# LEHMER'S CONJECTURE AND $p$-ADIC EQUIDISTRIBUTION FOR ALGEBRAIC NUMBERS WITH SMALL HEIGHT

ANUP B. DIXIT AND SUSHANT KALA

Abstract. For a non-zero algebraic number $\alpha$ of degree $d$, let $h(\alpha)$ denote its logarithmic Weil height. It is known that when $h(\alpha)$ is small, as $d$ increases the conjugates of $\alpha$ have angular equidistribution in the complex plane about the origin. In this paper, we establish a $p$-adic equidistribution theorem for $\alpha \in \overline{\mathbb{Q}}$ with small height. As a consequence, we prove Lehmer's conjecture for all $\alpha$ such that $\gg \sqrt{d \log d}$ many of its conjugates lie in a finite extension of $\mathbb{Q}_p$, for some prime $p$.

## 1. Introduction

For non-zero $\alpha \in \overline{\mathbb{Q}}$, let $h(\alpha)$ denote its logarithmic Weil height defined as

$$h(\alpha) := \sum_{v \in M_K} \log^+ |\alpha|_v,$$

where $M_K$ is the set of all places of $K \supseteq \mathbb{Q}(\alpha)$, $\log^+ x = \max(0, \log x)$ and $|\alpha|_v$ is the normalized valuation on $\alpha$ given by

$$|\alpha|_v := \begin{cases} (N\mathfrak{p})^{-\frac{ord_{\mathfrak{p}}(\alpha)}{[K:\mathbb{Q}]}} & \text{if } v \text{ is non-archimedean corresponding to the prime ideal } \mathfrak{p}, \\ |\sigma(\alpha)|^{\frac{[K_\nu:\mathbb{R}]}{[K:\mathbb{Q}]}} & \text{if } v \text{ is archimedean corresponding to the embedding } \sigma \text{ of } K. \end{cases}$$

By a classical theorem of Kronecker [18], $h(\alpha) = 0$ if and only if $\alpha$ is a root of unity. This height function quantifies the "complexity" of an algebraic number. Note that $h(2^{1/d}) = \frac{\log 2}{d}$ and therefore, there are algebraic numbers, other than roots of unity, with arbitrarily small height.

Suppose $\alpha \neq 0, \pm 1$ is totally real, i.e., all its Galois conjugates lie in $\mathbb{R}$, then Schinzel [30] in 1973 showed that

$$h(\alpha) \geq \frac{1}{2} \log \left( \frac{1 + \sqrt{5}}{2} \right).$$

Following the proof of Schinzel or a simpler proof due to Höhn-Skoruppa [17], one can obtain an explicit lower bound on $h(\alpha)$ even if a positive proportion of Galois conjugates of $\alpha$ lie in $\mathbb{R}$. More generally, the famous equidistribution theorem of Bilu [5] asserts that as $h(\alpha_n) \to 0$ over a family of $\alpha_n \in \overline{\mathbb{Q}}$, the Galois conjugates of $\alpha_n$ have angular equidistribution in $\mathbb{C}^*$. A quantitative version of this result due to Mignotte [22] can be stated as follows.

**Theorem** ([21], Theorem 15.2)**.** *For $\alpha \in \overline{\mathbb{Q}}$, let $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$. For any $\theta$ with $0 \leq \theta \leq 2\pi$ the number $n$ of conjugates of $\alpha$ in any fixed sector, based at the origin, of angle $\theta$ satisfies*

$$\left| n - \frac{\theta}{2\pi} d \right| \leq 24 \left( d^{2/3} (\log 2d)^{1/3} + d h(\alpha)^{1/3} \right). \tag{1}$$

2020 *Mathematics Subject Classification.* 11G50, 11R04, 11R06.

*Key words and phrases.* Lehmer's conjecture, $p$-adic equidistribution, Weil height.

Research of the first author was partially supported by the INSPIRE Faculty Fellowship.

By definition, as $h(\alpha)$ gets closer to 0, most of its conjugates are clustered around the unit circle. Furthermore, if $h(\alpha)$ is small and $d$ grows, then the number of conjugates of $\alpha$ in any sector is proportional to the angle $\theta$ of the sector. This can be thought of as refinement of a theorem of Erdős-Turán [15] on the distribution of zeros of polynomials, an improvement of which was obtained by Soundarajan [33]. This equidistribution theory has undergone extensive generalization (see [2], [3], [4], [9], [10], [16], [25], [28], [34]).

The non-archimedean analogue of totally real numbers are totally $p$-adic numbers. We say $\alpha \in \overline{\mathbb{Q}}$ is totally $p$-adic if all its Galois conjugates lie in $\mathbb{Q}_p$. If $\alpha$ is totally $p$-adic and not a $(p-1)$-th root of unity, then L. Pottmeyer [26] proved that

$$h(\alpha) \geq \frac{\log(p/2)}{p+1}.$$

More generally, suppose all Galois conjugates of $\alpha$ lie in a finite extension $K_\nu/\mathbb{Q}_p$, with ramification index $e_\nu$ and inertia degree $f_\nu$. Then, a result of Bombieri-Zannier [6, Theorem 2] implies that for any $\epsilon > 0$,

$$h(\alpha) \geq \frac{\log p}{2e_\nu(p^{f_\nu}+1)} - \epsilon$$

holds except for finitely many such $\alpha$'s.

