Durham University

Thesis

submitted for the degree of

MSc by Thesis

Around the p-adic Littlewood Conjecture

Submitted by:
Petra Staynova, MMathPhil
Department of Mathematical Sciences
Durham University

Supervisor:
Dr. Dzmitry Badziahin
Department of Mathematical Sciences
Durham University

June 3, 2015

Abstract

In this dissertation, we look at the Littlewood Conjecture and several related open problems. We introduce notions and theorems from various fields in order to properly formulate the conjectures and properly state the various results related to them. In Chapter 5, we investigate a potential counter-example to the p-adic Littlewood conjecture when $p = 2$ via an intricate construction, and show that this potential counter-example does indeed satisfy the premises of the conjecture.

Acknowledgements

It would be impossible to name all to whom I am indebted for helping and inspiring me throughout my studies, be it at postgraduate, undergraduate, or even school-level. First and foremost, I would like to thank my supervisor, Dr Dzmitry Badziahin, for his excellent supervision and patient help throughout my MRes research and studies. My previous formal training was mostly in very pure mathematics (set theory, set-theoretic topology and logic) and philosophy. Thus, I am greatly indebted to Dr Badziahin and, previously, to Dr Jonathan Pila (who supervised my 4th year Master's dissertation at the University of Oxford) for patiently guiding me into the beautiful world of number theory, and taking me on faith without any previous background in the field. Finally, I am also very grateful to the referees for their assiduous reading of the thesis, and helpful comments and suggestions.

Statement of Copyright

Around the p-adic Littlewood Conjecture

Petra Staynova

June 3, 2015

Contents

1 Introduction

The Littlewood Conjecture was first stated by John Littlewood in the 1930's in his book [Lit68]. Informally, it conjectures that for every pair of real numbers $\alpha, \beta \in \mathbb{R}$, the area of the rectangle formed between the point $(q\alpha, q\beta)$ (where $q \in \mathbb{N}$) and the nearest point with integer co-ordinates grows slower than $1/q$; in other words, that the product $q.||q\alpha||.||q\beta||$, where $||.||$ denotes the (Euclidean) distance to the nearest integer, gets arbitrarily close to 0. One can also re-state this as $\liminf_{q\to\infty} q.||q\alpha||.||q\beta|| = 0$.

This Thesis comprises of four main chapters. 'Taking a Dip into Diophantine Approximations' (Chapter 2) provides an overview of the machinery required to talk about and tackle problems in Diophantine Approximations which are close to the Littlewood conjecture. It gives a brief exposition of the needed theorems about continued fraction expansions, continues with the theorems of Dirichlet and Hurwitz, which are central to the field, and finishes by considering the class of badly approximable numbers and some of their properties. The next chapter, 'Some Words on Words', gives an exposition of some material from combinatorics on words that has been widely used in problems in Diophantine Approximations. Chapter 4, 'The Littlewood Conjecture and a Little More (or Less)' deals with the Littlewood conjecture, placing it in the wider context of Diophantine Approximations. It also provides information on work that has been done regarding this problem, including a survey of some state-of-the-art recent results. Also, the chapter includes information on several Littlewood-type questions, which, though currently also open, are considered more accessible than the standard Littlewood conjecture. One such problem is the so-called p-adic Littlewood Conjecture, which will be further studied in this Thesis. Some results on recent progress in those areas are also considered.

Finally, in Chapter 5, we focus on a partial case of the p-adic Littlewood Conjecture: the case when $p = 2$. We explore properties of the product $q|q|_2||q\alpha||$, and provide an upper bound for the $\liminf$ of the expression considered. While doing this, we find some interesting and unexpected relations to the Thue-Morse word (which will be introduced in Chapter 3.1) and some fractal-like structures briefly studied in subsection 5.3.2. We will conclude in Chapter 6 with open questions and point out possible directions for further research.

1.1 A Note on Notation

1.1 Note. Some of the notions for which the notation is now introduced will only be defined later on in the dissertation.

Notation. We denote by:

- $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ the set of natural, integer, rational, and real numbers, respectively;

- $\mathbb{N}^+$ the set of positive integers; otherwise, $\mathbb{N}$ is assumed to contain 0;
- ω the first infinite countable ordinal; we can think of ω as the natural numbers N with the usual order;
- $\mathrm{dom}(f)$ the domain of a function f;
- $\deg(f)$ for the degree of a polynomial f.

Notation. For a real number $x \in \mathbb{R}$, we write:

- $\lfloor x \rfloor$ for $\max\{z \in \mathbb{Z} : z \leqslant x\}$, in other words $\lfloor x \rfloor$ is the greatest integer less than x ($x \in \mathbb{R}$);
- $[x]$ for the integer part of x (note that, unlike $\lfloor x \rfloor$, $[x]$ is the least integer greater than x when x is negative);
- $\{x\}$ for the fractional part of x, in other words, $x - \lfloor x \rfloor$;
- $\ln(x)$ for the natural logarithm $\log_e(x)$;
- $x|n$, where $x, n \in \mathbb{Z}$, $x \neq 0$, if x divides n.

Notation. We denote by $||\theta||$ the (Euclidean) distance between θ and the nearest integer, in other words:

$$||\theta|| = \min\{|\theta - n| : n \in \mathbb{N}\}.$$

Notation. For a subset $A \subseteq \mathbb{R}$, we denote by:

- $\mathrm{int}(A)$ the topological interior of A in the usual Euclidean topology on $\mathbb{R}$;
- $\mathrm{cl}(A)$ the topological closure of A in the usual Euclidean topology on $\mathbb{R}$;
- $\mathrm{card}(A)$ to denote the cardinality of A;
- $\mu(A)$ the Lebesgue measure of A.

Notation. When I is an indexing set and $\{A_i\}_{i \in I}$ is a family of sets, we denote by $\prod_{i \in I} A_i$ the Cartesian product of the sets A_i.

1.1.1 Further Clarification of Notation Used

- ϵ will denote either a very small quantity or the empty word. Both should not occur in the same proof, and thus no confusion should arise from this.

- $|.|$ will denote: the (Euclidean) distance between two points, the length of an interval $(a, b) \subset \mathbb{R}$, or the length of a finite word w. The way in which it is used should be obvious from the context, but in the cases it might not be, it will be further clarified.

- $\{x\}$ could denote either the fractional part of a number x or the singleton which contains x as its only element. Moreover, there is a possible confusion with sequence $\{y_n\}_{n\in\mathbb{N}}$. However, the three should be distinguishable by context;

- $\prod$ can denote either multiplication of numbers or expressions (as in '$\prod_{i=1}^{n}(x-i)$'), or Cartesian product (in the case of sets, as specified above).

1.2 Some Background From Real and Functional Analysis

The study of badly approximable numbers and the Littlewood conjecture draws on material, notions and techniques from many different fields, including measure theory, graph theory, combinatorics on words, real analysis, ergodic theory, and many more. While in Chapters 2 and 3, we will respectively give the necessary background in number theory and properties of words, in this section, we will provide (mostly classical) material which will be needed in some theorems and their proofs further on.

In many fields of mathematics, various specific and interesting sets of numbers are defined, depending on the problems considered. Their investigation sometimes requires considering various measures of those sets, for example, Lebesgue measure, Hausdorff measure, and box product measure, on the set of real numbers. For the purposes of this dissertation, we will use the Lebesgue measure on the real numbers. The notions and theorems listed below can be found in, for example, Capinski and Kopp [CK03]. A special role in Number Theory is played by those subsets of $\mathbb{R}$ whose Lebesgue measure is zero. In Diophantine approximations, many important subsets of $\mathbb{R}$ (for example, the set of rational numbers, the set of badly approximable numbers, the set of well-approximable numbers, the set of algebraic numbers, and the set of transcendental numbers) have either Lebesgue measure zero, or their complement in $\mathbb{R}$ (or a subset of $\mathbb{R}$) has Lebesgue measure zero. For convenience, we will use the following notion:

1.2 Definition (null set)**.** A set $A \subset \mathbb{R}$ is called *(Lebesgue) null* if and only if $\mu(A) = 0$.

1.3 Example. The empty set is null. Also, any singleton $\{x\}$, where $x \in \mathbb{R}$, is null.

We also have:

1.4 Theorem. *If $A \subset \mathbb{R}$ is a countable set, then A is null.*

Moreover:

1.5 Example. There exist uncountable sets which are also null, such as the Cantor middle-third set (for an intuitive idea, the Cantor set is the intersection of a sequence of sets, the measure of each new element of which is 2/3 the measure of the previous one). We will see in Theorem 2.47 that the set of badly approximable numbers is another example of an uncountable null set.

Let us recall some properties of the Lebesgue measure:

1.6 Theorem. *The Lebesgue measure is invariant under translations, in other words, if A is a translation of the set B in $\mathbb{R}$, then $\mu(A) = \mu(B)$.*

1.7 Theorem. *If $A \subset B \subset \mathbb{R}$, then $\mu(A) \leqslant \mu(B)$.*

The following theorem will be essential in the proof of Theorem 2.47.

1.8 Theorem. *For any sequence $\{E_n\}_{n\in\mathbb{N}}$ of subsets of $\mathbb{R}$, we have*

$$\mu\left(\bigcup_{n=1}^{\infty} E_n\right) \leqslant \sum_{n=1}^{\infty} \mu(E_n)$$

The above are basic theorems in Lebesgue measure theory. The interested reader can find their proofs in Capinski and Kopp [CK03].

We continue with the definition of lim inf and lim sup, which will be needed in the formulation of the Littlewood and related conjectures. These can also be found in Capinski and Kopp [CK03].

1.9 Definition (limit inferior and limit superior)**.** Let $\{x_n\}_{n\in\mathbb{N}}$ be a sequence of real numbers. Then the limit inferior of this sequence is written

$$\liminf_{n\to\infty} x_n,$$

and defined as

$$\liminf_{n\to\infty} x_n = \lim_{n\to\infty}\left(\inf_{m\geqslant n} x_m\right).$$

Similarly, the limit superior is written $\limsup_{n\to\infty} x_n$ and defined as

$$\limsup_{n\to\infty} x_n = \lim_{n\to\infty}\left(\sup_{m\geqslant n} x_m\right).$$

It is easy to see that one may equivalently define:

$$\liminf_{n\to\infty} x_n = \sup\big\{ \inf\{x_m : m \geqslant n\} : n \geqslant 0\big\}.$$

In fact, from a topological point of view, the limit inferior of a sequence $\{x_n\}_{n\in\mathbb{N}}$ which is bounded above is the infimum of all accumulation points of the sequence, and the limit superior of a bounded below sequence $\{x_n\}_{n\in\mathbb{N}}$ is the supremum of all its accumulation points.

In Chapter 5, we will need the following theorems from real analysis, most of which are considered classical. We begin with one which is basic for any real analysis course:

1.10 Theorem (l'Hôpital)**.** *Let $a \in \mathbb{R}$, and suppose that $f(x), g(x)$ are functions such that $\lim_{x\to a} f(x)$ and $\lim_{x\to a} g(x)$ are either both zero or both infinite. If $f(x)$ and $g(x)$ are differentiable in a neighbourhood of the point a and*

$$\lim_{x\to a} \frac{f'(x)}{g'(x)}$$

exists (finite or infinite), then the limit of $f(x)/g(x)$ also exists, and moreover

$$\lim_{x\to a} \frac{f(x)}{g(x)} = \lim_{x\to a} \frac{f'(x)}{g'(x)}.$$

If $\lim_{x\to\pm\infty} f(x)$ and $\lim_{x\to\pm\infty} g(x)$ are either both zero or infinite, and if, from some point on, on the real line, $f(x)$ and $g(x)$ are differentiable, and

$$\lim_{x\to\pm\infty} \frac{f'(x)}{g'(x)}$$

exists (finite or infinite), then the limit of $f(x)/g(x)$ also exists, and moreover

$$\lim_{x\to\pm\infty} \frac{f(x)}{g(x)} = \lim_{x\to a} \frac{f'(x)}{g'(x)}.$$

We continue with two lesser-used theorems.

1.11 Theorem (n-th root test)**.** *Let $\sum_{n=1}^{\infty} a_n$ be a series of real (or complex) numbers. If*

$$\limsup_{n\to\infty} \sqrt[n]{|a_n|} < 1,$$

then the series is convergent.

Similarly to formal sums $\sum_{n=1}^{\infty} a_n$ whose convergence we can consider and investigate, we can consider the formal infinite product $\prod_{n=1}^{\infty} a_n$ of real numbers and call them convergent if the sequence of the partial products $\{P_n\}_{n\in\mathbb{N}}$, where $P_n = \prod_{i=1}^{n} a_i$, is convergent.

We have the following convergence criterion:

1.12 Theorem. *Let $\prod_{n=1}^{\infty} a_n$ be an infinite product of positive real numbers. If the series*

$$\sum_{n=1}^{\infty} \ln(a_n)$$

is convergent, then the product

$$\prod_{n=1}^{\infty} a_n$$

is convergent and non-zero.

Proof. Let $\{P_n\}_{n\in\mathbb{N}}$ be the sequence of partial products of $\prod_{n=1}^{\infty} a_n$. Note that the function $\ln : \mathbb{R}^+ \to \mathbb{R}$ is a continuous bijection. By the definition of Heine of continuity, if $\{a_n\}_{n\in\mathbb{N}}$ is a sequence of positive numbers converging to $a > 0$, then

$$\lim_{n\to\infty} \ln(a_n) = \ln(a),$$

and vice-versa.

Let $\lim_{n\to\infty} \ln(P_n)$ be $\geqslant 0$ and finite. Then, $P_n \to P > 0$. Note that

$$\ln(P_n) = \ln\left(\prod_{i=1}^{n} a_i\right) = \sum_{i=1}^{n} \ln(a_i).$$

Hence, if the sequence $\{\ln(P_n)\}_{n\in\mathbb{N}}$ converges, the series $\sum_{n=1}^{\infty} \ln(a_n)$ converges to a non-negative sum. Therefore, $\prod_{n=1}^{\infty} a_n$ converges to a positive limit. $\square$

2 Taking a Dip into Diophantine Approximation

Diophantine approximation is one of the oldest sub-fields of number theory. The field is named after the father of modern algebra, Diophantus of Alexandria, who is considered to be the first Greek mathematician to recognise fractions as numbers. Diophantine approximation deal with the question of how 'well' real numbers can be approximated by rationals, where the 'quality' of approximation is measured by the distance between the real and rational number, in comparison to the value of the rational number's denominator. This is also one of the most thriving fields of mathematical research today.

Diophantine approximation provides the context in which the Littlewood conjecture is formulated. The conjecture itself is part of a natural chain of questions, which begin with one of the fundamental theorems in Diophantine approximation, Dirichlet's Theorem. For this theorem, we first need to recall a couple of definitions. In this section, we will use material from [Cas57], [HW03], [Bug12], and [YIM95]. The interesting historical facts can primarily be found in [Bre91].

We first introduce the following function on $\mathbb{R}$, which is central to Diophantine approximation:

2.1 Definition (distance to the nearest integer)**.** Define $||.|| : \mathbb{R} \to [0, \frac{1}{2}]$ as $||x|| = \min\{|x - n| : n \in \mathbb{N}\}$. In other words, $||x||$ gives the distance between x and the nearest integer.

2.2 Example. Some values of the function $||.||$ are, for example:

- $||q|| = 0$ for any integer q;
- $||\frac{1}{3}|| = ||\frac{2}{3}|| = \frac{1}{3}$;
- $||\sqrt{8}|| = 3 - \sqrt{8} = 3 - 2\sqrt{2}$.

The function $||.||$ resembles in some way the distance function. For example, we have:

2.3 Proposition. *The function $||.|| : \mathbb{R} \to [0, \frac{1}{2}]$ satisfies the triangle inequality: for all $x, y \in \mathbb{R}$, we have*

$$||x + y|| \leqslant ||x|| + ||y||.$$

Thus, in particular,

$$||x|| \geqslant ||x + y|| - ||y||,$$

which will be useful later on.

Proof. Let $x, y \in \mathbb{R}$. Set $n \in \{m \in \mathbb{N} : |m - x| = ||x||\}$, in other words, let n be the nearest integer to x. Let $q \in \mathbb{Z}$ be arbitrary. We have

$$\begin{aligned} ||x + y|| &\leqslant |x + y - q| && \text{by definition of } ||.|| \\ &= |(x - n) + (y + n) - q| \\ &\leqslant |x - n| + |y + n - q| && \text{by the triangle inequality for the Euclidean distance} \\ &= ||x|| + |y + n - q| && \text{since } n = ||x||. \end{aligned}$$

Since q was arbitrary, we can take q to be the nearest integer to $y + n$, more formally, $q \in \{m \in \mathbb{N} : |m - y - n| = ||y + n||\}$, and thus obtain

$$||x + y|| \leqslant ||x|| + ||y||,$$

as required. □

2.4 Definition (best approximation, [YIM95])**.** Let $\alpha \in \mathbb{R}$. A fraction $\frac{p}{q} \in \mathbb{Q}$ is said to be a *best approximation to* α if for all $0 < q' \leqslant q$, $p \neq p'$, we have

$$|q\alpha - p| < |q'\alpha - p'|.$$

Equivalently, we can define a best approximation as:

2.5 Definition (best approximation, [Cas57])**.** A fraction $\frac{p}{q}$ gives a *best approximation* to $\alpha \in \mathbb{R}$ if

$$||q\alpha|| = |q\alpha - p|,$$

and if

$$||q'\alpha|| > ||q\alpha|| \text{ for } 0 < q' < q.$$

2.6 Note. It is important to note that a given number can have more than one best approximation. The reason behind defining best approximations is that not all fractions which are 'Euclidean-close' to a number give 'good enough' approximations. For example, we have that Euler's constant e is nearer in the Euclidean distance to 3 than to 2, and also nearer to 5/2 than to 3, but 5/2 does not give a better approximation of e than 3 does:

$$||e|| < ||2e||,$$

where we use Definition 2.5. Another best approximation to e is 8/3.

2.7 Example. The four best approximations to π with least denominators are 3, 22/7, 333/106, and 355/113.

Interestingly, while the approximation 22/7 was the most accurate estimate of π known in European mathematics well into the Middle Ages, the Chinese astronomer Tsu Ch'ung-Chih had proved that 355/113 is a better approximation around the 5th century AD. The estimate of 22/7 is commonly attributed to Euclid, whose methods have laid the foundations for finding the best approximations to a given number through its continued fraction expansion. This naturally brings us to the next subsection.

2.1 Commencing with Continued Fractions

The earliest example of an algorithm leading to a terminating continued fraction expansion is commonly attributed to Euclid, and relies on the geometry of line segments. However, the algorithm is believed to predate Euclid, and might be attributed to the ancient Greek mathematician Theaetetus. Ever since, continued fraction expansions have played an important part of mathematics. Leonard Euler used them to prove the irrationality of

e in what is considered to be the first more comprehensive account of continued fraction expansions in [Eul37], and Johan Lambert used continued fraction expansions to give the first proof that π is irrational [Lam68]. In recent times, they are used in many areas of number theory, for example Diophantine approximation. The theorems and concepts given here will be ubiquitous throughout this paper.

In this section, we present a short extract of the theory on continued fraction expansions which can be found in [HW03], [Cas57], [Bug12], [YIM95], [Hen06], [Bur01], and [Sch80]. Since similar theorems and propositions can be found in several different sources and the overview below is a distillation and amalgamation of the ones cited above, we will usually not cite where each of the theorems is from. For proofs of the classical theorems given here, the reader is referred to, for example, [HW03].

From now on in this section, when we talk about convergence, we mean convergence in the Euclidean topology on $\mathbb{R}$.

2.8 Definition (continued fraction)**.** A *finite continued fraction* is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\dots + \cfrac{1}{a_n}}},$$

where $a_0 \in \mathbb{Z}$ and $a_i, \in \mathbb{N}^+$ for $i \in \mathbb{N}^+$. In shorthand, we will denote this expression by $[a_0; a_1, \dots, a_n]$, and note that $[a_0; a_1, \dots, a_n] \in \mathbb{Q}$. If $a_0 \in \mathbb{Z}$ and $a_i \in \mathbb{N}^+$ for $i \in \mathbb{N}^+$, an *infinite continued fraction* is an expression of the form

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\dots}}} = \lim_{n\to\infty} [a_0; a_1, \dots, a_n],$$

provided that the limit of the sequence of rational numbers $\{[a_0; a_1, \dots, a_n]\}_{n\in\mathbb{N}}$ exists. We will write $[a_0; a_1, \dots, a_n, \dots]$ as shorthand for infinite continued fractions. A *continued fraction* is a finite or infinite continued fraction.

We will see that all real numbers have (at least one) representation as a continued fraction. Moreover, we have that this representation is unique for irrational numbers, and any infinite continued fraction converges to an irrational number.

The following algorithm gives an explicit procedure for computing a continued fraction expansion of a real number α. In the case when α is rational, one might notice distinct similarities between this and the well-known Euclidean algorithm for finding the greatest common divisor of two natural numbers.

2.9 Algorithm. Let $\alpha \in \mathbb{R}$, and define inductively a (possibly finite) sequence a_n of natural numbers and α_n of real numbers such that:

$$\begin{aligned}
\alpha_0 &= \alpha, \\
a_0 &= \lfloor \alpha \rfloor; \\
\text{if } a_n &\neq \alpha_n, \text{ define:} \\
\alpha_{n+1} &= \frac{1}{\alpha_n - a_n}, \\
a_{n+1} &= \lfloor \alpha_{n+1} \rfloor, \\
\text{if } a_n &= \alpha_n, \text{ the process stops with } a_n.
\end{aligned}$$

From this definition, we get the identity

$$\alpha_{n+1} = [a_{n+1}; a_{n+2}, \ldots],$$

which will be useful later on. Note that the algorithm above terminates if and only if α is a rational number (this will be made more precise in Theorem 2.12), and yields $\alpha = [a_0; a_1, \ldots]$, which possibly terminates at some $n \in \mathbb{N}$.

2.10 Definition (partial quotient and convergent of a continued fraction)**.** Given a (possibly infinite) continued fraction $[a_0; a_1, \ldots, a_n, \ldots]$, we define:

- its *nth partial quotient* to be the integer a_n; and
- its *nth convergent* to be the rational number (in lowest terms) $p_n/q_n = [a_0; a_1, \ldots, a_n]$.

Sometimes, we will write 'quotient' instead of 'partial quotient' for brevity.

The following theorem shows one of the many reasons why continued fractions are useful in Number Theory:

2.11 Theorem. *The convergents p_n/q_n of a continued fraction expansion of a number $\alpha \in \mathbb{R}$ are the best approximations of α.*

This theorem is central to both the proofs of the Dirichlet Theorem (Theorem 2.25) and the Hurwitz Theorem (Theorem 2.33) in the next section.

2.12 Theorem. *Every rational number has precisely two (finite) continued fraction expansions:*

$$[a_0; a_1, \ldots, a_n] \text{ , where } a_n \neq 1,$$

and

$$[a_0; a_1, \ldots, a_n - 1, 1].$$

Thus, we have that $\alpha \in \mathbb{R}$ is representable by a continued fraction with an odd number of convergents if and only if it is representable by one with an even number of convergents.

In view of Theorem 2.12, when we say '*the* continued fraction expansion of a number', we will mean the continued fraction expansion obtained in the manner of Algorithm 2.9, which is clearly unique.

2.13 Theorem. *Let us set*

$$p_{-1} = 1, q_{-1} = 0, p_0 = a_0, \text{ and } q_0 = 1.$$

Then, for any positive integer $n \in \mathbb{N}$, the following recurrent identities hold for the convergents p_n/q_n:

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2} \\ q_n &= a_n q_{n-1} + q_{n-2}. \end{aligned}$$

This theorem can be proved in a straightforward manner by induction using the recurrent identities and the definition of convergent. Theorem 2.13 will be used in the proof of Hurwitz' Theorem, as well as in proving that a real number is badly approximable if and only if the partial quotients of its continued fraction expansion are bounded in Theorem 2.38.

The next theorem will be used to prove Theorem 2.47, that the set of badly approximable numbers is Lebesgue null, as well as to show that a certain sequence of rational numbers is a sequence of odd convergents of a special irrational number in Corollary 5.16.

2.14 Theorem. *Let $\alpha \in \mathbb{R}$ be irrational. The convergents of α with even indices form a strictly increasing sequence, and it's convergents with odd indices form a strictly decreasing sequence. The sequence of convergents $\{p_n/q_n\}_{n\in\mathbb{N}}$ is convergent, and converges to α. Thus, we can set*

$$\alpha = [a_0; a_1, \ldots, a_n, \ldots].$$

We also have that the opposite the direction of Theorem 2.12 and Theorem 2.14 holds:

2.15 Theorem. *Every finite continued fraction $[a_0; a_1, \ldots, a_n]$ expresses a rational number, and every infinite continued fraction $[a_0; a_1, \ldots, a_n, \ldots]$ converges to an irrational number.*

Next, we have another very useful theorem, which will make appearances in several places throughout this dissertation. The the first part of Theorem 2.16 will be important in proving the Lagrange's Theorem (Theorem 2.40), while latter part will be crucial to showing that the set of badly approximable numbers is of Lebesgue measure zero (Theorem 2.47).

