THE CASSELS HEIGHTS OF CYCLOTOMIC INTEGERS

JAMES MCKEE, BYEONG-KWEON OH, AND CHRIS SMYTH

Abstract. We study the set $\mathscr{C}$ of mean square values of the moduli of the conjugates of cyclotomic integers β. For its kth derived set $\mathscr{C}^{(k)}$, we show that $\mathscr{C}^{(k)} = (k+1)\mathscr{C}$ $(k \geq 0)$, so that also $\mathscr{C}^{(k)} + \mathscr{C}^{(\ell)} = \mathscr{C}^{(k+\ell+1)}$ $(k, \ell \geq 0)$. We also calculate the order type of $\mathscr{C}$, and show that it is the same as that of the set of PV numbers.

Furthermore, we describe precisely the restricted set $\mathscr{C}_p$ where the β are confined to the ring $\mathbb{Z}[\omega_p]$, where p is an odd prime and ω_p is a primitive pth root of unity. In order to do this, we prove that both of the quadratic polynomials $a^2 + ab + b^2 + c^2 + a + b + c$ and $a^2 + b^2 + c^2 + ab + bc + ca + a + b + c$ are universal.

1. Introduction

A *cyclotomic integer* is an algebraic integer β that can be written as a sum of roots of unity. Any such β lies in $\mathbb{Z}[\omega_n]$ for some n, where ω_n is a primitive nth root of unity, and it is well known that $\mathbb{Z}[\omega_n]$ is the ring of integers of the field $\mathbb{Q}(\omega_n)$. If $\beta_1 = \beta, \beta_2, \ldots, \beta_d$ are the Galois conjugates of β (or indeed a list that includes each Galois conjugate the same number of times), we define, following Cassels [5], $\mathscr{M}(\beta)$ by

$$\mathscr{M}(\beta) = \frac{1}{d}\sum_{j=1}^{d} |\beta_j|^2.$$

Let us call this value the *Cassels height of* β. Because, as first noted by Robinson [15], the $|\beta_j|^2$ are the conjugates of $|\beta|^2$ (something that is not true for algebraic integers generally), $\mathscr{M}(\beta)$ is rational, with denominator dividing d. From the AM-GM inequality it follows immediately that $\mathscr{M}(\beta) \geq 1$ for $\beta \neq 0$. Two nonzero cyclotomic integers are said to be *equivalent* if dividing the first by some conjugate of the second gives a root of unity. Equivalent cyclotomic integers have the same Cassels height.

The aim of this paper is to study the set

$$\mathscr{C} = \{\mathscr{M}(\beta) \mid \beta \text{ a nonzero cyclotomic integer}\}.$$

This set has an interesting structure. In 2009 Stan and Zaharescu [19, Theorem 4] proved the following results concerning $\mathscr{C}$:

(i) **Closure.** The set $\mathscr{C}$ is a closed subset of $\mathbb{Q}$. (See also [4, Theorem 9.1.1]).

(ii) **Additivity.** The set $\mathscr{C}$ is closed under addition. (This also follows from (i) and Proposition 10 below.)

2010 *Mathematics Subject Classification.* 11D85, 11R18.

Key words and phrases. cyclotomic integers, Cassels height, universal quadratic polynomials.

(iii) For every rational number $r \in [0,1)$ there is an integer n_0 such that $r+n \in \mathscr{C}$ for all $n \geq n_0$.

They applied their results to deducing facts about character values of finite groups.

Recall that the *derived set* of a set S of real numbers is the set, $S^{(1)}$ say, of its limit points. More generally, for $S^{(0)} := S$ and $k \geq 1$ we call the derived set of $S^{(k-1)}$ *the kth derived set of* S, and denote it by $S^{(k)}$.

We extend (i) and (ii) to obtain the following results, connecting the kth derived set $\mathscr{C}^{(k)}$ of $\mathscr{C}$ and the Minkowski sumset

$$k\mathscr{C} := \{c_1 + c_2 + \cdots + c_k \mid c_1, c_2, \ldots, c_k \in \mathscr{C}\}. \tag{1}$$

Theorem 1. *For $k \geq 1$ the kth derived set $\mathscr{C}^{(k)}$ of $\mathscr{C}$ is equal to the sumset $(k+1)\mathscr{C}$. Furthermore every element of $\mathscr{C}^{(k)}$ is a limit from both sides of elements of $\mathscr{C}^{(k-1)}$.*

The following is an immediate consequence.

Corollary 2. *The smallest element of $\mathscr{C}^{(k)}$ $(k \geq 0)$ is $k+1$. Furthermore, a stronger version of additivity holds, namely that $\mathscr{C}^{(k)} + \mathscr{C}^{(\ell)} = \mathscr{C}^{(k+\ell+1)}$ $(k, \ell \geq 0)$.*

Sets having similar topological (though not algebraic) structure as $\mathscr{C}$ have been found before. Salem [16] proved that the set S of all Pisot-Vijayaraghavan (PV) numbers is closed in $\mathbb{R}$. The sets $S^{(k)}$ are known to be nonempty, with the smallest element being at least $\sqrt{k}$ – see [1]. Also, Boyd and Mauldin in 1996 [3] proved that for $k \geq 1$ every member of $S^{(k)}$ is a limit from both sides of elements of $S^{(k-1)}$. This enabled them to specify the order type of S. With this in mind, and recalling that Axel Thue [20] was the discoverer of the PV numbers, we define a *Thue set* T to be a subset of the positive real line with the following properties:

(i) The set T is a closed subset of $\mathbb{R}_+$;
(ii) For $k \geq 1$ the kth derived set $T^{(k)}$ of T is nonempty, and every element of it is a limit from both sides of elements of $T^{(k-1)}$;
(iii) $t_k := \min\{t \mid t \in T^{(k)}\} \to \infty$ as $k \to \infty$.

So S is a Thue set.

