

LOWER BOUNDS FOR THE MAHLER MEASURE AND INERTIA DEGREES OF PRIMES

SHANTA LAISHRAM  and GOREKH PRASAD  

(Received 21 September 2024; accepted 4 October 2024)

Abstract

We investigate the relationship between lower bounds for the Mahler measure and splitting of primes, and prove various lower bounds for the Mahler measure of algebraic integers in terms of the least common multiples of all inertia degrees of primes. The results generalise work of the second author and Kumar [‘Lehmer’s problem and splitting of rational primes in number fields’, *Acta Math. Hungar.* **169**(2) (2023), 349–358].

2020 *Mathematics subject classification*: primary 11R06; secondary 11G50, 11S15.

Keywords and phrases: Lehmer’s problem, Mahler measure, absolute Weil height, prime factorisation, inertia degree.

1. Introduction

The *Mahler measure* of an algebraic number α , denoted by $M(\alpha)$, is defined by

$$M(\alpha) = |a_d| \prod_{i=1}^d \max\{1, |\alpha_i|\},$$

and its *absolute logarithmic height* (*Weil height*) is defined by

$$h(\alpha) = \frac{\log M(\alpha)}{d}, \tag{1.1}$$

where $\alpha_1, \dots, \alpha_d$ are the conjugates of α over \mathbb{Q} and a_d is the leading coefficient of the minimal polynomial of α over \mathbb{Z} . Kronecker [4] proved that $M(\alpha) = 1$ if and only if α is either zero or a root of unity. In [5], Lehmer investigated algebraic integers with small Mahler measure. He showed that if $\alpha \in \mathbb{C}$ is a root of

$$X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1 = 0,$$

then $M(\alpha) = 1.176\dots$ and could not find any algebraic integer α with $M(\alpha) < 1.176\dots$. Lehmer asked whether there exists a constant $c > 1$ such that $M(\alpha) > c$ for any nonzero

The first author acknowledges the support of a SERB CRG Grant while working during the project.

© The Author(s), 2024. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc.



algebraic integer α which is not a root of unity. This question is now known as *Lehmer’s problem*. Though this problem is still open, it has been solved for various classes of α . If α is a nonreciprocal algebraic integer which is not a root of unity, then Smyth [9] proved that $M(\alpha) \geq 1.3247\dots$, the smallest Pisot number, which is the real root of the polynomial $x^3 - x - 1$. The best unconditional lower bound for $M(\alpha)$ is given by Voutier [10], who improved the lower bound of Dobrowolski [1]. Voutier proved that if α is a nonzero algebraic integer of degree $d > 2$ and is not a root of unity, then $M(\alpha) > 1 + \frac{1}{4}(\log \log d / \log d)^3$.

The relationship between lower bounds for the Mahler measure and splitting of primes has been explored by several mathematicians. For example, Mignotte [6] proved that if there exists a rational prime $p < d \log d$ which is unramified in $\mathbb{Q}(\alpha)$, then $M(\alpha) \geq 1.2$. In particular, by taking $d \geq 3$, if 2 is unramified in $\mathbb{Q}(\alpha)$, then $M(\alpha) \geq 1.2$. In the opposite direction, Garza [3] proved that if 2 is totally ramified in $\mathbb{Q}(\alpha)$, then $M(\alpha) \geq 2^{1/4} = 1.189\dots$. The second author and Kumar [8] generalised Garza’s result by showing that if all the inertia degrees of primes of $\mathcal{O}_{\mathbb{Q}(\alpha)}$ which lie above 2 are equal to one, then $M(\alpha) \geq 2^{1/4}$. Also, in [7], the second author generalised the results of [8] to arbitrary base number fields. We further generalise these results, without putting any conditions on the ramification index, and prove various lower bounds for the Mahler measure of algebraic integers in terms of the least common multiple of all inertia degrees of primes.

THEOREM 1.1. *Fix any $r \in \mathbb{N}$. Let $\bar{f} = (f_1, f_2, \dots, f_r)$ be any r -tuple of natural numbers and $f = \text{lcm}(f_1, \dots, f_r)$. Consider the set $S_{\bar{f}}$ defined by*

$$\{\alpha \in \bar{\mathbb{Q}} : 2\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \cdots \mathcal{P}_r^{e_r} \text{ with } [\mathcal{O}_{\mathbb{Q}(\alpha)} / \mathcal{P}_i : \mathbb{Z} / 2\mathbb{Z}] = f_i \text{ for all } i \in \{1, \dots, r\}\}.$$

Then, for any $\alpha \in S_{\bar{f}}$ which is neither zero nor a root of unity,

$$M(\alpha) \geq \begin{cases} 2^{(f+1)/4(2^f-1)} & \text{if } f \neq 6 \text{ and } f \neq f_i \text{ for all } i \in \{1, \dots, r\}, \\ 2^{1/4(2^f-1)} & \text{if } f = 6 \text{ or } f = f_i \text{ for some } i \in \{1, \dots, r\}. \end{cases}$$

REMARK 1.2. Taking $\bar{f} = (1, 1, \dots, 1)$ in Theorem 1.1 yields [8, Theorem 1]. Also, for any $n \in \mathbb{N}$, by taking $\bar{f} = (n, n, \dots, n)$ in Theorem 1.1, we deduce that if all the inertia degrees of primes of $\mathcal{O}_{\mathbb{Q}(\alpha)}$ which lie above 2 are equal to n , then either $M(\alpha) \geq 2^{1/4(2^n-1)}$ or $M(\alpha) = 1$.

We prove the following result for odd rational primes.