2.16 Theorem. *Let $n \in \mathbb{N}$ be a positive integer and $\alpha \in \mathbb{R}$ be irrational number with $\alpha = [a_0; a_1, \ldots]$. Then*

$$\alpha = [a_0; a_1; \ldots, a_n, \alpha_{n+1}] = \frac{p_n \alpha_{n+1} + p_{n-1}}{q_n \alpha_{n+1} + q_{n-1}} \tag{1}$$

and

$$q_n \alpha - p_n = \frac{(-1)^n}{q_n \alpha_{n+1} + q_{n-1}} = \frac{(-1)^n}{q_n} \times \frac{1}{\alpha_{n+1} + [0; a_n, a_{n-1}, \ldots, a_1]}.$$

Furthermore, the set of real numbers whose continued fraction expansions begin with the partial quotients $a_0, a_1, \ldots, a_n$ is precisely the closed interval bounded by the points $(p_{n-1} + p_n)/(q_{n-1} + q_n)$ and p_n/q_n, which are respectively equal to $[a_0; a_1, \ldots, a_n, 1]$ and $[a_0; a_1, \ldots, a_n]$.

Theorem 2.16 also has a very useful corollary:

2.17 Corollary. *For any irrational number α and any non-negative integer $n \in \mathbb{N}$, we have*

$$\frac{1}{q_n(q_n + q_{n+1})} < \left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}}.$$

Proof. Write $\alpha = [a_0; a_1, \ldots]$, and recall $\alpha_n := [a_n; a_{n+1}, \ldots]$.

Note that $a_n < \alpha_n < a_n + 1$. Thus, from Theorem 2.16 we obtain that

$$\frac{1}{q_n((a_{n+1} + 1)q_n + q_{n-1})} < \left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n(a_{n+1} q_n + q_{n-1})}.$$

Thus, from Theorem 2.13 we get that

$$\frac{1}{q_n(q_n + q_{n+1})} < \left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n q_{n+1}},$$

as required. □

One may wonder: what happens if equality (1) in Proposition 2.16 holds for some given integers and reals, without us knowing whether they are related in any way? For example, if we are given two irrationals α and β and two rational numbers p/q, r/s, such that

$$\alpha = \frac{p\beta + r}{q\beta + s},$$

can we think about r/s and p/q as two consecutive convergents of α? The following proposition addresses this:

2.18 Proposition. *If $\alpha, \beta \in \mathbb{R}$ are real numbers and p, q, r, s are integers such that*

$$\alpha = \frac{p\beta + r}{q\beta + s}, \ q > s > 0, \ ps - qr = \pm 1,$$

then r/s and p/q are two consecutive convergents of the continued fraction expansion of α.

Proposition 2.18 allows us to decide whether a given pair of rational numbers is in fact a pair of consecutive convergents. It would be useful to have a criterion for finding whether a single rational number is a convergent of a given real number. The following theorem provides a partial result in this direction:

2.19 Theorem. *Let $\alpha \in \mathbb{R}$ be a real number. If, for a rational number $p/q \in \mathbb{Q}$, we have that*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2},$$

then p/q is a convergent in the continued fraction expansion of α.

Since this theorem will play an important role later on, we will provide its proof.

Proof. Assume that $\alpha \in \mathbb{R}$, $p/q \in \mathbb{Q}$ are such that

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

Assume further $\alpha \neq p/q$, since otherwise the fraction is obviously a convergent of itself. Then, we can write

$$\frac{p}{q} - \alpha = \frac{\epsilon\theta}{q^2},$$

where $\epsilon = \pm 1$ and $0 < \theta < \frac{1}{2}$.

Let us write $\frac{p}{q}$ as a finite continued fraction

$$[a_0, a_1, \ldots, a_n];$$

By Theorem 2.12, we can choose to make n odd or even; thus we may write that

$$\epsilon = (-1)^{n-1}.$$

Denoting by $\frac{p_n}{q_n}$, $\frac{p_{n-1}}{q_{n-1}}$ the last and the last-but-one convergents to the continued fraction for $\frac{p}{q}$, we write

$$\alpha = \frac{\beta p_n + p_{n-1}}{\beta q_n + q_{n-1}}.$$

Then

$$\frac{\epsilon\theta}{q_n^2} = \frac{p_n}{q_n} - \alpha = \frac{p_n q_{n-1} - p_{n-1} q_n}{q_n(\beta q_n + q_{n-1})} = \frac{\epsilon}{q_n(\beta q_n + q_{n-1})},$$

which can be rewritten as

$$\frac{q_n}{\beta q_n + q_{n-1}} = \theta.$$

Thus

$$\beta = \frac{1}{\theta} - \frac{q_{n-1}}{q_n} > 1$$

(recalling that $0 < \theta < \frac{1}{2}$); and so, by Proposition 2.18, $\frac{p_{n-1}}{q_{n-1}}$ and $\frac{p_n}{q_n}$ are consecutive convergents to α. Noting that $\frac{p_n}{q_n} = \frac{p}{q}$, we complete the proof. □

The above Theorem 2.19 can be found in many textbooks on continued fractions. But what happens if we relax the condition in 2.19 and require that the difference be bounded just by $1/q^2$? A less-known but very interesting result by Fatou [Fat04] provides an answer to this, creating a pleasing complement to the previous theorem.

2.20 Theorem (as seen in [Bug12])**.** *Let $\alpha \in \mathbb{R}$ be a real number and $p/q \in \mathbb{Q}$ be rational. If*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2},$$

then there exists an index $n \in \mathbb{N}$ such that p/q is an element of the set of three numbers

$$\left\{\frac{p_n}{q_n}, \frac{p_{n+1} + p_n}{q_{n+1} + q_n}, \frac{p_{n+2} - p_{n+1}}{q_{n+2} - q_{n+1}}\right\}.$$

Continuing in a similar vein, the reverse direction of Theorem 2.19 also provides an analogous inequality:

2.21 Theorem. *Let $\alpha \in \mathbb{R}$ be expanded into a continued fraction. Then at least one of every two of its consecutive convergents satisfies the inequality*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{2q^2}.$$

We will need many of the above theorems in Chapter 5 to show that a certain convergent sequence is actually a sequence of convergents of its limit, and some more interesting observations related to this.

On a more immediate note, Proposition 2.18 might prompt us to define an equivalence relation on the real numbers, which will be needed in the proof of Lagrange's Theorem in the next subsection:

2.22 Definition (equivalent numbers)**.** Two numbers $\alpha, \beta \in \mathbb{R}$ are called *equivalent* if and only if there exist integers $a, b, c, d \in \mathbb{N}$ such that

$$ad - bc = \pm 1$$
$$\beta = \frac{a\alpha + b}{c\alpha + d}.$$

This equivalence corresponds to the 'left shift' operator on the word obtained from the continued fraction expansion of a number (see Section 3). It can also be expressed in terms of tails of the numbers' continued fraction expansions:

2.23 Proposition. *Two irrational numbers α and β are equivalent if the tails of their continued fractions agree, in other words,*

$$\alpha = [a_0, a_1, \ldots, a_j, c_0, c_1, \ldots]$$
$$\beta = [b_0, b_1, \ldots, b_k, c_0, c_1, \ldots].$$

Finally, we have all the machinery necessary to begin exploring the path through Diophantine Approximations which leads to the Littlewood (and p-adic Littlewood) conjecture.

2.2 Two Classical Theorems

This section deals with two classical theorems in the field of Diophantine approximation: those of Dirichlet and Hurwitz. Both theorems are precisely about how well real numbers can be approximated by rationals, which is the main idea behind Diophantine approximation.

Many contemporary questions in this field stem from a deceptively simple theorem, formulated and proved by Dirichlet in 1842. Here, we will give several equivalent formulations. Then, we will look at two different approaches to proving the theorem. To complete the part about Dirichlet, we will give examples of several streams of research which are still active, and all of which originate from the Dirichlet inequality, given below.

Let us begin by providing the original formulation from [Dir42]:

2.24 Theorem (Dirichlet)**.** *For any real θ and any number $Q \in \mathbb{N}$ there exist integers p and q such that $1 \leqslant q < Q$ and*

$$\left|\theta - \frac{p}{q}\right| \leqslant \frac{1}{qQ}.$$

Essentially, it is a statement about how well real numbers can be approximated by rationals with relatively 'small' denominators. In [Khi26], Khintchine observed that the exponent -1 of Q in Theorem 2.24 cannot be improved (say, to $-1-\epsilon$) for any $\theta \in \mathbb{R}$. In other words, for any $\epsilon > 0$ there exists a $\theta \in \mathbb{R}$ such that there are no q with $1 \leqslant q < Q$ such that

$$\left|\theta - \frac{p}{q}\right| \leqslant \frac{1}{qQ^{1+\epsilon}}.$$

Theorem 2.24 can be re-formulated as:

2.25 Theorem. *Let $Q \geqslant 1$ be arbitrary but fixed. Then for any real number θ there exist at least two coprime integers $p, q \in \mathbb{N}$ such that $1 \leqslant q < Q$ and*

$$|q\theta - p| \leqslant \frac{1}{Q}.$$

This can further be written in more modern notation as:

$$||q\theta|| \leqslant \frac{1}{Q}. \tag{2}$$

Note that if we take $Q \in \mathbb{N}$ and $\theta = 1/Q$, then for all p and for any $1 \leqslant q < Q$, we will get that $|q\theta - p| \geqslant 1/Q$, and hence the $\leqslant$ in equation (2) (and the equivalent ones in Theorems 2.24 and 2.25) cannot be improved to a strict inequality.

Dirichlet's Theorem is more powerful than an initial observation might suggest. For instance, it can give us information about approximating rational numbers by other rational numbers which have smaller denominators, as the following example illustrates:

2.26 Example. Taking $\theta = 26/135$ and $N = 100$, Theorem 2.24 states that we can find a rational number p/q whose distance to θ is less than $\frac{1}{100}$ and such that $q < 100$. Indeed, for example, we can take $p = 5$ and $q = 26$ to get

$$\left|\theta - \frac{p}{q}\right| = \frac{1}{3510} < \frac{1}{100},$$

as required.

Theorem 2.24 is very reminiscent of the Pigeonhole Principle. This relation is reflected in the Theorem's original proof, which we will now paraphrase.

Proof. To prove this theorem, we will use Dirichlet's Pigeonhole Principle: that if we have $n+1$ items placed in n places, at least two items will have to share a place.

First, let us consider the $Q+1$ numbers

$$A := \{\{q\theta\} : q = 0, 1, \ldots, Q-1\} \cup \{1\} \subset [0, 1].$$

Now, let us divide the unit interval $[0, 1]$ into Q subintervals U_i, for $i = 0, 1, \ldots, Q-1$ by:

$$U_i := \left[\frac{i}{Q}, \frac{i+1}{Q}\right),$$

where we set U_{Q-1} to include the end-point 1. Then, since $\mathrm{card}(A) = Q+1$ and

$$A \subset \bigcup_{i=0,\ldots,Q-1} U_i,$$

Dirichlet's Pigeonhole Principle implies that two points in A are in the same subinterval. Call these points $\{q_1\theta\}$ and $\{q_2\theta\}$, which can correspondingly be written as sums of whole and rational parts as $q_j\theta = r_j + \{q_j\theta\}$, with $j = 1, 2$. Since all intervals U_i are of length $1/Q$, we have

$$|(q_1\theta - r_1) - (q_2\theta - r_2)| \leqslant \frac{1}{Q}, \tag{3}$$

which we can rewrite as (recalling that $q_1, q_2, r_1, r_2 \in \mathbb{N}$)

$$||(q_1 - q_2)\theta|| \leqslant \frac{1}{Q}.$$

Now, setting $q = |q_1 - q_2|$ and recalling that $0 \leqslant q_1, q_2 < Q-1$, we obtain a q with $0 < q \leqslant Q$ and

$$||q\theta|| \leqslant \frac{1}{Q},$$

as required.

□

It is useful to note that there are other proofs of Dirichlet's Theorem. For example, one can utilise the theory of continued fraction expansions:

Proof of Theorem 2.25 using continued fractions: If θ is rational, say $\theta = \frac{r}{p}$, and $1 \leqslant p < Q$, then setting $q = p$ gives the required result.

So assume that either θ is irrational or $\theta = \frac{r}{p}$ with $p > Q$. Then θ has a (possibly finite) continued fraction expansion $\theta = [a_0; a_1, \ldots]$ with partial quotients $\frac{P_n}{Q_n}$. Let Q_n be the greatest denominator of the partial quotients which is less than or equal to Q (we know that this exists, because a_0 is an integer). This Q_n is not the denominator of the final partial quotient, since we assumed that if $\theta = \frac{r}{p}$, then $p > Q$. Thus Q_{n+1} exists and is greater than Q.

From the general properties of partial quotients of the continued fraction expansion (Corollary 2.17), we have that

$$\left|\theta - \frac{P_{n+1}}{Q_{n+1}}\right| \leqslant \frac{1}{Q_{n+1}Q_{n+2}} \leqslant \frac{1}{Q_n Q_{n+1}} < \frac{1}{QQ_n}, \tag{4}$$

since by assumption, $Q_{n+1} > Q > Q_n$.

Note that if θ is rational and all denominators are less than or equal to Q_{n+1}, then in (4) we will have equality instead of non-strict inequality.

Thus, (4) gives us

$$|Q_{n+1}\theta - P_{n+1}| < \frac{1}{Q},$$

in other words, taking the definition of $||.||$ as a minimum, we obtain

$$||Q_{n+1}\theta|| = \min\{|Q_{n+1}\theta - k| : k \in \mathbb{N}\} \leqslant |Q_{n+1}\theta - P_{n+1}| < \frac{1}{Q},$$

which is the required inequality.

$\square$

It is important to note that this proof relies implicitly on Theorem 2.11, that the convergents to a continued fraction expansion are in fact its best approximations.

As observed previously, Khintchine showed that the exponent of Q in Theorem 2.24 cannot be improved. However, what happens if we instead fix θ, and replace the requirement of 'for all $Q \in \mathbb{N}$' with 'there exist arbitrarily large $Q \in \mathbb{N}$'? In this case, the thus amended inequality can have solutions for some integers $p, q \in \mathbb{N}$ with $1 \leqslant q \leqslant Q$ [BL07]. This motivates the following definition:

2.27 Definition ($\hat{w}_1(\theta)$)**.** For an irrational number θ, define $\hat{w}_1(\theta)$ as the supremum of values w such that for all sufficiently large numbers $Q \in \mathbb{N}$, the equation

$$||q\theta|| < Q^{-w}$$

has a solution $1 \leqslant q \leqslant Q$.

One can relax the requirements on Q even further:

2.28 Definition ($w_1(\theta)$)**.** For an irrational number θ, define $w_1(\theta)$ as the supremum of values w such that there exist arbitrarily large numbers $Q \in \mathbb{N}$ such that the equation

$$||q\theta|| < Q^{-w}$$

has a solution $1 \leqslant q \leqslant Q$.

The author of this paper first came accross these definitions in a lecture by Yann Bugeaud given at the 'Easter School in Dynamics and Number Theory' in 2014 in Durham University; more general versions of them (for greater dimensions) can be found in [BL07]. One can readily note that

$$w_1(\theta) \geqslant \hat{w}_1(\theta),$$

and can enquire whether further bounds can be imposed on w_1 or $\hat{w}_1$ for certain θ. One may also study the set of all $\theta \in \mathbb{R}$ for which the constants above have given values.

In fact, there are many more similar 'exponents of Diophantine approximation' which are either related to relaxing some of the requirements in Dirichlet's Theorem, requiring simultaneous approximations, or related to changing the required inequality to another with a similar flavour. Mahler [Mah32] and Koksma [Kok39] defined two more such constants, which can be used to classify numbers in terms of their approximations by algebraic numbers. Note that since we are no longer approximating by rationals, we are a bit outside the classic setting of Diophantine Approximations; this material is (briefly) mentioned for interest and to show that many different streams of research can stem from the deceptively simple Dirichlet inequality (2). Recalling that the height H of an algebraic number $\theta \in \mathbb{R}$ is the maximum of the moduli of the coefficients of its minimal polynomial, we have:

2.29 Definition ($w_n^*(\theta)$)**.** For an irrational number θ and for a natural number $n \in \mathbb{N}$, define $w_n^*(\theta)$ as the supremum of values w^* such that there exist arbitrarily large H such that the equation

$$|\theta - \alpha| < H^{-w^*-1}$$

has a solution α, such that α is an algebraic number of degree $\leqslant n$ and height $H(\alpha) = H$.

To give an idea of the depth of the constant in Definition 2.29, the following is still an open problem:

2.30 Conjecture (Wirsing, [Wir61])**.** *For any transcendental number $\theta \in \mathbb{R}$ and for any $n \in \mathbb{N}^+$, we have*

$$w_n^*(\theta) \geqslant n.$$

Mahler and Koksma also defined and studied:

2.31 Definition ($w_n(\theta)$)**.** For an irrational number θ and for a natural number $n \in \mathbb{N}$, define $w_n(\theta)$ as the supremum of values w such that there exist arbitrarily large H such that the equation

$$|P(\theta)| < H^{-w}$$

has a solution $P(x) \in \mathbb{Z}(x)$ of degree $\leqslant n$ and height $H(P) \leqslant H$.

One may also consider a similar exponent for simultaneous approximations to a number and its powers, for example see [Roy04]. To give an idea of the depth and breadth of study of these and other exponents, we mention a few papers in this respect: [BL07], [BL05], [Dys47], [Jar50], [Jar54].

We now return to the question - how well can we improve the estimate Q in Dirichlet's Theorem? For example, can we improve it to Q^2, or to aQ for some $a \in \mathbb{R}$? Arguments similar to the ones used in the proof of Theorem 2.25 can be used to show that $||q\theta||$ can be estimated with order $1/q^2$:

2.32 Corollary. *For all irrational $\theta \in \mathbb{R}$, there exist infinitely many coprime pairs $p, q \in \mathbb{Z}$ such that*

$$\left|\frac{p}{q} - \theta\right| < \frac{1}{q^2}.$$

If we consider the inequality

$$\left|\frac{p}{q} - \theta\right| < \frac{1}{aq^2},$$

the above Corollary 2.32 implies that the constant a can be made as large as 1. Can we improve on this? In other words, is there a precise constant a beyond which there exist θ such that we can no longer estimate $|p/q - \theta|$ with accuracy $1/aq^2$? In 1891, Hurwitz showed that the constant can be improved to $\sqrt{5}$ in the following Theorem which bears his name. The example following the theorem shows that the estimate is sharp in the case of the Golden Ratio, and thus the constant $\sqrt{5}$ the best possible.

2.33 Theorem (Hurwitz, [Hur91])**.** *Let $\alpha \in \mathbb{R}$ be irrational. Then there exist infinitely many rational numbers $p/q \in \mathbb{Q}$ such that*

$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{\sqrt{5}q^2}. \tag{5}$$

Proof. Let $\alpha \in \mathbb{R}$ be irrational and let $[a_0; a_1, \ldots, a_n, \ldots]$ be its continued fraction expansion.

We will show that at least one of every three consecutive convergents to α,

$$\frac{p_{n-2}}{q_{n-2}}, \frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n}$$

strictly satisfies inequality (5). Recall the definition of α_i from Algorithm 2.9, and let β_i be the ratio

$$\beta_i = \frac{q_{i-2}}{q_{i-1}}.$$

Then, we can write $\alpha = [a_0, \ldots, a_n, \alpha_{n+1}]$, and so by Theorem 2.16, we obtain

$$\alpha q_n - p_n = \frac{(-1)^n}{\alpha_{n+1} q_n + q_{n-1}}.$$

Thus, the distance to α is

$$\left| \alpha - \frac{p_n}{q_n} \right| = \frac{1}{q_n(\alpha_{n+1} q_n + q_{n-1})} = \frac{1}{q_n^2(\alpha_{n+1} + \beta_{n+1})}.$$

Now we only need to show that for at least one of the three integers $i = n-1, n, n+1$ we have $\alpha_i + \beta_i > \sqrt{5}$.

For a contradiction, let us assume that for all three $i = n-1, n, n+1$, we have

$$\alpha_i + \beta_i \leqslant \sqrt{5}. \tag{6}$$

By Algorithm 2.9,

$$\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}.$$

We also have

$$\frac{1}{\beta_n} = \frac{q_{n-1}}{q_{n-2}} = a_{n-1} + \frac{q_{n-3}}{q_{n-2}} = a_{n-1} + \beta_{n-1},$$

so if we assume inequality (6) holds for $i = n-1$, the above two equalities give us

$$\frac{1}{\alpha_n} + \frac{1}{\beta_n} = \alpha_{n-1} + \beta_{n-1} \leqslant \sqrt{5},$$

which we can rewrite as

$$\frac{1}{\alpha_n} \leqslant \sqrt{5} - \frac{1}{\beta_n}. \tag{7}$$

Therefore,

$$\begin{aligned} 1 &\leqslant \alpha_n \left(\sqrt{5} - \frac{1}{\beta_n} \right) \quad \text{by (7)} \\ &\leqslant (\sqrt{5} - \beta_n) \left(\sqrt{5} - \frac{1}{\beta_n} \right) \quad \text{by (6) for } i = n, \end{aligned}$$

which is equivalent to

$$\beta_n^2 - \sqrt{5}\beta_n + 1 \leqslant 0. \tag{8}$$

The quadratic expression on the left has roots

$$x_{1,2} = \frac{\sqrt{5} \pm 1}{2},$$

and thus inequality (8) combined with the fact that β_n are rational gives us the strict inequalities

$$\frac{1}{2}(\sqrt{5}-1) < \beta_n < \frac{1}{2}(\sqrt{5}+1). \tag{9}$$

Similarly, for $i = n$, we get

$$\frac{1}{\beta_{n+1}} < \frac{2}{\sqrt{5}-1}. \tag{10}$$

Therefore, we obtain

$$\begin{aligned}
1 \leqslant a_n &= \frac{q_n}{q_{n-1}} - \frac{q_{n-2}}{q_{n-1}} && \text{by Theorem 2.13} \\
&= \frac{1}{\beta_{n+1}} - \beta_n && \text{by definition of } \beta_n \\
&< \frac{1}{\beta_{n+1}} - \frac{1}{2}(\sqrt{5}-1) && \text{by (9)} \\
&< \frac{2}{\sqrt{5}-1} - \frac{\sqrt{5}-1}{2} && \text{by (10)} \\
&= 1,
\end{aligned}$$

which is the required contradiction. □

The constant above, $1/\sqrt{5}$, is the best possible, as the following example shows:

2.34 Example (The Golden Ratio)**.** If we take the golden ratio

$$\phi = \frac{1+\sqrt{5}}{2} = [1; 1, 1, 1, \ldots], \tag{11}$$

we will obtain that for all convergents $\frac{p_i}{q_i}$, we have

$$\left|\phi - \frac{p_i}{q_i}\right| = \frac{1}{\sqrt{5}q^2}.$$

A more detailed proof of the last equality in equation (11) can be found in, for example, [Cas57].

Example 2.34 inspires us to consider how well (or respectively, badly) irrational numbers can be approximated by rationals, which will be further explored in the following sub-section.

2.3 The Badly Approximable Numbers

From Example 2.34 we have that for all $p/q \in \mathbb{Q}$,

$$\left|\phi - \frac{p}{q}\right| \geqslant \frac{1}{\sqrt{5}q^2},$$

which can be re-written as

$$q||q\phi|| \geqslant \frac{1}{\sqrt{5}},$$

for all $q \in \mathbb{N}$. Combining this inequality with Theorem 2.11 (the convergents to a continued fraction of a number are that number's best approximations), allows us to conclude that

$$\liminf_{q\to\infty} q||q\phi|| = \frac{1}{\sqrt{5}}.$$

From Hurwitz' Theorem 2.33, we know that for all $\alpha \in \mathbb{R}$,

$$\liminf_{q\to\infty} q||q\alpha|| \leqslant \frac{1}{\sqrt{5}}.$$

This leads us to define the following constant $c(\alpha)$ (also known as Lagrange's constant), which we can then use to classify numbers $\alpha \in \mathbb{R}$:

2.35 Definition (approximation constant [Bug12])**.** For each number $\alpha \in \mathbb{R}$, we define its approximation constant $c(\alpha)$ as

$$c(\alpha) := \liminf_{n\to\infty} n||n\alpha||.$$

For any rational number, we clearly have that $c(\alpha) = 0$ (consider the sequence of multiples of its denominator). In fact, in Theorem 2.47 we will see that for 'most' numbers $\alpha \in \mathbb{R}$, this $c(\alpha) = 0$. On the other hand, Example 2.34 shows that for the Golden Ratio ϕ, we have $c(\phi) = 1/\sqrt{5} \neq 0$. This prompts us to define:

2.36 Definition (badly approximable number)**.** We call $\alpha \in \mathbb{R}$ *badly approximable* iff $c(\alpha) > 0$. We will denote by BAD the set of badly approximable numbers.