Corollary 3. *The set $\mathscr{C}$ is a Thue set.*

It is immediately clear that all derived sets of a Thue set are again Thue sets. In particular all the derived sets $\mathscr{C}^{(k)}$ for $k \geq 1$ are also Thue sets.

It may be that the set of all Mahler measures of polynomials in any number of variables and having integer coefficients also forms a Thue set. Boyd [2] conjectured that this set is closed. There is some further evidence for the set being a Thue set in [18].

Our second main result concerns the set of those $\mathscr{M}(\beta)$ where, for a given odd prime p, β is a sum of $2p$th roots of unity. We denote this set by $\mathscr{C}_p$, so that

$$\mathscr{C}_p = \{\mathscr{M}(\beta) \mid \beta \in \mathbb{Z}[\omega_p]\},$$

where ω_p is a primitive pth root of unity.

Theorem 4. *For all primes $p \geq 5$ the set $\mathscr{C}_p$ is given by*

$$\mathscr{C}_p = \left\{ \frac{1}{p'} \left(\tfrac{1}{2} s(p-s) + rp \right) \mid s = 0, 1, \ldots, p' \text{ and } r \geq 0 \right\}. \tag{2}$$

Here $p' := (p-1)/2$.

It is easy to check that the elements specified by (2) are all distinct.

For $p = 3$ the set $\mathscr{C}_3$ a proper subset of the set given by the RHS of (2). Indeed $\mathscr{C}_3$ is easily seen to be the set of integers of the form $(a + b\omega_3)(a + b\omega_3^2) = a^2 - ab + b^2$, namely all integers N with prime factorisation of the form $N = \prod_q q^{e_q}$, where e_q is even for all primes $q \equiv 2 \pmod 3$. However for $p = 3$ the set on the RHS of (2) consists of all integers $N \not\equiv 2 \pmod 3$. So for instance $6, 10, 15$ and 18 belong to this set, but do not belong to $\mathscr{C}_3$.

For the proof in the case $p = 5$ we need to prove the universality of two ternary quadratic polynomials.

Theorem 5. *Each of the quadratic polynomials*

$$a^2 + ab + b^2 + c^2 + a + b + c \tag{3}$$

and

$$a^2 + b^2 + c^2 + ab + bc + ca + a + b + c \tag{4}$$

represents all positive integers for integer values of their variables (i.e., each is **universal***).*

Of course it would be interesting to study $\mathscr{C}_n := \{\mathscr{M}(\beta) \mid \beta \in \mathbb{Z}[\omega_n]\}$ for n composite, too.

1.1. **Background.** The study of cyclotomic integers began in earnest with a paper of Raphael Robinson in 1965 [15]. In it he stated two problems and proposed five conjectures about them. Schinzel [17] solved his second problem and proved his third conjecture. In 1968 Jones [6] proved Robinson's fifth conjecture. Cassels solved Robinson's Conjecture 2 in [5], with the help of his $\mathscr{M}$ function. Loxton [10] solved Robinson's first problem, and also improved on Schinzel's solution of the second problem. In 2013 F. Robinson and M. Wurtz [14] proved Robinson's fourth conjecture. (They also said that the first conjecture had been proved, although this does not seem to be the case.)

Cassels [5] also showed that the only $\mathscr{M}(\beta) < 2$ were for β that can be written as a sum of at most two roots of unity; this implies that 2 is the smallest limit point of $\mathscr{C}$.

In 2011 Calegari, Morrison and Snyder [4] studied cyclotomic integers β with a view to applications to fusion categories and subfactors. As part of this study (their Theorem 9.0.1) they found all β with $\mathscr{M}(\beta) < 9/4$.

2. Proof of Theorem 1

For the proof, we need a qualitative version of a very precise theorem of Loxton.

Theorem 6 ([9, eqn. (6.1)]). *There is a strictly increasing (concave) function g such that for every cyclotomic integer β we have $\mathscr{M}(\beta) \geq g(\mathscr{N}(\beta))$.*

Here $\mathscr{N}(\beta)$ is the smallest number of roots of unity whose sum is β. Thus, given $B > 0$ there is a number $B' > 0$ such that if $\mathscr{M}(\beta) \leq B$ then $\mathscr{N}(\beta) \leq B'$.

For any algebraic integer α we denote the 'mean trace' (trace $(\alpha))/[\mathbb{Q}(\alpha) : \mathbb{Q}]$ of α by $\overline{\mathrm{tr}}(\alpha)$. This is the mean of the conjugates of α. So $\mathscr{M}(\beta) = \overline{\mathrm{tr}}(|\beta|^2)$. We need the following basic property of the mean trace.

Lemma 7. *For any algebraic numbers α, γ we have*

$$\overline{\mathrm{tr}}(\alpha + \gamma) = \overline{\mathrm{tr}}(\alpha) + \overline{\mathrm{tr}}(\gamma). \tag{5}$$

Proof. Let F be the normal closure of $\mathbb{Q}(\alpha, \gamma)$. Then

$$\overline{\mathrm{tr}}(\alpha) = \frac{1}{[F : \mathbb{Q}]} \sum_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \sigma(\alpha),$$

from which, using the corresponding formula for β and for $\alpha + \beta$, the result follows. □

Lemma 8. *For β a nonzero cyclotomic integer, with say $\beta \in \mathbb{Z}[\omega_n]$, there is some power ω_n^i of ω_n such that $\omega_n^i \beta$ has nonzero trace.*

Proof. We can write $\beta = \sum_{k=0}^{d-1} a_k \omega_n^k$, where the a_k are integers, and $d = \varphi(n)$. Then the trace of β (the sum of its conjugates) is

$$\frac{d'}{d} \sum_{\substack{j=1 \\ \gcd(j,n)=1}}^{d-1} \sum_{k=0}^{d-1} a_k \omega_n^{jk},$$

where $d' = [\mathbb{Q}(\beta) : \mathbb{Q}]$. Suppose that the trace of $\omega_n^i \beta$ is 0 for all $i = 0, \ldots, n-1$. Then the traces of all $a_k \omega_n^{-k} \beta$ would be 0, and so the trace of $\sum_{k=0}^{d-1} a_k \omega_n^{-k} \beta = |\beta|^2$ would be 0. But we know that the conjugates, $|\beta_j|^2$ say, of $|\beta|^2$ are all positive, so its trace is positive. □

We use $\mu_\varphi(n)$ to denote $\mu(n)/\varphi(n)$, where μ is the Möbius μ-function, and φ is the Euler φ-function. Thus the mean trace of ω_n is $\mu_\varphi(n)$. Lemma 7 states that the mean trace is additive. Of course it is not generally multiplicative, but there is a special case where this property too holds.

