$, and that either:

(1) $i = 1$,
(2) $i = 3$ and $3|j$,
(3) $i = 4$ and $2|j$,
(4) $i = 7$ and $7|j$,
(5) $i = 12$ and $6|j$,
(6) $i = 21$ and $21|j$,
(7) $i = 28$ and $14|j$.
(8) $i = 84$ and $42|j$.

We remark that this computation also covers the cases where $\mathscr{N}(\alpha) = 1$ or $\mathscr{N}(\gamma) = 1$, since $\zeta_{84}^k = \zeta_{84}^{k-14} + \zeta_{84}^{k+14}$. We find that the smallest largest conjugates are $\sqrt{5}$, which is on our list, and $2\cos(\pi/30) + 2\cos(13\pi/30) \geq 76/33$. □

We note there is a symmetry between (α, γ) and $(\overline{\alpha}, \overline{\gamma})$. Without loss of generality, we assume that $\mathscr{N}(\alpha) \geq \mathscr{N}(\gamma)$, and that $\mathscr{N}(\alpha) \geq 3$.

Lemma 8.6.2. *At least one of the following holds*:

(1) At least two of $\{\gamma, \alpha - \gamma, \overline{\alpha} - \gamma\}$ are roots of unity.
(2) Both $\alpha - \overline{\alpha}$ and $\gamma - \overline{\gamma}$ are roots of unity, and every element in $\{\gamma, \alpha - \gamma, \overline{\alpha} - \gamma\}$ is a sum of at most two roots of unity.

Proof. Note that $\mathscr{N}(\alpha) \geq 3$, and so $\mathscr{M}(\alpha) \geq 2$. Suppose that $\alpha - \overline{\alpha}$ and $\gamma - \overline{\gamma}$ are not both roots of unity, and at most one of $\{\gamma, \alpha - \gamma, \overline{\alpha} - \gamma\}$ is a root of unity. then

$$\mathscr{M}(\beta) \geq (1 + 5/3 + 5/3 + 2)/2 + (1 + 5/3)/4 = 23/6.$$

Conversely, if $\alpha - \overline{\alpha}$ and $\gamma - \overline{\gamma}$ are both roots of unity, at most one of $\{\gamma, \alpha - \gamma, \overline{\alpha} - \gamma\}$ is a root of unity, and at most two of $\{\gamma, \alpha - \gamma, \overline{\alpha} - \gamma\}$ are the sum of 2 roots of unity, then

$$\mathscr{M}(\beta) \geq (1 + 5/3 + 2 + 2)/2 + (1 + 1)/4 = 23/6.$$

□

8.6.3. $X = 4$, $p = 5$, $\lambda = 0$, and two of $\{\gamma, \alpha - \gamma, \overline{\alpha} - \gamma\}$ are roots of unity. If γ is a root of unity, then so is $\overline{\gamma}$. Since at least one of $\alpha - \gamma$ and $\alpha - \overline{\gamma}$ is also a root of unity, we deduce that $\mathcal{N}(\alpha) \leq 2$, and we are done by Lemma 8.6.1. Thus we may assume that $\mathcal{N}(\alpha - \gamma) = \mathcal{N}(\overline{\alpha} - \gamma) = 1$. Recall that by Lemma 6.4.1, we may assume that α and γ are distinct from their conjugates. Write $\alpha - \gamma = \zeta_{84}^{i}$ and $\overline{\alpha} - \gamma = \zeta_{84}^{j}$. We deduce that $\alpha - \overline{\gamma} = \zeta_{84}^{-j}$. Thus

$$\alpha - \overline{\alpha} = (\alpha - \gamma) - (\overline{\alpha} - \gamma) = \zeta_{84}^{i} - \zeta_{84}^{j}$$

and

$$\gamma - \overline{\gamma} = (\alpha - \overline{\gamma}) - (\alpha - \gamma) = \zeta_{84}^{-j} - \zeta_{84}^{i}$$

are purely imaginary. Since $\zeta_{84}^{i} - \zeta_{84}^{j}$ is purely imaginary, it follows that

$$\zeta_{84}^{i} - \zeta_{84}^{j} + \zeta_{84}^{-i} - \zeta_{84}^{-j} = 0.$$

This is a vanishing sum of length four, so it must be comprised of two subsums of length 2. If $\zeta_{84}^{i} = \zeta_{84}^{j}$ then $\alpha - \overline{\alpha} = 0$, which is a contradiction. If $\zeta_{84}^{i} = \zeta_{84}^{-j}$, then $\gamma - \overline{\gamma} = 0$, which is also a contradiction. Thus $\zeta_{84}^{i} = -\zeta_{84}^{-i}$ and $\zeta_{84}^{j} = -\zeta_{84}^{-j}$. It follows that $\zeta_{84}^{i} = \pm\sqrt{-1}$ and $\zeta_{84}^{j} = \pm\sqrt{-1}$. Yet, for each of these possibilities, it is the case that ζ_{84}^{i} is equal to ζ_{84}^{j} or ζ_{84}^{-j}, and hence either $\alpha = \overline{\alpha}$ or $\gamma = \overline{\gamma}$, a contradiction.

8.6.4. $X = 4$, $p = 5$, $\lambda = 0$, at most one of $\{\gamma, \alpha - \gamma, \overline{\alpha} - \gamma\}$ is a root of unity. It follows from Lemma 8.6.2 that either $\mathcal{N}(\gamma) + \mathcal{N}(\alpha - \gamma) \leq 3$ or $\mathcal{N}(\gamma) + \mathcal{N}(\alpha - \overline{\gamma}) \leq 3$. If $\mathcal{N}(\gamma) = 1$, then we let $\gamma = \zeta_{84}^{i}$, and $\alpha = \zeta_{84}^{i} + \zeta_{84}^{j} + \zeta_{84}^{k}$ and enumerate, or $\alpha = \zeta_{84}^{-i} + \zeta_{84}^{j} + \zeta_{84}^{k}$ and enumerate. If $\mathcal{N}(\gamma) = 2$, we let $\gamma = \zeta_{84}^{i} + \zeta_{84}^{j}$, and $\alpha = \zeta_{84}^{i} + \zeta_{84}^{j} + \zeta_{84}^{k}$, or $\zeta_{84}^{-i} + \zeta_{84}^{-j} + \zeta_{84}^{k}$. Enumerating over all such possibilities, we find that the smallest largest conjugates that arise are $\sqrt{5}$ and $2\cos(\pi/30) + 2\cos(13\pi/30)$.

8.7. The case when $X = 5$ and $p = 5$. In this case, by Lemma 6.4.1, we can reduce to the case that $X < 5$. This completes the proof of Theorem 1.0.5

9. $\mathscr{M}(\beta)$ is Discrete in an Interval Beyond 2

We have seen that the values of $\boxed{\beta}$ for real cyclotomic integers are discrete in $[0, 76/33]$ away from a limit point (from below) at 2. In this section, we show (now for all cyclotomic integers) that $\mathscr{M}(\beta)$ is discrete in $[0, 9/4]$, away from a limit point (from both sides) at 2. This is an easy consequence of the following theorem.

Theorem 9.0.1. *Let β be a cyclotomic integer, and suppose that $\mathscr{M}(\beta) < 9/4$. Then, up to a root of unity, either*:

(1) $\beta = 0$ *or* $\beta = 1$.
(2) β *is a sum of two roots of unity.*
(3) $\beta = 1 + \zeta_7^{i} + \zeta_7^{j}$, *where* (i, j) *are distinct and non-zero.*
(4) $\beta = \zeta_3^{\pm 1} - (\zeta_5^{i} + \zeta_5^{j})$, *where* (i, j) *are distinct and non-zero.*

Proof. Our proof follows the same lines as the arguments in Sects. 5.2–8, although it is much easier. Assume that $\mathscr{M}(\beta) < 9/4$. Suppose that $\beta \in \mathbf{Q}(\zeta_N)$, where N is the conductor of $\mathbf{Q}(\beta)$, and suppose that β is *minimal*, that is, no root of unity times β lies in a field of smaller conductor. Let $p^m \| N$, and write $\beta = \sum \alpha_i \zeta^i$, where ζ is a $p^{m\text{th}}$ root of unity and the $\alpha_i \in \mathbf{Q}(\zeta_M)$, for $N = pM$. If $p^2 | N$, then $\beta = \sum \mathscr{M}(\alpha_i)$. If this sum consists of at least three non-zero terms, then $\mathscr{M}(\beta) \geq 3$. If this sum consists of two non-zero terms, and at least one of the α_i is not a root of unity, then $\mathscr{M}(\beta) \geq 1 + 3/2 > 9/4$. Hence, either β is the sum of two roots of unity, or there is only one non-zero term, contradicting minimality. Thus we may suppose that N is squarefree.

Suppose that $p|N$ for $p > 7$. Since

$$\mathscr{M}(\beta) = 9/4 < \frac{11+1}{4},$$

by Lemma 1 of [7] we deduce that one can write β as a sum of $X \leq (p-1)/2$ non-zero terms. Suppose that $X \geq 3$. It follows from Eq. 2 that

$$(p-1)\mathscr{M}(\beta) \geq X(p-X) \geq 3(p-3),$$

from which it follows that $\mathscr{M}(\beta) \geq 12/5 > 9/4$. Thus we may assume that $X = 2$, and $\beta = \alpha + \zeta\gamma$. If α and γ are roots of unity, then β is a sum of two roots of unity. If at least one of α or γ is not a root of unity, then

$$(p-1)\mathscr{M}(\beta) \geq (p-2)(1+3/2),$$

and hence $\mathscr{M}(\beta) \geq 9/4$, a contradiction. Thus, we may assume that N divides 105.

