LIND-LEHMER CONSTANT FOR GROUPS OF THE FORM $\mathbb{Z}_p^n$

by

DILUM P. DE SILVA

B.S., University of Sri Jayewardenepura, Sri Lanka, 2008
M.S., Kansas State University, 2010

AN ABSTRACT OF A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas
2013

Abstract

For a polynomial $F = F(x) \in \mathbb{C}[x]$, the logarithmic Mahler measure of F is defined by

$$m(F) = \int_0^1 \log |F(e^{2\pi i x})| \, dx.$$

Lind viewed $[0,1]$ as the group $\mathbb{R}/\mathbb{Z}$ and extended the concept of the Mahler measure to arbitrary compact abelian groups. In this thesis we study the additive group $G := \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, where $\mathbb{Z}_p = \mathbb{Z}/(p)$. For $F \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ the logarithmic Lind-Mahler measure of F over G is given by

$$m_G(F) := \frac{1}{p^n} \sum_{j_1=0}^{p-1} \sum_{j_2=0}^{p-1} \cdots \sum_{j_n=0}^{p-1} \log |F(e^{2\pi i j_1/p}, e^{2\pi i j_2/p}, \ldots, e^{2\pi i j_n/p})|.$$

Analogous to the classic Lehmer problem one can ask what is the smallest nonzero Lind-Mahler measure, that is, what is the value of the Lind-Lehmer constant of G defined as follows:

$$\lambda(G) := \inf\{m_G(F) \mid F \in \mathbb{Z}[x_1, x_2, \ldots, x_n], m_G(F) > 0\}.$$

Lind found the Lind-Lehmer constant for many groups of the form $\mathbb{Z}_n$. Lind also conjectured the value of $\lambda(\mathbb{Z}_2^n)$. Here we verify the Lind conjecture and more generally evaluate $\lambda(\mathbb{Z}_p^n)$ for arbitrary primes p and $n \in \mathbb{N}$, obtaining for any $p \geq 3$,

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

where

$$\mathcal{M}_n := \min\{a^{p^{n-1}} (\bmod\ p^n) \mid 2 \leq a \leq p-1\}.$$

We will also show how bounds on $\mathcal{M}_n$ can be obtained from bounds on Heilbronn type exponential sums $H_{p^n}(y)$, where $H_{p^n}(y) := \sum_{x=0}^{p-1} e_{p^n}(y x^{p^{n-1}})$ with $e_{p^n}(x) := e^{2\pi i x/p^n}$.

LIND-LEHMER CONSTANT FOR GROUPS OF THE FORM $\mathbb{Z}_p^n$

by

DILUM P. DE SILVA

B.S., University of Sri Jayewardenepura, Sri Lanka, 2008
M.S., Kansas State University, 2010

A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas
2013

Approved by:

Co-Major Professor
Chris Pinner

Approved by:

Co-Major Professor
Todd Cochrane

Abstract

For a polynomial $F = F(x) \in \mathbb{C}[x]$, the logarithmic Mahler measure of F is defined by

$$m(F) = \int_0^1 \log |F(e^{2\pi i x})| \, dx.$$

Lind viewed $[0,1]$ as the group $\mathbb{R}/\mathbb{Z}$ and extended the concept of the Mahler measure to arbitrary compact abelian groups. In this thesis we study the additive group $G := \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p$, where $\mathbb{Z}_p = \mathbb{Z}/(p)$. For $F \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ the logarithmic Lind-Mahler measure of F over G is given by

$$m_G(F) := \frac{1}{p^n} \sum_{j_1=0}^{p-1} \sum_{j_2=0}^{p-1} \cdots \sum_{j_n=0}^{p-1} \log |F(e^{2\pi i j_1/p}, e^{2\pi i j_2/p}, ..., e^{2\pi i j_n/p})|.$$

Analogous to the classic Lehmer problem one can ask what is the smallest nonzero Lind-Mahler measure, that is, what is the value of the Lind-Lehmer constant of G defined as follows:

$$\lambda(G) := \inf\{m_G(F) \mid F \in \mathbb{Z}[x_1, x_2, \ldots, x_n], m_G(F) > 0\}.$$

Lind found the Lind-Lehmer constant for many groups of the form $\mathbb{Z}_n$. Lind also conjectured the value of $\lambda(\mathbb{Z}_2^n)$. Here we verify the Lind conjecture and more generally evaluate $\lambda(\mathbb{Z}_p^n)$ for arbitrary primes p and $n \in \mathbb{N}$, obtaining for any $p \geq 3$,

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

where

$$\mathcal{M}_n := \min\{a^{p^{n-1}} (\bmod\ p^n) \mid 2 \leq a \leq p-1\}.$$

We will also show how bounds on $\mathcal{M}_n$ can be obtained from bounds on Heilbronn type exponential sums $H_{p^n}(y)$, where $H_{p^n}(y) := \sum_{x=0}^{p-1} e_{p^n}(yx^{p^{n-1}})$ with $e_{p^n}(x) := e^{2\pi i x/p^n}$.

Table of Contents

List of Tables

Acknowledgments

Foremost, I would like to express my sincere gratitude to my advisers Professor Chris Pinner and Professor Todd Cochrane for their continuous support of my Ph.D. study and research, for their patience, motivation, enthusiasm, and immense knowledge. Their guidance helped me in all the time of research and writing of this thesis. I could not have imagined having better advisers and mentors for my Ph.D study.

Besides my advisers, I would like to thank the rest of my thesis committee: Professor Craig Spencer and Professor Bharat Ratra, for their encouragement, insightful comments, and hard questions.

I thank Vincent Pigno and Misty Long for the stimulating discussions, and for all the fun we have had in the last few years.

Last but not the least, I would like to thank my family: my mother Nirmala Warnakulasuriya and father the late Chandrasiri De Silva, for giving birth to me in the first place and supporting me spiritually throughout my life, and also my loving wife Paramee Thanthrige for being so supportive.

Dedication

I dedicate my dissertation work to my family and many friends. A special feeling of gratitude to my loving parents, Nirmala Warnakulasuriya and the late Chandrasiri De Silva whose words of encouragement and push for tenacity ring in my ears.

I also dedicate this dissertation to my loving wife and my sister.

Chapter 1

Introduction

The primary goal of this thesis is the study of the Lind-Lehmer constant for groups of the form $\mathbb{Z}_p^n$. As we discover, the value of the Lind-Lehmer constant can be expressed in terms of the quantity

$$\mathcal{M}_n := \min\{a^{p^{n-1}} \pmod{p^n} \mid 2 \leq a \leq p-1\}.$$

Thus, the second part of the thesis is devoted to the estimation of $\mathcal{M}_n$.

The results in the first part of the thesis have been accepted by the Proceeding of the AMS [1].

1.1 Mahler Measure and the Lind-Lehmer Constant

For a polynomial $F = F(x) \in \mathbb{C}[x]$, with factorization

$$F(x) = a_n \prod_{i=1}^{n} (x - \alpha_i) \ , \alpha_i \in \mathbb{C},$$

the Mahler measure of F is defined by

$$M(F) := |a_n| \prod_{i=1}^{n} \max\{1, |\alpha_i|\},$$

and the logarithmic Mahler measure is defined by

$$m(F) := \log M(F).$$

Plainly if $F \in \mathbb{Z}[x]$ then $M(F) \geq 1$. For any cyclotomic polynomial F, $M(F) = 1$. The classic Lehmer problem asks whether for any $\epsilon > 0$ there is a polynomial $F \in \mathbb{Z}[x]$ such that $1 < M(F) < 1 + \epsilon$. Currently the smallest known value larger than 1, found by Lehmer is $M(F) = 1.176280818...$ for the polynomial

$$x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + x + 1.$$

Lind [2] generalized Lehmer's problem to an arbitrary compact abelian group by making use of the following formula for the logarithmic Mahler measure,

$$m(F) = \int_0^1 \log |F(e^{2\pi i x})| dx;$$

see Section 2.1 for a proof of the formula. Now let G be a compact abelian group with normalized Haar measure μ, $\hat{G}$ denote its (multiplicative) dual group of characters, and $\mathbb{Z}[\hat{G}]$ be the ring of integral combinations of characters. For $f \in \mathbb{Z}[\hat{G}]$ we define the logarithmic Mahler measure of f over G to be

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

The Lind-Lehmer constant of G is defined by

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

Then the classic Lehmer problem asks whether $\lambda(\mathbb{T}) = 0$, where $\mathbb{T}$ is the abelian group $\mathbb{T} = \mathbb{R}/\mathbb{Z}$ under addition, and μ is Lebesgue measure normalized so that $\mu(\mathbb{T}) = 1$.

Lind [2] established the following upper bound on $\lambda(G)$ for any finite abelian group:

Lemma 1.1.1. *(Lind [2]) Let G be a finite abelian group with cardinality $|G| \geq 3$. Then*

$$\lambda(G) \leq \frac{1}{|G|} \log(|G| - 1).$$

As we shall see in the next section, sometimes this upper bound is attained.

1.2 Lind-Lehmer Constant for $\mathbb{Z}_m$

We start by considering the cyclic group

$$\mathbb{Z}_m := \mathbb{Z}/m\mathbb{Z}$$

under addition for $m \in \mathbb{N}$. In this case the character group $\hat{\mathbb{Z}}_m$ is a cyclic group generated by the character χ given by

$$\chi(j) := \omega^j,$$

for $j \in \mathbb{Z}_m$, where $\omega := e^{\frac{2\pi i}{m}}$. Thus a typical element of $\mathbb{Z}[\hat{\mathbb{Z}}_m]$ is of the form $F(\chi)$ where $F(x) \in \mathbb{Z}[x]$. We define the logarithmic Mahler measure $m(F) = m_{\mathbb{Z}_m}(F)$ of $F(x)$ with respect to $\mathbb{Z}_m$ to simply be the logarithmic Mahler measure of $F(\chi)$. It is easy to see in this case (see Section 2.2) that

$$m(F) = \frac{1}{m} \log |M(F)|,$$

where

$$M(F) = \prod_{j=0}^{m-1} F(\omega^j).$$

The Lind-Lehmer constant for $\mathbb{Z}_m$ is thus given by

$$\lambda(\mathbb{Z}_m) = \frac{1}{m} \log \mathcal{M}(m),$$

where

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

As we show in Proposition 2.9.2, $M(F)$ is always an integer, and thus $\mathcal{M}(m) \geq 2$. Therefore we have the lower bound

$$\lambda(\mathbb{Z}_m) \geq \frac{1}{m} \log 2. \tag{1.1}$$

By Lemma 1.1.1 we have $\lambda(\mathbb{Z}_m) \leq \frac{1}{m}\log(m-1)$, for $m \geq 3$. Indeed, in this case the upper bound is achieved by the polynomial $\left(\dfrac{x^m - 1}{x - 1}\right) - 1$; see Section 2.12 for a proof.

Lind [2] obtained the following improvement. Let $\rho(m)$ denote the smallest prime that does not divide m,

$$\rho(m) := \min_{\substack{p \text{ prime} \\ p \nmid m}} p.$$

Denote p does not divide m by $p \nmid m$.

Theorem 1.2.1. *(Lind [2]) For any integer $m \geq 2$ we have that*

$$\lambda(\mathbb{Z}_m) \leq \frac{1}{m} \log \rho(m).$$

Lind in fact showed that this upper bound is achieved for the polynomial $\dfrac{x^{\rho(m)}-1}{x-1}$. Since we know that $\lambda(\mathbb{Z}_m) \geq \frac{1}{m} \log 2$ by (1.1), we get the following corollary.

Corollary 1.2.1. *(Lind [2]) If m is odd, then*

$$\lambda(\mathbb{Z}_m) = \frac{1}{m} \log 2.$$

Equivalently we have that

$$\mathcal{M}(m) = 2$$

if m is odd. Lind [2] further conjectured that $\lambda(\mathbb{Z}_m) = \frac{1}{m} \log \rho(m)$ for all $m \geq 2$, but this was proven to be false by Kaiblinger [3].

Kaiblinger extended Lind's result and obtained the following bounds. Let

$$\rho_1(m) := \min \left\{ \min_{\substack{p \text{ prime} \\ p \nmid m}} p, \min_{\substack{p \text{ prime} \\ p^k \| m}} p^{k+1} \right\},$$

and

$$\rho_2(m) := \min \left\{ \min_{\substack{p \text{ prime} \\ p \nmid m}} p, \min_{\substack{p \text{ prime} \\ p^k \| m}} p^{p^k} \right\}.$$

Theorem 1.2.2. *(Kaiblinger [3]) For $\mathcal{M}(m) \geq 2$ we have $\mathcal{M}(m) \nmid m$ and*

$$\rho_1(m) \leq \mathcal{M}(m) \leq \rho_2(m).$$

Consequently, for all m with $420 \nmid m$,

$$\mathcal{M}(m) = \rho_1(m) = \rho_2(m).$$

Equality in these lower and upper bounds gives the following:

$$\begin{aligned}
\mathcal{M}(m) &= 3 \quad \text{if } m = 2k,\ 3 \nmid k,\\
\mathcal{M}(m) &= 4 \quad \text{if } m = 2\cdot 3k,\ 2 \nmid k,\\
\mathcal{M}(m) &= 5 \quad \text{if } m = 2^2\cdot 3k,\ 5 \nmid k,\\
\mathcal{M}(m) &= 7 \quad \text{if } m = 2^2\cdot 3\cdot 5k,\ 7 \nmid k.
\end{aligned}$$

From Theorem 1.2.2 we get that

$$\mathcal{M}(420) \in \{8, 9, 11\}.$$

Pigno and Pinner[4] showed that

$$\mathcal{M}(420) = 11.$$

More generally, they extended Kaiblinger's result and came up wih the following:

Theorem 1.2.3. *(Pigno and Pinner [4]) For $m \in \mathbb{N}$ we have,*

$$\begin{aligned}
\mathcal{M}(m) &= 11 \quad \textit{if } m = 2^2\cdot 3\cdot 5\cdot 7k,\ 11 \nmid k,\\
\mathcal{M}(m) &= 13 \quad \textit{if } m = 2^2\cdot 3\cdot 5\cdot 7\cdot 11k,\ 13 \nmid k,\\
\mathcal{M}(m) &= 16 \quad \textit{if } m = 2^2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13k,\ 2 \nmid k,\\
\mathcal{M}(m) &= 17 \quad \textit{if } m = 2^3\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13k,\ 17 \nmid k,\\
\mathcal{M}(m) &= 19 \quad \textit{if } m = 2^3\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17k,\ 19 \nmid k,\\
\mathcal{M}(m) &= 23 \quad \textit{if } m = 2^3\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19k,\ 23 \nmid k.
\end{aligned}$$

Therefore the first unresolved case is now

$$\mathcal{M}(2^3\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23) \in \{25, 27\}.$$

1.3 The Lind-Lehmer Constant for Finite Abelian Groups

The formulation

$$m(F) = \int_0^1 \log \left| F\left(e^{2\pi i x}\right) \right| \, dx$$

allows one to generalize the concept of Mahler measure to a more general setting. For $F \in \mathbb{C}[x_1, x_2, ..., x_n]$ we define

$$m(F) := \int_0^1 \cdots \int_0^1 \log \left| F\left(e^{2\pi i x_1}, e^{2\pi i x_2}, \ldots, e^{2\pi i x_n}\right) \right| \, dx_1 \cdots dx_n.$$

A theorem of Lawton [5] states that

$$m\left(F(x_1, x_2, \ldots, x_n)\right) = \lim_{k \to +\infty} m(F(x, x^k, x^{k^2}, \ldots, x^{k^{n-1}})),$$

and thus the infimum of the multidimensional measures greater than one of polynomials with integer coefficients can be reduced to studying the measure of polynomials in one variable.

