

ARITHMETIC PROPERTIES OF VALUES OF LACUNARY SERIES

By

Ryan Bradshaw, B.Sc., M.Sc.

September 2013

A Thesis

submitted to the School of Graduate Studies and Research

in partial fulfillment of the requirements

for the degree of

Master of Science in Mathematics¹

© Ryan Bradshaw, Ottawa, Canada, 2013

by Ryan Bradshaw, B.Sc., M.Sc., Ottawa, Canada

¹The M.Sc. Program is a joint program with Carleton University, administered by the Ottawa-Carleton Institute of Mathematics and Statistics

Abstract

A lacunary series is a Taylor series with large gaps between its non-zero coefficients. In this thesis we exploit these gaps to obtain results of linear independence of values of lacunary series at integer points. As well, we will study different methods found in Diophantine approximation which we use to study arithmetic properties of values of lacunary series at algebraic points. Among these methods will be Mahler's method and a new approach due to Jean-Paul Bézivin.

Acknowledgements

I would like to thank my supervisor, Professor Damien Roy, for his guidance and support throughout the past 2 years. He has given me an abundance of his time to advise me through the writing process of this thesis. Without his expertise and patience, this exposition would not be at its current standing.

Dedication

I dedicate this work to my father and mother, Tom and Gerrette, for their support throughout my academic career.

Contents

Abstract	ii
Acknowledgements	iii
Dedication	iv
1 Introduction	1
2 Linear Independence	4
2.1 Warm-up: Fredholm Series	5
2.1.1 Irrationality of $f(q)$	5
2.1.2 The Gap-Method: First Look	6
2.2 Main Result	14
2.2.1 Preliminaries	15
2.2.2 Cubes	17
2.2.3 General Case	25
3 Method of Bézivin	30
3.1 Preliminaries	31
3.1.1 Linear Recurrence Sequences	31
3.1.2 Hankel Determinant	37
3.1.3 Length of Polynomials	38
3.1.4 The Permanent	42
3.2 Motivation	43

3.3	Estimation of Degree and Length	46
3.4	Estimation of Absolute Value	51
3.5	Estimation of the Content	57
3.6	Conclusion	64
4	Mahler Functions of One Variable	66
4.1	Preliminaries	67
4.2	Construction of Auxiliary Polynomials	68
4.3	Estimation of Absolute Value	69
4.4	Estimation of the Size and Denominator	70
4.5	Conclusion	74
4.6	Application	75
	Bibliography	78

Chapter 1

Introduction

In 1853 Liouville showed that algebraic numbers cannot be well approximated by rational numbers. This gave many examples of transcendental numbers. For example the truncations of the series

$$\theta = \sum_{n=0}^{\infty} \frac{1}{10^{n!}}$$

yield good enough rational approximations to deduce transcendence of θ from Liouville's Theorem. However this method has its limitations. For example, when studying arithmetic properties of values of the Fredholm series

$$f(z) = \sum_{n=0}^{\infty} z^{2^n}$$

at algebraic points, Liouville's Theorem will not suffice.

Over eighty years ago, Mahler introduced a new approach for studying arithmetic properties of certain functions satisfying a functional equation (see [8]). With his method he was able to show that for an algebraic number α with $0 < |\alpha| < 1$,

$$f(\alpha) = \sum_{n=0}^{\infty} \alpha^{2^n}$$

is transcendental. But Mahler's method also has its limitations. For instance, when studying arithmetic properties of the function

$$h_k(z) = \sum_{n=0}^{\infty} \frac{1}{z^{n^k}},$$

where k is a positive integer greater than 1, Mahler's method cannot be applied due to the fact that $h_k(z)$ doesn't satisfy a functional equation of the required type. In chapter 4, we introduce the theory of Mahler following Kumiko Nishioka [7, chap I]. The presentation of Kumiko Nishioka is very general and the computations are involved. In this chapter, we weaken the hypothesis of the main theorem and make use of this to simplify some of the more involved computations. The special case that we prove is enough to show the transcendence of $f(\alpha)$ where α is an algebraic number satisfying $0 < |\alpha| < 1$.

In chapter 2, we give a separate proof of $f(1/q)$ being transcendental where q is an integer greater than or equal to 2. Then, we use the method developed towards this proof to investigate properties of values of $h_k(z)$ at integer points. Namely we show that for any positive integer $q > 1$, the set

$$\{1, h_k(q), \dots, h_k^{k-1}(q)\}$$

is linearly independent over \mathbb{Q} or equivalently, that $h_k(q)$ is not algebraic of degree $< k$. The key ingredient in our proof lies in the fact that the series expansions representing

$$1, h_k(q), \dots, h_k^{k-1}(q) \tag{1}$$

share common large gaps between their non-zero terms. However if we want to extend the above result by showing that

$$\{1, h_k(q), \dots, h_k^k(q)\}$$

is linearly independent over \mathbb{Q} , we run into a problem. The large gaps between the non-zero terms of the values (1) begin to fill in for

$$h_k^k(q) = \sum_{\substack{n_1 \geq 0 \\ \dots \\ n_k \geq 0}} \frac{1}{q^{n_1^k + \dots + n_k^k}}.$$

This is linked to Waring's problem of representing positive integers as a sum of m non-negative k^{th} powers. It is important to note that the linear independence of the values

(1) is probably well known, however an exact reference is unknown at this moment in time. Moreover, the method presented in this chapter, from my acknowledgement, is original. I will go into a bit more details of this at the beginning of chapter 2.

In chapter 3, we turn our attention to a method of Bézivin. He introduced a new approach for studying arithmetic properties of the commonly named Tschakaloff function

$$f(z) = \sum_{n=0}^{\infty} \frac{z^n}{q^{n(n+1)/2}},$$

where $|q| > 1$ is a rational number, at algebraic points. In chapter 3 we focus on a specific case. Namely we show that for any positive integer $q \geq 2$, the number

$$\theta = \sum_{n=0}^{\infty} \frac{1}{q^{n(n+1)/2}}$$

is non-quadratic. The idea is to use the truncations of θ to construct auxiliary matrices. Then after assuming that θ is quadratic, we use the relationship between the Hankel determinant and linear recurrence sequences to arrive at a contradiction.

Bézivin's method can be used to show non-quadraticity of

$$h_2(q) = \sum_{n=0}^{\infty} \frac{1}{q^{n^2}},$$

for any integer $q \geq 2$. So perhaps it can be adapted to deduce linear independence over \mathbb{Q} of

$$\{1, h_k(q), \dots, h_k^k(q)\}$$

for any integer $q \geq 2$. But this is another project in itself.

Chapter 2

Linear Independence of Values of Lacunary Series

Let $k \in \mathbb{Z}$ with $k \geq 3$. We then set

$$h(z) = \sum_{n=0}^{\infty} \frac{1}{z^{nk}}. \quad (2)$$

Our main goal in this chapter is to prove the following result.

Theorem 2.0.1. *Let $q \in \mathbb{Z}$ with $q > 1$, then $\{1, h(q), \dots, h^{k-1}(q)\}$ is linearly independent over \mathbb{Q} .*

As stated in the introduction, this result is probably well known, however an exact reference is unknown to us. Moreover, the method that we develop for the proof is due to many one on one sessions between my supervisor and myself. Thus no references were used. The motivation came from the observation that we are able to utilize the large gaps between the non-zero terms of

$$\sum_{n=0}^{\infty} \frac{1}{q^{2^n}},$$

where q is an integer greater than or equal to 2, to deduce irrationality of this series (see §2.1.1). This led us to develop a “gap-method” first to prove the transcendence of the above series (see the next section) and then to prove Theorem 2.0.1.

2.1 Warm-up: Fredholm Series

In this section we study arithmetic properties of values of the so-called Fredholm Series

$$f(z) = \sum_{n=0}^{\infty} \frac{1}{z^{2^n}}$$

at integer points. Namely, we will prove the following result.

Theorem 2.1.1. *Let $q \in \mathbb{Z}_{>1}$. Then $f(q) \notin \overline{\mathbb{Q}}$.*

We will generalize the above result in chapter 4, §4.6 using a powerful method of Mahler. But for now what is important is the method we develop to prove the transcendence of $f(q)$. This will give an outline our “gap-method” in a simpler context compared to the proof of Theorem 2.0.1.

We begin by first proving that $f(q)$ is irrational.

2.1.1 Irrationality of $f(q)$

Suppose there exist $a, b \in \mathbb{Z}$ with $b > 0$ such that $f(q) = a/b$. Now by fixing $k \in \mathbb{N}^*$, we have

$$\frac{a}{b} - \sum_{n=0}^k \frac{1}{q^{2^n}} = \sum_{n=k+1}^{\infty} \frac{1}{q^{2^n}} > 0.$$

Letting

$$c = \sum_{n=0}^k q^{2^k - 2^n},$$

then on the left hand side we have

$$\begin{aligned} \frac{a}{b} - \sum_{n=0}^k \frac{1}{q^{2^n}} &= \frac{a}{b} - \frac{c}{q^{2^k}} \\ &= \frac{aq^{2^k} - cb}{bq^{2^k}} \\ &\geq \frac{1}{bq^{2^k}}, \end{aligned}$$

since $aq^{2^k} - cb \in \mathbb{Z}_{>0}$. Where on the right hand side we have

$$\begin{aligned} \sum_{n=k+1}^{\infty} \frac{1}{q^{2^n}} &\leq \sum_{n=2^{k+1}}^{\infty} \frac{1}{q^n} \\ &= \frac{1}{q^{2^{k+1}}} \left(\frac{q}{q-1} \right) \\ &\leq \frac{2}{q^{2^{k+1}}}, \end{aligned}$$

where the last inequality follows from $q \geq 2$. Putting all of this together we conclude that

$$\frac{1}{bq^{2^k}} \leq \frac{2}{q^{2^{k+1}}},$$

which implies that

$$\frac{1}{2b} \leq \frac{1}{q^{2^{k+1}-2^k}}.$$

But this is impossible if we choose k sufficiently large enough since

$$\lim_{k \rightarrow \infty} \frac{1}{q^{2^{k+1}-2^k}} = 0.$$

Therefore $f(q) \notin \mathbb{Q}$.

The main idea behind the above proof is based on the observation that the truncations

$$\sum_{n=0}^k \frac{1}{q^{2^n}}$$

provide good enough rational approximations to $f(q)$ to deduce irrationality. However they will not be sufficient enough to deduce non-quadraticity of $f(q)$ from Liouville's Theorem. This leads us to the next section.

2.1.2 The Gap-Method: First Look

In what follows is a proof by contradiction of Theorem 2.1.1.

Suppose $f(q)$ is algebraic of degree $k \geq 2$. Then there exist $a_0, a_1, \dots, a_k \in \mathbb{Z}$ with $a_k \geq 1$ such that

$$\begin{aligned} 0 &= a_0 + a_1 f(q) + \dots + a_k f^k(q) \\ &= a_0 + \sum_{n \geq 0} \frac{a_1}{q^{2^n}} + \sum_{\substack{n_1 \geq 0 \\ n_2 \geq 0}} \frac{a_2}{q^{2^{n_1} + 2^{n_2}}} + \dots + \sum_{\substack{n_1 \geq 0 \\ \dots \\ n_k \geq 0}} \frac{a_k}{q^{2^{n_1} + \dots + 2^{n_k}}}. \end{aligned} \quad (3)$$

We will now turn our attention to the exponents

$$2^{n_1} + \dots + 2^{n_\ell}$$

appearing in equation (3).

Our first goal is to compute an upper bound on the number of ways we can write a positive integer m in the form

$$m = 2^{n_1} + \dots + 2^{n_\ell}.$$

We begin by introducing some new notation.

Definition 2.1.2. For each $m \in \mathbb{N}$ and $\ell > 0$, let

- 1) $D_\ell(m) := \{(n_1, \dots, n_\ell) \in \mathbb{N}^\ell; 2^{n_1} + \dots + 2^{n_\ell} = m\}$,
- 2) $r_\ell(m) := |D_\ell(m)|$,
- 3) $s_\ell(m) := |\{(n_1, \dots, n_\ell) \in D_\ell(m); n_1 \leq \dots \leq n_\ell\}|$,
- 4) $E_\ell(m) := \{n \in \mathbb{N}; \exists (n_1, \dots, n_\ell) \in D_\ell(m) \text{ where } n = \max(n_1, \dots, n_\ell)\}$.

So by the above definition our first goal is to compute an upper bound for $r_\ell(m)$. Note, we extend the definition of $r_\ell(m)$ for $\ell = 0$ by setting $r_0(0) = 1$ and $r_0(m) = 0$ for every positive integer $m \neq 0$.

Proposition 2.1.3. For all $m \in \mathbb{N}$ and $\ell > 0$, $|E_\ell(m)| \leq \log_2(\ell) + 1$.

Proof. Let $n \in E_\ell(m)$. We then have that

$$2^n \leq m \leq \ell 2^n,$$

which implies that

$$\frac{m}{\ell} \leq 2^n \leq m.$$

Hence we get that

$$\log_2 \left(\frac{m}{\ell} \right) \leq n \leq \log_2 (m).$$

Thus $|E_\ell(m)|$ is less than or equal to the length of the interval

$$\left[\log_2 \left(\frac{m}{\ell} \right), \log_2 (m) \right]$$

plus one, i.e.

$$|E_\ell(m)| \leq \log_2 (\ell) + 1.$$

□

Proposition 2.1.4. *For all $m \in \mathbb{N}$ and $\ell > 0$, we have that $s_\ell(m) \leq (\log_2 (\ell) + 1)^\ell$.*

Proof. We Proceed by induction on ℓ . When $\ell = 1$, then clearly

$$s_1(m) = |\{n \in \mathbb{N}; 2^n = m\}| \leq 1 = \log_2 (1) + 1.$$

So suppose the claim is true for some $\ell \geq 1$. Now for each $(n_1, \dots, n_{\ell+1}) \in \mathbb{N}^{\ell+1}$ satisfying $2^{n_1} + \dots + 2^{n_{\ell+1}} = m$ and $n_1 \leq \dots \leq n_{\ell+1}$, we have that

$$m - 2^{n_{\ell+1}} = 2^{n_1} + \dots + 2^{n_\ell}.$$

Thus by the induction hypothesis, we obtain

$$s_{\ell+1}(m) \leq \sum_{n \in E_{\ell+1}(m)} s_\ell(m - 2^n) \leq |E_{\ell+1}(m)| (\log_2 (\ell) + 1)^\ell.$$

But by Proposition 2.1.3, we know that $|E_{\ell+1}(m)| \leq \log_2 (\ell + 1) + 1$. Consequently since $\log_2 (\ell) + 1 < \log_2 (\ell + 1) + 1$, we attain

$$s_{\ell+1}(m) < (\log_2 (\ell + 1) + 1) (\log_2 (\ell + 1) + 1)^\ell = (\log_2 (\ell + 1) + 1)^{\ell+1}.$$

Therefore by induction our claim is proven. □

Corollary 2.1.5. *For all $m \in \mathbb{N}$ and $\ell > 0$, we have $r_\ell(m) \leq \ell! (\log_2(\ell) + 1)^\ell$*

Proof. Since for any

$$(n_1, \dots, n_\ell) \in D_\ell(m),$$

there are $\ell!$ ways to rearrange (n_1, \dots, n_ℓ) , we then conclude that

$$r_\ell(m) = \ell! s_\ell(m) \leq \ell! (\log_2(\ell) + 1)^\ell.$$

□

The reason why we are interested in computing an upper bound on $r_i(m)$ follows from the following observation,

$$f^i(q) = \sum_{m \geq 0} \frac{r_i(m)}{q^m}.$$

This allows us to rewrite (3) as

$$0 = \sum_{i=0}^k a_i \sum_{m=0}^{\infty} \frac{r_i(m)}{q^m} = \sum_{m=0}^{\infty} \left(\sum_{i=0}^k a_i r_i(m) \right) \frac{1}{q^m}. \quad (4)$$

We now consider the following Lemma.

Lemma 2.1.6. *For each $m \in \mathbb{N}$, set*

$$u_m := \sum_{i=0}^k a_i r_i(m).$$

There exists a positive constant K such that

$$|u_m| \leq K,$$

for every positive integer m .

Proof. By Corollary 2.1.5 and the triangle inequality we obtain

$$\begin{aligned} |u_m| &\leq \sum_{i=0}^k |a_i i! (\log_2(i) + 1)^i| \\ &\leq k! (\log_2(k) + 1)^k \sum_{i=0}^k |a_i| \\ &= K. \end{aligned}$$

□

Definition 2.1.7. For each $m \in \mathbb{N}$, let

$$b(m) := \text{number of ones in the binary expansion of } m.$$

Then for each integer $\ell > 0$, we set

$$U_\ell := \{m \in \mathbb{N}; b(m) \leq \ell\}.$$

So, U_ℓ is the set positive integers whose binary expansion contains at most ℓ ones.

It is worth noting that for each integer $\ell \geq 1$ we have that $0 \in U_\ell$, and also $U_1 \subseteq U_2 \subseteq U_3 \subseteq \dots$.

The next definition uses the integer $k \geq 1$ fixed at the beginning of this section.

Definition 2.1.8. For any $n \in \mathbb{N}$ with $n > k$ we define

$$A_n = 2^n, \quad B_n = 2^n - 2^{n-k}, \quad \text{and} \quad C_n = 2^n - 2^{n-k} - 2^{n-k-1}.$$

By definition it is clear that the binary expansions of A_n, B_n , and C_n are

- 1) $A_n = (\underbrace{10 \dots 0}_{n+1})_2$
- 2) $B_n = (\underbrace{11 \dots 1}_k \underbrace{0 \dots 0}_{n-k})_2$
- 3) $C_n = (\underbrace{1 \dots 101}_{k+1} \underbrace{0 \dots 0}_{n-k-1})_2$.

Thus we have that $b(A_n) = 1$ and $b(B_n) = b(C_n) = k$, and so, by the above remark following definition 2.1.7, we have that $A_n \in U_k$ and $B_n, C_n \in U_k \setminus U_{k-1}$.

Lemma 2.1.9. *Let $n \in \mathbb{N}$ with $n > k$. There does not exist a positive integer $m \in U_k$ such that*

$$m \in (B_n, A_n) \quad \text{or} \quad m \in (C_n, B_n).$$

We articulate the above Lemma by saying that the two intervals (B_n, A_n) and (C_n, B_n) are gaps of U_k (see definition 2.2.1 in the next section).

Proof. Suppose there exists $m \in U_k$ such that $B_n < m < A_n$, and let $m = (i_1, \dots, i_n)_2$ be the binary expansion of m . Then $i_1 = \dots = i_k = 1$ and at least one of i_{k+1}, \dots, i_n is equal to 1. Hence $b(m) \geq k + 1$, but this is impossible since $m \in U_k$. The same argument shows that $C_n < m < B_n$ is impossible. Therefore concludes the proof of the Lemma. \square

Lemma 2.1.10. *For $m \in \mathbb{N}$, we have $r_\ell(m) > 0$ if and only if $m \geq \ell$ and $m \in U_\ell$.*

Proof. We only prove the ‘only if’ implication since it is the only direction necessary for this exposition. Thus the ‘if’ direction is left as an exercise for the reader.

If $r_\ell(m) > 0$ then there exist $(n_1, \dots, n_\ell) \in \mathbb{N}^\ell$ such that

$$m = 2^{n_1} + \dots + 2^{n_\ell}.$$

It is then clear that

$$m \geq 2^0 + \dots + 2^0 = \ell.$$

To prove that $m \in U_\ell$ it suffices to show that $b(m) \leq \ell$. We proceed by induction on ℓ . If $r_1(m) > 0$, then we know there exists $n \in \mathbb{N}$ such that $m = 2^n$, and hence $b(m) = 1$.