It is difficult to realize a $p$-adic analogue of the angular equidistribution property, since there is no notion of sectors. As a first step, in [13], the authors established an absolute lower bound on $h(\alpha)$, when a positive proportion of the Galois conjugates of $\alpha$ lie in a finite extension of $\mathbb{Q}_p$. More precisely, let $K_\nu/\mathbb{Q}_p$ be a finite extension with residue field $\mathbb{F}_q$ and suppose $\psi_q$ is the proportion of Galois conjugates of $\alpha$ in $K_\nu$. Then, for any $\epsilon > 0$, except for finitely many such $\alpha \in \overline{\mathbb{Q}}$,

$$h(\alpha) \geq \psi_q \frac{\log q}{q+1} - \epsilon.$$

The objective of this paper is to refine this $p$-adic equidistribution property by relaxing the positive proportion condition and still obtaining a meaningful lower bound on $h(\alpha)$. By analogy, we say that the conjugates of $\alpha \in \overline{\mathbb{Q}}$ satisfy $p$-adic equidistribution property if a "small" number of them lie in any fixed local field $K_\nu/\mathbb{Q}_p$. The reader must note that angular equidistribution in the complex plane does not imply $p$-adic equidistribution. For instance, all conjugates of $2^{1/(p-1)}$ are given by $\{2^{1/(p-1)}\zeta_{p-1}^m\}$, where $\zeta_{p-1} = e^{\frac{2\pi i}{p-1}}$ is the primitive $(p-1)$-th root of unity and $0 \leq m \leq p-2$. Thus, this set of conjugates have angular equidistribution in the complex plane. However, since $\zeta_{p-1} \in \mathbb{Q}_p$, the extension $K_\nu := \mathbb{Q}_p(2^{1/(p-1)})$ contains all conjugates of $2^{1/(p-1)}$. In other words, the smallest extension of $\mathbb{Q}_p$ containing $2^{1/(p-1)}$ in fact contains all its conjugates.

Let $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ be the minimal polynomial of $\alpha$. Then, its Mahler measure is defined as

$$M(\alpha) := |a_n| \prod_i \max(1, |\alpha_i|),$$

where $\alpha_i$'s denote the Galois conjugates of $\alpha$. Mahler measure is connected to the height of $\alpha$ by the relation

$$\log M(\alpha) = h(\alpha)\,[\mathbb{Q}(\alpha):\mathbb{Q}].$$

A long standing problem in the theory of heights is Lehmer's conjecture. In 1933, Lehmer [19] initiated the study of obtaining small values of $h(\alpha)$, when $\alpha$ is not a root of unity. He constructed a polynomial, also known as the Lehmer polynomial, namely

$$L(x) = x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1.$$

For a root $\alpha$ of $L(x)$, the Mahler measure $M(\alpha) = 1.76280\ldots$ and the height $h(\alpha) = 0.0162\ldots$. To this day, $L(x)$ is the polynomial with smallest Mahler measure. This prompted Lehmer to make the following conjecture. Denote by $\mu_\infty$ the set of all roots of unity in $\overline{\mathbb{Q}}$.

**Conjecture 1.1** (Lehmer)**.** *Let $\alpha \in \overline{\mathbb{Q}} \setminus \mu_\infty$ be a non-zero algebraic number. Then, there exists an absolute constant $c > 0$ such that*

$$h(\alpha) > \frac{c}{[\mathbb{Q}(\alpha) : \mathbb{Q}]}.$$

In other words, $M(\alpha) > 1 + \delta$ for an absolute constant $\delta > 0$ for $\alpha \notin \mu_\infty$. It is also expected that the constant $c = 0.00162$ as in the case of the Lehmer polynomial. If $\alpha \in \overline{\mathbb{Q}}$ is an algebraic non-integer, then by definition $M(\alpha) \geq 2$. Hence, in the context of Lehmer's conjecture, we can restrict ourselves to only algebraic integers. Although this conjecture remains open, significant progress has been made in recent times. Using a sharpened version of Siegel's lemma and thereby constructing an auxiliary polynomial with small coefficients, Dobrowolski [14] proved that for non-zero $\alpha$ not a root of unity,

$$\log M(\alpha) \geq c \left( \frac{\log \log d}{\log d} \right)^3,$$

where $d = [\mathbb{Q}(\alpha) : \mathbb{Q}]$ and $c > 0$ is an absolute constant. Subsequently, this constant $c$ has been improved in the works of U. Rausch [27] and P. Voutier [36]. In 1971, C. Smyth [31] showed that Lehmer's conjecture holds for all non-reciprocal algebraic numbers. We call $\alpha \in \overline{\mathbb{Q}}$ reciprocal if $\alpha$ and $1/\alpha$ are conjugates. This result, with a weaker constant, was also obtained by R. Breusch [8] in 1951. On another front, suppose $\alpha \in \overline{\mathbb{Q}}$ is such that the Galois closure of $\mathbb{Q}(\alpha)/\mathbb{Q}$, say $K_\alpha$ has relatively smaller degree, i.e., $[K_\alpha : \mathbb{Q}]$ is polynomial in $[\mathbb{Q}(\alpha) : \mathbb{Q}]$, then F. Amoroso and S. David [1] proved that Lehmer's conjecture holds for all such $\alpha$. For all $\alpha$ satisfying a non-cyclic irreducible polymonial with odd coefficients, Borwein, Dobrowolski and Mossinghoff [7] proved that Lehmer's conjecture holds. A weaker version of Lehmer's conjecture was proposed by A. Schinzel and H. Zassenhaus [29], which was recently resolved by V. Dimitrov [11]. The reader may refer to the excellent survey articles [32] and [35] for a comprehensive account of Lehmer's problem.