Here we study the case of the finite abelian group

$$G := \mathbb{Z}_p^n = \mathbb{Z}_p \times \mathbb{Z}_p \times \cdots \times \mathbb{Z}_p,$$

where p is a prime and n is any positive integer. In this case, for $F \in \mathbb{Z}[x_1, x_2, \ldots, x_n]$ the logarithmic Mahler measure of F over G is given by

$$m(F) = m_G(F) = \frac{1}{p^n} \sum_{j_1=0}^{p-1} \sum_{j_2=0}^{p-1} \cdots \sum_{j_n=0}^{p-1} \log \left| F\left(\omega^{j_1}, \omega^{j_2}, \ldots, \omega^{j_n}\right) \right|,$$

where $\omega = e^{\frac{2\pi i}{p}}$; see Section 2.3. The Lind-Lehmer constant of G is given by

$$\lambda(G) := \inf\{m_G(F) \ : \ F \in \mathbb{Z}[x_1, x_2, \ldots, x_k], m_G(F) > 0\}.$$

For $F \in \mathbb{Z}[x_1, \ldots, x_n]$ we define

$$M(F) = M_G(F) := \prod_{j_1=0}^{p-1} \cdots \prod_{j_n=0}^{p-1} F(\omega^{j_1}, \ldots, \omega^{j_n}).$$

Observing that $m(F) = \frac{1}{p^n} \log |M(F)|$ we see that

$$\lambda(G) = \frac{1}{p^n} \inf\{\log |M(F)| : \ |M(F)| > 1\}.$$

Thus, since $M(F)$ is always an integer it is plain that $\lambda(\mathbb{Z}_p^n) \geq \frac{1}{p^n} \log 2$. Moreover, for the polynomial $F = \prod_{k=1}^{n} \left(\frac{x_k^p - 1}{x_k - 1} \right) - 1$, we have $m(F) = \frac{1}{p^n} \log(p^n - 1)$ as shown in Proposition 2.13.1. Thus we have the trivial bounds

$$\frac{1}{p^n} \log 2 \leq \lambda(\mathbb{Z}_p^n) \leq \frac{1}{p^n} \log(p^n - 1). \tag{1.2}$$

Lind further conjectured that for all $n \geq 2$ we have

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

Here we prove Lind's conjecture, and give an extension of it valid for any prime p.

1.4 Main results

Here we establish the following theorem.

Theorem 1.4.1. *For $n \geq 2$,*

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

For $n \geq 1$ and any prime $p \geq 3$,

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

where $\mathcal{M}_n$ is defined by

$$\mathcal{M}_n := \min\{a^{p^{n-1}} \pmod{p^n} \mid 2 \leq a \leq p - 1\}.$$

Therefore calculating $\lambda(\mathbb{Z}_p^n)$ reduces to finding the smallest non-trivial positive integer solution to the congruence $x^{p-1} \equiv 1 \pmod{p^n}$. For example if 2 satisfies this congruence, that is $2^{p-1} \equiv 1 \pmod{p^n}$, then we would achieve the lower bound in (1.2). For $n = 2$, such primes are called *Wieferich primes*, and the only known examples are $p = 1093$ and $p = 3511$. Thus for any Wieferich prime we have $\lambda(\mathbb{Z}_p^2) = \frac{1}{p^2}\log 2$. On the other hand, Theorem 3.0.1 also shows that we achieve the upper bound in (1.2) when $p = 2$ and $p = 3$; see Corollary 3.0.1. The proof of Theorem 3.0.1 is given in Section 3.3.

Regarding the estimation of $\mathcal{M}_n$ we will obtain the following estimate, relating it to the estimation of the n-th order Heilbronn sum

$$H_{p^n}(y) := \sum_{x=0}^{p-1} e_{p^n}\left(yx^{p^{n-1}}\right),$$

where $e_{p^n}(x) := e^{2\pi i x/p^n}$. Put

$$H_{p^n} := \max_{p\nmid y} |H_{p^n}(y)|.$$

Then we have the following theorem.

Theorem 1.4.2. *For any prime p and positive integer n we have*

$$\mathcal{M}_n \ll p^{n-1} H_{p^n}.$$

The trivial estimate for $\mathcal{M}_n$ is p^n, and the trivial estimate for H_{p^n} is p. Thus we see that any nontrivial estimate of H_{p^n} leads to a corresponding nontrivial estimate for $\mathcal{M}_n$. In Chapter 4 we prove Theorem 1.4.2 and give a discussion of the current best available estimates for H_{p^n}. For example, when $n = 2$, we have

$$H_{p^2} \ll p^{31/36} \log^{1/6} p,$$

by the recent work of Shkredov [6], and so we obtain

$$\mathcal{M}_2 \ll p^{67/36} \log^{1/6} p$$

and

$$\lambda(\mathbb{Z}_p^2) = \frac{1}{p^2}\log(\mathcal{M}_2) \le \frac{67}{36} \cdot \frac{\log p}{p^2} + O\left(\frac{\log\log p}{p^2}\right).$$

Chapter 2

Background Material

2.1 Proof of the Integral Formulation of Logarithmic Mahler Measure

We begin the chapter by deriving the integral formulation for the logarithmic Mahler measure. Recall, that for non zero $F(x) \in \mathbb{Z}[x]$, with

$$F(x) = a_n \prod_{i=1}^{n} (x - \alpha_i) \ , \alpha_i \in \mathbb{C},$$

the classical Mahler measure of F is defined by

$$M(F) := |a_n| \prod_{i=1}^{n} \max\{1, |\alpha_i|\},$$

and the logarithmic Mahler measure is defined by,

$$m(F) := \log M(F).$$

The integral formulation follows from the following well known formula of Jensen.

Theorem 2.1.1. *(Conway [7, page 280]) Let F be an analytic function on the disk $|z| \leq r$, $F(0) \neq 0$ and $\alpha_1, \ldots, \alpha_k$ be the zeros of F in $|z| < r$ counted with multiplicity. Then*

$$\int_0^1 \log \left|F\left(re^{2\pi i\theta}\right)\right| d\theta = \log |F(0)| + \sum_{j=1}^{k} \log \left|\frac{r}{\alpha_j}\right| . \tag{2.1}$$

Theorem 2.1.2. *For any nonzero $F(x) \in \mathbb{Z}[x]$ we have*

$$\log M(F) = \int_0^1 \log \left|F\left(e^{2\pi i\theta}\right)\right| d\theta.$$

Proof. Let $F(x) = a_n \prod_{i=1}^{n}(x - \alpha_i)$. Putting $r = 1$ in (2.1) we get

$$\begin{aligned}\int_0^1 \log |F(e^{2\pi i\theta})| d\theta &= \log |a_n \alpha_1 \cdots \alpha_n| - \sum_{|\alpha_i|<1} \log |\alpha_i| \\ &= \log |a_n| + \sum_{|\alpha_i|\geq 1} \log |\alpha_i| \\ &= \log \left(|a_n| \prod_{i=1}^{n} \max\{1, |\alpha_i|\} \right) \\ &= \log M(F).\end{aligned}$$

□

2.2 Logarithmic Mahler Measure on $\mathbb{Z}_m$

In the next two sections we derive the formula for the logarithmic Mahler measure on a finite abelian group. First, lets recall Lind's definition for a more general compact abelian group. Let G be a compact abelian group with normalized Haar measure μ, $\hat{G}$ denote its (multiplicative) dual group of characters, and $\mathbb{Z}[\hat{G}]$ be the ring of integral linear combinations of characters. For $f \in \mathbb{Z}[\hat{G}]$ we define the logarithmic Mahler measure of f over G to be

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

This definition was motivated by the integral formulation of the classical logarithmic Mahler measure. The Lind-Lehmer constant of G is defined by

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

In the classical case, the compact abelian group is just the torus $\mathbb{T} := \mathbb{R}/\mathbb{Z}$ under addition, together with the normalized Lebesgue measure. The characters on $\mathbb{T}$ are functions

$\chi_k : \mathbb{T} \to \mathbb{C}$, $k \in \mathbb{Z}$, given by $\chi_k(x) := e^{2\pi i k x}$. A typical element of $f \in \mathbb{Z}[\hat{\mathbb{T}}]$ is given by $f = \sum_{k\in\mathcal{I}} a_k\chi_k$, $a_k \in \mathbb{Z}$, for some finite index set $\mathcal{I} \subseteq \mathbb{Z}$. Then for $x \in \mathbb{T}$,

$$f(x) = \sum a_k\chi_k(x) = \sum a_k \left(e^{2\pi i x}\right)^k = F\left(e^{2\pi i x}\right),$$

where $F(x) = \sum_{k\in\mathcal{I}} a_k x^k$. Thus Lind's definition of logarithmic Mahler measure says $m(f) = \int_{\mathbb{T}} \log|f| d\mu = \int_0^1 \log\left|F\left(e^{2\pi i k x}\right)\right| dx$, which coincides, in the case of polynomial F, with the classical logarithmic Mahler measure of F by Theorem 2.1.2.

For the purpose of this thesis, we are only interested in the Haar measure for finite abelian groups. Being translation invariant the Haar measure must assign the same mass to every point of the group, and thus being countably additive, if the measure is normalized so that $\mu(G) = 1$ we must have $\mu(\{g\}) = 1/|G|$ for any point $g \in G$, and $\mu(S) = |S|/|G|$ for any subset $S \subseteq G$. Such a measure is also called the discrete measure on G. Thus, for the case of an additive group $\mathbb{Z}_m$ we let μ be the discrete measure normalized so that $\mu(\mathbb{Z}_m) = 1$. For any subset $S \subseteq \mathbb{Z}_m$, we have $\mu(S) = |S|/m$, and for any real valued function $h : \mathbb{Z}_m \to \mathbb{R}$, the integral of h on $\mathbb{Z}_m$ with respect to μ is given by

$$\int_{\mathbb{Z}_m} h(x)\, d\mu := \frac{1}{m}\sum_{x\in\mathbb{Z}_m} h(x) = \frac{1}{m}\sum_{x=0}^{m-1} h(x),$$

where in the latter sum we have identified $\mathbb{Z}_m$ with the set of integer representatives $\{0, 1, \ldots, m-1\}$. For $0 \le k < m$ we let χ_k denote the additive character on $\mathbb{Z}_m$,

$$\chi_k : \mathbb{Z}_m \to \mathbb{C}, \qquad \chi_k(x) = e^{2\pi i k x/m},$$

and $\hat{\mathbb{Z}}_m$ denote the group of characters on $\mathbb{Z}_m$,

$$\hat{\mathbb{Z}}_m := \{\chi_k : 0 \le k < m\}.$$

Let $\mathbb{Z}[\hat{\mathbb{Z}}_m]$ denote the set of all integer linear combinations of characters on $\mathbb{Z}_m$. Then for any $f \in \mathbb{Z}[\hat{\mathbb{Z}}_m]$, the logarithmic Mahler measure of f is given by

$$m(f) = m_{\mathbb{Z}_m}(f) := \int_{\mathbb{Z}_m} \log|f|\, d\mu = \frac{1}{m}\sum_{x=0}^{m-1} \log|f(x)|. \tag{2.2}$$

Now $f = \sum_{k=0}^{m-1} a_k \chi_k$ for some integers a_k, $0 \leq k < m$, and so for $x \in \mathbb{Z}_m$,

$$f(x) = \sum_{k=0}^{m-1} a_k \chi_k(x) = \sum_{k=0}^{m-1} a_k e^{2\pi i k x/m} = \sum_{k=0}^{m-1} a_k \left(e^{2\pi i x/m}\right)^k .$$

Putting

$$F = F(X) := \sum_{k=0}^{m-1} a_k X^k \in \mathbb{Z}[X],$$

(where X is an indeterminate symbol) we see that for $x \in \mathbb{Z}_m$, $f(x) = F(e^{2\pi i x/m})$ and

$$m(f) = \frac{1}{m} \sum_{x=0}^{m-1} \log \left| F\left(e^{2\pi i x/m}\right) \right| = \frac{1}{m} \log \left| \prod_{x=0}^{m-1} F\left(e^{2\pi i x/m}\right) \right| .$$

Setting

$$M(F) = M_{\mathbb{Z}_m}(F) := \prod_{x=0}^{m-1} F\left(e^{2\pi i x/m}\right),$$

we see that the logarithmic Mahler measure of f is given by

$$m(f) = \frac{1}{m} \log |M(F)| .$$

Note that $M(F) = 0$ if and only if F vanishes at an m-th root of unity, in which case the corresponding logarithmic Mahler measure of $f(x) = F(e^{2\pi i x/m})$ is undefined (or taken to be $-\infty$.) Thus we restrict our attention to polynomials F not vanishing at any m-th root of unity. We also note that $M(F)$ is an algebraic integer contained in $\mathbb{Q}$ and therefore an ordinary integer. It takes on the value ±1 if and only if $F(x)$ is a unit in the quotient ring $Z[X]/(X^m - 1)$ as shown by Pinner and Vaaler [8]. The same authors observed that one can say $M(F) = 0$ if and only if F is a zero divisor in $\mathbb{Z}[X]/(X^m - 1)$.

