

# Diophantine Approximation and Transcendence Theory

Benjamin Church

October 29, 2021

## Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Algebraic Numbers and Cantor's Theorem</b>	<b>2</b>
<b>3</b>	<b>Diophantine Approximation</b>	<b>3</b>
<b>4</b>	<b>Irrationality Measure</b>	<b>6</b>
<b>5</b>	<b>Liouville Numbers</b>	<b>8</b>
<b>6</b>	<b>Measure Theory of Approximable Numbers</b>	<b>9</b>

# 1 Introduction

The rational numbers ( $\mathbb{Q}$ ) are incomplete in two different ways. Firstly,  $\mathbb{Q}$  is not algebraically closed because there exist polynomials with rational coefficients which have no roots in  $\mathbb{Q}$ . For example,  $x^2 - 2 = 0$ . Furthermore,  $\mathbb{Q}$  is not complete because there are sequences of rational numbers which converge in the real numbers but not in the rational numbers. For example, let  $F_n$  be the  $n$ -th Fibonacci number then  $\lim_{n \rightarrow \infty} \frac{F_{n+1}}{F_n} = \varphi$  where  $\varphi = \frac{1+\sqrt{5}}{2} \notin \mathbb{Q}$ . If we complete  $\mathbb{Q}$  by adding in the limit of every sequence, we get the real numbers  $\mathbb{R}$ . If take the algebraic closure of  $\mathbb{Q}$  by adding in the roots of every polynomial with coefficients in  $\mathbb{Q}$  we get the algebraic numbers  $\overline{\mathbb{Q}}$ . The relationship between these two sets was of great historical importance. In particular,  $\overline{\mathbb{Q}}$  contains complex numbers (for example  $i$  solves  $x^2 + 1 = 0$ ) and  $\mathbb{R}$  does not. The question arises, is  $\mathbb{R}$  contained in  $\overline{\mathbb{Q}}$ . Equivalently, does there exist a non-algebraic real number. Such a number is called *transcendental* because the number “transcends” algebraic definition.

# 2 Algebraic Numbers and Cantor’s Theorem

**Definition:**  $\mathbb{Q}[X]$  is the set of polynomials with coefficients in  $\mathbb{Q}$  and  $\mathbb{Z}[X]$  is the set of polynomials with coefficients in  $\mathbb{Z}$ .

**Definition:** A complex number  $\alpha \in \mathbb{C}$  is *algebraic* if there exists a polynomial  $f \in \mathbb{Q}[X]$  such that  $f(\alpha) = 0$ . Otherwise,  $\alpha$  is *transcendental*.

**Proposition.**  $\alpha \in \mathbb{C}$  is algebraic if there exists a nonzero polynomial  $f \in \mathbb{Z}[X]$  with *integer* coefficients such that  $f(\alpha) = 0$ .

*Proof.* Let  $\alpha \in \mathbb{C}$  be a root of a polynomial  $f \in \mathbb{Z}[X]$ . Because  $\mathbb{Z} \subset \mathbb{Q}$  then  $\mathbb{Z}[X] \subset \mathbb{Q}[X]$  so  $f \in \mathbb{Q}[X]$  so  $\alpha$  is algebraic. Conversely, let  $\alpha \in \mathbb{C}$  be algebraic. Then  $\alpha$  is the root of some polynomial with rational coefficients,

$$\begin{aligned} f(\alpha) &= \frac{p_n}{q_n} \alpha^n + \cdots + \frac{p_1}{q_1} \alpha + \frac{p_0}{q_0} \\ &= p_n(q_{n-1}q_{n-2} \cdots q_0) \alpha^n + \cdots + p_1(q_n q_{n-1} \cdots q_2 q_0) \alpha + p_0(q_n q_{n-1} \cdots q_2 q_1) \\ &= 0 \end{aligned}$$

Therefore,  $\alpha$  is the root of a polynomial with coefficients in  $\mathbb{Z}$ . □

**Definition:** Let  $\alpha \in \mathbb{C}$  be algebraic. The degree of  $\alpha$ , denoted as  $\deg \alpha$ , is the minimum degree of a nonzero polynomial  $f \in \mathbb{Z}[X]$  such that  $f(\alpha) = 0$ .

**Definition:** A function  $f : X \rightarrow Y$  is a *surjection* if for every  $y \in Y$  there exists  $x \in X$  such that  $f(x) = y$ .