An alternative and more explicit formulation of this is given in [Bug12] and [Bur01]:

2.37 Definition. A number $\alpha \in \mathbb{R}$ is called *badly approximable* iff there is a positive constant $c = c(\alpha)$ such that for all rational $\frac{p}{q}$ we have

$$\left|\alpha - \frac{p}{q}\right| > \frac{c}{q^2}.$$

These numbers are called 'badly approximable', since there is a non-zero constant beyond which they cannot be approximated. In other words, all approximations of these numbers are 'relatively far' away from the numbers themselves.

Given the above definitions, it initially seems that examples of badly approximable numbers are very difficult to find. One natural starting point is the Golden Ratio. In the previous section, we noticed that its continued fraction expansion exhibits an interesting pattern - it is just the constant number 1. This prompts us to ask whether it might be possible to characterize badly approximable numbers in terms of their continued fraction expansion. Indeed, this is the case, as the following Theorem illustrates.

2.38 Theorem. *A number $\alpha \in \mathbb{R}$ is badly approximable iff the partial quotients a_n in its continued fraction expansion are bounded.*

Proof. We follow the proof given in [Bur01] and in [Bug12].

First, let $\alpha \in \mathbb{R}$ be badly approximable with approximation constant $c(\alpha) > 0$, and let $n \in \mathbb{N}$ be a positive integer.

Combining the inequality for $c(\alpha)$ with Corollary 2.17, we obtain

$$\frac{c}{q_{n-1}^2} < \left| \alpha - \frac{p_{n-1}}{q_{n-1}} \right| < \frac{1}{q_n q_{n-1}},$$

and thus

$$q_n \leqslant \frac{q_{n-1}}{c}.$$

By Theorem 2.13, we have that $q_n > a_n q_{n-1}$; thus $a_n \leqslant \frac{1}{c}$. Thus, the sequence of partial quotients is bounded.

For the converse, assume that the partial quotients of α are bounded, say by some $M \in \mathbb{R}$. Then, for any non-negative integer $n \in \mathbb{N}$,

$$q_{n+1} \leqslant (M+1) q_n.$$

Also, by Theorem 2.19, we have that if there are positive numbers $p, q \in \mathbb{N}$ such that

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{2q^2},$$

then p/q is a convergent in the continued fraction expansion of α, in other words, there is an $n \in \mathbb{N}$ such that $p = p_n$ and $q = q_n$. Thus, by Corollary 2.17, we have that

$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{q(q + q_{n+1})} \geqslant \frac{1}{(M+2)q^2}.$$

Thus, by Theorem 2.15, we can conclude that α is badly approximable. $\square$

Thus, it is relatively easy to imagine the continued fraction expansion of a badly approximable number. Also, we can describe all badly approximable numbers via their continued fraction expansion. Moreover, by a Cantor-type argument, we can construct uncountably many such numbers.

However, if we do not want to resort to continued fraction expansions, do we know of any numbers besides the Golden Ratio which occur 'naturally' in mathematics and are badly approximable? In 1748, Euler derived the continued fraction expansion of e [Eul48]:

$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, 12, 1, 1, 14, 1, 1, 16, 1, 1, 18, 1, 1, 20, \ldots].$$

A more comprehensible proof of the above equality can be found in [Old70], who won the Chauvenet Prize in 1973 for his exposition of this derivation. In fact, the continued fraction expansion of e has unbounded partial quotients, and thus e is not badly approximable. The beautiful patterns exhibited in it, and in the continued fraction expansions of its rational powers, have spurred numerous research, including [Els99], [Kom07], and [BBG04].

What about another irrational favourite, π? Its continued fraction expansion is

$$\pi = [3, 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, 2, 2, 1, 84, 2, 1, 1, 15, 3, 13, 1, 4, 2, 6, \ldots].$$

There are no known arithmetical relations between the partial quotients of its continued fraction expansion [Gar95], and, as far as the author knows, it is still open whether or not π is badly approximable.

If we move away from transcendental numbers like π and e, what can we say about algebraic irrationals? The Golden Ratio ϕ is a quadratic irrational; looking at its continued fraction expansion, we notice its partial quotients are in fact a constant - $a_0 = a_1 = \ldots = 1$ - and thus this quadratic irrational is badly approximable. So, we can ask ourselves: is this a coincidence, or does it reveal some deeper pattern about partial quotients and quadratic numbers? The following theorem of Lagrange answers this very elegantly: a number has an eventually periodic continued fraction expansion if and only if it is a quadratic irrational. For completeness and rigour, we define:

2.39 Definition (quadratic irrational)**.** A *quadratic irrational* is a number of the form $a \pm \sqrt{b}$, where a and b are rational and b is not the square of another rational number.

2.40 Theorem (Lagrange)**.** *An irrational number $x \in \mathbb{R}$ is a quadratic irrational if and only if its continued fraction expansion is eventually periodic.*

This theorem shows how to 'explain' the continued fraction expansion of a quadratic irrational number.

We will need the following Lemma:

2.41 Lemma ([Ros93])**.** *If α is a quadratic irrational and if $r, s, t, u \in \mathbb{Z}$, then*

$$\frac{r\alpha + s}{t\alpha + u}$$

is either rational or a quadratic irrational.

We first prove only the first direction of the implication of Lagrange's Theorem:

2.42 Proposition. *If the real number α expands into an infinite continued fraction which is eventually periodic, then α is a quadratic irrational number.*

Proof. Let α expand into $[a_0; a_1, a_2, \ldots, \overline{a_N, a_{N+1}, \ldots, a_{N+k}}]$. Then α is irrational, since every rational number has a finite continued fraction expansion.

Let

$$\beta = [\overline{a_N, a_{N+1}, \ldots, a_{N+k}}].$$

Then, by Theorem 2.16,

$$\beta = \frac{p_k + \beta p_{k-1}}{q_k + \beta q_{k-1}},$$

thus

$$q_{k-1}\beta^2 + (q_k - p_{k-1})\beta - p_k = 0.$$

Therefore, β is a quadratic irrational.

By Theorem 2.16 again,

$$\alpha = \frac{p_{N-1}\beta + p_{N-1}}{q_{N-1}\beta + q_{N-2}},$$

and thus Lemma 2.41 gives us that α is also a quadratic irrational (since α is not a rational number, because its continued fraction expansion is infinite). □

2.43 Note. In fact, over here we are using the equivalence defined in Proposition 2.23, and Lemma 2.41 states that two continued fractions which are equivalent in that sense also share certain properties (of being either rational or quadratic irrational numbers).

2.44 Note. There are several proofs for the other direction, which follow a common arc of reasoning. They show that there is a sequence of quadratic polynomials $f_n(x) \in \mathbb{Z}[x]$ which share the same discriminant, whose coefficients can be bounded independently of n, and such that $f_n(\alpha_n) = 0$ for all n. They can thus conclude that two of the elements of the sequence $\{\alpha_n\}_{n\in\mathbb{N}}$ have to be equal, hence the sequence $\{\alpha_n\}$ is eventually periodic, and with it $\{a_n\}$ is also eventually periodic. The main difference between the proofs is in the manner in which the f_n are constructed and the way in which the coefficients are bounded.

We now follow [Ste92] for the other direction.

2.45 Proposition. *The continued fraction for a quadratic irrational is eventually periodic.*

Proof. Let α be a quadratic irrational.

Recall Algorithm 2.9:

$$\begin{aligned} a_n &= [\alpha_n] \ (n \geqslant 0,\ \alpha_0 = \alpha), \\ \alpha_n &= a_n + \frac{1}{\alpha_{n+1}}. \end{aligned} \tag{12}$$

In other words, we have $\alpha_{n+1} = \frac{1}{\alpha_n - a_n}$. We will use induction to show that for each $n \geqslant 0$ there is a polynomial

$$f_n(x) = A_n x^2 + B_n x + C_n,$$

with A_n, B_n, C_n integers, which has a non-square, positive determinant, and is such that $f_n(\alpha_n) = 0$.

Base case: For $n = 0$, we already have that α is a quadratic irrational, so it is the solution of some function $f_0(x) = A_0 x^2 + B_0 x + C_0$.

Induction step: Suppose that such an f_n exists for some $n \geqslant 0$; in other words, $f_n(x) = A_n x^2 + B_n x + C_n$, with integer coefficients and a positive, not-square determinant, such that $f_n(\alpha_n) = 0$. Then equation (12) gives us

$$\begin{aligned} 0 &= f_n\left(a_n + \frac{1}{\alpha_{n+1}}\right) \\ &= A_n\left(a_n + \frac{1}{\alpha_{n+1}}\right)^2 + B_n\left(a_n + \frac{1}{\alpha_{n+1}}\right) + C_n \\ &= A_n \frac{1}{\alpha_{n+1}^2} + (2A_n a_n + B_n)\frac{1}{\alpha_{n+1}} + A_n a_n^2 + B_n a_n + C_n. \end{aligned}$$

Multiplying by α_{n+1}^2, we get

$$0 = \alpha_{n+1}^2 \left(A_n a_n^2 + B_n a_n + C_n\right) + \alpha_{n+1}\left(2A_n a_n + B_n\right) + A_n = 0,$$

so in fact

$$\begin{aligned} A_{n+1} &= A_n a_n^2 + B_n a_n + C_n, \\ B_{n+1} &= 2A_n a_n + B_n, && (13) \\ C_{n+1} &= A_n. && (14) \end{aligned}$$

Thus, we have reached an f_{n+1} such that $f_{n+1}(\alpha_{n+1}) = 0$. We now show it satisfies the remaining conditions. Its coefficients are obviously integers, as sums and products of such. As for the determinant, we have that

$$\begin{aligned} B_{n+1}^2 - 4A_{n+1}C_{n+1} &= (2A_n a_n + B_n)^2 - 4(A_n a_n^2 + B_n a_n + C_n)A_n \\ &= B_n^2 - 4C_n A_n =: D, && (15) \end{aligned}$$

which by hypothesis is greater than 0 and not a square.

In order to get a bound for the coefficients for some of the f_n's, we need to look at the sequence $\{A_n\}_{n\geqslant 0}$. This sequence changes sign infinitely often. Indeed, if A_n became of constant sign after a certain index m (without loss of generality, $A_n > 0$), then equation (13) would give us that $\{B_n\}_{n\geqslant 0}$ would become a strictly increasing sequence after index m, and would thus become strictly positive after some index, say $l \geqslant m$, since $a_n > 0$ for $n \geqslant 1$. Combining this with (14) yields that for $n > l$, $A_n > 0$, $B_n > 0$, $C_n > 0$. But this is impossible, since $\alpha_n > 0$, and $f_n(\alpha_n) = A_n\alpha_n^2 + B_n\alpha_n + C_n = 0$. A similar argument gives a contradiction when $\{A_n\}_{n\geqslant 0}$ becomes a strictly decreasing sequence after a certain index, since then $f_n(\alpha_n)$ would be strictly negative after a certain higher index.

Therefore, A_n changes sign infinitely often, and thus

$$A_n A_{n-1} < 0 \tag{16}$$

on some infinite set $E \subset \mathbb{N}$. Recalling the definition of C_n from equation (14), this means that $A_n C_n < 0$ for $n \in E$.

Hence, by (15)

$$\begin{aligned} |B_n| &< \sqrt{D}, \\ |A_n| &\leqslant \frac{1}{4}D, \\ |C_n| &\leqslant \frac{1}{4}D, \end{aligned}$$

for $n \in E$.

Since the value of D is independent of n, we have that for $N \in E$ there are finitely many possible values for A_n, B_n, C_n, and thus there are only finitely many distinct polynomials f_n. Thus, two of the α_n are equal, say $\alpha_{n_0} = \alpha_{n_1}$ and thus we have $a_{n_0+1} = a_{n_1+1}$. Therefore, the continued fraction of α will eventually become periodic. $\square$

It is conjectured that none of the algebraic numbers of degree greater than 2 are badly approximable, but is currently unresolved [BvdPSZ14]. The best known general result in this direction is currently the Thue-Siegel-Roth Theorem, for which Roth received a Fields medal. It can be found in Baker [Bak90]:

2.46 Theorem (Thue-Siegel-Roth's Theorem)**.** *Let α be an algebraic irrational. Then for any $\epsilon > 0$, the inequality*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\epsilon}}$$

has only finitely many solutions $p/q \in \mathbb{Q}$.

Even though there are uncountably many badly approximable numbers, the set BAD is in some sense 'small', as the following theorem states:

2.47 Theorem. *The set BAD of badly approximable numbers has Lebesgue measure zero.*

We completely rewrite the proof given in [HW03] to give a more set-theoretic and measure-theoretic exposition than the one presented there.

Proof. Throughout this proof, we will write 'perforated interval' from a to b (where $a, b \in \mathbb{R}$) for a real interval $(a, b) \subset \mathbb{R}$ without the rational points (in other words, $(a, b) \setminus \mathbb{Q}$). Throughout this proof, the length of the interval is considered to be its Lebesgue measure (which coincides with 'Euclidean' length), and we note that, by Theorem 1.4, the measure of a perforated interval is the same as the length of the interval itself.

Note that $\mu(\text{BAD}) = \sum_{k\in\mathbb{Z}} \mu(\text{BAD} \cap [k, k+1])$. Since both Lebesgue measure (Theorem 1.6) and the set of badly approximable numbers are invariant under translation by integers, we have that $\forall k, l \in \mathbb{Z}$,

$$\mu(\text{BAD} \cap [k, k+1]) = \mu(\text{BAD} \cap [l, l+1]).$$

Thus, we can initially investigate $\mu(\text{BAD}\cap[0, 1])$ without any loss of generality. Moreover, since the set of rational number is null (by Theorem 1.4), we may without loss of generality restrict ourselves to $\mu\big((\text{BAD} \cap [0, 1]) \setminus \mathbb{Q}\big)$; in other words, to the set of irrational badly approximable numbers in $(0, 1)$.

By Theorem 2.38, this coincides with the set of numbers in $(0, 1)$ whose continued fraction expansions are infinite and bounded.

We note that the set of irrationals with bounded partial quotients is the countable union of the set of irrationals whose partial quotients are bounded by M, for $M \in \mathbb{N}$. Let us denote the set of irrational numbers in $(0,1)$ whose partial quotients are bounded by $M \in \mathbb{N}$ by F_M. Thus, it is sufficient to prove that for all $M \in \mathbb{N}$, the set F_M is null.

From here on, let $M \in \mathbb{N}$ be arbitrary but fixed. Denote by $E_{a_1,\ldots,a_n}$ the set of irrationals whose first $n+1$ partial quotients are $0, a_1, \ldots, a_n$. Now note that F_M is in fact the countable intersection

$$\begin{aligned} F_M &= \left(\bigcup_{a_1 \leqslant M} E_{a_1} \right) \cap \left(\bigcup_{a_1, a_2 \leqslant M} E_{a_1,a_2} \right) \cap \ldots \cap \left(\bigcup_{a_1,\ldots,a_n \leqslant M} E_{a_1,\ldots,a_n} \right) \cap \ldots \\ &= \bigcap_{n \in \mathbb{N}^+} \left(\bigcup_{\substack{a_i \leqslant M \\ 1 \leqslant i \leqslant n}} E_{a_1,\ldots,a_n} \right). \end{aligned}$$

Thus, for all $n \in \mathbb{N}$,

$$F_M \subset \bigcup_{a_i \leqslant M, 1 \leqslant i \leqslant n} E_{a_1,\ldots,a_n}.$$

Write

$$G_{n,M} := \bigcup_{a_i \leqslant M, 1 \leqslant i \leqslant n} E_{a_1,\ldots,a_n}.$$

We will show that $G_{n,M}$ lie in the finite union of disjoint intervals, whose number goes to infinity as $n \to \infty$ slower than their lengths go to zero, and hence $\lim_{n\to\infty} \mu(G_{n,M}) = 0$. Note that, for $a_m \neq a_n$, we have that

$$E_{a_1,\ldots,a_m} \cap E_{a_1,\ldots,a_n} = \emptyset,$$

thus we already have that $G_{n,M}$ consists of disjoint intervals. In particular, this means that

$$\mu(G_{n,M}) := \sum_{a_i \leqslant M, 1 \leqslant i \leqslant n} \mu\left(E_{a_1,\ldots,a_n}\right). \tag{17}$$

We will now proceed to prove that $\mu(G_{n,M}) \to 0$ as $n \to \infty$.

Note that $E_{a_1,\ldots,a_n}$ is the open perforated interval with endpoints

$$[a_1, a_2, \ldots, a_{n-1}, a_n + 1],\ [a_1, \ldots, a_{n-1}, a_n],$$

which can be easily seen from Theorem 2.16.

Thus, $E_{a_1,\ldots,a_n}$ is the union of the perforated intervals

$$E_{a_1,\ldots,a_n,1}, E_{a_1,\ldots,a_n,2}, \ldots E_{a_1,\ldots,a_n,k}, \ldots;$$

in other words,

$$E_{a_1,\ldots,a_n} = \bigcup_{k\in\mathbb{N}^+} E_{a_1,\ldots,a_n,k}.$$

By Theorem 2.16, the end-points of $E_{a_1,\ldots,a_n}$ can also be expressed as

$$\frac{(a_n+1)p_{n-1}+p_{n-2}}{(a_n+1)q_{n-1}+q_{n-2}},\ \frac{a_np_{n-1}+p_{n-2}}{a_nq_{n-1}+q_{n-2}};$$

from which we can calculate (again by Theorem 2.16)

$$\mu(E_{a_1,\ldots,a_n}) = \frac{1}{((a_n+1)q_{n-1}+q_{n-2})(a_nq_{n-1}+q_{n-2})} = \frac{1}{(q_n+q_{n-1})q_n}, \tag{18}$$

noting that the perforated interval has the same Lebesgue measure as the normal interval. Thus,

$$\mu(E_{a_1}) = \frac{1}{(a_1+1)a_1}.$$

Denote

$$H_{a_1,\ldots,a_n;k} := \bigcup_{a_{n+1}\leqslant k} E_{a_1,\ldots,a_n,a_{n+1}}.$$

The end-points of the perforated interval $E_{a_1,\ldots,a_n,a_{n+1}}$ are

$$[a_1,\ldots,a_{n+1}+1],\ [a_1,\ldots,a_{n+1}].$$

From an argument similar to the proof of Theorem 2.14, the rationals associated with these continued fraction expansions are either monotone increasing or decreasing, and therefore the end-points of the perforated interval $H_{a_1,\ldots,a_n,k}$ are

$$[a_1,\ldots,a_n,k+1],\ [a_1,a_2,\ldots,a_n,1],$$

which by Theorem 2.16 can be expressed as the rational numbers

$$\frac{(k+1)p_n+p_{n-1}}{(k+1)q_n+q_{n-1}},\ \frac{p_n+p_{n-1}}{q_n+q_{n-1}}.$$

Thus, the length of the perforated interval $H_{a_1,\ldots,a_n,k}$ is

$$\mu(H_{a_1,\ldots,a_n,k}) = \frac{k}{((k+1)q_n+q_{n-1})(q_n+q_{n-1})}. \tag{19}$$

If we wish to express this in terms of the length of $E_{a_1,\ldots,a_n}$, we get that, for all $a_1, \ldots, a_n$,

$$\frac{\mu(H_{a_1,\ldots,a_n;k})}{\mu(E_{a_1,\ldots,a_n})} = \frac{kq_n}{(k+1)q_n + q_{n-1}} < \frac{k}{k+1}, \tag{20}$$

which is obtained by equations (18) and (19).

Recalling the definition of $G_{n,M}$ and note that

$$G_{1,M} = \bigcup_{a_1=1,\ldots,M} E_{a_1}, \tag{21}$$

and thus

$$\begin{aligned}
\mu(G_{1,M}) &= \sum_{a_1=1}^{M} \frac{1}{a_1(a_1+1)} \\
&= \frac{1}{1\times 2} + \frac{1}{2\times 3} + \frac{1}{3\times 4} + \ldots + \frac{1}{M\times(M+1)} \\
&= 1 - \frac{1}{M+1} = \frac{M}{M+1},
\end{aligned}$$

where the next-to-last equality follows from an easy induction on M.

Note that inequality (20) can be re-written as

$$\mu(H_{a_1,\ldots,a_n;k}) < \frac{k}{k+1}\mu(E_{a_1,\ldots,a_n}). \tag{22}$$

Thus, in general,

$$\begin{aligned}
\mu(G_{n+1,M}) &= \sum_{\substack{a_1\leqslant M\\ \cdots \\ a_n\leqslant M}} \mu(H_{a_1,\ldots,a_n;M}) && \text{by Definition of } G_{n,M} \text{ and } H_{a_1,\ldots,a_n;M} \\
&\leqslant \frac{M}{M+1} \sum_{\substack{a_1\leqslant M\\ \cdots \\ a_n\leqslant M}} \mu(E_{a_1,\ldots,a_n}) && \text{by equation (22)} \\
&= \frac{M}{M+1}\mu(G_{n,M}) && \text{again by definition of } G_{n,M}.
\end{aligned}$$

Through this formula and equality (21), we derive

$$\mu(G_{n+1,M}) < \left(\frac{M}{M+1}\right)^{n+1}$$

Next, we note that, for any arbitrary but fixed $M \in \mathbb{N}$, this measure goes to zero as

n goes to infinity:

$$\lim_{n\to\infty} \mu(G_{n+1,M}) = \lim_{n\to\infty} \left(\frac{M}{M+1}\right)^{n+1} = 0.$$

By monotonicity of Lebesgue measure (Theorem 1.7), $\mu(F_M) \leqslant \mu(G_{n,M})$ for all $n \in \mathbb{N}$ and hence $\mu(F_M) = 0$ for all $M \in \mathbb{N}$, which concludes the proof. $\square$

In light of the usefulness of Theorem 2.38 in the proof of Theorem 2.47 and in 'generating' badly approximable numbers, we can shift our focus from studying badly approximable numbers to investigating infinite continued fraction expansions with bounded partial quotients. Informally, we could consider the finite number of distinct integers which occur in the continued fraction expansion of $x \in \mathrm{BAD}$ as distinct 'letters' in an 'alphabet'. Thus, the continued fraction expansion can be seen as an infinite 'word' over the alphabet. In the following section, we will make this intuition more rigorous.

3 Some Words on Words

Throughout this section, we will expand on material presented in [Lot02], unless otherwise stated. We will provide a more rigorous exposition of definitions, theorems, and proofs, and also provide one or two novel theorems. We will also rigorously define concepts used intuitively in the book. As in [Lot02], the introduction might be a bit dry in the sense of many definitions without much immediate applications; however, this lays a rigorous background for swifter formulations later on, both in algebraic combinatorics over words, and in this Thesis in general.

From here on, the adjective 'countable' will refer to infinite countable sets; in other words, to sets which are in bijection with the natural numbers.

3.1 Definition (alphabet, letter of an alphabet)**.** We define *an alphabet* to be a set A. The elements of this set are called *letters* of the alphabet. We write $a \in A$ to mean a is a letter of the alphabet A.

From here on, we will always assume that the alphabet A is finite.

3.2 Definition (space of words over an alphabet)**.** We denote by A^* the set of finite ordered sequences of elements of A, which we will call *words* over the alphabet A. We also define the empty word e, the word composed of no letters, and consider it as an element of A^*. We note that letters in A can also be considered words over A.

To avoid confusion between words and letters, we will use a bold script for the words and a normal script for the letters. We will write a word $\mathbf{w} \in A^*$ as $\mathbf{w} = w_1 \dots w_n$, where $w_1, \dots, w_n$ are letters of the alphabet A. Note that the letters $w_1, \dots, w_n$ are not necessarily distinct.

3.3 Definition (length of a word)**.** If $\mathbf{w} = w_1 \dots w_n$ is a word in A^*, then n is called the *length* of $\mathbf{w}$ and denoted by $|\mathbf{w}|$.

We may observe the following:

3.4 Note. We can view A^* as the set of maps from some subsets of $\mathbb{N}$ into A in the following sense: for every word $\mathbf{w} = w_1 \dots w_n$ we define a map $f_{\mathbf{w}} : \{0, \dots, n-1\} \to A$ by $f_{\mathbf{w}}(i) = w_{i+1}$ for $i \in \{0, \dots, n-1\}$, and vice-versa - for every map $f : \{0, \dots, n-1\} \to A$ we define a word $\mathbf{w} = w_1 \dots w_n$ with $w_i = f(i-1)$.

