Lehmer's conjecture via model theory

By Haydar GÖRAL

Department of Mathematics, Izmir Institute of Technology, 35430 Urla-Izmir, Turkey

(Communicated by Kenji FUKAYA, M.J.A., June 13, 2022)

Abstract: In this short note, we study Lehmer's conjecture in terms of stability theory. We state Bounded Lehmer's conjecture, and we prove that if a certain formula is uniformly stable in a class of structures, then Bounded Lehmer's conjecture holds. Our proof is based on Van der Waerden's theorem from additive combinatorics.

Key words: Lehmer's conjecture; Mahler measure; model theory; stability.

1. Introduction. For a non-zero polynomial

$$f(X) = a_d(X-\alpha_1)\cdots(X-\alpha_d) \in \mathbf{C}[X],$$

its *Mahler measure* is defined by the finite product

$$\mathrm{m}(f) = |a_d|\prod_{j=1}^{d}\max\{1,|\alpha_j|\}.$$

By Jensen's formula from complex analysis, we have the following integral representation for the Mahler measure of f

$$\mathrm{m}(f) = \exp\left(\frac{1}{2\pi}\int_0^{2\pi}\log(|f(e^{i\theta})|)d\theta\right),$$

which gives rise to a generalization of the Mahler measure for polynomials in several variables. Let $\overline{\mathbf{Q}}$ be the field of algebraic numbers and α be an element of $\overline{\mathbf{Q}}$. The Mahler measure of α, denoted by $\mathrm{m}(\alpha)$, is defined to be $\mathrm{m}(f)$, where f is the irreducible polynomial of α lying in $\mathbf{Z}[X]$. An open question in diophantine geometry is *Lehmer's conjecture*, and it states that there exists an absolute constant $c > 1$ such that if $\mathrm{m}(\alpha) > 1$ then $\mathrm{m}(\alpha) \geq c$. In other words, Lehmer's conjecture states that 1 is not a limit point of the set

$$\{\mathrm{m}(\alpha) : \alpha \in \overline{\mathbf{Q}}\}.$$

Lehmer [8] asked this question around 1933. Moreover, he also claimed that the polynomial

$$p(X) = X^{10} + X^9 - X^7 - X^6 - X^5 - X^4 - X^3 + X + 1$$

has the smallest Mahler measure among polynomials in $\mathbf{Z}[X]$, which are not products of cyclotomic polynomials. We also know that $\mathrm{m}(p)$ is approximately 1.17628, and this is still the smallest known Mahler measure of a polynomial in the set

$$\{f \in \mathbf{Z}[X] : \mathrm{m}(f) > 1\}.$$

In terms of degrees of algebraic numbers, Dobrowolski [3] obtained the best known quantitative result:

$$\mathrm{m}(\alpha) > 1 + \frac{1}{1200}\frac{(\log\log d)^3}{\log d} = 1 + u(d),$$

where $d = \deg(\alpha) \geq 2$. However, when d tends to infinity, the function $u(d)$ tends to zero.

For a given positive integer n, let $\tau(n)$ be the number of positive divisors of n. For instance, $\tau(p) = 2$ for any prime number p. It is also known that τ is multiplicative. Moreover, if $p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ is the prime factorization of n, then it follows that

$$\tau(n) = \tau(p_1^{\alpha_1}\cdots p_k^{\alpha_k}) = (\alpha_1+1)\cdots(\alpha_k+1).$$

The summatory function of $\tau(n)$ has been studied broadly, and one has that [1, Chapter 3]

$$\sum_{n\leq x}\tau(n) \sim x\log x.$$

Using the multiplicative property of τ, one can show that for a given $\varepsilon > 0$ there exist $n_0 = n_0(\varepsilon) \geq 1$ and $C_\varepsilon > 0$ such that if $n \geq n_0$ then $\tau(n) \leq C_\varepsilon n^\varepsilon$. Estimating the error term in the asymptotic expansion of the summatory function of τ is a recurrent topic in number theory, and it is known as the Dirichlet divisor problem [6].