**Definition:** A set  $X$  is *countable* if there is a surjection  $f : \mathbb{N} \rightarrow X$ . Otherwise,  $X$  is *uncountable*. Such a function is called a list of  $X$ .

**Definition:** The set  $\overline{\mathbb{Q}} \subset \mathbb{C}$  is the set of algebraic numbers. That is, given a complex number  $\alpha \in \mathbb{C}$  then  $\alpha \in \overline{\mathbb{Q}}$  if and only if  $\alpha$  is the root of some rational polynomial  $p \in \mathbb{Q}[X]$ .

**Theorem 2.1.**  $\overline{\mathbb{Q}}$  is countable.

*Proof.* Every polynomial has a finite number of roots so it suffices to show that we can list all polynomials with integer coefficients. The list goes as follows, list all polynomials with degree less than  $n$  and coefficients with absolute value less than  $n$ . There are a finite number of such polynomials so we will list every polynomial by incrementally increasing  $n$ . This is surjective because given a polynomial of degree  $n$  there are a finite number of polynomials with smaller degree and smaller coefficients so the function will reach this given polynomial in a finite number of steps.  $\square$

**Theorem 2.2** (Cantor).  $\mathbb{R}$  is uncountable.

*Proof.* This is a classic proof by contradiction. Suppose I had such a function  $f : \mathbb{N} \rightarrow \mathbb{R}$ . Now, I will construct some  $r \in \mathbb{R}$  not in the image of  $f$ . For simplicity let us only take real numbers on the interval  $[0, 1]$  this will suffice. Let  $r_i$  be the  $i$ -th digit of  $r$  in some base  $b$ . Define the number  $s \in \mathbb{R}$  by its expansion base  $b$  as  $s_i = f(i)_i + 1 \bmod b$ . This is the  $i$ -th digit of the  $i$ -th number plus one reduced by  $b$ . I claim that there does not exist any  $n \in \mathbb{N}$  such that  $f(n) = s$ . Suppose such an  $n$  exists. Then  $s_n = f(n)_n + 1 \bmod b$  but  $s = f(n)$  so  $s_n = f(n)_n$  which is a contradiction. Therefore,  $f$  cannot be a bijection.  $\square$

**Corollary 2.3.** Transcendental numbers exist.

*Proof.* If  $\mathbb{R} \subset \overline{\mathbb{Q}}$  then because  $\overline{\mathbb{Q}}$  is countable then  $\mathbb{R}$  would be countable because any surjection onto  $\overline{\mathbb{Q}}$  can be reduced to a surjection onto  $\mathbb{R}$  by mapping every  $x \in \overline{\mathbb{Q}}$  such that  $x \notin \mathbb{R}$  to some fixed point of  $\mathbb{R}$ . However,  $\mathbb{R}$  is uncountable so there must be some  $r \in \mathbb{R}$  such that  $r \notin \overline{\mathbb{Q}}$ .  $\square$

### 3 Diophantine Approximation

Diophantine approximation is the process of finding successively better rational approximations to irrational numbers. The fact that any irrational number can be approximated arbitrarily closely by rational numbers is, of course, just the fact that  $\mathbb{Q} \subset \mathbb{R}$  is dense. That said, Diophantine approximation is the study of how *well* or *quickly* such approximations can be made. The theory of Diophantine approximation is built on the following fundamental lemma.

**Lemma 3.1** (Dirichlet). For any  $\alpha \in \mathbb{R}$  and  $N \in \mathbb{Z}^+$  there exists,  $p, q \in \mathbb{Z}$  such that  $1 \leq q \leq N$  and,

$$|q\alpha - p| < \frac{1}{N}$$

*Proof.* For each  $1 \leq q \leq N$  there is exactly one  $p$  such that  $0 \leq q\alpha - p < 1$ . Split the interval  $[0, 1)$  into  $N$  segments,

$$[0, \frac{1}{N}), [\frac{1}{N}, \frac{2}{N}), \dots, [\frac{N-1}{N}, 1)$$

Thus  $q\alpha - p$  lands in one of these  $N$  segments for each  $q$  in  $1 \leq q \leq N$ . Therefore, by the pigeonhole principle, either for some  $q$  we have  $q\alpha - p \in [0, \frac{1}{N})$  in which case we are done or there exist two pairs  $(p, q)$  and  $(p', q')$  which fall in the same interval. We may assume that  $1 \leq q < q' \leq N$  and then,

$$|(q' - q)\alpha - (p' - p)| = |(q'\alpha - p') - (q\alpha - p)| < \frac{1}{N}$$

where  $1 \leq q' - q \leq N$ . □

**Corollary 3.2.** *Let  $\alpha \in \mathbb{R}$  be irrational then there exist infinitely many  $\frac{p}{q} \in \mathbb{Q}$  such that,*