Suppose the claim holds true for some $\ell \geq 1$. If $r_{\ell+1}(m) > 0$ then there exists $(n_1, \dots, n_{\ell+1}) \in \mathbb{N}^{\ell+1}$ such that

$$m = 2^{n_1} + \dots + 2^{n_{\ell+1}}.$$

If the exponents $n_1, \dots, n_{\ell+1}$ are all distinct then we have that $b(m) = \ell + 1$, and hence $m \in U_{\ell+1}$. Otherwise there exist a least two indices $1 \leq i, j \leq \ell + 1$ such that $n_i = n_j$. Without loss of generality we may assume that $i = 1$ and $j = 2$. Then we can write m as

$$\begin{aligned} m &= 2^{n_1} + 2^{n_2} + \dots + 2^{n_{\ell+1}} \\ &= 2^{n_1+1} + 2^{n_3} + \dots + 2^{n_{\ell+1}}. \end{aligned}$$

Hence we have that $r_\ell(m) > 0$. Thus by the induction hypothesis we get

$$m \in U_\ell \subseteq U_{\ell+1}.$$

Therefore by induction on ℓ , we have that $m \in U_\ell$ if $r_\ell(m) > 0$.

□

Lemma 2.1.11. *For any $m \in \mathbb{N}$, we have $u_m = 0$ if $C_n < m < B_n$ or $B_n < m < A_n$.*

Proof. If $C_n < m < B_n$ or $B_n < m < A_n$, then by Lemma 2.1.9 we know that $m \notin U_k$. By the remark following Definition 2.1.7 we then conclude that

$$m \notin U_1 \cup \cdots \cup U_k.$$

Hence by the contrapositive of Lemma 2.1.10 we have that

$$r_1(m) = \cdots = r_k(m) = 0.$$

Therefore $u_m = 0$.

□

Lemma 2.1.12. *For each integer n with $n > k$, we have that*

$$u_{B_n} = a_k r_k(B_n) \neq 0 \quad \text{and} \quad u_{C_n} = a_k r_k(C_n) \neq 0.$$

Proof. We will only prove the first assertion since the same argument can be applied to prove the second.

Since $B_n \in U_k \setminus U_{k-1}$, then it is clear that

$$r_1(B_n) = \cdots = r_{k-1}(B_n) = 0 \quad \text{and} \quad r_k(B_n) \neq 0.$$

Moreover, by definition, $r_0(B_n) = 0$ since $B_n \neq 0$. Therefore

$$u_{B_n} = a_k r_k(B_n) \neq 0.$$

□

Taking into account Lemma 2.1.11 and Lemma 2.1.12, we rewrite equation (4) as

$$0 = \sum_{m \leq C_n} \frac{u_m}{q^m} + \frac{u_{B_n}}{q^{B_n}} + \sum_{m \geq A_n} \frac{u_m}{q^m}. \quad (5)$$

Lemma 2.1.13. *If n is large enough then*

$$\left| \sum_{m \leq C_n} \frac{u_m}{q^m} + \frac{u_{B_n}}{q^{B_n}} \right| \geq \frac{1}{q^{B_n}}.$$

Proof. It suffices to show that for sufficiently large n we have

$$\sum_{m \leq C_n} \frac{u_m}{q^m} + \frac{u_{B_n}}{q^{B_n}} \neq 0,$$

since this would imply that

$$\sum_{m \leq C_n} \frac{u_m}{q^m} + \frac{u_{B_n}}{q^{B_n}}$$

is a non-zero rational number with denominator q^{B_n} , and hence

$$\left| \sum_{m \leq C_n} \frac{u_m}{q^m} + \frac{u_{B_n}}{q^{B_n}} \right| \geq \frac{1}{q^{B_n}}.$$

So suppose

$$\sum_{m \leq C_n} \frac{u_m}{q^m} + \frac{u_{B_n}}{q^{B_n}} = 0. \tag{6}$$

Then

$$\sum_{m \leq C_n} \frac{u_m}{q^m} \neq 0$$

since otherwise we would have that

$$\frac{u_{B_n}}{q^{B_n}} = 0,$$

which contradicts Lemma 2.1.12. Hence

$$\sum_{m \leq C_n} \frac{u_m}{q^m}$$

is a non-zero rational number with denominator q^{C_n} . Thus it is clear that

$$\left| \sum_{m \leq C_n} \frac{u_m}{q^m} \right| \geq \frac{1}{q^{C_n}}.$$

On the other hand, by applying Lemma 2.1.6 to equation (6) we obtain

$$\left| \sum_{m \leq C_n} \frac{u_m}{q^m} \right| \leq \frac{K}{q^{B_n}}.$$

Hence by putting the above two inequalities together we get

$$\frac{1}{q^{C_n}} \leq \frac{K}{q^{B_n}},$$

a contradiction for sufficiently large n .

□

Lemma 2.1.14. *For each $n \geq 1$ we have*

$$\left| \sum_{m \geq A_n} \frac{u_m}{q^m} \right| \leq \frac{2K}{q^{A_n}}.$$

Proof. After observing that

$$\sum_{m \geq A_n} \frac{1}{q^m} = \frac{1}{q^{A_n}} \left(\frac{q}{q-1} \right) \leq \frac{2}{q^{A_n}},$$

then by Lemma 2.1.6 we obtain

$$\left| \sum_{m \geq A_n} \frac{u_m}{q^m} \right| \leq K \sum_{m \geq A_n} \frac{1}{q^m} \leq \frac{2K}{q^{A_n}}.$$

□

Applying the above two Lemmas to equation (5) we get

$$\frac{1}{q^{B_n}} \leq \left| \sum_{m \leq C_n} \frac{u_m}{q^m} + \frac{u_{B_n}}{q^{B_n}} \right| = \left| \sum_{m \geq A_n} \frac{u_m}{q^m} \right| \leq \frac{2K}{q^{A_n}} \quad (7)$$

for each sufficiently large n . But since $A_n - B_n \rightarrow \infty$ as $n \rightarrow \infty$, this is impossible.

This contradiction proves Theorem 2.1.1, namely that $f(q) \notin \overline{\mathbb{Q}}$.

2.2 Main Result

Now that we have finished our warm-up, we will begin by making the notion of ‘gap’ more precise.

2.2.1 Preliminaries

Definition 2.2.1. A gap of a subset S of \mathbb{Z} is a closed interval I of \mathbb{R} whose end points are in S but whose interior does not contain any element of S .

Example 2.2.2. If $S = 2\mathbb{Z}$, then $[2, 4]$ is a gap of S . But $[3, 4]$, $(2, 4]$, and $(2, 4)$ are not gaps of S .

Note, Lemma 2.1.9 also provides concrete examples of gaps.

Definition 2.2.3. The span of a subset S of \mathbb{Z} , denoted $\text{span}(S)$, is the smallest closed interval in \mathbb{R} containing S .

Remark 2.2.4. If a finite interval is contained in $\text{span}(S)$ and has no points of S in its interior, then it is contained in a gap of S .

Definition 2.2.5. Given a finite interval I in \mathbb{R} where a and b are the two boundary points of I . We set $\mathcal{L}(I) := |a - b|$ to be the length of I with respect to the standard metric on \mathbb{R} .

Lemma 2.2.6. Let $a, b \in \mathbb{Z}$ such that $a < b$ and let $L > 0$. Then for any subset S of \mathbb{Z} with no gap of length $\geq L$ inside $[a, b]$, we have

$$|S \cap [a, b]| > \frac{b - a}{L} - 1.$$

Note that, in the above Lemma, the number L doesn't need to be an integer.

Proof. Without loss of generality we may assume $b \geq a + L$, since otherwise

$$\frac{b - a}{L} - 1 < 0$$

and hence the claim is trivial. Now let

$$n := \max\{m \in \mathbb{N}; a + mL \leq b\}.$$

Since we are assuming $b \geq a + L$ then we know $n > 0$. Moreover, since the intervals

$$[a + (i - 1)L, a + iL)$$

have length L for all $i = 1, \dots, n$, then by the hypothesis

$$S \cap [a + (i - 1)L, a + iL] \neq \emptyset$$

for all $i = 1, \dots, n$. Thus the number of points in the intersection of S and $[a, b]$ is at least the number of intervals $[a + (i - 1)L, a + iL]$ contained in $[a, b]$. We then conclude that

$$|S \cap [a, b]| \geq n = \left\lfloor \frac{b - a}{L} \right\rfloor > \frac{b - a}{L} - 1.$$

□

Lemma 2.2.7. *Let S be a finite subset of \mathbb{N} with $|S| \geq 2$, let $[a, b] = \text{span}(S)$, and let A be the set of all gaps of S . Then*

$$[a, b] = \bigcup_{I \in A} I \text{ and } |A| = |S| - 1.$$

Proof. Write $S = \{x_1, \dots, x_n\}$ where $x_1 < x_2 < \dots < x_n$. Then it is clear that $x_1 = a, x_n = b$ and that the gaps of S are

$$[x_1, x_2], [x_2, x_3], \dots, [x_{n-1}, x_n].$$

Thus we have that

$$|A| = |S| - 1$$

and

$$\bigcup_{I \in A} I = \bigcup_{i=1}^{n-1} [x_i, x_{i+1}] = [a, b] = \text{span}(S).$$

□

Lemma 2.2.8. *Let $S \subseteq T$ be finite subsets of \mathbb{N} with $\text{span}(S) = \text{span}(T)$, and let A be the collection of all gaps of S . Then*

$$|T| - 1 = \sum_{I \in A} (|I \cap T| - 1).$$

Proof. Let $T = \{x_1, \dots, x_n\}$ and $S = \{y_1, \dots, y_m\}$ be ordered in the usual way. Since $S \subseteq T$ then for each $1 \leq i \leq m$ there exists a unique $1 \leq j \leq n$ such that $y_i = x_j$. We also have

$$[x_1, x_n] = \text{span}(T) = \text{span}(S) = [y_1, y_m].$$

Thus by the above two observations we can conclude that

$$T \setminus S = \coprod_{i=1}^{m-1} (T \cap (y_i, y_{i+1})),$$

where \coprod denotes disjoint union. Hence we have

$$|T \setminus S| = \sum_{i=1}^{m-1} |T \cap (y_i, y_{i+1})|.$$

Since on the left hand side we have

$$|T \setminus S| = |T| - m,$$

whereas on the right hand side we get

$$\begin{aligned} \sum_{i=1}^{m-1} |T \cap (y_i, y_{i+1})| &= \sum_{i=1}^{m-1} (|T \cap [y_i, y_{i+1}]| - 2) \\ &= \left(\sum_{I \in \mathcal{A}} |T \cap I| - 1 \right) - (m - 1), \end{aligned}$$

we then conclude that

$$|T| - 1 = \sum_{I \in \mathcal{A}} (|I \cap T| - 1).$$

□

2.2.2 Cubes

In this section we will focus on the specific case $k = 3$ of Theorem 2.0.1. Namely, by letting

$$h(q) = \sum_{n=0}^{\infty} \frac{1}{q^{n^3}}$$

where $q \in \mathbb{Z}_{>1}$, we will prove the following result.

Theorem 2.2.9. $\{1, h(q), h^2(q)\}$ is linearly independent over \mathbb{Q} .

The proof uses the same method applied in the proceeding section. Namely, we will show that one can find gaps between consecutive sums of two cubes contained in the interval $[N^3, 8N^3]$ for all $N \gg 1$. Moreover, these gaps will grow in length as N tends to infinity. This will allow us to show that no non-zero degree 2 polynomial with rational coefficients vanishes at $h(q)$.

Note, this is enough to prove Theorem 2.2.9. Since, if there exists a non-zero polynomial $p(x) \in \mathbb{Q}[x]$ of degree 1 that vanishes at $h(q)$, then by multiplying that polynomial by x , we get a new polynomial of degree two which also vanishes at $h(q)$. But we know that this is impossible.

We now turn our attention to finding these gaps.

Gaps between Consecutive Sums of Two Cubes

We will begin with a definition and then carry forward with a few Lemmas which will draw out the needed gaps from the shadows.

Definition 2.2.10. For each integers $k, \ell \geq 1$, we define

$$\mathcal{C}_\ell^{(k)} := \{n_1^k + \cdots + n_\ell^k; n_1, \dots, n_\ell \in \mathbb{N}\}.$$

Also, for $a, b \in \mathbb{Z}$ with $a < b$ we let

$$\mathcal{C}_\ell^{(k)}(a, b) := \mathcal{C}_\ell^{(k)} \cap [a, b].$$

By the above definition it is clear that $\mathcal{C}_1^{(k)}(a, b) \subseteq \mathcal{C}_2^{(k)}(a, b) \subseteq \mathcal{C}_3^{(k)}(a, b) \subseteq \cdots$. Moreover, in this section we are interested in $\mathcal{C}_2^{(3)}$. So for simplicity we will let \mathcal{C} denote $\mathcal{C}_2^{(3)}$ for the remainder of this section. However we will come back to the original notation introduced in the above definition when we prove the general case.

Lemma 2.2.11. Let $n \in \mathbb{Z}_{\geq 1}$ and I be a gap of \mathcal{C} contained in $[n^3, (n+1)^3]$. Then $\mathcal{L}(I) < 28n^{\frac{4}{3}}$.

Proof. Let

$$k = \max\{m \in \mathbb{N}; n^3 + m^3 < (n+1)^3\}.$$

As a function of m , the difference

$$(n^3 + (m+1)^3) - (n^3 + m^3) = 3m^2 + 3m + 1$$

is strictly increasing, hence for $0 \leq m \leq k$

$$|(n^3 + (k+1)^3) - (n^3 + k^3)| \geq |(n^3 + (m+1)^3) - (n^3 + m^3)|. \quad (8)$$

Moreover, by the choice of k we have that

$$\begin{aligned} n^3 + k^3 < (n+1)^3 &\Rightarrow k^3 < 3n^2 + 3n + 1 \leq 7n^2 \\ &\Rightarrow k < 2n^{\frac{2}{3}}. \end{aligned} \quad (9)$$

Since $n^3, n^3+1, \dots, n^3+k^3, (n+1)^3 \in \mathcal{C}(n^3, (n+1)^3)$, then I must be contained in one of the intervals

$$[n^3, n^3+1], [n^3+1, n^3+8], \dots, [n^3+k^3, (n+1)^3].$$

Otherwise I would contain at least one of the points $n^3, n^3+1, \dots, n^3+k^3$, or $(n+1)^3$ which would contradict the fact that $\overset{\circ}{I} \cap \mathcal{C} = \emptyset$, where $\overset{\circ}{I}$ denotes the interior of I . Hence by (8) we get

$$\begin{aligned} \mathcal{L}(I) &\leq |(n^3 + (k+1)^3) - (n^3 + k^3)| \\ &= 3k^2 + 3k + 1 \\ &\leq 7k^2. \end{aligned}$$

Therefore by (9), we conclude

$$\mathcal{L}(I) \leq 7k^2 < 28n^{\frac{4}{3}}. \quad \square$$

Lemma 2.2.12. *Suppose $n \geq 280$ and let L be a real number with $0 < L \leq \frac{1}{3}n^2$. If there is at most one gap I of $\mathcal{C}(n^3, (n+1)^3)$ with $\mathcal{L}(I) \geq L$, then*

$$|\mathcal{C}(n^3, (n+1)^3)| \geq \frac{(n+1)^3 - n^3}{2L}.$$

Proof. Suppose first there is a gap I of $\mathcal{C}(n^3, (n+1)^3)$ with $\mathcal{L}(I) \geq L$. Upon writing $I = [a, b]$, we have $a, b \in \mathbb{Z}$, $b - a > L$, and that

$$|\mathcal{C}(n^3, (n+1)^3)| = |\mathcal{C}(n^3, a)| + |\mathcal{C}(b, (n+1)^3)|.$$

On account of I being a gap of \mathcal{C} contained in $[n^3, (n+1)^3]$ with $\mathcal{L}(I) \geq L$, and our hypothesis, we conclude that there are no gaps of \mathcal{C} contained in $[n^3, a]$ or $[b, (n+1)^3]$ of length greater or equal to L . Hence by Lemma 2.2.6 we obtain

- $|\mathcal{C}(n^3, a)| > \frac{a - n^3}{L} - 1$
- $|\mathcal{C}(b, (n+1)^3)| > \frac{(n+1)^3 - b}{L} - 1$

It then follows that

$$|\mathcal{C}(n^3, (n+1)^3)| > \frac{a - n^3 + (n+1)^3 - b}{L} - 2.$$

But note by Lemma 2.2.11,

$$\begin{aligned} a - n^3 + (n+1)^3 - b &= |(n+1)^3 - n^3| - \mathcal{L}(I) \\ &> (n+1)^3 - n^3 - 28n^{\frac{4}{3}}. \end{aligned}$$

So

$$\begin{aligned} |\mathcal{C}(n^3, (n+1)^3)| &> \frac{(n+1)^3 - n^3 - 28n^{\frac{4}{3}}}{L} - 2 \\ &= \frac{(n+1)^3 - n^3 - (28n^{\frac{4}{3}} + 2L)}{L}. \end{aligned}$$

In view of $n \geq 280$ and $L \leq \frac{1}{3}n^2$, we have $28n^{\frac{4}{3}} \leq \frac{3}{4}n^2$ and $2L \leq \frac{3}{4}n^2$. Consequently

$$28n^{\frac{4}{3}} + 2L \leq \frac{3n^2}{2} < \frac{1}{2}(3n^2 + 3n + 1) = \frac{1}{2}((n+1)^3 - n^3).$$

The conclusion then follows.

The case of there being no gap I satisfying the above conditions is easier and left as an exercise to the reader. \square

Lemma 2.2.13. *Let $N \in \mathbb{Z}$ with $N > 1$, then $|\mathcal{C}(0, N^3)| \leq 3N^2$.*

Proof.

$$\begin{aligned} |\mathcal{C}(0, N^3)| &\leq |\{(r, s) \in \mathbb{N}^2; r^3 + s^3 \leq N^3\}| \\ &\leq |\{(r, s) \in \mathbb{N}^2; r, s \leq N\}| \\ &= (N + 1)^2 \\ &= N^2 + 2N + 1 \\ &\leq 3N^2 \end{aligned}$$

The last inequality holds since $N > 1$. □

If you are wondering why we took the upper bound for $|\mathcal{C}(0, N^3)|$ to be $3N^2$ instead of $4N^2$, it will become clear at the end of the proof of the following Lemma.

Lemma 2.2.14. *Let $N \in \mathbb{N}$ with $N \geq 280$. Then there exists $n \in \mathbb{N}$ with $N \leq n \leq 2N - 1$ such that $\mathcal{C}(n^3, (n + 1)^3)$ admits at least two disjoint gaps of length $\geq \frac{N}{4}$.*

Proof. Suppose otherwise. Then for each $n = N, \dots, 2N - 1$, there is at most one gap of $\mathcal{C}(n^3, (n + 1)^3)$ of length $\geq \frac{N}{4}$. For each of the n , the hypotheses of Lemma 2.2.12 are then satisfied with $L = N/4$, since $N/4 \leq N^2/4 \leq n^2/3$, and so

$$|\mathcal{C}(n^3, (n + 1)^3)| \geq \frac{(n + 1)^3 - n^3}{N/2}.$$

Therefore we conclude that

$$\begin{aligned} |\mathcal{C}(N^3, 8N^3)| &= 1 + \sum_{n=N}^{2N-1} (|\mathcal{C}(n^3, (n + 1)^3)| - 1) \\ &\geq \sum_{n=N}^{2N-1} \left(\frac{(n + 1)^3 - n^3}{N/2} - 1 \right) \\ &= \frac{(2N)^3 - N^3}{N/2} - N \\ &= 14N^2 - N \\ &\geq 13N^2. \end{aligned}$$

But by Lemma 2.2.13,

$$|\mathcal{C}(N^3, 8N^3)| \leq |\mathcal{C}(0, 8N^3)| \leq 3(2N)^2 = 12N^2,$$

a contradiction. \square

Conclusion

We are now ready to prove the main result of this section. Let $p(x) = c_0 + c_1x + c_2x^2 \in \mathbb{Z}[x]$ such that $p(h(q)) = 0$. By the remark following Theorem 2.2.9 it suffices to show that $c_2 = 0$.