From (1), we can conclude that an algebraic number which fails to admit angular equidistribution must satisfy Lehmer's conjecture. In particular, for all $\alpha \in \overline{\mathbb{Q}}$ satisfying

$$\left| n - \frac{\theta}{2\pi} d \right| \gg \left( d^2 \log d \right)^{1/3},$$

with the implied constant > 24, Lehmer's conjecture holds. The aim of this paper is to realize a $p$-adic analogue of the above phenomenon. We show that when $h(\alpha)$ is small, as the degree $d$ of $\alpha$ increases, there are very few conjugates of $\alpha$ in any given finite extension of $\mathbb{Q}_p$.

Let $K_\nu/\mathbb{Q}_p$ be a finite extension of degree $d_\nu$ and residue field $\mathbb{F}_q$. Let $g : \mathbb{N} \to \mathbb{R}$ be a non-negative arithmetic function. Denote by $d := [\mathbb{Q}(\alpha) : \mathbb{Q}]$ the degree of $\alpha$ over $\mathbb{Q}$. Define

$$S_{g,\nu} = \left\{ \alpha \in \overline{\mathbb{Q}} \mid \text{at least } g(d) \text{ many conjugates of } \alpha \text{ lie in } K_\nu \right\}.$$

**Theorem 1.2.** *Let $g$ and $K_\nu$ be as above. For any $\epsilon > 0$, for all but finitely many $\alpha \in S_{g,\nu}$,*

$$h(\alpha) \geq \frac{1}{2\, d_\nu} \left( \frac{g(d)}{d} \right)^2 \frac{\log q}{q+1} - \epsilon.$$

The method of proof of the above theorem can be used to derive the following consequences.

**Proposition 1.3.** *Let $K_\nu$ be as above. For $c > 0$, let $S_c$ denote the set of non-zero $\alpha \in \overline{\mathbb{Q}} \smallsetminus \mu_\infty$ such that*

$$\sqrt{\left(\frac{2(q+1)\, d_\nu\, d}{\log q}\right)\left(c + \frac{\log qd}{2}\right)}$$

*many conjugates of $\alpha$ lie in $K_\nu$. Then, except for finitely many $\alpha \in S_c$*

$$h(\alpha) \geq \frac{c}{d}.$$

*In other words, Lehmer's conjecture holds for $S_c$.*

This proves that a condition much weaker than "positive proportion" of conjugates in $K_\nu$ is sufficient to establish Lehmer's conjecture. In particular, it is enough to show that $\gg \sqrt{d \log d}$ many conjugates of $\alpha$ lie in a fixed local field, with a suitable implied constant. As a corollary of the above proposition, we have the following.

**Corollary 1.4.** *Let $K_\nu$ be as above. Suppose*

$$S := \left\{\alpha \in \overline{\mathbb{Q}} \smallsetminus \{\mu_\infty\} \mid \text{ at least } (q^3 d_\nu\, d \log d)^{1/2} \text{ many conjugates of } \alpha \text{ lie in } K_\nu\right\}.$$

*Then, Lehmer's conjecture holds for $S$. In fact, $M(\alpha) \to \infty$ as $d \to \infty$.*

Rather than fixing one local field, one can consider several local fields over multiple primes to obtain a potentially better lower bound on $h(\alpha)$. However, this makes the explicit version a bit cumbersome. Towards this, we first set up some notation.

Let $\alpha \in \overline{\mathbb{Q}} \smallsetminus \mu_\infty$ be a fixed non-zero algebraic number. Let $\mathcal{F}_p$ denote the set of all finite extensions of $\mathbb{Q}_p$. We have a partial ordering on $\mathcal{F}_p$ respecting the inertia degree. With respect to $\alpha$, we give a total ordering on $\mathcal{F}_p$ as follows. Denote by $\mathcal{F}_p^{(i)}$ the set of all finite extensions of $\mathbb{Q}_p$ whose residue field is $\mathbb{F}_q$, where $q = p^i$. Define a total order $<$ on $\mathcal{F}_p^{(i)}$ such that for $K_\nu, K_\omega \in \mathcal{F}_p^{(i)}$, we say $K_\nu < K_\omega$ if

(i) $[K_\nu : \mathbb{Q}_p] < [K_\omega : \mathbb{Q}_p]$ or

(ii) $[K_\nu : \mathbb{Q}_p] = [K_\omega : \mathbb{Q}_p]$ and $|\{\alpha_1, \alpha_2, \ldots, \alpha_d\} \cap K_\nu| < |\{\alpha_1, \alpha_2, \ldots, \alpha_d\} \cap K_\omega|$.

If $[K_\nu : \mathbb{Q}_p] = [K_\omega : \mathbb{Q}_p]$ and $|\{\alpha_1, \alpha_2, \ldots, \alpha_d\} \cap K_\nu| = |\{\alpha_1, \alpha_2, \ldots, \alpha_d\} \cap K_\omega|$, then for all such $\nu, \omega$, we force a fixed well-ordering with respect to $<$. Further, for any $K_\nu \in \mathcal{F}_p^{(i)}$ and $K_\omega \in \mathcal{F}_p^{(j)}$ such that $i < j$, define $K_\nu < K_\omega$. Hence, $(\mathcal{F}_p, <)$ is a totally ordered set. It is in fact a well ordered set with the given order.