THEOREM 1.3. *Fix any $r \in \mathbb{N}$. Let $\bar{f} = (f_1, f_2, \dots, f_r)$ be any r -tuple of natural numbers with $f = \text{lcm}(f_1, \dots, f_r)$. Let p be any odd rational prime. Define the set $S_{p, \bar{f}}$ by*

$$\{\alpha \in \bar{\mathbb{Q}} : p\mathcal{O}_{\mathbb{Q}(\alpha)} = \mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \cdots \mathcal{P}_r^{e_r} \text{ with } [\mathcal{O}_{\mathbb{Q}(\alpha)} / \mathcal{P}_i : \mathbb{Z} / p\mathbb{Z}] = f_i \text{ for all } i \in \{1, \dots, r\}\}.$$

Then, for any algebraic unit $\alpha \in S_{p, \bar{f}}$ which is neither zero nor a root of unity,

$$M(\alpha) \geq \begin{cases} \left(\frac{p}{2}\right)^{1/p(p^f-1)} & \text{if } (f, p) = (2, 2^s - 1) \text{ for some } s \in \mathbb{N} \\ & \text{or } f = f_i \text{ for some } i \in \{1, \dots, r\}, \\ \left(\frac{p}{2}\right)^{(f+1)/p(p^f-1)} & \text{otherwise.} \end{cases}$$

REMARK 1.4. Taking $\bar{f} = (1, 1, \dots, 1)$ in Theorem 1.3 shows that if all the inertia degrees of primes of $\mathcal{O}_{\mathbb{Q}(\alpha)}$ which lie above p are equal to 1, then $M(\alpha) \geq (p/2)^{1/p(p-1)}$. A similar type of lower bound for $M(\alpha)$ is obtained in [8, Theorem 3] with the additional assumption that $\max\{e_i\}_{1 \leq i \leq r} \leq p \leq \sqrt{[\mathbb{Q}(\alpha) : \mathbb{Q}]}$.

We also give generalisations of these results to an arbitrary base number field K .

THEOREM 1.5. Fix any $r \in \mathbb{N}$. Let $\bar{f} = (f_1, f_2, \dots, f_r)$ be any r -tuple of natural numbers. Let K be a number field of degree d over \mathbb{Q} . Let \mathcal{P} be a prime ideal of \mathcal{O}_K which lies above 2. Consider the set $S_{\bar{f}}$ defined by

$$\{\alpha \in \bar{\mathbb{Q}} : \mathcal{P}\mathcal{O}_{K(\alpha)} = \mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \dots \mathcal{P}_r^{e_r}, [\mathcal{O}_{K(\alpha)}/\mathcal{P}_i : \mathcal{O}_K/\mathcal{P}] = f_i \text{ for all } i \in \{1, \dots, r\}\}.$$

Then, for any algebraic unit $\alpha \in S_{\bar{f}}$ which is neither zero nor a root of unity, $M(\alpha) \geq C(K, f)$, where $C(K, f) > 1$ is a constant which depends only on $[K : \mathbb{Q}] = d$ and $f = \text{lcm}(f_1, \dots, f_r)$.

THEOREM 1.6. Fix any $r \in \mathbb{N}$. Let $\bar{f} = (f_1, f_2, \dots, f_r)$ be any r -tuple of natural numbers. Let K be a number field of degree d over \mathbb{Q} . Let \mathcal{P} be a prime ideal of \mathcal{O}_K which lies above the odd prime p . Consider the set $S_{p, \bar{f}}$ defined by

$$\{\alpha \in \bar{\mathbb{Q}} : \mathcal{P}\mathcal{O}_{K(\alpha)} = \mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \dots \mathcal{P}_r^{e_r}, [\mathcal{O}_{K(\alpha)}/\mathcal{P}_i : \mathcal{O}_K/\mathcal{P}] = f_i \text{ for all } i \in \{1, \dots, r\}\}.$$

Then, for any algebraic unit $\alpha \in S_{\bar{f}}$ which is neither zero nor a root of unity, $h(\alpha) \geq c$, where $c > 0$ is a constant which depends only on p , $[K : \mathbb{Q}] = d$ and $f = \text{lcm}(f_1, \dots, f_r)$.

Our paper is organised as follows. In Section 2, we recall necessary results on absolute values on number fields and results on Zsigmondy primes. We will prove Theorems 1.1 and 1.3 in Section 3 and Theorems 1.5 and 1.6 in Section 4.

2. Preliminaries

2.1. Valuations. Let K be a number field and $|\cdot|$ be a nontrivial absolute value on K . It induces a topology on K . Two absolute values on K are said to be equivalent if they induce the same topology on K . In each equivalence class v of nontrivial absolute values, we choose the representative $|\cdot|_v$ which is normalised in the following way:

$$\begin{cases} |x|_v = x & \text{if } x \in \mathbb{Q}, x > 0 \text{ and } v \text{ is Archimedean,} \\ |p|_v = 1/p & \text{if } v \text{ extends the } p\text{-adic absolute value on } \mathbb{Q}. \end{cases}$$

Indeed, if v is Archimedean, then there exists an embedding $\sigma : K \rightarrow \mathbb{C}$ such that $|x|_v = |\sigma(x)|$ for all $x \in K$. Similarly, if v extends the p -adic absolute value on \mathbb{Q} , then there exists a prime ideal \mathcal{P} in \mathcal{O}_K such that $|x|_v = p^{-v_{\mathcal{P}}(x)/v_{\mathcal{P}}(p)}$ for all $x \in K$, where $v_{\mathcal{P}}(x)$ is the exponent of \mathcal{P} appearing in the prime factorisation of the ideal $x\mathcal{O}_K$; set $|x|_v = |x|_{\mathcal{P}}$. Let M_K be the set of all nontrivial normalised absolute values on K . For any $v \in M_K$, let K_v be the completion of K with respect to v and \mathbb{Q}_v be the completion of \mathbb{Q} with respect to the restriction of v to \mathbb{Q} . Put $d_v = [K_v : \mathbb{Q}_v]$. For all $\alpha \in K^\times$, we have the product formula (see [11, page 74])

$$\prod_{v \in M_K} |\alpha|_v^{d_v} = 1. \tag{2.1}$$

For any fixed $w \in M_{\mathbb{Q}}$, we write $v \mid w$ if $v \in M_K$ and the restriction of v to \mathbb{Q} is w . Then we have the degree formula (see [11, page 74])

$$\sum_{v \in M_K, v \mid w} [K_v : \mathbb{Q}_w] = [K : \mathbb{Q}]. \tag{2.2}$$

For any number field K containing α ,

$$h(\alpha) = \frac{1}{[K : \mathbb{Q}]} \sum_{v \in M_K} d_v \log(\max\{1, |\alpha|_v\}) \tag{2.3}$$

(see [11, page 79]). Comparing (1.1) and (2.3) gives

$$M(\alpha) = \prod_{v \in M_{\mathbb{Q}(\alpha)}} \max\{1, |\alpha|_v\}^{d_v}.$$

2.2. Zsigmondy primes. Let a and n be integers greater than 1. A Zsigmondy prime for (a, n) is a prime p such that $p \mid (a^n - 1)$ but $p \nmid (a^i - 1)$ for $1 \leq i < n$. If p is a Zsigmondy prime for (a, n) , then $p \equiv 1 \pmod{n}$ and so $p \geq n + 1$. The following result of Zsigmondy describes the cases in which Zsigmondy primes exist.