Now let us consider $\beta \in \mathbf{Q}(\zeta_{105})$. Write $\beta = \sum \alpha_i \zeta^i$, and suppose there are X non-zero terms. We consider the various possible values of X, as in §8.

(1) If $X = 1$, then $\beta \in \mathbf{Q}(\zeta_{21})$. Hence the result follows from Corollary 7.0.4.

(2) If $X = 2$, then $\beta = \alpha + \gamma\zeta$, and

$$4\mathscr{M}(\beta) = 3\mathscr{M}(\alpha) + 3\mathscr{M}(\gamma) + \mathscr{M}(\alpha - \gamma).$$

If α and γ are roots of unity, then β is a sum of two roots of unity. If $\alpha = \gamma$ is not a root of unity, then $\mathscr{M}(\beta) \geq 9/4$. If α and γ are distinct, and at least one is not a root of unity, then

$$4\mathscr{M}(\beta) \geq 3(1 + 5/3) + 1,$$

and it follows easily that $\mathscr{M}(\beta) \geq 9/4$.

(3) If $X = 3$, $\beta = \sum \alpha_i \zeta^i$, then we may assume that not all the α_i are the same, since otherwise we may subtract $\sum \zeta^i \alpha$ from β and assume that $X = 2$. Thus, at least two of the $\alpha_i - \alpha_j$ are non-zero, and hence

$$4\mathscr{M}(\beta) \geq 2 \sum \mathscr{M}(\alpha_i) + 2.$$

If at least one of the α_i is not a root of unity, then $\mathscr{M}(\beta) \geq 7/3 > 9/4$. Thus, we may assume that all the α_i are roots of unity. Moreover, at least two of the α_i must coincide, since otherwise $4\mathscr{M}(\beta) \geq 6 + 3$ and thus $\mathscr{M}(\beta) \geq 9/4$. We may therefore assume, after multiplying by a root of unity, that

$$\beta = \alpha + \zeta^i + \zeta^j,$$

where (i, j) are distinct and non-zero, and α is a root of unity. Since

$$4\mathscr{M}(\beta) = 6 + 2\mathscr{M}(\alpha - 1),$$

we find that $\mathscr{M}(\beta) \geq 9/4$ unless $\alpha - 1$ is also a root of unity. If $\alpha - 1$ and α are both roots of unity then $\alpha = -\zeta_3^{\pm 1}$. Hence, up to a root of unity, $\beta = \zeta_3^{\pm 1} - (\zeta^i + \zeta^j)$.

(4) If $X = 4$, then we may assume that all the α_i are distinct. Then

$$4\mathscr{M}(\beta) \geq \sum \mathscr{M}(\alpha_i - \alpha_j) \geq 10,$$

and $\mathscr{M}(\beta) \geq 5/2 > 9/4$.

(5) If $X = 5$, we may subtract a multiple of $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$ to reduce to a previous case. □

Remark 9.0.2. The exceptional values (with $\mathscr{M}(\alpha) = 2$) occurring in Theorem 9.0.1 were already noticed by Cassels [7, Lemma 3].

The discreteness of $\mathscr{M}(\beta)$ away from 2 follows from the fact that, given an n^{th} root of unity ζ, we have

$$\mathscr{M}(1 + \zeta) = 2\left(1 + \frac{\mu(n)}{\varphi(n)}\right),$$

where $\mu(n)$ is the Möbius μ-function and $\varphi(n)$ is Euler's totient function — as n increases this converges to 2.

We deduce the following:

Corollary 9.0.3. *Let β be a real cyclotomic integer, and suppose that $\mathscr{M}(\beta) < 9/4$. Then, up to sign, either*:

(1) β is conjugate to $2\cos(2\pi/n)$ for some integer n.
(2) β is conjugate to $1 + 2\cos(2\pi/7)$.
(3) β is conjugate to $\eta := \zeta_{12} + \zeta_{20} + \zeta_{20}^{17} = 2\cos(\pi/30) + 2\cos(13\pi/30)$.

Proof. We use the fact (Lemma 4.1.3) that if β is totally real and $\mathscr{N}(\beta) \leq 3$, then, up to sign, $\beta = 0, 1, \eta, \zeta^i + \zeta^{-i}$, or $1 + \zeta^i + \zeta^{-i}$ (the sign is unnecessary in the first, third, or fourth cases). □

9.1. A general sparseness result on the set of values of $\mathscr{M}(\beta)$ for β a cyclotomic integer.

Theorem 9.1.1. *Let $\mathscr{L} \subset \mathbf{R}$ denote the closure of the set of real numbers of the form $\mathscr{M}(\beta)$ for cyclotomic integers β. Then $\mathscr{L}$ is a closed subset of $\mathbf{Q}$.*

Proof. If $U \subset \mathbf{R}$ is a set, let U^n for any positive integer n denote the set of sums of at most n elements of U. If U is closed, then so is U^n. Let $\mathscr{L}(d) \subset \mathscr{L}$ denote $\mathscr{L} \cap [0, d]$. Since $\mathscr{L}(1) = \{0, 1\}$, it suffices to show that there exists an integer m (depending on d) such that

$$\mathscr{L}(d + 1/2) \subset \mathscr{L}(d)^m \cup \mathbf{Q},$$

since then the result follows by induction. Let γ denote a point in $\mathscr{L}(d + 1/2)$. There exists a sequence β_k of cyclotomic integers with $\mathscr{M}(\beta_k) = \gamma_k$ such that $\lim_{\to} \gamma_k = \gamma$. We note the following theorem of Loxton [25, §6.1, p. 81]:

Theorem 9.1.2 (Loxton). *There exists a continuous increasing unbounded function $g(t)$ such that $\mathscr{M}(\beta) \geq g(\mathscr{N}(\beta))$. In particular, any bound on $\mathscr{M}(\beta)$ yields an upper bound on $\mathscr{N}(\beta)$.*

Since $\mathscr{M}(\beta_k) = \gamma_k$ converges to $\gamma \leq d + 1/2$, it follows that γ_k is bounded above by $d + 1$ for sufficiently large k. Without loss of generality, we may assume this bound holds for all k. It follows from Loxton's theorem that the β_k can be written as the sum of at most $m = m(d)$ roots of unity for some m. Let N_k denote the conductor of β_k. Recall that $\mathscr{M}(\alpha) \cdot [\mathbf{Q}(\alpha) : \mathbf{Q}] \in \mathbf{Z}$. If the N_k are bounded, then the fields $\mathbf{Q}(\beta_k)$ are of bounded degree, and hence the $\mathscr{M}(\beta_k) = \gamma_k$ have bounded denominators, and $\mathscr{M}(\beta) \in \mathbf{Q}$. Hence, we may assume that the conductors N_k grow without bound. Let $p_k^{n_k}$ denote the largest prime power divisor of N_k. For each k, we may write $\beta_k = \sum \alpha_i \zeta^i$, where the sum runs over a set of cardinality m (allowing some of the α_i to be zero). Assuming that β_k is minimal (which we may do without changing the value of $\mathscr{M}(\beta_k)$) we may assume that there are at least two non-zero α_i. We consider two cases:

(1) Suppose that $n_k > 1$ for infinitely many k. For such k, we have

$$\mathscr{M}(\beta_k) = \sum \mathscr{M}(\alpha_i).$$

Since at least two of the α_i are non-zero, $\mathscr{M}(\alpha_i) \leq \gamma_k - 1 < d$. Thus $\mathscr{M}(\alpha_i) \in \mathscr{L}(d)$, and $\mathscr{M}(\beta_k) \in \mathscr{L}(d)^m$. Since the latter is closed, we deduce that $\mathscr{M}(\beta) \in \mathscr{L}(d)^m$.

(2) Suppose that $n_k = 1$ for infinitely many k. We deduce that

$$(p_k - 1)\mathscr{M}(\beta_k) = (p_k - m) \sum \mathscr{M}(\alpha_i) + \sum \mathscr{M}(\alpha_i - \alpha_j).$$

Since at least two of the α_i are non-zero, we deduce that

$$\mathscr{M}(\alpha_i) \leq \left(\frac{p_k - 1}{p_k - m}\right) \cdot \gamma_k - 1 < d,$$

the last inequality holding for sufficiently large k (equivalently, p_k). Thus $\mathscr{M}(\alpha_i) \leq d$ for sufficiently large k. From the AM-GM inequality, we deduce that

$$\sum \mathscr{M}(\alpha_i - \alpha_j) \leq 2 \sum \mathscr{M}(\alpha_i) + 2 \sum \mathscr{M}(\alpha_j) \leq 4d \binom{m}{2}.$$

As k increases, therefore, the contribution of this term to $\mathscr{M}(\beta_k)$ converges to zero, and hence

$$\mathscr{M}(\beta) = \lim_{\to} \mathscr{M}(\beta_i) = \lim_{\to} \sum \mathscr{M}(\alpha_i),$$

and thus $\gamma = \mathscr{M}(\beta)$ lies in the closure of $\mathscr{L}(d)^m$. Since $\mathscr{L}(d)$ is closed, $\gamma \in \mathscr{L}(d)^m$. □

Remark 9.1.3. Since closed subsets of $\mathbf{Q}$ are very far from being dense, we see that this result is in stark contrast to the analogous set constructed out of $\mathscr{M}(\beta)$ for totally real integers β, which is dense in $[2, \infty)$.