For each integer $\ell \geq 1$, define

$$r_\ell(m) := |\{(n_1, \dots, n_\ell) \in \mathbb{N}^\ell ; n_1^3 + \dots + n_\ell^3 = m\}|.$$

We extend the above definition by letting $r_0(0) = 1$ and $r_0(m) = 0$ for every integer $m \neq 0$. We know by Lemma 2.2.14 that for any integer $N \geq 280$ there exists $n \in \mathbb{N}$ with $N \leq n \leq 2N - 1$ such that $\mathcal{C}(n^3, (n+1)^3)$ admits at least two disjoint gaps of length $\geq \frac{N}{4}$. Let $I = [a_I, b_I]$ and $J = [a_J, b_J]$ be two of these gaps ordered so that $b_I < a_J$. Remembering that by definition $a_I, b_I, a_J, b_J \in \mathcal{C}$, we then write $h^2(q)$ as

$$h^2(q) = \sum_{m \geq 0} \frac{r_2(m)}{q^m} = \sum_{m \leq a_I} \frac{r_2(m)}{q^m} + \sum_{m=b_I}^{a_J} \frac{r_2(m)}{q^m} + \sum_{m \geq b_J} \frac{r_2(m)}{q^m} \quad (10)$$

where $r_2(m) \neq 0$ for $m = a_I, b_I, a_J, b_J$. With this in mind we have

$$0 = c_0 + c_1h(q) + c_2h^2(q) = \sum_{\substack{m \leq a_I \\ 0 \leq i \leq 2}} \frac{c_i r_i(m)}{q^m} + \sum_{\substack{m \geq b_I \\ 1 \leq i \leq 2}} \frac{c_i r_i(m)}{q^m} \quad (11)$$

$$= \sum_{\substack{m \leq a_I \\ 0 \leq i \leq 2}} \frac{c_i r_i(m)}{q^m} + \sum_{m=b_I}^{a_J} \frac{c_2 r_2(m)}{q^m} + \sum_{\substack{m \geq b_J \\ 1 \leq i \leq 2}} \frac{c_i r_i(m)}{q^m} \quad (12)$$

where the middle sum in equation (12) involves just c_2 since there are no cubes in the interval $(a_I, b_J) \subset (n^3, (n+1)^3)$.

Before we continue we need the following Lemmas.

Lemma 2.2.15. *For each $q \in \mathbb{Z}_{>1}$ and for each $b \in \mathbb{N}$, we have $\sum_{m \geq b} \frac{m}{q^m} \leq \frac{2b+2}{q^b}$.*

Proof. First we rewrite our summation as

$$\sum_{m \geq b} \frac{m}{q^m} = b \sum_{m \geq b} \frac{1}{q^m} + \frac{1}{q^{b+1}} \sum_{k=1}^{\infty} \frac{k}{q^{k-1}}.$$

Then by letting

$$g(x) = \sum_{k=0}^{\infty} x^k,$$

we recall that that

$$g(x) = \frac{1}{1-x}$$

for $|x| < 1$. Thus by taking the derivative we find that

$$g'(x) = \sum_{k=1}^{\infty} kx^{k-1} = \frac{1}{(1-x)^2}$$

for $|x| < 1$. Hence we get

$$\sum_{k=1}^{\infty} \frac{k}{q^{k-1}} = g'(1/q) = \frac{q^2}{(q-1)^2}.$$

Moreover we have that

$$\sum_{m \geq b} \frac{1}{q^m} \leq \frac{2}{q^b}$$

since the condition $q \in \mathbb{Z}_{>1}$ implies $\sum_{n=0}^{\infty} \frac{1}{q^n} = \frac{q}{q-1} \leq 2$. Therefore

$$\sum_{m \geq b} \frac{m}{q^m} \leq \frac{2b}{q^b} + \frac{q}{q^b(q-1)^2} \leq \frac{2b+2}{q^b}.$$

□

Lemma 2.2.16. $r_2(m) < m$ for all $m > 27$.

Proof. By definition we have

$$\begin{aligned}
r_2(m) &= |\{(n_1, n_2) \in \mathbb{N}^2 ; n_1^3 + n_2^3 = m\}| \\
&\leq |\{(n_1, n_2) \in \mathbb{N}^2 ; n_1, n_2 \leq m^{1/3}\}| \\
&= (1 + m^{1/3})^2 \\
&< 3m^{2/3} \\
&< m
\end{aligned}$$

since $m > 27$. □

From Lemmas 2.2.15 and 2.2.16 we deduce that, for any integer $b > 27$, we have

$$\left| \sum_{\substack{m \geq b \\ 1 \leq i \leq 2}} \frac{c_i r_i(m)}{q^m} \right| < \sum_{\substack{m \geq b \\ 1 \leq i \leq 2}} \frac{|c_i| m}{q^m} \leq \frac{K}{q^b}$$

where $K = (2b + 2)(|c_1| + |c_2|)$. Thus from (11) we have

$$\begin{aligned}
\left| \sum_{\substack{m \leq a_I \\ 0 \leq i \leq 2}} \frac{c_i r_i(m)}{q^m} \right| &= \left| \sum_{\substack{m > b_I \\ 1 \leq i \leq 2}} \frac{c_i r_i(m)}{q^m} \right| \\
&< \frac{K}{q^{b_I}} \\
&\leq \frac{K}{q^{a_I + N/4}} \\
&< \frac{1}{q^{a_I}}
\end{aligned}$$

for sufficiently large N .

A remark about the last inequality; recall from Lemma 2.2.14 that the lengths of the gaps I and J are bounded below by $\frac{N}{4}$. Thus as N grows so does their lengths, hence the last inequality in the above equation. With all of this in mind and the fact that

$$\sum_{\substack{m \leq a_I \\ 0 \leq i \leq 2}} \frac{c_i r_i(m)}{q^m}$$

is a rational number with denominator q^{a_I} , we conclude that

$$\sum_{\substack{m \leq a_I \\ 0 \leq i \leq 2}} \frac{c_i r_i(m)}{q^m} = 0.$$

From here equation (12) becomes

$$\sum_{m=b_I}^{a_J} \frac{c_2 r_2}{q^m} + \sum_{\substack{m \geq b_J \\ 1 \leq i \leq 2}} \frac{c_i r_i(m)}{q^m} = 0.$$

But by the same reasoning as above we get

$$\left| \sum_{\substack{m \geq b_J \\ 1 \leq i \leq 2}} \frac{c_i r_i(m)}{q^m} \right| < \frac{1}{q^{a_J}}$$

for sufficiently large N . Hence

$$\sum_{m=b_I}^{a_J} \frac{c_2 r_2(m)}{q^m} = 0,$$

which implies that $c_2 = 0$ since $r_2(m) > 0$ for $b_I \leq m \leq a_J$.

Therefore $\{1, h(q), h^2(q)\}$ is linearly independent over \mathbb{Q} .

2.2.3 General Case

We are now ready to prove Theorem 2.0.1.

Suppose $k > 3$ and $(c_0, c_1, \dots, c_{k-1}) \in \mathbb{Z}^k$ where $c_{k-1} \geq 0$ such that

$$c_0 + c_1 h(q) + \dots + c_{k-1} h(q)^{k-1} = 0. \quad (13)$$

Recalling definition 2.2.10, we put

$$r_\ell(m) := |\{(n_1, \dots, n_\ell) \in \mathbb{N}^\ell ; n_1^k + \dots + n_\ell^k = m\}|.$$

We then rewrite $h^\ell(q)$ as

$$h^\ell(q) = \sum_{m \geq 0} \frac{r_\ell(m)}{q^m}.$$

Following the same recipe as for the cubic case, we would like to rewrite (13) in the form

$$\sum_{\substack{m \leq a_I \\ 0 \leq i \leq k-1}} \frac{c_i r_i(m)}{q^m} + \sum_{m=b_I}^{a_J} \frac{c_{k-1} r_{k-1}(m)}{q^m} + \sum_{\substack{m \geq b_J \\ 1 \leq i \leq k-1}} \frac{c_i r_i(m)}{q^m} = 0, \quad (14)$$

where $b_I - a_I$ and $b_J - a_J$ can be made arbitrarily large.

To ensure that the middle term in (14) only depends on c_{k-1} , we need to find large gaps G of $\mathcal{C}_{k-2}^{(k)}$ which contain two large gaps $I = [a_I, b_I]$, $J = [a_J, b_J]$ of $\mathcal{C}_{k-1}^{(k)}$. In doing so we get $[a_I, b_J] \subseteq G$ and hence (a_I, b_J) contains no elements of $\mathcal{C}_{k-2}^{(k)} \supseteq \mathcal{C}_{k-3}^{(k)} \supseteq \cdots \supseteq \mathcal{C}_1^{(k)}$, i.e. $r_\ell(m) = 0$ for all $0 \leq \ell \leq k-2$ and $a_I < m < b_J$.

This leads us to consider the following result.

Proposition 2.2.17. *Let $C = 6(3/2)^{k-2} + 1$, then for each integer $N \geq 2^{k(k+1)}C$ there exists a gap G of $\mathcal{C}_{k-2}^{(k)}(N^k, (2N)^k)$ which contains at least two gaps of $\mathcal{C}_{k-1}^{(k)}$ with length $\geq N/C$.*

Note, if we assume that the above Proposition holds then the proof of Theorem 2.0.1 follows exactly the same argument given in the conclusion of section 2.2.2 except for a small change in Lemma 2.2.16 which becomes the following.

Lemma 2.2.18. *$r_{k-1}(m) < m$ if $m > 2^{k(k-1)}$.*

Proof. By definition we have

$$\begin{aligned} r_{k-1}(m) &= |\{(n_1, \dots, n_{k-1}) \in \mathbb{N}^{k-1}; n_1^k + \cdots + n_{k-1}^k = m\}| \\ &\leq |\{(n_1, \dots, n_{k-1}) \in \mathbb{N}^{k-1}; n_1, \dots, n_{k-1} \leq m^{1/k}\}| \\ &\leq (1 + m^{1/k})^{k-1} \\ &\leq 2^{k-1} m^{(k-1)/k} \\ &< m \end{aligned}$$

since $m > 2^{k(k-1)}$. □

Thus to confirm Theorem 2.0.1, it then suffices to prove Proposition 2.2.17. Before we begin carrying out this task, we need to generalize a few of the Lemmas from the previous section.

Lemma 2.2.19. *Let I be a gap of $\mathcal{C}_{k-1}^{(k)}$ contained in a gap G of $\mathcal{C}_{k-2}^{(k)}$. Then $\mathcal{L}(I) < 2^k \mathcal{L}(G)^{(k-1)/k}$.*

Proof. Let $a < b$ be the end points of G . Since G is a gap of $\mathcal{C}_{k-2}^{(k)}$, then we know that $a, b \in \mathcal{C}_{k-2}^{(k)}$. Now by letting $\ell := \max\{r \in \mathbb{N}; a + r^k < b\}$, it is clear that

$$a + 1, a + 2^k, \dots, a + \ell^k \in \mathcal{C}_{k-1}^{(k)}(G).$$

As a function of $r \in \mathbb{N}$, the difference

$$(a + (r + 1)^k) - (a + r^k) = \sum_{i=1}^k \binom{k}{i} r^{k-i}$$

is strictly increasing. Hence for all $0 \leq r \leq \ell$

$$\mathcal{L}[a + \ell^k, a + (\ell + 1)^k] \geq \mathcal{L}[a + r^k, a + (r + 1)^k]. \quad (15)$$

Moreover I must be contained in one of the intervals

$$[a, a + 1], [a + 1, a + 2^k], \dots, [a + \ell^k, b],$$

since otherwise the interior of I would contain one of the points

$$a + 1, a + 2^k, \dots, a + \ell^k$$

of $\mathcal{C}_{k-1}^{(k)}$. Thus by (15) we obtain

$$\begin{aligned} \mathcal{L}(I) &\leq \mathcal{L}[a + \ell^k, a + (\ell + 1)^k] \\ &= (\ell + 1)^k - \ell^k \\ &= \sum_{i=1}^k \binom{k}{i} \ell^{k-i} \\ &\leq \left(\sum_{i=1}^k \binom{k}{i} \right) \ell^{k-1} \\ &= 2^k \ell^{k-1}. \end{aligned}$$

But by the choice of ℓ we have that $a + \ell^k < b$, and so

$$\ell < \mathcal{L}[a, b]^{1/k}.$$

Therefore $\mathcal{L}(I) < 2^k \mathcal{L}([a, b])^{(k-1)/k}$. □

Lemma 2.2.20. *For any integer $N \geq 1$, we have $|\mathcal{C}_\ell^{(k)}(N^k, (2N)^k)| \leq (2N + 1)^\ell$.*

Proof.

$$\begin{aligned} |\mathcal{C}_\ell^{(k)}(N^k, (2N)^k)| &\leq |\mathcal{C}_\ell^{(k)}(0, (2N)^k)| \\ &\leq |\{(n_1, \dots, n_\ell) \in \mathbb{N}; n_1^k + \dots + n_\ell^k \leq (2N)^k\}| \\ &\leq |\{(n_1, \dots, n_\ell) \in \mathbb{N}; n_1, \dots, n_\ell \leq 2N\}| \\ &= (2N + 1)^\ell. \quad \square \end{aligned}$$

Lemma 2.2.21. *Let G be a gap of $\mathcal{C}_{k-2}^{(k)}$. Suppose that G contains at most one gap of $\mathcal{C}_{k-1}^{(k)}(G)$ of length $\geq L$ for some real number $L \geq 2^{k(k+1)}$. Then*

$$|\mathcal{C}_{k-1}^{(k)}(G)| > \frac{\mathcal{L}(G)}{2L} - 2.$$

Proof. If G contains no such gap then by Lemma 2.2.6 we know

$$|\mathcal{C}_{k-1}^{(k)}(G)| > \frac{\mathcal{L}(G)}{L} - 1 > \frac{\mathcal{L}(G)}{2L} - 2.$$

So suppose G contains such a gap I . From the choice of L we know that

$$2^{k(k+1)} \leq \mathcal{L}(I) \leq \mathcal{L}(G)$$

Hence by Lemma 2.2.19 we get

$$\mathcal{L}(I) \leq 2^k \mathcal{L}(G)^{(k-1)/k} \leq \mathcal{L}(G)/2.$$

Letting $\overset{\circ}{I}$ denote the interior of I we write

$$G \setminus \overset{\circ}{I} = I_1 \cup I_2,$$

where I_1 and I_2 are two disjoint closed intervals. By our hypothesis the closed intervals I_1 and I_2 contain no gaps of $\mathcal{C}_{k-1}^{(k)}$ of length $\geq L$. Thus by Lemma 2.2.6

$$|\mathcal{C}_{k-1}^{(k)}(I_j)| > \frac{\mathcal{L}(I_j)}{L} - 1, \quad \text{for } j = 1, 2.$$

Therefore

$$\begin{aligned} |\mathcal{C}_{k-1}^{(k)}(G)| &= |\mathcal{C}_{k-1}^{(k)}(I_1)| + |\mathcal{C}_{k-1}^{(k)}(I_2)| \\ &> \frac{\mathcal{L}(I_1)}{L} - 1 + \frac{\mathcal{L}(I_2)}{L} - 1 \\ &\geq \frac{\mathcal{L}(G)}{2L} - 2. \end{aligned}$$

Note, the last inequality comes from the fact that $\mathcal{L}(I_1) + \mathcal{L}(I_2) \geq \mathcal{L}(G)/2$ since $\mathcal{L}(I) \leq \mathcal{L}(G)/2$. \square

Proof of Proposition. Suppose the converse. Then every gap G of $\mathcal{C}_{k-2}^{(k)}(N^k, (2N)^k)$ contains at most one gap of $\mathcal{C}_{k-1}^{(k)}(N^k, (2N)^k)$ with length $\geq N/C$. Let A denote the set of all gaps of $\mathcal{C}_{k-2}^{(k)}(N^k, (2N)^k)$. Then by Lemma 2.2.8 we have

$$\begin{aligned} |\mathcal{C}_{k-1}^{(k)}(N^k, (2N)^k)| &= \sum_{G \in A} (|\mathcal{C}_{k-1}^{(k)}(G)| - 1) + 1 \\ &> \frac{\sum_{G \in A} \mathcal{L}(G)}{2N/C} - 3|A|. \quad (\text{Lemma 2.2.21}) \end{aligned}$$

Also by Lemmas 2.2.7 and 2.2.20 we conclude that

$$|A| = |\mathcal{C}_{k-2}^{(k)}(N^k, (2N)^k)| - 1 \leq (2N + 1)^{k-2}$$

and $[N^k, (2N)^k] = \bigcup_{G \in A} G$ which implies that

$$\sum_{G \in A} \mathcal{L}(G) = N^k(2^k - 1).$$

Hence

$$\begin{aligned} |\mathcal{C}_{k-1}^{(k)}(N^k, (2N)^k)| &> \frac{\sum_{G \in A} \mathcal{L}(G)}{2N/C} - 3|A| \\ &\geq \frac{CN^{k-1}(2^k - 1)}{2} - 3(2N + 1)^{k-2} \\ &\geq \frac{CN^{k-1}2^{k-1}}{2} - 3^{k-1}N^{k-1} \\ &= N^{k-1}(3^{k-1} + 2^{k-2}). \end{aligned}$$

But from Lemma 2.2.20 we know

$$|\mathcal{C}_{k-1}^{(k)}(N^k, (2N)^k)| \leq (2N + 1)^{k-1} \leq 3^{k-1}N^{k-1},$$

a contradiction. \square

Chapter 3

Method of Bézivin

Let q be a positive integer greater than or equal to 2 and set

$$\theta = \sum_{n=0}^{\infty} q^{-n(n+1)/2}.$$

The objective of this chapter is to prove the following result due to D. Duverney [2],

Theorem 3.0.1. *θ is not quadratic.*

We will use the method of Bézivin, which can be applied to show a more general result [1]. Namely Bézivin showed that if α is an algebraic number contained in a quadratic extension \mathbb{K} of \mathbb{Q} and $q = \frac{a}{b}$ is a non-zero rational number which satisfies $\gamma := \log |a| / \log |b| > 14$, then $f(\alpha) \notin \mathbb{K}$ where

$$f(x) = \sum_{n=0}^{\infty} \frac{x^n}{q^{-n(n+1)/2}}.$$

His method is a generalization of the technique we used for showing irrationality of values of the Fredholm series at integer points (Chapter 2.1, §2.1.1). We will come back to this in more detail in section 3.2 when we use this technique to prove that θ is irrational.

We begin with the following preliminaries.

3.1 Preliminaries

3.1.1 Linear Recurrence Sequences

Consider the set $\mathbb{C}^{\mathbb{N}}$ of functions from \mathbb{N} to \mathbb{C} . Given $a(n) \in \mathbb{C}^{\mathbb{N}}$, we may view $a(n)$ as an infinite sequence $(a_n)_{n \geq 0}$ of complex numbers where $a_n := a(n)$ for all $n \geq 0$. Under component wise addition, $\mathbb{C}^{\mathbb{N}}$ becomes an infinite dimensional complex vector space with basis $\{(\delta_{ij})_{j \geq 0}\}_{i=1}^{\infty}$ where $\delta_{ij} = 1$ if $j = i$ and zero otherwise.

Note, in this section we follow [6, chap I].

Definition 3.1.1. Let $\tau : \mathbb{C}^{\mathbb{N}} \rightarrow \mathbb{C}^{\mathbb{N}}$ be the map which sends $(a_n)_{n \geq 0} \mapsto (a_{n+1})_{n \geq 0}$. This map is called the *shift operator* and is \mathbb{C} -linear.

Remark 3.1.2. Given $p(x) = \sum_{k=0}^m z_k x^k \in \mathbb{C}[x]$ and $a_n \in \mathbb{C}^{\mathbb{N}}$, τ induces the following $\mathbb{C}[x]$ -module structure on $\mathbb{C}^{\mathbb{N}}$,

$$p(x) \cdot (a_n)_{n \geq 0} := (p(\tau)(a_n))_{n \geq 0}$$

where $p(\tau)(a_n) = \sum_{k=0}^m z_k a_{n+k}$.