LEMMA 2.1 [2, Theorem 2.2]. *If a and n are integers greater than 1, then there exists a Zsigmondy prime for (a, n) unless $(a, n) = (2, 6)$ or $n = 2$ and $a = 2^s - 1$ for some $s \in \mathbb{N}$.*

3. Proof of Theorems 1.1 and 1.3

PROOF OF THEOREM 1.1. Put $K = \mathbb{Q}(\alpha)$. We are given $2\mathcal{O}_K = \mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \dots \mathcal{P}_r^{e_r}$, with $[\mathcal{O}_K/\mathcal{P}_i : \mathbb{Z}/2\mathbb{Z}] = f_i$. So, we have $|\mathcal{O}_K/\mathcal{P}_i| = 2^{f_i}$ for all $i \in \{1, \dots, r\}$. It follows that, $\alpha^{2^{f_i}} - \alpha \in \mathcal{P}_i$ for all $i \in \{1, \dots, r\}$. If α is not a unit, then $M(\alpha) \geq 2$. So, we can assume that α is a unit in \mathcal{O}_K which implies that $\alpha^{2^{f_i}-1} - 1 \in \mathcal{P}_i$ for all $i \in \{1, \dots, r\}$. Let $F = \text{lcm}(2^{f_1} - 1, 2^{f_2} - 1, \dots, 2^{f_r} - 1)$. Since $2^{f_i} - 1 \mid F$ and, for any $n \in \mathbb{N}$,

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \dots + xy^{n-2} + y^{n-1}), \tag{3.1}$$

we deduce that $\alpha^F - 1 \in \mathcal{P}_i$ for all $i \in \{1, \dots, r\}$.

For each $i \in \{1, \dots, r\}$, choose s_i minimal such that $2^{s_i} \geq e_i$. For any fixed i , by the minimality of s_i , we have $2^m \leq e_i$ for each $m = 0, 1, \dots, s_i - 1$. Since $2O_K = \mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \dots \mathcal{P}_r^{e_r} \subseteq \mathcal{P}_i^{e_i} \subseteq \mathcal{P}_i^{2^m}$ for $m = 0, 1, \dots, s_i - 1$, we have $2 \in \mathcal{P}_i^{2^m}$ for $m = 0, 1, \dots, s_i - 1$. Since $2 \in \mathcal{P}_i$ and $\alpha^F - 1 \in \mathcal{P}_i$, we have $\alpha^F - 1 + 2 = \alpha^F + 1 \in \mathcal{P}_i$, whence $\alpha^{2^F} - 1 \in \mathcal{P}_i^2$. Since $2 \in \mathcal{P}_i^{2^m}$ for $m = 0, 1, \dots, s_i - 1$, by repeating this argument, $\alpha^{2^{s_i F}} - 1 \in \mathcal{P}_i^{2^{s_i}} \subseteq \mathcal{P}_i^{e_i}$. Since $2 \in \mathcal{P}_i^{e_i}$, we have $\alpha^{2^{s_i F}} - 1 + 2 = \alpha^{2^{s_i F}} + 1 \in \mathcal{P}_i^{e_i}$. Thus, $\alpha^{2^{s_i+1} F} - 1 \in \mathcal{P}_i^{2e_i}$ for each $i \in \{1, \dots, r\}$.

Define $s = \max\{s_1, s_2, \dots, s_r\}$. Without loss of generality, assume $s = s_1$, so that

$$\alpha^{2^{s+1} F} - 1 \in \mathcal{P}_1^{2e_1}.$$

Take any $i \neq 1$. Then, $\alpha^{2^{s_i+1} F} - 1 \in \mathcal{P}_i^{2e_i}$. Since $2 \in \mathcal{P}_i$ and $\alpha^{2^{s_i+1} F} - 1 \in \mathcal{P}_i$, we have $\alpha^{2^{s_i+1} F} + 1 \in \mathcal{P}_i$, whence $\alpha^{2^{s_i+2} F} - 1 \in \mathcal{P}_i^{2e_i+1}$. Applying the same method inductively yields $\alpha^{2^{s_i+s-s_i+1} F} - 1 \in \mathcal{P}_i^{2e_i+s-s_i}$. Thus, $\alpha^{2^{s+1} F} - 1 \in \mathcal{P}_i^{2e_i+s-s_i} \subseteq \mathcal{P}_i^{2e_i}$. So,

$$|\alpha^{2^{s+1} F} - 1|_{\mathcal{P}_i} \leq 2^{-2e_i/e_i} = \frac{1}{4} \leq \frac{1}{4} \max\{1, |\alpha|_{\mathcal{P}_i}\}^{2^{s+1} F} \quad \text{for all } i \in \{1, \dots, r\}.$$

If $v \mid \infty$, then $|\alpha^{2^{s+1} F} - 1|_v \leq |\alpha|_v^{2^{s+1} F} + 1 \leq 2 \max\{1, |\alpha|_v^{2^{s+1} F}\}$. Thus,

$$|\alpha^{2^{s+1} F} - 1|_v \leq \begin{cases} \frac{1}{4} \max\{1, |\alpha|_v\}^{2^{s+1} F} & \text{if } v \mid 2, \\ \max\{1, |\alpha|_v\}^{2^{s+1} F} & \text{if } v \nmid 2, v \nmid \infty, \\ 2 \max\{1, |\alpha|_v\}^{2^{s+1} F} & \text{if } v \mid \infty. \end{cases} \tag{3.2}$$