Lemma 9. *Let m, n be coprime integers and let $\alpha \in \mathbb{Q}(\omega_n)$. Then*

(i) $\overline{\mathrm{tr}}(\omega_m \alpha) = \overline{\mathrm{tr}}(\omega_m)\overline{\mathrm{tr}}(\alpha) = \mu_\varphi(m)\overline{\mathrm{tr}}(\alpha)$*;*

(ii) if also m is odd, one still has $\overline{\mathrm{tr}}(\omega_{2m}\alpha) = \overline{\mathrm{tr}}(\omega_{2m})\overline{\mathrm{tr}}(\alpha) = -\mu_\varphi(m)\overline{\mathrm{tr}}(\alpha)$*, regardless of the parity of n.*

Proof. Since m and n are coprime, $\omega_m \omega_n$ is a primitive mn-th root of unity, and the $\varphi(mn)$ automorphisms of $\mathbb{Q}(\omega_m \omega_n)$ are defined by $\omega_m \omega_n \mapsto \omega_m^a \omega_n^b$ where a is coprime to m and b is coprime to n. From this the formula in (i) is immediate. For (ii), given m is odd one has that $-\omega_{2m}$ is a primitive mth root of unity and since $\overline{\mathrm{tr}}(-\beta) = -\overline{\mathrm{tr}}(\beta)$ one deduces (ii) from (i). □

Proposition 10. *Let $\mathcal{L}$ be an infinite increasing sequence of positive integers, and γ_1 and γ_2 be nonzero cyclotomic integers. Then*

$$\lim_{\substack{\ell\to\infty\\ \ell\in\mathcal{L}}} \mathscr{M}(\gamma_1+\omega_\ell\gamma_2) = \mathscr{M}(\gamma_1)+\mathscr{M}(\gamma_2).$$

Also, $\mathcal{L}$ can be chosen so that infinitely many of the values $\mathscr{M}(\gamma_1+\omega_\ell\gamma_2)$ are distinct, so that $\mathscr{M}(\gamma_1)+\mathscr{M}(\gamma_2)$ is a genuine limit point of the sequence $\{\mathscr{M}(\gamma_1+\omega_\ell\gamma_2)\}_{\ell\in\mathcal{L}}$. Furthermore, $\mathcal{L}$ can be chosen so that the limit is approached either from above or from below.

Proof. Now from Lemma 7

$$\begin{aligned}\mathscr{M}(\gamma_1+\omega_\ell\gamma_2) &= \overline{\mathrm{tr}}(|\gamma_1+\omega_\ell\gamma_2|^2)\\ &= \mathscr{M}(\gamma_1)+\mathscr{M}(\gamma_2)+\overline{\mathrm{tr}}(\omega_\ell^{-1}\gamma_1\overline{\gamma_2})+\overline{\mathrm{tr}}(\omega_\ell\overline{\gamma_1}\gamma_2). \qquad (6)\end{aligned}$$

Choosing n so that $\gamma_1,\gamma_2\in\mathbb{Q}(\omega_n)$, with say

$$\gamma_1\overline{\gamma_2} = \sum_k a_k\omega_n^k,$$

we see that

$$\overline{\mathrm{tr}}(\omega_\ell^{-1}\gamma_1\overline{\gamma_2}) = \overline{\mathrm{tr}}(\omega_\ell\overline{\gamma_1}\gamma_2) = \sum_k a_k\overline{\mathrm{tr}}(\omega_\ell\omega_n^{-k}) = \sum_k a_k\overline{\mathrm{tr}}(\omega_{\ell'}) = \sum_k a_k\mu_\varphi(\ell'),$$

where $\omega_\ell\omega_n^{-k}=\omega_{\ell'}$, say, where ℓ' depends on k. Since $\ell'\to\infty$ as $\ell\to\infty$, and $\mu_\varphi(\ell')\to 0$ as $\ell'\to\infty$, we see that as $\ell\to\infty$

$$\mathscr{M}(\gamma_1+\omega_\ell\gamma_2)\to\mathscr{M}(\gamma_1)+\mathscr{M}(\gamma_2),$$

as claimed.

To ensure that this is a genuine limiting process, we need to have $\mathscr{M}(\gamma_1+\omega_\ell\gamma_2)\neq\mathscr{M}(\gamma_1)+\mathscr{M}(\gamma_2)$ for infinitely many values of ℓ. We now show that $\mathcal{L}$ can be chosen so that this is true.