The above correspondence justifies the author of this dissertation to formulate and prove the theorem:

3.5 Theorem. *The set of finite words A^* is bijective to $\bigcup_{n\in\mathbb{N}} \prod_{0\leqslant i<n} A_i$, where $A_i = A$ for all $i \leqslant n$ and $\forall n \in \mathbb{N}$.*

Proof. We construct a bijection $f : A^* \to \bigcup_{n\in\mathbb{N}} \prod_{0\leqslant i<n} A_i$ in the following manner.

For a word $\mathbf{w} \in A^*$, $\mathbf{w} = w_1 \dots, w_m$, we set $f(\mathbf{w}) = (w_1, \dots, w_m) \in \prod_{0\leqslant i<m} A_i$. The map f is onto: each word of length m corresponds to an ordered m-tuple in $\prod_{0\leqslant i<m} A_i$, and each ordered m-tuple $(w_1, \dots, w_m)$ is the image of a word $\mathbf{w} = w_1 \dots, w_m$. Moreover, f is one-to-one: if $\mathbf{u}, \mathbf{w} \in A^*$ and $\mathbf{w} \neq \mathbf{u}$, then either $|\mathbf{w}| \neq |\mathbf{u}|$ (thus the ordered tuples would be of different lengths and trivially not equal), or $|\mathbf{w}| = |\mathbf{u}|$ (say $= m$) and without loss of generality, there exists $j \leqslant |\mathbf{w}|$ such that such that $w_j \neq u_j$. Then $f(\mathbf{w}) = (w_1, \dots, w_j, \dots, w_m) \neq (u_1 \dots, u_j, \dots, u_m) = f(\mathbf{u})$. □

3.6 Note. It is easy to see the two sets in question have the same cardinality. However, the bijection we just constructed has a further 'nice' property, namely, that it can be modified to be order-preserving in the following sense. If we have an order on the alphabet A, we can extend it to an order on A^* by setting $\mathbf{w} < \mathbf{u}$ if and only if $|\mathbf{w}| < |\mathbf{u}|$ or $|\mathbf{w}| = |\mathbf{u}|$ and there is an index $i \leqslant |\mathbf{w}|$ such that $w_j = u_j$ for $j < i$ and $w_i < u_i$. It is easy to see how the construction above can be slightly modified to preserve this order. Moreover, from a purely set-theoretic point of view, the construction above does not rely on the Axiom of Choice.

This is a very natural bijection, which we will even consider as 'canonical'. It justifies identifying the two spaces, and gives a more concrete object to think about when considering the space A^*.

3.7 Note. In the train of thought of Note 3.4, we can view the length $|.|$ as a function $|.| : A^* \to \mathbb{N}$, $|\mathbf{w}| = |\mathrm{dom} f_{\mathbf{w}}|$, where $f_{\mathbf{w}}$ is the unique map defined in Note 3.4. We will take the convention that the length of the empty word ϵ is $|\epsilon| = 0$.

3.8 Definition (concatenation)**.** On the space A^*, we will define a binary operation, called *concatenation of words*. It maps the pair of words $\mathbf{w} = w_1 \dots w_n$ and $\mathbf{u} = u_1 \dots u_m$ to the word $\mathbf{wu} = w_1 \dots w_n u_1 \dots u_n$. If we have $\mathbf{w} = \mathbf{uv}$ for some words $\mathbf{u}, \mathbf{v}, \mathbf{w}$, will also say that the word $\mathbf{w}$ can be *factorized* into the words $\mathbf{u}$ and $\mathbf{v}$.

Note that concatenation is associative. This will be useful in the next subsection, when we consider some structure on the space of words induced by this binary operation.

3.9 Definition (conjugate)**.** Let $\mathbf{w} \in A^*$ be a word. We say that the word $\mathbf{u} \in A^*$ is a *conjugate* of $\mathbf{w}$ iff there exist words $\mathbf{s}, \mathbf{t} \in A^*$ such that $\mathbf{w} = \mathbf{st}$ and $\mathbf{u} = \mathbf{ts}$. Note that in this case, $|\mathbf{w}| = |\mathbf{u}| = |\mathbf{s}| + |\mathbf{t}|$.

3.10 Definition (conjugacy class)**.** The *conjugacy class* of a word $\mathbf{w} \in A^*$ is the set of all of its conjugates. More formally, if $\mathbf{w} = w_1 \dots w_n$, then the conjugacy class of $\mathbf{w}$, denoted by $\mathrm{Conj}(\mathbf{w})$, is

$$\mathrm{Conj}(\mathbf{w}) = \{\mathbf{w}\} \cup \{\mathbf{u} \in A^* : \mathbf{u} = w_i w_{i+1} \dots w_n w_1 \dots w_{i-1}, 1 < i \leqslant n\}$$

In order to study the space A^* of finite words, we can introduce some structure on it. For example, we can define several orders on A^*: the prefix, radix, and lexicographic ones. The first one is a partial order, while the latter two are total orders which refine the prefix order, but can only be defined when the alphabet A is ordered. For the purposes of this thesis, we will only need the lexicographic order (defined below). The reader interested in these and more possible orders on words is refered to [Lot02] and [CJS09], and the reader interested in more on different types of orders on sets and their properties is refered to the classical book of Set-Theory, [Kun11].

3.11 Definition (prefix)**.** A word $\mathbf{u} = u_1 \dots u_n$ is a *prefix* of a word $\mathbf{w} = w_1 \dots w_k$ if and only if $n \leqslant k$ and the letters $u_i = w_i$ for $1 \leqslant i \leqslant n$. In this case, we will write $\mathbf{w} = \mathbf{uw}'$ with the implicit assumption that $\mathbf{w}' = w_{n+1} \dots w_k$.

In Chapter 5, we will come accross several occasions when one finite word is 'not quite' a prefix of another. Thus, the author of this dissertation introduces the following definition here:

3.12 Definition (near-prefix of order n)**.** Let $\mathbf{v}, \mathbf{w} \in A^*$, $\mathbf{v} = v_1 \dots v_k$, $\mathbf{w} = w_1 \dots w_m$ with $k < m$. For a positive integer $n < k$, we call $\mathbf{v}$ a *near-prefix of order n of* $\mathbf{w}$, if for all $i = 1, \dots k - n$, we have $v_i = w_i$.

Intuitively, the above definition says that the word $\mathbf{v}$ is a prefix of $\mathbf{w}$, with the possible exception of its last n letters.

3.13 Definition (lexicographic order)**.** Let A be an ordered alphabet and let $\mathbf{u}$ and $\mathbf{w}$ be words over A. The *lexicographic order* on A^* is defined in the following manner. We say $\mathbf{u} \leqslant \mathbf{w}$ if and only if either $\mathbf{u}$ is a prefix of $\mathbf{w}$, or there exist factorizations $\mathbf{u} = \mathbf{v}a\mathbf{u}'$, $\mathbf{w} = \mathbf{v}b\mathbf{w}'$, where $\mathbf{v}, \mathbf{u}', \mathbf{w}'$ are words and a and b are letters with $a < b$.

3.14 Definition (Lyndon word)**.** We call a word $\mathbf{w} \in A^*$ a *Lyndon word* if and only if it is minimal with respect to the lexicographic order in its conjugacy class.

In order to deal with infinite continued fraction expansions with bounded partial quotients, we consider the following notion:

3.15 Definition (space of infinite words over a finite alphabet)**.** We denote by $A^{\mathbb{N}}$ the set of infinite ordered sequences of elements of A, which we will call *(infinite) words* over the alphabet A.

3.16 Definition (prefix of length n)**.** For an infinite word $\mathbf{x} \in A^{\mathbb{N}}$, we define the finite word $Pref_n(\mathbf{x}) \in A^*$ as the prefix of length n of $\mathbf{x}$.

For example, if $\mathbf{v}$ is a near-prefix of order n of $\mathbf{w}$ with $|\mathbf{v}| = k$, $|\mathbf{w}| = m$, we have $Pref_{k-n}(\mathbf{v}) = Pref_{k-n}(\mathbf{w})$.

Periodic words will play an especially important part later in Chapter 4 and Chapter 5; thus, we introduce the notion here.

3.17 Definition (periodic infinite word)**.** An infinite word $\mathbf{w} = w_1 \dots w_n \dots \in A^{\mathbb{N}}$ is called *periodic* if for some $N \in \mathbb{N}$, we have that for all $i \in \mathbb{N}$, $w_i = w_{i+N}$. The least N for which this equality holds is called the *period* of the word $\mathbf{w}$. If an infinite word $\mathbf{w} \in A^{\mathbb{N}}$ is periodic and $\mathbf{w} = \mathbf{uuuuu}\dots$ for some finite word $\mathbf{u} = u_1 \dots u_n \in A^*$, we will write $\mathbf{w} = (\overline{\mathbf{u}}) = (\overline{u_1 \dots u_n})$.

There are also words which are similar to the periodic ones, but not necessarily periodic themselves:

3.18 Definition (recurrent word)**.** An infinite word $\mathbf{w} = w_1 \dots w_n \dots \in A^{\mathbb{N}}$ is called *recurrent* if every finite block $\mathbf{u} \in A^*$ occuring in $\mathbf{w}$ occurs infinitely often.

Note that every periodic word is recurrent; however, not every recurrent word is periodic. For an example, the interested reader is directed to [Lot02].

3.19 Definition (distance on $A^{\mathbb{N}}$)**.** We define a *distance* $d : A^{\mathbb{N}} \to \mathbb{R}^+ \cup \{0\}$ on the set of infinite words, by $d(\mathbf{x}, \mathbf{y}) = 2^{-n}$, where $\mathbf{x} = x_1 \dots x_n \dots,\ \mathbf{y} = y_1 \dots y_n \dots$ and

$$n = \min\{k \in \mathbb{N} : x_k \neq y_k\}.$$

We implicitly define $d(\mathbf{x}, \mathbf{x}) = 0$.

In the next section, we will consider a natural extension of this notion of distance to the space $A^{\mathbb{N}} \cup A^*$.

Now, we complement the exposition in Lothaire by showing that the function defined above indeed satisfies the required distance axioms. Let $\mathbf{x}, \mathbf{y}, \mathbf{z} \in A^{\mathbb{N}}$. Indeed, since $2^{-n} > 0$ for all $n \in \mathbb{N}^+$ and we have defined $d(\mathbf{x}, \mathbf{x}) = 0$, we have that $d(\mathbf{x}, \mathbf{y}) \geqslant 0$. Also, $d(\mathbf{x}, \mathbf{y}) = 0$ if and only if $\mathbf{x} = \mathbf{y}$, since otherwise $2^{-n} > 0$. This function is obviously symmetric, by symmetry of equality. Finally, we show that the triangle inequality holds. Without loss of generality, assume that $\mathbf{x}, \mathbf{y}, \mathbf{z}$ are all distinct (the case when two are equal is obvious).

For words $\mathbf{u}, \mathbf{v} \in A^{\mathbb{N}}$, define $n(\mathbf{u}, \mathbf{v}) = \min\{k \in \mathbb{N} : u_k \neq v_k\}$. Note that for $0 < i < n(\mathbf{x}, \mathbf{y})$, we have $x_i = y_i$.

Say $n(\mathbf{x}, \mathbf{y}) = N$.

We have two cases.

Case I: if $N > n(\mathbf{x}, \mathbf{z})$, then $n(\mathbf{y}, \mathbf{z}) = n(\mathbf{x}, \mathbf{z})$, since $y_i = x_i$ for $i < N$. Thus,

$$2^{-N} < 2 \times 2^{-N} \leqslant 2^{-n(\mathbf{x},\mathbf{z})} + 2^{-n(\mathbf{z},\mathbf{y})},$$

as required.

Case II: Assume $N \leqslant n(\mathbf{x}, \mathbf{z})$; in particular, this means that $x_N = z_N$, and so $z_N \neq y_N$ by definition of N. Thus, $n(\mathbf{y}, \mathbf{z}) = N$, since for $i < N$, we have $x_i = y_i = z_i$ by the above assumptions. Therefore,

$$2^{-N} < 2^{-N} + 2^{-n(\mathbf{x},\mathbf{z})} \leqslant 2^{-n(\mathbf{y},\mathbf{z})} + 2^{-n(\mathbf{x},\mathbf{z})},$$

which finally shows that the distance defined indeed satisfies the triangle inequality, and thus is indeed a distance.

This distance gives rise to a topology on $A^{\mathbb{N}}$.

We finish with one more notion needed later on:

3.20 Definition (shift operator)**.** The *shift operator* is the function $\sigma : A^{\mathbb{N}} \to A^{\mathbb{N}}$ defined for a word $\mathbf{w} = w_1 w_2 \ldots \in A^{\mathbb{N}}$ as $\sigma(w_1 w_2 w_3 \ldots) = w_2 w_3 \ldots$.

3.1 More Words on Morphic Words

The material in this subsection will be needed for some very interesting observations in Chapter 5, where certain sequences of numbers have an unexpected pattern in their binary expansions.

The definition of concatenation justifies viewing the space of words over an alphabet as an example of a semigroup. We recall the definition of the latter:

3.21 Definition (semigroup)**.** A semigroup is a set with an associative binary operation.

In order to define some interesting infinite words, we also need the notion of a semigroup morphism.

3.22 Definition (semigroup morphism)**.** Let S and T be semigroups with binary operations $\cdot_S$ and $\cdot_T$, respectively. We define a *semigroup morphism* f from S to T as a mapping $f : S \to T$ such that, for all $u, w \in S$, we have $f(u \cdot_S w) = f(u) \cdot_T f(w)$

We will now focus on some more specific types of morphisms between spaces of words: the nonerasing morphisms.

3.23 Definition (nonerasing morphism)**.** We call a morphism $h : A^* \to A^*$ *nonerasing* if and only if the image of each letter is a non-empty word.

In Lothaire, we have the following definition of a morphic word:

3.24 Definition (morphic word, [Lot02])**.** A morphic word $\mathbf{x}(h, a)$ is obtained from a nonerasing morphism $h : A^* \to A^*$ and from a letter $a \in A$ such that $h(a) = a\mathbf{s}$ for some non-empty word $\mathbf{s}$ in the following manner:

$$\mathbf{x}(h, a) = a\mathbf{s}h(\mathbf{s})h^2(\mathbf{s}) \ldots h^n(\mathbf{s}) \ldots .$$

In order to justify the above definition (in other words, that there are words which satisfy its conditions), we have the following Theorem 3.25 formulated in Lothaire:

3.25 Theorem. *Let $h : A^* \to A^*$ be a nonerasing morphism, and let $a \in A$ be a letter such that $h(a) = a\mathbf{s}$ for some nonempty word $\mathbf{s}$. For $n \in \mathbb{N}$, denote*

$$\mathbf{u}_n := h^n(a), \ \mathbf{v}_n = h^n(\mathbf{s}).$$

Then

1. $\mathbf{u}_{n+1} = \mathbf{u}_n\mathbf{v}_n$. *In particular, for all $n \in \mathbb{N}$, we have that $\mathbf{u}_n$ is a prefix of $\mathbf{u}_{n+1}$.*
2. $\mathbf{u}_{n+1} = a\mathbf{v}_0\mathbf{v}_1 \ldots \mathbf{v}_n$
3. *We have*
$$\mathbf{x}(h, a) = \lim_{n\to\infty} \mathbf{u}_n;$$
moreover, $\mathbf{x}(h, a)$ is a fixed point of h and is the unique fixed point of h starting from the letter a.

We note that the problem of finite words converging to infinite ones is not addressed at all in Lothaire. We also note that the infinite word $\mathbf{x}(h, a)$ is not in the domain of the morphism h, and thus we cannot talk about it being a fixed point, as claimed in part 3.

We propose a solution as follows. First, we expand the alphabet to $A \cup \{\aleph\}$, where $\aleph$ is a symbol (letter) not in A. Then, we consider each finite word $\mathbf{u} \in A^*$ as an infinite word $\mathbf{u}\overline{\aleph}$ over the alphabet $A \cup \{\aleph\}$. We note that $\mathcal{A}^{\mathbb{N}} \subset (A \cup \{\aleph\})^{\mathbb{N}}$, and that A^* has a natural embedding ι into $(A \cup \{\aleph\})^{\mathbb{N}}$ given by $\iota(\mathbf{u}) = \mathbf{u}\overline{\aleph}$. In this setting, it now makes sense to talk about finite words in A^* converging to an infinite word in $A^{\mathbb{N}}$, by continuity of h, distance, and ι. Finally, we observe that in part 3 of Theorem 3.25, we are in fact considering the natural extension of the morphism h to $(A \cup \{\aleph\})^{\mathbb{N}}$, noting that a morphism is uniquely defined by its values on the alphabet A.

We now proceed to provide a more rigorous and detailed proof than the one found in [Lot02]:

Proof. We have that:

1. $\mathbf{u}_{n+1} = h^{n+1}(a) = h^n(h(a)) = h^n(a\mathbf{s}) = h^n(a)h^n(\mathbf{s}) = \mathbf{u}_n\mathbf{v}_n$, where the next-to-last equality follows from the fact that h is a morphism.

2. We show part 2 by induction. It clearly holds for the base case $n = 0$. For the inductive step, let us assume that for some $n \in \mathbb{N}$, we have $\mathbf{u}_n = a\mathbf{v}_0 \dots \mathbf{v}_{n-1}$. Then

$$\begin{aligned} \mathbf{u}_{n+1} &= \mathbf{u}_n\mathbf{v}_n && \text{by part 1} \\ &= a\mathbf{v}_0 \dots \mathbf{v}_{n-1}\mathbf{v}_n && \text{by the inductive hypothesis.} \end{aligned}$$

3. By parts 1 and 2, it is clear that the word $\mathbf{x}$ is the limit of (the extensions of) its prefixes. To show it is a fixed point of the extension of h, we note that

$$h(\mathbf{x}) = h(a)h(\mathbf{s})h^2(\mathbf{s}) \dots = \mathbf{x}.$$

   It is the unique fixed point starting with the letter a, since

$$\lim_{n\to\infty} h^n(a) = \lim_{n\to\infty} \mathbf{u}_n$$

   by definition of $\mathbf{u}_n$. Moreover, it is easily seen that the distance between the expansions of $\mathbf{u}_n$ in $A^{\mathbb{N}}$ tends to zero as $n \to \infty$.

□

One important example of a morphic word is the Thue-Morse word, which will make several surprising appearances later on.

3.26 Definition (Thue-Morse word, [AS99]). Let $A = \{0, 1\}$. Define a non-erasing morphism $\phi : A^{\mathbb{N}} \to A^{\mathbb{N}}$ by

$$\phi(0) = 01$$
$$\phi(1) = 10.$$

The *Thue-Morse word* $\mathbf{t}$ is defined as the limit

$$\mathbf{t} = \lim_{n \to \infty} \phi^n(0).$$

Note that by Theorem 3.25, the Thue-Morse word $\mathbf{t}$ is the unique fixed point of the nonerasing morphism ϕ starting from the letter 0.

The first couple of letters of $\mathbf{t}$ are

$$\mathbf{t} = 0110100110010110100101100110100110010110011010010110100110010110\ldots$$

The Thue-Morse word is fascinating both in its wide scope of applications and appearances, from number theory and recurrent geodesics to chess games [Euw29], astronomy [Rou07], physics in general [AP89], [AAK$^+$86], and in its rich and complex history, which also reflects the word's ubiquity in various mathematical (and extra-mathematical) fields. It was defined independently by many mathematicians and non-mathematicians, in fundamentally different settings. For example, world chess champion Max Euwe implicitly used its properties in his 1929 paper [Euw29] to define sequences of moves which would lead to infinite repetition in a game of chess. For a more complete and fascinating overview, the interested reader is refered to [AS99].

We will now focus on the three most significant mathematicians who came upon this sequence in three completely different contexts. In 1851, Prouhet implicitly discovered this sequence in his number-theoretic work [Pro51]. However, it was only in 1912 that Axel Thue explicitly defined the word in his paper [Thu12] on combinatorics on words. Thue was probably completely unaware of Prouhet's work; ironically, since Thue's own paper was in an obscure Norwegian journal, it also did not gather the amount of attention it deserved. Definition 3.27 below can be found in his 'Satz 5', or Theorem 2.4 in [Ber94], which is a translation of two papers of Thue. These papers of Thue would become one of the foundations of the field of combinatorics on words, which would gain greater popularity a bit later on in the 1900's. The sequence was 'discovered' yet a third time by Marston Morse in 1921 [Mor21] in differential geometry.

This brings us to some alternative ways of defining the Thue-Morse word, which are not at all obviously equivalent.

3.27 Definition (Thue-Morse word [Lot02])**.** Let $A = \{0, 1\}$. Define sequences of words $\{\mathbf{u}_n\}_{n\geqslant 0}$ $\{\mathbf{v}_n\}_{n\geqslant 0}$ over the binary alphabet A by

$$\begin{aligned} &\mathbf{u}_0 = 0, && \mathbf{v}_0 = 1, && \\ &\mathbf{u}_{n+1} = \mathbf{u}_n\mathbf{v}_n, && \mathbf{v}_{n+1} = \mathbf{v}_n\mathbf{u}_n, && n \geqslant 0. \end{aligned}$$

The *Thue-Morse word* $\mathbf{t}$ is defined as the limit

$$\mathbf{t} = \lim_{n\to\infty} \mathbf{u}_n.$$

3.28 Note. Through Definition 3.27, one can easily see that the prefixes $\mathbf{u}_n$ of the Thue-Morse word of length 2^n have the following structure (for $n \geqslant 1$):

$$\mathbf{u}_n = \mathbf{u}_{n-1}\underline{\mathbf{u}_{n-1}},$$

where by $\underline{\mathbf{w}}$ we denote the binary word obtained from $\mathbf{w}$ by changing all the 0's to 1's and vice-versa.

3.29 Definition (Thue-Morse word, [AS03])**.** The Thue-Morse word $\mathbf{t} = t_1t_2\dots t_n\dots$ is the unique infinite word over the binary alphabet satisfying the following condition: for $n \in \mathbb{N}$,

- $t_n = 1$ if the number of 1's in the binary expansion of n is odd;
- $t_n = 0$ otherwise (if the number of 1's in the binary expansion of n is even).

To give a flavour of precisely how ubiquitous and strange this sequence is, here is yet another definition:

3.30 Definition (Thue-Morse word, [AC85])**.** Inductively define a sequence of numbers $\{\alpha_n\}_{n\geqslant 0}$ by $\alpha_0 = 1$, and

$$\alpha_{n+1} := \begin{cases} +1 & \text{if } \left(\frac{1}{2}\right)^{\alpha_0} \times \left(\frac{3}{4}\right)^{\alpha_1} \times \dots \times \left(\frac{2n+1}{2n+2}\right)^{\alpha_n} > \frac{\sqrt{2}}{2}, \\ -1 & \text{if } \left(\frac{1}{2}\right)^{\alpha_0} \times \left(\frac{3}{4}\right)^{\alpha_1} \times \dots \times \left(\frac{2n+1}{2n+2}\right)^{\alpha_n} < \frac{\sqrt{2}}{2}. \end{cases}$$

Then the sequence $\{\alpha_n\}_{n\geqslant 0}$ is equal to the Thue-Morse sequence on the alphabet $\{-1, +1\}$. Alternatively, for all $n \geqslant 0$ we have $\alpha_n = (-1)^{t_n}$, where t_n is the nth letter of $\mathbf{t}$.

3.31 Theorem. *Definitions 3.26, 3.27, 3.29 and 3.30 are all equivalent.*

For a proof of the equivalences in Theorem 3.31, the interested reader is referred to [AS03], [Lot02] and [AC85].

3.32 Theorem. *The words* 111 *and* 000 *are not factors of the Thue-Morse word.*

We mention the above Theorem 3.32 out of interest; it will not be central to the rest of this thesis. A proof of this can be found in [Lot02]

The Thue-Morse word has made many unexpected appearances in very diverse fields, from mathematics to physics and beyond. It will make at least one more such appearance later on in this Thesis.

3.2 Words in Diophantine Approximations

What do combinatorics on words have to do with Diophantine approximation?

We can consider the continued fraction expansions of badly approximable numbers as words over finite alphabets: we know that they are bounded, and each one of the convergents can be considered as a letter in the alphabet.

Notation. For a badly approximable number $\alpha \in \mathbb{R}$, we will denote by $\mathbf{w}(\alpha)$ the word obtained from its continued fraction expansion.

For example, the Golden ratio is the infinite word composed of just one letter:

$$\mathbf{w}(\phi) = 1111\ldots1\ldots = (\overline{\mathbf{1}}).$$

More generally, we have:

3.33 Corollary (Corollary to Lagrange's Theorem)**.** *Let $\alpha \in [0,1]$ be a quadratic irrational. By Theorem 2.40, its continued fraction expansion is bounded, say by $M \in \mathbb{N}$. Then $\mathbf{w}(\alpha)$ is an eventually periodic word over the alphabet $A = \{0,1,\ldots,M\}$.*

Moreover, the expansions of real numbers in a given base can be considered as words. For the purposes of this dissertation, we will only need to consider the binary expansions of numbers in the unit interval $[0,1]$.