In the Lehmer problem, the goal is to determine the minimum value of $|M(F)|$ over all polynomials F with $|M(F)| \geq 2$, the polynomials that are neither units nor zero divisors in $\mathbb{Z}[X]/(X^m - 1)$.The Lind-Lehmer constant for $\mathbb{Z}_m$ is defined by

$$\begin{aligned} \lambda(\mathbb{Z}_m) &:= \inf\{m_{\mathbb{Z}_m}(f) \ : f \in \mathbb{Z}[\hat{G}], m_G(f) > 0\} \\ &= \frac{1}{m} \inf\{\log |M(F)| : F(x) \in \mathbb{Z}[x], \deg(F) < m, |M(F)| > 1\}. \end{aligned} \tag{2.3}$$

We note that the infimum would not change if we allowed polynomials F of arbitrary degree in the preceding formula.

To get the reader better acquainted with the Lind-Lehmer constant, we show how to compute it directly in the simplest cases $m = 1, 2$ and 3; see also Lind [2] for the same examples.

Example 2.2.1. Trivially we have $\lambda(\mathbb{Z}_1) = \log 2$. Here $M(F) = F(1)$ so the smallest possible value for $|M(F)|$ is 2, since $M(F) \in \mathbb{Z}$. This can be achieved by polynomials such as $F(x) = 2$ or $F(x) = x + 1$.

Example 2.2.2. Let $G = \mathbb{Z}_2$ and $F(x) = a + bx \in \mathbb{Z}[x]$. Letting $\omega_2 = e^{2\pi i/2} = -1$, we have

$$\begin{aligned} M(F) &= \prod_{j=0}^{1} F\left(\omega_2^j\right) \\ &= F(1)F(-1) \\ &= (a+b)(a-b) \\ &= a^2 - b^2. \end{aligned}$$

Thus, we need to find the minimum value of $|a^2 - b^2|$ for $a, b \in \mathbb{Z}$. Observing that

$$a^2 - b^2 \equiv \{0,1\} - \{0,1\} \equiv \{0,1,-1\} \pmod 4,$$

we see that the equation

$$a^2 - b^2 = \pm 2$$

has no solutions. So the minimum possible value for $|M(F)|$ is 3 which in fact is attained by the polynomial $F(x) = 2 + x$. Therefore $\lambda(\mathbb{Z}_2) = \frac{1}{2}\log 3$.

Example 2.2.3. Let $G = \mathbb{Z}_3$ and $F(x) = a + bx + cx^2 \in \mathbb{Z}[x]$. Letting $\omega_3 = e^{2\pi i/3}$, and making use of the identity $1 + \omega_3 + \omega_3^2 = 0$, we obtain

$$\begin{aligned} M(F) &= \prod_{j=0}^{2} F(\omega_3^j) \\ &= F(1)F(\omega_3)F(\omega_3^2) \\ &= (a+b+c)(a+b\omega_3+c\omega_3^2)(a+b\omega_3^2+c\omega_3^4) \\ &= (a+b+c)[a^2+b^2+c^2+(ab+bc+ac)(\omega_3+\omega_3^2)] \\ &= (a+b+c)[a^2+b^2+c^2-(ab+bc+ac)] \\ &= a^3+b^3+c^3-3abc. \end{aligned}$$

Letting $a = b = 1$ and $c = 0$ we get the value 2 for $M(F)$. Therefore 2 is the smallest possible value greater than 1, since a, b, c are all integers. So $\lambda(\mathbb{Z}_3) = \frac{1}{3}\log 2$.

2.3 Lind-Lehmer Constant for Finite Abelian Groups

Now let G be any finite abelian group. Then G is isomorphic to a direct sum of cyclic groups, and so we may assume that

$$G = \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_n},$$

for some positive integers m_i, $1 \le i \le n$. A typical character on G has the form

$$\chi_{e_1,\ldots,e_n}(x_1,\ldots,x_n) := e^{2\pi e_1 x_1 i/m_1} \cdots e^{2\pi e_n x_n i/m_n}$$

for $(x_1,\ldots,x_n) \in G$, where the e_i are integers with $0 \le e_i < m_i$, $1 \le i \le n$.

Our interest here is the case of $\mathbb{Z}_p^n$, in which case, letting $\omega = e^{2\pi i/p}$ we have

$$\chi_{e_1,\ldots,e_n}(x_1,\ldots,x_n) = \omega^{e_1 x_1} \cdots \omega^{e_n x_n}.$$

A typical element of the ring $\mathbb{Z}[\hat{\mathbb{Z}_p^n}]$ has the form

$$f = \sum_{e_1=0}^{p-1} \cdots \sum_{e_n=0}^{p-1} a_{e_1,\ldots,e_n}\chi_{e_1,\ldots,e_n},$$

for some integers $a_{e_1,\ldots,e_n}$. Evaluated at $(x_1,\ldots,x_n) \in \mathbb{Z}_p^n$, we have

$$\begin{aligned} f(x_1,\ldots,x_n) &= \sum_{e_1=0}^{p-1} \cdots \sum_{e_n=0}^{p-1} a_{e_1,\ldots,e_n} \chi_{e_1,\ldots,e_n}(x_1,\ldots,x_n) \\ &= \sum_{e_1=0}^{p-1} \cdots \sum_{e_n=0}^{p-1} a_{e_1,\ldots,e_n} \omega^{e_1 x_1} \cdots \omega^{e_n x_n} \\ &= F(\omega^{x_1},\ldots,\omega^{x_n}), \end{aligned}$$

where $F(X_1,\ldots,X_n)$ is a polynomial over $\mathbb{Z}$ of degree less than p in each variable given by

$$F(X_1,\ldots,X_n) = \sum_{e_1=0}^{p-1} \cdots \sum_{e_n=0}^{p-1} a_{e_1,\ldots,e_n} X_1^{e_1} \cdots X_n^{e_n}.$$

Letting μ denote the discrete measure on G we see that

$$\begin{aligned} \int_G \log|f|\; d\mu &= \frac{1}{p^n} \sum_{x_1=1}^{p} \cdots \sum_{x_n=1}^{p} \log\left|f\left(x_1,\ldots,x_n\right)\right| \\ &= \frac{1}{p^n} \sum_{x_1=1}^{p} \cdots \sum_{x_n=1}^{p} \log\left|F\left(\omega^{x_1},\ldots,\omega^{x_n}\right)\right| \\ &= \frac{1}{p^n} \log\left|\prod_{x_1=0}^{p-1} \cdots \prod_{x_n=0}^{p-1} F\left(\omega^{x_1},\ldots,\omega^{x_n}\right)\right|. \end{aligned}$$

Thus, defining $M(F)$ to be

$$M(F) := \prod_{x_1=0}^{p-1} \cdots \prod_{x_n=0}^{p-1} F\left(\omega^{x_1},\ldots,\omega^{x_n}\right),$$

we see that the logarithmic Mahler measure of f is given by

$$m(f) := \frac{1}{p^n} \int_G \log|f|\; d\mu = \frac{1}{p^n} \log|M(F)|.$$

Our goal is to determine the minimum value of $|M(F)|$ over all integer polynomials with $|M(F)| > 1$.

2.4 Early Calculations

In order to gain an understanding of the size of $M(F)$ we wrote a program in C++ to calculate $M(F)$ for polynomials F with small coefficients. The program is given in Appendix

B. The following are some examples of the record breaking polynomials we discovered doing this search.

Example 2.4.1. For the group $\mathbb{Z}_5^2$, we got $|M(F)| = 7$, for the polynomial

$$F = -(1+x)\left(1+y+y^2+y^3+y^4\right) + x^3y^2\left(1+y+y^2\right).$$

As we show later in Theorem 3.0.1, the value $|M(F)| = 7$ is the minimal possible value for $|M(F)|$ for this group.

Example 2.4.2. For the group $\mathbb{Z}_7^2$, we got $|M(F)| = 19$, for the polynomial

$$F = -\left(1+x^4\right)\left(1+y+y^2+y^3+y^4\right) - x\left(1+x^2\right)\left(1+y+y^3+y^4\right) - x^2\left(1-y^2+y^4\right).$$

In Theorem 3.0.1, we show that the minimal value of $|M(F)|$ is actually $|M(F)| = 18$.

2.5 Field Extensions and Isomorphisms

Definition 2.5.1. a) A field K is said to be an extension field of a field L if L is a subfield of K. In this case, K is a vector space over L. The dimension of the L-vector space K will be denoted by $[K : L]$.

b) An element $\alpha \in K$ is said to be algebraic over L if α is the zero of a nonzero polynomial with coefficients in L.

c) The field K is said to be algebraic over L if every element of K is algebraic over L.

d) If $\alpha \in K$ is algebraic over L, then the minimal polynomial for α is the monic polynomial of smallest degree over L that α is a zero of. In this case we say α is algebraic of degree d over L, where d is the degree of the minimal polynomial.

e) If $\alpha \in K$, we let

$$L[\alpha] = \{p(\alpha) : p(x) \in L[x]\},$$
$$L(\alpha) = \{\tfrac{p(\alpha)}{q(\alpha)} : p(x), q(x) \in L[x], q(\alpha) \neq 0\}.$$

The following is a standard theorem on the dimension of an algebraic extension.

Theorem 2.5.1. *If K is an extension field of L and $\alpha \in K$ is algebraic of degree d over L, then $L(\alpha)$ is a field extension of L of dimension d over L.*

Next let us recall the definition of a field isomorphism.

Definition 2.5.2. Let K_1, K_2 be fields containing a field L. A mapping $\eta : K_1 \to K_2$ is called an isomorphism fixing L (or relative to L) if

$$\begin{aligned} i)&\ \eta(xy) = \eta(x)\eta(y) \text{ for all } x, y \in K_1,\\ ii)&\ \eta(x+y) = \eta(x) + \eta(y) \text{ for all } x, y \in K_1,\\ iii)&\ \eta(x) = x \text{ for all } x \in L,\\ iv)&\ \eta \quad \text{is one to one and onto.} \end{aligned}$$

If $K_1 = K_2$ then η is called an automorphism of K_1.

We note that properties $i), ii)$ and $iii)$ imply property $iv)$. We have the following standard theorem from Field Theory.

Theorem 2.5.2. *Let K be a finite extension of $\mathbb{Q}$ of dimension n. Then there exist n isomorphisms of K into $\mathbb{C}$.*

Next, we recall the notion of an “integer” in an algebraic extension of $\mathbb{Q}$.

Definition 2.5.3. a) An element $\alpha \in \mathbb{C}$ is called an algebraic integer if α is a zero of a monic polynomial over $\mathbb{Z}$.

b) If K is an algebraic extension of $\mathbb{Q}$, then the set of algebraic integers in K is called the ring of integers in K.

We note that the ring of integers in K is in fact a ring. In particular, it is closed under addition and multiplication. We also have the following well known theorem.

Theorem 2.5.3. *Let $\alpha \in \mathbb{C}$ be algebraic over $\mathbb{Q}$. Then α is an algebraic integer if and only if the minimal polynomial for α over $\mathbb{Q}$ has integer coefficients.*

2.6 The Cyclotomic Field $\mathbb{Q}(\omega)$

Let $\omega = e^{2\pi i/p}$. The field $\mathbb{Q}(\omega)$ is called a cyclotomic extension of the rationals. It is well known that the minimal polynomial of ω is

$$\Phi(x) = 1 + x + x^2 + \cdots + x^{p-1},$$

called a cyclotomic polynomial, and thus

$$[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1.$$

The automorphisms of $\mathbb{Q}(\omega)$ fixing $\mathbb{Q}$ are given by $\sigma_k : \mathbb{Q}(\omega) \rightarrow \mathbb{Q}(\omega)$, $1 \leq k \leq p-1$, where

$$\sigma_k(\omega) = \omega^k.$$

Finally, we observe that the ring of integers in $\mathbb{Q}(\omega)$ is a particularly nice looking set.

Theorem 2.6.1. *The ring of integers in the cyclotomic field $\mathbb{Q}(\omega)$ is just*

$$\mathbb{Z}[\omega] = \{a_0 + a_1\omega + \cdots + a_{p-2}\omega^{p-2} : a_i \in \mathbb{Z}, 0 \leq i \leq p-2\}.$$

2.7 Norms, Units and Irreducibles

Definition 2.7.1. Let K be a finite extension of $\mathbb{Q}$ of degree n, with isomorphisms σ_k, $1 \leq k \leq n$, from K into $\mathbb{C}$. For any $\alpha \in K$, we define the norm of α over $\mathbb{Q}$ to be

$$N_{K/\mathbb{Q}}(\alpha) := \prod_{k=1}^{n} \sigma_k(\alpha).$$

We note that the norm of any element of K is always a rational number. If α is an algebraic integer, then so is every conjugate of α, (since it has the same minimal polynomial) and thus so is $N_{K/\mathbb{Q}}(\alpha)$. But the only algebraic integers in $\mathbb{Q}$ are just rational integers and so we have the following proposition.

Proposition 2.7.1. If α is an algebraic integer in K, then $N_{K/\mathbb{Q}}(\alpha) \in \mathbb{Z}$.

Next, lets return to the cyclotomic number field $K = \mathbb{Q}(\omega)$ with $\omega = e^{2\pi i/p}$. For any $\alpha \in K$ we have

$$N(\alpha) = N_{\mathbb{Q}(\omega)/\mathbb{Q}}(\alpha) := \prod_{k=1}^{p-1} \sigma_k(\alpha).$$

with the σ_k being the automorphisms as defined above.

Proposition 2.7.2. Let $\pi := 1 - \omega$. Then $N(\pi) = p$

Proof. Let $\Phi(x)$ be the minimal polynomial for ω,

$$\Phi(x) = x^{p-1} + \cdots + 1 = \prod_{k=1}^{p-1}(x - \omega^k).$$

Then we have

$$N(\pi) = N(1 - \omega) = \prod_{k=1}^{p-1}(1 - \omega^k) = \Phi(1) = p.$$

□

Definition 2.7.2. An element $u \in \mathbb{Z}[\omega]$ is called a unit in $\mathbb{Z}[\omega]$ if $u^{-1} \in \mathbb{Z}[\omega]$.

Proposition 2.7.3. For $p > 2$ an element $u \in \mathbb{Z}[\omega]$ is a unit in $\mathbb{Z}[\omega]$ if and only if $N(u) = 1$.

Proof. Suppose $u \in \mathbb{Z}[\omega]$ is a unit in $\mathbb{Z}[\omega]$. Let $v \in \mathbb{Z}[\omega]$ be such that $u \cdot v = 1$. Then $N(u)N(v) = N(1) = 1$ and since u and v are algebraic integers $N(u), N(v) \in \mathbb{Z}$. Since conjugates come in complex conjugate pairs, $N(u) > 0$ and thus $N(u) = 1$.