Since α is not a root of unity, $\alpha^{2^{s+1} F} - 1 \neq 0$. Applying the product formula (2.1) to the element $\alpha^{2^{s+1} F} - 1$ and using (3.2),

$$\begin{aligned} 0 &= \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log |\alpha^{2^{s+1} F} - 1|_v \\ &\leq \sum_{v \mid 2} [K_v : \mathbb{Q}_v] \{-\log 4 + 2^{s+1} F \max\{0, \log |\alpha|_v\}\} \\ &\quad + \sum_{v \nmid 2, v \nmid \infty} [K_v : \mathbb{Q}_v] \{2^{s+1} F \max\{0, \log |\alpha|_v\}\} \\ &\quad + \sum_{v \mid \infty} [K_v : \mathbb{Q}_v] \{\log 2 + 2^{s+1} F \max\{0, \log |\alpha|_v\}\} \\ &= \sum_{v \mid 2} -[K_v : \mathbb{Q}_v] \log 4 + \sum_{v \mid \infty} [K_v : \mathbb{Q}_v] \log 2 + \sum_{v \in M_K} 2^{s+1} F \max\{0, \log |\alpha|_v\} [K_v : \mathbb{Q}_v]. \end{aligned}$$

By (2.2), $\sum_{v \mid 2} [K_v : \mathbb{Q}_v] = [K : \mathbb{Q}]$ and $\sum_{v \mid \infty} [K_v : \mathbb{Q}_v] = [K : \mathbb{Q}]$. By (2.3),

$$\sum_{v \in M_K} [K_v : \mathbb{Q}_v] \max\{0, \log |\alpha|_v\} = [K : \mathbb{Q}] h(\alpha).$$

Therefore,

$$0 \leq -[K : \mathbb{Q}] \log 4 + [K : \mathbb{Q}] \log 2 + 2^{s+1} F [K : \mathbb{Q}] h(\alpha),$$

which implies

$$h(\alpha) \geq \frac{\log 2}{2^{s+1}F}.$$

Using the minimality of s , we have $2^{s+1} < 4e_1 \leq 4[\mathbb{Q}(\alpha) : \mathbb{Q}]$. So

$$\frac{\log M(\alpha)}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \geq \frac{\log 2}{4[\mathbb{Q}(\alpha) : \mathbb{Q}]F}$$

from which $M(\alpha) \geq 2^{1/4F}$.

Case 1. Let $f \neq 6$ and $f \neq f_i$ for $i \in \{1, \dots, r\}$. In this case, by Lemma 2.1, there is a Zsigmondy prime for $(2, f)$ and it is greater than or equal to $f + 1$. So,

$$F = \text{lcm}(2^{f_1} - 1, 2^{f_2} - 1, \dots, 2^{f_r} - 1) \leq \frac{2^f - 1}{f + 1}.$$

Therefore, $M(\alpha) \geq 2^{(f+1)/4(2^f-1)}$.

Case 2. Let $f = 6$ or $f = f_i$ for some $i \in \{1, \dots, r\}$. In this case, a Zsigmondy prime for $(2, f)$ does not exist. So, $F = \text{lcm}(2^{f_1} - 1, 2^{f_2} - 1, \dots, 2^{f_r} - 1) \leq 2^f - 1$. Therefore, $M(\alpha) \geq 2^{1/4(2^f-1)}$. This completes the proof of Theorem 1.1. \square

PROOF OF THEOREM 1.3. Put $K = \mathbb{Q}(\alpha)$. We are given $p\mathcal{O}_K = \mathcal{P}_1^{e_1}\mathcal{P}_2^{e_2} \dots \mathcal{P}_r^{e_r}$, with $[\mathcal{O}_K/\mathcal{P}_i : \mathbb{Z}/p\mathbb{Z}] = f_i$. Let $E = \text{lcm}(p^{f_1} - 1, p^{f_2} - 1, \dots, p^{f_r} - 1)$. Following exactly the arguments in the first paragraph of the proof of Theorem 1.1, we deduce

$$\alpha^E - 1 \in \mathcal{P}_i \quad \text{for all } i \in \{1, \dots, r\}.$$

Let $A = \{i \in \{1, \dots, r\} : e_i > p\}$. For each $i \in A$, choose s_i minimal such that $p^{s_i} \geq e_i$. For any fixed $i \in A$, we have $p^n < e_i$ for $n = 1, \dots, s_i - 1$, so that

$$p\mathcal{O}_K \subseteq \mathcal{P}_i^{p^n} \quad \text{for all } n = 1, \dots, s_i - 1. \tag{3.3}$$

Taking the p th power (up to s_i many times) of the element $\alpha^E - 1$ and using (3.3), we deduce

$$\alpha^{p^{s_i}E} - 1 \in \mathcal{P}_i^{p^{s_i}} \subseteq \mathcal{P}_i^{e_i} \quad \text{for all } i \in A.$$

Define $s = \max\{s_i\}_{i \in A}$. Then $(\alpha^{p^{s_i}E} - 1)^{p^{s-s_i}} \in \mathcal{P}_i^{e_i}$. Using (3.1), we deduce

$$\alpha^{p^sE} - 1 \in \mathcal{P}_i^{e_i} \quad \text{for all } i \in A. \tag{3.4}$$

Suppose there exists $i \in \{1, \dots, r\}$ such that $e_i \leq p$. Since $\alpha^E - 1 \in \mathcal{P}_i$, it follows that $\alpha^{p^sE} - 1 \in \mathcal{P}_i^p \subseteq \mathcal{P}_i^{e_i}$ and from (3.1), we deduce that $\alpha^{p^sE} - 1 \in \mathcal{P}_i^{e_i}$. Therefore, from (3.4),

$$\alpha^{p^sE} - 1 \in \mathcal{P}_i^{e_i} \quad \text{for all } i \in \{1, \dots, r\}.$$