10. Galois Groups of Graphs

Let Γ be a connected graph with $|\Gamma|$ vertices. Fix a vertex v of Γ, and let Γ_n denote the sequence of graphs obtained by adding a 2-valent tree of length $n - |\Gamma|$ to Γ at v. Let M_n denote the adjacency matrix of Γ_n, and let $P_n(x)$ denote the characteristic polynomial of M_n. By construction, Γ_n has n vertices, and thus the degree of $P_n(x)$ is n. The main result of this section is the following:

Theorem 10.0.1. *For any Γ, there exists an effective constant N such that for all $n \geq N$, either*:

(1) All the eigenvalues of M_n are of the form $\zeta + \zeta^{-1}$ for some root of unity ζ, and the graphs Γ_n are the Dynkin diagrams A_n or D_n.
(2) There exists at least one eigenvalue λ of M_n of multiplicity one such that $\mathbf{Q}(\lambda^2)$ is not abelian.

Remark 10.0.2. We shall also prove a stronger version of this result which only looks at the largest eigenvalue (Theorem 11.0.1). We include this result because, although Theorem 11.0.1 is also (in principle) effective, the bound on n arising in Theorem 10.0.1 is easily computed, and all our intended applications satisfy the conditions of Theorem 10.0.1.

Corollary 10.0.3. *For any Γ, there exists an effective constant N such that for all $n \geq N$, either*:

(1) Γ_n is the Dynkin diagram A_n or D_n.
(2) Γ_n is not the principal graph of a subfactor.

Proof. This is an immediate consequence of Theorem 10.0.1 and Lemma 3.0.7. □

10.1. Adjacency matrices. We begin by recalling some basic facts about the eigenvalues of M_n.

Lemma 10.1.1. *Let $x = t + t^{-1}$, and write $P_n(x) = F_n(t) \in \mathbf{Z}[t, t^{-1}]$.*

(1) The matrix M_n is symmetric and the roots of $P_n(x)$ are all real.
(2) The polynomials P_n satisfy the recurrence:

$$P_n(x) = x P_{n-1}(x) - P_{n-2}(x).$$

(3) There is a fixed Laurent polynomial $A(t) \in \mathbf{Z}[t, t^{-1}]$ such that:

$$F_n(t)\left(t - \frac{1}{t}\right) = t^n \cdot A(t) - t^{-n} \cdot A(t^{-1}).$$

We are particularly interested in the roots of $P_n(x)$ of absolute value larger than 2, or, equivalently, the real roots of $F_n(t)$ of absolute value larger than 1. The following facts will be useful to note.

Lemma 10.1.2. *Denote the roots of $P_n(x)$ by λ_i for $i = 1$ to n.*

(1) If the roots of $P_{n-1}(x)$ are μ_i for $i = 1$ to $n - 1$, then, with the natural ordering of the roots,

$$\lambda_1 \leq \mu_1 \leq \lambda_2 \leq \mu_2 \cdots \leq \mu_{n-1} \leq \lambda_n.$$

(2) *The number of roots of $P_n(x)$ of absolute value larger than 2 are bounded.*
(3) *The largest real root of $P_n(x)$ is bounded.*
(4) *For sufficiently large n, the real roots of $P_n(x)$ of absolute value larger than 2 are bounded uniformly away from 2.*

Proof. The first claim is the interlacing theorem; see ([14], Theorem 9.1.1). By Descartes' rule of signs, the polynomial $F_n(t)$ has a bounded number of real roots, which implies the second claim. The largest real root of $F_n(t)$ converges to the largest real root ρ_∞ of $A(t)$ (compare Lemma 12 of [26]) and hence the largest real root of $P_n(x)$ converges to $\lambda_\infty = \rho_\infty + \rho_\infty^{-1}$. The final claim follows immediately from the first two. □

We use the letter λ to refer to a root of $P_n(x)$, and the letter ρ to refer to the corresponding roots of $F_n(t)$, where $\lambda = \rho + \rho^{-1}$.

Lemma 10.1.3. *There exists a polynomial $B(t)$ such that for n larger than some effectively computable constant, every repeated root of $F_n(t)$ on the unit circle is a root of $B(t)$.*

Proof. The polynomial $A(t)$ is monic. In particular, if $A(t)$ has a root on the unit circle, then $A(t)$ has a factor $B(t)$ which is a reciprocal polynomial. It follows that we can write

$$t^n \cdot F_n(t)\left(t - \frac{1}{t}\right) = B(t)\left(t^{2n} \cdot C(t) - C(t^{-1})\right),$$

where $A(t) = B(t)C(t)$ and $C(t)$ has no roots on the unit circle. Suppose that $F_n(t)$ has a repeated root ρ on the unit circle. Then either ρ is a root of $B(t)$, or it is a root of $t^{2n}C(t) - C(t^{-1})$. Yet the absolute value of the derivative of this expression is, by the triangle inequality, greater than

$$2n|C(t)| - |C'(t)| - |C'(t^{-1})|.$$

Since $C(t)$ has no roots on the unit circle, for all n larger than some effectively computable constant this expression is positive. □

Lemma 10.1.4. *For all sufficiently large n, there exists a constant $K(\Gamma)$ such that*

$$\sum(\lambda^2 - 2)^2 = 2n + K(\Gamma).$$

Proof. Clearly $(\lambda^2 - 2)^2 = \rho^4 + 2 + \rho^{-4}$. Since there is a pair of inverse roots of $F_n(t)$ corresponding to every root λ of $P_n(x)$, it follows that $\sum(\lambda^2 - 2)^2 = 2n + \sum \rho^4$. The sum of the 4^{th} powers of the roots of $F_n(t)$ depends only on the first four coefficients of $F_n(t)$, which is clearly independent of n, when n is sufficiently large compared to $\deg(A)$. □

Recall that $\eta := 2\cos(\pi/30) + 2\cos(13\pi/30)$ has degree 8 over $\mathbf{Q}$.

Lemma 10.1.5. *The polynomials $\prod_{1,2,4}(x^2 - 3 - 2\cos(2\pi k/7))$ and $\prod_{i=1}^{8}(x^2 - 2 - \sigma_i\eta)$ divide $P_n(x)$ a uniformly bounded and effectively computable number of times.*

Proof. Since the polynomials in question have at least one real root larger than 2, the number of factors of $P_n(x)$ of this form is clearly at most the number of real roots of $P_n(x)$ of size larger than 2. □

Let us now complete the proof of Theorem 10.0.1. By Lemma 10.1.3, we deduce that for n sufficiently large, there is a uniformly bounded (with multiplicity) number of roots which have multiplicity ≥ 2. Moreover, if Γ_n is not A_n or D_n, then the number roots of the form $\zeta + \zeta^{-1}$ is also uniformly and effectively bounded, by the main theorem of [15]. Finally, the number of roots λ such that $\lambda^2 - 2 = 1 + 2\cos(2\pi/7)$ or η is also uniformly bounded. Let R denote the set of roots in any of these three categories. Clearly, we have

$$\sum_{\lambda \notin R} (\lambda^2 - 2)^2 \leq 2n + K(\Gamma).$$

On the other hand, by assumption, each $\lambda^2 - 2$ with $\lambda \notin R$ is a cyclotomic integer. If $\lambda^2 - 2 = \zeta + \zeta^{-1}$, then $\lambda = \zeta^{1/2} - \zeta^{-1/2}$ lies in R. If $\lambda^2 - 2 = 1 + 2\cos(2\pi/7)$ or $\lambda^2 - 2 = \eta$, then λ also lies in R. Thus, by Corollary 9.0.3, $\mathscr{M}(\lambda^2 - 2) \geq 9/4$ for all $\lambda \notin R$. Hence

$$2n + K(\Gamma) \geq \sum_{\lambda \notin R} (\lambda^2 - 2)^2 \geq \frac{9(n - |R|)}{4}.$$

Combining these two inequalities, we obtain a contradiction whenever $n \geq 4K(\Gamma)+9|R|$, as long as n is big enough for the conclusions of Lemma 10.1.3 and 10.1.4 to hold.

Remark 10.1.6. In practice, one can improve the bound on n by noting that the cyclotomic factors and repeated factors (that one knows explicitly) contribute to the sum $\sum(\lambda^2 - 2)^2$, thus enabling one to obtain a smaller bound on $\sum_{\notin R}(\lambda^2 - 2)^2$.

Remark 10.1.7. Suppose that $A(t)$ has exactly one root of absolute value larger than 1. Then the polynomials $P_n(x)$ have a unique root larger than 2, and $P_n(x)$ factors as a Salem polynomial times a product of cyclotomic polynomials. (A Salem polynomial is an irreducible polynomial with a unique root of absolute value larger than 1.) Similarly, if Γ is bipartite, and $A(t)$ has a pair of roots (equal up to sign) of absolute value larger than 1, then $P_n(x)$ factors into cyclotomic polynomials and a factor $S(x^2)$, where $S(x)$ is a Salem polynomial — in particular, in these cases, $P_n(x)$ will never have repeating roots that are not cyclotomic.