Definition 3.1.3. A sequence $a_n \in \mathbb{C}^{\mathbb{N}}$ is called a *linear recurrence sequence* if there exists $t \in \mathbb{Z}_{\geq 0}$ and $z_1, \dots, z_t \in \mathbb{C}$ such that

$$a_n = z_1 a_{n-1} + \dots + z_t a_{n-t}$$

for all $n \geq t$.

Proposition 3.1.4. Given a polynomial $p(x) = x^t - z_1 x^{t-1} - \dots - z_t \in \mathbb{C}[x]$ and a vector $\vec{a} = (a_0, \dots, a_{t-1}) \in \mathbb{C}^t$, we can extend \vec{a} to a recurrence sequence $(a_n)_{n \geq 0} \in \mathbb{C}^{\mathbb{N}}$ where

$$a_{n+t} = z_1 a_{n+t-1} + \dots + z_t a_n$$

for $n \geq 0$.

Since we have defined the extension $(a_n)_{n \geq 0}$ of \vec{a} by a recurrence relation, the proof of the above Proposition is trivial.

Now given $p(x) \in \mathbb{C}[x]$ as above, we define

$$V_p := \{\mathbf{a} \in \mathbb{C}^{\mathbb{N}} ; p(\tau)(\mathbf{a}) = 0\}.$$

It is clear that V_p is the kernel of the linear map $p(\tau) : \mathbb{C}^{\mathbb{N}} \rightarrow \mathbb{C}^{\mathbb{N}}$ and hence is a subspace of $\mathbb{C}^{\mathbb{N}}$.

After considering the linear map $\varphi : \mathbb{C}^t \rightarrow V_p$, which sends a vector $\vec{a} = (a_0, \dots, a_{t-1}) \in \mathbb{C}^t$ to the recurrence sequence $(a_n)_{n \geq 0}$ as defined above, it is clear that $(a_n)_{n \geq 0} \in V_p$. Hence $(a_n)_{n \geq 0}$ is a recurrence sequence satisfying the following relation,

$$a_n = z_1 a_{n-1} + \dots + z_t a_{n-t}$$

for $n \geq t$. Moreover, φ is clearly a bijection. This proves the following Corollary.

Corollary 3.1.5. $\dim(V_p) = \deg(p(x))$.

Definition 3.1.6. Given a recurrence sequence $\mathbf{a} \in \mathbb{C}^{\mathbb{N}}$, we form the ideal

$$\text{Ann}(\mathbf{a}) = \{q(x) \in \mathbb{C}[x] ; q(x) \cdot \mathbf{a} = 0\} \subseteq \mathbb{C}[x].$$

Since $\mathbb{C}[x]$ is a Euclidean Domain then it is also Principal, hence $\text{Ann}(\mathbf{a}) = (p(x))$ for a unique monic polynomial $p(x) \in \mathbb{C}[x]$. The polynomial $p(x)$ is called the *companion polynomial* of $\mathbf{a} \in \mathbb{C}^{\mathbb{N}}$ and its roots are called the *frequencies* of \mathbf{a} . For now on we let $c_{\mathbf{a}}(x)$ denote the companion polynomial for a recurrence sequence $\mathbf{a} \in \mathbb{C}^{\mathbb{N}}$ and write it in the form $c_{\mathbf{a}}(x) = x^t - z_1 x^{t-1} - \dots - z_t$. From here we then say that $\mathbf{a} = (a_n)_{n \geq 0}$ is of order $t = \deg(c_{\mathbf{a}}(x))$ with initial values a_0, \dots, a_{t-1} .

Proposition 3.1.7. *Suppose $(a_n)_{n \geq 0}$ and $(b_n)_{n \geq 0}$ are linear recurrence sequences of order t and s respectively. Then $(a_n + b_n)_{n \geq 0}$ is a linear recurrence sequence of order at most $t + s$.*

Proof. Let $c_{\mathbf{a}}(x)$ and $c_{\mathbf{b}}(x)$ be the companion polynomials for $(a_n)_{n \geq 0}$ and $(b_n)_{n \geq 0}$ respectively. Then without much effort we obtain

$$\begin{aligned} (c_{\mathbf{a}}(x)c_{\mathbf{b}}(x)) \cdot (a_n + b_n)_{n \geq 1} &= c_{\mathbf{b}}(\tau)(c_{\mathbf{a}}(\tau)(a_n))_{n \geq 1} + c_{\mathbf{a}}(\tau)(c_{\mathbf{b}}(\tau)(b_n))_{n \geq 1} \\ &= 0. \end{aligned}$$

This implies that $(a_n + b_n)_{n \geq 1} \in V_{c_{\mathbf{a}}c_{\mathbf{b}}}$ and hence $(a_n + b_n)_{n \geq 1}$ is a linear recurrence sequence. Moreover, since $\deg(c_{\mathbf{a}}c_{\mathbf{b}}) = t + s$ then it is clear by definition that the order of $(a_n + b_n)_{n \geq 1}$ is at most $t + s$. \square

Proposition 3.1.8. *Let $(a_n)_{n \geq 0} \in \mathbb{C}^{\mathbb{N}}$ and $p(x) \in \mathbb{C}[x]$. Suppose that $p(x)$ factors into $p(x) = (x - \alpha_1) \dots (x - \alpha_s)$ where the α_i 's are distinct. Then $(a_n)_{n \geq 0} \in V_p$ if and only if there exist $z_1, \dots, z_s \in \mathbb{C}$ such that $a_n = \sum_{i=1}^s z_i \alpha_i^n$, and then z_1, \dots, z_s are uniquely determined by $(a_n)_{n \geq 0}$.*

Proof. It suffices to show that $\{(\alpha_i^n)_{n \geq 0}\}_{i=1}^s \subseteq \mathbb{C}^{\mathbb{N}}$ is a basis for V_p . We begin by showing that for any $i \in \{1, \dots, s\}$,

$$\begin{aligned} (\tau - \alpha_i)(\alpha_i^n)_{n \geq 0} &= \tau(\alpha_i^n)_{n \geq 0} - (\alpha_i^{n+1})_{n \geq 0} \\ &= (\alpha_i^{n+1})_{n \geq 0} - (\alpha_i^{n+1})_{n \geq 0} \\ &= 0. \end{aligned}$$

Hence $\text{span}\{(\alpha_1^n)_{n \geq 0}, \dots, (\alpha_s^n)_{n \geq 0}\} \subseteq V_p$. By Corollary 3.1.5 we know that $\dim V_p = \deg(p(x)) = s$. Hence all that is left to show is that $\{(\alpha_i^n)_{n \geq 0}\}_{i=1}^s$ is linearly independent. This follows from noticing that the Vandermonde determinant

$$\begin{vmatrix} \alpha_1^0 & \alpha_1^1 & \dots & \alpha_1^{s-1} \\ \vdots & & & \vdots \\ \alpha_s^0 & \alpha_s^1 & \dots & \alpha_s^{s-1} \end{vmatrix} = \pm \prod_{i \neq j} (\alpha_i - \alpha_j)$$

is non-zero since $\alpha_i \neq \alpha_j$ for all $i \neq j$. Thus the rows are linearly independent and hence so is $\{(\alpha_i^n)_{n \geq 0}\}_{i=1}^s$. Therefore $\{(\alpha_i^n)_{n \geq 0}\}_{i=1}^s$ forms a basis for V_p . \square

Theorem 3.1.9. *Let $(a_n)_{n \geq 0} \in \mathbb{C}^{\mathbb{N}} \setminus \{0\}$ and $p(x) \in \mathbb{C}[x]$. Suppose $p(0) \neq 0$ and write $p(x) = \prod_{i=1}^s (x - \alpha_i)^{e_i}$ where $\alpha_1, \dots, \alpha_s \in \mathbb{C}$ are distinct and $e_1, \dots, e_s \in \mathbb{N}^*$. Then $(a_n)_{n \geq 0} \in V_p$ if and only if there exist $p_1(x), \dots, p_s(x) \in \mathbb{C}[x] \setminus \{0\}$ with $\deg(p_i(x)) \leq e_i - 1$ ($1 \leq i \leq s$) such that $a_n = \sum_{i=1}^s p_i(n) \alpha_i^n$. When this holds, the polynomials $p_1(x), \dots, p_s(x)$ are uniquely determined by $(a_n)_{n \geq 0}$.*

To prove this Theorem we will need the following results.

Proposition 3.1.10. *Let $p, q \in \mathbb{C}[x] \setminus \{0\}$ such that $\gcd(p, q) = 1$. Then $V_{pq} = V_p \oplus V_q$.*

Proof. Let $\mathbf{u} \in V_p + V_q$. Write $\mathbf{u} = u_p + u_q$ where $u_p \in V_p$ and $u_q \in V_q$.

Suppose $\mathbf{u} \in V_p \cap V_q$. Then \mathbf{u} is annihilated by both $p(x)$ and $q(x)$. Hence $p, q \in \text{Ann}(\mathbf{u}) = (c_{\mathbf{u}}(x))$, where $c_{\mathbf{u}}(x)$ is the companion polynomial of \mathbf{u} . Thus $c_{\mathbf{u}}$ must be a divisor of both p and q . But $\gcd(p, q) = 1$, hence $c_{\mathbf{u}} = 1$. This forces $\mathbf{u} = 0$, which implies $V_p \cap V_q = \{0\}$.

To show that $V_p + V_q = V_{pq}$ we first note that

$$(p(x)q(x)) \cdot \mathbf{u} = q(\tau)(p(\tau)(u_p)) + p(\tau)(q(\tau)(u_q)) = 0.$$

Hence $V_p + V_q \subseteq V_{pq}$. Moreover,

$$\begin{aligned} \dim(V_p + V_q) &= \dim V_p + \dim V_q - \dim(V_p \cap V_q) \\ &= \dim V_p + \dim V_q \quad (\text{since } V_p \cap V_q = \{0\}) \\ &= \deg(p) + \deg(q) \quad (\text{Corollary 3.1.5}) \\ &= \deg(pq) \\ &= \dim V_{pq}. \end{aligned}$$

Therefore $V_p + V_q = V_{pq}$. □

Corollary 3.1.11. *Suppose that $p(x) \in \mathbb{C}[x]$ factors as $p(x) = (x - \alpha_1)^{e_1} \cdots (x - \alpha_t)^{e_t}$ where the α_i 's are all distinct and non-zero. Then $V_p = \bigoplus_{i=1}^t V_{(x - \alpha_i)^{e_i}}$.*

The proof of the above Corollary follows from induction on t and the use of Proposition 3.1.10.

Proposition 3.1.12. *Let $\alpha \in \mathbb{C} \setminus \{0\}$ and $e \in \mathbb{Z}_{>0}$. Then $0 \neq (a_n)_{n \geq 0} \in V_{(x - \alpha)^e}$ if and only if there exist a polynomial $p(x) \in \mathbb{C}[x] \setminus \{0\}$ with $\deg(p(x)) < e$ such that $a_n = p(n)\alpha^n$ for every $n \geq 0$. When this holds, this polynomial $p(x)$ is uniquely determined by $(a_n)_{n \geq 0}$.*

Proof. Suppose $a_n = p(n)\alpha^n$ for every $n \geq 0$. Then

$$\begin{aligned} (x - \alpha) \cdot a_n &= a_{n+1} - \alpha a_n \\ &= p(n+1)\alpha^{n+1} - p(n)\alpha^{n+1} \\ &= \alpha(p(n+1) - p(n))\alpha^n \end{aligned}$$

where after expanding we find that the degree of the polynomial in front of α^n is $\deg(p(x)) - 1 < e - 1$. Then by reiterating the above process we deduce that $(x - \alpha)^e \cdot a_n = 0$ for all $n \geq 0$, i.e., $(a_n)_{n \geq 0} \in V_{(x-\alpha)^e}$.

From what we have just shown, it becomes clear that

$$\{(\alpha^n)_{n \geq 0}, (n\alpha^n)_{n \geq 0}, \dots, (n^{e-1}\alpha^n)_{n \geq 0}\} \subseteq V_{(x-\alpha)^e}.$$

This set is clearly linearly independent and hence, since $\dim V_{(x-\alpha)^e} = e$, it follows that $\{(\alpha^n)_{n \geq 0}, (n\alpha^n)_{n \geq 0}, \dots, (n^{e-1}\alpha^n)_{n \geq 0}\}$ forms a basis for $V_{(x-\alpha)^e}$. Therefore if $(a_n)_{n \geq 0} \in V_{(x-\alpha)^e}$, then $a_n = p(n)\alpha^n$ for every $n \geq 0$ where $p(x)$ is a unique non-zero complex polynomial with $\deg(p) < e$. \square

From here it is clear that Theorem 3.1.9 follows directly from Corollary 3.1.11 and Proposition 3.1.12.

We end this section with an important application of Theorem 3.1.9 that will be useful when showing that θ is not quadratic.

Proposition 3.1.13. *Let $(a_n)_{n \geq 0} \in \mathbb{C}^{\mathbb{N}} \setminus \{0\}$ and let q be a complex number which is not a root of unity. If $(a_n)_{n \geq 0}$ satisfies the following relation*

$$a_{n+1} = q^{n+1}a_n - 1$$

for every $n \geq 0$, then $(a_n)_{n \geq 0}$ is not a linear recurrence sequence.

Proof. Suppose otherwise and let

$$c_{\mathbf{a}}(x) = \prod_{j=1}^s (x - \alpha_j)^{e_j}$$

be the companion polynomial of a_n where the α_j 's are distinct complex numbers. Then by Theorem 3.1.9 there exist unique polynomials $p_1(x), \dots, p_s(x) \in \mathbb{C}[x] \setminus \{0\}$ with $\deg(p_i(x)) \leq e_i - 1$, for all $1 \leq i \leq s$, such that

$$a_n = \sum_{i=1}^s p_i(n)\alpha_i^n \tag{16}$$

for every $n \geq 0$. By applying (16) to the hypothesis we get

$$\sum_{i=1}^s p_i(n+1)\alpha_i^{n+1} = \left(\sum_{i=1}^s qp_i(n)(q\alpha_i)^n \right) - 1 \quad (17)$$

for every $n \geq 0$.

It is clear that both a_n and $q^{n+1}a_n - 1$ are linear recurrence sequences with representations given in formula (17) and that $q\alpha_1, \dots, q\alpha_s$ are all distinct.

If $1 \neq q\alpha_i$ for any $i = 1, \dots, s$, then $1, q\alpha_1, \dots, q\alpha_s$ are all distinct. Hence the equation on the right hand side of (17) is the unique representation of $q^{n+1}a_n - 1$ by Theorem 3.1.9. Thus by the uniqueness of the companion polynomial we conclude from (17) that

$$\prod_{j=1}^s (x - \alpha_j)^{e_j} = \prod_{j=1}^s (x - q\alpha_j)^{e_j} (x - 1),$$

which is clearly absurd. Hence there must exist an $i \in \{1, \dots, s\}$ such that $1 = q\alpha_i$.

Then by comparing the frequencies of the linear recurrence sequences on both sides of (17), we deduce that

$$\{\alpha_1, \dots, \alpha_s\} = \{q\alpha_1, \dots, q\alpha_s\}.$$

This implies that

$$q\alpha_i \in \{\alpha_1, \dots, \alpha_s\}$$

for all $i = 1, \dots, s$. Then for every $n \geq 1$ we obtain

$$q^n \alpha_i \in \{\alpha_1, \dots, \alpha_s\}$$

for all $i = 1, \dots, s$. Thus there must exist positive integers n and m with $n > m$ such that

$$q^n \alpha_1 = q^m \alpha_1.$$

By dividing both sides by $q^m \alpha_1$ we deduce that $q^{n-m} = 1$, i.e. q is a root of unity, contradiction. Therefore $(a_n)_{n \geq 0}$ is not a linear recurrence sequence. \square

3.1.2 Hankel Determinant

In this section we follow the paper [9, p.2-5] written by Robert Rumely.

Definition 3.1.14. Let $\mathbf{a} = (a_n)_{n \geq 0} \in \mathbb{C}^{\mathbb{N}}$. We define the Hankel Determinant on the sequence \mathbf{a} to be

$$K_n := \begin{vmatrix} a_0 & a_1 & \cdots & a_n \\ a_1 & a_2 & \cdots & a_{n+1} \\ \vdots & & & \vdots \\ a_n & a_{n+1} & \cdots & a_{2n} \end{vmatrix} = \det(a_{i+j})_{0 \leq i, j \leq n}.$$

Proposition 3.1.15. Let $(a_n)_{n \geq 0} \in \mathbb{C}^{\mathbb{N}}$ and let $m \in \mathbb{N}$. Then the following conditions are equivalent.

- 1) $K_n = 0$ for all $n > m$, but $K_m \neq 0$.
- 2) $(a_n)_{n \geq 0}$ is a linear recurrence sequence of order $m + 1$.

Proof. Suppose there exists $m \in \mathbb{N}$ such that $K_m \neq 0$ but $K_{m+t} = 0$ for all $t \geq 1$. Since $K_m \neq 0$ but $K_{m+1} = 0$ then the $(m + 2) \times (m + 2)$ matrix

$$(a_{i+j})_{0 \leq i, j \leq m+1} = \begin{pmatrix} a_0 & \cdots & a_m & a_{m+1} \\ \vdots & & \vdots & \vdots \\ a_m & \cdots & a_{2m} & a_{2m+1} \\ a_{m+1} & \cdots & a_{2m+1} & a_{2(m+1)} \end{pmatrix}$$

has rank $m + 1$. Hence there exists unique constants $z_1, \dots, z_{m+1} \in \mathbb{C}$ such that

$$a_n = \sum_{j=1}^{m+1} z_j a_{n-j}$$

for $n = m + 1, \dots, 2(m + 1)$. Setting

$$s(a_n) = a_n - \sum_{j=1}^{m+1} z_j a_{n-j},$$

it then becomes apparent that to show that $(a_n)_{n \geq 0}$ is a linear recurrence sequence of order $m + 1$ it suffices to show that $s(a_n) = 0$ for all $n \geq m + 1$. We have just shown that this hold for $n = m + 1, \dots, 2(m + 1)$. So suppose $s(a_n) = 0$ holds for all $m + 1 \leq n < t$, where $t = (m + 1) + N$ for some $N > (m + 1)$. Letting C_i denote the i^{th} column of the matrix $A_N = (a_{i+j})_{0 \leq i, j \leq N}$, we apply the following column operations

$$C_i \longrightarrow s(C_i) = C_i - \sum_{j=1}^{m+1} z_j C_{i-j}$$

on columns $C_N, C_{N-1}, \dots, C_{m+1}$. By our induction hypothesis this gives the following matrix,

$$\tilde{A}_N = \begin{pmatrix} a_0 & \cdots & a_m & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & & \vdots \\ a_m & \cdots & a_{2m} & 0 & \cdots & 0 \\ a_{m+1} & \cdots & a_{2m+1} & 0 & \cdots & s(a_t) \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ a_N & \cdots & a_{N+m} & s(a_t) & \cdots & s(a_{2N}) \end{pmatrix}.$$

From here we conclude that

$$K_N = \det(\tilde{A}_N) = \pm K_m s(a_t)^{N-t}.$$

However, since $K_N = 0$ and $K_m \neq 0$, then $s(a_t) = 0$.

Therefore by induction

$$a_n = \sum_{j=1}^{m+1} z_j a_{n-j}$$

for all $n \geq m + 1$.

The other direction uses the same techniques, thus is left as an exercise to the reader. □

3.1.3 Length of Polynomials

Definition 3.1.16. Let $p(x) = \sum_{j=0}^n a_j x^j \in \mathbb{C}[x]$. We define the *length* of $p(x)$ to be $L(p(x)) := \sum_{j=0}^n |a_j|$.

