The Lind–Lehmer Constant for cyclic groups of order less than 892,371,480

Vincent Pigno · Christopher Pinner

Published Version Information

Citation: Pigno, V., & Pinner, C. (2014). The Lind-Lehmer Constant for cyclic groups of order less than 892,371,480. *Ramanujan Journal*, 33(2), 295-300.

Digital Object Identifier (DOI): 10.1007/s11139-012-9443-1

Publisher's Link: http://link.springer.com/article/10.1007/s11139-012-9443-1

THE LIND-LEHMER CONSTANT FOR CYCLIC GROUPS OF ORDER LESS THAN 892, 371, 480.

VINCENT PIGNO AND CHRISTOPHER PINNER

Abstract. We determine the Lind Lehmer constant for the cyclic group $\mathbb{Z}_n$ when n is not a multiple of $892,371,480 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23$.

1. Introduction

In [4] Lind introduced the concept of Mahler measure and Lehmer constant for arbitrary compact abelian groups, with the classical Mahler measure and Lehmer problem corresponding to the group $\mathbb{R}/\mathbb{Z}$. In [1] the constant was determined for the groups $\mathbb{Z}_p^k$. Here we consider cyclic groups. We write $\mathbb{Z}_n$ for $\mathbb{Z}/n\mathbb{Z}$. For a polynomial F in $\mathbb{Z}[x]$ one can define its *logarithmic Mahler measure over* $\mathbb{Z}_n$ as

$$m_n(F) := \frac{1}{n} \log |M_n(F)|$$

where

$$M_n(F) := \prod_{j=1}^{n} F(w_n^j), \quad w_n := e^{2\pi i/n}.$$

The Lind-Lehmer constant for $\mathbb{Z}_n$ then corresponds to the smallest non-zero measure over $\mathbb{Z}_n$

$$\lambda(\mathbb{Z}_n) := \frac{1}{n} \log \mathscr{M}_n$$

where

$$\mathscr{M}_n := \min\{|M_n(F)| \ : \ F \in \mathbb{Z}[x], \ \ |M_n(F)| > 1\}.$$

Lind showed that

$$\mathscr{M}_n = 2 \text{ if } n \text{ is odd}.$$

Kaiblinger [2] obtained the bounds

$$\rho_1(n) \leq \mathscr{M}_n \leq \rho_2(n)$$

where

$$\rho_2(n) = \min\left\{\min_{p \nmid n} p, \min_{p^\alpha || n} p^{p^\alpha}\right\},$$

and

$$\rho_1(n) = \min\left\{\min_{p \nmid n} p, \min_{p^\alpha || n} p^{\alpha+1}\right\}.$$

Date: April 4, 2014.

1991 *Mathematics Subject Classification.* Primary: 11R06, 11R09; Secondary: 11B83, 11C08, 11G50, 11T22.

Key words and phrases. Mahler measure, Lind's Lehmer Problem, finite abelian groups .

Equality in these upper and lower bounds immediately gives:

$$\begin{aligned}
\mathscr{M}_n &= 3 \text{ if } n = 2m,\ 3 \nmid m,\\
\mathscr{M}_n &= 4 \text{ if } n = 2 \cdot 3m,\ 2 \nmid m,\\
\mathscr{M}_n &= 5 \text{ if } n = 2^2 \cdot 3m,\ 5 \nmid m,\\
\mathscr{M}_n &= 7 \text{ if } n = 2^2 \cdot 3 \cdot 5m,\ 7 \nmid m.
\end{aligned}$$

Kaiblinger's upper bound $\rho_2(n)$ is achievable, with $M_n(\Phi_{p^{\alpha+1}}) = p^{p^\alpha}$ if $p^\alpha || n$, $\alpha \geq 0$. Kaiblinger's lower bound $\rho_1(n)$ follows at once from his observation that if $p \mid M_n(F)$ with $p^\alpha || n$ then $p^{\alpha+1} \mid M_n(F)$. Kaiblinger proves this using a result of Newman [5] on determinants of circulant matrices but we give an independent proof of this in part (ii) of Lemma 2.1 below.

For the first undetermined value Kaiblinger's results show that $\mathscr{M}_{420} = 8, 9$ or 11. Here we are able to rule out $\mathscr{M}_n = 2^{\alpha+1}$ when $2^\alpha || n$, $\alpha \geq 2$ (see Lemma 3.1), or $3^{\alpha+1}$ if $3^\alpha || n$ when $12 \mid n$ (see Lemma 3.2), replacing the $2^{\alpha+1}$ and $3^{\alpha+1}$ in Kaiblinger's lower bound by $2^{\alpha+2}$ and $3^{\alpha+2}$ when $12 \mid n$. With this we immediately extend the list of known $\mathscr{M}_n$.