Remark 10.1.8. In practice, the limiting factor in applying this argument is the bound coming from Gross-Hironaka-McMullen [15] for roots of the form $\zeta_N + \zeta_N^{-1}$. The argument in [15] proceeds in two steps. First, there is a uniform bound on N. Second, for each fixed N the P_n which have such a root are precisely those in certain classes modulo N. Let $\widetilde{A}$ be A divided by all its cyclotomic factors, let $\ell(\widetilde{A})$ be the number of nonzero coefficients of $\widetilde{A}$. The argument in [15] shows that if $\zeta_N + \zeta_N^{-1}$ is a root of $P_n(x)$ for some n such that ζ_N is not a root of $A_n(t)$, then N divides $m \prod_{p \leq 2\ell(\widetilde{A})} p$ for some integer $m \leq 4 \deg \widetilde{A}$ (this is not the exact statement of [15, Thm 2.1], but the proof is the same). It seems in the cases that we have looked at that there is a much stronger bound on N, and proving an improved bound would substantially increase the effectiveness of our technique.

Example 10.1.9. We compute three applications of Theorem 10.0.1. Consider the graphs $\Gamma_{i,n}$ for $i = 1, 2, 3$, where the graphs Γ_i are given below in Fig. 3. The graphs $\Gamma_{1,n}$ and $\Gamma_{2,n}$ are the two infinite families which arise in the classification of Haagerup [16]. It was shown by Bisch [6] (using a fusion ring argument) that none of the $\Gamma_{2,n}$ are the principal graph of a subfactor. The corresponding result for $\Gamma_{1,n}$ and $n > 10$ was

proved by Asaeda–Yasuda [3] using number theoretic methods. The family $\Gamma_{3,n}$ is one of several families arising in ongoing work of V. Jones, Morrison, Peters, Penneys, and Snyder, extending the classification of Haagerup beyond $3+\sqrt{3}$. We compute that

$$K(\Gamma_1) = 2, \qquad K(\Gamma_2) = 4, \qquad K(\Gamma_3) = 8,$$

where Lemma 10.1.4 applies for $n \geq 8$, $n \geq 7$, and $n \geq 11$ respectively. Similarly, we find that the cyclotomic factors of $P_n(x)$ depend (for $n \geq 11$) only on $n \mod 24$, $n \mod 12$, and $n \mod 24$ for $i = 1, 2, 3$, and have degree at most 9, 6, and 8 respectively. The polynomials $A(t)$ are given as follows:

$$\begin{aligned} A_1(t) &= (t^2+1)(t^4+1)(t^6-t^4-t^2-1)t^{-11}, \\ A_2(t) &= (t^2-t+1)(t^2+t+1)(t^6-2t^4-1)t^{-9}, \\ A_3(t) &= (t^2-t+1)(t^2+t+1)(t^{10}-2t^8-t^6-t^4-1)t^{-13}. \end{aligned}$$

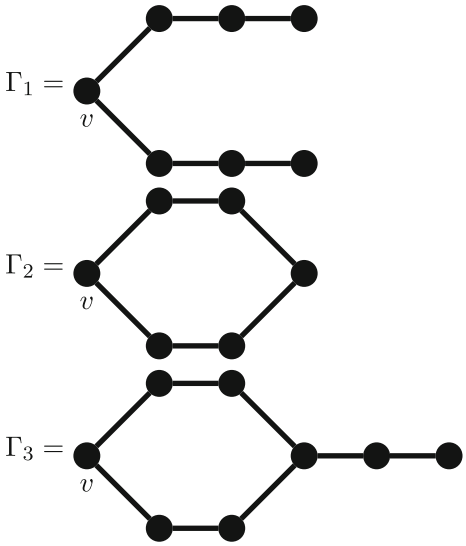

Fig. 3. The graphs Γ_i

In each case, we deduce that the only repeated factors of $F_n(t)$ on the unit circle can occur at roots of unity. In all cases, the graphs $\Gamma_{i,n}$ are bipartite, and, moreover, the polynomials $A_i(t)$ have a unique pair of roots of absolute value larger than 1. It follows that $P_n(x)$ can be written as the product of cyclotomic factors and a factor $S(x^2)$, where $S(x)$ is a Salem polynomial. From this we can directly eliminate the possible occurrence of a root λ of $P_n(x)$ of the form $\lambda^2 - 2 = 1 + 2\cos(2\pi/7)$ or $\lambda^2 - 2 = \eta$ whenever the degree of $S(x)$ is greater than 7, or when $n \geq 16$. It follows that $\Gamma_{n,i}$ does not correspond to a subfactor whenever $n \geq N$, where

$$\begin{aligned} N(\Gamma_1) &= 9 \cdot R(\Gamma_1) + 4 \cdot K(\Gamma_1) = 9 \cdot 9 + 4 \cdot 2 = 89, \\ N(\Gamma_2) &= 9 \cdot R(\Gamma_2) + 4 \cdot K(\Gamma_2) = 9 \cdot 6 + 4 \cdot 4 = 70, \\ N(\Gamma_3) &= 9 \cdot R(\Gamma_3) + 4 \cdot K(\Gamma_3) = 9 \cdot 8 + 4 \cdot 8 = 104. \end{aligned}$$

We may explicitly enumerate the polynomials for smaller n, and our results are as follows:

Corollary 10.1.10. *The graphs $\Gamma_{i,n}$ are not the principal graphs of subfactors for all (i,n) with the possible exception of the pairs $(i,n) = (1,7), (1,8), (1,10), (1,14), (2,6), (2,7), (2,8), (2,9), (2,11)$ and $(3,8)$. In these cases, we observe the following possibilities:*

(1) $\Gamma_{1,7} = \widetilde{A_7}$, *and* $\|\Gamma\| = \lambda^2 = (2\cos(\pi/8))^2 = 2+\sqrt{2}$.
(2) $\Gamma_{1,8} = \widetilde{E_7}$, *the extended Dynkin diagram of* E_7, *and* $\|\Gamma\| = \lambda^2 = 4$.
(3) $\Gamma_{1,10}$ *corresponds to the Haagerup subfactor [2], and* $\|\Gamma\| = \lambda^2 = \frac{5+\sqrt{13}}{2}$.
(4) $\Gamma_{1,14}$ *corresponds to the extended Haagerup subfactor [5], and*

$$\|\Gamma\| = \lambda^2 = 3+\zeta+\zeta^{-1}+\zeta^3+\zeta^{-3}+\zeta^4+\zeta^{-4}, \quad \textit{with} \quad \zeta^{13} = 1.$$

(5) $\Gamma_{2,6} = \widetilde{A_5}$, *the extended Dynkin diagram of* A_5, *and* $\|\Gamma\| = \lambda^2 = 4$.
(6) $\Gamma = \Gamma_{2,7}$, *and* $\|\Gamma\| = \lambda^2 = 3+\sqrt{2}$.
(7) $\Gamma = \Gamma_{2,8}$, *and* $\|\Gamma\| = \lambda^2 = (5+\sqrt{17})/2$.
(8) $\Gamma = \Gamma_{2,9}$, *and* $\|\Gamma\| = \lambda^2 = (7+\sqrt{5})/2$.
(9) $\Gamma = \Gamma_{2,11}$, *and* $\|\Gamma\| = \lambda^2 = 2-\zeta^4-\zeta^{-4}-\zeta^6-\zeta^{-6}$ *for* $\zeta^{13} = 1$.
(10) $\Gamma = \Gamma_{3,8} = \Gamma_{2,8}$.

In each of the cases $\Gamma_{2,7}$, $\Gamma_{2,8} = \Gamma_{3,8}$, $\Gamma_{2,9}$, and $\Gamma_{2,11}$, we may rule out the existence of a corresponding subfactor for each choice of fixed leaf by computing the global dimension Δ and checking that, for some Galois automorphism σ, the ratio $\sigma(\Delta)/\Delta$ is not an algebraic integer [27].

11. An Extension of Theorem 10.0.1

In this section, we prove the following extension of Theorem 10.0.1.

Theorem 11.0.1. *For sufficiently large n, either*:

(1) All the eigenvalues of M_n are of the form $\zeta+\zeta^{-1}$ for some root of unity ζ, and the graphs Γ_n are the Dynkin diagrams A_n or D_n.
(2) The largest eigenvalue λ of M_n is greater than 2, and the field $\mathbf{Q}(\lambda^2)$ is not abelian.

Remark 11.0.2. The proof of this theorem was found before the proof of Theorem 10.0.1. In our intended applications, all the conditions of Theorem 10.0.1 are met, however, this generalization may still be of interest.

Definition 11.0.3. *Let $\Phi_m(x)$ be the polynomial such that if $x = t+t^{-1}$, then $\Phi_m(x) = t^m + t^{-m}$.*

Remark 11.0.4. The polynomials $\Phi_m(x)$ are the Chebyshev polynomials, appropriately scaled so that all their roots are contained in the interval $[-2,2]$. If m is even, then $\Phi_m(x)$ is a polynomial in x^2.

11.1. Heights and algebraic integers. The goal of this section is to show that the fields $\mathbf{Q}(\rho)$ for any real root $\rho > 1$ of $F_n(t)$ have degree asymptotically bounded below by a linear function in n.