From Lemma 8, we can choose an integer i such that $\overline{\mathrm{tr}}(\omega_n^i\overline{\gamma_1}\gamma_2)\neq 0$. Then also $\overline{\mathrm{tr}}(\omega_n^{-i}\gamma_1\overline{\gamma_2})\neq 0$. Next, define the sequence $\mathcal{L}$ of integers ℓ by $\omega_\ell=\omega_{\ell^*}\omega_n^i$, where the integers ℓ^* are odd primes not dividing n. Then, using Lemma 9(i),

$$\overline{\mathrm{tr}}(\omega_\ell\overline{\gamma_1}\gamma_2) = \overline{\mathrm{tr}}(\omega_{\ell^*}\,\omega_n^i\overline{\gamma_1}\gamma_2) = \overline{\mathrm{tr}}(\omega_{\ell^*})\overline{\mathrm{tr}}(\omega_n^i\overline{\gamma_1}\gamma_2) = -\frac{1}{\ell^*-1}\overline{\mathrm{tr}}(\omega_n^i\overline{\gamma_1}\gamma_2),$$

which is nonzero for all ℓ. Hence, from (6), $\mathscr{M}(\gamma_1+\omega_\ell\gamma_2)$ tends to $\mathscr{M}(\gamma_1)+\mathscr{M}(\gamma_2)$ from either above or below (say, above), depending on the sign of $\overline{\mathrm{tr}}(\omega_n^i\overline{\gamma_1}\gamma_2)$; it never equals $\mathscr{M}(\gamma_1)+\mathscr{M}(\gamma_2)$.

Finally, if we replace ℓ^* by $2\ell^*$ in the argument (and see Lemma 9(ii)), then $-\frac{1}{\ell^*-1}$ is replaced by $\frac{1}{\ell^*-1}$, so that $\mathscr{M}(\gamma_1+\omega_\ell\gamma_2)$ tends to $\mathscr{M}(\gamma_1)+\mathscr{M}(\gamma_2)$ from below. ☐

Note that Proposition 10 tells us that $2\mathscr{C}\subseteq\mathscr{C}^{(1)}$.

Proposition 11. *Let $\gamma_0, \gamma_1, \dots, \gamma_r$ be fixed cyclotomic integers, and for all $n \geq 1$ define*

$$\beta_n := \gamma_0 + \gamma_1\omega_{n_1} + \gamma_2\omega_{n_2} + \cdots + \gamma_r\omega_{n_r},$$

where $n_1, \dots, n_r$ are integers each tending to infinity as $n \to \infty$, and such that for all k, ℓ with $1 \leq k < \ell \leq r$ the order of $\omega_{n_\ell}/\omega_{n_k}$ also tends to infinity as $n \to \infty$. Then the sequence $\{\mathscr{M}(\beta_n)\}$ converges, say to $\mathscr{M}(\beta)$, with

$$\mathscr{M}(\beta) = \mathscr{M}(\gamma_0) + \mathscr{M}(\gamma_1) + \cdots + \mathscr{M}(\gamma_r).$$

Proof. Now putting $n_0 = 1$ we have

$$|\beta_n|^2 = \sum_{k=0}^{r} |\gamma_k|^2 + \sum_{\substack{k,\ell=0\\ k\neq\ell}}^{r} \gamma_k\overline{\gamma_\ell}\frac{\omega_{n_k}}{\omega_{n_\ell}}.$$

Choose an integer t so that all the γ_k belong to $\mathbb{Z}[\omega_t]$. Then taking the mean trace of this expression we obtain $\mathscr{M}(\beta_n) = \sum_{k=0}^{r} \mathscr{M}(\gamma_k)$ plus a sum of terms of the form $\overline{\mathrm{tr}}(a\omega_t^h\omega_{n_k}/\omega_{n_\ell})$, where a and h are integers. Putting $\omega_t^h\omega_{n_k}/\omega_{n_\ell} = \omega_N$ say, we have

$$\overline{\mathrm{tr}}(a\omega_t^h\omega_{n_k}/\omega_{n_\ell}) = a\mu_\varphi(N).$$

Since $N \to \infty$ as $n \to \infty$ we see that as $n \to \infty$ these terms all tend to 0, so that $\mathscr{M}(\beta_n) \to \sum_{k=0}^{r} \mathscr{M}(\gamma_k)$. □

Proposition 12. *Let $k \geq 1$. Every element of $(k+1)\mathscr{C}$ belongs to $\mathscr{C}^{(k)}$ and is a limit from both sides of elements of $k\mathscr{C}$.*

Proof. The case $k = 1$ has been done in Proposition 10. So take $k \geq 2$ and assume the result is true for $k-1$. For cyclotomic integers $\gamma_1, \dots, \gamma_k, \gamma_{k+1}$, consider

$$m_{k+1} := \mathscr{M}(\gamma_1) + \cdots + \mathscr{M}(\gamma_k) + \mathscr{M}(\gamma_{k+1}) \in (k+1)\mathscr{C}.$$

By the induction hypothesis, for fixed ℓ the value

$$m_{k,\ell} := \mathscr{M}(\gamma_1) + \cdots + \mathscr{M}(\gamma_{k-1}) + \mathscr{M}(\gamma_k + \omega_\ell\gamma_{k+1})$$

belongs to $\mathscr{C}^{(k-1)}$, and is a limit from above of elements of $(k-1)\mathscr{C}$. Using Proposition 10 again, we see that m_{k+1} is a limit from above of elements of $k\mathscr{C} \subseteq \mathscr{C}^{(k-1)}$, namely the $m_{k,\ell}$, as $\ell \to \infty$, for ℓ in some sequence $\mathcal{L}$. Hence $m_{k+1} \in \mathscr{C}^{(k)}$. Since we can replace 'above' by 'below' in the two previous sentences, this proves the result for k.

□

So certainly the kth derived set $\mathscr{C}^{(k)}$ of $\mathscr{C}$ contains $(k+1)\mathscr{C}$. We need to show that in fact equality holds.

