PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 142, Number 6, June 2014, Pages 1935–1941
S 0002-9939(2014)11954-X
Article electronically published on February 26, 2014

THE LIND LEHMER CONSTANT FOR $\mathbb{Z}_p^n$

DILUM DESILVA AND CHRISTOPHER PINNER

(Communicated by Matthew A. Papanikolas)

ABSTRACT. We determine the Lind Lehmer constant for groups of the form $\mathbb{Z}_p^n$.

1. INTRODUCTION

Let G be a compact abelian group with normalized Haar measure μ and dual group of multiplicative characters $\hat{G}$. For f in $\mathbb{Z}[\hat{G}]$, the ring of integral combinations of characters, Lind [6] defines a logarithmic Mahler measure of f over G,

$$m(f) = m_G(f) = \int_G \log |f| d\mu,$$

and an associated Lehmer constant for G,

$$\lambda(G) = \inf \left\{ m_G(f) \ : \ f \in \mathbb{Z}[\hat{G}],\ m_G(f) > 0 \right\}.$$

The usual Mahler measure and Lehmer Problem thus correspond to taking $G = \mathbb{R}/\mathbb{Z}$.

Here we shall be concerned with finite abelian groups. We shall write $\mathbb{Z}_n$ for the cyclic groups $\mathbb{Z}/n\mathbb{Z}$. In [6] Lind shows that for odd n,

$$\lambda(\mathbb{Z}_n) = \frac{1}{n} \log 2,$$

that

$$\lambda(\mathbb{Z}_2) = \frac{1}{2} \log 3, \qquad \lambda(\mathbb{Z}_2^2) = \frac{1}{4} \log 3,$$

and conjectures from numerical evidence that for all $n \geq 2$,

$$\lambda(\mathbb{Z}_2^n) = \frac{1}{2^n} \log(2^n - 1). \tag{1.1}$$

Further values of $\lambda(\mathbb{Z}_n)$, for example when $420 \nmid n$, are obtained in [2]. Here we determine the value of $\lambda(\mathbb{Z}_p^n)$ for any prime p. In particular we verify Lind's $p = 2$ conjecture (1.1).

Theorem 1.1. *For $n \geq 2$,*

$$\lambda(\mathbb{Z}_2^n) = \frac{1}{2^n} \log(2^n - 1).$$

Received by the editors March 30, 2012 and, in revised form, July 10, 2012.
2010 *Mathematics Subject Classification.* Primary 11R06, 11R09; Secondary 11B83, 11C08, 11G50, 11T22.
Key words and phrases. Mahler measure, Lind's Lehmer Problem, finite abelian groups.

For all $n \geq 1$,

$$\lambda(\mathbb{Z}_3^n) = \frac{1}{3^n} \log(3^n - 1),$$

and for any prime $p \geq 5$,

$$\lambda(\mathbb{Z}_p^n) = \frac{1}{p^n} \log \mathscr{M}_n,$$

with

$$\mathscr{M}_n = \min\{a^{p^{n-1}} \mod p^n \ : \ 2 \leq a \leq p-2\},$$

where the $a^{p^{n-1}} \bmod p^n$ *in the definition of* $\mathscr{M}_n$ *indicates the least positive residue.*

Note that the case $p = 3$ can be combined with $p \geq 5$ if one takes $2 \leq a \leq p-1$ in the definition of $\mathscr{M}_n$. It is not hard to see that the $a^{p^{n-1}} \bmod p^n$, $1 \leq a \leq p-1$, are exactly the $p-1$ solutions to

$$x^{p-1} \equiv 1 \mod p^n. \tag{1.2}$$

Thus $\mathscr{M}_n$ can be equivalently defined as the smallest non-trivial positive integer solution to (1.2). In particular we have $\lambda(\mathbb{Z}_p^2) = \frac{1}{p^2} \log 2$ if and only if p is a Wieferich prime.