Proposition 3.1.17. *Let $f_1, \dots, f_s \in \mathbb{C}[x]$ and let $d = \deg(f_1 \cdots f_s)$. Then*

$$1) L(\sum_{v=1}^s f_v) \leq \sum_{v=1}^s L(f_v)$$

$$2) L(f_1 \cdots f_s) \leq L(f_1) \cdots L(f_s) \leq 2^d L(f_1 \cdots f_s).$$

The proof of part 1 of Proposition 3.1.17 follows directly from the triangle inequality. Thus we will omit this part and focus on proving 2. This was studied in more generality by Mahler in his paper [5], where he uses results drawn from an earlier paper he wrote, [4]. To get started we introduce the following definition which is found in [5].

Definition 3.1.18. Let $f \in \mathbb{C}[x]$. The *Mahler measure* of f , denoted $M(f)$, is defined to be

$$M(f) = \begin{cases} \exp\left(\frac{1}{2\pi} \int_0^{2\pi} \log |f(e^{i\theta})| d\theta\right) & \text{if } f \neq 0 \\ 0 & \text{otherwise} \end{cases}$$

the geometric mean of $|f(x)|$ on the unit circle.

Remark 3.1.19. It can be shown that the above definition is well defined, even if f has zeros on the unit circle. Moreover, since the exponential function takes strictly positive values on \mathbb{R} it becomes clear that $M(f) > 0$ for $f \neq 0$.

Proposition 3.1.20. *Given $f, g \in \mathbb{C}[x]$, we have $M(fg) = M(f)M(g)$.*

Proof. If either f or g is zero then the proposition becomes trivial. So suppose f and g are both non-zero. Then

$$\begin{aligned} M(fg) &= \exp \frac{1}{2\pi} \int_0^{2\pi} \log |f(e^{i\theta})g(e^{i\theta})| d\theta \\ &= \exp \frac{1}{2\pi} \int_0^{2\pi} (\log |f(e^{i\theta})| + \log |g(e^{i\theta})|) d\theta \\ &= \exp \left(\frac{1}{2\pi} \int_0^{2\pi} \log |f(e^{i\theta})| d\theta \right) \exp \left(\frac{1}{2\pi} \int_0^{2\pi} \log |g(e^{i\theta})| d\theta \right) \\ &= M(f)M(g). \end{aligned}$$

□

Lemma 3.1.21. *Let $f \in \mathbb{C}[x]$. Then $|f(e^{i\theta})| \leq L(f)$ for any $\theta \in \mathbb{R}$.*

Proof. Write $f(x) = \sum_{j=0}^n a_j x^j$. Then

$$|f(e^{i\theta})| \leq \sum_{j=0}^n |a_j| |e^{i\theta}|^j = \sum_{j=0}^n |a_j| = L(f).$$

□

Lemma 3.1.22. *Let $f \in \mathbb{C}[x]$. Then $M(f) \leq L(f)$.*

Proof. Once again the case where $f = 0$ is trivial. So suppose otherwise, then from Lemma 3.1.21 and the fact $\exp(x)$ and $\log(x)$ are strictly increasing functions we get

$$\begin{aligned} M(f) &= \exp \frac{1}{2\pi} \int_0^{2\pi} \log |f(e^{i\theta})| d\theta \\ &\leq \exp \frac{1}{2\pi} \int_0^{2\pi} \log |L(f)| d\theta \\ &= \exp \frac{1}{2\pi} 2\pi \log |L(f)| \\ &= L(f). \end{aligned}$$

□

For the next Lemma write $f(x) = \sum_{j=0}^n a_j x^j \in \mathbb{C}[x]$. We assume that $f(0) \neq 0$, and that ξ_1, \dots, ξ_n are the zeros of f , counting multiplicity, with the following ordering

$$|\xi_1| \leq |\xi_2| \leq \dots \leq |\xi_N| \leq 1 < |\xi_{N+1}| \leq \dots \leq |\xi_n|. \quad (18)$$

We now recall Jensen's formula from Complex Analysis,

$$\begin{aligned} \log(M(f)) &= \log |f(0)| + \sum_{v=1}^N \log \frac{1}{|\xi_v|} \\ &= \log \left| \frac{a_0}{\xi_1 \xi_2 \dots \xi_N} \right|. \end{aligned} \quad (19)$$

We will not prove this here but the proof can be found in many graduate text books on Complex Analysis, for example [3, chap XII, §1].

Remark 3.1.23. Since $a_n \xi_1 \dots \xi_n = \mp a_0$, then from (19) it becomes clear that

$$M(f) = \left| \frac{a_0}{\xi_1 \xi_2 \dots \xi_N} \right| = |a_n \xi_{N+1} \dots \xi_n|. \quad (20)$$

Lemma 3.1.24. *With the above notation, for each $k = 0, \dots, n$, we have*

$$|a_k| \leq \binom{n}{k} M(f).$$

Proof. For any integers $1 \leq i_1 < i_2 < \dots < i_m \leq n$, we find that

$$|a_n \xi_{i_1} \xi_{i_2} \cdots \xi_{i_m}| \leq |a_n \xi_{N+1} \cdots \xi_n| = M(f)$$

by (18) and (20). Thus for each $k = 0, \dots, n$, we conclude that

$$\begin{aligned} |a_k| &= \left| \sum_{0 \leq i_1 < \dots < i_k \leq n} a_n \xi_{i_1} \cdots \xi_{i_k} \right| \\ &\leq \sum_{0 \leq i_1 < \dots < i_k \leq n} |a_n \xi_{i_1} \cdots \xi_{i_k}| \\ &\leq \binom{n}{k} M(f). \end{aligned} \quad \square$$

Lemma 3.1.25. *For any $f(x) \in \mathbb{C}[x]$ of degree less than or equal to n , we have that $L(f) \leq 2^n M(f)$.*

Proof. Suppose first that $f(0) \neq 0$. With the notation of Lemma 3.1.24, we have $|a_k| \leq \binom{n}{k} M(f)$. It then follows that

$$L(f) = \sum_{j=0}^n |a_j| \leq \sum_{j=0}^n \binom{n}{j} M(f) = 2^n M(f).$$

If $f(0) = 0$, then we can write $f(x)$ as

$$f(x) = x^m g(x)$$

for some integer $m \geq 1$ and for some $g(x) \in \mathbb{C}[x]$ where $g(0) \neq 0$. It is then easily seen that

$$L(f) = L(x^m g) = L(g), \text{ and } M(f) = M(g).$$

The conclusion then follows from applying the same argument as above to $g(x)$. \square

Proof of Proposition 3.1.17: Part 2. For each $v = 1, \dots, s$, write $f_v(x) = \sum_{j=0}^{n_v} a_{vj}x^j$.

We first obtain, by the triangle inequality, that

$$\begin{aligned}
 L(f_1 \cdots f_s) &= L\left(\sum_{l=0}^d \left(\sum_{k_1+\dots+k_s=l} a_{1k_1} \cdots a_{sk_s}\right) x^l\right) \\
 &= \sum_{l=0}^d \left| \sum_{k_1+\dots+k_s=l} a_{1k_1} \cdots a_{sk_s} \right| \\
 &\leq \sum_{l=0}^d \left(\sum_{k_1+\dots+k_s=l} |a_{1k_1}| \cdots |a_{sk_s}|\right) \\
 &= \prod_{v=1}^s \left(\sum_{j=0}^{n_v} |a_{vj}|\right) \\
 &= L(f_1) \cdots L(f_s).
 \end{aligned}$$

Moreover, by combining Lemma 3.1.22, Lemma 3.1.25, and Proposition 3.1.20 we achieve

$$\begin{aligned}
 L(f_1) \cdots L(f_s) &\leq 2^{n_1+\dots+n_s} M(f_1) \cdots M(f_s) \\
 &= 2^d M(f_1 \cdots f_s) \\
 &\leq 2^d L(f_1 \cdots f_s).
 \end{aligned}$$

□

3.1.4 The Permanent

Definition 3.1.26. Let $A = (a_{i,j})$ be a $n \times n$ square matrix. The *permanent* of A is defined as

$$\text{perm}(A) := \sum_{\sigma \in S_n} \prod_{i=1}^n a_{i,\sigma(i)}$$

where S_n denotes the group of all permutations of $\{1, 2, \dots, n\}$.

Lemma 3.1.27. Let $A = (a_{i,j})$ be a $n \times n$ square matrix with polynomial entries. Then

$$L(\det(A)) \leq \text{perm}(L(a_{i,j})).$$

Proof. This follows directly from Proposition 3.1.17. Namely,

$$\begin{aligned} L(\det(A)) &\leq \sum_{\sigma \in S_n} L\left(\prod_i^n a_{i,\sigma(i)}\right) \\ &\leq \sum_{\sigma \in S_n} \prod_{i=1}^n L(a_{i,\sigma(i)}) \\ &= \text{perm}(L(a_{i,j})). \end{aligned}$$

□

3.2 Motivation

We begin by noticing that the truncations

$$\sum_{k=0}^n q^{-k(k+1)/2}$$

of the series defining θ provide good rational approximations to θ . This leads us to the following result.

Proposition 3.2.1. $\theta \notin \mathbb{Q}$.

Proof. Suppose otherwise and let a and b be positive integers such that $\theta = \frac{a}{b}$. Set $v_n := v_n(\theta)$ where

$$v_n(x) = q^{n(n+1)/2} \left(x - \sum_{k=0}^n q^{-k(k+1)/2} \right) \in \mathbb{Z}[x]. \quad (21)$$

Letting $c = v_n(0) \in \mathbb{Z}$, we observe that

$$\begin{aligned} \frac{a}{b} - \sum_{k=0}^n q^{-k(k+1)/2} &= \frac{a}{b} - \frac{c}{q^{n(n+1)/2}} \\ &= \frac{aq^{n(n+1)/2} - bc}{bq^{n(n+1)/2}}. \end{aligned}$$

Since

$$\frac{a}{b} - \sum_{k=0}^n q^{-k(k+1)/2} = \sum_{k=n+1}^{\infty} q^{-k(k+1)/2}$$

is positive, then it becomes clear that $aq^{n(n+1)/2} - bc$ is a positive integer. Hence

$$\frac{a}{b} - \sum_{k=0}^n q^{-k(k+1)/2} \geq \frac{1}{bq^{n(n+1)/2}}.$$

We now conclude that

$$\begin{aligned} v_n &= q^{n(n+1)/2} \left(\frac{a}{b} - \sum_{k=0}^n q^{-k(k+1)/2} \right) \\ &\geq q^{n(n+1)/2} \left(\frac{1}{bq^{n(n+1)/2}} \right) \\ &= \frac{1}{b}. \end{aligned}$$

On another note,

$$\begin{aligned} v_n &= q^{n(n+1)/2} \left(\sum_{k=n+1}^{\infty} q^{-k(k+1)/2} \right) \\ &= \frac{1}{q^{n+1}} + \frac{1}{q^{(n+2)+(n+1)}} + \frac{1}{q^{(n+3)+(n+2)+(n+1)}} + \dots \\ &= \frac{1}{q^{n+1}} \left(1 + \frac{1}{q^{n+2}} + \frac{1}{q^{(n+3)+(n+2)}} + \dots \right) \\ &\leq \frac{1}{q^{n+1}} \left(1 + \frac{1}{q^2} + \frac{1}{q^3} + \dots \right) \\ &\leq \frac{S}{q^{n+1}} \end{aligned}$$

where $S = \frac{q}{q-1} \leq 2$. This upper bound clearly tends to zero as n goes to infinity, thus so does v_n . This leads to a contradiction.

Therefore $\theta \notin \mathbb{Q}$. □

We see that the above proof is based on the observation that the truncations give good enough approximations to deduce irrationality of θ . However if one was to apply Liouville's Theorem we would find that the truncations aren't enough to deduce non-quadraticity of θ . This leads us to Bézivin's method which is a generalization of the above proof of irrationality. This method contains three main parts which heavily focus on the following definition.

Definition 3.2.2. For $h, \ell \geq 1$, we let $V_{h,\ell}(x) \in \mathbb{Z}[x]$ denote the Hankel Determinant of order $\ell + 1$ on the sequence $(v_n(x))_{n \geq h}$ defined by (21). Namely,

$$V_{h,\ell}(x) := \begin{vmatrix} v_h(x) & v_{h+1}(x) & \dots & v_{h+\ell}(x) \\ v_{h+1}(x) & v_{h+2}(x) & \dots & v_{h+\ell+1}(x) \\ \vdots & & & \vdots \\ v_{h+\ell}(x) & v_{h+\ell+1}(x) & \dots & v_{h+2\ell}(x) \end{vmatrix} = \det(v_{h+i+j-2}(x))_{1 \leq i, j \leq \ell+1}.$$

Roughly speaking the idea is to give estimates on the length and content of $V_{1,\ell}(x)$ as well as on the absolute value of $V_{1,\ell}(\theta)$. This will allow us to deduce that $V_{1,\ell}(\theta)$ vanishes for all $\ell \gg 1$ if θ is quadratic. But we will show that this is impossible.

To give some motivation behind what was discussed above we consider the following. By expanding $v_n := v_n(\theta)$ in terms of powers of q^{-1} , we find that

$$\begin{aligned} v_n = v_n(\theta) &= \sum_{k=n+1}^{\infty} q^{n(n+1)/2 - k(k+1)/2} \\ &= \sum_{k=1}^{\infty} q^{n(n+1)/2 - (n+k)(n+k+1)/2} \\ &= \sum_{k=1}^{\infty} q^{-kn - k(k+1)/2} \\ &= \frac{1}{q^{n+1}} + \frac{1}{q^{2n+3}} + \dots + \frac{1}{q^{kn + \binom{k+1}{2}}} + \dots \end{aligned} \quad (22)$$

This gives the following Lemma.

Lemma 3.2.3. *For any fixed $t \geq 1$, we have that*

$$v_n^{(t)} := \sum_{k=1}^t q^{-\binom{k+1}{2}} q^{-kn}$$

is a linear recurrence sequence of order t with companion polynomial

$$c_t(x) = \prod_{k=1}^t \left(x - \frac{1}{q^k} \right).$$

Proof. It is clear that $(q^{-kn})_{n \geq 0}$ is a linear recurrence sequence with companion polynomial $x - \frac{1}{q^k}$, for every $k \geq 1$. Since q^{-1}, \dots, q^{-t} are distinct, then by Proposition 3.1.8, $\{(q^{-kn})_{n \geq 0}\}_{k=1}^t$ is a basis of V_{c_t} . From here we conclude that $v_n^{(t)} \in V_{c_t}$. Since the coefficients $q^{-\binom{k+1}{2}}$ are non-zero, $v_n^{(t)}$ is a linear recurrence sequence with companion polynomial c_t . \square

From (22) it becomes apparent that v_n can be approximated as well as we want by the linear recurrence sequence $v_n^{(t)}$ upon choosing t sufficiently large. Moreover, by substituting $v_n^{(t)}$ for $v_n(x)$ in $V_{1,\ell}(x)$, we know from Hankel's criterion (Proposition 3.1.15) that

$$\det(v_{i+j-1}^{(t)})_{1 \leq i, j \leq \ell+1} = 0$$

for all $\ell \gg 1$. Putting all of this together leads us to suspect that $|V_{1,\ell}(\theta)|$ should get small as ℓ gets large. This gives the possibility of $V_{1,\ell}(\theta)$ vanishing for all $\ell \gg 1$ if θ is quadratic.

Now that we have a game plan laid out lets begin with the first estimation.

3.3 Estimation of Degree and Length

The main task in this section is to obtain control on the growth of the length of $V_{h,\ell}(x)$. But before we get to that we will give an estimate on the degree of $V_{h,\ell}(x)$.

It is clear by definition that $V_{h,\ell}(x)$ is a polynomial with integer coefficients and the matrix corresponding to $V_{h,\ell}(x)$ has integer polynomial entries of degree less than or equal to 1. Hence it becomes clear that $\deg V_{h,\ell}(x) \leq \ell + 1$

We now state the main result in this section.

Proposition 3.3.1. $\deg(V_{h,\ell}(x)) \leq \ell + 1$ and $L(V_{h,\ell}(x)) \leq q^{2\ell^3/3 + \ell^2 h + \ell h^2/2 + O(h^2 + \ell^2)}$.

To achieve the estimate of the length we will need the following two Lemmas.

Lemma 3.3.2. For all $n \geq 1$, $L(v_n(x)) \leq 3q^{n(n+1)/2}$.

Proof. We observe that

$$\begin{aligned} \sum_{k=0}^n q^{n(n+1)/2-k(k+1)/2} &\leq \sum_{k=0}^n q^{n(n+1)/2-k} \\ &\leq \sum_{k=0}^n 2^{-k} q^{n(n+1)/2} \\ &\leq 2q^{n(n+1)/2} \end{aligned}$$

where the second last inequality uses the hypothesis $q \geq 2$. We then deduce that

$$\begin{aligned} L(v_n(x)) &= q^{n(n+1)/2} + \sum_{k=0}^n q^{n(n+1)/2-k(k+1)/2} \\ &\leq 3q^{n(n+1)/2}. \end{aligned} \quad \square$$

Lemma 3.3.3. *Let $(a_i)_{i \geq 1}$ be a sequence of real numbers that satisfy*

$$a_{i+2} - 2a_{i+1} + a_i \geq 0$$

for all $i \geq 1$. Then for all positive integers n and q , we have

$$\text{perm} \begin{pmatrix} q^{a_1} & q^{a_2} & \cdots & q^{a_n} \\ q^{a_2} & q^{a_3} & \cdots & q^{a_{n+1}} \\ \vdots & & & \vdots \\ q^{a_n} & q^{a_{n+1}} & \cdots & q^{a_{2n-1}} \end{pmatrix} \leq n! q^{a_1 + a_3 + \cdots + a_{2n-1}}.$$

Proof. By definition

$$\text{perm}(q^{a_{i+j-1}})_{1 \leq i, j \leq n} = \sum_{\sigma \in S_n} \prod_{i=1}^n q^{a_{i+\sigma(i)-1}}.$$

Thus it suffices to show that

$$\sum_{i=1}^n a_{i+\sigma(i)-1} \leq a_1 + a_3 + \cdots + a_{2n-1} \quad (23)$$

for all $\sigma \in S_n$.

The case $n = 1$ is trivial, so let $n \geq 2$ and suppose (23) holds for all $(n-1) \times (n-1)$ matrices. Let $\sigma \in S_n$.

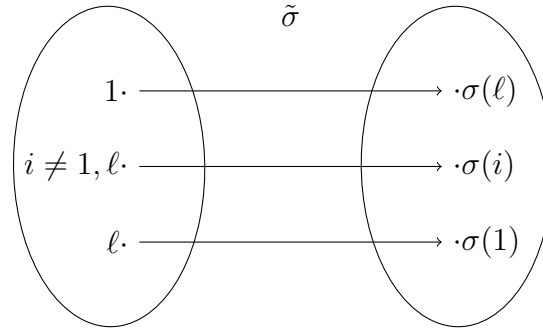
Case 1 : If $\sigma(1) = 1$, then by applying the induction hypothesis to the $(n-1) \times (n-1)$ matrix obtained by deleting the first row and column from $(q^{a_i+j-1})_{1 \leq i, j \leq n}$ and to the restriction of σ to $\{2, \dots, n\}$, we achieve

$$\sum_{i=2}^n a_{i+\sigma(i)-1} \leq a_3 + a_5 + \dots + a_{2n-1}.$$

Hence (23) follows since $a_{1+\sigma(1)-1} = a_1$.