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}$$

*Proof.* For each  $N \in \mathbb{Z}^+$  there exists  $p, q \in \mathbb{Z}$  with  $1 \leq q \leq N$  such that,

$$|q\alpha - p| < \frac{1}{N}$$

Since  $\alpha \notin \mathbb{Q}$  this difference cannot be zero. Dividing by  $q$  we find,

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{Nq} < \frac{1}{q^2}$$

Therefore the required inequality has a solution for any  $N \in \mathbb{Z}^+$ . In particular this implies infinitely many solutions since the difference  $\alpha - \frac{p}{q}$  is arbitrarily small and thus cannot be bounded below by any best approximation. □

*Remark 3.0.1.* The above corollary motivates the following definition. We want to say that any irrational  $\alpha \in \mathbb{R}$  is 2-approximable where we define:

**Definition:** For  $\alpha \in \mathbb{R}$ , an  $n$ -good Diophantine approximation is  $\frac{p}{q} \in \mathbb{Q}$  so that,

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^n}$$

**Definition:** A number  $\alpha \in \mathbb{R}$  is  $n$ -approximable if there exist infinitely many  $n$ -good Diophantine approximations.

**Definition:**

$$G_n(\alpha) = \left\{ \frac{p}{q} \in \mathbb{Q} \left| 0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^n} \right. \right\}$$

the set of  $n$ -good approximations of  $\alpha$ .  $\alpha$  is  $n$ -approximable when  $|G_n(\alpha)| = \infty$ .

*Remark 3.0.2.* The degree of goodness of an approximation in the above sense does not take into account the constants or tightness of the denominator bound only that infinitely many such solutions exist. In fact one can show that the tightest possible bound is given by the following theorem.

**Theorem 3.3** (Hurwitz). *For any irrational  $\xi \in \mathbb{R}$  there exist infinitely many rational  $\frac{p}{q} \in \mathbb{Q}$  such that,*

$$\left| \xi - \frac{p}{q} \right| < \frac{1}{\sqrt{5} q^2}$$

*and this does not hold for any constant denominator  $C > \sqrt{5}$ .*

**Definition:** We say that  $\alpha \in \mathbb{R}$  is badly-approximable if there exists some  $c > 0$  such that for all  $\frac{p}{q} \in \mathbb{Q}$ ,

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

Otherwise  $\alpha$  is well-approximable.

**Theorem 3.4** (Thue–Siegel–Roth, 1955). *If  $\alpha$  is irrational algebraic and  $\varepsilon > 0$  then there exists a positive constant  $C(\alpha, \varepsilon)$  such that  $\forall \frac{p}{q} \in \mathbb{Q}$ ,*

$$\left| \alpha - \frac{p}{q} \right| > \frac{C(\alpha, \varepsilon)}{q^{2+\varepsilon}}$$

*Remark 3.0.3.* Klaus Roth was awarded the Fields Medal for the proof of this theorem. Needless to say, we will not prove it here. Instead we will prove a weaker classical result of Liouville.

**Lemma 3.5** (Liouville). *Let  $\alpha$  be a root of  $f \in \mathbb{Z}[X]$  with  $\deg f = n$  then there exists  $C \in \mathbb{R}^+$  such that for every  $\frac{p}{q} \in \mathbb{Q}$  such that  $\frac{p}{q} \neq \alpha$  we have,*

$$\left| \alpha - \frac{p}{q} \right| > \frac{C}{q^n}$$

*Proof.* Let  $f(x) = a_n x^n + \dots + a_0$  with coefficients  $a_i \in \mathbb{Z}$ . Take  $f(\alpha) = 0$ . There are at most  $n$  roots of  $f$  labeled  $\alpha_1, \alpha_2, \dots, \alpha_k$  and  $\alpha$ . Define,

$$r = \min\{|\alpha - \alpha_1|, |\alpha - \alpha_2|, \dots, |\alpha - \alpha_k|\}$$