Notation. Let $\alpha \in [0,1]$ be a number. We will denote by $\mathbf{w}^{(2)}(\alpha)$ the word obtained from its binary expansion, which will be a word over the binary alphabet $A = \{0,1\}$.

3.34 Example. For example, we have:

1. $\mathbf{w}^{(2)}(1/4) = 01$,
2. $\mathbf{w}^{(2)}(1/3) = 01010101\ldots = (\overline{01})$.

The theory of combinatorics on words has been useful not only as a language with which to talk about continued fraction expansions or binary expansions of certain numbers, but also has been useful in the study of those numbers. For example, Theorem 4.6

considers badly approximable numbers α such that $\mathbf{w}(\alpha)$ is a recurrent word. There are many other applications in results related to badly approximable numbers, as we will see in Sections 4 and 5.

We now have all the necessary machinery to continue onto the Littlewood and related conjectures.

4 The Littlewood Conjecture and a Little More (or Less)

The Littlewood Conjecture was first stated by John Littlewood in the 1930's in his book [Lit68], but is more often cited as first mentioned in a 1942 paper by one of his students, D. Spencer [Spe42]. It has since become a major problem in Diophantine approximation, which unfortunately is currently considered out of reach. It has nonetheless spurred a lot of research, as evidenced by the number of papers in preparation or that have been recently published in the area. Moreover, study of the Littlewood Conjecture has inspired several other 'Littlewood-type' problems to be asked. In this thesis, we will focus on two of them: the Mixed Littlewood Conjecture, and a special case - the p-adic Littlewood Conjecture.

4.1 The Littlewood Conjecture

Dirichlet's Theorem 2.24 can be re-stated as: for any irrational number α, there exist infinitely many integers $n \in \mathbb{N}$ such that

$$n||n\alpha|| \leqslant 1.$$

It is natural to ask what happens in higher dimensions. In particular, what can we say about a pair of numbers $\alpha, \beta \in \mathbb{R}$? Dirichlet's inequality implies that for all pairs $(\alpha, \beta) \in \mathbb{R}^2$, there are infinitely many $n \in \mathbb{N}$ such that

$$n.||n\alpha||.||n\beta|| < 1.$$

Littlewood conjectured that the constant 1 on the right-hand side of the above inequality can be replaced by an arbitrarily small value:

4.1 Conjecture (Littlewood Conjecture)**.** *For every pair of real numbers $\alpha, \beta \in \mathbb{R}$, we have:*

$$\liminf_{q\to\infty,\ q\in\mathbb{N}} q.||q\alpha||.||q\beta|| = 0. \tag{23}$$

From now on, whenever we talk about $\liminf_{q\to\infty} P(q)$, where $P(q)$ is some expression, we implicitly assume that $q \in \mathbb{N}$.

Note that, if Dirichlet's inequality is a statement about how well a real number can be approximated by a rational number with a relatively small denominator, then the Littlewood Conjecture is a statement about how well rational numbers with the same denominator can simultaneously approximate pairs of reals. However, this conjecture is incredibly difficult to prove. It is not even known whether the Littlewood Conjecture holds for $\alpha = \sqrt{2}$ and $\beta = \sqrt{3}$ [HM14]! More generally, it is still open whether the conjecture holds in the case when α and β are quadratic irrationals which are linearly independent over $\mathbb{Q}$.

So, for which numbers do we know that the Littlewood conjecture is satisfied? Firstly, equation (23) obviously holds for any pair of rational numbers $p_1/q_2, p_2/q_2 \in \mathbb{Q}$. Moreover, whenever $\alpha \notin$ BAD, the pair (α, β) satisfies Littlewood for any $\beta \in \mathbb{R}$. By looking at (24), one can intuitively see why the badly approximable numbers are the natural set of counter-examples to consider. This is made more rigorous in the following Proposition:

4.2 Proposition. *For any real $\alpha \notin BAD$, we have*

$$\liminf_{n\to\infty} n||n\alpha||.||n\beta|| = 0$$

Proof. Let $\alpha \notin$ BAD. Then there is a sequence $\{n_k\}_{k\in\mathbb{N}}$ of natural numbers such that

$$\lim_{k\to\infty} n_k||n_k\alpha|| = 0.$$

Note that for all $\beta \in \mathbb{R}$, for all $n \in \mathbb{N}$, the value $||n\beta||$ is bounded above by $1/2$. Therefore, for all $\beta \in \mathbb{R}$,

$$\lim_{k\to\infty} n_k||n_k\alpha||.||n_k\beta|| = 0,$$

and thus

$$\liminf_{n\to\infty} n||n\alpha||.||n\beta|| = 0,$$

as required. □

How big is the set of possible counter-examples to the Littlewood Conjecture? Ideally, we would want the Conjecture to be true, and thus would want the set to be empty. Until the conjecture is proven, we can try to provide some estimates on the size of the set of numbers which might be counter-examples to it. We have seen that in the 1-dimensional case, for badly approximable numbers α we have

$$\liminf_{n\to\infty} n||n\alpha|| > 0. \tag{24}$$

This, coupled with Proposition 4.2 gives that the set of possible counter-examples to the Littlewood conjecture is a subset of the badly approximable pairs. Therefore, the set of potential counter-examples is in one sense very small - as a corollary to Theorem 2.47, we have that it also has Lebesgue measure zero. However, the set BAD is in another sense 'large' - it has full Hausdorff dimension in $\mathbb{R}$. We will not go into details of Hausdorff dimension here, but intuitively such sets have a very 'rich' structure. Recently, Pollington and Velani [PV00] have shown that if $\alpha \in$ BAD, then set of $\beta \in$ BAD such that $1, \alpha, \beta$ are linearly independent over $\mathbb{Q}$ and the Littlewood Conjecture holds for α and β has full Hausdorff dimension. We would want a better restriction on its Hausdorff dimension than the one available through [PV00]. A more recent result by Einsiedler, Katok and Lindenstrauss [EKL06] provides just that: it states that the set of exceptions to the Littlewood Conjecutre has zero Hausdorff dimension. Still, we do not know anything about the cardinality of the set of potential counter-examples. Though it has both Lebesgue measure zero and Hausdorff dimension zero, it might still be uncountable. Of course, if the Littlewood Conjecture holds, the set of its counter-examples would be empty; however, we can currently not even restrict its cardinality to be countable.

The Pollington-Vellani Theorem [PV00] states that the structure of pairs of possible counter-examples is very 'rich', but provides no specific example of such pairs. Cassels and Swinnerton-Dyer showed that the Littlewood conjecture is satisfied for pairs of numbers that belong to the same cubic field [CSD55]. Moreover, Peck [Pec61] has shown that, if α, β are both cubic irrationals in the same cubic field, the following inequality is satisfied infinitely often:

$$q||q\alpha||.||q\beta|| \leqslant \frac{1}{\ln q}.$$

If it were true that the only badly approximable algebraic irrationals are the quadratic ones, then Peck's Theorem (and the Cassels-Swinnerton-Dyer result) would follow immediately from Proposition 4.2. However, as previously mentioned, it is still unknown whether the cubic irrationals are badly approximable or not. So far we do not have any specific example of a badly approximable pair of numbers which satisfies the Littlewood Conjecture.

The above inequality from Peck's Theorem might make one wonder: what will happen if we consider a variation of the expression in equation (23)? In 2011, Badziahin showed that

4.3 Theorem ([Bad11])**.** *For any $\alpha \in \mathbb{R}$, the set of numbers $\beta \in \mathbb{R}$ for which*

$$inf_{q \geqslant 3} q. \ln q \ln \ln q.||q\alpha||.||q\beta|| > 0$$

has full (Hausdorff) dimension.

However, there are other modifications of equation (23) which lead to new open questions. This brings us to the next subsection.

4.2 The Mixed Littlewood Conjecture

It is natural to ask: what makes the Littlewood conjecture so difficult? One possible intuitive answer would be the addition of another number, β. So perhaps, if one were to replace $||n\beta||$ by something else which depends perhaps on n or α in equation (23), the question would become easier to tackle.

One such variation was proposed by de Mathan and Teulié in [dMT04], where they use a 'generalisation' of the p-adic norm (discussed further in the next subsection):

4.4 Conjecture (Mixed Littlewood Conjecture, [dMT04]). *Let $D = \{d_k\}_{k\geqslant 1}$ be a sequence of integers such that $d_k \geqslant 2$ for all $k \in \mathbb{N}$, and define integers e_n (for $n \in \mathbb{N}$) by:*

$$\begin{aligned} e_0 &= 1 \\ e_n &= \prod_{1\leqslant k\leqslant n} d_k. \end{aligned}$$

For an integer p, we define

$$w_D(p) := \sup\{n \geqslant 0 : p \in e_n\mathbb{Z}\},$$

and

$$|p|_D = \frac{1}{e_{w_D(p)}} = \inf\left\{\frac{1}{e_n} : p \in e_n\mathbb{Z}\right\}.$$

Then, for all $\alpha \in \mathbb{R}$, we conjecture that

$$\liminf_{q\to\infty} q.||q\alpha||.|q|_D = 0.$$

Note that α must be badly approximable. We can draw some parallels with the Littlewood Conjecture. Just as the Littlewood Conjecture has been established for pairs of numbers in the same cubic field, so do we have, by a 2004 result of de Mathan and Teuilie, that a very strong inequality holds for quadratic irrationals in a special case - note the additional factor of $\log n$ in the inequality below:

4.5 Theorem ([dMT04]). *For any bounded sequence D of integers greater or equal to 2 and for any $\alpha \in \mathbb{R}$, if α is a quadratic irrational, then*

$$\liminf_{n\to\infty} n|n|_D||n\alpha|| \ln n < \infty.$$

Another proof of Theorem 4.5 follows from [BBEK14, Section 6].

We finish this section with a very interesting result linking the Mixed Littlewood Conjecture to the word obtained from the continued fraction expansion of a number:

4.6 Theorem ([BBEK14])**.** *Let $\{a_n\}_{n\in\mathbb{N}^+}$ be a sequence of positive integers. If there exists $m \in \mathbb{N}$ such that the infinite word $a_{m+1}a_{m+2}\dots$ is recurrent, then, for every sequence D of integers greater than or equal to 2, the real number $\alpha := [0; a_1, a_2, \dots]$ satisfies*

$$\inf_{q\geqslant 1} q.|q|_D.||q\alpha|| = 0.$$

4.3 The p-adic Littlewood Conjecture

A slight weakening of the Mixed Littlewood conjecture is the p-adic Littlewood conjecture, which takes the sequence D to be just the constant sequence $\{p\}_{n\in\mathbb{N}}$, where p is some prime number. Thus, the valuation $|.|_D$ introduced in the Mixed Littlewood Conjecture (4.4) becomes the p-adic norm.

For completeness, we introduce the notion of p-adic norm; for theory related to p-adic analysis, we use [Gou93] and [Rob00].

4.7 Definition (p-adic valuation on $\mathbb{Z}$)**.** Let $p \in \mathbb{Z}$ be prime. We define the *p-adic valuation on $\mathbb{Z}$* as the map $\nu_p(x) : \mathbb{Z} \to \mathbb{N}$ given by $\nu_p(x) = q$. For $x \in \mathbb{Z} \setminus \{0\}$, we define q as the greatest power of p in the prime factorization of x, in other words,

$$p^q \mid x \text{ and } p^{q+1} \nmid x,$$

and we set $\nu_p(0) = \infty$.

4.8 Definition (p-adic norm)**.** Let $p \in \mathbb{Z}$ be prime. We define the *p-adic norm $|.|_p$ on $\mathbb{Z}$* as the function $|.|_p : \mathbb{Z} \to \mathbb{R}$ defined by

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

The p-adic norm can be generalized for rational numbers, but the above definition suffices for the purposes of this thesis.

Note that, for all $m, n \in \mathbb{N}$ and all prime $p \in \mathbb{Z}$, $p^m|p^n|_p = p^{m-n}$.

The p-adic Littlewood Conjecture states:

4.9 Conjecture (p-adic Littlewood Conjecture)**.** *For all $\alpha \in \mathbb{R}$, for all prime $p \in \mathbb{Z}$, we have*

$$\liminf_{n\to\infty} n|n|_p||n\alpha|| = 0. \tag{25}$$

When a real number α satisfies the p-adic Littlewood Conjecture, we will write $pLC(\alpha)$ for brevity.

The Conjecture was formulated by de Mathan and Teuille in [dMT04], and is believed more accessible than the classic Littlewood conjecture. We can say something about quadratic irrationals in the p-adic case (analogous to the Mixed Littlewood Case), by setting the sequence D to be the constant sequence $\{x_n\}_{n\in\mathbb{N}}, x_n = p\ \forall n \in \mathbb{N}$, in Theorem 4.5. An alternative proof of the p-adic version of Theorem 4.5, using connections between the chromatic number of Cayley graphs and Diophantine approximation, can be found in [HM14].

Similarly as in the case of the Littlewood conjecture, we can naturally try to establish some sort of measures on the sets of numbers which satisfy the p-adic Littlewood Conjecture. We automatically have that the set of possible counter-examples is a subset of BAD and thus has Lebesgue measure zero. Einsiedler and Kleinbock used the same method as in [EK07] to show that, for any prime $p \in \mathbb{Z}$, the set of real numbers α for which the ordered pair (α, p) satisfy (25) is 'small' (it has Hausdorff dimension zero).

There are also relations between the word obtained from a number α's continued fraction expansion and whether it satisfies the p-adic Littlewood Conjecture; namely, if it contains arbitrarily long periodic parts, it satisfies the p-adic Littlewood Conjecture:

4.10 Theorem ([BDdM07]). *Let the badly approximable number $\alpha \in \mathbb{R}$ be expanded into a continued fraction as $\alpha = [a_1; a_2 \ldots,]$. Let $T \in \mathbb{N}^+$ and let $b_1, \ldots, b_T \in \mathbb{N}^+$. If there exist two sequences $\{m_k\}_{k\geqslant 1}$, $\{h_k\}_{k\geqslant 1}$, $m_k, h_k \in \mathbb{N}^+$, such that $\{h_k\}_{k\geqslant 1}$ is unbounded and also such that, for every $j = 1, \ldots, T$ and every $n = 0 \ldots, h_k - 1$,*

$$a_{m_k+j+nT} = b_j,$$

then for any prime $p \in \mathbb{Z}$, we have that the ordered pair (α, p) satisfies the p-adic Littlewood Conjecture.

We have that 'most' numbers clearly satisfy the p-adic Littlewood Conjecture. In the following chapter, we will investigate a certain special number, and show that it satisfies the p-adic Littlewood conjecture when $p = 2$.

5 Looking at a Potential Counter-example to the 2-adic Littlewood Conjecture

Studying particular cases of a conjecture is useful, because it gives concrete examples, based on which further generalisations and observations about the conjecture can be made. In this section, we will consider a partial case of the p-adic Littlewood conjecture when $p = 2$, and obtain a possible upper bound for the corresponding expression in equation (25). Through this method of construction, we will see that this bound will also be a potential counter-example to the Conjecture, since the expression on the left hand side of (25) will be in some sense 'large' (Corollary 5.12). We will also explore some interesting connections with algebraic combinatorics on words, especially the Thue-Morse word. Finally, we will pose some open problems and give directions for further development.

Obviously, we have that

$$\liminf_{q\to\infty} q|q|_p||q\alpha|| \leqslant \frac{1}{2}$$

for any $\alpha \in \mathbb{R}$ and any prime $p \in \mathbb{N}$. However, there are no known non-trivial upper bounds for the expression on the left hand side of (25), even in the case when $p = 2$. In this section, we will provide such a bound, c, which will be the limit of a decreasing sequence $\{c_n\}_{n\in\mathbb{N}}$; moreover, we have that $c_1 = 1/3 < 1/2$, which makes c a much better upper bound for the expression.

Setting $p = 2$ in the p-adic Littlewood Conjecture, we obtain a more particular case:

5.1 Conjecture (The 2-adic Littlewood Conjecture)**.** *For all $\alpha \in \mathbb{R}$, we have*

$$\liminf_{q\to\infty} q|q|_2||q\alpha|| = 0. \tag{26}$$

For brevity, if $\alpha \in \mathbb{R}$ satisfies equation (26), we will write $2LC(\alpha)$.

A natural step towards proving the 2-adic Littlewood Conjecture would be to find an upper bound for the value of $\liminf_{q\to\infty} q|q|_2||q\alpha||$. In other words, we would want to find some constant $c \geqslant 0$ such that for every $\alpha \in \mathbb{R}$ we have

$$\liminf_{q\to\infty} q|q|_2||q\alpha|| \leqslant c,$$

and moreover make c as small as possible (ideally, equal to zero).

We have that

$$\liminf_{q\to\infty} q|q|_2||q\alpha|| \leqslant \liminf_{n\to\infty} 2^n|2^n|_2||2^n\alpha|| = \liminf_{n\to\infty} ||2^n\alpha||;$$

thus, we could begin by finding an upper bound for the right-hand-side lim inf in the above inequality. We can do this by attempting to find either

$$\gamma = \sup_{\alpha\in\mathbb{R}} \Big\{ \liminf_{n\to\infty} ||2^n\alpha|| \Big\},$$

or finding another (best achievable) upper bound for

$$\liminf_{n\to\infty} ||2^n\alpha||.$$

Let us point out that, if found, this γ could serve another purpose: it could help us find a potential counter-example for the 2-adic Littlewood Conjecture, since for it, $\liminf_{n\to\infty} ||2^n\alpha||$ is as big as possible. If $\gamma = 0$, then the conjecture is true. If $\gamma > 0$, then we might proceed to construct a potential counter-example.

5.2 Definition. Define $T : \mathbb{R}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$ as

$$T(x) := 2x \mod 1.$$

In other words, $T^n(x)$ is multiplication of x by 2^n and mapping back into $[0, 1]$.

5.3 Note. Note that $||T^n(\alpha)|| = ||2^n\alpha||$ for any $n \in \mathbb{N}$ and $\alpha \in \mathbb{R}$. Thus, T does not change the lim inf and we can equivalently be aiming to find

$$\sup_{\alpha\in\mathbb{R}} \{ \liminf_{n\to\infty} ||T^n(\alpha)|| \}.$$

5.1 Definining the Sequence $\{c_n\}_{n\in\mathbb{N}}$

We want to find the set of α such that

$$\liminf_{n\to\infty} ||2^n\alpha|| \geqslant \alpha,$$

for some $\alpha \in [0, 1/2]$. In order to do that, we make the following definition:

5.4 Definition. We define inductively the following sets:

- U_n, the set of $x \in [0, \frac{1}{2}]$ for which $||2^n x|| \geqslant x$;
- $V_n' := \bigcap_{k\leqslant n} U_k$ - the set for which $||2^k x|| \geqslant x$ for all $k \leqslant n$;
- $V_n := \mathrm{cl}(\mathrm{int}(V_n'))$;
- $\alpha_n := \max\{r : r \in V_n\}$.

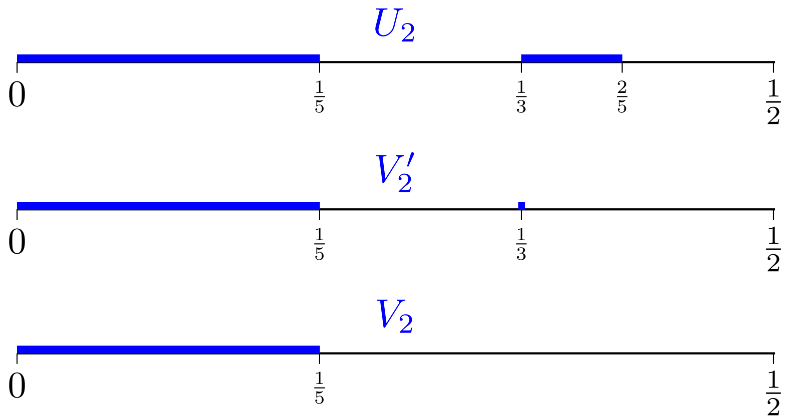
It is easy to check that, for $n \in \mathbb{N}$, we have

$$\alpha_n := \sup_{\alpha\in\mathbb{R}} \{ \inf_{k=1,\dots,n} ||T^k(\alpha)|| \},$$

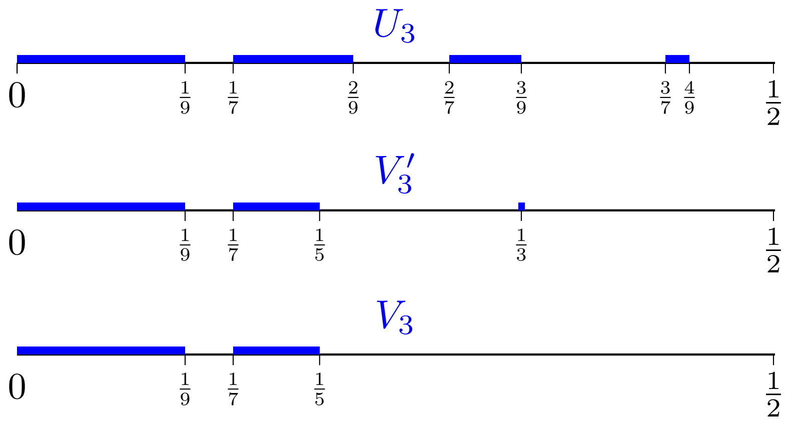
thus again linking the α_n to the function T defined earlier.

V_n' has some isolated points, and thus we need to take V_n to remove all those isolated points. For example:

5.5 Example. We have that $U_1 = [0, 1/3] = V_1$, $U_2 = [0, 1/5] \cup [1/3, 2/5]$ and respectively $V_2 = [0, 1/5]$.



For $n = 3$, we have:



5.6 Proposition. *The sets U_n are unions of the following intervals:*

$$U_n = \bigcup_{0 \leqslant i < 2^{n-1}} \left[\frac{i}{2^n - 1}, \frac{i+1}{2^n + 1} \right]$$

Indeed, we can easily see that for small n, we have

$$U_1 = \bigcup_{0 \leqslant i < 1} \left[\frac{i}{1}, \frac{i+1}{3} \right] = \left[0, \frac{1}{3} \right]$$

$$U_2 = \bigcup_{0 \leqslant i < 2} \left[\frac{i}{3}, \frac{i+1}{5} \right] = \left[0, \frac{1}{5} \right] \cup \left[\frac{1}{3}, \frac{2}{5} \right]$$

$$U_3 = \bigcup_{0 \leqslant i < 3} \left[\frac{i}{7}, \frac{i+1}{9} \right] = \left[0, \frac{1}{9} \right] \cup \left[\frac{1}{7}, \frac{2}{9} \right] \cup \left[\frac{2}{7}, \frac{3}{9} \right] \cup \left[\frac{3}{7}, \frac{4}{9} \right].$$

Proof. For the inclusion $U_n \subseteq \bigcup_{0\leqslant i<2^{n-1}} \left[\frac{i}{2^n-1}, \frac{i+1}{2^n+1}\right]$, we have that $x \in U_n$ if and only if $||2^n x|| \geqslant x$. Now, let $k \geqslant 0$ be the unique integer such that $k \leqslant 2^n x < k+1$. Note that since $x \leqslant 1/2$, then immediately we have $k \leqslant 2^{n-1}$. Also,

$$\min\{2^n x - k, k+1-2^n x\} \geqslant x.$$

Representing this as a system of two inequalities, we get that

$$\begin{aligned} 2^n x - k &\geqslant x \\ k+1-2^n x &\geqslant x; \end{aligned}$$

which can be solved as

$$\begin{aligned} x &\geqslant \frac{k}{2^n-1} \\ x &\leqslant \frac{k+1}{2^n+1}, \end{aligned}$$

in other words,

$$x \in \left[\frac{k}{2^n-1}, \frac{k+1}{2^n+1}\right] \subset \bigcup_{0\leqslant i<2^{n-1}} \left[\frac{i}{2^n-1}, \frac{i+1}{2^n+1}\right],$$

as required.

For the reverse inclusion, we have

$$x \in \bigcup_{0\leqslant i<2^{n-1}} \left[\frac{i}{2^n-1}, \frac{i+1}{2^n+1}\right]$$

if and only if there is an integer k, $0 \leqslant k < n$, such that

$$x \in \left[\frac{k}{2^n-1}, \frac{k+1}{2^n+1}\right].$$

Note in particular, $x \leqslant \frac{k+1}{2^n+1}$.