Conversely, suppose $N(u) = 1$. Then $1 = N(u) = \prod_{k=1}^{p-1} \sigma_k(u) = u \prod_{k=2}^{p-1} \sigma_k(u)$. Now since $\prod_{k=2}^{p-1} \sigma_k(u) \in \mathbb{Z}[\omega]$, we get that u is a unit in $\mathbb{Z}[\omega]$. □

Proposition 2.7.4. For $1 \leq a \leq p-1$, $1 + \omega + \cdots + \omega^{a-1}$ is a unit in $\mathbb{Z}[\omega]$. In fact we have

$$N(1 + \omega + \cdots + \omega^{a-1}) = 1.$$

Proof. We have

$$1 + \omega + \cdots + \omega^{a-1} = \frac{\omega^a - 1}{\omega - 1}.$$

Now $N(\omega^a - 1) = N(\omega - 1)$ since these are conjugate values, and so we get

$$N(1 + \omega + \cdots + \omega^{a-1}) = \frac{N(\omega^a - 1)}{N(\omega - 1)} = 1,$$

whence we deduce from Proposition 2.7.3 that $1 + \omega + \cdots + \omega^{a-1}$ is an unit. □

Definition 2.7.3. An element $\alpha \in \mathbb{Z}[\omega]$ is said to be irreducible in $\mathbb{Z}[\omega]$ if whenever $\alpha = uv$ for some $u, v \in \mathbb{Z}[\omega]$, either u or v is a unit in $\mathbb{Z}[\omega]$.

Proposition 2.7.5. If $\alpha \in \mathbb{Z}[\omega]$ and $|N(\alpha)|$ is a prime in $\mathbb{Z}$, then α is an irreducible in $\mathbb{Z}[\omega]$.

Proof. Suppose that $\alpha = u \cdot v$, with $u, v \in \mathbb{Z}[\omega]$. Then $|N(\alpha)| = |N(u)||N(v)|$ is prime. Thus $N(u)$ or $N(v)$ is a unit in $\mathbb{Z}$. Therefore $N(u) = \pm 1$ or $N(v) = \pm 1$. Now by Proposition 2.7.3 we get that u or v is a unit in $\mathbb{Z}[\omega]$. Hence α is a prime in $\mathbb{Z}[\omega]$. □

Proposition 2.7.6. Let $\pi = 1 - \omega$. Then π is irreducible in $\mathbb{Z}[\omega]$.

Proof. The result is immediate from Propositions 2.7.2 and 2.7.5. Indeed, $N(\pi) = p$, a prime. □

2.8 Projective n-space $P_n(\mathbb{Z}_p)$

We start by defining an equivalence relation on $\mathbb{Z}_p^n \backslash \{\mathbf{0}\}$ by setting $\mathbf{u} \sim \mathbf{v}$ for $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_p^n \backslash \{\mathbf{0}\}$, if $\mathbf{u} = \lambda \mathbf{v}$ for some nonzero $\lambda \in \mathbb{Z}_p$. This partitions $\mathbb{Z}_p^n \backslash \{\mathbf{0}\}$ into $I := \frac{p^n - 1}{p-1}$ equivalence classes. Projective n-space $P_n(\mathbb{Z}_p)$ is just the set of these equivalence classes. We shall denote an element $\mathbf{u} \in P_n(\mathbb{Z}_p)$ by

$$\mathbf{u} = (u_1 : u_2 : \cdots : u_n).$$

A standard set of representatives for these equivalence classes can be chosen so that the leading nonzero coordinate of each representative is equal to 1. Thus there are p^{n-1} representatives of the form $(1 : u_2 : \cdots : u_n)$, p^{n-2} representatives of the form $(0 : 1 : u_3 : \cdots : u_n)$, $\ldots$, and one representative of the form $(0 : 0 : \cdots : 0 : 1)$, giving altogether

$$p^{n-1} + p^{n-2} + \cdots + 1 = \frac{p^n - 1}{p - 1}$$

representatives.

2.9 Expressing $M(F)$ as a Product of Norms

We observe that if $\mathbf{j} = (j_1 : \cdots : j_n) \in P_n(\mathbb{Z}_p)$ then the quantity

$$\begin{aligned} N(F\left(\omega^{j_1}, \omega^{j_2}, \ldots, \omega^{j_n}\right)) &= \prod_{k=1}^{p-1} \sigma_k(F\left(\omega^{j_1}, \omega^{j_2}, \ldots, \omega^{j_n}\right)) \\ &= \prod_{k=1}^{p-1} F\left(\sigma_k\left(\omega^{j_1}\right), \sigma_k\left(\omega^{j_2}\right), \ldots, \sigma_k\left(\omega^{j_n}\right)\right) \\ &= \prod_{k=1}^{p-1} F(\omega^{j_1 k}, \omega^{j_2 k}, \ldots, \omega^{j_n k}) \end{aligned}$$

is well defined, as the n-tuple of exponents on ω in the final product just runs through the set of representatives for the equivalence class $\mathbf{j}$. This leads us to the following expression for $M(F)$.

Proposition 2.9.1. Let $F \in \mathbb{Z}[x_1, \ldots, x_n]$, $G = \mathbb{Z}_p^n$ and $M_n(F) = M_G(F)$. Then we have

$$M_n(F) = F(1, 1, \ldots, 1) \prod_{\mathbf{j} \in P_n(\mathbb{Z}_p)} N\left(F\left(\omega^{j_1}, \omega^{j_2}, \ldots, \omega^{j_n}\right)\right).$$

Proof. By definition,

$$M_n(F) := \prod_{j_1=0}^{p-1} \prod_{j_2=0}^{p-1} \cdots \prod_{j_n=0}^{p-1} F\left(\omega^{j_1}, \omega^{j_2}, \ldots, \omega^{j_n}\right).$$

We pull off the term $F(1, 1, \ldots, 1)$ and then partition the remaining nonzero n-tuples $\mathbf{j}$ into the I equivalence classes comprising $P_n(\mathbb{Z}_p)$. The product of the $F(\omega^{j_1}, \ldots, \omega^{j_n})$ over a given equivalence class $\mathbf{j}$ is just $N\left(F\left(\omega^{j_1}, \ldots, \omega^{j_n}\right)\right)$ as shown above, and so we obtain the desired formula. □

Thus we can write

$$M_n(F) = F(1, 1, \ldots, 1) N_1 N_2 \cdots N_I, \tag{2.4}$$

where the N_i are norms of the type $N_i := N\left(F\left(\omega^{j_1}, \omega^{j_2}, \ldots, \omega^{j_n}\right)\right)$, with the $(j_1, \ldots, j_n)$ running through a set of representatives for $P_n(\mathbb{Z}_p)$. In particular, since by Proposition 2.7.1 the norm of any algebraic integer is in $\mathbb{Z}$, we have the following proposition.

Proposition 2.9.2. For any polynomial $F \in \mathbb{Z}[x_1, \ldots, x_n]$, we have $M_n(F) \in \mathbb{Z}$.

The decomposition of $M_n(F)$ in (2.4) is one of the key ideas in proving our main theorem. We also employ a similar decomposition in Section 2.12 to give a new proof of Theorem 2.12.1.

2.10 p-adic Absolute Value

Definition 2.10.1. Fix a prime number $p \in \mathbb{Z}$. The p-adic valuation on $\mathbb{Z}$ is the function

$$\nu_p : \mathbb{Z}\backslash\{0\} \to \mathbb{R}$$

defined as follows: for each integer $n \in \mathbb{Z}$, $n \neq 0$, let $\nu_p(n)$ be the unique positive integer satisfying

$$n = p^{\nu_p(n)} n' \text{ with } \ p \nmid n'.$$

We extend ν_p to the field of rational numbers as follows: if $x = a/b \in \mathbb{Q}\backslash\{0\}$, then

$$\nu_p(x) = \nu_p(a) - \nu_p(b).$$

Definition 2.10.2. For any $x \in \mathbb{Q}$, we define the p-adic absolute value of x by

$$|x|_p = p^{-\nu_p(x)}$$

if $x \neq 0$, and set $|0|_p = 0$.

Note that for any $x \in \mathbb{Z}$ we have $|x|_p \leq 1$. It is called an absolute value because it satisfies the familiar properties of our ordinary absolute value.

Proposition 2.10.1. For any $a, b \in \mathbb{Q}$ we have,

$$|a \cdot b|_p = |a|_p |b|_p.$$

Proposition 2.10.2. The Triangle Inequality. For any $a, b \in \mathbb{Q}$ we have

$$|a + b|_p \leq \max\{|a|_p, |b|_p\} \leq |a|_p + |b|_p.$$

We note that the p-adic absolute value on $\mathbb{Q}$ has a unique extension to an absolute value $|\cdot|_p$ on the cyclotomic field $\mathbb{Q}(\omega)$ since the ideal (p) in $\mathbb{Z}$ factors in the manner $(p) = (\pi)^{p-1}$ in $\mathbb{Z}[\omega]$, where $\pi = 1 - \omega$; see proof of Proposition 2.10.4. The extension satisfies the standard properties given in the preceding two propositions. From Proposition 2.10.2 if α is an algebraic integer in $\mathbb{Q}(\omega)$, that is, $\alpha \in \mathbb{Z}[\omega]$ then $|\alpha|_p \leq 1$.

Proposition 2.10.3. If u is a unit in $\mathbb{Z}[\omega]$, then $|u|_p = 1$.

Proof. If u is a unit then $uv = 1$ for some $v \in \mathbb{Z}[\omega]$. Then $|uv|_p = |1|_p = 1$ and so $|u|_p|v|_p = 1$. However, since u, v are algebraic integers we must have $|u|_p \leq 1$ and $|v|_p \leq 1$. Therefore we must have $|u|_p = |v|_p = 1$. □

Proposition 2.10.4. Let $\pi = 1 - \omega$. Then $|\pi|_p = p^{\frac{-1}{p-1}} < 1$.

Proof. First note that for any $k \in \mathbb{N}$ we have $(1 - \omega^k) = (1 - \omega)u_k$ for some $u_k = 1 + \omega + \cdots + \omega^{k-1} \in \mathbb{Z}[\omega]$, and so by the multiplicative property of norms,

$$N(1 - \omega^k) = N(1 - \omega)N(u_k).$$

But if $p \nmid k$, then $N(1 - \omega^k) = N(1 - \omega) = p$, and so we deduce that $N(u_k) = 1$. Thus u_k is a unit, and we have $p = \prod_{k=1}^{p-1}(1 - \omega^k) = (1 - \omega)^{p-1} \cdot u$, for some unit $u = u_1 u_2 \cdots u_{p-1}$. That is, $p = \pi^{p-1}u$. Taking absolute values gives

$$\tfrac{1}{p} = |p|_p = |\pi|_p^{p-1}|u|_p = |\pi|_p^{p-1},$$

and the result follows. □

Proposition 2.10.5. If $a, b \in \mathbb{Z}$ and $a \equiv b \pmod{\pi}$ then $a \equiv b \pmod{p}$.

Proof. We have $\pi x = a - b$ for some $x \in \mathbb{Z}[\omega]$. Thus $|a - b|_p = |\pi|_p|x|_p < 1$ and so $p \mid (a - b)$. □

Proposition 2.10.6. For any polynomial $F(x) \in \mathbb{Z}[x]$, $N\left(F\left(\omega\right)\right) \equiv F(1)^{p-1} \pmod{p}$.

Proof. Now $\pi = 1-\omega$. Therefore we have $\omega \equiv 1 \pmod{\pi}$ and so $\omega^j \equiv 1^j \equiv 1 \pmod{\pi}$ for $j \in \mathbb{N}$. Thus we get $F(\omega^j) \equiv F(1) \pmod{\pi}$, which implies $\prod_{j=1}^{p-1} F(\omega^j) \equiv F(1)^{p-1} \pmod{\pi}$. Finally we have $N(F(\omega)) \equiv F(1)^{p-1} \pmod{\pi}$, which implies that $N(F(\omega)) \equiv F(1)^{p-1} \pmod{p}$, by Proposition 2.10.5. Here $F(1) \in \mathbb{Z}$ and $N(F(\omega)) \in \mathbb{Z}$ since $F(\omega)$ is an algebraic integer. □

Proposition 2.10.7. For any prime p and $n, L, j \in \mathbb{N}$ with $1 \le L < n$ and $1 \le j \le p^L$ we have

$$\nu_p\left(\left(p^{n-L}\right)^j \binom{p^L}{j}\right) \ge n.$$

Proof. We first observe that $\nu_p\left(\binom{p^L}{j}\right) \ge L - \nu_p(j)$ since $\binom{p^L}{j} = \frac{p^L}{j}\binom{p^L-1}{j-1}$. Thus,

$$\begin{aligned}
\nu_p\left(\left(p^{n-L}\right)^j \binom{p^L}{j}\right) &= j(n-L) + \nu_p(\binom{p^L}{j}) \\
&\ge j(n-L) + L - \nu_p(j) \\
&= jn - L(j-1) - \nu_p(j) \\
&\ge jn - (n-1)(j-1) - \nu_p(j) \quad \text{since } L \le n-1 \\
&= n - 1 + (j - \nu_p(j)) \\
&\ge n.
\end{aligned}$$

The latter step follows by the fact that $j - \nu_p(j) \ge 1$ for $j \ge 1$. □

2.11 Congruence Identities

We first recall the test for determining when an integer is a k-th power $\pmod{p^n}$, where p is an odd prime. Let $U(p^n)$ denote the group of units $\pmod{p^n}$, a cyclic group of order $\phi(p^n) = p^n - p^{n-1}$. For any positive integer k, the set of k-th powers in $U(p^n)$ is a subgroup of order $\phi(p^n)/(\phi(p^n), k)$, and thus an element $a \in U(p^n)$ is in this subgroup if and only $a^{\phi(p^n)/(\phi(p^n),k)} = 1$. This yields the following proposition.

Proposition 2.11.1. Let p be an odd prime and $n \in \mathbb{N}$. An integer a relatively prime to p is a k-th power $\pmod{p^n}$ if and only if

$$a^{\frac{\phi(p^n)}{(\phi(p^n),k)}} \equiv 1 \pmod{p^n}.$$

In the course of our proofs in the next chapter we shall appeal to the following well known identity.