We use the notation $\nu$ for the $\nu$-adic valuation on the local field $K_\nu$. Denote by $d_\nu$ the degree of the extension $K_\nu/\mathbb{Q}_p$ and $\mathbb{F}_{q_\nu}$ the residue field of $K_\nu/\mathbb{Q}_p$. For each $K_\nu \in \mathcal{F}_p$ and $x \in \mathbb{F}_{q_\nu}$, define

$$N_{\nu,x} := \#\left\{\alpha_i \in K_\nu : \alpha_i \notin K_\omega \text{ for } K_\omega < K_\nu, \text{ and } \alpha_i \equiv x \bmod q_\nu\right\},$$

where $\alpha_i$'s run over all the Galois conjugates of $\alpha$. For $x \in \mathbb{F}_{q_\nu}$, also define

$$\delta_{x,\nu} := \begin{cases} 1 & \text{if } N_{\nu,x} > 0 \\ 0 & \text{otherwise.} \end{cases}$$

Denote by $\mathcal{F}_{p,\alpha}$ the smallest subset of $\mathcal{F}_p$ such that $N_{x,\nu} = 0$ for all $K_\nu \in \mathcal{F}_p \smallsetminus \mathcal{F}_{p,\alpha}$ and for all $x \in \mathbb{F}_{q_\nu}$. By definition, $\mathcal{F}_{p,\alpha}$ is a finite set.

**Theorem 1.5.** *Let $\alpha \in \overline{\mathbb{Q}} \smallsetminus \{\mu_\infty\}$ be a non-zero algebraic integer. Let $\mathcal{F}_{p,\alpha}$ and $N_{\nu,x}$ be as above. Denote*

$$r_\nu := \frac{\log q_\nu}{d_\nu}.$$

*Then,*

$$h(\alpha) \geq \frac{1}{2} \sum_p \left( \frac{1}{\sum_{\nu \in \mathcal{F}_{p,\alpha}} \frac{q_\nu}{r_\nu}} \right) \left( 1 - \left( \frac{\sum_{\nu \in \mathcal{F}_{p,\alpha}} \sum_{x \in \mathbb{F}_{q_\nu}} \delta_{x,\nu}\, r_\nu}{\sum_{\nu \in \mathcal{F}_{p,\alpha}} \sum_{x \in \mathbb{F}_{q_\nu}} N_{\nu,x}^2\, r_\nu} \right)^{1/2} \right) - \frac{\log d}{2d}.$$

Note that the term inside the outer parenthesis above is always non-negative. For a totally $p-$adic algebraic integer, not a root of unity, Theorem 1.5 implies that

$$h(\alpha) \geq \frac{1}{2} \left( 1 - \frac{1}{d} \right) \frac{\log p}{p} - \frac{\log d}{2d}.$$

Hence, by Northcott's theorem (Theorem 2.1), for any $\epsilon > 0$, except for finitely many $\alpha \in \mathbb{Z}_p$,

$$h(\alpha) \geq \frac{\log p}{2p} - \epsilon.$$

It is important to note that our method can be used to extend Theorem 1.5 to algebraic numbers at the cost of a slightly weaker lower bound. Since Lehmer's conjecture is the theme of this article, we restrict ourselves to algebraic integers, as Lehmer's conjecture trivially holds for algebraic non-integers.

**Corollary 1.6.** *Let $N_\nu$ be the total number of conjugates of $\alpha$ in $K_\nu$. Let $\alpha \in \overline{\mathbb{Q}} \setminus \{\mu_\infty\}$ be a non-zero algebraic integer and $\mathcal{F}_{p,\alpha}$ be as above. Then*

$$h(\alpha) \geq \frac{1}{2} \sum_p \left( \sum_{\nu \in \mathcal{F}_{p,\alpha}} \left( \frac{N_\nu^2}{q_\nu} - N_\nu \right) \frac{\log q_\nu}{d_\nu} \right) - \frac{\log d}{2d}.$$

In other words, if conjugates of $\alpha$ lie in several local fields $K_\nu$ with small inertia degree, then we obtain a meaningful lower bound for $h(\alpha)$. This can be compared with a theorem of Mignotte [23], which states that if there exists a prime $p \leq d \log d$, which splits completely in $\mathbb{Q}(\alpha)$, then $M(\alpha) \geq 1.2$. An improvement due to Silverman (alluded to in the literature but unpublished) states that if there are $d$ distinct prime ideals in $\mathbb{Q}(\alpha)$ with norm $\leq \sqrt{d \log d}$, then $M(\alpha) \geq 1 + c$ for some $c > 0$. Indeed, if there are several primes with small norms in $K = \mathbb{Q}(\alpha)$, by Weil's explicit formula, one can obtain a sharper bound on the absolute discriminant $|\Delta(K/\mathbb{Q})|$. For $\alpha$ an algebraic integer, we have $\Delta(K/\mathbb{Q})$ divides $D(m_\alpha)$, the discriminant of the minimal polynomial of $\alpha$. Thus, Mahler's inequality (Theorem 2.2) can be applied and one obtains a lower bound on $h(\alpha)$. This phenomenon is explicitly demonstrated in [12] by the authors .

## 2. **Preliminaries**

In this section, we recall some definition and results which will be used towards the proof of our theorems.