Therefore,  $f$  has no roots except  $\alpha$  on the interval  $(\alpha - r, \alpha + r)$ . Define,

$$M = \max\{|f'(x)| \mid x \in (\alpha - r, \alpha + r)\}$$

and take any positive real number  $C < \min\{r, \frac{1}{M}\}$ . Now, take any  $\frac{p}{q} \in \mathbb{Q}$  with  $\frac{p}{q} \neq \alpha$ . If  $\left| \alpha - \frac{p}{q} \right| > C > \frac{C}{q^n}$  then we are done. Otherwise,  $\left| \alpha - \frac{p}{q} \right| \leq C < r$  so  $\frac{p}{q} \in (\alpha - r, \alpha + r)$  but  $\alpha \neq \frac{p}{q}$  so  $f(\frac{p}{q}) \neq 0$  because there are no other roots on this interval. Consider,

$$q^n f\left(\frac{p}{q}\right) = a_n p^n + a_{n-1} p^{n-1} q + \dots + a_0 q^n \in \mathbb{Z}$$

However,  $q^n f(\frac{p}{q}) \neq 0$  so  $|q^n f(\frac{p}{q})| \geq 1$  because it is a nonzero positive integer so,

$$\left| f\left(\frac{p}{q}\right) \right| \geq \frac{1}{q^n}$$

By the mean value theorem, there exists  $\xi \in (\alpha, \frac{p}{q}) \subset (\alpha - r, \alpha + r)$  such that,

$$f'(\xi) = \frac{f(\frac{p}{q}) - f(\alpha)}{\frac{p}{q} - \alpha}$$

Therefore,

$$\left| \alpha - \frac{p}{q} \right| = \left| \frac{f(\frac{p}{q})}{f'(\xi)} \right|$$

However,  $|f'(\xi)| \leq M$  and  $|f(\frac{p}{q})| \geq \frac{1}{q^n}$  so,

$$\left| \alpha - \frac{p}{q} \right| = \left| \frac{f(\frac{p}{q})}{f'(\xi)} \right| \geq \frac{1}{Mq^n} > \frac{C}{q^n}$$

□

**Corollary 3.6.** *Let  $\alpha$  be algebraic with degree  $n$ , then for any  $k > n$ ,  $\alpha$  is not  $k$ -approximable.*

*Proof.* Suppose that  $k > n$  and  $\alpha$  is  $k$ -approximable then  $G_k(\alpha)$  is infinite and thus must contain  $\frac{p}{q}$  with arbitrarily large  $q$ . Therefore, given any  $C \in \mathbb{R}^+$  we can choose  $\frac{p}{q} \in G_k(\alpha)$  such that  $q^{k-n} > C$  which is possible because  $k - n > 0$ . Then, because  $\frac{p}{q} \in G_k(\alpha)$ ,

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^k} = \frac{C}{q^n} \cdot \frac{C}{q^{n-k}} < \frac{C}{q^n}$$

Since  $\frac{p}{q} \neq \alpha$ , this contradicts the previous lemma because  $\alpha$  is a root to some  $f \in \mathbb{Z}[X]$  with  $\deg f = n$ . However, there cannot exist any  $C \in \mathbb{R}^+$  such that,

$$\left| \alpha - \frac{p}{q} \right| > \frac{C}{q^n}$$

for every  $\frac{p}{q} \in \mathbb{Q}$  with  $\frac{p}{q} \neq \alpha$ . Thus,  $\alpha$  is not  $n$ -approximable. □

## 4 Irrationality Measure

We can use the previous definitions and results to define a measure of how irrational a number is. Essentially, the irrationality measure tells us how well a number can be approximated by rational numbers. Perhaps unintuitively, the more irrational the number, the *better* it can be approximated by rationals.

**Definition:** The *irrationality measure* is  $\mu(\alpha) = \sup\{n \in \mathbb{R}^+ \mid |G_n(\alpha)| = \infty\}$

**Proposition.** If  $\alpha \in \mathbb{Q}$  then  $\mu(\alpha) = 1$

*Proof.* Take  $\epsilon < 1$  and  $\alpha = \frac{p}{q}$ . Then, for any  $n \in \mathbb{N}$  consider  $p_n = np + 1$  and  $q_n = nq$ . Now,  $\alpha - \frac{p_n}{q_n} = \frac{np - p_n}{nq} = \frac{1}{nq} = \frac{1}{q_n}$ . Also,  $q_n^\epsilon < q_n$ . Therefore,

$$0 < \left| \alpha - \frac{p_n}{q_n} \right| = \frac{1}{q_n} < \frac{1}{q_n^\epsilon}$$