Proposition 2.11.2. Let p be a prime. For any integers x, y or variable symbols x, y we have

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

More generally, for integers (or variable symbols) $x_1, \ldots, x_n$ we have

$$(x_1 + \cdots + x_n)^p \equiv x_1^p + \cdots + x_n^p \pmod{p}.$$

Proof. Now, since $p \mid \binom{p}{j}$ for $1 \leq j \leq p-1$ we have

$$\begin{aligned}(x+y)^p &= \sum_{j=0}^{p} \binom{p}{j} x^{p-j} y^j \\ &= x^p + y^p + p(x^{p-1}y + \cdots + xy^{p-1}) \\ &\equiv x^p + y^p \pmod{p}.\end{aligned}$$

To prove the general case we use induction on n. Suppose that

$$(x_1 + \cdots + x_n)^p \equiv (x_1^p + \cdots + x_n^p) \pmod{p}, \tag{2.5}$$

for a given $n \in \mathbb{N}$. Then we have

$$\begin{aligned}(x_1 + \cdots + x_n + x_{n+1})^p &= [(x_1 + \cdots + x_n) + x_{n+1}]^p \\ &\equiv (x_1 + \cdots + x_n)^p + x_{n+1}^p \pmod{p},\end{aligned}$$

the latter step following from the $n = 2$ case. Then using the induction assumption (2.5) we get

$$(x_1 + \cdots + x_k + x_{k+1})^p \equiv (x_1^p + \cdots x_k^p) + x_{k+1}^p \pmod{p},$$

proving the induction step.

□

Proposition 2.11.3. If p is a prime and $a, b \in \mathbb{Z}$ with $a \equiv b \pmod{p}$, then for any $k \geq 1$,

$$a^{p^{k-1}} \equiv b^{p^{k-1}} \pmod{p^k}.$$

Proof. We prove by induction on k. When $k = 1$ the result is trivial. Assume the result for k, so that

$$a^{p^{k-1}} = b^{p^{k-1}} + mp^k$$

for some $m \in \mathbb{Z}$. Then, since $p \mid \binom{p}{j}$ for $1 \leq j \leq p-1$ we have

$$\begin{aligned}
a^{p^k} &= \left(a^{p^{k-1}}\right)^p = \left(b^{p^{k-1}} + mp^k\right)^p \\
&= \sum_{j=0}^{p} \binom{p}{j} \left(b^{p^{k-1}}\right)^{p-j} \left(mp^k\right)^j \\
&= \left(b^{p^{k-1}}\right)^p + \left(p(b^{p^{k-1}})^{p-1} mp^k + \cdots + (mp^k)^p\right) \\
&= b^{p^k} + p^{k+1} \left((b^{p^{k-1}})^{p-1} m + \cdots + m^p p^{k(p-1)-1}\right) \\
&\equiv b^{p^k} \pmod{p^{k+1}},
\end{aligned}$$

proving the induction step. □

2.12 Polynomials with Small Mahler Measure over $\mathbb{Z}_m$

In this section we digress from our main target of studying the group $\mathbb{Z}_p^n$ in order to recover Lind's upper bound on $\lambda(\mathbb{Z}_m)$ for arbitrary m. For $F(x) \in \mathbb{Z}[x]$, we let

$$M(F) = M_{\mathbb{Z}_m}(F) = \prod_{k=0}^{m-1} F(\omega_m^k),$$

where $\omega_m = e^{2\pi i/m}$. First, we obtain an example with $|M(F)| = m - 1$.

Proposition 2.12.1. For any $m \in \mathbb{N}$ and $F(x) = \frac{x^m - 1}{x - 1} - 1$, we have $|M(F)| = m - 1$.

Proof. Note that

$$\begin{aligned}
F(x) &= \frac{x^m - 1}{x - 1} - 1 \\
&= x^{m-1} + x^{m-2} + \cdots + x.
\end{aligned}$$

Now we have

$$\begin{aligned} M(F) &= \prod_{k=0}^{m-1} F(\omega_m^k) \\ &= F(1) \prod_{k=1}^{m-1} F(\omega_m^k) \\ &= (m-1) \prod_{k=1}^{m-1} \left(\frac{\omega_m^{km} - 1}{\omega_m^k - 1} - 1 \right) \\ &= (m-1) \prod_{k=1}^{m-1} (-1) \\ &= (-1)^{m-1}(m-1). \end{aligned}$$

Therefore $|M(F)| = m - 1$. □

Next, we give the following improvement.

Theorem 2.12.1. *For any positive integer a with $(a, m) = 1$ and*

$$F(x) = 1 + x + x^2 + \cdots + x^{a-1} - k\left(\frac{x^m - 1}{x - 1}\right) = \frac{x^a - 1}{x - 1} - k\left(\frac{x^m - 1}{x - 1}\right),$$

we have $M(F) = a - km$.

In order to minimize $|M(F)|$ with $|M(F)| > 1$, we would just take $k = 0$ and let a be the minimal positive integer relatively prime to m, which of course is just the minimal prime not dividing m, denoted $\rho(m)$. Thus, for this choice of F we have $M(F) = \rho(m)$ and we recover Lind's upper bound

$$\lambda(\mathbb{Z}_m) \leq \frac{1}{m} \log \rho(m).$$

Proof. The proof here is quite different from the proof of Lind, and exploits the decomposition of $M(F)$ as a product of norms. Because m is allowed to be composite here, we need to generalize some of the notions we discussed earlier in this chapter. For any positive divisor d of m, let $\omega_d = e^{2\pi i/d}$ and $\Phi_d(x)$ denote the cyclotomic polynomial of order d,

$$\Phi_d(x) = \prod_{\substack{j=1 \\ (j,d)=1}}^{d} (x - \omega_d^j).$$

In particular,

$$(x^m - 1) = \prod_{d|m} \Phi_d(x).$$

By definition, for any polynomial F we have

$$M(F) = \prod_{i=0}^{m-1} F(\omega_m^i) = \prod_{d|m} \prod_{\substack{j=1 \\ (j,d)=1}}^{d} F(\omega_d^j) = \prod_{d|m} N_d,$$

where $N_d = N_{\mathbb{Q}(\omega_d)/\mathbb{Q}}(F(\omega_d))$.

Now, let $F(x) = \frac{x^a-1}{x-1} - k(x^m - 1)$. Then for $d = 1$, $N_1 = F(1) = a$. For $d|m$, $d > 1$ we have $F(\omega_d) = \frac{\omega_d^a-1}{\omega_d-1}$, an element of norm 1, that is, $N_d = 1$. This follows in the same manner as Proposition 2.12.1 since $(a, d) = 1$ and therefore $\omega_d^a - 1$ is a conjugate of $\omega_d - 1$, whence they have the same norm. Thus we obtain $M(F) = a \cdot 1 \cdots 1 = a$. □

2.13 Polynomials with Small Mahler Measure over $\mathbb{Z}_p^n$

Proposition 2.13.1. For any prime $p, n \in \mathbb{N}$ and $F(x_1, \ldots, x_n) = \displaystyle\prod_{k=1}^{n} \left(\frac{x_k^p - 1}{x_k - 1} \right) - 1 = \prod_{k=1}^{n} \Phi(x_k) - 1$, we have $|M(F)| = p^n - 1$.

Proof. We have

$$\begin{aligned} M(F) &= \prod_{j_1=0}^{p-1} \prod_{j_2=0}^{p-1} \cdots \prod_{j_n=0}^{p-1} F(\omega^{j_1}, \omega^{j_2}, \ldots, \omega^{j_n}) \\ &= \prod_{j_1=0}^{p-1} \prod_{j_2=0}^{p-1} \cdots \prod_{j_n=0}^{p-1} \left(\Phi(\omega^{j_1}) \cdots \Phi(\omega^{j_n}) - 1 \right). \end{aligned}$$

Now if all $j_i = 0$ then the term is $\Phi(1)^n - 1$, while if some $j_i \neq 0$ then the term is -1, and so we get

$$\begin{aligned} M(F) &= \left(\Phi(1)^n - 1\right)(-1)^{p^n-1} \\ &= \left(p^n - 1\right)(-1)^{p^n-1}. \end{aligned}$$

Therefore we get that,

$$|M(F)| = p^n - 1.$$

□

Chapter 3

Main Result

In this chapter we discuss and prove the main result of our work. We define, for any odd prime p and $n \in \mathbb{N}$,

$$\mathcal{M}_n := \min\{a^{p^{n-1}} (\bmod\ p^n) \mid 2 \leq a \leq p-1\}. \tag{3.1}$$

We may restrict a to a value less than p, since if $a \equiv b \pmod{p}$ then $a^{p^{n-1}} \equiv b^{p^{n-1}} \pmod{p^n}$, by Proposition 2.11.3. Let us first observe that one can also define $\mathcal{M}_n$ in the following equivalent manner.

Proposition 3.0.2. For any odd prime p and $n \in \mathbb{N}$, we have

$$\mathcal{M}_n = \min\{x \in \mathbb{Z} : x > 1, x^{p-1} \equiv 1 \pmod{p^n}\}.$$

Proof. Let $2 \leq a \leq p-1$. Then $a^{p^{n-1}} \not\equiv 1 \pmod{p^n}$, since $a^{p^{n-1}} \equiv a \not\equiv 1 \pmod{p}$. Also,

$$(a^{p^{n-1}})^{p-1} \equiv a^{\phi(p^n)} \equiv 1 \pmod{p^n},$$

by Euler's Theorem.

Conversely, if $x > 1$ and $x^{p-1} \equiv 1 \pmod{p^n}$ then

$$x^{\frac{\phi(p^n)}{(\phi(p^n),p^{n-1})}} \equiv x^{p-1} \equiv 1 \pmod{p^n},$$

and therefore x is a p^{n-1}-th power $\pmod{p^n}$ by Proposition 2.11.1. Since $x \not\equiv 1 \pmod{p^n}$ it follows that $x \equiv a^{p^{n-1}} \pmod{p^n}$ for some $2 \leq a \leq p-1$. □

Recall the definition,

$$\lambda(\mathbb{Z}_p^n) = \frac{1}{p^n}\{\log|M(F)| : \ |M(F)| > 1\}.$$

Recall also the trivial bound

$$\frac{1}{p^n}\log(2) \leq \lambda(\mathbb{Z}_p^n) \leq \frac{1}{p^n}\log(p^n - 1). \tag{3.2}$$

Our main theorem is the following.

Theorem 3.0.1. *For $n \geq 2$*

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

For $n \geq 1$ and any prime $p \geq 3$,

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

where $\mathcal{M}_n$ is defined as in (3.1).

Corollary 3.0.1. *For $n \geq 1$ we have*

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

Proof. In view of the preceding proposition, $\mathcal{M}_n$ is the minimal solution of the congruence $x^2 \equiv 1 \pmod{3^n}$ with $x > 1$. Since the solutions of this congruence are $x \equiv \pm 1 \pmod{3^n}$, it is plain that the minimal solution with $x > 1$ is $x \equiv 3^n - 1$, and thus $\mathcal{M}_n = 3^n - 1$. The corollary now follows from the main theorem. □

In particular we see that the trivial upper bound in (3.2) is attained for $p = 2$ and $p = 3$.

3.1 The Congruence Lemmas

Let us recall that for $F \in \mathbb{Z}[x]$, and $G = \mathbb{Z}_p$, we define

$$M_G(F) = \prod_{j=0}^{n} F(\omega^j),$$

where $\omega = e^{2\pi i/p}$.

Lemma 3.1.1. *For $F \in \mathbb{Z}[x]$, p a prime, and $G = \mathbb{Z}_p$, we have*

$$M_G(F) \equiv F(1) \pmod{p}. \tag{3.3}$$

Proof. We have

$$M_G(F) = \prod_{j=0}^{p-1} F(\omega^j) = N\left(F(\omega)\right) F(1).$$

Then by Proposition 2.10.6 we get that $M_G(F) \equiv F(1)^p \pmod{p}$. Hence by Fermat's Little Theorem we have $M_G(F) \equiv F(1) \pmod{p}$.

□

This lemma generalizes to n-dimensions as follows.

Lemma 3.1.2. *For $n \in \mathbb{N}$, $F \in \mathbb{Z}[x_1, \ldots, x_n]$ and $G = \mathbb{Z}_p^n$, we have*

$$M_G(F) \equiv F(1, \ldots, 1)^{p^{n-1}} \pmod{p^n}. \tag{3.4}$$

Proof. The proof is by induction on the dimension n. For convenience we put $M_n(F) = M_G(F)$ for $G = \mathbb{Z}_p^n$. The case $n = 1$ is just the preceding lemma. Suppose now that

$$M_t(F) \equiv F(1, \ldots, 1)^{p^{t-1}} \pmod{p^t},$$

for all $t < n$, and any polynomial F in t-variables over $\mathbb{Z}$. We define a polynomial $G(\mathbf{x}) \in \mathbb{Z}[x_1, \ldots, x_n]$ by

$$G(\mathbf{x}) = G(x_1, \ldots, x_n) := \prod_{k_1=0}^{p-1} \cdots \prod_{k_n=0}^{p-1} F(x_1^{k_1}, \ldots, x_n^{k_n}). \tag{3.5}$$

By expanding the product and gathering like monomials, we can write

$$G(\mathbf{x}) = \sum_{\ell_1 < C_1, \ldots, \ell_n < C_n} b(\ell_1, \ldots, \ell_n) x_1^{\ell_1} \cdots x_n^{\ell_n},$$

for some positive integers $C_1, \ldots, C_n$, and coefficients $b(\ell_1, \ldots, \ell_n) \in \mathbb{Z}$.

Now $x_r^p \equiv 1 \pmod{x_r^p - 1}$ for $1 \leq r \leq n$, and so we can write

$$G(\mathbf{x}) = \sum_{0 \leq \ell_1, \ldots, \ell_n \leq p-1} a(\ell_1, \ldots, \ell_n) x_1^{\ell_1} \cdots x_n^{\ell_n} + J_1(x_1, \ldots, x_n)(x_1^p - 1) + \ldots \\ + J_n(x_1, \cdots, x_n)(x_n^p - 1), \tag{3.6}$$

for some integers $a(\ell_1, \ldots, \ell_n)$ and polynomials $J_1(x_1, \ldots, x_n), \ldots, J_n(x_1, \ldots, x_n)$ over $\mathbb{Z}$.

Now, consider the evaluation of

$$G(\omega^{j_1}, \ldots, \omega^{j_n})$$

where $j_r \in \mathbb{Z}$ and $0 \leq j_r \leq p-1$ for $1 \leq r \leq n$. First we observe that by (3.6) we have

$$G(\omega^{j_1}, \ldots, \omega^{j_n}) = \sum_{l_1=0}^{p-1} \cdots \sum_{l_n=0}^{p-1} a(l_1, \ldots, l_n) \omega^{j_1 l_1} \cdots \omega^{j_n l_n}. \tag{3.7}$$

Next we go back to the Definition 3.5 to evaluate the same quantity.

<u>Case i:</u> Suppose that $j_r = 0$ for $1 \leq r \leq n$. Then we have by 3.5,

$$G(1, \ldots, 1) = F(1, \ldots, 1)^{p^n} \equiv F(1, \ldots, 1)^{p^{n-1}} \pmod{p^n}, \tag{3.8}$$

by Euler's Theorem.