Case 2 : If $\sigma(1) \neq 1$, then by letting $k = \sigma(1)$ and $\ell = \sigma^{-1}(1)$, we define $\tilde{\sigma} \in S_n$ as

$$\tilde{\sigma}(i) = \begin{cases} \sigma(i), & \text{if } i \neq 1, \ell \\ \sigma(\ell), & \text{if } i = 1 \\ \sigma(1), & \text{if } i = \ell. \end{cases}$$



We then attain

$$\sum_{\substack{i=1 \\ i \neq 1, \ell}}^n a_{i+\sigma(i)-1} = \sum_{\substack{i=1 \\ i \neq 1, \ell}}^n a_{i+\tilde{\sigma}(i)-1}$$

where the left hand side is equal to

$$\sum_{i=1}^n a_{i+\sigma(i)-1} - a_{1+\sigma(1)-1} - a_{\ell+\sigma(\ell)-1}$$

and the right hand side is equal to

$$\sum_{i=1}^n a_{i+\tilde{\sigma}(i)-1} - a_{1+\tilde{\sigma}(1)-1} - a_{\ell+\tilde{\sigma}(\ell)-1}.$$

After rearranging we obtain

$$\begin{aligned} \sum_{i=1}^n a_{i+\sigma(i)-1} &= \sum_{i=1}^n a_{i+\tilde{\sigma}(i)-1} + (a_{1+\sigma(1)-1} + a_{\ell+\sigma(\ell)-1} - a_{1+\tilde{\sigma}(1)-1} - a_{\ell+\tilde{\sigma}(\ell)-1}) \\ &= \sum_{i=1}^n a_{i+\tilde{\sigma}(i)-1} + (a_k + a_\ell - a_1 - a_{\ell+k-1}). \end{aligned}$$

Since $\tilde{\sigma}(1) = 1$, then by case 1 we know

$$\sum_{i=1}^n a_{i+\tilde{\sigma}(i)-1} \leq a_1 + a_3 + \cdots + a_{2n-1}.$$

Thus it suffices to show that

$$a_k + a_\ell - a_1 - a_{\ell+k-1} \leq 0$$

for all $k, \ell \geq 2$. Well this relation holds if and only if

$$(\tau^{k+\ell-2} - \tau^{k-1} - \tau^{\ell-1} + 1)a_1 \geq 0$$

for all $k, \ell \geq 2$, where τ denotes the shift operator. After noting that

$$\tau^{k-1} - 1 = (\tau - 1)(1 + \tau + \tau^2 + \cdots + \tau^{k-2}),$$

we get

$$\begin{aligned} (\tau^{k+\ell-2} - \tau^{k-1} - \tau^{\ell-1} + 1) &= (\tau^{k-1} - 1)(\tau^{\ell-1} - 1) \\ &= \left(\sum_{n=0}^{k-2} \tau^n \right) \left(\sum_{n=0}^{\ell-2} \tau^n \right) (\tau - 1)^2 \end{aligned}$$

where

$$(\tau - 1)^2 a_i = a_{i+2} - 2a_{i+1} + a_i \geq 0$$

for all $i \geq 1$.

This completes the proof of the Lemma. □

Proof of Proposition 3.3.1. By Lemmas 3.1.27 and 3.3.2 we obtain

$$\begin{aligned} L(V_{h,\ell}(x)) &\leq \text{perm}(L(v_{h+i+j-2}(x)))_{1 \leq i,j \leq \ell+1} \\ &\leq 3^{\ell+1} \text{perm} \begin{pmatrix} q^{\binom{h+1}{2}} & \dots & q^{\binom{h+\ell+1}{2}} \\ \vdots & & \vdots \\ q^{\binom{h+\ell+1}{2}} & \dots & q^{\binom{h+2\ell+1}{2}} \end{pmatrix}. \end{aligned} \quad (24)$$

Our next step is to apply Lemma 3.3.3 to (24). To do so we need the Lemma's hypothesis to be satisfied; we achieve this by applying the identity $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ to get

$$\begin{aligned} \binom{h+i+2}{2} - 2\binom{h+i+1}{2} + \binom{h+i}{2} &= \binom{h+i+1}{1} + \binom{h+i+1}{2} - 2\binom{h+i+1}{2} + \binom{h+i}{2} \\ &= \binom{h+i+1}{1} - \binom{h+i}{1} - \binom{h+i}{2} + \binom{h+i}{2} \\ &= \binom{h+i+1}{1} - \binom{h+i}{1} \\ &= 1 \end{aligned}$$

for all $i \geq 1$. Hence by Lemma 3.3.3 we conclude that

$$L(V_{h,\ell}(x)) \leq 3^{\ell+1}(\ell+1)!q^{\binom{h+1}{2}+\binom{h+3}{2}+\dots+\binom{h+2\ell+1}{2}}.$$

After observing that

1. $3^{\ell+1} \leq 2^{\ell^2} \leq q^{\ell^2}$, for $\ell \geq 2$
2. $(\ell+1)! \leq (\ell+1)^{\ell+1} \leq (2^\ell)^{\ell+1} \leq q^{2\ell^2}$,

it then becomes clear that to prove our claim it suffices to show that

$$\sum_{i=0}^{\ell} \binom{h+2i+1}{2} \leq \frac{2}{3}\ell^3 + \ell^2 h + \frac{1}{2}\ell h^2 + O(\ell^2 + h^2).$$

We achieve this by noting that the function

$$f(x) = \binom{h+2x+1}{2} = \frac{(h+2x+1)(h+2x)}{2}$$

is strictly increasing on the interval $[0, \infty)$. This gives

$$\begin{aligned}
\sum_{i=0}^{\ell} \binom{h+2i+1}{2} &\leq \int_0^{\ell+1} \binom{h+2x+1}{2} dx \\
&= \int_0^{\ell+1} \left(2x^2 + 2xh + x + \frac{h^2+h}{2} \right) dx \\
&= \left(\frac{2x^3}{3} + x^2h + \frac{x^2}{2} + \frac{x(h^2+h)}{2} \right)_0^{\ell+1} \\
&\leq \frac{2}{3}\ell^3 + \ell^2h + \frac{1}{2}\ell h^2 + O(\ell^2 + h^2).
\end{aligned}$$

□

Corollary 3.3.4. $L(V_{1,\ell}(x)) \leq q^{\frac{2}{3}\ell^3 + O(\ell^2)}$.

3.4 Estimation of Absolute Value

In this section we will show that the absolute value of $V_{1,\ell}(\theta)$ tends to zero as ℓ goes to infinity. This follows directly from the main result of this section which we will now state.

Proposition 3.4.1. $|V_{h,\ell}(\theta)| \leq q^{-\frac{1}{2}\ell^3 - \frac{1}{2}h\ell^2 + O(\ell^2 + h\ell)}$.

To compute this upper bound we need the following collection of Lemmas.

Lemma 3.4.2. *For any $p(x) = \sum_{i=0}^m a_i x^i \in \mathbb{C}[x]$, the shift operator τ induces the following action on our sequence v_n*

$$p(\tau)v_n = \sum_{k=1}^{\infty} p(1/q^k) q^{-kn - k(k+1)/2}.$$

Proof. By definition $p(\tau)v_n = \sum_{i=0}^m a_i v_{n+i}$. Using the expansion of v_n found in (22), we find that

$$\begin{aligned}
v_{n+i} &= \frac{1}{q^{(n+i)+1}} + \frac{1}{q^{2(n+i)+3}} + \cdots + \frac{1}{q^{k(n+i) + \binom{k+1}{2}}} + \cdots \\
&= \frac{1}{q^i} \left(\frac{1}{q^{n+1}} \right) + \frac{1}{q^{2i}} \left(\frac{1}{q^{2n+3}} \right) + \cdots + \frac{1}{q^{ki}} \left(\frac{1}{q^{kn + \binom{k+1}{2}}} \right) + \cdots.
\end{aligned}$$

Substituting this expansion into $p(\tau)v_n = \sum_{i=0}^m a_i v_{n+i}$ we conclude that

$$\begin{aligned} p(\tau)v_n &= \sum_{i=0}^m \sum_{k=1}^{\infty} a_i (q^{-k})^i \left(q^{-kn - \binom{k+1}{2}} \right) \\ &= \sum_{k=1}^{\infty} p(1/q^k) q^{-kn - k(k+1)/2}. \end{aligned} \quad \square$$

By the above lemma we get

$$\begin{aligned} c_{i-1}(\tau)c_{j-1}(\tau)v_h &= \sum_{k=1}^{\infty} c_{i-1} \left(\frac{1}{q^k} \right) c_{j-1} \left(\frac{1}{q^k} \right) q^{-kh - \frac{1}{2}k(k+1)} \\ &= \sum_{k=\max(i,j)}^{\infty} c_{i-1} \left(\frac{1}{q^k} \right) c_{j-1} \left(\frac{1}{q^k} \right) q^{-kh - \frac{1}{2}k(k+1)}, \end{aligned} \quad (25)$$

where the last equality follows since for $k < \max(i, j)$ at least one of the polynomials $c_{i-1}(x)$ and $c_{j-1}(x)$ vanishes at $\frac{1}{q^k}$; refer back to Lemma 3.2.3.

This leads us to consider the following.

Lemma 3.4.3. *For each $i = 0, \dots, \ell$, let $p_i(x)$ and $q_i(x)$ be monic polynomials of degree i . Then*

$$V_{h,\ell}(x) = \det((p_{i-1}(\tau)q_{j-1}(\tau)v_h)(x))_{1 \leq i,j \leq \ell+1}.$$

Proof. For each $i = 0, \dots, \ell$, write

$$p_i(x) = \sum_{s=0}^i a_{i,s} x^s \quad \text{and} \quad q_i(x) = \sum_{r=0}^i b_{i,r} x^r$$

where $a_{i,i} = b_{i,i} = 1$.

First we apply the following row operations sequentially on the rows

$$R_{\ell+1}, \dots, R_1$$

of the matrix $(v_{h+i+j-2}(x))_{1 \leq i,j \leq \ell+1}$

$$R_i \longrightarrow R_i + a_{i-1,i-2}R_{i-1} + \dots + a_{i-1,0}R_1.$$

Then the $(i, j)^{th}$ entry in our new matrix is

$$\begin{aligned}
& v_{h+i+j-2}(x) + a_{i-1,i-2}v_{h+i-1+j-2}(x) + \cdots + a_{i-1,0}v_{h+j-2}(x) \\
&= \sum_{s=0}^{i-1} a_{i-1,s}v_{h+s+1+j-2}(x) \\
&= \sum_{s=0}^{i-1} a_{i-1,s}\tau^s v_{h+j-1}(x) \\
&= p_{i-1}(\tau)v_{h+j-1}(x).
\end{aligned}$$

Hence

$$V_{h,\ell}(x) = \det((p_{i-1}(\tau)v_{h+j-1})(x))_{1 \leq i,j \leq \ell+1}.$$

Next we apply the following column operations sequentially on the columns

$$C_{\ell+1}, \dots, C_1$$

of the matrix $((p_{i-1}(\tau)v_{h+j-1})(x))_{1 \leq i,j \leq \ell+1}$

$$C_j \longrightarrow C_j + b_{j-1,j-2}C_{j-1} + \cdots + b_{j-1,0}C_1.$$

The new $(i, j)^{th}$ entry is

$$\begin{aligned}
& p_{i-1}(\tau)v_{h+j-1}(x) + b_{j-1,j-2}(p_{i-1}(\tau)v_{h+j-2})(x) + \cdots + b_{j-1,0}(p_{i-1}(\tau)v_h)(x) \\
&= p_{i-1}(\tau) \sum_{r=0}^{j-1} b_{j-1,r}v_{h+r}(x) \\
&= p_{i-1}(\tau) \sum_{r=0}^{j-1} b_{j-1,r}\tau^r v_h(x) \\
&= (p_{i-1}(\tau)q_{j-1}(\tau)v_h)(x).
\end{aligned}$$

Therefore

$$V_{h,\ell}(x) = \det((p_{i-1}(\tau)q_{j-1}(\tau)v_h)(x))_{1 \leq i,j \leq \ell+1}.$$

□

By applying the above Lemma to $V_{h,l}(\theta)$ with $p_i(x) = q_i(x) = c_i(x)$, where we set $c_0(x) = 1$ and for $i \geq 1$ we let $c_i(x)$ be as defined in Lemma 3.2.3, we deduce that

$$V_{h,\ell}(\theta) = \det(c_{i-1}(\tau)c_{j-1}(\tau)v_h)_{1 \leq i,j \leq \ell+1}$$

(recall $v_n := v_n(\theta)$).

Lemma 3.4.4. *Fix $i \geq 1$. Then for all $k \geq i$, $\left|c_{i-1}\left(\frac{1}{q^k}\right)\right| \leq q^{-\binom{i}{2}}$.*

Proof. The case where $i = 1$ is trivial. So suppose $i > 1$. Then by definition

$$\begin{aligned} \left|c_{i-1}\left(\frac{1}{q^k}\right)\right| &= \prod_{r=1}^{i-1} \left|\frac{1}{q^k} - \frac{1}{q^r}\right| \\ &= \prod_{r=1}^{i-1} \left|1 - \frac{1}{q^{k-r}}\right| \left(\frac{1}{q^r}\right). \end{aligned}$$

By the choice of k we know $k - r \geq 1$, hence $1 - \frac{1}{q^{k-r}} \leq 1$ for all $r = 0, \dots, i-1$. Therefore

$$\left|c_{i-1}\left(\frac{1}{q^k}\right)\right| \leq \prod_{r=1}^{i-1} \frac{1}{q^r} = q^{-\binom{i}{2}}.$$

□

Lemma 3.4.5. *Let $(m_k)_{k \geq 1}$ be a strictly increasing sequence of positive integers. Then $\sum_{k=1}^{\infty} q^{-m_k} \leq 2q^{-m_1}$.*

Proof. From the conditions placed on $(m_k)_{k \geq 1}$, we know $0 \geq m_1 - m_i > m_1 - m_{i+1}$ for all $i \geq 1$. Therefore

$$\begin{aligned} \sum_{k=1}^{\infty} q^{-m_k} &= q^{-m_1} \sum_{k=1}^{\infty} q^{m_1 - m_k} \\ &\leq q^{-m_1} \sum_{k=0}^{\infty} q^{-k} \\ &\leq q^{-m_1} \sum_{k=0}^{\infty} 2^{-k} \quad (\text{since } q \geq 2) \\ &= 2q^{-m_1}. \end{aligned}$$

□

After applying Lemma 3.4.4 in succession with Lemma 3.4.5 to (25), we obtain

$$\begin{aligned} |c_{i-1}(\tau)c_{j-1}(\tau)v_h| &\leq q^{-\binom{i}{2}-\binom{j}{2}} \sum_{k=\max(i,j)}^{\infty} q^{-kh-\frac{1}{2}k(k+1)} \\ &\leq 2q^{-c_{ij}} \end{aligned}$$

where

$$c_{i,j} = \binom{i}{2} + \binom{j}{2} + \max(i,j)h + \binom{\max(i,j)+1}{2}.$$

Utilizing this upper bound with Lemma 3.4.3, we conclude that

$$\begin{aligned} |V_{h,\ell}(\theta)| &\leq 2^{\ell+1} \text{perm}(q^{-c_{ij}})_{1 \leq i,j \leq \ell+1} \\ &= 2^{\ell+1} \left(\prod_{i=1}^{\ell+1} q^{-\binom{i}{2}} \right) \left(\prod_{j=1}^{\ell+1} q^{-\binom{j}{2}} \right) \text{perm}(q^{-b_{ij}})_{1 \leq i,j \leq \ell+1} \\ &= 2^{\ell+1} q^{-2\binom{\ell+2}{3}} \text{perm}(q^{-b_{ij}})_{1 \leq i,j \leq \ell+1} \end{aligned} \tag{26}$$

where

$$b_{ij} = \max(i,j)h + \binom{\max(i,j)+1}{2}.$$

Lemma 3.4.6. $\text{perm}(q^{-b_{ij}})_{1 \leq i,j \leq \ell+1} \leq (\ell+1)! q^{-(\frac{\ell+2}{2})h - \binom{\ell+2}{3}}.$

Proof. By definition we get

$$\begin{aligned} \text{perm}(q^{-b_{ij}}) &= \sum_{\sigma \in S_{\ell+1}} \prod_{i=1}^{\ell+1} q^{-b_{i\sigma(i)}} \\ &\leq (\ell+1)! \max_{\sigma \in S_{\ell+1}} \prod_{i=1}^{\ell+1} q^{-b_{i\sigma(i)}} = (\ell+1)! q^{-d}. \end{aligned}$$

where

$$d = \min_{\sigma \in S_{\ell+1}} \sum_{i=1}^{\ell+1} b_{i\sigma(i)}.$$

Therefore after making the following observation

$$\begin{aligned}
\sum_{i=1}^{\ell+1} b_{i\sigma(i)} &= \sum_{i=1}^{\ell+1} \left(\max(i, \sigma(i))h + \binom{\max(i, \sigma(i)) + 1}{2} \right) \\
&\geq \sum_{i=1}^{\ell+1} \left(ih + \binom{i+1}{2} \right) \\
&\geq \sum_{i=1}^{\ell+1} \left(ih + \binom{i}{2} \right) \\
&= \binom{\ell+2}{2}h + \binom{\ell+2}{3},
\end{aligned}$$

we conclude that

$$\text{perm}(q^{-b_{ij}}) \leq (\ell+1)!q^{-\binom{\ell+2}{2}h - \binom{\ell+2}{3}}.$$

□

We now apply the above Lemma to (26) to achieve

$$|V_{h,\ell}(\theta)| \leq 2^{\ell+1}(\ell+1)!q^{-3\binom{\ell+2}{3} - h\binom{\ell+2}{2}}. \quad (27)$$

Finally after making the following computations

1. $2^{\ell+1} \leq q^{\ell+1} = q^{O(\ell^2)}$
2. $(\ell+1)! \leq (\ell+1)^{\ell+1} \leq (2^\ell)^{\ell+1} \leq q^{2\ell^2} = q^{O(\ell^2)}$
3. $3\binom{\ell+2}{3} = 3\frac{(\ell+2)(\ell+1)\ell}{6} = \frac{1}{2}\ell^3 + O(\ell^2)$
4. $h\binom{\ell+2}{2} = h\frac{(\ell+2)(\ell+1)}{2} = \frac{1}{2}h\ell^2 + O(h\ell),$

we can conclude, from (27), that

$$|V_{h,\ell}(\theta)| \leq q^{-\frac{1}{2}\ell^3 - \frac{1}{2}h\ell^2 + O(\ell^2 + h\ell)}.$$

This finishes the proof of Proposition 3.4.1. Thus as stated at the beginning of this section, we obtain the following corollary.

Corollary 3.4.7. $|V_{1,\ell}(\theta)| \leq q^{-\frac{\ell^3}{2} + O(\ell^2)}.$

3.5 Estimation of the Content

In this section we compute the final estimation needed for proving non-quadraticity of θ . Namely we give an estimation on the content of $V_{1,\ell}(x)$ (the gcd of its coefficients in \mathbb{Z}), which we will now state as the main result in this section.

Proposition 3.5.1. $V_{1,\ell}(x) \equiv 0 \pmod{q^{\frac{1}{8}\ell^3 + O(\ell^2)}} \mathbb{Z}[x]$

We begin by applying the change of variables $k \mapsto n - k$ in the formula (21) for $v_n(x)$. This gives us

$$\begin{aligned} v_n(x) &= q^{n(n+1)/2} x - \sum_{k=0}^n q^{n(n+1)/2 - (n-k)(n-k+1)/2} \\ &= q^{n(n+1)/2} x - \sum_{k=0}^n q^{kn - k(k-1)/2} \\ &= q^{n(n+1)/2} x - 1 - q^n - q^{2n-1} - \dots - q^{n^2 - n(n-1)/2}. \end{aligned} \quad (28)$$

From here we make the following observation.

Lemma 3.5.2. *Fix an integer $s \geq 1$ and set*

$$u_n^{(s)} = - \sum_{k=0}^{s-1} q^{kn - \binom{k}{2}}$$

for all $n \geq 0$. Then $(u_n^{(s)})_{n \geq 0}$ is a linear recurrence sequence of order s with companion polynomial

$$r_s(x) = (x-1)(x-q) \cdots (x-q^{s-1})$$

The proof of the above Lemma follows the same argument as Lemma 3.2.3.

Note, when $s = 0$, we define $u_n^{(0)} = 0$ for all $n \geq 0$. Then $(u_n^{(0)})_{n \geq 0}$ is a linear recurrence sequence with companion polynomial $r_0(x) = 1$.

On the basis of (28), we can prove the following.