For any positive integer B, define

$$\mathcal{A}_B = \{\alpha \in \overline{\mathbf{Q}} : \tau(\deg(\alpha)) \leq B\}.$$

2020 Mathematics Subject Classification. Primary 12L12, 11G50; Secondary 03C45.

doi: 10.3792/pjaa.98.010

To illustrate, $A_1 = \mathbf{Q}$, and for any $1 \leq n < m$, the difference $\mathcal{A}_m \setminus \mathcal{A}_n$ is infinite. Now, we are ready to state Bounded Lehmer's conjecture.

Bounded Lehmer's conjecture. For any positive integer B, there is a constant $c_B > 1$ such that if $\alpha \in \mathcal{A}_B$ and $\mathrm{m}(\alpha) > 1$, then $\mathrm{m}(\alpha) \geq c_B$.

In other words, Bounded Lehmer's conjecture states that for any positive integer B, 1 is not a limit point of the set $\{\mathrm{m}(\alpha) : \alpha \in \mathcal{A}_B\}$. Note that Lehmer's conjecture implies Bounded Lehmer's conjecture.

A real algebraic integer $\alpha > 1$ is called a *Salem number* if α and $1/\alpha$ are Galois conjugate and all other Galois conjugates of α are of absolute value 1. Observe that if α is a Salem number, then $\mathrm{m}(\alpha) = \alpha$. Lehmer [8] gave the smallest known Salem number as a root of the previously mentioned polynomial

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

A weaker version of Lehmer's conjecture is *Lehmer's conjecture for Salem numbers*, and it states that 1 is not a limit point of Salem numbers, and this is still an open problem. An algebraic number α is said to be *reciprocal* if it is Galois conjugate to $1/\alpha$. For instance, a Salem number is reciprocal. Smyth [11] proved that if α is not reciprocal, then its Mahler measure is far away from 1, precisely

$$\mathrm{m}(\alpha) \geq \mathrm{m}(X^3 - X - 1) \approx 1.3247.$$

For a nice survey on Salem numbers, we refer the reader to [10].

Let M be an L-structure and $\varphi(\bar{x}, \bar{y})$ be an L-formula. The formula $\varphi(\bar{x}, \bar{y})$ has the *k-order property* in M if there are $\bar{a}_i, \bar{b}_i$ in M for $1 \leq i \leq k$ such that $\varphi(\bar{a}_i, \bar{b}_j)$ holds if and only if $i \leq j$. If $\varphi(\bar{x}, \bar{y})$ does not have the k-order property in M, then $\varphi(\bar{x}, \bar{y})$ is said to be *k-stable* in M. Let T be a complete theory in the language L. A formula $\varphi(\bar{x}, \bar{y})$ is called *stable* for T if it is k-stable for any model M of T for some positive integer k. The theory T is said to be *stable* if any L-formula $\varphi(\bar{x}, \bar{y})$ is stable for T. In stable theories, there is a notion of *independence*, which is called the *forking* independence. For instance, the theory of algebraically closed fields is stable and the forking independence coincides with the algebraic independence. A theory is said to be *simple*, if the forking independence is symmetric. To add, stable theories are simple, see [13].

Using a result of Mann [9], Zilber [14] showed that the pair $(\mathbf{C}, \mu) \equiv (\overline{\mathbf{Q}}, \mu)$ is ω-stable (so stable) where μ is the group of complex roots of unity. Later on, van den Dries and Günaydın [4] generalized Zilber's result to algebraically closed fields with a multiplicative subgroup satisfying the Mann property. Kronecker's theorem [2, 1.5.9] states that if $\alpha \in \overline{\mathbf{Q}}$ is a non-zero algebraic number, then $\mathrm{m}(\alpha) = 1$ if and only if α is a root of unity. Assembling Zilber's result [14] with Kronecker's theorem, one can conclude that the pair

$$(\overline{\mathbf{Q}}, \{a \in \overline{\mathbf{Q}} : \mathrm{m}(a) = 1\})$$

is ω-stable.