Recall that the Weil height of an algebraic number $\gamma = \alpha/\beta$ such that $K = \mathbf{Q}(\gamma)$ is defined to be

$$h(\gamma) := \frac{1}{[K : \mathbf{Q}]} \sum_v \log \max\{|\alpha|_v, |\beta|_v\}.$$

If $\lambda_\infty \leq 2$ then every root of $P_n(x)$ has absolute value at most 2, and thus every root ρ of $F_n(t)$ has absolute value 1. Yet then $h(\rho) = 0$ for all roots ρ of $F_n(t)$. A theorem of Kronecker says that $h(\gamma) > 0$ unless γ is zero or a root of unity. Hence, in this case, we are in the first case of Theorem 11.0.1.

The following lemma is well known, and is a consequence of the triangle inequality.

Lemma 11.1.1. *If $\phi : \mathbf{P}^1 \to \mathbf{P}^1$ is a homomorphism of finite degree, then $h(\phi(P)) \geq \deg(\phi) \cdot h(P) + C(\phi)$, for some constant $C(\phi)$ depending only on ϕ.*

Using this, we may deduce the following:

Lemma 11.1.2. *There exists an explicit constant c depending only on Γ such that for sufficiently large n, and for every root ρ of $F_n(t)$ there is an inequality:*

$$h(\rho) \leq \frac{c}{n}.$$

Proof. Consider the rational map $\phi : \mathbf{P}^1 \to \mathbf{P}^1$ defined by sending t to $\frac{A(t^{-1})}{A(t)}$. Since $\phi(\rho) = \rho^{2n}$, we deduce that

$$2n \cdot h(\rho) = h(\rho^{2n}) = h(\phi(\rho)) \leq \deg(\phi) \cdot h(\rho) + C(\phi).$$

The lemma follows, taking $c = C(\phi)$ and $n \geq \deg(\phi)$. □

Lemma 11.1.3. *There exists a constant a such that if ρ is a root of $F_n(t)$, then either ρ is a root of unity or $[\mathbf{Q}(\rho) : \mathbf{Q}] \geq a \cdot n$ for sufficiently large n.*

Proof. For sufficiently large n, the real roots of absolute value larger than 1 of $F_n(t)$ are bounded away from 1, by Lemma 10.1.2 (4). If ρ is a root of $F_n(t)$ that is not a root of unity, then it has at least one conjugate of absolute value larger than 1, by Kronecker's theorem. It follows from the definition of height that for sufficiently large n,

$$[\mathbf{Q}(\rho) : \mathbf{Q}] \cdot h(\rho) \geq d$$

for some absolute constant d. In light of the previous lemma, this suffices to prove the result with $a = d/c$. □

Note that if $\lambda = \rho + \rho^{-1}$, then $[\mathbf{Q}(\rho) : \mathbf{Q}(\lambda)] \leq 2$, and so the same result (with a different d) applies to $[\mathbf{Q}(\lambda) : \mathbf{Q}]$.

Lemma 11.1.4. *Fix an integer m. For sufficiently large n, if λ is a root of $P_n(x)$, then*

$$\frac{1}{[\mathbf{Q}(\lambda) : \mathbf{Q}]} \sum \Phi_m^2(\sigma\lambda) \leq 5,$$

where the sum runs over all conjugates of λ.

Proof. If $|x| \leq 2$ then $\Phi_m^2(x) \leq 4$. If $\lambda = \rho + \rho^{-1}$ and ρ is a root of unity the result is obvious. Thus we may assume (after conjugation if necessary) that $\rho > 1$. Suppose that λ has R conjugates of absolute value larger than 2. Each of these roots is bounded by λ_∞, and the number of such roots is also uniformly bounded, by Lemma 10.1.2. Note that

$$\frac{1}{[\mathbf{Q}(\lambda) : \mathbf{Q}]} \sum \Phi_m^2(\sigma\lambda) \leq 4 + R \cdot \frac{\Phi_m^2(\lambda_\infty) - 4}{[\mathbf{Q}(\lambda) : \mathbf{Q}]}.$$

Since $[\mathbf{Q}(\lambda) : \mathbf{Q}]$ becomes arbitrarily large by Lemma 11.1.3, the right-hand side is bounded by 5 for sufficiently large n. □

The following result is an immediate consequence of Loxton's theorem (Theorem 9.1.2) quoted previously:

Corollary 11.1.5. *If β is a cyclotomic integer such that $\mathscr{M}(\beta) \leq 5$, then $\mathscr{N}(\beta)$ is bounded by some absolute constant, which we denote by C.*

11.2. Proof of Theorem 11.0.1. If $\lambda_\infty \leq 2$ then the first claim follows from [30, Theorem 2]. We may assume that $\lambda_\infty > 2$. By Lemma 10.1.2 (4), we may assume that for all n, $P_n(x)$ has no roots in the interval $(2, \alpha)$ for some $\alpha > 2$. Choose an even integer m such that $\Phi_m(\alpha) > C$, where C is to be chosen later. By Lemma 11.1.4, we deduce that if n is sufficiently large, then for any root λ of $P_n(x)$,

$$\mathscr{M}(\Phi_m(\lambda)) = \frac{1}{[\mathbf{Q}(\lambda) : \mathbf{Q}]} \sum \Phi_m^2(\sigma\lambda) \leq 5.$$

We assume that $\mathbf{Q}(\lambda^2)$ is abelian for some $\lambda > 2$ and derive a contradiction. Since m is even, $\beta = \Phi_m(\lambda) \in \mathbf{Q}(\lambda^2)$, and hence β is cyclotomic. Moreover, $\mathscr{M}(\beta) \leq 5$.

Choosing C to be as in the above corollary, we deduce that $\mathscr{N}(\beta) \leq C$. Since $\lambda > 2$, however, $\lambda \geq \alpha$ and hence $\beta > C$. Yet the sum of C roots of unity has absolute value at most C, by the triangle inequality. This completes the proof of Theorem 11.0.1.

Acknowledgements. We would like to thank MathOverflow where this collaboration began (see "Number theoretic spectral properties of random graphs" http://mathoverflow.net/questions/5994/). We would also like to thank Feng Xu for helpful conversations, and Victor Ostrik for writing the Appendix. Frank Calegari was supported by NSF Career Grant DMS-0846285, NSF Grant DMS-0701048, and a Sloan Foundation Fellowship, Scott Morrison was at the Miller Institute for Basic Research at UC Berkeley, and Noah Snyder was supported by an NSF Postdoctoral Fellowship.

Appendix A. A Pseudo-Unitary Fusion Category with an Object of Dimension $\frac{\sqrt{3}+\sqrt{7}}{2}$. by Victor Ostrik

A.1. The goal of this Appendix is to construct a fusion category $\mathcal{V}$ over $\mathbf{C}$ with an object $\mathbf{V}$ such that $\mathrm{FP}(\mathbf{V}) = \frac{\sqrt{3}+\sqrt{7}}{2}$ (notice that since $\frac{\sqrt{3}+\sqrt{7}}{2} < 1 + \sqrt{2}$, the object $\mathbf{V}$ is automatically simple). We do not attempt to classify all fusion categories generated by such an object.

The category we construct is pseudo-unitary (i.e. it is endowed with a spherical structure and $\mathrm{FP}(X) = \dim(X)$ for any object X); moreover all the categories considered in this Appendix are pseudo-unitary as well.

A.2. Preliminaries. In this section we collect necessary definitions and results. We refer the reader to [11,13] for a general theory of fusion and braided fusion categories.

Let $\mathcal{C}$ be a pre-modular fusion category, see e.g. [11, Def. 2.29]. Following [23] we will consider commutative associative unital algebras $A \in \mathcal{C}$ satisfying the following assumptions:

(i) $\dim \mathrm{Hom}(\mathbf{1}, A) = 1$;
(ii) the pairing $A \otimes A \to \mathbf{1}$ defined as a composition of the multiplication $A \otimes A \to A$ and a non-zero morphism $A \to \mathbf{1}$ is non-degenerate and $\dim(A) \neq 0$;
(iii) the balance isomorphism $\theta_A = \mathrm{id}_A$.

In [23] the algebras A satisfying these conditions were called "rigid $\mathcal{C}-$algebras with $\theta_A = \mathrm{id}_A$"; to abbreviate we will call such algebras "$\mathcal{C}-$algebras" here.

Given a pre-modular fusion category $\mathcal{C}$ and a $\mathcal{C}-$algebra $A \in \mathcal{C}$, one considers the category $\mathcal{C}_A$ of right $A-$modules. The category $\mathcal{C}_A$ has a natural structure of spherical fusion category, see [23, Theorem 3.3, Remark 1.19]. It contains a full fusion subcategory $\mathcal{C}_A^0$ of *dyslectic* modules, see [23, Def. 1.8]. The category $\mathcal{C}_A^0$ has a natural structure of pre-modular category. If $\mathcal{C}$ is pseudo-unitary the same is true for $\mathcal{C}_A$ and $\mathcal{C}_A^0$.

For a braided fusion category $\mathcal{C}$ let $\mathcal{C}^{op}$ denote the *opposite* category ($\mathcal{C}^{op} = \mathcal{C}$ as a fusion category and the braiding in $\mathcal{C}^{op}$ is the inverse of the braiding in $\mathcal{C}$). Let $\mathcal{Z}(\mathcal{A})$ denote the Drinfeld center of a fusion category $\mathcal{A}$.