Then

$$\begin{aligned} 2^n x &\in \left[\frac{2^n k}{2^n-1}, \frac{2^n(k+1)}{2^n+1}\right] \\ &= \left[k + \frac{k}{2^n-1}, k+1-\frac{k+1}{2^n+1}\right], \end{aligned}$$

and thus

$$||2^n x|| > \max\left\{\frac{k}{2^n-1}, \frac{k+1}{2^n+1}\right\} = \frac{k+1}{2^n+1} \geqslant x,$$

in other words, $||2^n x|| \geqslant x$, so $x \in U_n$ as required. This completes the proof. □

We would ideally like to give a formula for the α_n, or at least an upper bound, for each n. We give an upper bound through the following definition and Theorem 5.9.

5.7 Definition. We define the sequence $\{c_n\}_{n\in\mathbb{N}}$ of rational numbers by setting $c_0 = \frac{1}{3}$, and for $n \in \mathbb{N}^+$, setting

$$c_n = \frac{\prod_{i=0}^{n-1}\left(2^{2^i}-1\right)}{2^{2^n}+1}.$$

We begin with the following observation:

5.8 Proposition. *The sequence $\{c_n\}_{n\in\mathbb{N}}$ defined above is a strictly decreasing sequence of positive numbers, hence convergent.*

Proof. For all $n \in \mathbb{N}$, it is obvious that $c_n > 0$. To check the sequence is strictly decreasing, we note that

$$c_{n+1} = \frac{\left(2^{2^n}+1\right)\left(2^{2^n}-1\right)\prod_{j=0}^{n-1}\left(2^{2^j}-1\right)}{\left(2^{2^{n+1}}+1\right)\left(2^{2^n}+1\right)} = c_n\frac{2^{2^{n+1}}-1}{2^{2^{n+1}}+1},$$

where the fraction on the right-hand side is always positive and strictly less than 1. □

5.9 Theorem. *For all $n \in \mathbb{N}$ and for all $m \in \{0, 1, \ldots, 2^n - 1\}$, we have that*

$$c_n > \alpha_{2^n+m}.$$

In other words, c_n is an upper bound for the respective α_{2^n+m}.

Proof. We use induction on n.

Base case: We already have computed that $\alpha_1 = 1/3 = c_0$, and so $\alpha_1 \leqslant c_0$, as required. Similarly, one could also compute $\alpha_2 = 1/5 = c_1$, and thus check that indeed, $\alpha_2 \leqslant c_1$.

Inductive step: Assume that for some $n \in \mathbb{N}^+$ and for all $m \in \{0, 1, \ldots, 2^n - 1\}$, we have

$$c_n > \alpha_{2^n+m}.$$

By Definition 5.4 of α_n, this means that c_n is an upper bound for V_{2^n+m} for all $m \in \{0, 1, \ldots, 2^n - 1\}$. For brevity, write $P(n) = \prod_{i=0}^{n-1}\left(2^{2^i}-1\right)$. Note that

$$c_n = \frac{P(n)}{2^{2^n}+1} = \frac{P(n+1)}{2^{2^{n+1}}-1},$$

and thus the single point $\{c_n\}$ is the intersection of the two intervals

$$I_0 = \left[\frac{P(n)-1}{2^{2^n}-1}, \frac{P(n)}{2^{2^n}+1}\right], \text{ and}$$
$$I_1 = \left[\frac{P(n+1)}{2^{2^{n+1}}-1}, \frac{P(n+1)+1}{2^{2^{n+1}}+1}\right].$$

By Proposition 5.6, we have that $I_0 \subset U_{2^n}$ and $I_1 \subset U_{2^{n+1}}$. Thus, c_n is an isolated point of $U_{2^n} \cap U_{2^{n+1}}$ and is therefore not an element of $V_{2^{n+1}}$, by Definition 5.4 of V_n. We note that the interval of $U_{2^{n+1}}$ which immediately precedes I_1 is

$$\left[\frac{P(n+1)-1}{2^{2^{n+1}}-1}, \frac{P(n+1)}{2^{2^{n+1}}+1}\right] = \left[\frac{P(n+1)-1}{2^{2^{n+1}}-1}, c_{n+1}\right].$$

Combining this with the inductive hypothesis that c_n was an upper bound for V_{2^n}, and with the structure of U_n given by Proposition 5.6, we obtain that c_{n+1} is an upper bound for $V_{2^{n+1}}$, as required. □

Besides being upper bounds for the α_n's, the numbers c_n are also interesting in the following sense - for certain values of k, the expression $||kc_n||$ is 'relatively large':

5.10 Theorem. *For all $q, n \in \mathbb{N}$, we have*

$$||2^q c_n|| \geqslant c_n.$$

Proof. For brevity, we again write $P(n) = \prod_{i=0}^{n}\left(2^{2^i}-1\right)$. We begin with the following observation about the values of $||2^m c_n||$, for $m \in \mathbb{N}$. First, since $P(n)$ is an integer, we note that $||2^m P(n) - x|| = ||x||$, for any $x \in \mathbb{R}$, for any $n, m \in \mathbb{N}$.

Let $m \in \mathbb{N}$ be arbitrary but fixed. We note that

$$\begin{aligned} ||2^{2^n+m} c_n|| &= \left|\left|\frac{2^{2^n} 2^m P(n)}{2^{2^n}+1}\right|\right| \\ &= \left|\left|2^m P(n) - \frac{2^m P(n)}{2^{2^n}+1}\right|\right| \\ &= \left|\left|\frac{2^m P(n)}{2^{2^n}+1}\right|\right| \\ &= ||2^m c_n||. \end{aligned}$$

Thus, the expression $||2^m c_n||$ is periodic, can take only finitely many values for $m \in \mathbb{N}$, and moreover, $||2^m c_n||$ takes at most 2^n distinct values. Therefore, it is sufficient to show that for all $n \in \mathbb{N}$,

$$\begin{aligned} ||c_n|| &\geqslant c_n, \\ ||2c_n|| &\geqslant c_n, \\ &\vdots \\ ||2^n c_n|| &\geqslant c_n. \end{aligned}$$

We do this by induction on n.

Base case: For $n = 0$, we have $||c_0|| = 1/3 \geqslant 1/3 = c_0$, as required. Moreover, we can check that $||2c_0|| = 1/3 \geqslant c_0$, as well, and that since $0 < c_n \leqslant 1/3$, we have that for all $n \in \mathbb{N}$, $||2c_n|| \geqslant c_n$.

Inductive step: Assume that for some $n \in \mathbb{N}$, we have that for all $m = 0, \ldots, n$,

$$||2^m c_n|| \geqslant c_n.$$

We want to show that for $n+1$ and $m = 0, \ldots, n+1$, we also have that

$$||2^m c_{n+1}|| \geqslant c_{n+1}.$$

We first calculate

$$c_n - c_{n+1} = \frac{2c_n}{2^{2^{n+1}} + 1}.$$

Thus, for $m = 0, \ldots, n$, we have

$$\begin{aligned} ||2^m c_{n+1}|| &= \left|\left| 2^m c_n - \frac{2^{m+1} c_n}{2^{2^{n+1}} + 1} \right|\right| && \text{and by Proposition 2.3,} \\ &\geqslant ||2^n c_{n+1}|| - \left|\left| \frac{2^{m+1} c_n}{2^{2^{n+1}} + 1} \right|\right| && \text{and by the Inductive Hypothesis,} \\ &\geqslant c_n - \left|\left| \frac{2^{m+1} c_n}{2^{2^{n+1}} + 1} \right|\right| && \text{and since } 0 < c_n < 1/2 \text{ and } 0 < \frac{2}{2^{2^{n+1}} + 1} < 1, \\ &= c_n - \frac{2\,||2^m c_n||}{2^{2^{n+1}} + 1} && \text{and again applying the Inductive Hypothesis,} \\ &\geqslant c_n - \frac{2c_n}{2^{2^{n+1}} + 1} && \text{which, by the previous calculations, is just} \\ &= c_{n+1} \end{aligned}$$

Now all we need to complete the induction is to show that $||2^{n+1} c_{n+1}|| \geqslant c_{n+1}$. Indeed, we have

$$\begin{aligned}
\left|\left|2^{n+1}c_{n+1}\right|\right| &= \left|\left|2^{n+1}c_n\right|\right| - \left|\left|\frac{2^{n+2}c_n}{2^{2^{n+1}}+1}\right|\right| && \text{and since } ||2^n c_n|| \text{ has period } 2^n, \\
&= ||2c_n|| - \left|\left|\frac{2^{n+2}c_n}{2^{2^{n+1}}+1}\right|\right| && \text{by the Inductive Hypothesis,} \\
&\geqslant c_n - \frac{2\,||2^{n+1}c_n||}{2^{2^{n+1}}+1} && \text{and as previously,} \\
&\geqslant c_n - \frac{2c_n}{2^{2^{n+1}}+1} = c_{n+1}.
\end{aligned}$$

This completes the proof.

□

We have in fact shown that

5.11 Corollary (to Theorem 5.10). *For all $n \in \mathbb{N}$,*

$$c_n \in \bigcap_{k=0,\ldots,n} U_k.$$

We have also shown that,

5.12 Corollary (to Theorem 5.10). *For all $n \in \mathbb{N}$,*

$$\liminf_{q\to\infty} ||2^q c_n|| = c_n.$$

Proof. Let $n \in \mathbb{N}$ be arbitrary but fixed. Theorem 5.10 gives us that

$$\liminf_{q\to\infty} ||2^q c_n|| \geqslant c_n, \tag{27}$$

since all of the elements of the sequence $\{||2^q c_n||\}_{q\in\mathbb{N}}$ are greater than or equal to c_n. To show that in fact we have equality, we note that in the proof of Theorem 5.10, we showed that $||2^{2^n+m}c_n|| = ||2^m c_n||$. Setting $m = 0$, we obtain that $||2^{2^n}c_n|| = ||c_n|| = c_n$. Thus, the subsequence $\left\{||2^{2^q}c_n||\right\}_{q\in\mathbb{N}}$ is the constant sequence $\{c_n\}_{q\in\mathbb{N}}$, so

$$\lim_{q\to\infty} \left|\left|2^{2^q}c_n\right|\right| = c_n.$$

Thus, we have shown that in fact, we have equality in (27), as required. □

5.13 Corollary. *For all $n \in \mathbb{N}$,*

$$\liminf_{q\to\infty} q|q|_2||qc_n|| \leqslant c_n.$$

Proof. Let $n \in \mathbb{N}$ be arbitrary but fixed. From Corollary 5.12, we have that

$$\liminf_{q\to\infty} q|q|_2||qc_n|| \leqslant \liminf_{m\to\infty} 2^m|2^m|_2||2^m c_n|| = \liminf_{m\to\infty} ||2^m c_n|| = c_n,$$

as required. □

Recalling Definition 3.12 of near-prefix, we observe an interesting pattern: the word $\mathbf{w}(c_n)$ obtained from the expansion of c_n (sans c_0) into a continued fraction is in fact a near-prefix of order 1 of $\mathbf{w}(c_{n+1})$. Slightly abusing notation, we can see this for small n:

$$\begin{aligned}
c_1 &= \frac{1}{5} = [0; 5] \\
c_2 &= \frac{3}{17} = [0; 5, 1, 2] \\
c_3 &= \frac{45}{257} = [0; 5, 1, 2, 2, 6] \\
c_4 &= \frac{11475}{65537} = [0; 5, 1, 2, 2, 6, 2, 1, 2, 9, 1, 2] \\
c_5 &= [0; 5, 1, 2, 2, 6, 2, 1, 2, 9, 1, 2, 2, 1, 1, 21, 1, 10, 2, 1, 1, 1, 5] \\
c_6 &= [0; 5, 1, 2, 2, 6, 2, 1, 2, 9, 1, 2, 2, 1, 1, 21, 1, 10, 2, 1, 1, 1, \mathit{4}, \mathit{1}, 2, 29, 1, 24, 1, 1, 7, 11, 3, 2, \\
&\qquad 5, 1, 1, 1, 89] \\
c_7 &= [\mathbf{w}(c_6) - \text{last letter of } c_6 + 88, 1, 1, 1, 6, 1, 1, 33, 2, 6, 1, 24, 1, 5, 212, 2, 1, 10, 1, 3, \\
&\qquad 11, 2, 1, 2, 1, 10, 11, 2, 3, 2549, 1, 2]
\end{aligned}$$

If we can prove this property, it would justify studying the properties of the continued fraction expansion of the limit c through studying the continued fraction expansions of the c_n. We indirectly do this by using Proposition 2.19, and showing that for all $n \in \mathbb{N}$, c_n is a convergent of c_{n+1}:

5.14 Proposition. *For each $n \in \mathbb{N}$, c_n is a convergent in the continued fraction expansion of c_{n+1}.*

In particular, this means that, with some trivial exceptions, the word obtained from the continued fraction expansion of c_n is a prefix of the word obtained from the continued fraction expansion of c_{n+1}, as required.

Proof. Recall that

$$c_n = \frac{\prod_{j=0}^{n-1}\left(2^{2^j} - 1\right)}{2^{2^n} + 1}.$$

We prove, by induction on n, that the inequality from Proposition 2.19 holds for c_n and c_{n+1}; in other words, that for all $n \in \mathbb{N}$, c_n is a convergent of c_{n+1}.

We first rewrite the inequality which we wish to verify:

$$
\begin{aligned}
\left|\frac{\prod_{j=0}^{n-1}\left(2^{2^j}-1\right)}{2^{2^n}+1}-\frac{\prod_{j=0}^{n}\left(2^{2^j}-1\right)}{2^{2^{n+1}}+1}\right| &< \frac{1}{2\left(2^{2^n}+1\right)^2} \Leftrightarrow \\
\left|\frac{\left(2^{2^{n+1}}+1\right)\prod_{j=0}^{n-1}\left(2^{2^j}-1\right)-\left(2^{2^n}+1\right)\prod_{j=0}^{n}\left(2^{2^j}-1\right)}{\left(2^{2^n}+1\right)\left(2^{2^{n+1}}+1\right)}\right| &< \frac{1}{2\left(2^{2^n}+1\right)^2} \Leftrightarrow \\
\left|\frac{2\prod_{j=0}^{n-1}\left(2^{2^j}-1\right)}{\left(2^{2^{n+1}}+1\right)\left(2^{2^n}+1\right)}\right| &< \frac{1}{2\left(2^{2^n}+1\right)^2} \Leftrightarrow \\
\left|\frac{4\prod_{j=0}^{n-1}\left(2^{2^j}-1\right)}{2^{2^{n+1}}+1}\right| &< \frac{1}{2^{2^n}+1} \Leftrightarrow \\
\frac{4\left(2^{2^n}+1\right)\prod_{j=0}^{n-1}\left(2^{2^j}-1\right)}{2^{2^{n+1}}+1} &< 1,
\end{aligned}
$$

noting that we may omit the modulus symbol in the last line, since the expression inside is positive.

We will show this by induction on $n \in \mathbb{N}$. Since c_0 is not a convergent of c_1, the base case for our induction will begin at $n = 2$.

Base case: We check that the inequality holds for $n = 2$; indeed, it becomes

$$\frac{204}{257} < 1,$$

which is correct.

Inductive step: Assume that, for $n \geqslant 2$, $n \in \mathbb{N}$, the following inequality holds:

$$\frac{4\left(2^{2^n}+1\right)\prod_{j=0}^{n-1}\left(2^{2^j}-1\right)}{2^{2^{n+1}}+1} < 1. \tag{28}$$

For $n+1$, we have

$$\begin{aligned}
&\frac{4\left(2^{2^{n+1}}+1\right)\prod_{j=0}^{n}\left(2^{2^j}-1\right)}{2^{2^{n+2}}+1} = \\
&= \frac{4\left(2^{2^n}+1\right)\prod_{j=0}^{n-1}\left(2^{2^j}-1\right)}{2^{2^{n+1}}+1}\frac{\left(2^{2^{n+1}}+1\right)^2\left(2^{2^n}-1\right)}{\left(2^{2^n}+1\right)\left(2^{2^{n+2}}+1\right)} < \text{ by IH} \\
&< \frac{\left(2^{2^{n+1}}+1\right)^2\left(2^{2^n}-1\right)}{\left(2^{2^n}+1\right)\left(2^{2^{n+2}}+1\right)} =: f(n)
\end{aligned}$$

If we set $2^{2^n} = x$, we get $2^{2^{n+1}} = 2^{2^n 2} = x^2$ and $2^{2^{n+2}} = 2^{2^n 2^2} = x^4$, and thus $f(n)$ can be rewritten as

$$g(x) := \frac{\left(x^2+1\right)^2(x-1)}{(x+1)(x^4+1)},$$

where we note $f : \mathbb{N} \to \mathbb{R}$, $g : \mathbb{R} \to \mathbb{R}$, and $f = g|_{\mathbb{N}}$, in other words, the function f is the restriction of g to the natural numbers.

Note that, by analysis,

$$\lim_{x\to\infty} g(x) = 1.$$

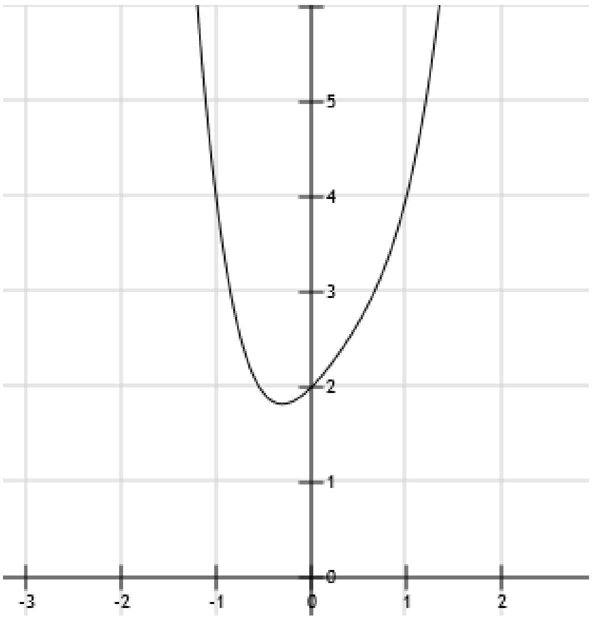
We can directly show that $g(x) < 1$ by expanding out the brackets and noting that the denominator is always $\geqslant 0$ for positive values of the variable x:

$$x^5 - x^4 + 2x^3 - 2x^2 + x - 1 < x^5 + x^4 + x + 1.$$

It is easy to check (by looking at first and second derivatives and plotting the functions) that for all $x \in \mathbb{R}$,

$$\begin{aligned}
&-x^4 + 2x^3 - 2x^2 + x - 1 < x^4 + x + 1 \iff \\
&0 < x^4 - x^3 + x^2 + x + 2.
\end{aligned}$$

The polynomial on the right-hand side of the inequality above is plotted below:



Therefore, we have the required inequality, which completes the inductive step. $\square$

5.15 Corollary. *The constant* $c = \lim_{n\to\infty} c_n$ *is irrational.*

Proof. By the previous proposition, the lengths of the continued fraction expansions of the c_n's form a monotone increasing sequence. By Theorem 2.15, any number with an infinite continued fraction expansion is irrational. $\square$

5.16 Corollary. *The rationals* $\{c_n\}_{n\in\mathbb{N}}$ *are odd convergents of* c.

Proof. This follows from Theorem 2.14 and the fact that, by Proposition 5.8, the $\{c_n\}_{n\in\mathbb{N}}$ is a strictly decreasing sequence. $\square$

We want to check whether c satisfies the 2-adic Littlewood Conjecture; moreover, we constructed c as a possible counter-example to the conjecture. In view of the fact that the set of possible counterexamples to the 2-adic Littlewood Conjecture is a subset of the badly approximable numbers, it is sensible to ask:

1 Question. Is the constant c badly approximable?

One might try to show that c is badly approximable by considering certain subsequences of convergents of its continued fraction expansion. Unfortunately, the sequence $\{c_n\}_{n\in\mathbb{N}}$ is not 'sufficient' to show that the 2-adic Littlewood Conjecture holds for c. Intuitively speaking, the current approximations c_n are not good enough for this purpose, since they do not contain large powers of 2 in their denominators. Thus, we adopt a new approach.

We look at a given function and some rational approximations of it which have certain 'helpful' properties. First, we need to translate our problem about the sequence $\{c_n\}_{n\in\mathbb{N}}$ and its limit, c, into a problem about some functions, which are appropriately defined.

5.17 Theorem. *Define a sequence of functions* $f_n : (1, +\infty) \to \mathbb{R}$ *by*

$$f_n(t) = \frac{\prod_{k=0}^{n-1}(t^{2^k} - 1)}{t^{2^n} + 1},$$

and define the function $f : (1, +\infty) \to \mathbb{R}$ *by*

$$f(t) = \lim_{n\to\infty} f_n(t).$$

Moreover, for any $n \in \mathbb{N}$, $c_n = f_n(2)$, *and also* $c = f(2)$.

Proof. Obviously, we have that

$$c_n = \frac{\prod_{k=0}^{n-1}(2^{2^k} - 1)}{2^{2^n} + 1},$$

are evaluations at the point $t = 2$ of the sequence of functions f_n,

$$f_n(t) = \frac{\prod_{k=0}^{n-1}(t^{2^k} - 1)}{t^{2^n} + 1}.$$

By real analysis, we can take the pointwise limit of the sequence of functions $\{f_n\}_{n\in\mathbb{N}}$:

$$\begin{aligned}
\lim_{n\to\infty} f_n(t) &= \lim_{n\to\infty} \frac{\prod_{k=0}^{n-1}(t^{2^k} - 1)}{t^{2^n} + 1} \\
&= \lim_{n\to\infty} \frac{t^{2^{n-1}}(1 - t^{-2^{n-1}})\prod_{k=0}^{n-2}(t^{2^k} - 1)}{t^{2^n}(1 + t^{-2^n})} \\
&= \lim_{n\to\infty} \frac{t^{2^{n-1}}(1 - t^{-2^{n-1}})\prod_{k=0}^{n-2}(t^{2^k} - 1)}{\left(t^{2^{n-1}}\right)^2(1 + t^{-2^n})} \\
&= \lim_{n\to\infty} \frac{(1 - t^{-2^{n-1}})\prod_{k=0}^{n-2}(t^{2^k} - 1)}{t^{2^{n-1}}(1 + t^{-2^n})}.
\end{aligned}$$

Continuing in this way, we obtain

$$\lim_{n\to\infty} f_n(t) = \lim_{n\to\infty} \frac{\prod_{k=0}^{n-1}\left(1 - t^{-2^k}\right)}{t\,(1 + t^{-2^n})}.$$

We define

$$f(t) = \lim_{n\to\infty} f_n(t).$$

Thus,

$$f(t) = \frac{\prod_{k=0}^{\infty}\left(1 - t^{-2^k}\right)}{t},$$

Thus, we obtain pointwise convergence of $\{f_n\}_{n\in\mathbb{N}}$ to f.

Finally, it is obvious that $c = f(2)$. □

In order to justify the study of f, we also want to show that f is not the zero function - that its product is indeed convergent. For this, we need some preliminary theorems.

5.18 Theorem. *The sequence* $\left\{\prod_{n=1}^{N}\left(1 - t^{-2^n}\right)\right\}_{N\in\mathbb{N}}$ *is monotone decreasing.*

Proof. Note that,

$$x_n = x_{n-1}\left(1 - t^{-2^n}\right),$$

where $\left(1 - t^{-2^n}\right)$ is strictly less than 1 for positive values of t (which are the only ones for which we are considering this sequence). □

5.19 Theorem. *The formal product*

$$\prod_{k=0}^{\infty}\left(1 - t^{-2^k}\right)$$

converges to a non-zero limit, for all $t > 1$.