So, for all $i \in \{1, \dots, r\}$,

$$|\alpha^{p^sE} - 1|_{\mathcal{P}_i} \leq p^{-e_i/e_i} \leq \frac{1}{p} \max\{1, |\alpha|_{\mathcal{P}_i}\}^{p^sE}.$$

If $v \mid \infty$, then $|\alpha^{p^s E} - 1|_v \leq |\alpha|_v^{p^s E} + 1 \leq 2 \max\{1, |\alpha|_v^{p^s E}\}$. Thus,

$$|\alpha^{p^s E} - 1|_v \leq \begin{cases} p^{-1} \max\{1, |\alpha|_v\}^{p^s E} & \text{if } v \mid p, \\ \max\{1, |\alpha|_v\}^{p^s E} & \text{if } v \nmid p, v \nmid \infty, \\ 2 \max\{1, |\alpha|_v\}^{p^s E} & \text{if } v \mid \infty. \end{cases} \tag{3.5}$$

Since α is not a root of unity, $\alpha^{p^s E} - 1 \neq 0$. Applying the product formula (2.1) to the element $\alpha^{p^s E} - 1$ and using (3.5),

$$\begin{aligned} 0 &= \sum_{v \in M_K} [K_v : \mathbb{Q}_v] \log |\alpha^{p^s E} - 1|_v \\ &\leq \sum_{v \mid p} [K_v : \mathbb{Q}_v] \{-\log p + p^s E \max\{0, \log |\alpha|_v\}\} \\ &\quad + \sum_{v \nmid p, v \nmid \infty} [K_v : \mathbb{Q}_v] \{p^s E \max\{0, \log |\alpha|_v\}\} \\ &\quad + \sum_{v \mid \infty} [K_v : \mathbb{Q}_v] \{\log 2 + p^s E \max\{0, \log |\alpha|_v\}\} \\ &= \sum_{v \mid p} -[K_v : \mathbb{Q}_v] \log p + \sum_{v \mid \infty} [K_v : \mathbb{Q}_v] \log 2 + \sum_{v \in M_K} p^s E \max\{0, \log |\alpha|_v\} [K_v : \mathbb{Q}_v]. \end{aligned}$$

By (2.2), $\sum_{v \mid p} [K_v : \mathbb{Q}_v] = [K : \mathbb{Q}]$ and $\sum_{v \mid \infty} [K_v : \mathbb{Q}_v] = [K : \mathbb{Q}]$, and by (2.3),

$$\sum_{v \in M_K} [K_v : \mathbb{Q}_v] \max\{0, \log |\alpha|_v\} = [K : \mathbb{Q}] h(\alpha).$$

Therefore,

$$0 \leq -[K : \mathbb{Q}] \log p + [K : \mathbb{Q}] \log 2 + p^s E [K : \mathbb{Q}] h(\alpha),$$

which implies $h(\alpha) \geq \log(p/2)/p^s E$. However, $p^s \leq p[\mathbb{Q}(\alpha) : \mathbb{Q}]$ from the minimality of s , so

$$\frac{\log M(\alpha)}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \geq \frac{\log(p/2)}{p[\mathbb{Q}(\alpha) : \mathbb{Q}]E}.$$

Thus, $M(\alpha) \geq (p/2)^{1/p^s E}$.

Case 1. Let $(f, p) = (2, 2^s - 1)$ for some $s \in \mathbb{N}$ or $f = f_i$ for some $i \in \{1, \dots, r\}$. In this case, by Lemma 2.1, a Zsigmondy prime for (p, f) does not exist and

$$E = \text{lcm}(p^{f_1} - 1, p^{f_2} - 1, \dots, p^{f_r} - 1) \leq p^f - 1.$$

Therefore, $M(\alpha) \geq (p/2)^{1/p(p^f-1)}$.

Case 2. Let $(f, p) \neq (2, 2^s - 1)$ and $f \neq f_i$ for all $i \in \{1, \dots, r\}$. In this case, a Zsigmondy prime for (p, f) exists and is greater than or equal to $f + 1$. So, $E = \text{lcm}(p^{f_1} - 1, p^{f_2} - 1, \dots, p^{f_r} - 1) \leq (p^f - 1)/(f + 1)$. Therefore, $M(\alpha) \geq (p/2)^{(f+1)/p(p^f-1)}$. This completes the proof of Theorem 1.3. \square

4. Proof of Theorems 1.5 and 1.6

For the proof of our theorems, we need the following result from [7].

LEMMA 4.1 [7, Lemma 1]. *Let K be a number field and S be a finite set of places of K over a rational prime p . Let $\gamma_1, \gamma_2 \in \mathcal{O}_K$ and $\rho > 0$ be such that for all $v \in S$,*

$$|\gamma_1 - \gamma_2|_v \leq p^{-\rho}.$$

Define an integer $k = k_{p,\rho}$ by $k = 0$ if $(p - 1)\rho > 1$ and by $p^{k-1}(p - 1)\rho \leq 1 < p^k(p - 1)\rho$ otherwise. Also, for any nonnegative integer λ , define $s_{p,\rho}(\lambda) = p^k\rho + \max\{0, \lambda - k\}$. Then, for any nonnegative integer λ and for all $v \in S$,

$$|\gamma_1^{p^\lambda} - \gamma_2^{p^\lambda}|_v \leq p^{-s_{p,\rho}(\lambda)}.$$

PROOF OF THEOREM 1.5. Put $L = K(\alpha)$. We are given $\mathcal{PO}_L = \mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \dots \mathcal{P}_r^{e_r}$ with $f_i = [O_L/\mathcal{P}_i : O_K/\mathcal{P}]$. Let f^* be the inertia degree of \mathcal{P} over 2. Then, $|O_L/\mathcal{P}_i| = 2^{f^* f_i}$ for $i \in \{1, \dots, r\}$ and so $\alpha^{2^{f^* f_i}} - \alpha \in \mathcal{P}_i$ for $i \in \{1, \dots, r\}$. Since α is a unit, this gives $\alpha^{2^{f^* f_i - 1}} - 1 \in \mathcal{P}_i$ for $i \in \{1, \dots, r\}$. Since $f_i \mid f$, applying (3.1), we have $\alpha^{2^{f^* f - 1}} - 1 \in \mathcal{P}_i$ for all $i \in \{1, \dots, r\}$.

