Journal de Théorie des Nombres de Bordeaux

Artūras Dubickas
Chris J. Smyth

The Lehmer constants of an annulus

Journal de Théorie des Nombres de Bordeaux, tome 13, n° 2 (2001), p. 413-420
<http://www.numdam.org/item?id=JTNB_2001__13_2_413_0>

Journal de Théorie des Nombres
de Bordeaux **13** (2001), 413–420

The Lehmer constants of an annulus

par ARTŪRAS DUBICKAS et CHRIS J. SMYTH

RÉSUMÉ. Soit $M(\alpha)$ la mesure de Mahler d'un nombre algébrique α, et V un ouvert de $\mathbb{C}$. Alors sa *constante de Lehmer* $L(V)$ est égale à inf $M(\alpha)^{1/\deg(\alpha)}$, l'infimum étant évalué sur tous les nombres algébriques non cyclotomiques α dont tous les conjugués sont à l'extérieur de V. Nous calculons $L(V)$ lorsque V est une couronne centrée en 0. Nous faisons de même pour la constante de Lehmer transfinie $L_\infty(V)$.

Nous démontrons également la réciproque d'un théorème de Langevin, qui affirme que $L(V) > 1$ si V contient un élément de module 1, ainsi que le résultat analogue avec $L_\infty(V)$.

ABSTRACT. Let $M(\alpha)$ be the Mahler measure of an algebraic number α, and V be an open subset of $\mathbb{C}$. Then its *Lehmer constant* $L(V)$ is inf $M(\alpha)^{1/\deg(\alpha)}$, the infimum being over all non-zero non-cyclotomic α lying with its conjugates outside V. We evaluate $L(V)$ when V is any annulus centered at 0. We do the same for a variant of $L(V)$, which we call the transfinite Lehmer constant $L_\infty(V)$.

Also, we prove the converse to Langevin's Theorem, which states that $L(V) > 1$ if V contains a point of modulus 1. We prove the corresponding result for $L_\infty(V)$.

1. Introduction and results

Let V be an open subset of $\mathbb{C}$. In 1985, Langevin [La1] introduced the following function, the *Lehmer constant*[1] *of* V (see [La3]), defined as

$$L(V) = \inf M(\alpha)^{1/\deg(\alpha)},$$

where the infimum is taken over every non-zero non-cyclotomic algebraic number α lying with its conjugates in $\mathbb{C}\backslash V$. Here $M(\alpha)$ is the *Mahler measure* of α:

$$M(\alpha) = |a_0| \prod_{i=1}^{d} \max(1, |\alpha_i|),$$

Manuscrit reçu le 9 novembre 1999.

[1]Strictly speaking, we should call $L(V)$ the *best* Lehmer constant, according to Langevin's original definition

where $\alpha = \alpha_1$ has minimal polynomial $a_0 z^d + ... + a_d \in \mathbb{Z}[z]$, and the α_i are the conjugates of α. As $M(\alpha) \geqslant 1$, $L(V) \geqslant 1$.

We define also a variant of $L(V)$, denoted $L_\infty(V)$, which we call the *transfinite Lehmer constant of* V, given by

$$L_\infty(V) = \lim_{d\to\infty} \inf M(\alpha)^{1/\deg(\alpha)} \geqslant 1,$$

where this time the infimum is taken over all α of degree $\geqslant d$ lying with their conjugates in $\mathbb{C}\backslash V$. Note that here, as distinct from in the definition of $L(V)$, α may be cyclotomic.

The main aim of the paper is to evaluate both $L(V)$ and $L_\infty(V)$ when V is an open annulus centered at 0. So, for $0 < r < R$ let

$$A(r,R) = \{z \in \mathbb{C} : r < |z| < R\}.$$

Then our main result is the following.