Theorem A.2.1 (cf. [23, Theorem 4.5], [10, Remark 4.3], [13, Theorem 2.15]). *Assume that the category $\mathcal{C}$ is* modular. *We have*

(i) $\dim \mathcal{C}_A = \frac{\dim \mathcal{C}}{\dim(A)}$ *and* $\dim \mathcal{C}_A^0 = \frac{\dim \mathcal{C}}{\dim(A)^2}$;
(ii) *the category $\mathcal{C}_A^0$ is modular;*
(iii) *there is a braided equivalence $\mathcal{Z}(\mathcal{C}_A) = \mathcal{C} \boxtimes (\mathcal{C}_A^0)^{op}$.* □

Recall (see e.g. [11, §2.12]) that a braided fusion category $\mathcal{E}$ is called *Tannakian* if it is braided equivalent to the representation category $\mathrm{Rep}(G)$ of a finite group G. Let $\mathcal{E}$ be a Tannakian subcategory of a braided fusion category $\mathcal{C}$. Recall ([11, §5.4.1]) that in this situation one defines a *fiber category* $\mathcal{E}'_{\mathcal{C}} \boxtimes_{\mathcal{E}} \mathrm{Vec}$.

Theorem A.2.2 ([12, Theorem 1.3]). *Let $\mathcal{C}$ be a modular category with Tannakian subcategory $\mathcal{E} = Rep(G)$. Assume that $\mathcal{E}'_{\mathcal{C}} \boxtimes_{\mathcal{E}} Vec \simeq \mathcal{Z}(\mathcal{A})$ for a fusion category $\mathcal{A}$. Then $\mathcal{C} \simeq \mathcal{Z}(\mathcal{B})$, where $\mathcal{B} = \bigoplus_{g \in G} \mathcal{B}_g$ is a faithfully $G-$graded fusion category with trivial component $\mathcal{B}_1$ equivalent to $\mathcal{A}$.* □

A.3. Affine Lie algebras and conformal embeddings. Let $\mathfrak{g}$ be a finite dimensional simple Lie algebra and let $\hat{\mathfrak{g}}$ be the corresponding affine Lie algebra, see e.g. [4, §7.1]. For $k \in \mathbf{Z}_{>0}$ let $\mathcal{C}(\mathfrak{g}, k)$ denote the category of integrable highest weight $\hat{\mathfrak{g}}-$modules of level k (this category is denoted by $\mathcal{O}_k^{int}$ in *loc. cit.*). It is well known that the category $\mathcal{C}(\mathfrak{g}, k)$ has a natural structure of pseudo-unitary modular tensor category, see e.g. [4, Theorem 7.0.1]. The unit object of the category $\mathcal{C}(\mathfrak{g}, k)$ is the *vacuum $\hat{\mathfrak{g}}-$module* of level k.

Let $\mathfrak{g} \subset \mathfrak{g}'$ be an embedding of simple (or, more generally, semisimple) Lie algebras. It defines an embedding $\hat{\mathfrak{g}} \subset \hat{\mathfrak{g}}'$. This embedding does not preserve the level; we will write $(\hat{\mathfrak{g}})_k \subset (\hat{\mathfrak{g}}')_{k'}$ if the pullback of a $\hat{\mathfrak{g}}'-$module of level k' under this embedding is a $\hat{\mathfrak{g}}-$module of level k (it is clear that k is uniquely determined by k'). Recall (see e.g. [9]) that a *conformal embedding* $(\hat{\mathfrak{g}})_k \subset (\hat{\mathfrak{g}}')_{k'}$ is an embedding as above such that the

pullback of any module from $\mathcal{C}(\mathfrak{g}', k')$ is a *finite* direct sum of modules from $\mathcal{C}(\mathfrak{g}, k)$. Let $(\hat{\mathfrak{g}})_k \subset (\hat{\mathfrak{g}}')_{k'}$ be a conformal embedding. Then the pullback of the vacuum $\hat{\mathfrak{g}}'-$module of level k' is an object A of $\mathcal{C}(\mathfrak{g}, k)$ which has a natural structure of $\mathcal{C}(\mathfrak{g}, k)-$algebra, see [23, Theorem 5.2]. Moreover, there is a natural equivalence $\mathcal{C}(\mathfrak{g}, k)_A^0 \simeq \mathcal{C}(\mathfrak{g}', k')$, see *loc. cit.*

Example A.3.1. The following is a toy version of our main construction. There exists a conformal embedding $(\hat{sl}_2)_4 \subset (\hat{sl}_3)_1$, see e.g. [9]. Let $A_0 \in \mathcal{C}(sl_2, 4)$ be the corresponding $\mathcal{C}(sl_2, 4)-$algebra. Recall (cf. [4, §3.3]) that the category $\mathcal{C}(sl_2, 4)$ has 5 simple objects of dimensions $1, \sqrt{3}, 2, \sqrt{3}, 1$; in particular $\dim \mathcal{C}(sl_2, 4) = 12$. The category $\mathcal{C}(sl_3, 1)$ is pointed with underlying group $\mathbf{Z}/3\mathbf{Z}$; in particular $\dim \mathcal{C}(sl_3, 1) = 3$. We deduce from Theorem A.2.1 (i) that $\dim(A_0) = 2$ and $\dim \mathcal{C}(sl_2, 4)_{A_0} = 6$. Notice that the category $\mathcal{C}(sl_2, 4)_{A_0}$ contains an object of dimension $\sqrt{3}$ since its center does (see Theorem A.2.1 (iii)); this object is automatically simple. It follows that the category $\mathcal{C}(sl_2, 4)_{A_0}$ has precisely 4 simple objects: 3 from the subcategory $\mathcal{C}(sl_2, 4)_{A_0}^0$ and one more of dimension $\sqrt{3}$. Furthermore this implies that the category $\mathcal{C}(sl_2, 4)_{A_0}$ is a Tambara-Yamagami category associated to $\mathbf{Z}/3\mathbf{Z}$ [32]. In particular, $\mathcal{C}(sl_2, 4)_{A_0}$ is $\mathbf{Z}/2\mathbf{Z}-$graded with trivial component $\mathcal{C}(sl_2, 4)_{A_0}^0 = \mathcal{C}(sl_3, 1)$.

We now show that this example is an illustration of Theorem A.2.2. Since $\dim(A_0) = 2$, we see that A_0 is a direct sum of two invertible objects. It follows that the subcategory $\mathcal{E}$ of $\mathcal{C}(sl_2, 4)$ generated by the invertible objects is Tannakian and is equivalent to $\mathrm{Rep}(\mathbf{Z}/2\mathbf{Z})$ (see also [23, Theorem 6.5]). It follows from the definitions that in this case $\mathcal{E}'_{\mathcal{C}(sl_2,4)} \boxtimes_{\mathcal{E}} \mathrm{Vec} = \mathcal{C}(sl_2, 4)_{A_0}^0 = \mathcal{C}(sl_3, 1)$, see e.g. [11, Prop. 4.56 (i)]. Notice that $\mathcal{E} = \mathcal{E} \boxtimes \mathbf{1}$ can be considered as a subcategory of $\mathcal{C}(sl_2, 4) \boxtimes \mathcal{C}(sl_3, 1)^{op}$. Clearly we have

$$\mathcal{E}'_{\mathcal{C}(sl_2,4)\boxtimes\mathcal{C}(sl_3,1)^{op}} \boxtimes_{\mathcal{E}} \mathrm{Vec} = (\mathcal{E}'_{\mathcal{C}(sl_2,4)} \boxtimes_{\mathcal{E}} \mathrm{Vec}) \boxtimes \mathcal{C}(sl_3, 1)^{op} = \mathcal{C}(sl_3, 1) \boxtimes \mathcal{C}(sl_3, 1)^{op}.$$

Since $\mathcal{C}(sl_3, 1) \boxtimes \mathcal{C}(sl_3, 1)^{op} = \mathcal{Z}(\mathcal{C}(sl_3, 1))$ (see e.g. [11, Prop. 3.7]), Theorem A.2.2 says that $\mathcal{C}(sl_2, 4) \boxtimes \mathcal{C}(sl_3, 1)^{op} = \mathcal{Z}(\mathcal{B})$, where $\mathcal{B}$ is a $\mathbf{Z}/2\mathbf{Z}-$graded category with trivial component $\mathcal{C}(sl_3, 1)$. This is indeed so since by Theorem A.2.1 (iii),

$$\mathcal{Z}(\mathcal{C}(sl_2, 4)_{A_0}) = \mathcal{C}(sl_2, 4) \boxtimes (\mathcal{C}(sl_2, 4)_{A_0}^0)^{op} = \mathcal{C}(sl_2, 4) \boxtimes \mathcal{C}(sl_3, 1)^{op}.$$

A.4. Izumi-Xu category $\mathcal{IX}$. We will consider here another example for the formalism from §A.3. Let $\mathfrak{g}_{G_2}$ and $\mathfrak{g}_{E_6}$ be the simple Lie algebras of type G_2 and E_6. There exists a conformal embedding $(\hat{\mathfrak{g}}_{G_2})_3 \subset (\hat{\mathfrak{g}}_{E_6})_1$, see e.g. [9]. Let $A_1 \in \mathcal{C}(\mathfrak{g}_{G_2}, 3)$ be the corresponding $\mathcal{C}(\mathfrak{g}_{G_2}, 3)-$algebra.