Proof of Theorem 1. The theorem holds trivially for $k = 0$. So take $k \geq 1$ and assume that it holds for $k-1$. We need to prove that $\mathscr{C}^{(k)} \subseteq (k+1)\mathscr{C}$. Take $\mathscr{M}(\beta) \in \mathscr{C}^{(k)}$. Then $\mathscr{M}(\beta)$ is a genuine limit of a convergent sequence $\{\mathscr{M}(\beta_n)\}_{n\in\mathbb{N}}$ say, in $\mathscr{C}^{(k-1)}$. By the induction hypothesis, $\mathscr{C}^{(k-1)} \subseteq k\mathscr{C}$, so that for each β_n there are cyclotomic integers γ_{in} $(i = 1, \dots, k)$ such that

$$\mathscr{M}(\beta_n) = \mathscr{M}(\gamma_{1n}) + \mathscr{M}(\gamma_{2n}) + \cdots + \mathscr{M}(\gamma_{kn}). \tag{7}$$

Now the sequence $\{\mathscr{M}(\beta_n)\}$ is bounded, so the sequences $\{\mathscr{M}(\gamma_{in})\}$ $(i = 1,\dots,k)$ are also bounded, with the same bound, B say. Thus by replacing $\{\mathscr{M}(\gamma_{in})\}$ by an appropriate subsequence we can assume that each $i = 1,\dots,k$ the sequence $\{\mathscr{M}(\gamma_{in})\}$ converges. Because the set $\mathscr{C}$ is closed, the limit will be $\mathscr{M}(\gamma_{i\infty})$, say, for some cyclotomic integer $\gamma_{i\infty}$. Note too that $\mathscr{M}(\gamma_{i\infty})$ must be a genuine limit point of $\{\mathscr{M}(\gamma_{in})\}$ for at least one value of i.

Further, by Loxton's Theorem 6, there is an integer N' such that all γ_{in} can be expressed as the sum of at most N' roots of unity. Hence by replacing $\{\mathscr{M}(\beta_n)\}$ by a suitable subsequence we may assume that for each i the numbers γ_{in} can be expressed as the sum of the same number, N_i say, of roots of unity. By writing each γ_{in} as a sum of a minimal number $\mathscr{N}(\gamma_{in})$ of roots of unity, we will have $\mathscr{N}(\gamma_{in}) = N_i$ for each n.

We now study one of these sequences $\{\mathscr{M}(\gamma_{in})\}$. For this purpose we temporarily drop the 'i' subscript, and study the convergent sequence $\{\mathscr{M}(\gamma_n)\}$, where each γ_n is the sum of the same number, N say, of roots of unity. By replacing γ_n by an equivalent cyclotomic integer we can assume that

$$\gamma_n = 1 + \sum_{j=2}^{N} \rho_{jn}, \tag{8}$$

say. By re-ordering the roots of unity, if necessary, we can also assume that the orders of these roots of unity increase nonstrictly monotonically with j. Consider the sequence $\{\rho_{2n}\}_{n\in\mathbb{N}}$. If infinitely many of these roots of unity are equal, then we can replace $\{\mathscr{M}(\beta_n)\}$ by an infinite subsequence so that all the ρ_{2n}'s are equal. We do the same for $\{\rho_{3n}\}$, $\{\rho_{4n}\},\dots,$ until we find a j_1 for which $\{\rho_{j_1n}\}$ contains only finitely many copies of every root of unity. In this situation the order of ρ_{j_1n} tends to infinity with n. We can then rewrite (8) as

$$\gamma_n = s_0 + \rho_{j_1n} + \rho_{j_1+1,n} + \cdots \tag{9}$$

where s_0 is a sum of roots of unity, all independent of n. Note that such a term $\rho_{j_1,n}$ must exist for all i with the property that $\mathscr{M}(\gamma_{i\infty})$ is a genuine limit point of $\{\mathscr{M}(\gamma_{in})\}$.

We now temporarily modify (9) to

$$\gamma_n = s_0 + \rho_{j_1n}(1 + \rho'_{j_1+1,n} + \rho'_{j_1+2,n} + \cdots). \tag{10}$$

say. We then reorder the sequence $\rho'_{j_1+1,n}, \rho'_{j_1+2,n}, \dots, \rho'_{N,n}$ so that their orders as roots of unity are (nonstrictly) monotonically increasing. If the sequence $\{\rho'_{j_1+1,n}\}_{n\in\mathbb{N}}$ has infinitely many equal terms, then we can take an infinite subsequence of $\{\mathscr{M}(\beta_n)\}$ where $\{\rho'_{j_1+2,n}\}$ is constant. We do the same for $\{\rho'_{j_1+2,n}\}$, if possible. We continue in this way until we encounter a sequence, $\{\rho_{j_2n}\}$ say, that contains only finitely many copies of each root of unity; we then define

$$s_1 := 1 + \sum_{j=j_1+1}^{j_2-1} \rho'_{jn}$$

so that we can rewrite (10) as

$$\gamma_n = s_0 + \rho_{j_1n}s_1 + \rho_{j_2n}(1 + \rho'_{j_2+1,n} + \rho'_{j_2+2,n} + \cdots). \tag{11}$$

Note that the order of ρ_{j_2n}/ρ_{j_1n} tends to infinity with n.

Continuing in this way, we can finally write γ_n as

$$\gamma_n = s_0 + \rho_{j_1n}s_1 + \rho_{j_2n}s_2 + \cdots + \rho_{j_rn}s_r, \tag{12}$$

where $r \geq 1$ for at least one value of i, and $s_0, s_0, \ldots, s_r$ are sums of roots of unity, all independent of n. In general they will, of course, depend on the (dropped) subscript i. Also, all of the s_k's must be nonzero, as γ_n has been written as the sum of a minimal number of roots of unity. Furthermore, for $k = 1, \ldots, r$ and $\ell = k+1, \ldots, r$ the order of $\rho_{j_\ell n}/\rho_{j_k n}$ tends to infinity with n. For if the sequence {order of $\rho_{j_\ell n}/\rho_{j_k n}$} were bounded, then we could assume, by the above subsequence argument, that it would be constant. Then the term $\rho_{j_\ell n} = \rho_{j_k n}(\rho_{j_\ell n}/\rho_{j_k n})$ would already have contributed a root of unity to s_k.