Theorem 1. *For* $0 < r < R$ *we have*

$$L(A(r,R)) = L_\infty(A(r,R)) = \begin{cases} \exp\left\{\frac{\log R \log(1/r)}{\log(R/r)}\right\} & \text{if } r < 1 < R \\ 1 & \text{if } r \geqslant 1 \text{ or } R \leqslant 1. \end{cases}$$

Corollary 1. *Let* $R > 1$ *and* $\gamma > 0$. *Then*

$$L\left(A\left(R^{-\gamma}, R\right)\right) = L_\infty\left(A\left(R^{-\gamma}, R\right)\right) = R^{\gamma/(1+\gamma)}.$$

Langevin [La1] proved the remarkable result that $L(V) > 1$ if V is an open set containing a point of modulus 1. (See also [M] and [D] for other proofs of Langevin's Theorem.) As we show in the proof of Theorem 2 (b), it follows immediately from this that also $L_\infty(V) > 1$. So the new part of our second result is that the converses also hold:

Theorem 2. *Let* V *be an open subset of* $\mathbb{C}$. *Then*

(a) $L(V) > 1$ *iff* V *contains a point of modulus 1.*

(b) $L_\infty(V) > 1$ *iff* V *contains a point of modulus 1.*

Furthermore, $L_\infty(V) \geqslant L(V)$.

Note that Theorem 2 is used in the proof of Theorem 1.

To date $L(V)$ has been evaluated for certain sectors

$$V_\theta = \{z : |\arg z| > \theta\}.$$

A result of Schinzel [Sc] is equivalent to $L(V_0) = \frac{1}{2}\left(1+\sqrt{5}\right)$. Rhin and Smyth [RS] evaluated $L(V_\theta)$ for θ belonging to nine subintervals of $[0,\pi]$, using a computational version of the method outlined in [La2]. In particular, $L\left(V_{\pi/2}\right) = 1.12933793...$ was evaluated.

Earlier, Langevin [La3] had found a lower bound for $L(\Delta) > 1.08$, where Δ was the interior of the circumcircle of the triangle with vertices 0 and $\left(1 \pm i\sqrt{399}\right)/20$. This implied that $L\left(V_{\pi/2}\right) > 1.08$. The results of [RS] also give lower bounds > 1 for $L(V_\theta)$ for $0 \leqslant \theta \leqslant \frac{2\pi}{3}$.

To our knowledge Theorem 1 contains the first exact evaluation of any $L_\infty(V) > 1$. However, Mignotte [M] showed that, for $\delta > 0$ there is an effective positive constant c such that $L_\infty(V_{\pi-\delta}) \geqslant 1 + c\delta^3$. Also, it is natural to conjecture that $L_\infty(V_0) = \ell^2$, where $\ell = 1.31427...$ is the constant given in [Sm], Theorem 1.

Langevin's choice of the name 'Lehmer constant' for the functions we have called $L(V)$ is because of Lehmer's 1933 question [Le1] as to whether there is an absolute constant $c > 1$ such that $M(\alpha) \geqslant c$ for any algebraic number α with $M(\alpha) > 1$. Langevin's result quoted in Theorem 2 (a) shows that if α and its conjugates are slightly restricted to keep away from a neighbourhood of a single point on the unit circle, then for some $c(V) > 1$ an exponentially stronger result $M(\alpha) \geqslant c(V)^{\deg(\alpha)}$ holds. In his review of [La3], Lehmer [Le2] has some dry observations on his still-unanswered question.

2. Proof of Theorem 1

For the proof, we need the corollary to the following lemma.

Lemma 1. *Let $C > 2$ and $a, b \in \mathbb{N}$, the set of positive integers. Then the polynomial $z^{a+b} + Cz^a + 1$ has b zeros in the annulus*

$$A\left((C-1)^{1/b}, (C+1)^{1/b}\right)$$

and a zeros in the annulus

$$A\left((C+1)^{-1/a}, (C-1)^{-1/a}\right).$$

Proof. Since $|Cz^a| > \left|z^{a+b} + 1\right|$ on $|z| = 1$, $z^{a+b} + Cz^a + 1$ has, by Rouché's Theorem, a zeros in $|z| < 1$, and so b zeros in $|z| > 1$. From $z^b + C + z^{-a} = 0$ we have for $|z| > 1$

$$C - 1 < |z^b| < C + 1$$

and for $|z| < 1$

$$C - 1 < \left|z^{-a}\right| < C + 1,$$

whence the results. The condition $C > 2$ ensures that the annuli do not overlap. □

We apply the lemma to a polynomial which was obtained by slightly perturbing the coefficients of the polynomial $\left(z^{mb}+\lambda^{mab}\right)\left(z^{ma}+\lambda^{-mab}\right)$, which clearly has mb zeros on $|z|=\lambda^{a}$ and ma zeros on $|z|=\lambda^{-b}$.