Lemma 3.5.3. *Fix a positive integer n . If k is an integer with $0 \leq k < n$ then*

$$v_n(x) \equiv -1 - q^n - q^{2n-1} - \dots - q^{kn - \binom{k}{2}} = u_n^{(k+1)} \pmod{q^{(k+1)n - \binom{k+1}{2}}} \mathbb{Z}[x].$$

Proof. Our first step is to show that as a function of k ,

$$f(k) = kn - \binom{k}{2} \quad (29)$$

increases for $k = 0, \dots, n$. This is easily seen since

$$kn - \binom{k}{2} \leq (k+1)n - \binom{k+1}{2}$$

if and only if

$$k = \binom{k+1}{2} - \binom{k}{2} \leq n.$$

Thus by (28) it suffices to show that

$$\binom{n+1}{2} \geq (k+1)n - \binom{k+1}{2} \quad (30)$$

for $k = 0, \dots, n-1$. From (29) we see that (30) holds if and only if

$$\binom{n+1}{2} \geq n^2 - \binom{n}{2},$$

which is equivalent to

$$n^2 = \binom{n+1}{2} + \binom{n}{2} \geq n^2.$$

This completes the proof. □

Lemma 3.5.4. *Fix an integer $s \geq 0$ and write*

$$r_s(x) = \sum_{i=0}^s a_i x^i$$

where $a_s = 1$. Then for each $i = 0, \dots, s$ we have

$$a_i \equiv 0 \pmod{q^{\binom{s-i}{2}}}.$$

Proof. The result is trivial for $i = s$ since $a_s = 1$. So suppose $0 \leq i \leq s - 1$. Then by the definition of $r_s(x)$ we have that

$$a_i = (-1)^{s-i} \sum_{0 \leq \ell_1 < \dots < \ell_{s-i} < s} q^{\ell_1 + \dots + \ell_{s-i}}$$

for $i = 0, \dots, s - 1$. After noting that

$$\min_{0 \leq \ell_1 < \dots < \ell_{s-i} < s} (\ell_1 + \dots + \ell_{s-i}) = 0 + 1 + \dots + (s - 1 - i) = \binom{s-i}{2}$$

for each $i = 0, \dots, s - 1$, the result then follows. \square

Lemma 3.5.5. *Fix a positive integer n . If s is an integer where $0 \leq s < n$, then*

$$(r_{s+1}(\tau)v_n)(x) \equiv 0 \pmod{q^{(s+1)n} \mathbb{Z}[x]}.$$

Proof. By Lemma 3.5.3 we can rewrite $v_n(x)$ as

$$v_n(x) = q^{(s+1)n - \binom{s+1}{2}} B_n(x) + u_n^{(s+1)}$$

for some $B_n(x) \in \mathbb{Z}[x]$. Then by applying Lemma 3.5.2 we obtain

$$\begin{aligned} r_{s+1}(\tau)v_n(x) &= r_{s+1}(\tau) \left(q^{(s+1)n - \binom{s+1}{2}} B_n(x) \right) + r_{s+1}(\tau) u_n^{(s+1)} \\ &= \sum_{i=0}^{s+1} a_i q^{(s+1)(n+i) - \binom{s+1}{2}} B_{n+i}(x). \end{aligned}$$

Hence from Lemma 3.5.4 we get that

$$r_{s+1}(\tau)v_n(x) \equiv 0 \pmod{q^E}$$

where

$$E = \min_{0 \leq i \leq s+1} \left(\binom{s+1-i}{2} + (s+1)(n+i) - \binom{s+1}{2} \right).$$

Finally after noticing that

$$\begin{aligned} \binom{s+1-i}{2} + (s+1)(n+i) - \binom{s+1}{2} &= (s+1)(n+i) - si + \binom{i}{2} \\ &= (s+1)n + i + \binom{i}{2} \\ &\geq (s+1)n \end{aligned}$$

for each $i = 0, \dots, s + 1$, we therefore can conclude that

$$(r_{s+1}(\tau)v_n)(x) \equiv 0 \pmod{q^{(s+1)n} \mathbb{Z}[x]}.$$

□

Lemma 3.5.6. *Let $f(x) \in \mathbb{Z}[x]$. Then for any choice of integers s and n with $-1 \leq s < n$ we have*

$$(r_{s+1}(\tau)f(\tau)v_n)(x) \equiv 0 \pmod{q^{(s+1)n} \mathbb{Z}[x]}.$$

Proof. The case where $s = -1$ is clear because $r_0(\tau) = 1$. So suppose $s \geq 0$. By Lemma 3.5.5 we know

$$(r_{s+1}(\tau)v_n)(x) \equiv 0 \pmod{q^{(s+1)n} \mathbb{Z}[x]}.$$

Hence for every $i \geq 0$

$$\begin{aligned} (r_{s+1}(\tau)v_{n+i})(x) &\equiv 0 \pmod{q^{(s+1)(n+i)} \mathbb{Z}[x]} \\ &\equiv 0 \pmod{q^{(s+1)n} \mathbb{Z}[x]}. \end{aligned}$$

Therefore

$$(r_{s+1}(\tau)f(\tau)v_n)(x) \equiv 0 \pmod{q^{(s+1)n} \mathbb{Z}[x]}.$$

□

Lemma 3.5.7. $V_{1,\ell}(x) = \det \left(r_{i-1-\lfloor \frac{i}{2} \rfloor}(\tau) r_{j-1-\lfloor \frac{j}{2} \rfloor}(\tau) v_{1+\lfloor \frac{i}{2} \rfloor + \lfloor \frac{j}{2} \rfloor}(x) \right)_{1 \leq i, j \leq \ell+1}$.

Proof. We apply Lemma 3.4.3 with

$$p_i(x) = q_i(x) = x^{\lfloor \frac{i+1}{2} \rfloor} r_{i-\lfloor \frac{i+1}{2} \rfloor}(x),$$

which are monic polynomials of degree i with integer coefficients ($1 \leq i \leq \ell + 1$).

This gives

$$V_{1,\ell}(x) = \det (p_{i-1}(\tau)q_{j-1}(\tau)v_1(x))_{1 \leq i, j \leq \ell+1}.$$

The conclusion then follows from observing that

$$p_{i-1}(\tau)q_{j-1}(\tau)v_1(x) = r_{i-1-\lfloor \frac{i}{2} \rfloor}(\tau)r_{j-1-\lfloor \frac{j}{2} \rfloor}(\tau)v_{1+\lfloor \frac{i}{2} \rfloor + \lfloor \frac{j}{2} \rfloor}(x).$$

□

Applying Lemma 3.5.6 we obtain

$$r_{i-1-\lfloor \frac{i}{2} \rfloor}(\tau)r_{j-1-\lfloor \frac{j}{2} \rfloor}(\tau)v_{1+\lfloor \frac{i}{2} \rfloor+\lfloor \frac{j}{2} \rfloor}(x) \equiv 0 \pmod{q^{E_{i,j}} \mathbb{Z}[x]}$$

where

$$E_{i,j} = \max \left(i - 1 - \left\lfloor \frac{i}{2} \right\rfloor, j - 1 - \left\lfloor \frac{j}{2} \right\rfloor \right) \left(1 + \left\lfloor \frac{i}{2} \right\rfloor + \left\lfloor \frac{j}{2} \right\rfloor \right).$$

Hence by Lemma 3.5.7 we conclude that

$$V_{1,\ell}(x) \equiv 0 \pmod{q^N \mathbb{Z}[x]} \quad (31)$$

where

$$N = \min_{\sigma \in S_{\ell+1}} \sum_{i=1}^{\ell+1} E_{i,\sigma(i)}.$$

From here it becomes clear that to finally prove the main result of this section it suffices to show that

$$N \geq \frac{1}{8}\ell^3 + O(\ell^2).$$

This is achieved by first noticing that since

$$k - 1 - \left\lfloor \frac{k}{2} \right\rfloor \geq \frac{k}{2} - 1 \quad \text{and} \quad \left\lfloor \frac{k}{2} \right\rfloor \geq \frac{k}{2} - \frac{1}{2}$$

for all $k \geq 1$, we then obtain the following lower bound for $E_{i,j}$,

$$\begin{aligned} E_{i,j} &\geq \max \left(\frac{i}{2} - 1, \frac{j}{2} - 1 \right) \left(\frac{i}{2} + \frac{j}{2} \right) \\ &= \frac{1}{4} (\max(i, j) - 2) (i + j) \\ &= \frac{1}{4} (\max(i, j)^2 + ij - 2i - 2j). \end{aligned}$$

We now make the following three combinatorial observations.

Lemma 3.5.8. *Fix any positive integer ℓ . We then have*

1. $A_1 := \min_{\sigma \in S_{\ell+1}} \left(\sum_{i=1}^{\ell+1} \max(i, \sigma(i))^2 \right) = \frac{1}{3}\ell^3 + O(\ell^2)$

$$2. A_2 := \min_{\sigma \in S_{\ell+1}} \sum_{i=1}^{\ell+1} i(\sigma(i)) = \frac{1}{6}\ell^3 + O(\ell^2)$$

$$3. A_3 := \max_{\sigma \in S_{\ell+1}} \sum_{i=1}^{\ell+1} (2i + 2\sigma(i)) = 2\ell^2 + O(\ell).$$

Proof. We consider each of the claims separately.

1. The first equality follows from the fact that for any permutation $\sigma \in S_{\ell+1}$ we have

$$\sum_{i=1}^{\ell+1} \max(i, \sigma(i))^2 \geq \sum_{i=1}^{\ell+1} i^2.$$

Thus it is clear that the permutation that gives the smallest such value is $\sigma = id$.

We then conclude that

$$\begin{aligned} A_1 &= \min_{\sigma \in S_{\ell+1}} \left(\sum_{i=1}^{\ell+1} \max(i, \sigma(i))^2 \right) = \sum_{i=1}^{\ell+1} i^2 \\ &= \frac{(\ell+1)(\ell+2)(2\ell+3)}{6} \\ &= \frac{1}{3}\ell^3 + O(\ell^2). \end{aligned}$$

2. We first observe that for any positive integer n and any collection of distinct positive integer i_1, \dots, i_k where $k \leq n$ we have that

$$\sum_{j=1}^k \sigma(i_j) \geq 1 + 2 + \dots + k.$$

for every $\sigma \in S_n$.

Applying this observation gives

$$\begin{aligned} \sum_{i=1}^{\ell+1} i(\sigma(i)) &= (\sigma(1) + \dots + \sigma(\ell+1)) + (\sigma(2) + \dots + \sigma(\ell+1)) + \dots + (\sigma(\ell+1)) \\ &\geq (1 + 2 + \dots + (\ell+1)) + (1 + 2 + \dots + \ell) + \dots + 1 \end{aligned}$$

for every $\sigma \in S_{\ell+1}$. After noticing that $\sigma = id$ gives equality in the above formula we conclude that

$$\begin{aligned} A_2 &= \min_{\sigma \in S_{\ell+1}} \sum_{i=1}^{\ell+1} i(\sigma(i)) = \sum_{k=1}^{\ell+1} \binom{\ell+2-k}{2} \\ &= \binom{\ell+2}{2} + \binom{\ell+1}{2} + \cdots + \binom{2}{2} \\ &= \binom{\ell+3}{3} \\ &= \frac{1}{6}\ell^3 + O(\ell^2). \end{aligned}$$

3. Once again since each $\sigma \in S_{\ell+1}$ permutes the elements of the set $\{1, \dots, \ell+1\}$ then for any permutation $\sigma \in S_{\ell+1}$ it is clear that

$$\sum_{i=1}^{\ell+1} (2i + 2\sigma(i)) = \sum_{i=1}^{\ell+1} 4i.$$

Thus we conclude that

$$A_3 = \max_{\sigma \in S_{\ell+1}} \sum_{i=1}^{\ell+1} (2i + 2\sigma(i)) = 4 \binom{\ell+2}{2} = 2\ell^2 + O(\ell).$$

□

With these three observations in hand along with the lower bound found for $E_{i,j}$ we finally achieve our objective, namely

$$\begin{aligned} N &\geq \frac{1}{4} (A_1 + A_2 - A_3) \\ &= \frac{1}{4} \left(\frac{1}{3} + \frac{1}{6} \right) \ell^3 + O(\ell^2) \\ &= \frac{1}{8} \ell^3 + O(\ell^2). \end{aligned}$$

This completes the proof of the main result in this section and thus we now have an estimate on the content of $V_{1,\ell}(\theta)$.

3.6 Conclusion

We are now ready to prove that θ is non-quadratic.

Suppose θ is quadratic and choose a non-zero positive integer d such that $d\theta$ is an algebraic integer. Let $L = \mathbb{Q}(\theta)$ and let \mathcal{O}_L denote the ring of integers of L . Since $V_{1,\ell}(x) \in \mathbb{Z}[x]$ and $d\theta \in \mathcal{O}_L$, then $V_{1,\ell}(d\theta)$ is an algebraic integer of \mathcal{O}_L .

By Proposition 3.5.1 we obtain

$$d^{\ell+1}V_{1,\ell}(\theta) = V_{1,\ell}(d\theta) \equiv 0 \pmod{\gamma_\ell \mathbb{Z}[d\theta]} \quad (32)$$

where $\gamma_\ell \geq q^{\frac{1}{8}\ell^3 + O(\ell^2)}$ denotes the content of $V_{1,\ell}(x)$ (the gcd of its coefficients in \mathbb{Z}).

Since $[L : \mathbb{Q}] = 2$, then we know that L admits exactly two \mathbb{Q} -embeddings

$$\sigma_1, \sigma_2 : L \longrightarrow \mathbb{C}$$

where

$$\sigma_1 : \theta \longmapsto \theta \quad \text{and} \quad \sigma_2 : \theta \longmapsto \bar{\theta}.$$

Here $\bar{\theta}$ denotes the complex conjugate of θ . We then have

$$\begin{aligned} |N_{\mathbb{Q}(\theta)/\mathbb{Q}}(d^{\ell+1}V_{1,\ell}(\theta))| &= d^{2\ell+2} |\sigma_1(V_{1,\ell}(\theta))| |\sigma_2(V_{1,\ell}(\theta))| \\ &= d^{2\ell+2} |V_{1,\ell}(\theta)| |V_{1,\ell}(\bar{\theta})|. \end{aligned} \quad (33)$$

By our estimate of the absolute value of $V_{1,\ell}(\theta)$ we know that

$$|V_{1,\ell}(\theta)| \leq q^{-\frac{1}{2}\ell^3 + O(\ell^2)}. \quad (34)$$

Whereas by the control we have on the growth of $L(V_{1,\ell}(x))$ we obtain

$$\begin{aligned} |V_{1,\ell}(\bar{\theta})| &= \left| \sum_{i=0}^{\ell+1} a_i \bar{\theta}^i \right| \\ &\leq \sum_{i=0}^{\ell+1} |a_i| |\bar{\theta}|^i \\ &\leq L(V_{1,\ell}(x)) (1 + |\bar{\theta}|)^{\ell+1} \\ &\leq q^{\frac{2}{3}\ell^3 + O(\ell^2)}. \end{aligned} \quad (35)$$

Putting together (33), (34), and (35) we achieve

$$|N_{\mathbb{Q}(\theta)/\mathbb{Q}}(d^{\ell+1}V_{1,\ell}(\theta))| \leq d^{2\ell+2}q^{-\frac{1}{2}\ell^3+O(\ell^2)}q^{\frac{2}{3}\ell^3+O(\ell^2)} = q^{\frac{1}{6}\ell^3+O(\ell^2)}.$$

On the other hand, if $V_{1,\ell}(\theta) \neq 0$, then by the estimate of the content of $V_{1,\ell}(x)$ we obtain

$$\begin{aligned} |N_{\mathbb{Q}(\theta)/\mathbb{Q}}(d^{\ell+1}V_{1,\ell}(\theta))| &\geq |N_{\mathbb{Q}(\theta)/\mathbb{Q}}(\gamma_\ell)| \\ &= \gamma_\ell^2 \\ &\geq q^{\frac{1}{4}\ell^3+O(\ell^2)}. \end{aligned}$$

Thus we conclude that if $V_{1,\ell}(\theta) \neq 0$ then

$$q^{\frac{1}{4}\ell^3+O(\ell^2)} \leq q^{\frac{1}{6}\ell^3+O(\ell^2)},$$

i.e. $\ell \ll 1$.

This shows that $V_{1,\ell}(\theta)$ vanishes for all sufficiently large ℓ . Hence by the criterion of Hankel we deduce that $v_n(\theta)$ is a linear recurrence sequence. But note v_n satisfies the following relation

$$\begin{aligned} v_{n+1} &= q^{(n+1)(n+2)/2} \left(\theta - \sum_{k=0}^{n+1} q^{-k(k+1)/2} \right) \\ &= q^{n+1} q^{n(n+1)/2} \left(\theta - \sum_{k=0}^n q^{-k(k+1)/2} \right) - 1 \\ &= q^{n+1} v_n - 1, \end{aligned}$$

which we know can't be satisfied by any linear recurrence sequence (see Proposition 3.1.13). Hence we arrive at a contradiction.

Therefore θ is not quadratic.

Chapter 4

Mahler Functions of One Variable

In this chapter we give another proof of

$$\sum_{n=0}^{\infty} \frac{1}{q^{2^n}} \notin \overline{\mathbb{Q}}, \quad (36)$$

when q is an integer ≥ 2 , which uses Mahler's theory. To be more precise, we actually prove a more general result (see §4.6) which implies (36). The proof is based on [7, chap I]. But note, in this chapter we present a special case with simplifications of the theory given in [7, chap I]. With this in mind, let's begin.

Let \mathbb{K} denote an algebraic number field, let $\mathcal{O}_{\mathbb{K}}$ denote the ring of integers of \mathbb{K} , and let $\mathbb{K}[[z]]$ denote the ring of formal power series in variable z with coefficients in \mathbb{K} .

Throughout this chapter we fix a series $f(z) \in \mathbb{K}[[z]]$ which has a radius of convergence $R > 0$ and satisfies a functional equation of the form

$$f(z^d) = \sum_{i=0}^m a_i(z) f(z)^i \quad (37)$$

where d and m are integers with $d \geq 2$ and $0 \leq m < d$, and where

$$a_i(z) = \sum_{j=0}^{n_i} a_{i,j} z^j \in \mathcal{O}_{\mathbb{K}}[z] \quad (38)$$

for each $i = 0, \dots, m$.

Our main goal in this chapter is to prove the following result due to Mahler.

Theorem 4.0.1. *Let $f(z) \in \mathbb{K}[[z]]$ be as above. Assume that $f(z)$ is not algebraic over $\mathbb{K}(z)$. If $\alpha \in \overline{\mathbb{Q}}$ satisfies*

$$0 < |\alpha| < \min\{1, R\}, \quad (39)$$

then $f(\alpha) \notin \overline{\mathbb{Q}}$.

Before we get to proving the above Theorem we will need to introduce some new terminology.

4.1 Preliminaries

Definition 4.1.1. Let α denote an algebraic number with minimal polynomial

$$\text{Irr}_{\mathbb{Q},\alpha}(x) \in \mathbb{Q}[x],$$

and let \mathcal{O} denote the ring of all algebraic integers of $\overline{\mathbb{Q}}$. We define the *degree*, *size*, and *denominator* of α as follows,

- i. $\deg(\alpha) := \deg(\text{Irr}_{\mathbb{Q},\alpha}(x))$
- ii. $|\overline{\alpha}| := \max\{|\alpha^\sigma| ; \sigma \in \text{Aut}(\overline{\mathbb{Q}}/\mathbb{Q})\}$
- iii. $\text{den}(\alpha) := \min\{d \in \mathbb{Z} ; d > 0, d\alpha \in \mathcal{O}\}$.

Lemma 4.1.2. *Let $\alpha, \beta \in \overline{\mathbb{Q}}$ and let $d \in \mathbb{Z}$. Then*

- i. $|\overline{\alpha + \beta}| \leq |\overline{\alpha}| + |\overline{\beta}|$
- ii. $|\overline{\alpha\beta}| \leq |\overline{\alpha}| |\overline{\beta}|$
- iii. *If $d\alpha, d\beta \in \mathcal{O}$, then $d(\alpha + \beta), d^2\alpha\beta \in \mathcal{O}$.*

The proof of the above Lemma is straightforward, thus is left as an exercise to the reader.