2. Lemmas

If $G = \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$, then the characters on G take the form

$$\chi_{r_1,...,r_n}(u_1, ..., u_n) = \exp(2\pi i r_1 u_1/m_1) \cdots \exp(2\pi i r_n u_n/m_n)$$

with $0 \leq r_1 \leq m_1 - 1$,..., $0 \leq r_n \leq m_n - 1$. For an

$$f(u_1, ..., u_n) = \sum_{0 \leq r_1 \leq m_1 - 1} \cdots \sum_{0 \leq r_n \leq m_n - 1} a(r_1, ..., r_n) \chi_{r_1,...,r_n}(u_1, ..., u_n)$$

in $\mathbb{Z}[\hat{G}]$ we have

$$m_G(f) = \frac{1}{m_1 \cdots m_n} \log |M(F)|,$$

where

$$F(x_1, ..., x_n) = \sum_{0 \leq r_1 \leq m_1 - 1} \cdots \sum_{0 \leq r_n \leq m_n - 1} a(r_1, ..., r_n) x_1^{r_1} \cdots x_n^{r_n} \in \mathbb{Z}[x_1, ..., x_n]$$

and

$$M(F) = \prod_{j_1=0}^{m_1-1} \cdots \prod_{j_n=0}^{m_n-1} F\left(w_1^{j_1}, ..., w_n^{j_n}\right), \quad w_1 = \exp(2\pi i/m_1), ..., w_n = \exp(2\pi i/m_n).$$

Thus if $G = \mathbb{Z}_p^n$, writing

$$w = \exp(2\pi i/p),$$

we just need to consider the values of

$$M_n(F) = \prod_{j_1=0}^{p-1} \cdots \prod_{j_n=0}^{p-1} F\left(w^{j_1}, ..., w^{j_n}\right),$$

for $F(x_1, ..., x_n) \in \mathbb{Z}[x_1, ..., x_n]$.

Note that one can write

$$M_n(F) = F(1, ..., 1) \prod_{i=1}^{I} N_i, \qquad I = \frac{p^n - 1}{p - 1}, \tag{2.1}$$

where the integers $N_1, ..., N_I$ are norms of the type

$$N(F(w^{j_1}, ..., w^{j_n})) = \prod_{l=1}^{p-1} F(w^{j_1 l}, ..., w^{j_n l}) \tag{2.2}$$

for a suitable choice of I values $\vec{j} = (j_1, ..., j_n)$ (for example, one could take all $\vec{j}$ of the form $(1, j_2, \ldots, j_n)$, $(0, 1, j_3, \ldots, j_n)$,...,$(0, \ldots, 0, 1)$ with $0 \leq j_2, \ldots, j_n < p$).

When $n = 1$ the measure can be expressed as a resultant,

$$M_1(F) = \mathrm{Res}(x^p - 1, F) = F(1)\mathrm{Res}(\Phi(x), F),$$

where

$$\Phi(x) = 1 + x + \cdots + x^{p-1}$$

is the pth cyclotomic polynomial. Lemma 5.4(ii) of Kaiblinger [3] then gives the congruence restriction

$$M_1(F) \equiv F(1) \bmod p.$$

The following lemma generalizes this to arbitrary n.

Lemma 2.1. *For $F \in \mathbb{Z}[x_1, ..., x_n]$,*

$$M_n(F) \equiv F(1, ..., 1)^{p^{n-1}} \mod p^n.$$

Proof. We use induction on the dimension n.

For $n = 1$, writing $\pi = 1 - w$ we have $F(w^j) \equiv F(1) \bmod \pi$ and

$$M_1(F) = \prod_{j=0}^{p-1} F(w^j) \equiv F(1)^p \bmod \pi.$$

Hence, since $M_1(F)$ and $F(1)^p$ are in $\mathbb{Z}$ and $|\pi|_p = p^{-\frac{1}{p-1}} < 1$, where $|\ |_p$ denotes the extension of the usual p-adic absolute value to $\mathbb{Q}(w)$, we have

$$M_1(F) \equiv F(1)^p \equiv F(1) \bmod p.$$

Setting

$$\begin{aligned} G(x_1, ..., x_n) &= \prod_{i_1=0}^{p-1} \cdots \prod_{i_n=0}^{p-1} F\left(x_1^{i_1}, ..., x_n^{i_n}\right) \\ &\equiv \sum_{0 \leq l_1 < p} \cdots \sum_{0 \leq l_n < p} a(l_1, ..., l_n) x_1^{l_1} \cdots x_n^{l_n} \mod \langle x_1^p - 1, ..., x_n^p - 1\rangle, \end{aligned}$$

for some $a(l_1, ..., l_n)$ in $\mathbb{Z}$, we consider

$$\begin{aligned} S &= \sum_{j_1=0}^{p-1} \cdots \sum_{j_n=0}^{p-1} G\left(w^{j_1}, ..., w^{j_n}\right) \\ &= \sum_{0 \leq l_1 < p} \cdots \sum_{0 \leq l_n < p} a(l_1, ..., l_n) \sum_{j_1=0}^{p-1} \cdots \sum_{j_n=0}^{p-1} w^{j_1 l_1} \cdots w^{j_n l_n}. \end{aligned}$$