Corollary 2. *Let $a,b\in\mathbb{N}$, $\lambda>1$ and $\varepsilon>0$ be given. Then for m sufficiently large the polynomial*

$$P(z)=z^{m(a+b)}+2\lfloor\lambda^{mab}/2\rfloor z^{ma}+2 \quad \in\mathbb{Z}[z]$$

has ma zeros in the annulus

$$e^{-\varepsilon}\lambda^{-b}<|z|<e^{\varepsilon}\lambda^{-b}$$

and mb zeros in the annulus

$$e^{-\varepsilon}\lambda^{a}<|z|<e^{\varepsilon}\lambda^{a}.$$

The corollary follows easily by applying the lemma to $P\left(2^{1/(m(a+b))}z\right)/2$.

We can now prove Theorem 1. We first do the case $r<1<R$. It is convenient to consider this case in the Corollary 1 form, i.e. when $r=R^{-\gamma}$ for $\gamma=-\log r/\log R>0$. It is enough to prove that $L\left(A\left(R^{-\gamma},R\right)\right)\geqslant R^{\gamma/(1+\gamma)}$ and that $L_{\infty}\left(A\left(R^{-\gamma},R\right)\right)\leqslant R^{\gamma/(1+\gamma)}$. For then the full result in the case $r<1<R$ follows from the inequality $L_{\infty}\geqslant L$ of Theorem 2.

So, we first prove that $L\left(A\left(R^{-\gamma},R\right)\right)\geqslant R^{\gamma/(1+\gamma)}$. Let α, of degree d, lie with its conjugates in $\mathbb{C}\backslash A\left(R^{-\gamma},R\right)$, with say $|\alpha_1|,\ldots,|\alpha_m|\geqslant R$ and $|\alpha_{m+1}|,\ldots,|\alpha_d|\leqslant R^{-\gamma}$. Then on the one hand

$$M(\alpha)\geqslant|\alpha_1|\ldots|\alpha_m|\geqslant R^{m}$$

while on the other hand

$$M(\alpha)=M(1/\alpha)\geqslant|\alpha_{m+1}|^{-1}\ldots|\alpha_d|^{-1}\geqslant R^{(d-m)\gamma}$$

Hence

$$M(\alpha)^{\gamma+1}\geqslant R^{m\gamma}.R^{(d-m)\gamma}=R^{d\gamma}$$

so that

$$M(\alpha)^{1/d}\geqslant R^{\gamma/(1+\gamma)}$$

giving the required inequality. Note that for the proof of this inequality we have not made use of the arithmetical nature of the coefficients of the minimal polynomial of α. Also, it is easy to see from the steps of the proof that the inequality is an equality precisely when α is a unit lying with its conjugates on the two circles $|z|=R$ and $|z|=R^{-\gamma}$. See [DS] for a complete characterisation of such α.

For the other inequality $L_\infty(A(R^{-\gamma}, R)) \leqslant R^{\gamma/(1+\gamma)}$, we use Corollary 2 to prove the existence of monic irreducible polynomials with integer coefficients having all their zeros close to one or other of the circles bounding the annulus. To do this, we must choose values of λ, a and b to apply Corollary 2. Essentially, b/a will be a rational approximation to γ, and λ a close approximation to $R^{1/a}$. To be precise, we want a, b and λ so that

$$e^{\varepsilon}\lambda^{-b} < R^{-\gamma} < e^{2\varepsilon}\lambda^{-b}$$

and

$$e^{-2\varepsilon}\lambda^{a} < R < e^{-\varepsilon}\lambda^{a}.$$

It is easy to check that all these inequalities will be satisfied provided that b/a is in the interval

$$\left(\frac{\gamma \log R + \varepsilon}{\log R + 2\varepsilon}, \frac{\gamma \log R + 2\varepsilon}{\log R + \varepsilon}\right) \tag{1}$$

and, having chosen such a b/a, that $\log \lambda$ is in the interval

$$\left(\max\left(\frac{1}{b}\left(\gamma \log R + \varepsilon\right), \frac{1}{a}\left(\log R + \varepsilon\right)\right),\right.$$
$$\left.\min\left(\frac{1}{b}\left(\gamma \log R + 2\varepsilon\right), \frac{1}{a}\left(\log R + 2\varepsilon\right)\right)\right).$$

Note that both of these intervals are non-empty!