<u>Case ii:</u> Suppose that $j_r \neq 0$ for $1 \leq r \leq n$. Then

$$\begin{aligned} G(\omega^{j_1}, \ldots, \omega^{j_n}) &= \prod_{k_1=0}^{p-1} \cdots \prod_{k_n=0}^{p-1} F(\omega^{j_1 k_1}, \ldots, \omega^{j_n k_n}) \\ &= \prod_{k_1=0}^{p-1} \cdots \prod_{k_n=0}^{p-1} F(\omega^{k_1}, \ldots, \omega^{k_n}) \\ &= M_n(F) \end{aligned} \tag{3.9}$$

<u>Case iii:</u> Suppose that $j_r = 0$ for exactly L values of r, for some L with $1 \leq L < n$. Without loss of generality say that

$$j_1 = \cdots = j_L = 0, \; j_{L+1} \neq 0, \ldots, j_n \neq 0.$$

Then

$$\begin{aligned} G(1, \ldots, 1, \omega^{j_{L+1}}, \ldots, \omega^{j_n}) &= \prod_{k_1=0}^{p-1} \cdots \prod_{k_n=0}^{p-1} F(1, \ldots, 1, \omega^{j_{L+1} k_{L+1}}, \ldots, \omega^{j_n k_n}) \\ &= \left(\prod_{k_{L+1}=0}^{p-1} \cdots \prod_{k_n=0}^{p-1} F\left(1, \ldots, 1, \omega^{k_{L+1}}, \ldots, \omega^{k_n}\right) \right)^{p^L} \\ &= M_{n-L}\left(F\left(1, \ldots, 1, x_{L+1}, \ldots, x_n\right)\right)^{p^L}. \end{aligned}$$

Now by the induction hypothesis we have,

$$M_{n-L}\left(F\left(1,\ldots,1,x_{L+1},\ldots,x_n\right)\right)=F(1,\ldots,1)^{p^{n-L-1}}+kp^{n-L}$$

for some integer k. Therefore

$$\begin{aligned}G(1,\ldots,1,\omega^{j_{L+1}},\ldots,\omega^{j_n})&=\left(F(1,\ldots,1)^{p^{n-L-1}}+kp^{n-L}\right)^{p^L}\\&=F(1,\ldots,1)^{p^{n-1}}+kp^nF(1,\ldots,1)^{p^{n-1}-1}+\cdots\\&\equiv F(1,\ldots,1)^{p^{n-1}}\pmod{p^n},\end{aligned}$$

the latter step following from Proposition 2.10.7. In summary, we have seen that

$$G(\omega^{j_1},\ldots,\omega^{j_n})\equiv F(1,\ldots,1)^{p^{n-1}}\pmod{p^n},\quad\text{if some } j_i\equiv 0\pmod{p},\tag{3.10}$$

and

$$G(\omega^{j_1},\ldots,\omega^{j_n})=M_n(F),\quad\text{if no } j_i\equiv 0\pmod{p}.\tag{3.11}$$

By (3.7) we have,

$$\begin{aligned}S:&=\sum_{j_1=0}^{p-1}\cdots\sum_{j_n=0}^{p-1}G(\omega^{j_1},\ldots,\omega^{j_n})\\&=\sum_{\ell_1=0}^{p-1}\cdots\sum_{\ell_n=0}^{p-1}a(\ell_1,\ldots,\ell_n)\ \sum_{j_1=0}^{p-1}\cdots\sum_{j_n=0}^{p-1}\omega^{j_1\ell_1}\cdots\omega^{j_n\ell_n}\\&=a(0,\ldots,0)\sum_{j_1=0}^{p-1}\cdots\sum_{j_n=0}^{p-1}1+\sum_{(\ell_1,\ldots,\ell_n)\neq(0,\ldots,0)}a(\ell_1,\ldots,\ell_n)\sum_{j_1=0}^{p-1}\omega^{j_1\ell_1}\cdots\sum_{j_n=0}^{p-1}\omega^{j_n\ell_n}.\end{aligned}$$

Thus, since $\sum_{j_i=0}^{p-1}\omega^{j_i\ell_i}=0$ for $0<\ell_i<p$, we obtain

$$S=a(0,\ldots,0)p^n\equiv 0\pmod{p^n}.\tag{3.12}$$

On the other hand, by (3.5) we have

$$S=\sum_{\text{some } j_i=0}G(\omega^{j_1},\ldots,\omega^{j_n})+\sum_{\text{no } j_i=0}G(\omega^{j_1},\ldots,\omega^{j_n}),$$

and so by (3.10) and (3.11) we get,

$$\begin{aligned} S &\equiv F(1,\dots,1)^{p^{n-1}}(p^n-(p-1)^n)+M_n(F)(p-1)^n \pmod{p^n} \\ &\equiv (p-1)^n(M_n(F)-F(1,\dots,1)^{p^{n-1}}) \pmod{p^n}. \end{aligned}$$

Since $S \equiv 0 \pmod{p^n}$ by (3.12) we get,

$$F(1,\dots,1)^{p^{n-1}} \equiv M_n(F) \pmod{p^n},$$

since $\gcd(p-1,p^n)=1$. □

3.2 Construction of a Polynomial F with Given Mahler Measure

In the previous section we showed that for any polynomial $F \in \mathbb{Z}[x_1,\dots,x_n]$, $M_n(F)$ is congruent to a p^{n-1}-th power $\pmod{p^n}$. Here we show conversely, that given any p^{n-1}-th power $\pmod{p^n}$ that is relatively prime to p, there exists a polynomial F with $M_n(F)$ taking on this value.

Lemma 3.2.1. *For any prime power p^n and integers k,a with $p \nmid a$, $a>0$, there exists a polynomial $F(x_1,\dots,x_n) \in \mathbb{Z}[x_1,\dots,x_n]$ with*

$$M_n(F)=a^{p^{n-1}}-kp^n. \tag{3.13}$$

Proof. Let p be a prime, $n,a \in \mathbb{N}$ and $k \in \mathbb{Z}$. We shall generate a sequence of polynomials $H_1(x),\dots,H_{n-1}(x) \in \mathbb{Z}[x]$ such that

$$(1+x+\cdots+x^{a-1})^{p^l} \equiv a^{p^{l-1}}+p^lH_l(x) \pmod{x^p-1}, \tag{3.14}$$

for $1 \le l \le n-1$.

Since $x^p \equiv 1 \pmod{x^p-1}$ we have for some $H_1(x) \in \mathbb{Z}[x]$,

$$\begin{aligned} (1+x+x^2+\cdots+x^{a-1})^p &= 1^p+x^p+x^{2p}+\cdots+x^{p(a-1)}+pH_1(x) \qquad (3.15) \\ &\equiv (1+1+\cdots+1)+pH_1(x) \pmod{x^p-1} \\ &\equiv a+pH_1(x) \pmod{x^p-1}, \end{aligned}$$

thus establishing (3.14) for the case $l=1$. Now by raising both sides to the p-th power we generate $H_2(x) \in \mathbb{Z}[x]$ as follows:

$$\begin{aligned}(1+x+x^2+\cdots+x^{a-1})^{p^2} &\equiv (a+pH_1(x))^p \pmod{x^p-1}\\ &\equiv a^p + p^2\left(H_1(x)a^{p-1}+\cdots\right) \pmod{x^p-1}\\ &\equiv a^p+p^2H_2(x) \pmod{x^p-1},\end{aligned}$$

for some $H_2(x) \in \mathbb{Z}[x]$. We generate the remaining $H_j(x)$ in the same manner. Suppose that $H_1(x), \ldots, H_j(x)$ have been constructed to satisfy (3.14). Then

$$\begin{aligned}(1+x+x^2+\cdots+x^{a-1})^{p^{j+1}} &\equiv \left(a^{p^{j-1}}+p^jH_j(x)\right)^p \pmod{x^p-1}\\ &\equiv a^{p^j}+p^{j+1}\left(H_j(x)a^{p^j-1}+\cdots\right) \pmod{x^p-1}\\ &\equiv a^{p^j}+p^{j+1}H_{j+1}(x) \pmod{x^p-1},\end{aligned}$$

for some $H_{j+1}(x) \in \mathbb{Z}[x]$.

From (3.14) we immediately obtain the identity

$$(1+x+\cdots+x^{a-1})^{p^l} = a^{p^{l-1}} + p^lH_l(x) + J_l(x)(x^p-1), \tag{3.16}$$

for some $J_l \in \mathbb{Z}[x]$. Putting $x=1$ in (3.16) yields

$$a^{p^l} = a^{p^{l-1}} + p^lH_l(1). \tag{3.17}$$

Putting $l=j+1$, $x=\omega$ in (3.16) yields

$$(1+\omega+\cdots+\omega^{a-1})^{p^l} = a^{p^{l-1}} + p^lH_l(\omega). \tag{3.18}$$

We define

$$F(x_1,\ldots,x_n) := (1+x_1+\cdots+x_1^{a-1}) + \sum_{j=1}^{n-1} H_j(x_{j+1})\prod_{i=1}^{j}\Phi(x_i) - k\prod_{i=1}^{n}\Phi(x_i), \tag{3.19}$$

where $\Phi(x) = 1+x+\cdots+x^{p-1}$. We claim that for this choice of F we have

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

thus establishing the lemma. To prove the claim, recall that by Proposition 2.9.1, $M_n(F)$ can be expressed as a product

$$M_n(F) = F(1, 1, \dots, 1)N_1N_2 \dots N_I, \tag{3.20}$$

where the N_i are norms of elements of the form $F(\omega^{j_1}, \dots, \omega^{j_n})$ with the j_i not all 0. We turn to the evaluation of $F(\omega^{j_1}, \dots, \omega^{j_n})$ for different choices of j_i. Suppose first that j_1 is not zero. Then, by the definition of F we have

$$F(\omega^{j_1}, \dots, \omega^{j_n}) = 1 + \omega^{j_1} + \dots + \omega^{j_1(a-1)}, \tag{3.21}$$

which, by Proposition 2.7.3, is an element of norm 1, that is

$$N(F(\omega^{j_1}, \dots, \omega^{j_n})) = 1. \tag{3.22}$$

Next, suppose that $j_1 = 0$ but not all j_i are zero. Say $j_1 = j_2 = \dots = j_l = 0$, $j_{l+1} \neq 0$, for some l, $1 \leq l < n$. Then, using the definition of F we have,

$$\begin{aligned} F(\omega^{j_1}, \dots, \omega^{j_n}) &= F(1, 1, \dots, 1, \omega^{j_{l+1}}, \dots, \omega^{j_n}) \\ &= a + \sum_{j=1}^{l-1} H_j(1) \prod_{i=1}^{j} \Phi(1) + H_l(\omega^{j_{l+1}}) \prod_{i=1}^{l} \Phi(1) - k \cdot 0 \\ &= a + pH_1(1) + \dots + p^{l-1}H_{l-1}(1) + p^l H_l(\omega^{j_{l+1}}). \end{aligned}$$

Now, by (3.17), we have $p^j H_j(1) = a^{p^j} - a^{p^{j-1}}$, and so the latter sum is a telescoping sum that simplifies to

$$a^{p^{l-1}} + p^l H_l(\omega^{j_{l+1}}) = \left(1 + \omega^{j_{l+1}} + \dots + \omega^{j_{l+1}(a-1)}\right)^{p^l},$$

the latter equality following from (3.18). We see again by Proposition 2.7.3, that the latter quantity is a unit in $\mathbb{Z}[\omega]$ of norm 1 and thus we again have (3.22). We now can conclude that all of the N_i in (3.20) are equal to 1.

Finally, if all of the j_i are zero, then we just have

$$\begin{aligned} F(1, \dots, 1) &= a + pH_1(1) + \dots + p^{n-1}H_{n-1}(1) - kp^n \\ &= a^{p^{n-1}} - kp^n \end{aligned} \tag{3.23}$$

by (3.17). Therefore, by (3.20) we conclude that

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

□

Example 3.2.1. For the case $a = 1$, the polynomial constructed in the proof is just

$$F(x_1, \dots, x_n) = 1 - k \prod_{i=1}^{n} \Phi(x_i),$$

since the H_i are all zero in this case. We see that for this polynomial we have

$$M_n(F) = 1 - kp^n.$$

By taking $k = 1$, we get a polynomial with $|M_n(F)| = p^n - 1$.

Example 3.2.2. Let us find the polynomial that gives the minimal value for $|M(F)|$ for the group $\mathbb{Z}_5 \times \mathbb{Z}_5$. First we figure out a and k values. So for $\mathcal{M}_2$ and $p = 5$ the minimum 5-th power $\pmod{25}$ is attained by $2^5 \equiv 7 \pmod{25}$. Therefore take $a = 2$. Next we choose $k = 1$ so that $2^5 - k \cdot 5^2 = 7$, and thus $|M(F)| = 7$ for the polynomial F defined in (3.19). To obtain F we plug in $p = 5$ and $a = 2$ in (3.15) to get

$$(1 + x)^5 = 1 + x^5 + 5H_1(x).$$

Therefore we get

$$H_1(x) = x + 2x^2 + 2x^3 + x^4$$

Finally by (3.19) we get,

$$\begin{aligned}
F(x_1, x_2) &= 1 + x_1 + H_1(x_2)\Phi(x_1) - 1 \cdot \Phi(x_1)\Phi(x_2) \\
&= 1 + x_1 + \left(x_2 + 2x_2^2 + 2x_2^3 + x_2^4\right)\left(1 + x_1 + x_1^2 + x_1^3 + x_1^4\right) \\
&\quad - \left(1 + x_1 + x_1^2 + x_1^3 + x_1^4\right)\left(1 + x_2 + x_2^2 + x_2^3 + x_2^4\right) \\
&= 1 + x_1 - \left(1 + x_1 + x_1^2 + x_1^3 + x_1^4\right)\left(x_2^2 + x_2^3 - 1\right).
\end{aligned}$$

We see that this polynomial is different than what we got using the computer in Example 2.4.1.