The Weil height gives a partial ordering on algebraic numbers with bounded degree. This follows from a classical result of Northcott [24].

**Theorem 2.1** (Northcott)**.** *There are finitely many algebraic numbers $\alpha \in \overline{\mathbb{Q}}$ with bounded degree $d$ and height $h(\alpha)$.*

To connect the Weil height with the discriminant of the minimal polynomial, we shall use Mahler's inequality [20].

**Theorem 2.2** (Mahler). *Let* $m_\alpha(x) = a_d x^d + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ *be a polynomial with roots* $\alpha_1, \alpha_2, \cdots, \alpha_d$. *Let*

$$D(m_\alpha) := a_d^{2d-2} \prod_{i>j} (\alpha_i - \alpha_j)^2$$

*be its discriminant. Then,*

$$|D(m_\alpha)| \leq d^d M(\alpha)^{2d-2}.$$

## 3. Proof of the main theorems

Let $K_\nu$ be a finite extension of $\mathbb{Q}_p$ and $g$ be a non-negative arithmetic function. Recall that

$$S_{g,\nu} = \{\alpha \in \overline{\mathbb{Q}} \mid \text{ at least } g(d) \text{ many conjugates of } \alpha \text{ lies in } K_\nu\}.$$

We set $\nu$ to be the unique valuation extending the usual $p$ -adic valuation on $K_\nu$. Our proof is inspired by the proof of [6, Theorem 2] due to Bombieri-Zannier.

*Proof of Theorem 1.2.* For $\alpha \in S_{g,\nu}$, let

$$m_\alpha(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0$$

be the minimal polynomial of $\alpha$ over $\mathbb{Q}$. Let $L_\omega$ be the splitting field of $m_\alpha(x)$ over $K_\nu$ with the unique valuation $\omega$ extending $\nu$ on $K_\nu$. Write

$$m_\alpha(x) = a_d (x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d),$$

where $\alpha_i \in L_\omega$ satisfy

$$\omega(\alpha_1) \geq \cdots \geq \omega(\alpha_r) \geq 0 > \omega(\alpha_{r+1}) \geq \cdots \geq \omega(\alpha_d).$$

The discriminant of $m_\alpha(x)$ is given by

$$D(m_\alpha) = a_d^{2d-2} \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

The contribution in the product where at least one $\omega(\alpha_j) < 0$ can be bounded by

$$\omega\left( \prod_{j=r+1}^{d} \prod_{i=1}^{j-1} (\alpha_j - \alpha_i) \right) \geq \sum_{j=r+1}^{d} (j-1)\, \omega(\alpha_j).$$

Hence, we obtain

$$\begin{aligned} \omega(D(m_\alpha)) &\geq (2d-2)\omega(a_d) + 2 \sum_{0<i<j\leq r} \omega(\alpha_j - \alpha_i) + 2 \sum_{j=r+1}^{d} (j-1)\, \omega(\alpha_j) \\ &\geq 2 \sum_{i<j\leq r} \omega(\alpha_j - \alpha_i) - 2 \sum_{j=r+1}^{d} (d-j)\, \omega(\alpha_j). \end{aligned} \tag{2}$$

Since $\omega(\alpha_j) < 0$ for $r+1 \leq j \leq d$, omitting a few non-negative terms, if necessary, gives the following inequality

$$\begin{aligned} \mathrm{ord}_p(D(m_\alpha)) = \omega(D(m_\alpha)) &\geq 2 \sum_{i<j\leq r} \omega(\alpha_j - \alpha_i) - 2 \sum_{j=r+1}^{d} (d-j)\, \omega(\alpha_j) \\ &\geq 2 \sum_{\substack{i<j\leq r \\ \alpha_i, \alpha_j \in K_\nu}} \nu(\alpha_j - \alpha_i) - 2 \sum_{\substack{r<j\leq d \\ \alpha_j \in K_\nu}} (d-j)\, \nu(\alpha_j). \end{aligned} \tag{3}$$

Let $N_x$ denote the number of roots $\alpha_j$ of the polynomial $m_\alpha$ in $K_\nu$, which lie in the residue class $x \bmod \nu$. If $\alpha_i, \alpha_j \in K_\nu$ lie in the same residue class modulo $\nu$, then $\nu(\alpha_i - \alpha_j) \geq \frac{1}{e_\nu}$. Hence,

$$\sum_{\substack{i<j\leq r \\ \alpha_i, \alpha_j \in K_\nu}} \nu(\alpha_j - \alpha_i) \geq \frac{1}{e_\nu} \sum_{x \in \mathbb{F}_q} \frac{N_x(N_x - 1)}{2},$$

where $q = p^{f_\nu}$. Let $d'$ (resp. $r'$) be the total number of conjugates (resp. $\nu$ -integral conjugates) of $\alpha$ lying in $K_\nu$. The second summation in (3) runs over all $d' - r'$ non-integral conjugates of $\alpha$ in $K_\nu$. Furthermore, since $d - j$ are all distinct positive integers, we have

$$\sum_{\substack{r<j\leq d \\ \alpha_j \in K_\nu}} (d-j) \geq \frac{(d'-r')(d'-r'-1)}{2}.$$

Note that $\nu(\alpha_i) \leq -\frac{1}{e_\nu}$ and therefore (3) implies that

$$\mathrm{ord}_p(D(m_\alpha)) \geq \frac{1}{e_\nu} \left( \sum_{x \in \mathbb{F}_q} N_x(N_x - 1) + (d'-r')(d'-r'-1) \right).$$