We finish this section with an important result, due to Liouville, which will be of great use when proving Theorem 4.0.1.

Lemma 4.1.3 (Liouville inequality). *Let n be a positive integer. If $\alpha \in \overline{\mathbb{Q}} \setminus \{0\}$ with $\deg(\alpha) \leq n$, then*

$$\log |\alpha| \geq -2n \max\{\log |\overline{\alpha}|, \log(\text{den}(\alpha))\}.$$

Proof. Let $L = \mathbb{Q}(\alpha)$ and let $d = \text{den}(\alpha)$. Since $d\alpha \in \mathcal{O}_L$, then we know that

$$0 \neq N_{L/\mathbb{Q}}(d\alpha) \in \mathcal{O}_L \cap \mathbb{Q} = \mathbb{Z}.$$

This implies that

$$\begin{aligned} 1 \leq |N_{L/\mathbb{Q}}(d\alpha)| &= d^{\deg(\alpha)} |N_{L/\mathbb{Q}}(\alpha)| \\ &= d^{\deg(\alpha)} \prod_{\sigma \in \text{Aut}(L/\mathbb{Q})} |\alpha^\sigma| \\ &\leq d^n |\alpha| |\overline{\alpha}|^{n-1}. \end{aligned}$$

Therefore

$$\begin{aligned} \log |\alpha| &\geq \log \left(\frac{1}{d^n |\alpha|^{n-1}} \right) \\ &= -n \log(d) - (n-1) \log |\overline{\alpha}| \\ &\geq -2n \max\{\log |\overline{\alpha}|, \log(d)\}. \end{aligned}$$

□

Remark 4.1.4. If $\alpha \in \mathcal{O} \setminus \{0\}$, then the above argument gives $|\overline{\alpha}| \geq 1$, since in this case we have that $d = 1$ and so

$$1 \leq N_{\mathbb{Q}(\theta)/\mathbb{Q}}(\alpha) \leq |\overline{\alpha}|^n.$$

4.2 Construction of Auxiliary Polynomials

Proposition 4.2.1. *Suppose $f(z)$ is not algebraic over $\mathbb{K}(z)$ and let p be a positive integer. Then there exists $p+1$ polynomials $A_0, \dots, A_p \in \mathcal{O}_{\mathbb{K}}[z]$ with $\deg(A_i) \leq p$ ($0 \leq i \leq p$) such that the auxiliary function*

$$E_p(z) = \sum_{j=0}^p A_j(z) f(z)^j = \sum_{h=0}^{\infty} b_h z^h \quad (40)$$

is not identically zero and all coefficients b_h , with $h \leq p^2$, vanish.

Proof. For each $0 \leq j \leq p$, write

$$A_j(z) = \sum_{l=0}^p x_{j,l} z^l$$

where the $x_{j,l}$ are variables. Then for each $h = 0, \dots, p^2$ the coefficients b_h in (40) are linear forms in $x_{j,l}$ ($0 \leq j, l \leq p$) with coefficients in \mathbb{K} . From here we would like to solve the following homogeneous linear system

$$b_0 = 0, b_1 = 0, \dots, b_{p^2} = 0. \quad (41)$$

Since this system has $p^2 + 1$ equations and $(p + 1)^2 > p^2 + 1$ variables, then (41) admits a non-trivial solution $\mathbf{x} = (x_{j,l}) \in \mathbb{K}^{(p+1)^2}$. We may take $\mathbf{x} \in \mathcal{O}_{\mathbb{K}}^{(p+1)^2}$ since by multiplying \mathbf{x} by

$$d = \prod_{0 \leq j, l \leq p} \text{den}(x_{j,l})$$

we have that $d\mathbf{x} \in \mathcal{O}_{\mathbb{K}}^{(p+1)^2}$ is a non-trivial solution of (41).

Moreover, since $f(z)$ is not algebraic over $\mathbb{K}(z)$ then $E_p(z)$ is not identically zero. \square

Remark 4.2.2. It is interesting to note that we do not give estimates on the size of the coefficients of $A_j(z)$. Surprisingly we will not need to. We will need to compute an estimate on the size of $E_p(\alpha^{d^k})$, where d and k are positive integers, which depend on the coefficients of $A_j(z)$. But we will see that as k tends to ∞ , the size of the coefficients of $A_j(z)$ will be of no concern.

4.3 Estimation of Absolute Value

Proposition 4.3.1. *Let $p \in \mathbb{Z}_{>0}$ be fixed and let $\alpha \in \mathbb{C}$ with $|\alpha| < \min\{1, R\}$, where R is the radius of convergence of $f(z)$. If $f(z)$ is not algebraic over $\mathbb{K}(z)$ then there exist positive constants $c_1(p)$ and $c_2(p)$ (depending on p) such that for all $m \geq c_1(p)$ we have*

$$0 \neq |E_p(\alpha^m)| \leq c_2(p) |\alpha|^{mp^2}.$$

Proof. By Proposition 4.2.1 we know that $E_p(z)$ is not identically zero and $b_h = 0$ for all $h \leq p^2$. So let

$$H := \min\{h \in \mathbb{Z} ; h > 0, b_h \neq 0\} > p^2.$$

Since $f(z)$ has radius of convergence R , then

$$E_p(z)z^{-H} = b_H + \sum_{h=H+1}^{\infty} b_h z^{h-H}$$

is holomorphic in $\{z \in \mathbb{C} ; |z| < R\}$ and thus continuous on the compact set

$$\{z \in \mathbb{C} ; |z| \leq |\alpha|\}$$

since $|\alpha| < \min\{1, R\}$. Hence there exists a constant $c_2(p)$ such that

$$|E_p(z)z^{-H}| \leq c_2(p)$$

for all $z \in \mathbb{C}$ with $|z| \leq |\alpha|$. This implies that

$$|E_p(z)| \leq c_2(p)|\alpha|^{mH} \leq c_2(p)|\alpha|^{mp^2}$$

for all $m \geq 1$, since $|\alpha^m| \leq |\alpha|$.

Moreover, since $E_p(z) \neq 0$ is holomorphic at 0 then we know that $E_p(z)$ admits a finite number of zeros in any sufficiently small neighbourhood of 0. Thus there exists a constant $c_1(p)$ such that for all $m \geq c_1(p)$ we have that $E_p(\alpha^m) \neq 0$, since $|\alpha| < \min\{1, R\}$. \square

Remark 4.3.2. We do not need to give precise estimates on the constant $c_2(p)$. All we need to know is that it exists. The reason behind this will become clear during the last steps of proving Theorem 4.0.1.

4.4 Estimation of the Size and Denominator

Throughout the rest of this chapter we will let α be as defined in Proposition 4.3.1. Before we get to the main result of this section we need the following Proposition.

Proposition 4.4.1. *Suppose $\alpha, f(\alpha) \in \mathbb{K}$, then $E_p(\alpha^{d^k}) \in \mathbb{K}$ for all $k \geq 0$.*

Proof. Since

$$E_p(\alpha^{d^k}) = \sum_{j=0}^p A_j(\alpha^{d^k}) f(\alpha^{d^k})^j$$

with $A_j(z) \in \mathcal{O}_{\mathbb{K}}[z]$, then it suffices to show that $f(\alpha^{d^k}) \in \mathbb{K}$ for all $k \geq 0$. We proceed by induction on k .

The case $k = 0$ is trivial. So suppose $f(\alpha^{d^k}) \in \mathbb{K}$ for some $k \geq 0$. Recall that $f(z)$ satisfies the following functional equation

$$f(z^d) = \sum_{i=0}^m a_i(z) f(z)^i$$

where m is an integer with $0 \leq m < d$, and $a_i(z) \in \mathcal{O}_{\mathbb{K}}[z]$ for each $i = 0, \dots, m$. Thus by our induction hypothesis and the fact that $\alpha \in \mathbb{K}$, it is then clear that

$$a_i(\alpha^{d^k}) \in \mathbb{K} \quad \text{and} \quad f(\alpha^{d^k})^i \in \mathbb{K}$$

for each $i = 0, \dots, m$. Hence

$$f(\alpha^{d^{k+1}}) = \sum_{i=0}^m a_i(\alpha^{d^k}) f(\alpha^{d^k})^i \in \mathbb{K}.$$

Therefore by induction, $f(\alpha^{d^k}) \in \mathbb{K}$ for all $k \geq 0$. □

In what follows let

- 1) $c_3 = \max\{1, |\alpha|, |\overline{f(\alpha)}|\}$
- 2) $r = \max\{1, \deg(a_0(z)), \dots, \deg(a_m(z))\}$
- 3) $c_4 = \sum_{\substack{0 \leq i \leq m \\ 0 \leq j \leq n_i}} \overline{|a_{i,j}|}$

where

$$a_i(z) = \sum_{j=0}^{n_i} a_{i,j} z^j$$

are the polynomials involved in the functional equation (38). Note that $c_4 \geq 1$ by virtue of the remark following Lemma 4.1.3.

We now state the main result of this section.

Proposition 4.4.2. *Suppose $\alpha, f(\alpha) \in \mathbb{K}$. Let D be a positive integer such that $D\alpha, Df(\alpha) \in \mathcal{O}_{\mathbb{K}}$. Then there exist constants $c_7(p) \geq 1$ and $c_8 \geq 1$, where $c_7(p)$ depends on p , such that*

$$\overline{|E_p(\alpha^{d^k})|} \leq c_7(p)c_8^{d^k p} \quad \text{and} \quad D^{(r+1)d^k p} E_p(\alpha^{d^k}) \in \mathcal{O}_{\mathbb{K}}$$

for any integer $k \geq 0$.

We will need the following two Lemmas.

Lemma 4.4.3. *Let k be an integer greater than or equal to zero. Then*

$$\overline{|f(\alpha^{d^k})|} \leq c_6^{d^k}$$

where $c_6 = c_4 c_3^r$.

Proof. We proceed by induction on k . When $k = 0$, we have

$$\overline{|f(\alpha)|} \leq c_3 \leq c_6^{d^0}$$

since $c_4 \geq 1$ and $r \geq 1$. So suppose

$$\overline{|f(\alpha^{d^k})|} \leq c_6^{d^k}$$

where $k \geq 0$. We then obtain that

$$\begin{aligned} \overline{|f(\alpha^{d^{k+1}})|} &\leq \sum_{i=0}^m \overline{|a_i(\alpha^{d^k})|} \overline{|f(\alpha^{d^k})|^i} \\ &\leq \sum_{i=0}^m \sum_{j=0}^{n_i} \overline{|a_{i,j}|} |\alpha|^{d^k j} c_6^{d^k i} \\ &\leq \left(\sum_{i=0}^m \sum_{j=0}^{n_i} \overline{|a_{i,j}|} \right) c_3^{d^k r} c_6^{d^k m} \\ &= c_4 c_3^{d^k r} c_6^{d^k m} \\ &\leq c_6^{d^{k+1}} \end{aligned}$$

since $c_4 \geq 1$ and $m < d$ implies that $c_4 c_3^{d^k r} \leq c_6^{d^k}$ and $c_6^{d^k(m+1)} \leq c_6^{d^{k+1}}$.

Therefore by induction the Lemma is proven. \square

Lemma 4.4.4. *For all $k \geq 0$, we have that $D^{d^k r} f(\alpha^{d^k}) \in \mathcal{O}_{\mathbb{K}}$.*

Proof. We proceed by induction on k . The case where $k = 0$ is trivial. So suppose

$$D^{d^k r} f(\alpha^{d^k}) \in \mathcal{O}_{\mathbb{K}}$$

where $k \geq 0$. Then by (37) we obtain that

$$D^{d^{k+1} r} f(\alpha^{d^{k+1}}) = \sum_{i=0}^m D^{d^k r(d-i)} a_i(\alpha^{d^k}) \left(D^{d^k r} f(\alpha^{d^k}) \right)^i. \quad (42)$$

Since $m < d$, then $d^k r(d-i) \geq d^k r$ for every $i = 0, \dots, m$. Thus by the induction hypothesis it suffices to show that

$$D^{d^k r} a_i(\alpha^{d^k}) \in \mathcal{O}_{\mathbb{K}}$$

for each $i = 0, \dots, m$. Recalling that $r = \max_{0 \leq i \leq m} \{1, \deg(a_i)\}$, we achieve

$$D^{d^k r} a_i(\alpha^{d^k}) = \sum_{j=0}^{n_i} a_{i,j} D^{d^k r - d^k j} (D\alpha)^{d^k j}$$

where $d^k r - d^k j \geq 0$ for every $j = 0, \dots, n_i$. Therefore, since $D\alpha$ and all the coefficients $a_{i,j}$ belong to $\mathcal{O}_{\mathbb{K}}$, we conclude that

$$D^{d^k r} a_i(\alpha^{d^k}) \in \mathcal{O}_{\mathbb{K}}.$$

\square

From the above two Lemmas we then conclude that

$$\begin{aligned} \overline{|E_p(\alpha^{d^k})|} &\leq \sum_{j=0}^p \overline{|A_j(\alpha^{d^k})|} \overline{|f(\alpha^{d^k})|}^j \\ &\leq \left(\sum_{j=0}^p \sum_{l=0}^p \overline{|x_{j,l}|} \overline{|\alpha|}^{d^k l} \right) c_6^{d^k p} \\ &\leq \left(\sum_{j=0}^p \sum_{l=0}^p \overline{|x_{j,l}|} \right) c_3^{d^k p} c_6^{d^k p} \\ &= c_7(p) c_8^{d^k p} \quad (\text{where } c_8 = c_3 c_6) \end{aligned}$$

and

$$D^{(r+1)d^k p} E_p(\alpha^{d^k}) = \sum_{j=0}^p \left(\sum_{l=0}^p x_{j,l} D^{d^k p} \alpha^{d^k l} \right) D^{d^k r p} f(\alpha^{d^k})^j \in \mathcal{O}_{\mathbb{K}}.$$

Therefore Proposition 4.4.2 is proven.

4.5 Conclusion

We are now ready to prove Theorem 4.0.1. Applying Proposition 4.4.2 we obtain

$$\max\{\log |\overline{E_p(\alpha^{d^k})}|, \log(\text{den}(E_p(\alpha^{d^k})))\} \leq \log(c_7(p)) + d^k p \log c_8 + (r+1)d^k p \log D$$

since $c_7(p) \geq 1$ and $c_8 \geq 1$. Hence by Proposition 4.3.1 and Liouville's inequality (Lemma 4.1.3) we obtain

$$\log(c_2(p)) + d^k p^2 \log |\alpha| \geq -2[\mathbb{K} : \mathbb{Q}] (\log(c_7(p)) + d^k p \log c_8 + (r+1)d^k p \log D)$$

for each k with $d^k > c_1(p)$. Dividing both sides by d^k and then letting k tend to infinity we achieve

$$p^2 \log |\alpha| \geq -2[\mathbb{K} : \mathbb{Q}] (p \log c_8 + (r+1)p \log D)$$

for every positive integer p .

Note, the constants $c_2(p)$ and $c_7(p)$, depending on p , have vanished. This is why we didn't need to give a precise upper bound for $|E_p(\alpha^m)|$ in Proposition 4.3.1 and for the size of the coefficients $x_{j,l}$ of the auxiliary polynomials $A_j(z)$ in Proposition 4.4.2.

Carrying on we now divide both sides of the above formula by p^2 and then let p tend to infinity. We then conclude that $\log |\alpha| \geq 0$, a contradiction since by the choice of α we have that $0 < |\alpha| < 1$.

Therefore $f(\alpha) \notin \overline{\mathbb{Q}}$.

4.6 Application

In this section we use Mahler's method to study arithmetic properties of values at algebraic points within the domain of convergence of the following power series

$$f(z) = \sum_{k=0}^{\infty} z^{d^k},$$

where d is a positive integer greater than 1. Namely, we will prove the following result.

Theorem 4.6.1. *If $\alpha \in \overline{\mathbb{Q}}$ with $0 < |\alpha| < 1$, then*

$$f(\alpha) = \sum_{k=0}^{\infty} \alpha^{d^k}$$

is transcendental.

Note, this is an extension of what was shown in Chapter 2.1 when proving transcendence of the so-called Fredholm Series at integer points.

We first make the observation that $f(z)$ satisfies the following functional equation

$$f(z^d) = f(z) - z \tag{43}$$

and has radius of convergence $R = 1$. Thus from Mahler's Theorem 4.0.1, it suffices to show that $f(z)$ is not algebraic over $\mathbb{C}(z)$. Kumiko Nishioka gives a simple proof of this, so we will follow her method [7, chap I, §1.1].

Suppose $f(z)$ satisfies an irreducible equation

$$f(z)^n + a_{n-1}(z)f(z)^{n-1} + \cdots + a_0(z) = 0 \tag{44}$$

where $a_i(z) \in \mathbb{C}(z)$ for $i = 0, \dots, n-1$. By substituting z^d for z in the above equation (44), we obtain

$$f(z^d)^n + a_{n-1}(z^d)f(z^d)^{n-1} + \cdots + a_0(z^d) = 0. \tag{45}$$

Using the functional equation (43), we see that

$$f(z^d)^k = (f(z) - z)^k = f(z)^k - kzf(z)^{k-1} + \cdots$$

for each $k = 0, \dots, n$. Hence (45) becomes

$$f(z)^n + (-nz + a_{n-1}(z^d))f(z)^{n-1} + \dots = 0. \quad (46)$$

Combining both (44) and (46), we see that as polynomials of $f(z)$, both left hand sides must agree. Thus we obtain

$$a_{n-1}(z) = -nz + a_{n-1}(z^d).$$

Writing $a_{n-1}(z) = a(z)/b(z)$, where $\gcd(a(z), b(z)) = 1$, the above equation then becomes

$$a(z)b(z^d) = -nzb(z)b(z^d) + a(z^d)b(z). \quad (47)$$

Since $a(z^d)$ and $b(z^d)$ are coprime, then by (47), $b(z^d)$ must divide $b(z)$. But since $\deg(b(z^d)) \geq \deg(b(z))$, then $\deg(b(z)) = 0$. Thus by comparing the degrees on both sides, we conclude that $\deg(a(z)) = 0$ and hence $-nz = 0$, a contradiction.

Therefore by Mahler's Theorem 4.0.1, $f(\alpha)$ is transcendental.

Bibliography

- [1] Bézivin, J.-P.; Sur les propriétés arithmétiques d'une fonction entière, *Math. Nachr.* **190** (1998), 31–42.
- [2] Duverney, D.; Sommes de deux carrés et irrationalité de valeurs de fonctions thêta, *C. R. Acad. Sci. Paris Sér. I Math.* **320** (1995), 1041–1044.
- [3] Lang, S.; *Complex Analysis*, Fourth edition, Graduate Texts in Mathematics **103**. Springer-Verlag, New York, 1999, xiv+485 pp.
- [4] Mahler, K.; An application of Jensen's formula to polynomials, *Mathematika* **7** (1960), 98–100.
- [5] Mahler, K.; On some inequalities for polynomials in several variables, *J. London Math. Soc.* **37** (1962), 341–344.
- [6] Everest, G.; van der Poorten, A.; Shparlinski, I.; Ward, T.; *Recurrence sequences*, Mathematical Surveys and Monographs **104**, American Mathematical Society, Providence, RI, 2003, xiv+318 pp.
- [7] Nishioka, K.; *Mahler functions and transcendence*, Lecture Notes in Mathematics **1631**, Springer-Verlag, Berlin, 1996, viii+185 pp.
- [8] Loxton, J. H.; van der Poorten, A. J.; Transcendence and algebraic independence by a method of Mahler, in: *Transcendence theory: advances and applications*, A. Baker and D. W. Masser Eds., Academic Press, London-New York, 1977, 211–226.

- [9] Rumely, R.; Notes on van der Poorten's proof of the Hadamard quotient theorem. I, II. in: *Séminaire de Théorie des Nombres, Paris 1986–87*, Progr. Math., **75**, Birkhuser Boston, Boston, MA, 1988, 349–382, 383–409.