Having chosen a, b and λ in this way, we see from Corollary 2 that $P(z)$ has all its zeros outside $A(R^{-\gamma}, R)$. Note too that P has mb zeros in the annulus $e^{-\varepsilon}\lambda^a < |z| < e^{\varepsilon}\lambda^a$ with, for ε sufficiently small, the other ma zeros inside the unit circle. Also, P is irreducible, by Eisenstein's Criterion, so for α a zero of P we have

$$\begin{aligned}
M(\alpha)^{1/\deg \alpha} &\leqslant \left(e^{\varepsilon}\lambda^{a}\right)^{mb/(m(a+b))} \\
&\leqslant \left(e^{3\varepsilon}R\right)^{1/(1+a/b)} \\
&\leqslant \left(e^{3\varepsilon}R\right)^{1/(1+(\log R+\varepsilon)/(\gamma \log R+2\varepsilon))} \\
&= f(\varepsilon, R) \ \text{say}
\end{aligned}$$

using (1).

Since $f(\varepsilon, R) \to R^{\gamma/(1+\gamma)}$ as $\varepsilon \to 0$, we have $L_\infty(A(R^{-\gamma}, R)) \leqslant R^{\gamma/(1+\gamma)}$, as required. This completes the proof of the theorem when $r < 1 < R$.

The proof of the cases $r \geqslant 1$ or $R \leqslant 1$ follows immediately from Theorem 2 (a), (b).

3. Proof of Theorem 2

For this proof, we need to recall the nth Chebyshev polynomial of the second kind, $U_n(x)$, defined by

$$U_n\left(z+\frac{1}{z}\right)=\frac{z^{n+1}-z^{-(n+1)}}{z-z^{-1}}.$$

It is well-known (and easily shown) that $U_n(x)$ is a monic polynomial with integer coefficients, with all its zeros lying in the interval $[-2,2]$. So $U_n'(x)$ is of degree $n-1$ with leading coefficient n, and all zeros in $(-2,2)$.

Lemma 2. *When n is even, the only cyclotomic factor of*

$$z^{n-1}U_n'(z+1/z)$$

is z^2+1. When n is odd, the polynomial has no cyclotomic factors.

This is an example in [BS], where an algorithm is given for finding all points on a curve whose coordinates are roots of unity. The algorithm is based on the observation that any root of unity ω is conjugate to one of $-\omega,\omega^2$, or $-\omega^2$. Using this observation, it can be shown that any such point on the curve also lies on another curve, so that, by intersecting the two curves, all these points can be found. In the case of this lemma, we apply the algorithm to a curve obtained from $z^{n-1}U_n'(z+1/z)$ essentially by making z^n a new variable.

Curiously, the result of Lemma 2 contrasts with the corresponding factorisation with U_n replaced by T_n the nth Chebyshev polynomial of the first kind, defined by $T_n(z+1/z)=z^n+z^{-n}$. Since $T_n'(x)=nU_{n-1}(x)$, *all* of the factors of $z^{n-1}T_n'(z+1/z)$ are cyclotomic!

To prove part (a) of Theorem 2, recall that, from [La1], $L(V)>1$ if V contains a point of modulus 1. Conversely, suppose that V contains no such points.

Putting

$$P(z)=z^{n-1}U_n'(z+1/z)=nz^{2n-2}+\ldots+n\in\mathbb{Z}[z],$$

we know that all zeros of P are on $|z|=1$ and that, by Lemma 2, none of the zeros are roots of unity for n odd.

Suppose that, for a fixed odd $n>1$, P factorises over $\mathbb{Z}$ as $P=\prod_j Q_j$, where Q_j has degree d_j, leading coefficient $f_j\geqslant 1$, and say β_j as one of its zeros. As we have just seen, no β_j is a root of unity. Then $\prod_j f_j=n$, $\sum_j d_j=2n-2$ and, since all the β_j and their conjugates have modulus 1, $M(\beta_j)=f_j$.