Theorem 1.1.

$$\begin{aligned}
\mathscr{M}_n &= 11 \ \textit{if}\ n = 2^2 \cdot 3 \cdot 5 \cdot 7m,\ 11 \nmid m,\\
\mathscr{M}_n &= 13 \ \textit{if}\ n = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11m,\ 13 \nmid m,\\
\mathscr{M}_n &= 16 \ \textit{if}\ n = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13m,\ 2 \nmid m,\\
\mathscr{M}_n &= 17 \ \textit{if}\ n = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13m,\ 17 \nmid m,\\
\mathscr{M}_n &= 19 \ \textit{if}\ n = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17m,\ 19 \nmid m,\\
\mathscr{M}_n &= 23 \ \textit{if}\ n = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19m,\ 23 \nmid m.
\end{aligned}$$

The first unresolved case now becomes $\mathscr{M}_{2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23} = 25$ or 27.

2. Preliminaries

The value of $M_n(F)$ can be written as a resultant

$$M_n(F) = \operatorname{Res}(x^n - 1, F)$$

and, using $\Phi_n(x)$ to denote the nth cyclotomic polynomial, plainly

$$M_n(F) = \prod_{d \mid n} T_d(F)$$

where the integers

$$T_d(F) := \operatorname{Res}(\Phi_d, F) = \prod_{\substack{j=1\\(j,d)=1}}^{d} F(w_d^j).$$

Observing that when $(r, s) = 1$ the rs-th primitive roots of unity are exactly the products of the primitive r-th and s-th roots of unity one can write

$$T_{rs}(F) = T_r(G), \quad G(x) := \prod_{\substack{j=1\\(j,s)=1}}^{s} F(w_s^j x), \tag{2.1}$$

with of course $G(x)$ in $\mathbb{Z}[x]$ when $F(x)$ is in $\mathbb{Z}[x]$.

We observe the following congruence relation, similar to Lemma 5.4 of Kaiblinger [3]:

Lemma 2.1. *(i) If $(r, p) = 1$ then for any j in $\mathbb{N}$*

$$T_{rp^j}(F) \equiv T_r(F)^{\phi(p^j)} \ \textit{mod}\ p.$$

In particular

$$T_{rp^j}(F) \equiv \begin{cases} 0 \ mod \ p, & if \ p \mid T_r(F), \\ 1 \ mod \ p, & otherwise. \end{cases}$$

(ii) If $p \mid M_n(F)$ and $p^\alpha || n$, $\alpha > 0$ then $p^{\alpha+1} \mid M_n(F)$.

Proof. (i) In view of (2.1) we can assume without loss of generality that $r = 1$. Writing $\pi = 1 - w_{p^j}$ we have

$$F(w_{p^j}^i) = F((1-\pi)^i) = F(1) + \pi u_i,$$

and hence

$$T_{p^j}(F) = F(1)^{\phi(p^j)} + \pi u,$$

for some u_i and u in $\mathbb{Z}[w_{p^j}]$. Taking $|x|_p$ to be the extension of the p-adic absolute value to $\mathbb{Q}(w_{p^j})$ we have $|\pi|_p = p^{-1/\phi(p^j)} < 1$ giving $\left|T_{p^j}(F) - F(1)^{\phi(p^j)}\right|_p < 1$. But $T_{p^j}(F)$ and $F(1)^{\phi(p^j)}$ are integers and so $T_{p^j}(F) \equiv F(1)^{\phi(p^j)} \bmod p$.

(ii) If $p \mid M_n(F)$ and $p^\alpha || n$, $\alpha > 0$ then $p \mid T_{rp^j}(F)$ some $rp^j | n$, $(r,p) = 1$, $j \leq \alpha$, and so by (i) the $p \mid T_{rp^i}$, $0 \leq i \leq \alpha$ and $p^{\alpha+1} \mid M_n(F)$. □

3. Key Lemmas

We rule out $|M_n(F)| = 8$ when $4 \mid n$, and more generally rule out $|M_n(F)| = 2^{\alpha+1}$ when $2^\alpha || n$, $\alpha \geq 2$, with the following Lemma:

Lemma 3.1. *(i) If $2 \mid T_r(F)$, $(r,2) = 1$, then $16 \mid T_r(F)T_{2r}(F)T_{4r}(F)$*

(ii) If $2 \mid M_n(F)$, $2^\alpha || n$, $\alpha \geq 2$ then $2^{\alpha+2} \mid M_n(F)$.