From (12) and Proposition 11 we see that $\mathscr{M}(\gamma_n) \to \mathscr{M}(s_0) + \mathscr{M}(s_1) + \cdots + \mathscr{M}(s_r)$ as $n \to \infty$. On reinstating the dropped subscript i, and applying this result to each sequence $\{\mathscr{M}(\gamma_{in})\}$, we see that for each i the limit of this sequence is a sum of $r_i := 1 + r$ elements of $\mathscr{C}$. We have seen above that $r_i \geq 2$ for at least one value of i, so that from (7) that $\mathscr{M}(\beta) = \lim_{n\to\infty} \mathscr{M}(\beta_n)$ is a sum of $k + t$ elements of $\mathscr{C}$, where $t \geq 1$. Since by additivity we can express a sum of t elements of $\mathscr{C}$ as a single element of $\mathscr{C}$, we have $\mathscr{M}(\beta) \in (k+1)\mathscr{C}$, as required. □

This completes the proof of Theorem 1. We now know that $\mathscr{C}$ is a countable closed set, having nonempty derived sets of all orders k, with every element of $\mathscr{C}^{(k)}$ being a two-sided limit of elements of $\mathscr{C}^{(k-1)}$, and with the smallest element of the kth derived set tending to infinity as k goes to infinity. Thus $\mathscr{C}$ is a Thue set, proving Corollary 3.

2.1. **Structure and labelling of Thue sets.** Two totally ordered sets are said to have the *same order type* if there is an order-preserving bijection between them. The *order type* of a set is then the ordinal having the same order type as the set. For the ordinal ω, put $a_1 = \omega + 1 + \omega^*$, and $a_{n+1} = a_n\omega + 1 + (a_n\omega)^*$ for $n \geq 1$. Here $()^*$ denotes the reverse order. Boyd and Mauldin [3] showed that the order type of the set of PV numbers is $\sum_{n=1}^{\infty} a_n$.

Let T be any Thue set. We will now build a finite string of integers to label a given element t of T. We proceed as follows. If $t < t_1$ then t is an element of the increasing sequence of all members of T that are less than t_1, which we label $\ell_{00}, \ell_{01}, \ell_{02}, \ldots$. For $t \geq t_1$ choose the largest k such that $t \geq t_k$. Take k as the first element of our string. Then there are no limit points of $T^{(k)}$ (i.e., elements of $T^{(k+1)}$) that are less than t, so that $T^{(k)}$ is discrete in the interval $[t_k, t_{k+1})$, which must contain t. We label the elements of $[t_k, t_{k+1}) \cap T^{(k)}$ in ascending order by $\ell_{k0}, \ell_{k1}, \ell_{k2}, \ldots$. Then t is in one of the half-open intervals $[\ell_{kr}, \ell_{k,r+1})$ say; we take r to be the second element of our string. If $t = \ell_{kr}$, end the string. Otherwise, we note that the elements of $T^{(k-1)}$ in the interval $(\ell_{kr}, \ell_{k,r+1})$ form a countable set with limit points precisely at both endpoints of the interval. For definiteness we label those in $[\frac{1}{2}(\ell_{kr} + \ell_{k,r+1}), \ell_{k,r+1})$ by $\ell_{kr0}, \ell_{kr1}, \ell_{kr2}, \ldots$ in ascending order, and those in $[\ell_{kr}, \frac{1}{2}(\ell_{kr} + \ell_{k,r+1}))$ by $\ell_{kr,-1}, \ell_{kr,-2}, \ell_{kr,-3}, \ldots$, in descending order. Again, t is in one of the half-open intervals defined by these points, so we label it by the left endpoint. Again, if t is equal to this endpoint, the label ends. Otherwise, we note that in the open interval there is a countable ascending string of elements of $T^{(k-2)}$ with limit points precisely at both endpoints of the interval. So we can proceed as before. Continuing in this way, the string ends by t being a left endpoint of an interval (the elements with the longest strings will be those t in an interval whose endpoints are in $T \setminus T^{(1)}$. Then t must equal the left endpoint of such an interval. Thus, in the end, every element of T is of the form ℓ_s, where s is a string of integers, which we call the *label* of ℓ_s; we have seen that s is of the form $s = kr_1 \cdots r_j$, where $k \geq 0$ and $1 \leq j \leq k+1$. This tells us that $t_k \leq t < t_{k+1}$ and that $t \in T^{(k-j+1)} \setminus T^{(k-j+2)}$.

The labelling described is ordered by the most significant digits, with the added rule that if two strings are of different lengths, but agree for the whole length of the shorter one, then this shorter one comes first in the ordering. Then this ordering coincides with the ordering on the real line.

Note that the allowable integer string labels are subject to the following constraints:

- The first term, k, is non-negative;
- If $k = 0$ then the second term is non-negative;
- The string must contain between 2 and $k+2$ terms.

Proposition 13. *Any two Thue sets have the same order type.*

3. Proof of Theorem 5.

Proof. First, note that for any integer $m \geq 0$

$$a^2 + ab + b^2 + c^2 + a + b + c = m$$

has an integer solution if and only if

$$3(2a + b + 1)^2 + (3b + 1)^2 + 3(2c + 1)^2 = 12m + 7$$

has an integer solution. Note that the class number of $x^2 + 3y^2 + 3z^2$ is 1 by [7], and by using [13, §102.5] and [12], one may easily check that there are integers x, y, and z such that

$$x^2 + 3y^2 + 3z^2 = 12m + 7.$$

Since x is not divisible by 3, by changing, if necessary, the sign of x, there is an integer b such that $3b + 1 = x$. Assume that x is even. Then b is odd. In this case, since $y - z$ is odd, without loss of generality, we may assume that y is odd. Therefore there are integers a and c such that

$$2a + b + 1 = z, \quad 2c + 1 = y.$$

Now, assume that x is odd. Then b is even and both y and z are odd. Therefore there are integers a and c satisfying the above. Thus (3) is universal, as claimed.

