ON THE LEHMER CONSTANT OF FINITE CYCLIC GROUPS

NORBERT KAIBLINGER

Abstract. Results of Lind on Lehmer's problem include the value of the Lehmer constant of the finite cyclic group $\mathbb{Z}/n\mathbb{Z}$, for $n \leq 5$ and all odd n. By complementary observations we determine the Lehmer constant of $\mathbb{Z}/n\mathbb{Z}$, for all n except for multiples of 420.

1. Introduction

Let n be a positive integer. Given a polynomial with integer coefficients, $f \in \mathbb{Z}[x]$, denote by $\mathsf{m}_n(f)$ its logarithmic Mahler measure over $\mathbb{Z}/n\mathbb{Z}$, defined by

$$\mathsf{m}_n(f) = \frac{1}{n}\sum_{k=0}^{n-1} \log|f(e^{2\pi ik/n})|.$$

By $\lambda_n > 0$ we denote the Lehmer constant of $\mathbb{Z}/n\mathbb{Z}$,

$$\lambda_n = \min_{\substack{f\in\mathbb{Z}[x],\\ \mathsf{m}_n(f)>0}} \mathsf{m}_n(f),$$

see [11]. We notice later that the minimum is indeed attained, and that it is the same if $\deg f \leq n-1$ is assumed. Lind [11] has given an upper bound for λ_n, see below, and he obtained the values

$$\lambda_1 = \log 2, \quad \lambda_2 = \frac{1}{2}\log 3, \quad \lambda_4 = \frac{1}{4}\log 3, \quad \text{and } \lambda_n = \frac{1}{n}\log 2 \ \text{ for all odd } n.$$

We sharpen his result, complement it by a lower bound, and obtain the value of λ_n for all n except for multiples of 420. The main result is formulated in Section 2 and it is proved in Section 3.

2. Main result

For a positive integer n, let $\begin{Bmatrix}\rho(n)\\ \rho'(n)\end{Bmatrix}$ denote the smallest $\begin{Bmatrix}\text{prime number}\\ \text{positive integer}\end{Bmatrix}$ that does not divide n. We write $p^k \parallel n$ when p^k is a principal divisor of n,

2010 *Mathematics Subject Classification.* Primary 11R09; Secondary 11B83, 11C08, 11T22.

Key words and phrases. Lind's Lehmer constants, logarithmic Mahler measure, finite cyclic group, cyclotomic polynomial.

Supported by the Austrian Science Fund FWF grant P 21339.

that is, if p is a prime and k is a positive integer such that $p^k \mid n$ and $p^{k+1} \nmid n$. Let

$$\rho''(n) = \min\left(\min_{p\nmid n} p,\ \min_{p^k\|n} p^{p^k}\right) = \min\left(\rho(n),\ \min_{p^k\|n} p^{p^k}\right).$$

Lind proved that $\lambda_n \leq \frac{1}{n}\log\rho(n)$, for all n. Extending his result we obtain the following theorem, our main result.

Theorem 1. *The Lehmer constant of $\mathbb{Z}/n\mathbb{Z}$ is of the form $\lambda_n = \frac{1}{n}\log\Lambda_n$, with an integer $\Lambda_n \geq 2$ not dividing n and in the range*

$$\rho'(n) \leq \Lambda_n \leq \rho''(n).$$

For all $n = 1, \dots, 419 \pmod{420}$, we have $\Lambda_n = \rho'(n) = \rho''(n)$.

Example 1. Example new values are $\lambda_6 = \frac{1}{6}\log 4$, $\lambda_8 = \frac{1}{8}\log 3$, or more generally,

$$\lambda_n = \frac{1}{n}\log 3 \quad \text{if, and only if, } n = 2k \text{ with } 3 \nmid k,$$
$$\lambda_n = \frac{1}{n}\log 4 \quad \text{if, and only if, } n = 6k \text{ with odd } k.$$

Remark 1. (i) Theorem 1 yields the exact value of λ_n when $\rho'(n) = \rho(n)$ or more generally, when $\rho'(n) = \rho''(n)$. Thus it also includes certain multiples of 420. For example, let $n = 6 \cdot k \cdot 420$ with $11 \nmid k$. Then $\rho'(n) = \rho(n) = 11$ and thus $\lambda_n = \frac{1}{n}\log 11$.
(ii) By Theorem 1 the known upper bound $\lambda_n \leq \frac{1}{n}\log\rho(n)$ is sharpened strictly for all $n = 6 \pmod{12}$, where it yields the exact value for λ_n, and also for certain multiples of 420. For example, let $n = 11 \cdot 13 \cdot 420$. Then the theorem implies $\lambda_n = \frac{1}{n}\log\Lambda_n$ with $\Lambda_n \in \{8, 9, 16\}$, while $\rho(n) = 17$.