Proof. (i) From (2.1) we assume again that $r = 1$ and $2 \mid T_1(F)$. Writing $F(x) = \sum_{i=0}^N a_i x^i$ and defining

$$A_j := \sum_{\substack{1 \leq i \leq N \\ i \equiv j \bmod 4}} a_i, \quad 0 \leq j \leq 3,$$

we have

$$T_1(F) = A_0 + A_1 + A_2 + A_3$$
$$T_2(F) = A_0 - A_1 + A_2 - A_3$$

and

$$\begin{aligned} T_4(F) &= (A_0 - A_2 + i(A_1 - A_3))(A_0 - A_2 - i(A_1 - A_3)) \\ &= (A_0 - A_2)^2 + (A_1 - A_3)^2. \end{aligned} \tag{3.1}$$

From Lemma 2.1 we know that $T_1(F), T_2(F)$ and $T_4(F)$ are all even. If $2 || T_4(F)$ then $A_0 - A_2$ and $A_1 - A_3$ (and hence $A_0 + A_2$ and $A_1 + A_3$) are both odd. If $A_0 + A_2$ and $A_1 + A_3$ are both 1 mod 4 or both 3 mod 4 then $4 \mid T_2(F) = (A_0 + A_2) - (A_1 + A_3)$. Otherwise $4 \mid T_1 = (A_0 + A_2) + (A_1 + A_3)$. Hence in all cases $2 \cdot 2 \cdot 4 \mid T_1(F)T_2(F)T_4(F)$.

(ii) If $2 \mid M_n(F)$, $2^\alpha || n$, $\alpha \geq 2$ then $2 \mid T_r(F)$ some $(r,2) = 1$ and $16 \mid T_r(F)T_{2r}(F)T_{4r}(F)$, with $2 \mid T_{2^i r}(F)$ for any $2 < i \leq \alpha$, and $2^{\alpha+2} \mid M_n$. □

Finally we also rule out $|M_n(F)| = 9$ for $12 \mid n$, and more generally rule out $|M_n(F)| = 3^{\alpha+1}$ when $12 \mid n$ with $3^\alpha || n$.

Lemma 3.2. *(i) $T_{4r}(F)$ is a sum of two squares. In particular if $p \equiv 3 \bmod 4$ and $p^\beta || T_{4r}(F)$ then β is even.*

(ii) If $T_r(F) = \pm 3$ then $r = 1$ or 2.

(iii) If $3 \mid T_r(F)$ or $T_{2r}(F)$ for some $(r,6) = 1$ then $T_{3r}(F)T_{4r}(F)T_{6r}(F)T_{12r}(F) \neq 3$.

(iv) If $12 \mid n$, $3^\alpha || n$ and $3 \mid M_n(F)$ then $|M_n(F)| \geq 3^{\alpha+2}$.

Proof. (i) From (2.1) it is enough to show that $T_{2^i}(F)$ is the sum of two squares for any $i \geq 2$. We write $F(x) = \sum_{k=0}^{\infty} a_k x^k$. For $T_4(F)$ the claim follows from (3.1) and any $T_{2^i}(F)$ with $i > 2$ can be reduced to a $T_4(F_0)$ for some F_0, since for $i \geq 2$

$$\begin{aligned} T_{2^i}(F) &= \prod_{\substack{1 \leq j \leq 2^i \\ j \text{ odd}}} F(w_{2^i}^j) = \prod_{\substack{1 \leq j \leq 2^{i-1} \\ j \text{ odd}}} F(w_{2^i}^j) F(-w_{2^i}^j) \\ &= \prod_{\substack{1 \leq j \leq 2^{i-1} \\ j \text{ odd}}} \left(\sum_{k=0}^{\infty} a_{2k} w_{2^{i-1}}^{jk} \right)^2 - w_{2^{i-1}}^j \left(\sum_{k=0}^{\infty} a_{2k+1} w_{2^{i-1}}^{jk} \right)^2 = T_{2^{i-1}}(H) \end{aligned}$$

where $H(x) = \left(\sum_{k=0}^{\infty} a_{2k} x^k\right)^2 - x \left(\sum_{k=0}^{\infty} a_{2k+1} x^k\right)^2$.

(ii) If $T_r(F) = \pm 3$, $(r, 3) = 1$ and $p \mid r$ then by Lemma 2.1(i) we have $\pm 3 \equiv 1 \bmod p$ and $p = 2$. By part (i) we know $2^2 \nmid r$ so $r = 1$ or 2.