Observing that $\sum_{j=0}^{p-1} w^{lj}$ equals 0 if $0 < l < p$ and equals p if $l = 0$, we see that

$$S = p^n a(0, ..., 0) \equiv 0 \bmod p^n.$$

Now if $j_1 \neq 0, ..., j_n \neq 0$ we have

$$G\left(w^{j_1}, ..., w^{j_n}\right) = M_n(F).$$

If exactly L of the $j_i = 0$ for some $1 \leq L < n$, say $j_1 = \cdots = j_L = 0$, $j_{L+1} \neq 0, ..., j_n \neq 0$, we have

$$G(1, ..., 1, w^{j_{L+1}}, ..., w^{j_n}) = M_{n-L}(F(1, ..., 1, x_{L+1}, ..., x_n))^{p^L}.$$

By the induction hypothesis,

$$M_{n-L}(F(1, ..., 1, x_{L+1}, ..., x_n)) = F(1, ..., 1)^{p^{n-L-1}} + kp^{n-L}$$

for some integer k, and so

$$\begin{aligned} G(1, ..., 1, w^{j_{L+1}}, ..., w^{j_n}) &= (F(1, ..., 1)^{p^{n-L-1}} + kp^{n-L})^{p^L} \\ &\equiv F(1, ..., 1)^{p^{n-1}} \bmod p^n. \end{aligned}$$

If $j_1 = \cdots = j_n = 0$, we have by Euler's Theorem,

$$G(1, ..., 1) = F(1, ..., 1)^{p^n} \equiv F(1, ..., 1)^{p^{n-1}} \bmod p^n.$$

Thus

$$0 \equiv S \equiv (p-1)^n M_n(F) + (p^n - (p-1)^n) F(1, ..., 1)^{p^{n-1}} \bmod p^n$$

and $M_n(F) \equiv F(1, ..., 1)^{p^{n-1}} \bmod p^n$. $\square$

Thus the only values achievable as $M_n(F)$ are the p^{n-1}th powers mod p^n. It remains to show in the following lemma that all integers of this type that are coprime to p can be achieved as measures. For $n = 1$ the resultant $M_1(F)$ will be a circulant determinant (see for example [2]) and the result of the lemma follows from a core result on integer circulant determinants obtained independently by Laquer [5, Theorem 4] and Newman [7, Theorem 1].

Lemma 2.2. *For any integers k and a with $p \nmid a$, $a > 0$, there exists a polynomial $F(x_1, ..., x_n)$ in $\mathbb{Z}[x_1, ..., x_n]$ with*

$$M_n(F) = a^{p^{n-1}} - kp^n.$$

Proof. The proof is entirely constructive. Suppose that p is odd. We begin by generating a sequence $H_1(x), ..., H_{n-1}(x)$ in $\mathbb{Z}[x]$ satisfying

$$(1 + x + \cdots + x^{a-1})^{p^l} \equiv a^{p^{l-1}} + p^l H_l(x) \bmod x^p - 1,$$

$l = 1, ..., n-1$. First noting that

$$(1 + x + \cdots + x^{a-1})^p \equiv 1 + x^p + \cdots + x^{p(a-1)} \bmod p,$$

we have

$$(1 + x + \cdots + x^{a-1})^p = 1 + x^p + \cdots + x^{p(a-1)} + pH_1(x) \equiv a + pH_1(x) \bmod x^p - 1$$

for some polynomial $H_1(x)$ in $\mathbb{Z}[x]$. Raising to pth powers we obtain an $H_2(x)$ in $\mathbb{Z}[x]$:

$$\begin{aligned} (1 + x + \cdots + x^{a-1})^{p^2} &\equiv (a + pH_1(x))^p \\ &\equiv a^p + p^2 H_2(x) \bmod x^p - 1 \end{aligned}$$

and successively the remaining $H_i(x)$ in $\mathbb{Z}[x]$:

$$\begin{aligned} (1 + x + \cdots + x^{a-1})^{p^{j+1}} &\equiv (a^{p^{j-1}} + p^j H_j(x))^p \\ &\equiv a^{p^j} + p^{j+1} H_{j+1}(x) \bmod x^p - 1. \end{aligned}$$