Open question: Determine $\lambda_n = \frac{1}{n}\log\Lambda_n$ for $n = 420$. By Theorem 1 we have $\Lambda_{420} \in \{8, 9, 11\}$.

3. Proof of Theorem 1

We have, for $f \in \mathbb{Z}[x]$,

$$\mathsf{m}_n(f) = \frac{1}{n}\log|\Delta_n(f)| \qquad \text{with} \qquad \Delta_n(f) = \prod_{k=0}^{n-1} f(e^{2\pi ik/n}). \tag{1}$$

The number $\Delta_n(f)$ is always an integer, and there is an elementary way to see that. To this end we recall the determinantal relation of [13], readily extended here to f of arbitrary degree. If $\deg f \leq n-1$, write $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$, with zero coefficients where necessary. If a polynomial of higher degree is given, with coefficients $a'_0, a'_1, \dots$, replace it first with f as above by defining $a_k = \sum_{l=k \pmod n} a'_l$. Let C_a denote the $n \times n$

integer circulant matrix with first row $a = (a_0, \dots, a_{n-1})$. Then $\det C_a = \prod_{k=0}^{n-1} f(e^{2\pi ik/n})$ and it implies

$$\Delta_n(f) = \det C_a. \tag{2}$$

Hence, $\Delta_n(f)$ is indeed an integer. Observe that expressing $\mathsf{m}_n(f)$ in terms of the integer $\Delta_n(f)$ justifies the definition of the Lehmer constant λ_n as a minimum, not just an infimum. We will also use the expression of $\Delta_n(f)$ as a resultant, for example see [2, 5, 11]. Indeed since $\operatorname{Res}\big(x^n - 1, f(x)\big) = \prod_{k=0}^{n-1} f(e^{2\pi ik/n})$, we have

$$\Delta_n(f) = \operatorname{Res}\big(x^n - 1, f(x)\big). \tag{3}$$

The more commonly used expression $\operatorname{Res}\big(f(x), x^n - 1\big)$, with interchanged arguments, works as well, as long as only absolute values are considered. Indeed the sign of the determinant in (2) or of the resultant in (3) is irrelevant for $\mathsf{m}_n(f)$. We remark that the opposite sign is obtained for the polynomial $f^\vee(x) = -x^{n-1}f(1/x)$, with coefficient sequence $(-a_{n-1}, -a_{n-2}, \dots, -a_0)$, the negative of the usual reciprocal polynomial.

Remark 2. (i) Lehmer and Pierce [10, 13] investigated the sequences $\big\{\Delta_1(f), \Delta_2(f), \dots\big\}$, for $f \in \mathbb{Z}[x]$. For example, $f(x) = 2 - x$ yields $\Delta_n(f) = 2^n - 1$, the Mersenne numbers; we refer to [6, 7, 8, 9]. For Lehmer's problem, formulated in [10], we refer to [3, 14] and the spectacular solution for odd coefficients in [2]. Lind's Lehmer constants λ_n relate to the family $\big\{\Delta_n(f) \colon f \in \mathbb{Z}[x]\big\}$, for fixed n.
(ii) Our approach highlights and makes use of the fact that finding possible (or minimal) values of the logarithmic Mahler measure over $\mathbb{Z}/n\mathbb{Z}$ is equivalent to finding possible (or minimal) values of integer circular determinants, an open problem attributed to Taussky-Todd [12].

Call $f \in \mathbb{Z}[x]$ cyclotomic if all its zeros lie on the complex unit circle. As a preliminary observation we determine, for all n, the exact value of a cyclotomic variant of Lind's Lehmer constants.

Lemma 1. *For cyclotomic polynomials $f \in \mathbb{Z}[x]$, the minimal possible value of $\mathsf{m}_n(f) > 0$ is determined by*

$$\min_{\substack{f \in \mathbb{Z}[x] \text{ cyclotomic} \\ \mathsf{m}_n(f) > 0}} \mathsf{m}_n(f) = \frac{1}{n} \log \rho''(n). \tag{4}$$

Proof. First, Kronecker's theorem implies that any cyclotomic polynomial $f \in \mathbb{Z}[x]$ is the product of some of $\Phi_1, \Phi_2, \dots$ and a constant, if necessary; here $\Phi_m \in \mathbb{Z}[x]$ denotes the m-th cyclotomic polynomial, i.e., the monic polynomial whose zeros are the primitive m-th roots of unity. Since always

$$\Delta_n(f_1 f_2) = \Delta_n(f_1)\Delta_n(f_2) \tag{5}$$

and consequently, $\mathsf{m}_n(f_1f_2) \le \mathsf{m}_n(f_1) + \mathsf{m}_n(f_2)$, we thus obtain

$$\min_{\substack{f\in\mathbb{Z}[x] \text{ cyclotomic} \\ \mathsf{m}_n(f)>0}} \mathsf{m}_n(f) = \min_{\substack{m=1,2,\dots \\ \mathsf{m}_n(\Phi_m)>0}} \mathsf{m}_n(\Phi_m). \tag{6}$$