Throughout this note, the language L_m will denote the language $\{1, \cdot\}$ where the binary operation $\cdot$ is the usual multiplication. Let $\mathbf{S}$ be the set of all Salem numbers. We put

$$P_b = \{a \in \overline{\mathbf{Q}}^{\times} : \mathrm{m}(a) \leq b\} \text{ and } \mathbf{S}_b = P_b \cap \mathbf{S}$$

where $b \geq 1$. By Kronecker's theorem, note that $P_1 = \mu$. Lehmer's conjecture and its version for Salem numbers state that there exists $b > 1$ such that $P_b = P_1 = \mu$ and $\mathbf{S}_b = \mathbf{S}_1 = \emptyset$ respectively. The pairs $(\overline{\mathbf{Q}}, P_b)$ and $(\overline{\mathbf{Q}}, \mathbf{S}_b)$ can be seen as $L_m(U) = L_m \cup \{U\}$ structures where U is a unary relation symbol whose interpretations are P_b and $\mathbf{S}_b$ respectively. In [5], the author showed that Lehmer's conjecture for Salem numbers holds if and only if the pair $(\overline{\mathbf{Q}}, \mathbf{S}_b)$ is simple in $L_m(U)$ for some $b > 1$. Here, we link Bounded Lehmer's conjecture and the stability of the pair $(\overline{\mathbf{Q}}, P_b)$. We prove that if a certain formula is uniformly stable in $(\overline{\mathbf{Q}}, P_b)$ for every sufficiently small $b > 1$, then Bounded Lehmer's conjecture holds.

Main Theorem. *Let M_b be the pair $(\overline{\mathbf{Q}}, P_b)$ in the language $L_m(U) = L_m \cup \{U\}$. Set*

$$\varphi(x, y, z) : U\left(\frac{zx}{y}\right).$$

(*a*) *If Lehmer's conjecture holds, then there exists a positive integer k such that for any sufficiently small $b > 1$, the formula $\varphi(x, y, z)$ is k-stable in M_b.*

(*b*) *Suppose that there exists a positive integer k such that for any sufficiently small $b > 1$, the formula $\varphi(x, y, z)$ is k-stable in M_b. Then, Bounded Lehmer's conjecture is true.*

2. Height function and arithmetic progressions.

2.1. Height function. In this subsection, we introduce the height function and list some of its properties. For more on the height function and its place in diophantine geometry, we direct the reader to [2,7]. For an algebraic number α with irreducible polynomial $f(x) \in \mathbf{Z}[X]$, the *height* of α is defined by

$$\mathrm{H}(\alpha) = \mathrm{m}(\alpha)^{1/d}$$

where $d = \deg f = \deg(\alpha)$.

The height function satisfies the following properties:

- $\mathrm{H}(0) = \mathrm{H}(1) = 1$.
- For a non-zero rational number a/b where a and b are coprime integers,
$$\mathrm{H}(a/b) = \max\{|a|, |b|\}.$$
- For all α in $\overline{\mathbf{Q}}$ and $n \in \mathbf{N}$, we have $\mathrm{H}(\alpha^n) = \mathrm{H}(\alpha)^n$.
- For all α and β in $\overline{\mathbf{Q}}$, we have $\mathrm{H}(\alpha\beta) \leq \mathrm{H}(\alpha)\mathrm{H}(\beta)$.
- For all non-zero α in $\overline{\mathbf{Q}}$, we have $\mathrm{H}(1/\alpha) = \mathrm{H}(\alpha)$.
- For all α and β in $\overline{\mathbf{Q}}$, we have $\mathrm{H}(\alpha + \beta) \leq 2\mathrm{H}(\alpha)\mathrm{H}(\beta)$.