Proof. By Theorem 1.12, we have that

$$\prod_{k=0}^{\infty}\left(1 - t^{-2^k}\right)$$

converges iff

$$\sum_{k=0}^{\infty}\ln\left(1 - t^{-2^k}\right)$$

converges. Note that, for $|t| > 1$,

$$\lim_{k\to\infty}(1 - \frac{1}{t^{2^k}}) = 1.$$

Since the logarithm function is continuous on $(0, \infty]$, we can conclude that

$$\lim_{k\to\infty}\ln\left(1 - \frac{1}{t^{2^k}}\right) = \ln(1) = 0.$$

We want to show that

$$\lim_{k\to\infty}\sqrt[k]{\left|\ln\left(1 - \frac{1}{t^{2^k}}\right)\right|} = 0 < 1.$$

so we can use the n-th root test (Theorem 1.11) to conclude that the product is indeed convergent and non-zero. Now, since for $t > 1$, we have $\ln(1 - t^{-2^k}) < 0$, so

$$\begin{aligned}\lim_{k\to\infty}\left|\ln\left(1-\frac{1}{t^{2^k}}\right)\right|^{\frac{1}{k}} &= \lim_{k\to\infty}\left(-\ln\left(1-\frac{1}{t^{2^k}}\right)\right)^{\frac{1}{k}} \\ &= \lim_{k\to\infty}\left(\ln\left(\frac{t^{2^k}}{t^{2^k}-1}\right)\right)^{\frac{1}{k}}. \qquad (29)\end{aligned}$$

Note this limit is of the sort '0^0', so we will need to use l'Hôpital's rule (Theorem 1.10), noting that, for functions $\phi(x), \psi(x)$ which tend to 0 as $x \to \infty$,

$$\lim_{x\to\infty}\phi(x)^{\psi(x)} = \lim_{x\to\infty} e^{\psi(x)\ln\phi(x)}.$$

We set

$$\begin{aligned}\phi(k) &= \ln\frac{t^{2^k}}{t^{2^k}-1} \\ \psi(k) &= \frac{1}{x},\end{aligned}$$

and first try to find $\lim_{k\to\infty}\psi(k)\ln\phi(k)$, again applying l'Hôpital's rule

$$\begin{aligned}\lim_{k\to\infty}\frac{1}{x}\ln\left(\ln\frac{t^{2^k}}{t^{2^k}-1}\right) &= -\ln 2\ln t\lim_{k\to\infty}\frac{2^k}{\left(t^{2^k}-1\right)\ln\frac{t^{2^k}}{t^{2^k}-1}} \\ &= -\ln 2\ln t\lim_{u\to\infty}\frac{u}{(t^u-1)\ln\frac{t^u}{t^u-1}}, \qquad (30)\end{aligned}$$

if we set $2^k = u$ and note that $k \to \infty$ implies $u \to \infty$. Let us first calculate the denominator of (30),

$$\begin{aligned}\lim_{u\to\infty}(t^u-1)\ln\frac{t^u}{t^u-1} &= \lim_{u\to\infty}(t^u-1)\ln\left(1+\frac{1}{t^u-1}\right) && \text{setting } w = t^u-1 \\ &= \lim_{w\to\infty} w\ln\left(1+\frac{1}{w}\right) && \text{setting } s = \frac{1}{w} \\ &= \lim_{s\to 0}\frac{\ln(1+s)}{s} && \text{finally, applying l'Hôpital} \\ &= \lim_{s\to 0}\frac{1}{1+s} \\ &= 1\end{aligned}$$

Thus, the expression in equation (30) becomes

$$(30) = -\ln 2 \ln t \lim_{u\to\infty} \frac{u}{1} = -\infty;$$

and so the original limit (29) becomes

$$\lim_{k\to\infty} \left(\ln \frac{t^{2^k}}{t^{2^k}-1} \right)^{\frac{1}{k}} = e^{-\infty} = 0 < 1,$$

and so we can successfully apply the nth root test to conclude that our product is convergent and non-zero. □

Thus, we are justified in studying $f(t)$ and some special approximations of it. To facilitate the process, we will first re-write $f(t)$ in terms of a power series. We first need to guarantee that the tail of the product in f does not 'change too much' the value of f.

5.20 Proposition. *We have that*

$$\lim_{l\to\infty} \prod_{n=l+1}^{\infty} (1 - t^{-2^n}) = 1,$$

for $t > 1$.

Proof. This is in fact a straightforward corollary to Theorem 5.18, since here we are considering the tail of an infinite product which converges to a positive number. □

Now, we are ready for the transformation of f into a power series.

5.21 Theorem. *We have that*

$$f(t) = \sum_{n\in\mathbb{N}} (-1)^{2^{\theta_n}} t^{-n}, \tag{31}$$

where $\theta_n = 1 - \sigma_n$, and σ_n is the nth letter of the Thue-Morse word.

5.22 Note. After formulating and proving Theorem 5.21, the author of this dissertation found this Theorem stated in [AS99], but without proof.

Proof. By Theorem 5.19 and Proposition 5.20, we are justified in expanding out $f(t)$ as follows:

$$
\begin{aligned}
f(t) &= \frac{1}{t}\prod_{k=0}^{\infty}(1-t^{-2^k}) \\
&= \frac{1}{t}(1-t^{-2^0})(1-t^{-2^1})(1-t^{-2^2})(1-t^{-2^3})\dots \\
&= (t^{-1}-t^{-2})(1-t^{-2^1})(1-t^{-2^2})(1-t^{-2^3})\prod_{k=4}^{\infty}(1-t^{-2^k}) \\
&= (t^{-1}-t^{-2}-t^{-3}+t^{-4})(1-t^{-2^2})(1-t^{-2^3})\prod_{k=4}^{\infty}(1-t^{-2^k}). \qquad (32)
\end{aligned}
$$

Each time we have an expression of the form

$$\phi(m,t) = a_1 t^{-1} + a_2 t^{-2} + \ldots + a_{2^m} t^{-2^m}$$

which we multiply by $(1-t^{-2^m})$ to obtain:

$$\psi(m+1,t) := \phi(m,t)(1-t^{-2^m}) = \phi(m,t) - t^{-2^m}\phi(m,t).$$

Thus, we have that the word $\mathbf{u}(m) = a_1 \dots a_{2^m}$ obtained from the coefficients of the expression $\phi(m,t)$ is a prefix of the word $\mathbf{u}(m+1) = a_1 \dots a_{2^m} \dots a_{2^{m+1}}$, obtained from the coefficients of the expression $\psi(m+1,t)$. Moreover, by Note 3.28 and the fact that $a_1 = (-1)^{2^1}$ and $a_2 = (-1)^{2^0}$, we have that indeed, the powers of 2 in the exponents of (-1), which we denote by θ_n, are obtained from the complements of the letters of the Thue-Morse word. More precisely, if σ_n is the n-th letter of the Thue-Morse word, then $\theta_n = 1 - \sigma_n = \underline{\sigma_n}$ (we remind the reader that the underline means that all the 0's are changed to 1's and vice-versa). Thus, we have that

$$
\begin{aligned}
(32) &= (-1)^{2^1}t^{-1} + (-1)^{2^0}t^{-2} + (-1)^{2^0}t^{-3} + (-1)^{2^1}t^{-4} + (-1)^{2^0}t^{-5} + \ldots \\
&= \sum_{n\in\mathbb{N}}(-1)^{2^{\theta_n}}t^{-n},, \qquad (33)
\end{aligned}
$$

which completes the proof. □

We continue with a theorem which will be central to our further investigations, especially in finding two sequences of functions which provide sufficiently good approximations to our function f.

5.23 Theorem. *The function f satisfies the following functional equation:*

$$f(t^2) = \frac{1}{1-t}f(t). \qquad (34)$$

Proof. To check that this is indeed so, we replace t by t^2, and obtain

$$\begin{aligned} f(t^2) &= \frac{1}{t^2}\prod_{k=0}^{\infty}\left(1-t^{-2^{k+1}}\right) \\ &= t^{-2}(1-t^{-2})(1-t^{-2^2})(1-t^{-2^3})\dots . \end{aligned}$$

Also,

$$\begin{aligned} f(t) &= \frac{1}{t}\prod_{k=0}^{\infty}\left(1-t^{-2^{k}}\right) \\ &= t^{-1}(1-t^{-1})(1-t^{-2})(1-t^{-2^2})(1-t^{-2^3})\dots . \end{aligned}$$

If we set

$$A(t) = (1-t^{-2})(1-t^{-2^2})(1-t^{-2^3})\dots = \prod_{k=1}^{\infty}(1-t^{-2^k}),$$

then we have

$$\begin{aligned} f(t^2) &= \frac{1}{t^2}A(t), \\ f(t) &= \frac{1}{t}\left(1-\frac{1}{t}\right)A(t). \end{aligned}$$

From the second equation, we obtain

$$A(t) = \frac{tf(t)}{1-\frac{1}{t}} = \frac{t^2f(t)}{t-1},$$

and substituting in the first,

$$f(t^2) = \frac{1}{t^2}A(t) = \frac{f(t)}{t-1},$$

as required. □

We want to find a "nice" rational approximation to $f(t)$, and we begin with a rational approximant with numerator and denominator both linear functions. To be more precise in what we mean by "nice", we introduce the following definition:

5.24 Definition (nice approximation to $f(t)$)**.** Let $n \in \mathbb{N}^+$ and let $\phi_n(t)/\psi_n(t)$ be a rational function with polynomial numerator and denominator both of degree at most n; in other words, $\phi_n(t), \psi_n(t) \in \mathbb{Z}[t]$, and $\deg(\phi_n), \deg(\psi_n) \leqslant n$. To say that $\phi_n(t)/\psi_n(t)$ is a *nice approximation to* $f(t)$, we mean that as many as possible large powers of the variable t become zero in the following expression:

$$\left| f(t) - \frac{\phi_n(t)}{\psi_n(t)} \right| ; \tag{35}$$

in other words, for any other $\phi_n^*(t), \psi_n^*(t) \in \mathbb{Z}[t]$ with $\deg(\phi_n^*), \deg(\psi_n^*) \leqslant n$, we have

$$\deg\left(f(t) - \frac{\phi_n(t)}{\psi_n(t)} \right) < \deg\left(f(t) - \frac{\phi_n^*(t)}{\psi_n^*(t)} \right).$$

Here, by degree of the expression (35), we mean the first non-zero term in the expansion. Moreover, we take as canonical the choice of ϕ_n, ψ_n with a leading coefficient of 1.

5.25 Proposition. *The following rational function*

$$\frac{1}{t+1}$$

is a nice approximation to $f(t)$*.*

Proof. To do this, we calculate the corresponding expression in (35), where we write $\phi_n(t) = a_1 t + a_0$ and $\psi_n(t) = b_1 t + b_0$:

$$\begin{aligned} &|b_1 t f(t) + b_0 f(t) - a_1 t - a_0| = \\ &| - a_1 t + (b_1 - a_0) + (b_0 - b_1)t^{-1} + (-b_0 - b_1)t^{-2} + (-b_0 + b_1)t^{-3} + \dots | \end{aligned} \tag{36}$$

and set as many coefficients as possible $= 0$ to get

$$\begin{aligned} a_1 &= 0 \\ b_1 - a_0 &= 0 \\ b_0 - b_1 &= 0. \end{aligned}$$

Solving the system of linear equations gives us

$$\begin{aligned} b_0 &= a_0 \\ b_1 &= a_0, \end{aligned}$$

and thus

$$\frac{a_1 t + a_0}{b_1 t + b_0} = \frac{1}{t+1}.$$

Thus, if we wanted $p_0(t), q_0(t) \in \mathbb{Z}[t]$ of degree at most 1 such that

$$\left| f(t) - \frac{p_0(t)}{q_0(t)} \right|$$

has as small a degree as possible, then the minimal solution would be $p_0(t) = 1$ and $q_0(t) = t + 1$.

Note that, plugging our values for the a_i and b_i, we get that the first term with a nonzero coefficient in equation (36) would be t^{-2}.

Now, combining equations (36) and (31), we get that

$$\left| f(t) - \frac{1}{t+1} \right| = \left| -2t^{-2} + 2t^{-6} - 2t^{-8} + \ldots \right| .$$

□

5.26 Proposition. *The following rational function*

$$\frac{t^2 - 2}{t^3 + t^2}$$

is a nice approximation of $f(t)$ with degree (at most) 3.

Proof. If we wanted to approximate $f(t)$ by a rational function with numerator $\phi_3(t)$ and denominator $\psi_3(t)$ of degree at most 3, we would consider

$$\left| f(t) - \frac{a_3t^3 + a_2t^2 + a_1t + a_0}{b_3t^3 + b_2t^2 + b_1t + b_0} \right|$$

and thus obtain

$$|b_3t^3f(t) + b_2t^2f(t) + b_1tf(t) + b_0 - a_2t^3 - a_2t^2 - a_1t - a_0| =$$
$$| - a_3t^3 + (-a_2 + b_3)t^2 + (-a_1 + b_2 - b_3)t + (-a_0 + b_1 - b_2 - b_3) + (b_0 - b_1 - b_2 + b_3)t^{-1}+$$
$$(-b_0 - b_1 + b_2 - b_3)t^{-2} + (-b_0 - b_1 - b_2 + b_3)t^{-3} + \ldots |.$$

To find the solution to the above system of equations, we need to find the reduced row echelon form of the following matrix, where the columns are $(b_0|b_1|b_2|b_3|a_0|a_1|a_2|a_3)$:

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & -1 & 0 & -1 & 0 & 0 \\ 0 & 1 & -1 & -1 & -1 & 0 & 0 & 0 \\ 1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 \\ -1 & -1 & 1 & -1 & 0 & 0 & 0 & 0 \\ -1 & -1 & -1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

After some calculations, we obtain the following reduced row echelon form, which gives us the required correspondences between the a_i and b_i:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Thus, we have

$$a_1 = a_3 = b_0 = b_1 = 0,\ a_0 = -2a_2,\ b_3 = a_2,\ b_2 = a_2,$$

and hence

$$\frac{\phi_3(t)}{\psi_3(t)} = \frac{a_2t^2 - 2a_2}{a_2t^3 + a_2t^2} = \frac{t^2 - 2}{t^3 + t^2}.$$

□

We have these two good functional approximations to f, and now we want to use them to find good approximations of the values of $f(t)$ for specific values of t - in other words, we want to use them to obtain good approximations by numbers of $f(t)$. For this purpose, we would like to find an estimate for how well $\phi_1(t)/\psi_1(t)$ approximated $f(t)$.

$$
\begin{aligned}
\left|f(t)-\frac{1}{t+1}\right| &= \left|\frac{1}{t+1}\right|\left|(t+1)\sum_{n\geqslant 1}(-1)^{2^{\theta_n}}t^{-n}-1\right| \\
&= \left|\frac{1}{t+1}\right|\left|\sum_{n\geqslant 3}(-1)^{2^{\theta_n}}t^{-n+1}+\sum_{n\geqslant 2}(-1)^{2^{\theta_n}}t^{-n}\right| \\
&\leqslant \left|\frac{2}{t^2(t+1)}\right|\left|\sum_{n\geqslant 0}t^{-n}\right| \\
&= \left|\frac{2}{t^2(t+1)(t-t^{-1})}\right| \\
&= \left|\frac{2}{t(t^2-1)}\right|.
\end{aligned}
$$

Thus, in short,

$$
\left|f(t)-\frac{1}{t+1}\right| \leqslant \left|\frac{2}{t(t^2-1)}\right|. \tag{37}
$$

Note that this is a general estimate, so it will also hold true if we substitute t^{2^n} for t:

$$
\left|f(t^{2^n})-\frac{1}{t^{2^n}+1}\right| \leqslant \frac{2}{t^{2^n}(t^{2^{n+1}}-1)}. \tag{38}
$$

We omit the modulus on the right hand side, since for $t > 1$, the expression is positive. We can use Proposition 5.23 to re-write this inequality as:

$$
\left|\frac{f(t)}{\prod_{j=1}^{n}\left(t^{2^{n-j}}-1\right)}-\frac{1}{t^{2^n}+1}\right| \leqslant \frac{2}{t^{2^n}(t^{2^{n+1}}-1)},
$$

and further as

$$
\left|f(t)-\frac{\prod_{j=1}^{n}\left(t^{2^{n-j}}-1\right)}{t^{2^n}+1}\right| \leqslant \frac{2\prod_{j=1}^{n}\left(t^{2^{n-j}}-1\right)}{t^{2^n}(t^{2^{n+1}}-1)}. \tag{39}
$$

$$
\tag{40}
$$

This observation motivates us to make the following definition:

5.27 Definition. Define

$$
\frac{p_n^*(t)}{q_n^*(t)} := \frac{\prod_{j=1}^{n}\left(t^{2^{n-j}}-1\right)}{t^{2^n}+1}.
$$

We would like to show that $p_n^*(t)/q_n^*(t)$ are ‘sufficiently close’ to $f(t)$. Ideally, we would like to show that, when evaluated at the point $t = 2$, they would yield convergents to $f(2) = c$; however, the 'next best thing' would be to show that they are bounded by the inverse of the square of their denominators. One easy way to do this would be to use estimate (39), and show that

$$\frac{2\prod_{j=1}^{n}\left(t^{2^{n-j}} - 1\right)}{t^{2^n}\left(t^{2^{n+1}} - 1\right)} < \frac{1}{\left(t^{2^n} + 1\right)^2}.$$

5.28 Proposition. *For all natural $n \geqslant 1$ and all $t > 1$, we have that*

$$\frac{(t^{2^n} + 1)^2 \prod_{j=1}^{n}\left(t^{2^{n-j}} - 1\right)}{t^{2^n}\left(t^{2^{n+1}} - 1\right)} < 1. \tag{41}$$

Proof. We prove this by induction on n.

Base case: for $n = 1$, (41) becomes

$$\frac{\left(t^2 - 1\right)^2 (t - 1)}{t^2(t^4 - 1)} = \frac{1}{t}\frac{t^2 + 1}{t^2 + t} < 1,$$

which holds for all $t > 1$.

Inductive step: suppose that, for some $n \geqslant 1$, we have

$$\frac{\left(t^{2^n} + 1\right)^2 \prod_{j=1}^{n}\left(t^{2^{n-j}} - 1\right)}{t^{2^n}\left(t^{2^{n+1}} - 1\right)} < 1. \tag{42}$$

Then, for $n + 1$, the left-hand side of inequality (41) becomes

$$\begin{aligned}
\frac{\left(t^{2^{n+1}} + 1\right)^2 \prod_{j=1}^{n+1}\left(t^{2^{n+1-j}} - 1\right)}{t^{2^{n+1}}\left(t^{2^{n+2}} - 1\right)} &= \frac{\left(t^{2^{n+1}} + 1\right)^2 \left(t^{2^n} - 1\right) \prod_{j=1}^{n}\left(t^{2^{n-j}} - 1\right)}{t^{2^{n+1}}\left(t^{2^{n+1}} - 1\right)\left(t^{2^{n+1}} + 1\right)} \\
&= \frac{\left(t^{2^{n+1}} + 1\right) \left(t^{2^n} - 1\right) \prod_{j=1}^{n}\left(t^{2^{n-j}} - 1\right)}{t^{2^{n+1}}\left(t^{2^{n+1}} - 1\right)} \\
&\leqslant \frac{\left(t^{2^n} - 1\right)\left(t^{2^{n+1}} + 2t^{2^n} + 1\right) \prod_{j=1}^{n}\left(t^{2^{n-j}} - 1\right)}{t^{2^{n+1}}\left(t^{2^{n+1}} - 1\right)} \\
&= \frac{\left(t^{2^n} - 1\right)\left(t^{2^n} + 1\right)^2 \prod_{j=1}^{n}\left(t^{2^{n-j}} - 1\right)}{\left(t^{2^n}\right)^2\left(t^{2^{n+1}} - 1\right)} \\
&\leqslant \frac{t^{2^n} - 1}{t^{2^n}} \\
&= 1 - \frac{1}{t^{2^n}} < 1,
\end{aligned}$$

where the next-to-last line follows by inductive hypothesis, and the last inequality holds for all $t > 1$.

$\square$

5.2 Interaction Between Functional and Rational Approximations

5.29 Lemma.

$$\left| f(t) - \frac{t^2 - 2}{t^3 + t^2} \right| \leqslant \left| \frac{2}{t^5(t^2 - 1)} \right|.$$

Proof. Recalling Theorem 5.21, that $\theta_n = 1 - \sigma_n$, where σ_n is the nth letter of the Thue-Morse word, and after some arithmetic manipulations, we obtain

$$\begin{aligned}
\left| f(t) - \frac{t^2 - 2}{t^3 + t^2} \right| &= \left| \frac{1}{t^3 + t^2} \right| \left| t^{-4} \sum_{n \geqslant 0} (-1)^{2^{\theta_n + 7}} t^{-n} + t^{-4} \sum_{n \geqslant 0} (-1)^{2^{\theta_n + 6}} t^{-n} \right| \\
&\leqslant \left| \frac{2t^{-4}}{t^3 + t^2} \right| \left| \frac{1}{1 - t^{-1}} \right| \\
&= \left| \frac{2}{t^5(t^2 - 1)} \right|,
\end{aligned}$$

as required. $\square$

5.30 Definition. We define

$$g_n(t) := \frac{\left(t^{2^{n+1}} - 2\right) \prod_{j=1}^{n} \left(t^{2^{n-j}} - 1\right)}{t^{2^{n+1}} \left(t^{2^n} + 1\right)}.$$

5.31 Theorem. *We have that*

$$|f(t) - g_n(t)| \leqslant \frac{1}{t^{2^{n+2}} \left(t^{2^n} + 1\right)^2}.$$

For the proof of Theorem 5.31, we need the following Proposition and Lemma:

5.32 Proposition. *We have that*

$$|f(t) - g_n(t)| \leqslant \frac{2 \prod_{j=1}^{n} \left(t^{2^{n-j}} - 1\right)}{t^{5 \times 2^n} \left(t^{2^{n+1}} - 1\right)}.$$

Proof. We substitute t^{2^n} for t in the estimate from Lemma 5.29 and obtain

$$\left| f(t^{2^n}) - \frac{t^{2^{n+1}} - 2}{t^{2^n.3} + t^{2^{n+1}}} \right| \leqslant \left| \frac{2}{t^{2^n 5}(t^{2^{n+1}} - 1)} \right|.$$

Next, we can use the functional equation from Theorem 5.23 and re-write this inequality as

$$\left| f(t) - \frac{\left(t^{2^{n+1}} - 2\right) \prod_{j=1}^{n} \left(t^{2^{n-j}} - 1\right)}{t^{2^{n+1}} \left(t^{2^n} + 1\right)} \right| \leqslant \frac{2 \prod_{j=1}^{n} \left(t^{2^{n-j}} - 1\right)}{t^{5 \times 2^n} \left(t^{2^{n+1}} - 1\right)},$$

which is the inequality we wanted. □

5.33 Lemma.

$$\frac{2 \prod_{j=1}^{k} \left(t^{2^{k-j}} - 1\right)}{t^{5 \times 2^k} \left(t^{2^{k+1}} - 1\right)} < \frac{1}{t^{2^{k+2}} \left(t^{2^k} + 1\right)^2}$$

Proof. We prove by induction on n that

$$\frac{2 \left(t^{2^n} + 1\right) \prod_{j=1}^{n} \left(t^{2^{n-j}} - 1\right)}{t^{2^n} \left(t^{2^n} - 1\right)} < 1. \tag{43}$$

Base case: For $n = 1$, inequality (43) becomes

$$\frac{2(t^2 + 1)}{t^2(t + 1)} < 1,$$

which can be re-written as

$$-t^3 + t^2 + 2 < 0. \tag{44}$$

This polynomial has one real root at approximately $t = 1.6956$, after which it becomes strictly negative. Since we are interested in values of t greater than 1.7 (we are interested in the valuation when $t = 2$), we can without loss of generality assume that the inequality holds.

Inductive step: assume that, for some $n \geqslant 1$, inequality (43) holds. Then for $n + 1$, we have

$$\frac{2 \left(t^{2^{n+1}} + 1\right) \prod_{j=1}^{n+1} \left(t^{2^{n+1-j}} - 1\right)}{t^{2^{n+1}} \left(t^{2^{n+1}} - 1\right)} \leqslant \frac{2 \left(t^{2^n} + 1\right) \left(t^{2^n} - 1\right) \prod_{j=1}^{n} \left(t^{2^{n-j}} - 1\right)}{\left(t^{2^n}\right)^2 \left(t^{2^n} - 1\right)}, \tag{45}$$

since we added a positive term to the numerator. By the inductive hypothesis, the right-hand side of equation (45) is less than

$$\frac{t^{2^n} - 1}{t^{2^n}} < 1,$$

as required. □

Now, the proof of Theorem 5.31 follows immediately from Lemma 5.32 and Lemma 5.33. Also, from Theorem 5.31, we have that $g_n(t)$ tends to $f(t)$ pointwise for $t > 1.7$, and in particular, $g_n(2) \to f(2) = c$. We will use this to show that c satisfies the 2-adic Littlewood conjecture, since $g_n(2)$ has large powers of 2 in the denominator.

5.34 Definition. Define the sequence $\{d_n\}_{n\in\mathbb{N}}$, which also tends to c, by:

$$d_n \coloneqq g_n(2).$$

5.35 Theorem. *We have that*

$$\liminf_{n\to\infty} n|n|_2||nc|| = 0.$$

Proof. For this, it is sufficient to consider an appropriate subsequence of the natural numbers, and show that for it, the expression tends to zero.