Let $\varphi(n)$ denote Euler's totient of n. We point out that

$$\begin{aligned} \Delta_n(\Phi_m) &= \operatorname{Res}\big(x^n-1, \Phi_m(x)\big) \\ &= \begin{cases} 0 & \text{if } m \mid n, \\ 1 & \text{if at least two distinct primes divide } m/\gcd(m,n), \\ p^{\varphi(q)} & \text{if } m/\gcd(m,n) \text{ is the power of a prime } p \nmid n \\ & \text{—here we write } \gcd(m,n) = q, \\ p^{\varphi(q)p^k} & \text{if } m/\gcd(m,n) \text{ is the power of a prime } p \mid n \\ & \text{—here we factorize } \gcd(m,n) = p^k q \text{ with } p^k \parallel n. \end{cases} \end{aligned} \tag{7}$$

We remark that by our approach no negative sign is needed here, for any m, n. This formula is obtained from [1, proof of Theorem 2], where it is used for a short proof of the formula for $\operatorname{Res}\big(\Phi_{m_1}(x), \Phi_{m_2}(x)\big)$; secondly, since

$$\operatorname{Res}\big(x^n-1, \Phi_m(x)\big) = \operatorname{Res}\big(\Phi_1(x^n), \Phi_m(x)\big), \tag{8}$$

the formula (7) also follows from applying [4, Proposition 14]; a third, convenient and direct source is [5, Theorem 3].

Notice that (7) implies for any n, m, that particularly

$$\Delta_n(\Phi_m) = 0, 1, \quad \text{or} \quad \Delta_n(\Phi_m) \ge \min\Big(\min_{p\nmid n} p, \min_{p^k\parallel n} p^{p^k}\Big) = \rho''(n). \tag{9}$$

Since (7) also yields

$$\begin{aligned} \Delta_n(\Phi_p) &= p && \text{for } p \nmid n, \quad \text{and} \\ \Delta_n(\Phi_{p^{k+1}}) &= p^{p^k} && \text{for } p^k \parallel n, \end{aligned} \tag{10}$$

we conclude that the inequality in (9) is sharp, that is,

$$\min_{\substack{m=1,2,\dots \\ \Delta_n(\Phi_m)\ge 2}} \Delta_n(\Phi_m) = \rho''(n). \tag{11}$$

Finally, since $\mathsf{m}_n(\Phi_m) = \frac{1}{n}\log\Delta_n(\Phi_m)$, the statement of the lemma follows by combining (6) and (11). $\square$

Lemma 2. *Let n satisfy $n \ne 6 \pmod{12}$ and $n \ne 0 \pmod{420}$. Then $\rho(n) = \rho'(n)$, that is, the least non-divisor of n is a prime (and not a prime power).*

Remark 3. The example given in Remark 1(i) shows that the implication of Lemma 2 cannot be reversed.

Proof of Lemma 2. Suppose that $n \neq 6 \pmod{12}$ and $\rho'(n) < \rho(n)$; we verify that it implies $420 \mid n$. First, if $6 \nmid n$, then either $\rho'(n) = \rho(n) = 2$ or $\rho'(n) = \rho(n) = 3$. This contradicts the assumption $\rho'(n) < \rho(n)$. Hence, we have $n = 6k$, for some k. The case k odd is excluded by the assumption $n \neq 6 \pmod{12}$, so we obtain k even. In other words, $n = 12k'$, for some k'. If $5 \nmid k'$, then we have $\rho'(n) = \rho(n) = 5$, in contradiction to the assumption $\rho'(n) < \rho(n)$. Therefore, we have $n = 60k''$, for some k''. Finally, if $7 \nmid k''$, then $\rho'(n) = \rho(n) = 7$, again in contradiction to $\rho'(n) < \rho(n)$. Thus we conclude that $n = 420k'''$, for some k'''. □

Proof of Theorem 1.

STEP I: First notice that indeed $\lambda_n = \frac{1}{n}\log\Lambda_n$ for an integer $\Lambda_n \geq 2$; in fact,

$$\Lambda_n = \min_{\substack{f\in\mathbb{Z}[x] \\ |\Delta_n(f)|\geq 2}} |\Delta_n(f)|. \tag{12}$$

Therefore, $\Lambda_n = |\Delta_n(f_0)|$, for some $f_0 \in \mathbb{Z}[x]$ with $\deg f_0 = n-1$. Upon replacing f_0 with $f_0^{\vee}$ defined above, if necessary, we can assume that $\Lambda_n = \Delta_n(f_0)$.