2.2. Arithmetic progressions. The sequence of numbers $h_1, \ldots, h_k$ is called a *k-term arithmetic progression* (k-AP) if there exists d such that $h_i = h_1 + (i-1)d$ for $i = 1, \ldots, k$. For instance, $a_1 < a_2 < a_3$ form a 3-term AP if a_2 is the arithmetic mean of a_1 and a_3, that is $a_2 = \frac{a_1+a_3}{2}$.

Now, we state Van der Waerden's theorem [12], and it will play an important role in the proof of our result.

Theorem 2.1. [12] *For any given positive integers r and k, there exists N such that if the set $\{1, 2, \ldots, N\}$ is colored using r different colors, then $\{1, 2, \ldots, N\}$ contains a k-AP whose members are of the same color.*

The least such N in the previous theorem is called the Van der Waerden's number $W(r,k)$. Finding a good upper bound for $W(r,k)$ is a very difficult problem. In some cases, it is possible to find the exact values of these numbers. For instance, $W(2,3) = 9$ and $W(3,3) = 27$, but not many of them are known.

3. Proof of the Main Theorem. (a) First, suppose that Lehmer's conjecture is true. This yields that for every sufficiently small $b > 1$, one has $P_b = \mu$ and $M_b = (\overline{\mathbf{Q}}, P_b) = (\overline{\mathbf{Q}}, \mu)$. By Zilber's result [14], we know that the pair $(\overline{\mathbf{Q}}, \mu)$ is ω-stable in $L_m(U)$. Thus, the formula

$$\varphi(x,y,z) : U\left(\frac{zx}{y}\right)$$

is k-stable in M_b for some positive integer k for every sufficiently small $b > 1$.

(b) Suppose that there exists a positive integer k such that for any sufficiently small $b > 1$, the formula $\varphi(x,y,z)$ is k-stable in M_b. Assume on the contrary that Bounded Lehmer's conjecture is false. So, there exists a positive integer B such that 1 is a limit point of the set

$$\{\mathrm{m}(\alpha) : \alpha \in \mathcal{A}_B\}$$

where

$$\mathcal{A}_B = \{\alpha \in \overline{\mathbf{Q}} : \tau(\deg(\alpha)) \leq B\}.$$

Let $\delta > 1$ be any real number. By Van der Waerden's theorem [12], if the set

$$\{1, \ldots, W(B, 2k+1)\}$$

is colored with B-many colors, then there is a monochromatic arithmetic progression of length $2k+1$. By the assumption, there exists an algebraic number $\alpha \in \mathcal{A}_B$ such that

$$1 < \mathrm{m}(\alpha) < \delta^{1/W(B,2k+1)}. \tag{1}$$

First, we observe that for any n, the inequality $m(\alpha^n) \leq m(\alpha)^n$ holds. Let $d = \deg(\alpha)$ and $d_n = \deg(\alpha^n)$. Since $\mathbf{Q}(\alpha^n)$ is a subfield of $\mathbf{Q}(\alpha)$, the integer d_n is a divisor of d. As

$$\mathrm{m}(\alpha) = \mathrm{H}(\alpha)^d,$$

by the properties of the height function, one has that

$$\mathrm{m}(\alpha^n) = \mathrm{H}(\alpha^n)^{d_n} = \mathrm{H}(\alpha)^{nd_n} \leq \mathrm{H}(\alpha)^{nd} = \mathrm{m}(\alpha)^n.$$

The previous observation together with (1) yield that for any $n \leq W(B, 2k+1)$, we have that

$$\mathrm{m}(\alpha^n) \leq \delta.$$

Recall that $d_n = \deg(\alpha^n) \mid d = \deg(\alpha)$ and $\tau(\deg(\alpha)) \leq B$. Without loss of generality, we may assume that $\tau(\deg(\alpha)) = B$ and $e_1 < \cdots < e_B$ are all divisors of d. Now, consider the coloring

$$\mathcal{C} : \{1, \ldots, W(B, 2k + 1)\} \to \{1, \ldots, B\}$$

where

$$\mathcal{C}(n) = r \text{ with } d_n = e_r.$$

By Van der Waerden's theorem, there is a monochromatic arithmetic progression of length $2k+1$ in $\{1, \ldots, W(B, 2k+1)\}$. In other words, there exist positive integers a and ℓ such that