Thus

$$a^{p^{l-1}} + p^l H_l(1) = a^{p^l}, \tag{2.3}$$

and for a primitive pth root of unity w_1,

$$a^{p^{l-1}} + p^l H_l(w_1) = (1 + w_1 + \cdots + w_1^{a-1})^{p^l}. \tag{2.4}$$

Set

$$F(x_1, ..., x_n) = (1 + x_1 + \cdots + x_1^{a-1}) + \sum_{j=1}^{n-1} H_j(x_{j+1}) \prod_{i=1}^{j} \Phi(x_i) - k \prod_{i=1}^{n} \Phi(x_i),$$

where $\Phi(x)$ is the pth cyclotomic polynomial. Now if w_1 is a primitive pth root of unity, then

$$F(w_1, x_2, ..., x_n) = 1 + w_1 + \cdots + w_1^{a-1}$$

for any choice of $x_2, ..., x_n$, while if $x_1 = \cdots = x_l = 1$ but $x_{l+1} = w_1$, then by (2.3) and (2.4) we have

$$\begin{aligned} F(1, ..., 1, w_1, ...) &= a + pH_1(1) + \cdots + p^{l-1} H_{l-1}(1) + p^l H_l(w_1) = a^{p^{l-1}} + p^l H_l(w_1) \\ &= (1 + w_1 + \cdots + w_1^{a-1})^{p^l}. \end{aligned}$$

Finally, by (2.3),

$$F(1, ..., 1) = a + pH_1(1) + \cdots + p^{n-1} H_{n-1}(1) - kp^n = a^{p^{n-1}} - kp^n.$$

Observing that $1+w_1+\cdots+w_1^{a-1}$ is a unit of norm 1 for $p \nmid a$ (the norms of $1-w_1$ and $1-w_1^a$ are plainly equal), we see from (2.1) that $M_n(F) = F(1, ..., 1) = a^{p^{n-1}} - kp^n$ as required.

For $p = 2$ and a odd we have $a^{2^{n-1}} \equiv 1 \bmod 2^n$, and plainly any value of the form $1 - 2^n k$ can be achieved with $1 - k \prod_{i=1}^n (1 + x_i)$. $\square$

3. Proof of Theorem 1.1

Since the

$$F(w^{j_1 i}, ..., w^{j_n i}) \equiv F(1, ..., 1) \bmod \pi,$$

we observe that

$$N(F(w^{j_1}, ..., w^{j_n})) \equiv F(1, ..., 1)^{p-1} \bmod p.$$

Hence if $p \mid M_n(F)$ we must have $p \mid F(1, ..., 1)$ and $p \mid N_i$ for each of the $(p_n - 1)/(p - 1)$ norms in (2.1), and so $p^{\frac{p^n-1}{p-1}+1} \mid M_n(F)$. Thus from Lemmas 2.1 and 2.2 when $p \geq 3$ the spectrum of values of $|M_n(F)|$ less than $p^{\frac{p^n-1}{p-1}+1}$ will be exactly the positive integers that are congruent mod p^n to some p^{n-1}th power $a^{p^{n-1}}$ with $p \nmid a$. Thus for $p \geq 5$ the smallest value greater than 1 will be $\mathscr{M}_n$ as claimed. For $p = 3$ we see that the $a^{3^{n-1}} \equiv \pm 1 \bmod 3^n$ for $3 \nmid a$ and the values between 1 and $3^{(3^n+1)/2}$ are exactly the $3^n k \pm 1$, k in $\mathbb{N}$; in particular, $\lambda(\mathbb{Z}_3^n) = 3^{-n} \log(3^n - 1)$. Similarly, when $p = 2$ we have $a^{2^{n-1}} \equiv 1 \bmod 2^n$ for $2 \nmid a$, and the $|M_n(F)|$ between 1 and 2^{2^n} are exactly those of the form $2^n k + 1$, $2^n k - 1$, k in $\mathbb{N}$; in particular, $\lambda(\mathbb{Z}_2^n) = 2^{-n} \log(2^n - 1)$.