Also the number of roots of $m_\alpha(x)$ in $K_\nu$ is at least $g(d)$, and hence,

$$d' - r' + \sum_{x \in \mathbb{F}_q} N_x \geq g(d).$$

Now, applying Cauchy-Schwarz inequality, we obtain

$$\begin{aligned}
\mathrm{ord}_p(D(m_\alpha)) &\geq \frac{1}{e_\nu} \left( \sum_{x \in \mathbb{F}_q} N_x(N_x - 1) + (d'-r')(d'-r'-1) \right) \\
&= \frac{1}{e_\nu} \left( \sum_{x \in \mathbb{F}_q} N_x^2 + (d'-r')^2 + O(d) \right) \\
&\geq \frac{1}{e_\nu} \left( \frac{g(d)^2}{q+1} + O(d) \right),
\end{aligned}$$

where the implied constant has absolute value $\leq 1$. Therefore,

$$\begin{aligned}
\log |D(m_\alpha)| &\geq \frac{1}{e_\nu} g(d)^2 \left( \frac{\log p}{q+1} \right) + O\left( d \frac{\log p}{e_\nu} \right) \\
&\geq \frac{1}{d_\nu} g(d)^2 \left( \frac{\log q}{q+1} \right) + O\left( d \, \frac{\log q}{d_\nu} \right).
\end{aligned}$$

Applying Mahler's inequality (Theorem 2.2), we deduce that

$$\begin{aligned}
d\, h(\alpha) = \log M(\alpha) &\geq \frac{\log |D(m_\alpha)|}{2d} - \frac{\log d}{2} \\
&\geq \frac{1}{2\, d_\nu} \left( \frac{g(d)^2}{d} \right) \frac{\log q}{(q+1)} + O\left( \frac{\log q}{d_\nu} \right) - \frac{\log d}{2}, \qquad (4)
\end{aligned}$$

with the implied constant in the $O$-term has absolute value $\leq 1/2$. Finally, for any $\epsilon > 0$, using Northcott's Theorem 2.1 we conclude the proof of Theorem 1.2.

□

*Proof of Proposition 1.3.* From (4), we deduce that if

$$g(d) \geq \sqrt{\left(\frac{2(q+1)\,d_\nu\,d}{\log q}\right)\left(c + \frac{\log qd}{2}\right)}$$

then

$$d\,h(\alpha) \geq c + \frac{\log q}{2} + O\left(\frac{\log q}{d_\nu}\right).$$

Since the absolute value of the implied constant of the $O$-term is bounded above by $1/2$, we conclude that

$$h(\alpha) \geq \frac{c}{d}.$$

□

*Proof of Corollary 1.4.* Taking $g(d) \geq (q^3\,d_\nu\,d\log d)^{1/2}$ in (4), we obtain

$$d\,h(\alpha) \quad \geq \quad \left(\frac{q^3\log q - q - 1}{2(q+1)}\right)\log d + O\left(\frac{\log q}{d_\nu}\right). \tag{5}$$

Note that for any real number $x \geq 2$,

$$\frac{x^3\,\log x - x - 1}{2(x+1)} \;\geq\; \frac{2}{5}.$$

This is because the function in the LHS is increasing for $x \geq 2$ and the inequality holds for $x = 2$. Applying this to (5), we obtain

$$d\,h(\alpha) \geq \frac{2}{5}\log d + O\left(\frac{\log q}{d_\nu}\right).$$

Therefore, as $d \to \infty$, the Mahler measure $M(\alpha) = d\,h(\alpha)$ also tends to infinity as required. □

*Proof of Theorem 1.5.* Let $\alpha \in \overline{\mathbb{Q}}$ and $m_\alpha(x) \in \mathbb{Z}[x]$ be its minimal polynomial and $D(m_\alpha)$ be its discriminant. We can write

$$|D(m_\alpha)| = \prod_i {p_i}^{\mathrm{ord}_{p_i}(D(m_\alpha))}.$$

Now, it follows from the definition of $\mathcal{F}_p$ that

$$\mathrm{ord}_p(D(m_\alpha)) = \sum_p \sum_{\nu\in\mathcal{F}_{p,\alpha}} \nu(D(m_\alpha)).$$

Thus, we have

$$\begin{aligned}\log|D(m_\alpha)| &\geq \sum_p \sum_{\nu\in\mathcal{F}_{p,\alpha}} \sum_{x\in\mathbb{F}_{q_\nu}} N_{\nu,x}\,(N_{\nu,x}-1)\,\frac{\log p}{e_\nu}\\ &\geq \sum_p \sum_{\nu\in\mathcal{F}_{p,\alpha}} \sum_{x\in\mathbb{F}_{q_\nu}} N_{\nu,x}\,(N_{\nu,x}-1)\,r_\nu,\end{aligned} \tag{6}$$

where $d_\nu = [K_\nu : \mathbb{Q}_p]$ and $r_\nu = (\log q_\nu)/d_\nu$. Since $\sum_{\nu\in\mathcal{F}_{p,\alpha}} \sum_{x\in\mathbb{F}_{q_\nu}} N_{\nu,x} = d$, using Cauchy-Schwarz inequality, we obtain