Proposition A.4.1. *The category $\mathcal{C}(\mathfrak{g}_{G_2}, 3)_{A_1}$ has precisely 4 simple objects $\mathbf{1}, \mathbf{g}, \mathbf{g}^2$ and $\mathbf{X}$. The subcategory generated by $\mathbf{1}, \mathbf{g}, \mathbf{g}^2$ is pointed with underlying group $\mathbf{Z}/3\mathbf{Z}$. The remaining fusion rules are*

$$\mathbf{g} \otimes \mathbf{X} = \mathbf{g}^2 \otimes \mathbf{X} = \mathbf{X} \otimes \mathbf{g} = \mathbf{X} \otimes \mathbf{g}^2 = \mathbf{X};\ \mathbf{X} \otimes \mathbf{X} = \mathbf{1} \oplus \mathbf{g} \oplus \mathbf{g}^2 \oplus 3\mathbf{X}.$$

Proof. The category $\mathcal{C}(\mathfrak{g}_{E_6}, 1)$ is pointed with underlying group $\mathbf{Z}/3\mathbf{Z}$. Hence the category $\mathcal{C}(\mathfrak{g}_{G_2}, 3)_{A_1}$ contains a pointed subcategory with underlying group $\mathbf{Z}/3\mathbf{Z}$, namely $\mathcal{C}(\mathfrak{g}_{G_2}, 3)_{A_1}^0 \simeq \mathcal{C}(\mathfrak{g}_{E_6}, 1)$. We will denote the simple objects of this subcategory by $\mathbf{1}$ (the unit object), $\mathbf{g}$ and $\mathbf{g}^2$.

Using [4, Theorem 7.0.2, Theorem 3.3.20] one computes

$$\dim \mathcal{C}(\mathfrak{g}_{G_2}, 3) = \frac{147}{(64 \sin(\frac{\pi}{21}) \sin(\frac{4\pi}{21}) \sin(\frac{5\pi}{21}) \sin(\frac{\pi}{7}) \sin(\frac{2\pi}{7}) \sin(\frac{3\pi}{7}))^2}$$
$$= 3\left(\frac{7+\sqrt{21}}{2}\right)^2.$$

Since $\dim \mathcal{C}(\mathfrak{g}_{G_2}, 3)^0_{A_1} = 3$, we deduce from Theorem A.2.1 (i) that $\dim(A_1) = \frac{7+\sqrt{21}}{2}$ and $\dim \mathcal{C}(\mathfrak{g}_{G_2}, 3)_{A_1} = \frac{21+3\sqrt{21}}{2}$. The sum of squares $\sum_i d_i^2$ of the dimensions of simple objects of the category $\mathcal{C}(\mathfrak{g}_{G_2}, 3)_{A_1}$ not lying in $\mathcal{C}(\mathfrak{g}_{G_2}, 3)^0_{A_1}$ is $\frac{15+3\sqrt{21}}{2}$. Notice that every $\alpha = d_i^2$ is a totally positive algebraic integer satisfying $\boxed{\alpha} = \alpha$. The proof of the following result is left to the reader:

Lemma A.4.2. *There are precisely three decompositions of* $\frac{15+3\sqrt{21}}{2}$ *into a sum of totally positive algebraic integers* α *satisfying* $\boxed{\alpha} = \alpha$, *namely*

(1) $\frac{15+3\sqrt{21}}{2} = \frac{15+3\sqrt{21}}{2}$;
(2) $\frac{15+3\sqrt{21}}{2} = \frac{5+\sqrt{21}}{2} + (5+\sqrt{21})$;
(3) $\frac{15+3\sqrt{21}}{2} = \frac{5+\sqrt{21}}{2} + \frac{5+\sqrt{21}}{2} + \frac{5+\sqrt{21}}{2}$.

Notice that in cases (2) and (3) the abelian subgroup $\mathbf{Z} \oplus \bigoplus_i \mathbf{Z} d_i \subset \mathbf{C}$ is not closed under multiplication. Hence the only possibility is the decomposition (1); thus the category $\mathcal{C}(\mathfrak{g}_{G_2}, 3)_{A_1}$ has precisely one simple object $\mathbf{X}$ that is not in $\mathcal{C}(\mathfrak{g}_{G_2}, 3)^0_{A_1}$; moreover $\dim(\mathbf{X}) = \sqrt{\frac{15+3\sqrt{21}}{2}} = \frac{3+\sqrt{21}}{2}$. The result follows. □

A fusion category with fusion rules as in Proposition A.4.1 was constructed by Izumi in [18]. The construction presented here is due to Feng Xu [33] (note that it is not clear whether the two constructions produce equivalent categories). Thus we call the category $\mathcal{C}(\mathfrak{g}_{G_2}, 3)_{A_1}$ the *Izumi–Xu category* and denote it by $\mathcal{IX}$.

Remark A.4.3. Both categories $\mathcal{C}(sl_3, 1)$ and $\mathcal{C}(\mathfrak{g}_{E_6}, 1)$ are pointed with underlying group $\mathbf{Z}/3\mathbf{Z}$. One observes (using [4, Theorem 3.3.20]) that these categories are opposite to each other. In particular, Theorem A.2.1 (iii) implies that

$$\mathcal{Z}(\mathcal{IX}) \simeq \mathcal{C}(\mathfrak{g}_{G_2}, 3) \boxtimes \mathcal{C}(\mathfrak{g}_{E_6}, 1)^{op} \simeq \mathcal{C}(\mathfrak{g}_{G_2}, 3) \boxtimes \mathcal{C}(sl_3, 1).$$

A.5. Main result.

Theorem A.5.1. *There exists a pseudo-unitary fusion category* $\mathcal{V}$ *such that*

(i) $\mathcal{Z}(\mathcal{V}) \simeq \mathcal{C}(\mathfrak{g}_{G_2}, 3) \boxtimes \mathcal{C}(sl_2, 4)$;
(ii) $\mathcal{V} = \mathcal{V}_0 \oplus \mathcal{V}_1$ *is* $\mathbf{Z}/2\mathbf{Z}$*−graded with trivial component* $\mathcal{V}_0$ *equivalent to the Izumi-Xu category* $\mathcal{IX}$;
(iii) $\mathcal{V}_1$ *contains three simple objects of dimensions* $\frac{\sqrt{3}+\sqrt{7}}{2}$ *and a simple object of dimension* $\sqrt{3}$.

Proof. We recall that the category $\mathcal{C}(sl_2, 4)$ contains a Tannakian subcategory $\mathcal{E} \simeq \mathrm{Rep}(\mathbf{Z}/2\mathbf{Z})$ such that $\mathcal{E}'_{\mathcal{C}(sl_2,4)} \boxtimes_{\mathcal{E}} \mathrm{Vec} \simeq \mathcal{C}(sl_3, 1)$, see Example A.3.1. Now we consider $\mathcal{E} = \mathbf{1} \boxtimes \mathcal{E}$ as a subcategory of $\mathcal{Z} := \mathcal{C}(\mathfrak{g}_{G_2}, 3) \boxtimes \mathcal{C}(sl_2, 4)$. Clearly, $\mathcal{E}'_{\mathcal{Z}} \boxtimes_{\mathcal{E}} \mathrm{Vec} \simeq \mathcal{C}(\mathfrak{g}_{G_2}, 3) \boxtimes \mathcal{C}(sl_3, 1)$. Thus Theorem A.2.2 and Remark A.4.3 imply that $\mathcal{Z} \simeq \mathcal{Z}(\mathcal{V})$, where $\mathcal{V}$ is $\mathbf{Z}/2\mathbf{Z}-$graded fusion category with trivial component $\mathcal{IX}$. Thus (i) and (ii) are proved.

To prove (iii) we observe that the category $\mathcal{Z}$ contains an object of dimension $\sqrt{3}$; hence the category $\mathcal{V}$ contains an object $\mathbf{M}$ of dimension $\sqrt{3}$. The object $\mathbf{M}$ is automatically simple and is contained in $\mathcal{V}_1$. Obviously, $\mathbf{M} \otimes \mathbf{M} = \mathbf{1} \oplus \mathbf{g} \oplus \mathbf{g}^2$. Hence $\mathbf{M} \simeq \mathbf{M}^*$ and $\mathrm{Hom}(\mathbf{M}, \mathbf{X} \otimes \mathbf{M}) = \mathrm{Hom}(\mathbf{M} \otimes \mathbf{M}^*, \mathbf{X}) = 0$. Furthermore, $\mathrm{Hom}(\mathbf{X} \otimes \mathbf{M}, \mathbf{X} \otimes \mathbf{M}) = \mathrm{Hom}(\mathbf{M}, \mathbf{X}^* \otimes \mathbf{X} \otimes \mathbf{M}) = \mathbf{C}^3$. Thus, $\mathbf{X} \otimes \mathbf{M} \in \mathcal{V}_1$ is a direct sum of three distinct simple objects $\mathbf{V}_1, \mathbf{V}_2, \mathbf{V}_3$, none of which is isomorphic to $\mathbf{M}$. Since $\dim \mathcal{V}_1 = \dim \mathcal{V}_0 = \frac{21+3\sqrt{21}}{2}$, we get that

$$\dim(\mathbf{V}_1)^2 + \dim(\mathbf{V}_2)^2 + \dim(\mathbf{V}_3)^2 = \frac{15 + 3\sqrt{21}}{2}.$$

Using Lemma A.4.2, we see that

$$\dim(\mathbf{V}_1) = \dim(\mathbf{V}_2) = \dim(\mathbf{V}_3) = \sqrt{\frac{5 + \sqrt{21}}{2}} = \frac{\sqrt{3} + \sqrt{7}}{2}.$$

Thus the theorem is proved. □

A.6. Fusion rules of the category $\mathcal{V}$. In this section we compute the fusion rules of the category $\mathcal{V}$ following a suggestion of Noah Snyder.