4. Sample $\mathscr{M}_n$ values for small p and n

We give the smallest non-trivial positive solution to $x^{p-1} \equiv 1 \bmod p^n$, for $p < 100$ and $n \leq 6$.

	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$
$p = 3$	8	26	80	242	728
$p = 5$	7	57	182	1068	1068
$p = 7$	18	18	1047	1353	34967
$p = 11$	3	124	1963	27216	284995
$p = 13$	19	239	239	109193	861642
$p = 17$	38	158	4260	15541	390112
$p = 19$	28	333	2819	133140	333257
$p = 23$	28	42	19214	495081	2818778
$p = 29$	14	1215	2463	1115402	42137700
$p = 31$	115	513	15714	2754849	8078311
$p = 37$	18	691	51344	1353359	33518159
$p = 41$	51	1172	20677	649828	92331463
$p = 43$	19	3038	3038	3228564	21583010
$p = 47$	53	295	224444	2359835	138173066
$p = 53$	338	1468	189323	4694824	8202731
$p = 59$	53	2511	11550	7044514	390421192
$p = 61$	264	15458	397575	28538377	1006953931
$p = 67$	143	3859	201305	1111415	77622331
$p = 71$	11	6372	15384	77588426	270657300
$p = 73$	306	923	840838	16178110	5915704483
$p = 79$	31	1523	1372873	2553319	522911165
$p = 83$	99	5436	1576656	9571390	2507851273
$p = 89$	184	1148	278454	158485540	1329885769
$p = 97$	53	412	1721322	18664438	2789067613

See [4] for extensive data on small values of $\mathscr{M}_n$ (a table of the $\mathscr{M}_2 < 100$ for $p < 10^6$ can be found in [1]). The only cases of $\mathscr{M}_2 = 2$ with $p < 1.25 \times 10^{15}$ are $p = 1093$ and $p = 3511$.

Acknowledgements

The authors thank Todd Cochrane, Vincent Pigno, Craig Spencer and Ben Wiles for discussions and computations related to this paper. They also thank the referee for directing them to existing $n = 1$ results in the literature.

References

[1] J. Brillhart, J. Tonascia, and P. Weinberger, *On the Fermat quotient*, Computers in number theory (Proc. Sci. Res. Council Atlas Sympos. No. 2, Oxford, 1969), Academic Press, London, 1971, pp. 213–222. MR0314736 (47 #3288)

[2] Norbert Kaiblinger, *On the Lehmer constant of finite cyclic groups*, Acta Arith. **142** (2010), no. 1, 79–84, DOI 10.4064/aa142-1-7. MR2601051 (2011e:11171)

[3] Norbert Kaiblinger, *Progress on Olga Taussky-Todd's circulant problem*, Ramanujan J. **28** (2012), no. 1, 45–60, DOI 10.1007/s11139-011-9354-6. MR2914452

[4] Wilfrid Keller and Jörg Richstein, *Solutions of the congruence* $a^{p-1} \equiv 1 \pmod{p^r}$, Math. Comp. **74** (2005), no. 250, 927–936 (electronic), DOI 10.1090/S0025-5718-04-01666-7. MR2114655 (2005i:11004)

[5] H. Turner Laquer, *Values of circulants with integer entries*, A collection of manuscripts related to the Fibonacci sequence, Fibonacci Assoc., Santa Clara, Calif., 1980, pp. 212–217. MR624127 (82g:15011)

[6] Douglas Lind, *Lehmer's problem for compact abelian groups*, Proc. Amer. Math. Soc. **133** (2005), no. 5, 1411–1416 (electronic), DOI 10.1090/S0002-9939-04-07753-6. MR2111966 (2006a:43004)

[7] Morris Newman, *On a problem suggested by Olga Taussky-Todd*, Illinois J. Math. **24** (1980), no. 1, 156–158. MR550657 (81b:15016)

Department of Mathematics, Kansas State University, Manhattan, Kansas 66506
Current address: BGSU Firelands, One University Drive, Huron, Ohio 44839
E-mail address: `dilumd@gmail.com`

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