$$a + 2k\ell \leq W(B, 2k + 1)$$

and

$$\deg(\alpha^{a+j\ell}) = e$$

for some divisor e of d, and $j = 0, \ldots, 2k$. Let

$$b = \mathrm{m}(\alpha^{a+k\ell}).$$

Note that $1 < b < \delta$. Moreover, for any $j = 0, \ldots, 2k$ and by the properties of the height function, we see that

$$\mathrm{m}(\alpha^{a+j\ell}) = \mathrm{H}(\alpha)^{e(a+j\ell)}.$$

Thus, we have the following inequalities

$$\mathrm{m}(\alpha^{a}) < \mathrm{m}(\alpha^{a+\ell}) < \cdots < \underbrace{\mathrm{m}(\alpha^{a+k\ell})}_{b} < \cdots < \mathrm{m}(\alpha^{a+2k\ell}). \tag{2}$$

Next, we show that the formula $\varphi(x, y, z)$ is not k-stable in the pair $M_b = (\overline{\mathbf{Q}}, P_b)$. Let $a_j = \alpha^{a+j\ell}$ and $\overline{b_j} = (\alpha^{a+j\ell}, \alpha^{a+k\ell})$ where $j = 1, \ldots, k$. Then, $\varphi(a_i, \overline{b_j})$ holds in M_b if and only if $\alpha^{a+(k+i-j)\ell}$ is in P_b, in other words,

$$\mathrm{m}(\alpha^{a+(k+i-j)\ell}) \leq \mathrm{m}(\alpha^{a+k\ell}).$$

By (2), the previous inequality holds if and only if $i \leq j$. Thus, we proved that $\varphi(a_i, \overline{b_j})$ holds in M_b if and only if $i \leq j$. Hence, the formula $\varphi(x, y, z)$ is not k-stable in the pair $M_b = (\overline{\mathbf{Q}}, P_b)$. This is a contradiction as $b > 1$ is sufficiently small, and the proof is now complete.

Acknowledgement. I am grateful to the referee for the comments which improved the quality of the paper.

References

[1] T. M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York, 1976.

[2] E. Bombieri and W. Gubler, *Heights in Diophantine geometry*, 1st ed., New Mathematical Monographs, 4, Cambridge University Press, Cambridge, 2006.

[3] E. Dobrowolski, On a question of Lehmer and the number of irreducible factors of a polynomial, Acta Arith. **34** (1979), no. 4, 391–401.

[4] L. van den Dries and A. Günaydın, The fields of real and complex numbers with a small multiplicative group, Proc. London Math. Soc. (3) **93** (2006), no. 1, 43–81.

[5] H. Göral, Algebraic numbers with elements of small height, Math. Logic Quart. **65** (2019), no. 1, 14–22.

[6] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 6th ed., Oxford University Press, Oxford, 2008.

[7] M. Hindry and J. H. Silverman, *Diophantine geometry*, Graduate Texts in Mathematics, 201, Springer-Verlag, New York, 2000.

[8] D. H. Lehmer, Factorization of certain cyclotomic functions, Ann. of Math. (2) **34** (1933), no. 3, 461–479.

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

[10] C. Smyth, Seventy years of Salem numbers, Bull. Lond. Math. Soc. **47** (2015), no. 3, 379–395.

[11] C. J. Smyth, On the product of the conjugates outside the unit circle of an algebraic integer, Bull. London Math. Soc. **3** (1971), no. 2, 169–175.

[12] B. L. Van der Waerden, Beweiseiner Baudetschen Vermutung, Nieuw Arch. Wisk. **15** (1927), 212–216.

[13] F. O. Wagner, *Simple theories*, Mathematics and its Applications, 503, Kluwer Academic Publishers, Dordrecht, 2000.

[14] B. Zilber, A note on the model theory of the complex field with roots of unity, 1990.