3.3 Proof of Theorem 3.0.1

First we consider the case $p = 2$. By Lemma 3.1.2 we have that for any $F \in \mathbb{Z}[x_1, \ldots, x_n]$, $M_n(F) \equiv a^{2^{n-1}} \pmod{2^n}$ for some integer a. Now if a is even, then $a^{2^{n-1}} \equiv 0 \pmod{2^n}$ since $2^{n-1} \geq n$ for any $n \in \mathbb{N}$. Thus, the minimal possible nonzero value for $|M_n(F)|$ is 2^n. If a is odd, then $a^{2^{n-1}} \equiv 1 \pmod{2^n}$ by Proposition 2.11.3, and thus the minimal possible value for $|M_n(F)|$ is $|1 - 2^n| = 2^n - 1$. In Example 3.2.1 we saw that this minimal value was actually attained by the polynomial

$$F(x_1, \ldots, x_n) = 1 - (x_1 + 1) \cdots (x_n + 1).$$

Next we consider the case of odd p. Now if $p \mid M_n(F)$ then $p \mid N_r$ for some r or $p \mid F(1, \ldots, 1)$, since $M_n(F) = F(1, \ldots, 1) \prod_{i=1}^{I} N_i$. Now since $\omega \equiv 1 \pmod{\pi}$ for any $(j_1, \ldots, j_n)$ we have $F(\omega^{j_1}, \ldots, \omega^{j_n}) \equiv F(1, \ldots, 1) \pmod{\pi}$, which implies $N_i \equiv F(1, \ldots, 1)^{p-1} \pmod{p}$ for any i. So we get that $p \mid F(1, \ldots, 1)$ and $p \mid N_i$ for all i. Therefore $p^{\frac{p^n-1}{p-1}+1} | M_n(F)$, hence $M_n(F) \geq p^{\frac{p^n-1}{p-1}+1}$. Therefore we can ignore these values of $M_n(F)$ which are divisible by p since those values are larger than the trivial upper bound $p^n - 1$.

By Lemma 3.1.2 we have that for any polynomial $F \in \mathbb{Z}[x_1, \ldots, x_n]$, $M_n(F)$ is a p^{n-1}-th power $\pmod{p^n}$. On the other hand, Lemma 3.2.1 shows that given any integer relatively prime to p that is a p^{n-1}-th power $\pmod{p^n}$, there exists a polynomial $F \in \mathbb{Z}[x_1, \ldots, x_n]$ with $M_n(F)$ equal to that value. Thus the minimal value of $|M_n(F)| > 1$ is just the minimal p^{n-1}-th power $\pmod{p^n}$ greater than 1. (We note that since p is odd, the p^{n-1}-th powers are symmetric about 0, and so we can restrict our attention to the minimal positive p^{n-1}-th power.)

Chapter 4

Heilbronn sums and the Estimation of $\mathcal{M}_n$

The second part of my thesis is devoted to the estimation of the quantity $\mathcal{M}_n$ defined in (3.1),

$$\mathcal{M}_n := \min\{a^{p^{n-1}} (\mathrm{mod}\ p^n) \mid 2 \le a \le p-1\}.$$

Putting this estimate together with Theorem 3.0.1 yields an explicit bound for $\lambda(\mathbb{Z}_p^n)$. Let K be the group of p^{n-1} powers (mod p^n) viewed as integers between 1 and $p^n - 1$. The first approach to estimating $\mathcal{M}_n$ is to let I be an interval $I := [2, \cdots, N] \subseteq \mathbb{Z}_p^n$, and to count the number of points in $K \cap I$ using a classic method of exponential sums. Let $e_{p^n}(x) := \exp\left(\frac{2\pi i x}{p^n}\right)$, for $x \in \mathbb{Z}_{p^n}$, $H_{p^n}(y)$ denote the n-th order Heilbronn exponential sum

$$H_{p^n}(y) := \sum_{x=0}^{p-1} e_{p^n}\left(yx^{p^{n-1}}\right),$$

and

$$\mathcal{H}_{p^n} := \max_{y \in \mathbb{Z}_{p^n} \setminus \{0\}} |H_{p^n}(y)|.$$

We prove the following estimate:

Theorem 4.0.1. *For any prime power p^n and interval $I = [2, \cdots, N]$ we have*

$$|K \cap I| = \frac{N}{p^{n-1}} + O\left(\mathcal{H}_{p^n} \log(p^n)\right).$$

In particular we deduce that if $N \gg p^{n-1}\mathcal{H}_{p^n} \log p^n$, then $|K \cap I| > 0$. We can remove the $\log(p^n)$ factor by using a weighted count. In this manner we will establish Theorem 4.3.1 below and deduce that $|K \cap I| > 0$, provided $N \geq p^{n-1}\mathcal{H}_{p^n}$. In particular we obtain

Theorem 4.0.2. *For any odd prime power p^n,*

$$\mathcal{M}_n \leq 2p^{n-1}\mathcal{H}_{p^n}. \tag{4.1}$$

The first nontrivial estimate for $\mathcal{H}_{p^n}$ was made by Heath-Brown [9] for the case $n = 2$, where he established $\mathcal{H}_{p^2} \ll p^{11/12} \log p$. Subsequent improvements were made in the $n = 2$ case by Heath-Brown & Konyagin [10], $\mathcal{H}_{p^2} \ll p^{7/8}$; Shkredov [11], $\mathcal{H}_{p^2} \ll p^{59/68} \log^{5/34} p$; and Shkredov [6], $\mathcal{H}_{p^2} \ll p^{31/36} \log^{1/6} p$. Using the latter bound, we deduce from Theorem 4.0.2 that $\mathcal{M}_2 \ll p^{67/36} \log^{1/6} p$.

For $n \geq 3$ Malykhin [12] showed that $\mathcal{H}_{p^n} \ll p^{1-\frac{1}{32\cdot 5^{n-3}}}$. Using Malykhin's estimate [12] for the higher order Heilbronn sums we get that

$$\mathcal{M}_n \ll p^{n-\frac{1}{32\cdot 5^{n-3}}},$$

for $n \geq 3$. Thus by the conclusion of Theorem 3.0.1, for $n = 2$, we have that for any odd prime power p^n,

$$\lambda(\mathbb{Z}_p^2) = \frac{1}{p^2}\log(\mathcal{M}_2) \leq \frac{67}{36} \cdot \frac{\log p}{p^2} + O\left(\frac{\log\log p}{p^2}\right),$$

and for $n \geq 3$,

$$\lambda(\mathbb{Z}_p^n) = \frac{1}{p^n}\log(\mathcal{M}_n) \leq \left(n - \frac{1}{32\cdot 5^{n-3}}\right)\frac{\log p}{p^n} + O\left(\frac{1}{p^n}\right).$$

4.1 Proof of Theorem 4.0.1

Let I be the interval

$$I := [b+1, b+2, \ldots, b+B] \subseteq \mathbb{Z}_{p^n}$$

of cardinality $|I| = B$, and 1_I denote the characteristic function of I. Then 1_I has a Fourier expansion

$$1_I(x) = \sum_{y=0}^{p^n-1} a(y) e_{p^n}(yx) \tag{4.2}$$

where for $y \in \mathbb{Z}_{p^n}$,

$$a(y) = \frac{1}{p^n} \sum_{x=0}^{p^n-1} 1_I(x) e_{p^n}(-yx), \tag{4.3}$$

the formula for $a(y)$ following from the basic identity:

$$\sum_{x=0}^{p^n-1} e_{p^n}(yx) = \begin{cases} p^n, & \text{if } y \equiv 0 \pmod{p^n}; \\ 0, & \text{if } y \not\equiv 0 \pmod{p^n}. \end{cases}$$

In particular

$$a(0) = \frac{1}{p^n} B \tag{4.4}$$

and for $y \neq 0$,

$$|a(y)| = \frac{1}{p^n} \frac{\left|\sin(\frac{\pi y B}{p^n})\right|}{\left|\sin(\frac{\pi y}{p^n})\right|}.$$

We observe that

$$\sum_{y=1}^{p^n-1} |a(y)| = \sum_{0<|y|\leq \frac{p^n-1}{2}} \frac{1}{p^n} \frac{\left|\sin(\frac{\pi y B}{p^n})\right|}{\left|\sin(\frac{\pi y}{p^n})\right|} \ll \frac{1}{p^n} \sum_{0<|y|\leq \frac{p^n-1}{2}} \frac{1}{|y|/p^n} \ll \log(p^n).$$

Then

$$\begin{aligned} |K \cap I| :&= |\{x^{p^{n-1}} : 1 \leq x \leq p-1, x^{p^{n-1}} \in I\}| \\ &= \sum_{x=0}^{p-1} 1_I(x^{p^n-1}) \\ &= \sum_{x=0}^{p-1} \sum_{y=0}^{p^n-1} a(y) e_{p^n}\left(yx^{p^{n-1}}\right) \\ &= a(0)p + \sum_{y=1}^{p^{n-1}} a(y) \sum_{x=0}^{p-1} e_{p^n}\left(yx^{p^{n-1}}\right) \\ &= \frac{B}{p^{n-1}} + \sum_{y=1}^{p^{n-1}} a(y) \sum_{x=0}^{p-1} e_{p^n}\left(yx^{p^{n-1}}\right). \end{aligned}$$

Now to estimate the quantity $\sum_{y=1}^{p^n-1} a(y) \sum_{x=0}^{p-1} e_{p^n}\left(yx^{p^{n-1}}\right)$, we write

$$\begin{aligned}\left|\sum_{y=1}^{p^n-1} a(y) \sum_{x=0}^{p-1} e_{p^n}\left(yx^{p^{n-1}}\right)\right| &\leq \sum_{y=1}^{p^n-1} |a(y)| \max_{y\in\mathbb{Z}_{p^n}\setminus\{0\}} \left|\sum_{x=0}^{p-1} e_{p^n}\left(yx^{p^{n-1}}\right)\right| \\ &= \max_{y\in\mathbb{Z}_{p^n}\setminus\{0\}} |H_{p^n}(y)| \sum_{y=1}^{p^n-1} |a(y)| \\ &= \mathcal{H}_{p^n} \sum_{y=1}^{p^n-1} |a(y)| \\ &= \mathcal{H}_{p^n} \log(p^n). \end{aligned} \tag{4.5}$$

So we get that

$$|K \cap I| = \frac{B}{p^{n-1}} + O\left(\mathcal{H}_{p^n} \log(p^n)\right), \tag{4.6}$$

which establishes Theorem 4.0.1.

4.2 Weighted Counting

The same proof given in the previous section can work just as well for any weighted function $\alpha(x)$ on I. Indeed, we shall prove the following.

Theorem 4.2.1. *For any function $\alpha:\ \mathbb{Z}_{p^n} \to \mathbb{C}$ with Fourier coefficients $a(y)$ we have*

$$\sum_{x=0}^{p-1} \alpha\left(x^{p^{n-1}}\right) = \frac{1}{p^{n-1}} \sum_{x=0}^{p^n-1} \alpha(x) + Error \tag{4.7}$$

where $|Error| \leq \mathcal{H}_{p^n} \sum_{y=1}^{p^n-1} |a(y)|$.

Proof. Now $\alpha(x)$ has Fourier expansion,

$$\alpha(x) = \sum_{y=0}^{p^n-1} a(y) e_{p^n}(yx),$$

where for $y \in \mathbb{Z}_{p^n}$,

$$a(y) = \frac{1}{p^n} \sum_{x=0}^{p^n-1} \alpha(x) e_{p^n}(-yx).$$

In particular,

$$a(0) = \frac{1}{p^n} \sum_{x=0}^{p^n-1} \alpha(x). \tag{4.8}$$

So using the Fourier expansion of $\alpha(x)$ we get that,

$$\begin{aligned}\sum_{x=0}^{p-1} \alpha(x^{p^{n-1}}) &= \sum_{x=0}^{p-1} \sum_{y=0}^{p^{n-1}} a(y) e_{p^n}\left(yx^{p^{n-1}}\right) \\ &= a(0)p + \sum_{y=1}^{p^{n-1}} a(y) \sum_{x=0}^{p-1} e_{p^n}\left(yx^{p^{n-1}}\right) \\ &= \frac{1}{p^{n-1}} \sum_{x=0}^{p^n-1} \alpha(x) + Error,\end{aligned}$$

where $Error := \sum_{y=1}^{p^{n-1}} a(y) \sum_{x=0}^{p-1} e_{p^n}\left(yx^{p^{n-1}}\right)$. So

$$\begin{aligned}|Error| &\leq \max_{y \in \mathbb{Z}_{p^n} \setminus \{0\}} \left| \sum_{x=0}^{p-1} e_{p^n}\left(yx^{p^{n-1}}\right) \right| \sum_{y=1}^{p^n-1} |a(y)| \\ &= \max_{y \in \mathbb{Z}_{p^n} \setminus \{0\}} |H_{p^n}(y)| \sum_{y=1}^{p^n-1} |a(y)| \\ &= \mathcal{H}_{p^n} \sum_{y=1}^{p^n-1} |a(y)|.\end{aligned}$$

□

Letting $\alpha = 1_I$ and using the estimate $\sum_{y=0}^{p^n-1} |a(y)| \ll \log(p^n)$ gives us the result of the previous section:

$$|K \cap I| = \frac{1}{p^{n-1}} B + O\left(\mathcal{H}_n \log(p^n)\right).$$

4.3 The Weighted Count $1_J * 1_J$

We recall that for any complex valued functions, β, γ on $\mathbb{Z}_p^n$, the convolution of β and γ, denoted $\beta * \gamma$, is defined by

$$(\beta * \gamma)(x) := \sum_{\substack{u=0 \\ u+v=x}}^{p^n-1} \sum_{v=0}^{p^n-1} \beta(u)\gamma(v).$$

Observe that $I * I = 0$ outside $[2, 2N]$. In this section we apply Theorem 4.2.1 to the function $1_J * 1_J$ where $J = [1, 2, \ldots, N] \subseteq \mathbb{Z}_{p^n}$, with $N < \frac{p^n}{2}$. Then $1_J * 1_J$ has Fourier expansion

$$(1_J * 1_J)(x) = \sum_{y=0}^{p^n-1} a(y) e_{p^n}(yx), \tag{4.9}$$

where the coefficients $a(y)$ are determined by using the following lemma.