Next, note that any integer $m \geq 0$, the equation

$$a^2 + b^2 + c^2 + ab + bc + ca + a + b + c = m$$

has an integer solution if and only if

$$6(2a + b + c + 1)^2 + 2(3b + c + 1)^2 + (4c + 1)^2 = 24m + 9$$

has an integer solution. Note that the class number of $x^2+2y^2+6z^2$ is 1 by [7], and by again using [13, §102.5], one may easily check that there are integers x, y, and z such that

$$x^2+2y^2+6z^2=24m+9.$$

Since x is odd, by changing the sign of x, if necessary, there is an integer c such that $4c+1=x$. Note that x is divisible by 3 if and only if y is divisible by 3. Hence there is an integer b such that $3b+c+1=y$ by changing, if necessary, the sign of y. Finally, since $y \equiv z \pmod 2$, there is an integer a such that $2a+b+c+1=z$. Thus (4) is universal. □

4. Proof of Theorem 4.

Proof. For p an odd prime, let $\beta=\sum_{i=0}^{p-1} a_i\omega_p^i \in \mathbb{Z}[\omega_p]$. These coefficients a_i are not uniquely determined by β: we can replace each a_i by a_i+t for any $t\in\mathbb{Z}$. Thus we can assume that $s:=\sum_{j=0}^{p-1} a_j \in [-p', p']$, where $p':=(p-1)/2$. In fact, since $\mathscr{M}(-\beta)=\mathscr{M}(\beta)$, we can assume for the study of $\mathscr{C}_p$ that s is an integer in $[0,p']$. Also write $\operatorname{var}(a_0,\ldots,a_{p-1})$ for the variance of $a_0,\ldots,a_{p-1}$. We need the following.

Lemma 14. *We have*

$$p'\mathscr{M}(\beta)=\frac{1}{2}\left(p\sum_{j=0}^{p-1}a_j^2-s^2\right) \tag{13}$$

$$=\frac{p^2}{2}\operatorname{var}(a_0,\ldots,a_{p-1})\,. \tag{14}$$

Proof of Lemma 14. We have

$$\begin{aligned}p'\mathscr{M}(\beta)&=\tfrac{1}{2}\sum_{i=1}^{p-1}\left(\sum_{j=0}^{p-1}a_j\omega_p^{ij}\sum_{k=0}^{p-1}a_k\omega_p^{-ik}\right)\\&=\tfrac{1}{2}\sum_{j=0}^{p-1}\sum_{k=0}^{p-1}a_ja_k\left(\sum_{i=1}^{p-1}\omega_p^{i(j-k)}\right)\\&=\tfrac{1}{2}\sum_{j=0}^{p-1}\sum_{k=0}^{p-1}a_ja_k\left(\sum_{i=0}^{p-1}\omega_p^{i(j-k)}-1\right)\\&=\tfrac{1}{2}\left(p\sum_{j=0}^{p-1}a_j^2-s^2\right),\end{aligned}$$

giving (13). This also equals

$$\tfrac{p^2}{2}\left(\tfrac{1}{p}\sum_{j=0}^{p-1}a_j^2-\left(\tfrac{s}{p}\right)^2\right)=\tfrac{p^2}{2}\operatorname{var}(a_0,\ldots,a_{p-1}).$$

□

Thus we can interpret the Cassels height $\mathscr{M}(\beta)$ as a fixed multiple (depending on p) of the variance of the sequence of coefficients a_i of β. Thus, for p and s given, $p'\mathscr{M}(\beta)$ is minimised when the a_i are as close as possible to each other (and to their mean, which lies in $[0, 1/2)$), and the minimum occurs precisely when s of the a_i equal 1, while the remaining $p-s$ are 0. From the formula (13), we see that this minimum of $p'\mathscr{M}(\beta)$ is $\frac{s(p-s)}{2}$. Furthermore, up to permutation of the a_k's, this is the only sequence for which the minimum occurs.

We must now show that for $p'\mathscr{M}(\beta)$ can take all integer values $\frac{s(p-s)}{2}+rp$, for all integers $r \geq 0$. We separate three cases.

- $p \geq 11$. From the s ones and $p-s$ zeroes in $a_0, a_1, \ldots, a_{p-1}$ we can choose $\lfloor \frac{s}{2} \rfloor + \lfloor \frac{p-2}{2} \rfloor > 4$ pairs of equal values (both 1 or both 0). Taking four of these pairs (a, a) and replacing each by $(a+n, a-n)$ for some integer n, we see from (13) that $p'\mathscr{M}(\beta)$ is increased by p times the sum of four squares of integers. Since every nonnegative integer r is the sum of four squares [8], we indeed have that $p'\mathscr{M}(\beta)$ can take every value $\frac{s(p-s)}{2} + rp$.
- $p = 7$. We have $s = 0, 1, 2$ and 3. Let $\underline{a} = (0, 0, 0, 0, 0, a_5, a_6)$, so that $s = a_5 + a_6$. Now change $\underline{a}$ to $\underline{a} = (-a, -b, -c, -d, a+b+c+d, a_5, a_6)$. Then s remains unchanged, while $\sum_{j=0}^{6} a_j^2$ increases by 7/2 times

$$a^2+b^2+c^2+d^2+(a+b+c+d)^2 = 2(a^2+b^2+c^2+d^2+a(b+c+d)+b(c+d)+cd). \quad (15)$$

  This quadratic form, with root lattice A_4, has class number 1 (see Nipp [11]), and locally represents all even integers. Hence by [2, §102.5], it represents all even positive integers. By choosing $a_5, a_6 = 0$ or 1, and so $s = 0, 1$ or 2 we see from (13) that $p'\mathscr{M}(\beta)$ can take all values $\frac{1}{2}s(7-s) + 7r$ for every integer $r \geq 0$, for these values of s. For $s = 3$ and $\underline{a} = (0, 0, 0, 0, 1, 1, 1)$ we change $\underline{a}$ to $\underline{a} = (a, b, c, -(a+b+c), d+1, -d+1, 1)$. Here still $s = 3$, while $\sum_{j=0}^{p-1} a_j^2$ increases by 7/2 times

$$a^2 + b^2 + c^2 + (a+b+c)^2 + (d+1)^2 + (-d+1)^2 = 2(a^2 + (b+c)a + b^2 + bc + c^2 + d^2).$$