Hence

$$n^{1/(2n-2)} = \left(\prod_j f_j\right)^{1/(2n-2)} = \prod_j \left(M(\beta_j)^{1/d_j}\right)^{d_j/(2n-2)}.$$

Now as the weights $d_j/(2n-2)$ sum to 1, we must have

$$M(\beta_j)^{1/d_j} \leqslant n^{1/(2n-2)}$$

for at least one j. Hence

$$1 \leqslant L(V) \leqslant \inf_{n \text{ odd}} n^{1/(2n-2)} = 1.$$

To prove (b), suppose first that V contains no point of modulus 1. Then all the nth roots of unity ω_n lie, with their conjugates, in $\mathbb{C}\backslash V$. But $M(\omega_n) = 1$, so that $L_\infty(V) = 1$.

Now suppose, on the contrary, that V contains a point of modulus 1. Then $\mathbb{C}\backslash V$ contains only finitely many conjugate sets of roots of unity. Such α can therefore be ignored in the definition of $L_\infty(V)$, showing that $L_\infty(V) \geqslant L(V) > 1$, using (a). This proves (b).

For the final remark, we have just seen that $L_\infty(V) \geqslant L(V)$ if V contains a point of $|z| = 1$, while from (a) and (b) $L_\infty(V) = L(V)$ if it does not contain such a point.

Acknowledgements. We gratefully acknowledge the support of the London Mathematical Society, enabling the first-named author to visit Edinburgh, where much of this work was done. He was also supported by the Lithuanian State Studies and Science Foundation.

References

[BS] F. Beukers, C. J. Smyth, *Cyclotomic points on curves.* Number Theory for the Millennium: Proc. Millennial Conf. Number Theory (B. C. Berndt et al., eds.), Urbana, Illinois, May 21 - 26, 2000, A K Peters, Ltd., Natick, MA (to appear 2002).

[D] A. Dubickas, *On the distribution of roots of polynomials in sectors. I.* Liet. Matem. Rink. **38** (1998), 34–58.

[DS] A. Dubickas, C. J. Smyth, *On the Remak height, the Mahler measure, and conjugate sets of algebraic numbers lying on two circles.* Proc. Edinburgh Math. Soc. **44** (2001), 1–17.

[La] M. Langevin, *Méthode de Fekete - Szegö et problème de Lehmer.* C. R. Acad. Sci. Paris Sér. I Math. **301** (1985), 463–466.

[La2] M. Langevin, *Minorations de la maison et de la mesure de Mahler de certains entiers algébriques.* C. R. Acad. Sci. Paris Sèr. I Math. **303** (1986), 523–526.

[La3] M. Langevin, *Calculs explicites de constantes de Lehmer.* Groupe de travail en théorie analytique et élémentaire des nombres, 1986-1987, 52–68, Publ. Math. Orsay, 88-01, Univ. Paris XI, Orsay, 1988.

[Le1] D. H. Lehmer, *Factorisation of certain cyclotomic functions.* Ann. of Math. (2) **34** (1933), 461–479.

[Le2] D. H. Lehmer, *Review of* [La3]. Math. Rev. 89j:11025.

[M] M. Mignotte, *Sur un théorème de M. Langevin.* Acta Arith. **54** (1989), 81–86.

[RS] G. Rhin, C. J. Smyth, *On the absolute Mahler measure of polynomials having all zeros in a sector.* Math. Comp. **65** (1995), 295–304.

[Sc] A. SCHINZEL, *On the product of the conjugates outside the unit circle of an algebraic number*. Acta Arith. **24** (1973), 385–399; Addendum **26** (1975), 329–331.

[Sm] C. J. SMYTH, *On the measure of totally real algebraic integers*. J. Austral. Math. Soc. Ser. A **30** (1980), 137–149.

Artūras DUBICKAS
Dept. of Mathematics and Informatics
Vilnius University
Naugarduko 24
Vilnius 2006
Lithuania
E-mail : arturas.dubickas@maf.vu.lt

Chris J. SMYTH
Dept. of Mathematics and Statistics
Edinburgh University
J.C.M.B, King's Buildings
Mayfield road
Edinburgh EH9 3JZ
Scotland
UK
E-mail : chris@maths.ed.ac.uk