For each $i \in \{1, \dots, r\}$, choose s_i minimal such that $2^{s_i} \geq e_i$. For any fixed i , by the minimality of s_i , we have $2^n < e_i$ for $n = 0, 1, \dots, s_i - 1$. Since

$$\mathcal{PO}_L = \mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \dots \mathcal{P}_r^{e_r} \subseteq \mathcal{P}_i^{e_i} \subseteq \mathcal{P}_i^{2^n} \quad \text{for } n = 0, 1, \dots, s_i - 1,$$

we have $2 \in \mathcal{P}_i^{2^n}$ for $n = 0, 1, \dots, s_i - 1$. Since $2 \in \mathcal{P}_i$ and $\alpha^{2^{f^* f - 1}} - 1 \in \mathcal{P}_i$, this gives $\alpha^{2^{f^* f - 1}} - 1 + 2 = \alpha^{2^{f^* f - 1}} + 1 \in \mathcal{P}_i$, whence $\alpha^{2^{f^* f + 1 - 2}} - 1 \in \mathcal{P}_i^{2^1}$. Using $2 \in \mathcal{P}_i^{2^n}$ for $n = 0, 1, \dots, s_i - 1$ and, applying the same method inductively,

$$\alpha^{2^{f^* f + s_i - 2^{s_i}}} - 1 \in \mathcal{P}_i^{2^{s_i}} \subseteq \mathcal{P}_i^{e_i}.$$

Define $s = \max\{s_1, s_2, \dots, s_r\}$. Without loss of generality, assume $s = s_1$ so that $\alpha^{2^{f^* f + s - 2^s}} - 1 \in \mathcal{P}_1^{e_1}$. Take any $i \neq 1$. Then, $\alpha^{2^{f^* f + s_i - 2^{s_i}}} - 1 \in \mathcal{P}_i^{e_i}$. Since $2 \in \mathcal{P}_i$ and $\alpha^{2^{f^* f + s_i - 2^{s_i}}} - 1 \in \mathcal{P}_i$, we have $\alpha^{2^{f^* f + s_i - 2^{s_i}}} + 1 \in \mathcal{P}_i$, whence $\alpha^{2^{f^* f + s_i + 1 - 2^{s_i + 1}}} - 1 \in \mathcal{P}_i^{e_i + 1}$. Applying the same method inductively yields $\alpha^{2^{f^* f + s_i + s - s_i - 2^{s_i + s - s_i}}} - 1 \in \mathcal{P}_i^{e_i + s - s_i}$. Thus, $\alpha^{2^{f^* f + s - 2^s}} - 1 \in \mathcal{P}_i^{e_i + s - s_i} \subseteq \mathcal{P}_i^{e_i}$ and

$$|\alpha^{2^{f^* f + s - 2^s}} - 1|_{\mathcal{P}_i} \leq 2^{-e_i/e_i e} = 2^{-1/e} \leq 2^{-1/d} \quad \text{for } i \in \{1, \dots, r\},$$

where e is the ramification degree of \mathcal{P} over 2. Let $S_{p,\rho}(\lambda)$ be as in the statement of Lemma 4.1. As $\lim_{\lambda \rightarrow \infty} S_{p,\rho}(\lambda) = \infty$, applying Lemma 4.1, we deduce that there exists a λ which depends only on d such that

$$|\alpha^{(2^{f^* f + s - 2^s})^{2^\lambda}} - 1|_{\mathcal{P}_i} \leq 2^{-2d} \quad \text{for } i = 1, \dots, r.$$

If $v \mid \infty$, then $|\alpha^{(2^{f^* f+s}-2^s)2^\lambda} - 1|_v \leq |\alpha|_v^{(2^{f^* f+s}-2^s)2^\lambda} + 1 \leq 2 \max\{1, |\alpha|_v\}^{(2^{f^* f+s}-2^s)2^\lambda}$. Thus,

$$|\alpha^{(2^{f^* f+s}-2^s)2^\lambda} - 1|_v \leq \begin{cases} 2^{-2d} \max\{1, |\alpha|_v\}^{(2^{f^* f+s}-2^s)2^\lambda} & \text{if } v \mid \mathcal{P}, \\ \max\{1, |\alpha|_v\}^{(2^{f^* f+s}-2^s)2^\lambda} & \text{if } v \nmid \mathcal{P}, v \nmid \infty, \\ 2 \max\{1, |\alpha|_v\}^{(2^{f^* f+s}-2^s)2^\lambda} & \text{if } v \mid \infty. \end{cases} \tag{4.1}$$

Since α is not a root of unity, $\alpha^{(2^{f^* f+s}-2^s)2^\lambda} - 1 \neq 0$. Applying the product formula (2.1) to the element $\alpha^{(2^{f^* f+s}-2^s)2^\lambda} - 1$ and using (4.1),

$$\begin{aligned} 0 &= \sum_{v \in M_L} [L_v : \mathbb{Q}_v] \log |\alpha^{(2^{f^* f+s}-2^s)2^\lambda} - 1|_v \\ &\leq \sum_{v \mid \mathcal{P}} [L_v : \mathbb{Q}_v] \{-2d \log 2 + (2^{f^* f+s} - 2^s)2^\lambda \max\{0, \log |\alpha|_v\}\} \\ &\quad + \sum_{v \nmid \mathcal{P}, v \nmid \infty} [L_v : \mathbb{Q}_v] \{(2^{f^* f+s} - 2^s)2^\lambda \max\{0, \log |\alpha|_v\}\} \\ &\quad + \sum_{v \mid \infty} [L_v : \mathbb{Q}_v] \{\log 2 + (2^{f^* f+s} - 2^s)2^\lambda \max\{0, \log |\alpha|_v\}\} \\ &\leq -2d \log 2 \sum_{v \mid \mathcal{P}} [L_v : \mathbb{Q}_v] + \log 2 \sum_{v \mid \infty} [L_v : \mathbb{Q}_v] \\ &\quad + (2^{f^* f+s} - 2^s)2^\lambda \sum_{v \in M_L} [L_v : \mathbb{Q}_v] \max\{0, \log |\alpha|_v\}. \end{aligned}$$