STEP II: We show that $\Lambda_n \nmid n$. Suppose that Λ_n divides n. Then there exists a prime p dividing both Λ_n and n. Let $p^m \parallel \Lambda_n$ and $p^k \parallel n$. Since $\Lambda_n \mid n$ we notice that $m \leq k$. On the other hand, let C_a be the $n\times n$ integer circulant matrix whose first row consists of the coefficients of f_0, so that

$$\Lambda_n = \Delta_n(f_0) = \det C_a. \tag{13}$$

Then we have $p^k \parallel n$ and $p^m \parallel \det C_a$, and a result by Newman [12, Theorem 2] thus implies that $m \geq k+1$, so we obtain a contradiction.

STEP III: The previous step yields that the positive integer Λ_n does not divide n. By definition, $\rho'(n)$ is the smallest number with this property. We thus obtain the lower bound $\rho'(n) \leq \Lambda_n$.

STEP IV: The upper bound $\Lambda_n \leq \rho''(n)$ is a consequence of Lemma 1.

STEP V: Suppose that $n = 6 \pmod{12}$. Then $2 \mid n$ and $3 \mid n$, while $4 \nmid n$. Hence, $\rho'(n) = 4$. On the other hand,

$$\min_{p^k\parallel n} p^{p^k} = 2^{2^1} = 4, \tag{14}$$

and thus $\rho''(n) = 4$; notice that $\rho(n) \geq 5$. Therefore in Theorem 1 the lower and upper bound coincide, and we obtain $\Lambda_n = \rho'(n) = \rho''(n) = 4$.

STEP VI: Suppose that $n \neq 6 \pmod{12}$ and $n \neq 0 \pmod{420}$. By Lemma 2 these conditions on n imply that $\rho(n) = \rho'(n)$. Since always $\rho'(n) \leq \rho''(n) \leq \rho(n)$, we conclude that $\rho'(n) = \rho''(n)$, Thus the lower and upper bound in Theorem 1 coincide and we obtain $\Lambda_n = \rho'(n) = \rho''(n)$. □

References

[1] T. M. Apostol, *Resultants of cyclotomic polynomials*, Proc. Amer. Math. Soc. 24 (1970), 457–462.

[2] P. Borwein, E. Dobrowolski, and M. J. Mossinghoff, *Lehmer's problem for polynomials with odd coefficients*, Ann. of Math. 166 (2007), 347–366.

[3] D. W. Boyd, *Mahler's measure and special values of L-functions*, Experiment. Math. 7 (1998), 37–82.

[4] C. C. Cheng, J. H. McKay, and S. S.-S. Wang, *Resultants of cyclotomic polynomials*, Proc. Amer. Math. Soc. 123 (1995), 1053–1059.

[5] J. E. Cremona, *Unimodular integer circulants*, Math. Comp. 77 (2008), 1639–1652.

[6] M. Einsiedler, G. Everest, and T. Ward, *Primes in sequences associated to polynomials (after Lehmer)*, LMS J. Comput. Math. 3 (2000), 125–139.

[7] G. Everest, P. Rogers, and T. Ward, *A higher-rank Mersenne problem*, in: Algorithmic Number Theory, W. L. Mang, C. Fieker, and D. R. Kohel (eds.), Springer, Berlin, 2002, 95–107.

[8] A. Flatters, *Primitive divisors of some Lehmer-Pierce sequences*, J. Number Theory 129 (2009), 209–219.

[9] C. J. Hillar and L. Levine, *Polynomial recurrences and cyclic resultants*, Proc. Amer. Math. Soc. 135 (2007), 1607–1618.

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

[11] D. Lind, *Lehmer's problem for compact abelian groups*, Proc. Amer. Math. Soc. 133 (2005), 1411–1416.

[12] M. Newman, *On a problem suggested by Olga Taussky-Todd*, Illinois J. Math. 24 (1980), 156–158.

[13] T. A. Pierce, *The numerical factors of the arithmetic forms* $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$, Ann. of Math. 18 (1916), 53–64.

[14] C. Smyth, *The Mahler measure of algebraic numbers: a survey*, in: Number Theory and Polynomials, J. McKee and C. Smyth (eds.), Cambridge Univ. Press, 2008, 322–349.

Faculty of Mathematics
University of Vienna
Nordbergstraße 15
1090 Vienna, Austria
E-mail: norbert.kaiblinger@univie.ac.at