  This quadratic form, with root lattice $A_3 \perp A_1$, has class number 1 (see [11]), and locally represents all even integers. Hence by [2, §102.5], it represents all even positive integers. Thus $p'\mathscr{M}(\beta)$ can take all values $\frac{1}{2}s(7-s) + 7r$ for every integer $r \geq 0$ for $s = 3$ also.
- $p = 5$. We have $s = 0, 1$ and 2. The case $s = 0$ is essentially the same as for $p = 7$: take $\underline{a} = (-a, -b, -c, -d, a+b+c+d)$, with again $\sum_{j=0}^{4} a_j^2$ given by (15). For $s = 1$, start with $\underline{a} = (0, 0, 0, 0, 1)$ and change it to $(0, -a, -b, -c, 1+a+b+c)$. Then $\sum_{j=0}^{4} a_j^2$ increases by 5/2 times

$$a^2 + b^2 + c^2 + (1+a+b+c)^2 - 1 = 2(a^2 + b^2 + c^2 + ab + bc + ca + a + b + c).$$

  Hence, by Theorem 5, $p'\mathscr{M}(\beta)$ can take all values $2 + 5r$ for every integer $r \geq 0$. For $s = 2$, start with $\underline{a} = (0, 0, 0, 1, 1)$ and change it to $(-a, -b, -c, 1+a+b, 1+c)$. Then $\sum_{j=0}^{4} a_j^2$ increases by 5/2 times

$$a^2 + b^2 + c^2 + (1+a+b)^2 + (1+c)^2 - 2 = 2(a^2 + ab + b^2 + c^2 + a + b + c).$$

  Hence, again by Theorem 5, $p'\mathscr{M}(\beta)$ can take all values $3 + 5r$ for every integer $r \geq 0$.

□

Note that it follows that, for $\beta \in \mathbb{Z}[\omega_p]$, $\mathscr{M}(\beta)$ depends only on the set $\{a_k\}$ of coefficients of β, and not on their order. (In fact it depends only on $\sum_k a_k$ and $\sum_k a_k^2$.) Thus in general there are many inequivalent $\beta \in \mathbb{Z}[\omega_p]$ with the same value of $\mathscr{M}(\beta)$. Note too that, having established Theorem 4, Lemma 14 provides a description of the possible values of the variance of a sequence of p integers.

References

[1] David W. Boyd. On the successive derived sets of the Pisot numbers. *Proc. Amer. Math. Soc.*, 73(2):154–156, 1979.

[2] David W. Boyd. Speculations concerning the range of Mahler's measure. *Canad. Math. Bull.*, 24(4):453–469, 1981.

[3] David W. Boyd and R. Daniel Mauldin. The order type of the set of Pisot numbers. *Topology Appl.*, 69(2):115–120, 1996.

[4] Frank Calegari, Scott Morrison, and Noah Snyder. Cyclotomic integers, fusion categories, and subfactors. *Comm. Math. Phys.*, 303(3):845–896, 2011.

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

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

[7] B. W. Jones. A table of Eisenstein-reduced positive ternary quadratic forms of determinant ≤ 200. *Bulletin of the National Research Council*, 97, 1935.

[8] P.G.L. Lagrange. Démonstration d'un théorème d'arithmétique. *Mém. Acad. Roy. Sci. Berlin*, 123, 1770. Also Oeuvres. vol. 3 1869, pp. 189–201.

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

[10] J. H. Loxton. On two problems of R. W. Robinson about sums of roots of unity. *Acta Arith.*, 26:159–174, 1974/75.

[11] Gordon L. Nipp. *Quaternary quadratic forms*. Springer-Verlag, New York, 1991. Computer generated tables, https://doi.org/10.1007/978-1-4612-3180-6.

[12] O. T. O'Meara. The integral representations of quadratic forms over local fields. *Amer. J. Math.*, 80:843–878, 1958.

[13] O. T. O'Meara. *Introduction to quadratic forms*. Die Grundlehren der mathematischen Wissenschaften, Bd. 117. Academic Press, Inc., Publishers, New York; Springer-Verlag, Berlin-Göttingen-Heidelberg, 1963.

[14] Frederick Robinson and Michael Wurtz. On the magnitudes of some small cyclotomic integers. *Acta Arith.*, 160(4):317–332, 2013.

[15] Raphael M. Robinson. Some conjectures about cyclotomic integers. *Math. Comp.*, 19:210–217, 1965.

[16] R. Salem. A remarkable class of algebraic integers. Proof of a conjecture of Vijayaraghavan. *Duke Math. J.*, 11:103–108, 1944.

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

[18] Chris Smyth. Closed sets of Mahler measures. *Proc. Amer. Math. Soc.*, 146(6):2359–2372, 2018.

[19] Florin Stan and Alexandru Zaharescu. Siegel's trace problem and character values of finite groups. *J. Reine Angew. Math.*, 637:217–234, 2009.

[20] A. Thue. Über eine Eigenschaft, die keine transzendente Größe haben kann. *Christiania Vidensk. selsk. Skrifter.*, 2(20), 1912. 15 pages.

Department of Mathematics, Royal Holloway, University of London, Egham Hill, Egham, Surrey, TW20 0EX, U.K.
Email address: james.mckee@rhul.ac.uk

Department of Mathematical Sciences and Research Institute of Mathematics, Seoul National University Seoul 08826, Republic of Korea
Email address: bkoh@snu.ac.kr

School of Mathematics, University of Edinburgh, Edinburgh EH9 3FD, Scotland, U.K.
Email address: c.smyth@ed.ac.uk