Since $\sum_{v \in M_L} [L_v : \mathbb{Q}_v] \max\{0, \log |\alpha|_v\} = [L : \mathbb{Q}]h(\alpha)$ and $\sum_{v \mid \infty} [L_v : \mathbb{Q}_v] = [L : \mathbb{Q}]$,

$$0 \leq -2d \log 2 \sum_{v \mid \mathcal{P}} [L_v : K_{\mathcal{P}}][K_{\mathcal{P}} : \mathbb{Q}_2] + [L : \mathbb{Q}] \log 2 + (2^{f^* f+s} - 2^s)2^\lambda [L : \mathbb{Q}]h(\alpha).$$

Using $\sum_{v \mid \mathcal{P}} [L_v : K_{\mathcal{P}}] = [L : K]$,

$$0 \leq -2d \log 2 \frac{[K_{\mathcal{P}} : \mathbb{Q}_2][L : \mathbb{Q}]}{[K : \mathbb{Q}]} + [L : \mathbb{Q}] \log 2 + (2^{f^* f+s} - 2^s)2^\lambda [L : \mathbb{Q}]h(\alpha).$$

Thus,

$$h(\alpha) \geq \frac{[K_{\mathcal{P}} : \mathbb{Q}_2] \log 4 - \log 2}{(2^{f^* f+s} - 2^s)2^\lambda} \geq \frac{\log 2}{2^s(2^{f^* f} - 1)2^\lambda}.$$

Using the minimality of s , we have $2^s < 2e_1 \leq 2[K(\alpha) : K] \leq 2[Q(\alpha) : \mathbb{Q}]$. Also, since $f^* \leq d$,

$$\frac{\log M(\alpha)}{[Q(\alpha) : \mathbb{Q}]} \geq \frac{\log 2}{2[Q(\alpha) : \mathbb{Q}](2^{df} - 1)2^\lambda}.$$

Thus, $M(\alpha) \geq 2^{1/2^{\lambda+1}(2^{df}-1)}$. Since λ is only a function of d , this completes the proof of Theorem 1.5. □

PROOF OF THEOREM 1.6. Put $L = K(\alpha)$. We are given $\mathcal{P}O_L = \mathcal{P}_1^{e_1} \mathcal{P}_2^{e_2} \dots \mathcal{P}_r^{e_r}$, with $[O_L/\mathcal{P}_i : O_K/\mathcal{P}] = f_i$. Let f^* be the inertia degree of \mathcal{P} over p . So $|O_L/\mathcal{P}_i| = p^{f^* f_i}$ for $i \in \{1, \dots, r\}$. Thus, $\alpha^{p^{f^* f_i}} - \alpha \in \mathcal{P}_i$ for $i \in \{1, \dots, r\}$. Since α is a unit, we have $\alpha^{p^{f^* f_i - 1}} - 1 \in \mathcal{P}_i$ for $i \in \{1, \dots, r\}$. Since $f_i \mid f$, applying (3.1), we deduce that $\alpha^{p^{f^* f - 1}} - 1 \in \mathcal{P}_i$ for $i \in \{1, \dots, r\}$.

Let $A = \{i \in \{1, \dots, r\} : e_i > p\}$. For each $i \in A$, choose s_i minimal such that $p^{s_i} \geq e_i$. So for any fixed $i \in A$, we have $p^n < e_i$ for $n = 1, \dots, s_i - 1$, and thus,

$$\mathcal{P}O_L \subseteq \mathcal{P}_i^{p^n} \quad \text{for } n = 1, \dots, s_i - 1. \tag{4.2}$$

Taking the p th power (up to s_i many times) of the element $\alpha^{p^{f^* f - 1}} - 1$ and using (4.2), we deduce that $\alpha^{p^{s_i(p^{f^* f - 1})}} - 1 \in \mathcal{P}_i^{p^{s_i}} \subseteq \mathcal{P}_i^{e_i}$ for $i \in A$. Define $s = \max\{s_i\}_{i \in A}$. Then, $(\alpha^{p^{f^* f - 1}} - 1)^{p^s} \in \mathcal{P}_i^{e_i}$. From (3.1),

$$\alpha^{p^s(p^{f^* f - 1})} - 1 \in \mathcal{P}_i^{e_i} \quad \text{for } i \in A.$$

Suppose there exists $i \in \{1, \dots, r\}$ such that $e_i \leq p$. Since $\alpha^{p^{f^* f - 1}} - 1 \in \mathcal{P}_i$, we have $\alpha^{p^{f^* f - 1}} - 1 \in \mathcal{P}_i^p \subseteq \mathcal{P}_i^{e_i}$, and using (3.1), we find $\alpha^{p^s(p^{f^* f - 1})} - 1 \in \mathcal{P}_i^{e_i}$. Therefore,

$$\alpha^{p^s(p^{f^* f - 1})} - 1 \in \mathcal{P}_i^{e_i} \quad \text{for } i \in \{1, \dots, r\}.$$

So, for $i \in \{1, \dots, r\}$,

$$|\alpha^{p^s(p^{f^* f - 1})} - 1|_{\mathcal{P}_i} \leq p^{-e_i/e_i e} = p^{-1/e} \leq p^{-1/d},$$

where e is the ramification index of \mathcal{P} over p . From Lemma 4.1, there exists a λ which depends only on p and d such that

$$|\alpha^{p^s(p^{f^* f - 1})} - 1|_{\mathcal{P}_i} \leq p^{-d} \quad \text{for } i \in \{1, \dots, r\}.$$