Lemma 4.3.1. *If $\beta, \gamma : \mathbb{Z}_p^n \to \mathbb{C}$ with Fourier coefficients $a_\beta(y), a_\gamma(y)$ respectively, then the Fourier coefficients of $\beta * \gamma$ are given by $a(y) = p^n a_\beta(y) a_\gamma(y)$.*

Proof.

$$\begin{aligned}
(\beta * \gamma)(x) :&= \sum_{\substack{u=0 \\ u+v=x}}^{p^n-1} \sum_{v=0}^{p^n-1} \beta(u)\gamma(v) \\
&= \sum_{u+v=x} \left(\sum_{y_1=0}^{p^n-1} a_\beta(y_1) e_{p^n}(uy_1) \right) \left(\sum_{y_2=0}^{p^n-1} a_\gamma(y_2) e_{p^n}(vy_2) \right) \\
&= \sum_{y_1=0}^{p^n-1} \sum_{y_2=0}^{p^n-1} a_\beta(y_1) a_\gamma(y_2) \sum_{u+v=x} e_{p^n}(uy_1 + vy_2) \\
&= \sum_{y_1=0}^{p^n-1} \sum_{y_2=0}^{p^n-1} a_\beta(y_1) a_\gamma(y_2) \sum_{u=0}^{p^n-1} e_{p^n}\left(uy_1 + (x-u)\, y_2\right) \\
&= \sum_{y_1=0}^{p^n-1} \sum_{y_2=0}^{p^n-1} a_\beta(y_1) a_\gamma(y_2) e_{p^n}(xy_2) \sum_{u=0}^{p^n-1} e_{p^n}\left(u\left(y_1 - y_2\right)\right) \\
&= p^n \sum_{\substack{y_1=0 \\ y_1=y_2}}^{p^n-1} \sum_{y_2=0}^{p^n-1} a_\beta(y_1) a_\gamma(y_2) e_{p^n}(xy_2) \\
&= \sum_{y=0}^{p^n-1} p^n a_\beta(y) a_\gamma(y) e_{p^n}(xy)
\end{aligned}$$

by taking $y = y_1 = y_2$. Thus we see that the Fourier coefficients of $\beta * \gamma$ are given by $a(y) = p^n a_\beta(y) a_\gamma(y)$. □

Thus for the function $1_J * 1_J$ we have $a(y) = p^n a_J^2(y)$. Now by Parseval's Identity, we have

$$\sum_{y=0}^{p^n-1} |a(y)| = p^n \sum_{y=0}^{p^n-1} |a_J(y)|^2 = p^n \left(\frac{1}{p^n} \sum_{x=0}^{p^n-1} |1_J|^2(x) \right) = \sum_{x=0}^{p^n-1} 1_J(x) = |J|.$$

Thus we have established the following: If $\alpha = 1_j * 1_J$, with Fourier coefficients $a(y)$, then

$$\sum_{y=0}^{p^{n-1}} |a(y)| = |J|. \tag{4.10}$$

Theorem 4.3.1. *For any odd prime power p^n and interval $J = [1, \cdots, N]$ we have*

$$\sum_{x=0}^{p-1} (1_J * 1_J)\left(x^{p^n-1}\right) = \frac{N^2}{p^{n-1}} + Error, \tag{4.11}$$

where $|Error| < N\mathcal{H}_{p^n}$.

We will deduce this from Theorem 4.2.1.

Proof. By letting $\alpha(x) = (1_J * 1_J)(x)$ in Theorem 4.2.1 we get

$$\begin{aligned}
\sum_{x=0}^{p^n-1} (1_J * 1_J)(x^{p^{n-1}}) &= \frac{1}{p^{n-1}} \sum_{x=0}^{p^n-1} 1_J * 1_J(x) + Error \\
&= \frac{1}{p^{n-1}} \sum_{x=0}^{p^n-1} \sum_{\substack{u\in J \\ u+v=x}} \sum_{v\in J} 1 + Error \\
&= \frac{1}{p^{n-1}} N^2 + Error \\
&= \frac{1}{p^{n-1}} N^2 + Error,
\end{aligned}$$

where

$$|Error| = \mathcal{H}_{p^n} \sum_{y=1}^{p^n-1} |a(y)| < \mathcal{H}_{p^n} \sum_{y=0}^{p^n-1} |a(y)| = N\mathcal{H}_{p^n}$$

the latter step following from (4.10).

□

Proof of Theorem 4.0.2. We conclude from Theorem 4.3.1 that $(1_J * 1_J)(x^{p^{n-1}}) > 0$ for some $x \in \mathbb{Z}_{p^n}$, and consequently $x^{p^{n-1}} \in [2, \ldots, 2N]$ for some $x \in \mathbb{Z}_{p^n}$, if

$$\frac{N}{p^{n-1}} \geq \mathcal{H}_{p^n},$$

that is

$$N \geq p^{n-1}\mathcal{H}_{p^n}.$$

Hence

$$\mathcal{M}_n \leq 2N \leq 2p^{n-1}\mathcal{H}_{p^n}.$$

□

Table 4.1 below gives the smallest non-trivial positive solutions to $x^{p-1} \equiv 1 \pmod{p^n}$, for $p < 100$ and $n \leq 6$. Values in this table were calculated using Maple. The code for the program is given in Appendix A.

Table 4.1: *Sample $\mathcal{M}_n$ values for small p and n*

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

Bibliography

[1] D. De Silva and C. Pinner. The Lind-Lehmer constant for $\mathbf{z}_p^n$. *Proc. AMS*, to appear.

[2] D. Lind. Lehmer's problem for compact abelian groups. *Proc. AMS*, 133:1411–1416, 2005.

[3] N. Kaiblinger. On the Lehmer constant of finite cyclic groups. *Acta Arith.*, 142:79–84, 2010.

[4] V. Pigno and C. Pinner. The Lind-Lehmer constant for cyclic groups of order less than 892,371,480. *Ramanujan J.*, to appear.

[5] W. M. Lawton. A problem of Boyd concerning geometric means of polynomials. *J. Number Theory*, 16:356–362, 1983.

[6] I. D. Shkredov. New bounds for Heilbronn's exponential sum. *arXiv:1302.3839v1 [math.NT]*, 2013.

[7] J. B. Conway. *Functions of one complex variable.* New York; Springer-Verlag, 1978.

[8] C. Pinner and J. Vaaler. Polynomials with Lind Mahler measure one. *Preprint.*

[9] D. R. Heath-Brown. An estimate for Heilbronn's exponential sum. *Analytic number theory: Proceedings of a conference in honor of Heini Halberstam*, pages 451–463, 1996.

[10] D. R. Heath-Brown and S. V. Konyagin. New bounds for Gauss sums derived from k-th powers, and for Heilbronn's exponential sum. *Quart. J. Math.*, 51:221–35, 2000.

[11] I. D. Shkredov. On Heilbronn's exponential sum. *arXiv:1208.6124v1 [math.NT]*, 2012.

[12] Yu. V. Malykhin. Estimates of trigonometric sums modulo p^r. *Mathematical Notes*, 80:748–752, 2006.

Appendix A

Program 1

```
for r from 2 to 6 do
 n:=r:
 p:=2:
 for q from 1 to 24 do
         p:=nextprime(p):
         d:=p^n:
         y:=p^n-1:
                 for j from 2 to (p-1) do
                 v:=j^(p^(n-1)) mod p^(n):
                 d:=min(v,d):
                 y:=min(d,y):
                 end do;
         lprint(p,d);
         d:=p^n:
 end do:
end do:
```

Appendix B

Program 2

```
#include ”stdafx.h”
#include <iostream>
#include <cmath>
#include <math.h>
#include <iomanip>

const double PI = std::atan(1.0)*4;

class complex
{
   private:
          double real;      // Real Part
          double imag;      //  Imaginary Part

   public:
          complex(double,double);
          complex(complex&);
          complex operator +(complex);
          complex operator -(complex);
          complex operator *(complex);
          complex operator /(complex);
                  complex operator ^(int);
          complex getconjugate();
          complex getreciprocal();
          double getmodulus();
          void setdata(double,double);
          void getdata();
          double getreal();
```

```
        double getimaginary();
        bool operator ==(complex);
        void operator =(complex);
        friend std::ostream& operator <<(std::ostream &s,complex &c);
};

//{{NO_DEPENDENCIES}}
// Microsoft Visual C++ generated include file.
// Used by app.rc


// stdafx.h : include file for standard system include
// files, or project specific include files that are
// used frequently, but are changed infrequently
//

#pragma once

// TODO: reference additional headers your program
//requires here



#include ”stdafx.h”

using namespace System;
using namespace System::Reflection;
using namespace System::Runtime::CompilerServices;
using namespace System::Runtime::InteropServices;
using namespace System::Security::Permissions;

//
// General Information about an assembly is controlled
// through the following set of attributes. Change
// these attribute values to modify the information
//associated with an assembly.
//
[assembly:AssemblyTitleAttribute(”Test4”)];
[assembly:AssemblyDescriptionAttribute(””)];
[assembly:AssemblyConfigurationAttribute(””)];
[assembly:AssemblyCompanyAttribute(”Microsoft”)];
[assembly:AssemblyProductAttribute(”Test4”)];
[assembly:AssemblyCopyrightAttribute(”Copyright (c) Microsoft 2011”)];
```

```
[assembly:AssemblyTrademarkAttribute("")];
[assembly:AssemblyCultureAttribute("")];

//
// Version information for an assembly consists of the
// following four values:
//
//      Major Version
//      Minor Version
//      Build Number
//      Revision
//
// You can specify all the value or you can default the Revision
// and Build Numbers by using the '*' as shown below:

[assembly:AssemblyVersionAttribute("1.0.*")];

[assembly:ComVisible(false)];

[assembly:CLSCompliantAttribute(true)];

[assembly:SecurityPermission(SecurityAction::RequestMinimum,
        UnmanagedCode = true)];

// stdafx.cpp : source file that includes just the standard includes
// Test4.pch will be the pre-compiled header
// stdafx.obj will contain the pre-compiled type information

#include "stdafx.h"




#include "stdafx.h"
#include "complex.h"


 using std::cin;
 using std::cout;
 using std::endl;
 using std::ostream;
 using std::ios;
```

```
        //                         CONSTRUCTOR

complex::complex(double r=0.0f,double im=0.0f)
{
         real=r;
   imag=im;
}

        //                    COPY CONSTRUCTOR
complex::complex(complex &c)
{
         this->real=c.real;
   this->imag=c.imag;
}


void complex::operator =(complex c)
{
   real=c.real;
   imag=c.imag;
}


complex complex::operator +(complex c)
{
         complex tmp;
   tmp.real=this->real+c.real;
   tmp.imag=this->imag+c.imag;
   return tmp;
}

complex complex::operator -(complex c)
{
         complex tmp;
   tmp.real=this->real - c.real;
   tmp.imag=this->imag - c.imag;
   return tmp;
}

                complex complex::operator *(complex c)
{
         complex tmp;
   tmp.real=(real*c.real)-(imag*c.imag);
```

```
    tmp.imag=(real*c.imag)+(imag*c.real);
    return tmp;
}

complex complex::operator /(complex c)
{
            double div=(c.real*c.real) + (c.imag*c.imag);
    complex tmp;
    tmp.real=(real*c.real)+(imag*c.imag);
    tmp.real/=div;
    tmp.imag=(imag*c.real)-(real*c.imag);
    tmp.imag/=div;
    return tmp;
}

/*
complex complex::operator ^(int power)
{
    complex tmp;
    double modulus = getmodulus();
    double angle;

    if(real == 0)
                angle = PI/2;
    else
                angle = atan(imag/real);
    tmp.real = modulus*cos((double)power*angle);
    tmp.imag = modulus*sin((double)power*angle);

    return tmp;
}
*/

complex complex::operator ^(int power)
{
    complex tmp(1,0);
    int i;

    if(power == 0)
                return complex(1,0);
    else
    {
                    if(power > 0)
                {
                        for(i=0;i<power;i++)
                                tmp = tmp*complex(*this);
                }
                else
                {
                        double modulus = getmodulus();
                   double angle;

                   if(real == 0)
                           angle = PI/2;
                   else
                           angle = atan(imag/real);
                   tmp.real = modulus*cos((double)power*angle);
                   tmp.imag = modulus*sin((double)power*angle);
                }
   }

   return tmp;
}

complex complex::getconjugate()
{
         complex tmp;
   tmp.real=this->real;
   tmp.imag=this->imag * -1;
   return tmp;
}

complex complex::getreciprocal()
{
         complex t;
   t.real=real;
   t.imag=imag * -1;
   double div;
   div=(real*real)+(imag*imag);
   t.real/=div;
   t.imag/=div;
   return t;
}

double complex::getmodulus()
{
        double z;
    z=(real*real)+(imag*imag);
    z=sqrt(z);
    return z;
}

void complex::setdata(double r,double i)
{
        real=r;
    imag=i;
}

void complex::getdata()
{
    cout<<”Enter Real:”;
    cin>>this->real;
    cout<<”Enter Imaginary:”;
    cin>>this->imag;

}

double complex::getreal()
{
        return real;
}

double complex::getimaginary()
{
        return imag;
}

bool complex::operator ==(complex c)
{
 return (real==c.real)&&(imag==c.imag) ? 1 : 0;
 }

ostream& operator <<(ostream &s,complex &c)
{
       // s<<”Real Part = ”<<c.real<<endl
       // <<”Imaginary Part = ”<<c.imag<<endl;
    s<<c.real<<setiosflags(ios::showpos)
          <<c.imag<<”i”<<endl<<resetiosflags(ios::showpos);
       return s;
```

```
}


 #include ”stdafx.h”

using namespace System;
using namespace System::Reflection;
using namespace System::Runtime::CompilerServices;
using namespace System::Runtime::InteropServices;
using namespace System::Security::Permissions;

//
// General Information about an assembly is controlled through the
// following set of attributes. Change these attribute values to
//  modify the information associated with an assembly.
//
[assembly:AssemblyTitleAttribute(”Test4”)];
[assembly:AssemblyDescriptionAttribute(””)];
[assembly:AssemblyConfigurationAttribute(””)];
[assembly:AssemblyCompanyAttribute(”Microsoft”)];
[assembly:AssemblyProductAttribute(”Test4”)];
[assembly:AssemblyCopyrightAttribute(”Copyright (c) Microsoft 2011”)];
[assembly:AssemblyTrademarkAttribute(””)];
[assembly:AssemblyCultureAttribute(””)];

//
// Version information for an assembly consists of the following
//four values:
//
//       Major Version
//       Minor Version
//       Build Number
//       Revision
//
// You can specify all the value or you can default the
//Revision and Build Numbers
// by using the ’*’ as shown below:

[assembly:AssemblyVersionAttribute(”1.0.*”)];

[assembly:ComVisible(false)];

[assembly:CLSCompliantAttribute(true)];
```

```
[assembly:SecurityPermission(SecurityAction::RequestMinimum,
   UnmanagedCode = true)];

// Test4.cpp : main project file.

#include ”stdafx.h”
#include <iostream>
#include <string>
#include ”Complex.h”
#include <math.h>
//#include <complex>

#define _USE_MATH_DEFINES

using namespace System;

using std::cin;
using std::cout;
using std::endl;


int main()
{
        cout<<”hello world”
        }
        //pause();
        return 0;
}

void pause()
{
        cin.ignore();//Ignores previous input, get cin.get
                     //working even with new line inputs.
        cin.get();
}
```