$$\sum_{\nu\in\mathcal{F}_{p,\alpha}} \sum_{x\in\mathbb{F}_{q_\nu}} N_{\nu,x}^2\,r_\nu \;\geq\; \frac{\left(\sum_{\nu\in\mathcal{F}_{p,\alpha}}\sum_{x\in\mathbb{F}_{q_\nu}} N_{\nu,x}\right)^2}{\left(\sum_{\nu\in\mathcal{F}_{p,\alpha}}\sum_{x\in\mathbb{F}_{q_\nu}} \frac{\delta_{x,\nu}}{r_\nu}\right)} \;\geq d^2\;\frac{1}{\left(\sum_{\nu\in\mathcal{F}_{p,\alpha}}\sum_{x\in\mathbb{F}_{q_\nu}} \frac{\delta_{x,\nu}}{r_\nu}\right)}$$

and

$$\sum_{\nu\in\mathcal{F}_{p,\alpha}}\sum_{x\in\mathbb{F}_{q_\nu}} N_{\nu,x}\, r_\nu \le \left(\sum_{\nu\in\mathcal{F}_{p,\alpha}}\sum_{x\in\mathbb{F}_{q_\nu}} N_{\nu,x}^2\, r_\nu\right)^{1/2}\left(\sum_{\nu\in\mathcal{F}_{p,\alpha}}\sum_{x\in\mathbb{F}_{q_\nu}} \delta_{x,\nu}\, r_\nu\right)^{1/2}$$

Combining these in (6), we have

$$\log|D(m_\alpha)| \ \ge\ d^2\sum_p\left(\frac{1}{\sum_{\nu\in\mathcal{F}_{p,\alpha}}\frac{q_\nu}{r_\nu}}\right)\left(1-\left(\frac{\sum_{\nu\in\mathcal{F}_{p,\alpha}}\sum_{x\in\mathbb{F}_{q_\nu}}\delta_{x,\nu}\, r_\nu}{\sum_{\nu\in\mathcal{F}_{p,\alpha}}\sum_{x\in\mathbb{F}_{q_\nu}}N_{\nu,x}^2\, r_\nu}\right)^{1/2}\right).$$

Finally, applying Mahler's inequality (Theorem 2.2), we obtain the theorem. □

*Proof of Corollary 1.6.* Recall the inequality (6)

$$\log|D(m_\alpha)| \ge \sum_p\sum_{\nu\in\mathcal{F}_{p,\alpha}}\sum_{x\in\mathbb{F}_{q_\nu}} N_{\nu,x}\,(N_{\nu,x}-1)\,\frac{\log q_\nu}{d_\nu}.$$

For $K_\nu\in\mathcal{F}_{p,\alpha}$, let $N_\nu=\sum_{x\in\mathbb{F}_{q_\nu}} N_{x,\nu}$ be the total number of conjugates of $\alpha\in K_\nu$. Again using Cauchy-Schwarz inequality, we obtain

$$\begin{aligned}\sum_{\nu\in\mathcal{F}_{p,\alpha}}\sum_{x\in\mathbb{F}_{q_\nu}} N_{\nu,x}\,(N_{\nu,x}-1)\,\frac{\log q_\nu}{d_\nu} &= \sum_{\nu\in\mathcal{F}_{p,\alpha}}\frac{\log q_\nu}{d_\nu}\sum_{x\in\mathbb{F}_{q_\nu}} N_{\nu,x}\,(N_{\nu,x}-1)\\ &\ge \sum_{\nu\in\mathcal{F}_{p,\alpha}}\left(\frac{N_\nu^2}{q_\nu}-N_\nu\right)\frac{\log q_\nu}{d_\nu}.\end{aligned}$$

The proof now follows by applying Mahler's inequality (Theorem 2.2). □

## 4. **Acknowledgements**

We thank Prof. Sinnou David for several fruitful discussions. We also thank Dr. Siddhi Pathak for helpful comments on an earlier version of this paper.

## References

[1] F. Amoroso, S. David, Le Probléme de Lehmer en Dimension Supérieure, *J. Reine Angew. Math.*, **513**, pp. 145-179, (1999).
[2] F. Amoroso, M. Mignotte, On the distribution of the roots of polynomials, *Ann. Inst. Fourier (Grenoble)*, **46(5)**, pp. 1275-1291, (1996).
[3] M. Baker, C. Petsche, Global discrepancy and small points on elliptic curves, *Int. Math. Res. Not.*, **2005**, no.61, pp. 3791–3834, (2005).
[4] M. Baker, R. Rumely, Equidistribution of small points, rational dynamics, and potential theory, *Ann. Inst. Fourier*, **56**, no.3, pp. 625–688 (2006).
[5] Y. Bilu, Limit distribution of small points on algebraic tori, *Duke Math. J.*, **89(3)**, pp. 465-476, (1997).
[6] E. Bombieri, U. Zannier, A note on heights in certain infinite extensions of $\mathbb{Q}$, *Atti. Acad. Naz. Lincei Cl. Sci. Mat. Fis. Natur. Rend. Lincei (9) Mat. Appl.*, **12**, pp. 5-14, (2001).
[7] P. Borwein, E. Dobrowolski and M.J. Mossinghoff, Lehmer's Problem for Polynomials With Odd Coefficients, *Ann. of Math.*, **166**, pp. 347-366, (2007).
[8] R. Breusch, On the distribution of the roots of a polynomial with integral coefficients, *Proc. Amer. Math. Soc.*, **2**, pp. 939-941, (1951).
[9] G. Burgos, J. Ignacio, P. Philippon, J. Rivera-Letellier, M. Sombra, The distribution of Galois orbits of points of small height in toric varieties, *Amer. J. Math.*, **141**, no. 2, pp. 309–381, (2019).
[10] A. Chambert-Loir, Mesures et équidistribution sur les espaces de Berkovich, *J. Reine Angew. Math.*, 595 , pp. 215–235, (2006).