If $v \mid \infty$, then $|\alpha^{p^s(p^{f^* f - 1})} - 1|_v \leq |\alpha|_v^{p^s(p^{f^* f - 1})} + 1 \leq 2 \max\{1, |\alpha|_v^{p^s(p^{f^* f - 1})}\}$. Thus,

$$|\alpha^{p^s(p^{f^* f - 1})} - 1|_v \leq \begin{cases} p^{-d} \max\{1, |\alpha|_v\}^{p^s(p^{f^* f - 1})} & \text{if } v \mid p, \\ \max\{1, |\alpha|_v\}^{p^s(p^{f^* f - 1})} & \text{if } v \nmid p, v \nmid \infty, \\ 2 \max\{1, |\alpha|_v\}^{p^s(p^{f^* f - 1})} & \text{if } v \mid \infty. \end{cases} \tag{4.3}$$

Since α is not a root of unity, $\alpha^{p^s(p^{f^* f - 1})} - 1 \neq 0$. Applying the product formula (2.1) to the element $\alpha^{p^s(p^{f^* f - 1})} - 1$ and using (4.3),

$$\begin{aligned} 0 &= \sum_{v \in M_L} [L_v : \mathbb{Q}_v] \log |\alpha^{p^s(p^{f^* f - 1})} - 1|_v \\ &\leq \sum_{v \mid p} [L_v : \mathbb{Q}_v] \{-d \log p + p^s(p^{f^* f - 1}) p^\lambda \max\{0, \log |\alpha|_v\}\} \\ &\quad + \sum_{v \nmid p, v \nmid \infty} [L_v : \mathbb{Q}_v] \{p^s(p^{f^* f - 1}) p^\lambda \max\{0, \log |\alpha|_v\}\} \end{aligned}$$

$$\begin{aligned}
 & + \sum_{v|\infty} [L_v : \mathbb{Q}_v] \{\log 2 + p^s(p^{f^*f} - 1)p^\lambda \max\{0, \log |\alpha|_v\}\} \\
 = & \sum_{v|p} -d[L_v : \mathbb{Q}_v] \log p + \sum_{v|\infty} [L_v : \mathbb{Q}_v] \log 2 \\
 & + \sum_{v \in M_L} p^s(p^{f^*f} - 1)p^\lambda \max\{0, \log |\alpha|_v\} [L_v : \mathbb{Q}_v].
 \end{aligned}$$

Since $\sum_{v \in M_L} [L_v : \mathbb{Q}_v] \max\{0, \log |\alpha|_v\} = [L : \mathbb{Q}]h(\alpha)$ and $\sum_{v|\infty} [L_v : \mathbb{Q}_v] = [L : \mathbb{Q}]$,

$$0 \leq -d \log p \sum_{v|p} [L_v : K_p] [K_p : \mathbb{Q}_p] + [L : \mathbb{Q}] \log 2 + p^s(p^{f^*f} - 1)p^\lambda [L : \mathbb{Q}]h(\alpha).$$

Using $\sum_{v|p} [L_v : K_p] = [L : K]$ gives

$$0 \leq -d \log p \frac{[K_p : \mathbb{Q}_p][L : \mathbb{Q}]}{[K : \mathbb{Q}]} + [L : \mathbb{Q}] \log 2 + p^s(p^{f^*f} - 1)p^\lambda [L : \mathbb{Q}]h(\alpha).$$

Thus,

$$h(\alpha) \geq \frac{[K_p : \mathbb{Q}_p] \log p - \log 2}{(p^{f^*f+s} - p^s)p^\lambda} \geq \frac{\log(p/2)}{p^s(p^{f^*f} - 1)p^\lambda}.$$

From the minimality of s , we have $p^s \leq p[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Moreover, $f^* \leq d$, so that

$$\frac{\log M(\alpha)}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} \geq \frac{\log(p/2)}{p[\mathbb{Q}(\alpha) : \mathbb{Q}](p^{df} - 1)p^\lambda}.$$

Thus, $M(\alpha) \geq (p/2)^{1/p^{d+1}(p^{df}-1)}$. Since λ is only a function of d , this completes the proof of Theorem 1.6. □

Acknowledgements

We are thankful to the referee for suggesting many useful changes to make the article more readable. The second author is thankful to the Indian Statistical Institute, Delhi, where this work was started when he was visiting the institute.

References

- [1] E. Dobrowolski, ‘On a question of Lehmer and the number of irreducible factors of a polynomial’, *Acta Arith.* **34**(4) (1979), 391–401.
- [2] W. Feit and G. M. Seitz, ‘On finite rational groups and related topics’, *Illinois J. Math.* **33**(1) (1989), 103–131.
- [3] J. Garza, ‘The Lehmer strength bounds for total ramification’, *Acta Arith.* **137**(2) (2009), 171–176.
- [4] L. Kronecker, ‘Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten’, *J. reine angew. Math.* **53** (1857), 173–175.
- [5] D. H. Lehmer, ‘Factorization of certain cyclotomic functions’, *Ann. of Math. (2)* **34**(3) (1933), 461–479.
- [6] M. Mignotte, ‘Entiers algébriques dont les conjugués sont proches du cercle unité’, *Sém. Delange-Pisot-Poitou, Théor. Nombres* **19**(2) (1977–78), Article no. 39, 6 pages.

- [7] G. Prasad, 'Height of algebraic units under splitting conditions', *Proc. Indian Acad. Sci. Math. Sci.* **133**(2) (2023), Article no. 16, 9 pages.
- [8] G. Prasad and K. S. Kumar, 'Lehmer's problem and splitting of rational primes in number fields', *Acta Math. Hungar.* **169**(2) (2023), 349–358.
- [9] C. J. Smyth, 'On the product of the conjugates outside the unit circle of an algebraic integer', *Bull. Lond. Math. Soc.* **3** (1971), 169–175.
- [10] P. Voutier, 'An effective lower bound for the height of algebraic numbers', *Acta Arith.* **74**(1) (1996), 81–95.
- [11] M. Waldschmidt, *Diophantine Approximation on Linear Algebraic Groups* (Springer, Berlin, 2000).

SHANTA LAISHRAM,
Indian Statistical Institute, New Delhi 110016, India
e-mail: shanta@isid.ac.in

GOREKH PRASAD, Harish-Chandra Research Institute,
A CI of Homi Bhabha National Institute, Prayagraj 211019, India
e-mail: gorekhprasad@hri.res.in