We consider the sequence $\left\{2^{2^{n+1}}\left(2^{2^n}+1\right)\right\}_{n\in\mathbb{N}}$, and note that

$$\begin{aligned} &||2^{2^{n+1}}\left(2^{2^n}+1\right)c|| = \\ &= ||2^{2^{n+1}}\left(2^{2^n}+1\right)(c+d_n-d_n)|| \\ &\leqslant ||2^{2^{n+1}}\left(2^{2^n}+1\right)(c-d_n)|| + ||2^{2^{n+1}}\left(2^{2^n}+1\right)d_n||, \end{aligned} \tag{46}$$

where the inequality follows from Proposition 2.3. By the Definition 5.34, the right summand of expression (46) is an integer, and so its norm is zero. Thus, expression 46 becomes

$$\begin{aligned} (46) &= ||2^{2^{n+1}}\left(2^{2^n}+1\right)(c-d_n)|| \\ &\leqslant \left|\left|\frac{2^{2^{n+1}}\left(2^{2^n}+1\right)}{2^{2^{n+2}}\left(2^{2^n}+1\right)^2}\right|\right| \text{ by Proposition 5.31} \\ &= \left|\frac{1}{2^{2^{n+1}}\left(2^{2^n}+1\right)}\right|, \end{aligned} \tag{47}$$

since the fraction is between 0 and $\frac{1}{2}$. Note this is strictly decreasing, tends to 0 as n goes to ∞. This gives us

$$\begin{aligned} \liminf_{n\to\infty} n|n|_2||nc|| &\leqslant \liminf_{n\to\infty} 2^{2^{n+1}}\left(2^{2^n}+1\right)\left|2^{2^{n+1}}\left(2^{2^n}+1\right)\right|_2 \left|\left|2^{2^{n+1}}\left(2^{2^n}+1\right)c\right|\right| \\ &\leqslant \liminf_{n\to\infty}\left|\frac{1}{2^{2^{n+1}}}\right| \text{ by Definition 4.8 and equation (47)} \\ &= 0 \end{aligned}$$

Therefore, the constant c satisfies the 2-adic Littlewood conjecture.

$\square$

5.3 Further Observations and Some Open Questions

There are several interesting observations related to the sequence $\{c_n\}_{n\in\mathbb{N}}$, which were omitted from the previous section for brevity, but can still be of interest for further investigation, both in Number Theory and in a more general mathematical setting.

5.3.1 A Link with the Thue-Morse Word

We notice an interesting pattern connecting the binary expansion of the rational numbers c_n and the Thue-Morse sequence.

First, we explore the binary expansion of the c_n's for small n, to notice the following interesting pattern:

$$c_1 = \frac{1}{3} = 0.\overline{01};$$
$$c_2 = \frac{1}{5} = 0.\overline{0011};$$
$$c_3 = \frac{3}{17} = 0.\overline{00101101}.$$

It seems the binary expansion is periodic, with period whose length grows by a factor of 2, and which is related to the binary expansion of the previous element of the sequence. Moreover, the sequence of 0's and 1's in the repeating part seem to follow a pattern we have seen before.

5.36 Theorem. *For $n \in \mathbb{N}$, the binary expansion of c_n is periodic with period 2^n.*

We will prove this Theorem just a bit later, along with another one, which requires a few preliminary definitions.

5.37 Definition. Assuming Theorem 5.36 holds, for $n \in \mathbb{N}$, we define $\mathbf{c}_n$ to be the word which comprises of the first 2^n numbers (considered as letters) of the binary expansion of c_n. In other words, we would have that

$$c_n =_2 0.\overline{\mathbf{c}_n}$$

5.38 Definition. For the Thue-Morse word $\mathbf{t} \in A^{\mathbb{N}}$, we define $\mathbf{l}_n$ as the Lyndon word for the conjugacy class of $Pref_n(\mathbf{t})$.

5.39 Theorem. *Recall Definition 3.16 of $Pref_n(\mathbf{x})$. We have that $Pref_{2^n-1}(\mathbf{c}_n) = Pref_{2^n-1}(\mathbf{l}_n)$.*

Proof of Theorem 5.36 and Theorem 5.39. From the formula for c_{n+1}, we obtain that

$$\begin{aligned}
c_{n+1} =& \frac{\prod_{j=0}^{n}(2^{2^j}-1)}{2^{2^{n+1}}+1} \\
=& \frac{\prod_{j=0}^{n}(2^{2^j}-1)}{2^{2^{n+1}}} \sum_{i=0}^{\infty} \left(\frac{-1}{2^{2^{n+1}}}\right)^i \\
=& \prod_{j=0}^{n}(2^{2^j}-1) \left[\frac{1}{2^{2^{n+1}}} - \frac{1}{(2^{2^{n+1}})^2} + \frac{1}{(2^{2^{n+1}})^3} - \frac{1}{(2^{2^{n+1}})^4} + \ldots + \frac{1}{(2^{2^{n+1}})^{2i-1}} - \frac{1}{(2^{2^{n+1}})^{2i}} + \ldots\right]
\end{aligned}$$

Grouping the sum into pairs of even and odd terms, we can rewrite the formula as:

$$\begin{aligned}
c_{n+1} &= \prod_{j=0}^{n}(2^{2^j}-1) \sum_{i=1}^{\infty} \left(\frac{1}{(2^{2^{n+1}})^{2i-1}} - \frac{1}{(2^{2^{n+1}})^{2i}}\right) \\
&= \prod_{j=0}^{n}(2^{2^j}-1) \sum_{i=1}^{\infty} \left(\frac{1}{2^{(2i-1)2^{n+1}}} - \frac{1}{2^{2i2^{n+1}}}\right) \\
&= \prod_{j=0}^{n}(2^{2^j}-1) \sum_{i=1}^{\infty} \left(\frac{2^{2^{n+1}}-1}{2^{2i2^{n+1}}}\right) \\
&= \prod_{j=0}^{n+1}(2^{2^j}-1) \sum_{i=1}^{\infty} \left(\frac{1}{2^{2i2^{n+1}}}\right).
\end{aligned}$$

Set

$$P_n = \prod_{j=0}^{n}(2^{2^j}-1),$$

and note that for all $n \in \mathbb{N}$, P_n is odd as a product of odd numbers. Thus, the numerator and denominator are coprime. Also, noting that the 2^n-th number of the binary expansion of P_n is always 1, we see that the binary expansion of P_n gives us a period of the binary expansion of c_{n+1}, namely 2^n. This proves Theorem 5.36.

Note that, moreover,

$$P_{n+1} = \prod_{j=0}^{n+1}(2^{2^j}-1) = (2^{2^{n+1}}-1)P_n = 2^{2^{n+1}}P_n - P_n.$$

From this, it becomes obvious that the word obtained from the binary expansion of P_n is a near-prefix of order 1 of the word of the binary expansion of P_{n+1}. Indeed, multiplying a number by $2^{2^{n+1}}$ adds 2^{n+1} zeroes at the end of its binary expansion, and subtracting a number whose binary expansion is of length 2^{n+1} from the previous number gives us the desired word, conjugate of a prefix of the Thue-Morse word of the appropriate length (this follows from Definition 3.27 of the Thue-Morse word). □

5.3.2 On an Interesting Structure Arising From the Sequence $\{c_n\}_{n\in\mathbb{N}}$

We introduce the following definitions:

5.40 Definition. Define $T : \mathbb{R}/\mathbb{Z} \to \mathbb{R}/\mathbb{Z}$ as

$$T(x) := 2x \mod 1.$$

In other words, $T^n(x)$ is multiplication of x by 2^n and mapping back into $[0, 1]$.

5.41 Definition. For $\alpha \in [0, \frac{1}{2})$, define

$$\begin{aligned} I(\alpha) &:= [0, \alpha) \cup (1 - \alpha, 1] \\ J(\alpha) &:= I(\alpha) \cup \bigcup_{n\in\mathbb{N}} T^{-n}(I(\alpha)). \end{aligned}$$

In other words, $I(\alpha)$ can be viewed as an open ball of radius α centred at $0 \equiv 1 \mod 1$, and $J(\alpha)$ is the set of all pre-images of $I(\alpha)$ under multiplication by 2^n in the quotient space $\mathbb{R}/\mathbb{Z}$.

Note that for $\beta \in [0, 1] \setminus J(\alpha)$, we have that

$$\liminf_{n\to\infty} ||2^n\beta|| \geqslant \alpha.$$

This motivates us to consider the set of such points and introduce the following notion:

5.42 Definition. For a real number $\alpha \in [0, 1/2]$, define $K(\alpha)$ as the points in $[0, 1]$ not covered by $J(\alpha)$, in other words,

$$K(\alpha) := [0, 1] \setminus J(\alpha).$$

Now, we can make some interesting observations about the structure of 'excluded points' $K(\alpha)$ in the case that $\alpha = c_n$.

5.43 Proposition. *For $c_0 = \frac{1}{3}$, $K(c_0) = \{\frac{1}{3}, \frac{2}{3}\}$.*

5.44 Note. The following proof might seem a bit laboured, but the method illustrated via this simpler example is believed by the author to illustrate one possible method of providing an answer to Question 2.

Proof. Indeed, $\{\frac{1}{3}, \frac{2}{3}\} \subseteq K(c_0)$, since a simple arithmetic check shows that for all $k \in \mathbb{N}$,

$$\left|\left|2^k\frac{1}{3}\right|\right| = \left|\left|2^k\frac{2}{3}\right|\right| = \frac{1}{3},$$

and thus both elements of the set satisfy the membership conditions of $K(c_0)$.

Also, $K(c_0) \subseteq \{\frac{1}{3}, \frac{2}{3}\}$.

Indeed, we can re-write $K(c_0)$ as:

$$\begin{aligned} Y_1 &= \{x \in [0,1] : \forall k \in \mathbb{N}\ ||2^k x|| \geqslant \frac{1}{3}\} \\ &= \bigcap_{k\in\mathbb{N}} \{x \in [0,1] : ||2^k x|| \geqslant \frac{1}{3}\}. \end{aligned}$$

This leads us to define intervals $I_k = \{x \in [0,1] : ||2^k x|| \geqslant \frac{1}{3}\}$.

Note $I_0 = [\frac{1}{3}, \frac{2}{3}]$, since $x \in I_0$ iff $||x|| \geqslant \frac{1}{3}$.

Similarly, $x \in I_1$ iff $||2x|| \geqslant \frac{1}{3}$ iff $\min\{|2x - n| : n \in \mathbb{N}\} \geqslant \frac{1}{3}$. Since we already have $I_0 = [\frac{1}{3}, \frac{2}{3}]$ and we are concerned with the intersection of I_0 and I_1, we only need to look at the $x \in I_0$ which will also be in I_1. Thus, if $x \in I_0$, we have $2x \in [\frac{2}{3}, \frac{4}{3}]$, and thus only need to consider $n = 0$ or $n = 1$ in the above min. Therefore, $x \in I_1$ iff

$$\left(|2x| \geqslant \frac{1}{3}\right) \ \vee\ \left(|2x - 1| \geqslant \frac{1}{3}\right),$$

but since the first inequality is true for all $x \in I_0$, we have that $x \in I_1$ iff

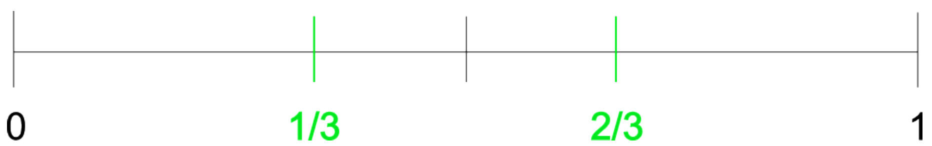
$$|2x - 1| \geqslant 1 \Leftrightarrow x \in [0, \frac{1}{3}] \cup [\frac{2}{3}, 1].$$

Thus,

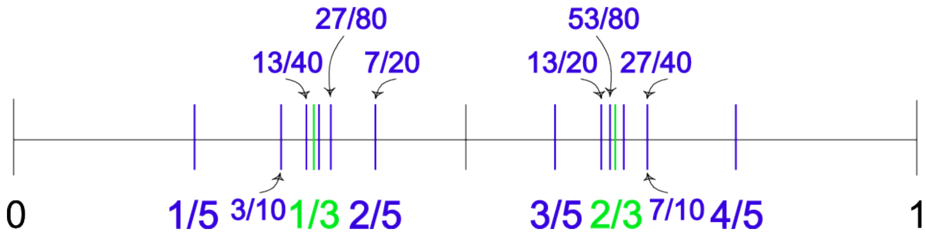
$$\left\{\frac{1}{3}, \frac{2}{3}\right\} = I_0 \cap I_1 \subseteq \bigcap_{k\in\mathbb{N}} I_k \subseteq \bigcap_{k\in\mathbb{N}} \left\{x \in [0,1] : ||2^k x|| \geqslant \frac{1}{3}\right\} = K(c_0),$$

which shows the required subset relation. $\square$

Thus, $K(c_0)$ can be illustrated (in green) as:



Moreover, $K(c_1)$ can be illustated (in blue) as:



Observation of the above graphs lead us to pose the following:

2 Question (Conjecture)**.** For each c_n, the set of rational points in $K(c_n)$ clusters at all points of $K(c_{n-1})$; in particular, the points in $K(\frac{1}{5})$ cluster at the points $\frac{1}{3}$ and $\frac{2}{3}$.

6 Conclusion

In this Thesis, we provided the necessary background for a non-trivial examination of the Littlewood Conjecture, as well as several other conjectures which relate to it, with a particular emphasis on the p-adic Littlewood Conjecture. In Chapter 5, we considered the case when $p = 2$. We constructed a special sequence which would tend to a possible counter-example, c, to the 2-adic Littlewood Conjecture, and justified considering it as a possible counter-example in Theorem 5.10. We proceeded to show that in fact, the 2-adic Littlewood Conjecture holds for this counter-example (Theorem 5.35). The method used can be generalised to the p-adic case. Throughout Chapter 5, we also looked at some interesting combinatorial properties of words related to the constant c, and in particular, related to the binary or continued fraction expansions of the sequence of convergents of c, $\{c_n\}_{n\in\mathbb{N}}$. Moreover, investigations of the sequence $\{c_n\}_{n\in\mathbb{N}}$ provided us with other observations in Section 5.3.2, which are of purely mathematical interest.

6.1 Various Questions for Further on

The initial hope of this disseration was to prove that the constant c is badly approximable. However, during the course of the dissertation, Badziahin and Zorin proved the following theorem:

6.1 Theorem ([BZ14])**.** *The constant c is not badly approximable.*

In fact, they show an even stronger property of c, namely that there is a constant $K > 0$ such that for infinitely many q, the following inequality holds:

$$||qc|| \leqslant \frac{K}{q(\log\log q)^2}.$$

However, a more general question still remains: is it possible to extend the methods used in Chapter 5 to include other sequences, perhaps obtaining a smaller constant c', which is badly approximable? Continuing this way, perhaps we could obtain a sequence of such bounds, which tends to 0, which would prove the 2-adic Littlewood Conjecture.

References

[AAK$^+$86] J.-P. Allouche, F. Axel, M. Kleman, M. Mendés France, and J. Peyriére. Vibrational modes in a one dimensinal "quasi-alloy". *J. Physique, Colloque C3, Supplement to No.7*, 47:C3–181–C3–186, 1986.

[AC85] J.-P. Allouche and H. Cohen. Dirichlet series and curious infinite products. *Bulletin of the London Mathematical Society*, 17:531–538, 1985.

[AP89] F. Axel and J. Peyriére. Spectrum and extended states in a harmonic chain with controlled disorder: effects of the Thue-Morse symmetry. *J. Statist. Phys.*, 57:1013–1047, 1989.

[AS99] Jean-Paul Allouche and Jeffrey Shallit. The ubiquitous Prouhet-Thue-Morse sequence. In *Sequences and their applications, Proceedings of SETA'98*, pages 1–16. Springer, 1999.

[AS03] Jean-Paul Allouche and Jeffrey Shallit. *Automatic Sequences: Theory, Applications, Generalizations*. Cambridge University Press, 2003.

[Bad11] Dzmitry Badziahin. On multiplicatively badly approximable numbers. *Mathematika*, 59(1):31–55, 2011.

[Bak90] Alan Baker. *Transcendental Number Theory*. Cambridge University Press, 1990.

[BBEK14] Dmitry Badziahin, Yann Bugeaud, Manfred Einsiedler, and Dmitry Kleinbock. On the complexity of a putative counterexample to the p-adic Littlewood conjecture. 2014.

[BBG04] Jonathan Borwein, David Bailey, and Roland Girgensohn. *Experimentation in Mathematics: Computational Paths to Discovery*. Wellesley, MA, 2004.

[BDdM07] Yann Bugeaud, Michael Drmota, and Bernard de Mathan. On a mixed Littlewood conjecture in Diophantine approximation. *Acta Arithmetica*, 128:107–124, 2007.

[Ber94] J Berstel. Axel thue's papers on repetitions in words: a translation. *Publications du Laboratoire de Combinatoire et d'Informatique Mathématique*, (20), 1994.

[BL05] Yann Bugeaud and M Laurent. Exponents of Diophantine Approximation and Sturmian Continued Fractions. *Ann. Inst. Fourier (Grenoble)*, 55:773–804, 2005.

[BL07] Yann Bugeaud and Michael Laurent. Exponents of Diophantine Approximation. volume CRM Series 4, pages 101–121, 2007.

[Bre91] Calude Brezinski. *History of Continued Fractions and Padè Approximants.* Springer-Verlag, 1991.

[Bug12] Yann Bugeaud. *Distribution modulo one and Diophantine approximation.* Cambridge University Press, 2012.

[Bur01] Edward B. Burger. *Exploring the Number Jungle: A Journey into Diophantine Analysis.* American Mathematical Society, 2001.

[BvdPSZ14] Jonathan Borwein, Alf van der Poorten, Jeffrey Shallit, and Wadim Zudilin. *Neverending Fractions: An Introduction to Continued Fractions*. Cambridge University Press, 2014.

[BZ14] Dzmitry Badziahin and Evgeniy Zorin. Thue–Morse constant is not badly approximable. *International Mathematics Research Notices*, 2014.

[Cas57] John William Scott Cassels. *An Introduction to Diophantine Approximation.* Cambridge University Press, 1957.

[CJS09] Christian Calude, Helmut Jürgensen, and Ludwig Staiger. Topology on words. *Elsevier*, pages 2323–2335, 2009.

[CK03] Marek Capiński and Ekkehard Kopp. *Measure, Integral and Probability.* Springer-Verlag, 2003.

[CSD55] John William Scott Cassels and Henry Peter Francis Swinnerton-Dyer. On the product of three homogeneous linear forms and indefinite ternary quadratic forms. *Philosophical Transactions of the Royal Society of London, Series A*, 248:73–96, 1955.

[Dir42] Johann Peter Gustav Lejeune Dirichlet. Verallgemeinerng eines Satzes aus der Lehre von den Kettenbrüchen nebst einiger Anwendungen auf die Theorie der Zahlen. *S.-B. Preuss. Akad. Wiss*, 1842.

[dMT04] Bernard de Mathan and O Teulié. Problémes Diophantiens simultanés. *Monatsh. Math.*, 143:229–245, 2004.

[Dys47] Freeman J. Dyson. On simultaneous Diophantine Approximations. *Proceedings of the London Mathematical Society*, 49:409–420, 1947.

[EK07] Manfred Einsiedler and Dmitry Kleinbock. Measure rigidity and the p-adic littlewood-type problems. *Compositio Math*, 143:689–702, 2007.

[EKL06] Manfred Einsiedler, Anatole Katok, and Elon Lindenstrauss. Invariant measures and the set of exceptions to Littlewood's conjecture. *Annals of Mathematics*, 164:513–560, 2006.

[Els99] Carsten Elsner. On arithmetic properties of the convergents of Euler's number. *Colloquium Mathematicum*, 79(1):133–145, 1999.

[Eul37] Leonard Euler. *De fractionibus continuis dissertatio*, volume 9. Comm. Acad. Sci. Petrop., 1737.

[Eul48] Leonard Euler. *Introduction analysin infinitorium*, volume 1. Lausanne, 1748.

[Euw29] Max Euwe. Mengentheoretische Betrachtungen über das Schachspiel. *Proc. Konin. Akad. Wetenschappen*, 32:633–642, 1929.

[Fat04] Pierre Fatou. Sur l'approximation des incommensurables et les séries trigonométriques. *C. R. Acad. Sci Paris*, 139:1019–1021, 1904.

[Gar95] Martin Gardner. *New Mathematical Diversions*. Mathematical Association of America, 1995.

[Gou93] Fernando Q. Gouvêa. *p-adic Numbers*. Springer-Verlag, 1993.

[Hen06] Doug Hensley. *Continued Fractions*. World Scientific Publishing, 2006.

[HM14] Alan Haynes and Sara Munday. Diophantine approximation and coloring. *American Mathematical Monthly*, 2014.

[Hur91] A. Hurwitz. Über die angenäherte Darstellung der Irrationalzahlen durch rationale Brüche (On the approximation of irrational numbers by rational numbers). *Math. Ann*, 39(2), 1891.

[HW03] Godfrey H. Hardy and Edward M. Wright. *An Introduction to the Theory of Numbers*. Oxford Science Publications, 2003.

[Jar50] Vojtěch Jarník. Une remarque sur les approximations diophantiennes linéaires. *Acta Sci. Math. Szeged*, 12:82–86, 1950.

[Jar54] Vojtěch Jarník. Contribution á la théorie des approximations diophantiennes linéaires et homogénes. *Czechoslovak Math. J.*, 4:330–353, 1954.

[Khi26] Aleksandr Y. Khintchine. Über eine Klasse linearer diophantischer Approximationen. *Rendiconti del Circolo Matematico di Palermo*, 50:170–195, 1926.

[Kok39] J. F. Koksma. Über die Mahlersche Klasseneinteilung der transzendenten Zahlen und die Approximation komplexer Zahlen durch algebraische Zahlen. *Monats. Math. Phys.*, (48):176–189, 1939.

[Kom07] Takao Komatsu. Some combinatorial properties of the leaping convergents. *Integers: Electronic Journal of Combinatorial Number Theory*, 7(2), 2007.

[Kun11] Kenneth Kunen. *Set Theory*. Individual Author and College Publications, 2011.

[Lam68] Johan Heinrich Lambert. Mémoire sur quelques propriétés remarquables des quantités transcendantes circulaires et logarithmiques. *Mémoires de l'Académie des sciences de Berlin*, 17:265–322, 1768.

[Lit68] John Edensor Littlewood. *Some problems in real and complex analysis*. D.C. Heath and Co. Raytheon Education Co., 1968.

[Lot02] M Lothaire. *Algebraic Combinatorics on Words*, volume 90 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, 2002.

[Mah32] K. Mahler. Zur Approximation der Exponentialfunktionen und des Logarithmus. *J. Reine Angew. Math.*, (199):118–150, 1932.

[Mor21] Harold Marston Morse. Recurrent geodesics on a surface of negative curvature. *Transactions of the American Mathematical Society*, 22(1):84–100, 1921.

[Old70] C. D. Olds. The simple continued fraction expansion of e. *The American Mathematical Monthly*, 77:968–974, 1970.

[Pec61] L. G. Peck. Simultaneous rational approximations to algebraic numbers. *Bulleting of American Mathematical Society*, 67:197–201, 1961.

[Pro51] Eugene Prouhet. Memoire sur quelques relations entre les puissances des nombres. *Comptes-Rendus de l'Académie des Sciences de Paris*, 33:225, 1851.

[PV00] A. D. Pollington and S. Velani. On a problem in simultaneous Diophantine approximation: Littlewood's conjecture. *Acta Mathematica*, 185:287–306, 2000.

[Rob00] Alain M Robert. *A course on p-adic Analysis.* Graduate Texts in Mathematics. Springer, 2000.

[Ros93] Kenneth H. Rosen. *Elementary Number Theory and Its Applications.* Addison-Wesley Publishing Company, third edition, 1993.

[Rou07] Daniel Rouan. Á la recherche d'une chaleur venue d'ailleurs: astronomie infrarouge, optique diophantienne. volume 33, page 225. Comptes-Rendus de l'Académie des Sciences de Paris, Juin 2007.

[Roy04] D. Roy. Diophantine approximation in small degree. *CRM Proc. Lecture Notes 36, Amer. Math. Soc., Providence, RI*, 36:269–285, 2004.

[Sch80] Wolfgang Schmidt. *Diophantine approximation.* Lecture notes in mathematics. Springer, 1980.

[Spe42] D. C. Spencer. The lattice points of tetrahedra. *J. Math. Phys. Mass. Inst. Tech.*, 21:189–197, 1942.

[Ste92] John Steinig. A proof of Lagrange's theorem on periodic continued fractions. *Arch. Math.*, 59:21–23, 1992.

[Thu12] Axel Thue. Über die gegenseitige Lage gleicher Teile gewisser Zeichenreihen. *Kra. Vidensk. Selsk. Skrifter. I. Mat.-Nat. Kl., Christiana*, (10), 1912.

[Wir61] E. Wirsing. Approximation mit algebraischen Zahlen beschränkten Grades. *J. reine angew. Math.*, 206:67–77, 1961.

[YIM95] A. A. Panchiskin Yurii I. Manin. *Number Theory I*, volume 49 of *Encyclopaedia of Mathematical Sciences.* Springer, 1 edition, 1995.