First, at least one of the objects $\mathbf{V}_1, \mathbf{V}_2, \mathbf{V}_3$ is self dual; we assume that $\mathbf{V}_1$ is self dual and use notation $\mathbf{V} := \mathbf{V}_1$. The dimension count shows that

$$\mathbf{V} \otimes \mathbf{V} \simeq \mathbf{V}_2 \otimes \mathbf{V}_2^* \simeq \mathbf{V}_3 \otimes \mathbf{V}_3^* \simeq \mathbf{1} \oplus \mathbf{X}.$$

It follows that $\mathbf{g} \otimes \mathbf{V} \not\simeq \mathbf{V}$ and $\mathbf{g}^2 \otimes \mathbf{V} \not\simeq \mathbf{V}$; thus we can (and will) assume that $\mathbf{V}_2 = \mathbf{g} \otimes \mathbf{V}$ and $\mathbf{V}_3 = \mathbf{g}^2 \otimes \mathbf{V}$.

We claim that $\mathbf{V} \otimes \mathbf{g} \not\simeq \mathbf{g} \otimes \mathbf{V}$. Assume for the sake of contradiction that $\mathbf{V} \otimes \mathbf{g} \simeq \mathbf{g} \otimes \mathbf{V}$. It follows that the Grothendieck ring $K(\mathcal{V})$ is commutative (since it is generated by the classes $[\mathbf{g}]$ and $[\mathbf{V}]$). Thus [13, Lemma 8.49] implies that the map $K(\mathcal{Z}(\mathcal{V})) \otimes \mathbf{Q} \to K(\mathcal{V}) \otimes \mathbf{Q}$ is surjective. But this is impossible since any object of $\mathcal{Z}(\mathcal{V}) = \mathcal{C}(\mathfrak{g}_{G_2}, 3) \boxtimes \mathcal{C}(sl_2, 4)$ is self dual and $(\mathbf{g})^* = \mathbf{g}^2 \not\simeq \mathbf{g}$.

It follows that $\mathbf{V} \otimes \mathbf{g} \simeq \mathbf{g}^2 \otimes \mathbf{V}$. The remaining fusion rules are easy to determine from the known information. We have

Proposition A.6.1. *The simple objects of the category $\mathcal{V}$ are* $\mathbf{1}, \mathbf{g}, \mathbf{g}^2, \mathbf{X}, \mathbf{M}, \mathbf{V}, \mathbf{gV} := \mathbf{g} \otimes \mathbf{V}, \mathbf{g}^2\mathbf{V} := \mathbf{g}^2 \otimes \mathbf{V}$. *The fusion rules are uniquely determined by Proposition* A.4.1 *and*

$$\begin{aligned}
&\mathbf{V} \otimes \mathbf{g} = \mathbf{g}^2\mathbf{V}, \ \mathbf{X} \otimes \mathbf{M} = \mathbf{M} \otimes \mathbf{X} = \mathbf{V} \oplus \mathbf{gV} \oplus \mathbf{g}^2\mathbf{V}, \\
&\mathbf{X} \otimes \mathbf{V} = \mathbf{V} \otimes \mathbf{X} = \mathbf{M} \oplus \mathbf{V} \oplus \mathbf{gV} \oplus \mathbf{g}^2\mathbf{V}, \\
&\mathbf{M} \otimes \mathbf{M} = \mathbf{1} \oplus \mathbf{g} \oplus \mathbf{g}^2, \ \mathbf{M} \otimes \mathbf{V} = \mathbf{V} \otimes \mathbf{M} = \mathbf{X}, \ \mathbf{V} \otimes \mathbf{V} = \mathbf{1} \oplus \mathbf{X}.
\end{aligned}$$

□

References

1. Asaeda, M.: Galois groups and an obstruction to principal graphs of subfactors. Internat. J. Math. **18**(2), 191–202 (2007)
2. Asaeda, M., Haagerup, U.: Exotic subfactors of finite depth with Jones indices $(5 + \sqrt{13})/2$ and $(5 + \sqrt{17})/2$. Commun. Math. Phys. **202**(1), 1–63 (1999)
3. Asaeda, M., Yasuda, S.: On Haagerup's list of potential principal graphs of subfactors. Commun. Math. Phys. **286**(3), 1141–1157 (2009)
4. Bakalov, B., Kirillov, A. Jr.: *Lectures on tensor categories and modular functors*. Volume **21** of University Lecture Series. Providence, RI: Amer. Math. Soc., 2001
5. Bigelow, S., Morrison, S., Peters, E., Snyder, N.: Constructing the extended Haagerup planar algebra. http://arxiv.org/abs/0909.4099v1 [math.OA], 2009
6. Bisch, D.: Principal graphs of subfactors with small Jones index. Math. Ann. **311**(2), 223–231 (1998)
7. Cassels, J.W.S.: On a conjecture of R. M. Robinson about sums of roots of unity. J. Reine Angew. Math. **238**, 112–131 (1969)
8. Conway, J.H., Jones, A.J.: Trigonometric Diophantine equations (On vanishing sums of roots of unity). Acta Arith. **30**(3), 229–240 (1976)
9. Di Francesco, P., Mathieu, P., Sénéchal, D.: *Conformal field theory*. Graduate Texts in Contemporary Physics. New York: Springer-Verlag, 1997
10. Drinfeld, V., Gelaki, S., Nikshych, D., Ostrik, V.: Group-theoretical properties of nilpotent modular categories. http://arxiv.org/abs/0704.0195v2 [math.QA], 2007
11. Drinfeld, V., Gelaki, S., Nikshych, D., Ostrik, V.: On braided fusion categories I. http://arxiv.org/abs/0906.0620v3 [math.QA], 2010
12. Etingof, P., Nikshych, D., Ostrik, V.: Weakly group-theoretical and solvable fusion categories. http://arxiv.org/abs/0809.3031v2 [math.QA], 2009
13. Etingof, P., Nikshych, D., Ostrik, V.: On fusion categories. Ann. of Math. (2) **162**(2), 581–642 (2005)
14. Godsil, C., Royle, G.: *Algebraic graph theory*, Volume **207** of Graduate Texts in Mathematics. New York: Springer-Verlag, 2001
15. Gross, B.H., Hironaka, E., McMullen, C.T.: Cyclotomic factors of Coxeter polynomials. J. Number Theory **129**(5), 1034–1043 (2009)
16. Haagerup, U.: Principal graphs of subfactors in the index range $4 < [M : N] < 3 + \sqrt{2}$. In: *Subfactors (Kyuzeso, 1993)*. River Edge, NJ: World Sci. Publ., 1994, pp. 1–38
17. Iwaniec, H.: On the error term in the linear sieve. Acta Arith. **19**, 1–30 (1971)
18. Izumi, M.: The structure of sectors associated with Longo-Rehren inclusions. II. Examples. Rev. Math. Phys. **13**(5), 603–674 (2001)
19. Jacobsthal, E.: Über Sequenzen ganzer Zahlen, von denen keine zu n teilerfremd ist. I, II, III. Norke Vid. Selsk. Forh. Trondheim **33**, 117–124, 125–131, 132–139 (1961)
20. Jones, A.J.: Sums of three roots of unity. Proc. Cambridge Philos. Soc. **64**, 673–682 (1968)
21. Jones, V.F.R.: Index for subfactors. Invent. Math. **72**(1), 1–25 (1983)
22. Kanold, H.-J.: Über eine zahlentheoretische Funktion von Jacobsthal. Math. Ann. **170**, 314–326 (1967)
23. Kirillov, A. Jr., Ostrik, V.: On a q-analogue of the McKay correspondence and the ADE classification of $\mathfrak{sl}_2$ conformal field theories. Adv. Math. **171**(2), 183–227 (2002)
24. Kronecker, L.: Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten. J. Reine Angew. Math. **53**, 173–175 (1857)
25. Loxton, J.H.: On the maximum modulus of cyclotomic integers. Acta Arith. **22**, 69–85 (1972)
26. McKee, J., Smyth, C.: Salem numbers, Pisot numbers, Mahler measure, and graphs. Experiment. Math. **14**(2), 211–229 (2005)
27. Ostrik, V.: On formal codegrees of fusion categories. Math. Research Letters **16**(5), 895–901 (2009)
28. Poonen, B., Rubinstein, M.: The number of intersection points made by the diagonals of a regular polygon. SIAM J. Discrete Math. **11**(1), 135–156 (electronic) (1998)
29. Siegel, C.L.: The trace of totally positive and real algebraic integers. Ann. of Math. (2) **46**, 302–312 (1945)
30. Smith J.H.: Some properties of the spectrum of a graph. In: *Combinatorial Structures and their Applications (Proc. Calgary Internat. Conf., Calgary, Alta., 1969)*, New York: Gordon and Breach, 1970, pp. 403–406
31. Smyth, C.J.: The mean values of totally real algebraic integers. Math. Comp. **42**(166), 663–681 (1984)
32. Tambara, D., Yamagami, S.: Tensor categories with fusion rules of self-duality for finite abelian groups. J. Algebra **209**(2), 692–707 (1998)
33. Xu, F.: Unpublished notes, 2001

Communicated by Y. Kawahigashi