[11] V. Dimitrov, A proof of the Schinzel-Zassenhaus conjecture on polynomials, *arXiv:1912.12545 [math.NT]*, (2019).
[12] A. B. Dixit, S. Kala, Lower bound on height of algebraic numbers and low lying zeros of the Dedekind zeta-function, *arXiv:2309.15872 [math.NT]*, (2023).
[13] A. B. Dixit, S. Kala, Bogomolov property for certain infinite non-Galois extensions, *arXiv:2404.11559 [math.NT]*, (2024).
[14] E. Dobrowolski, On a question of Lehmer and the number of irreducible factors of a polynomial, *Acta Arith.*, **34**, pp. 391-401, (1979).
[15] P. Erdös, P. Turán, On the distribution of roots of polynomials, *Ann. of Math. (2)*, **51**, pp. 105-119, (1950).
[16] P. Fili, Z. Miner, Equidistribution and the heights of totally real and totally p-adic numbers, *Acta Arith.*, **170(1)**, pp. 15-25, (2015).
[17] G. Höhn and N. P. Skoruppa, Un résultat de Schinzel, *J. Thor. Nombres Bordeaux*, **5**, no. 1, pp. 185, (1993).
[18] L. Kronecker, Zwei Sätze über Gleichungen mit Ganzzahligen Coefficienten, *J. Reine Angew. Math.*, **53**, pp. 173–175, (1857).
[19] D. H. Lehmer, Factorization of certain cyclotomic functions, *Ann. Math. 2.*, **34**, (3), pp. 461–479, (1933).
[20] K. Mahler, An inequality for the discriminant of a polynomial, *Michigan Math. J.*, **11**, pp. 257-262, (1964).
[21] D. Masser, Auxiliary Polynomials in Number Theory, *Cambridge Tracts in Mathematics*, **207**, Cambridge University Press, pp. 193-199, (2016).
[22] M. Mignotte, Sur un théorème de M. Langevin, *Acta Arith.*, **54**, no.1, pp. 81–86, (1989).
[23] M. Mignotte, Entiers Algébriques dont les Conjugués sont Proches du Cercle Unité, *Séminaire Delange-Pisot-Poitou, 19e année : 1977/78*, Théorie des Nombres, Fasc. 2, Exp. No. **39**, pp. 6, Paris (1978).
[24] D. G. Northcott, An inequality on the theory of arithmetic on algebraic varieties, *Proceedings of Cambridge Philosophical Soc.*, **45**, pp. 502-509, (1949).
[25] C. Petsche, A quantitative version of Bilu's equidistribution theorem, *Int. J. Number Theory*, **1**, no.2, pp. 281–291, (2005).
[26] L. Pottmeyer, Small totally $p$-adic algebraic numbers, *Int. J. Number theory*, **14**, no. 10, pp. 2687-2697, (2018).
[27] U. Rausch, On a theorem of Dobrowolski about the product of conjugate numbers, *Colloquium Mathematicum*, **50**, Issue. 1, pp. 137-142, (1985).
[28] R. Rumely, On Bilu's equidistribution theorem, *Contemp. Math.*, **237**, pp. 159–166, (1999).
[29] A. Schinzel, H. Zassenhaus, A refinement of two theorems of Kronecker, *Michigan Math J.*, **12**, pp. 81-85, (1965).
[30] A. Schinzel. On the product of the conjugates outside the unit circle of an algebraic number, *Acta Arith.*, **24**, pp. 385–399, (1973). Collection of articles dedicated to Carl Ludwig Siegel on the occasion of his seventy-fifth birthday. IV.
[31] C. J. Smyth, On the product of the conjugates outside the unit circle of an algebraic integer, *Bulletin of London Mathematical Society*, **3**, no. 2, pp. 169-175, (1971).
[32] C. J. Smyth, The Mahler Measure of Algebraic Numbers: A Survey, *Number Theory and Polynomials, London Math. Soc. Lecture Note Ser.*, **352**, Cambridge Univ. Press, Cambridge, pp. 322–349, (2008).
[33] K. Soundararajan, Equidistribution of zeros of polynomials, *Amer. Math. Monthly*, **126**, pp. 226-236, (2019).
[34] L. Szpiro, E. Ullmo and S. Zhang, Équirépartition des petits points, *Invent. Math.*, **127**, no. 2, pp. 337–347, (1997).
[35] J. Verger-Gaugry, A Survey on the Conjecture of Lehmer and the Conjecture of Schinzel-Zassenhaus, HAL-02315014, (2019).
[36] P. Voutier, An effective lower bound for the height of algebraic numbers, *Acta Arith.*, **74**, pp. 81-95, (1996).

Department of Mathematics, Institute of Mathematical Sciences (HBNI), CIT Campus, IV Cross Road, Chennai, India-600113
*Email address*: anupdixit@imsc.res.in

Department of Mathematics, Institute of Mathematical Sciences (HBNI), CIT Campus, IV Cross Road, Chennai, India-600113
*Email address*: sushant@imsc.res.in