(iii) From (2.1) we assume $r = 1$ and, replacing $F(x)$ by $F(-x)$ if necessary, that $3 \mid T_1(F)$. By Lemma 2.1 we have $3 \mid T_3(F)$ so $T_3(F)T_4(F)T_6(F)T_{12}(F) = 3$ can only happen if

$$T_3(F) = 3, \;\; T_4(F) = 1, \;\; T_6(F) = 1, \;\; T_{12}(F) = 1.$$

Writing $w = w_3$ and $\pi = 1 - w$ we work in $\mathbb{Z}[w]$. Observing that the norm $N(a + bw) = (a+bw)(a+bw^2) = a^2 - ab + b^2 = \frac{1}{4}\left((2a - b)^2 + 3b^2\right)$ it is readily seen that the only units in $\mathbb{Z}[w]$ are $\pm 1, \pm w, \pm(1+w)$, and only elements of norm 3 are $\pm(1-w)$, $\pm(2+w)$, $\pm(1+2w)$. Observe that $F(iw)F(-iw)$ is in $\mathbb{Z}[w]$. Since $T_{12}(F) = F(iw)F(-iw)F(iw^2)F(-iw^2) = 1$ plainly $F(iw)F(-iw)$ must be a unit, $\pm 1, \pm w, \pm(1 + w)$, since further

$$F(iw)F(-iw) = F(i - i\pi)F(-i + i\pi) \equiv F(i)F(-i) = T_4(F) = 1 \bmod \pi$$

we must have $F(iw)F(-iw) = 1, w$ or $-(1 + w)$. Writing

$$F(x) = \sum_{l=0}^{N} a_l x^l, \quad A_j = \sum_{\substack{l=0 \\ l \equiv j \bmod 4}}^{N} a_l w^l, \;\; 0 \leq j \leq 3,$$

we have

$$F(w) = A_0 + A_1 + A_2 + A_3, \qquad F(-w) = A_0 - A_1 + A_2 - A_3,$$

and

$$\begin{aligned} F(iw)F(-iw) = (A_0 - A_2)^2 + (A_1 - A_3)^2 &= \frac{1}{2}\left(F(w)^2 + F(-w)^2\right) - 4A_0A_2 - 4A_1A_3 \\ &\equiv \frac{1}{2}\left(F(w)^2 + F(-w)^2\right) \bmod 4. \end{aligned}$$

As $T_3(F) = 3$, $T_6(F) = 1$ plainly $F(w)$ has norm 3 and $F(-w)$ is a unit, but in addition $F(w) \equiv F(-w) \bmod 2$. Thus we have the twelve possibilities

$$(F(w), F(-w)) = (\pm(1 - w), \pm(1 + w)) \quad \text{or} \quad (\pm(2 + w), \pm w) \quad \text{or} \quad (\pm(1 + 2w), \pm 1),$$

giving respectively

$$\frac{1}{2}\left(F(w)^2 + F(-w)^2\right) = -w \;\; \text{or} \;\; 1 + w \;\; \text{or} \;\; -1.$$

But none of these are $\equiv 1, w$ or $-(1 + w) \bmod 4$.

(iv) If $12 \mid n$ with $3^\alpha || n$ and $3 \mid M_n(F)$ then $3 \mid T_r(F)$ some $(r, 3) = 1$ and $3 \mid T_{r3^j}(F)$, $0 \leq j \leq \alpha$ giving $3^{\alpha+1} \mid M_n(F)$. But $|M_n(F)| = 3^{\alpha+1}$ would require $|T_r(F)| = 3$, which by (ii) forces $r = 1$ or 2 and (iii) gives $T_3(F)T_4(F)T_6(F)T_{12}(F) \neq 3$. So we must pick up at least one extra prime and $3^{\alpha+2} \mid M_n(F)$ or $16 \cdot 3^{\alpha+1} \mid M_n(F)$ or $p^{\beta+1}3^{\alpha+1} \mid M_n(F)$ for some $p^\beta || n$, $\beta \geq 0$, $p \geq 5$, and $|M_n(F)| \geq 3^{\alpha+2}$.

∎

References

[1] D. DeSilva & C. G. Pinner, *The Lind-Lehmer constant for* $\mathbb{Z}_p^n$, Proc. AMS to appear.
[2] N. Kaiblinger, *On the Lehmer constant of finite cyclic groups*, Acta Arith. **142** (2010), no. 1, 79-84.
[3] N. Kaiblinger, *Progress on Olga Taussky-Todd's circulant problem*, Ramanujan J. **28** (2012), no. 1, 45-60.
[4] D. Lind, *Lehmer's problem for compact abelian groups*, Proc. Amer. Math. Soc. **133** (2005), 1411-1416.
[5] M. Newman, *On a problem suggested by Olga Taussky-Todd*, Illinois J. Math. **24** (1980), no. 1, 156-158.

Department of Mathematics, Kansas State University, Manhattan, KS 66506
E-mail address: pignovmath.ksu.edu

Department of Mathematics, Kansas State University, Manhattan, KS 66506
E-mail address: pinner@math.ksu.edu