Also,  $\frac{p_n}{q_n} = \frac{p}{q} + \frac{1}{nq}$  so these solutions are all distinct. Thus, there are infinitely many  $\epsilon$ -good approximations of  $\alpha$  so  $\mu(\alpha) \geq \epsilon$  for every  $\epsilon < 1$  so  $\mu(\alpha) \geq 1$ . Furthermore,  $\alpha = \frac{p}{q}$  solves  $f(x) = qx - p$  which has degree 1 so  $\mu(\alpha) \leq 1$ . Therefore,  $\mu(\alpha) = 1$ .  $\square$

**Proposition.** If  $\alpha \in \mathbb{R} \setminus \mathbb{Q}$  then  $\mu(\alpha) \geq 2$ .

*Proof.* This follows immediately from Dirichlet's approximation lemma. Since  $\alpha \in \mathbb{R} \setminus \mathbb{Q}$  then  $|G_2(\alpha)| = \infty$  meaning that,

$$\mu(\alpha) = \sup\{n \in \mathbb{R}^+ \mid |G_n(\alpha)| = \infty\} \geq 2$$

$\square$

**Proposition.** Let  $\alpha$  be algebraic of degree  $n$ , then  $\mu(\alpha) \leq n$ .

*Proof.* Suppose that  $\mu(\alpha) > n$ . Then there would exist some  $k > n$  such that  $|G_k(\alpha)| = \infty$  else the supremum would be  $n$ . However,  $\mu(\alpha)$  is algebraic of order  $n$  and  $k > n$  so  $\alpha$  is not  $k$ -approximable. Therefore,  $\mu(\alpha) \leq n$ .  $\square$

**Theorem 4.1** (Roth, 1955). *If  $\alpha$  is irrational algebraic then  $\mu(\alpha) = 2$ .*

**Example 4.1.** The best known upper bound on the irrationality measure of  $\pi$  was given in 2008 by Salikhov as  $\mu(\pi) \leq 7.6063$

**Example 4.2.** Borwein and Borwein proved in 1987 that  $\mu(e) = 2$ .

**Theorem 4.2.** *The image of the irrationality measure is  $\text{Im } \mu = \{1\} \cup [2, \infty]$  and is classified for any  $\alpha \in \mathbb{R}$  via,*

$$\begin{cases} \mu(\alpha) = 1 & \alpha \text{ is rational} \\ \mu(\alpha) = 2 & \alpha \text{ is irrational algebraic} \\ \mu(\alpha) \geq 2 & \alpha \text{ is transcendental} \\ \mu(\alpha) = \infty & \alpha \text{ is Liouville} \end{cases}$$

*Remark 4.0.1.* We will now explore that final class of numbers.

## 5 Liouville Numbers

**Definition:**  $L$  is a *Liouville number* if for every  $n \in \mathbb{Z}^+$  there exists  $\frac{p}{q} \in \mathbb{Q}$  such that,

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^n}$$

**Proposition.**  $L$  is Liouville if and only if  $\mu(L) = \infty$

*Proof.* Let  $\mu(L) = \infty$ . then for any  $n \in \mathbb{Z}^+$  there must be a  $k > n$  such that  $L$  is  $k$ -approximable because  $\mu(L) > n$ . Therefore, there is a solution  $\frac{p}{q} \in \mathbb{Q}$  (in fact infinitely many) to the inequality,

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^k} < \frac{1}{q^n}$$

so  $L$  is Liouville. Conversely, suppose that  $L$  is Liouville. Then take any  $k$  and choose  $n > k$  with  $n \in \mathbb{Z}^+$ . Because  $L$  is Liouville, for each  $n$  there must be a solution  $\frac{p_n}{q_n} \in \mathbb{Q}$  to,

$$0 < \left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n^n} < \frac{1}{p_n^k}$$

Therefore, each  $\frac{p_n}{q_n} \in G_k(L)$ . I claim that this is an infinite number of distinct solutions. Otherwise, there would be a single value  $\frac{p'}{q'}$  which appears infinitely many times. Thus,

$$0 < \left| \alpha - \frac{p'}{q'} \right| < \frac{1}{(q')^n}$$

for infinitely many values of  $n \in \mathbb{Z}^+$  which is impossible because,

$$\left| \alpha - \frac{p'}{q'} \right| \neq 0$$

but  $\frac{1}{(q')^n} \rightarrow 0$ . Therefore,  $|G_k(L)|$  is infinite for every  $k \in \mathbb{R}^+$ . Thus,  $\mu(L) \geq k$  for all  $k \in \mathbb{R}^+$  so  $\mu(L) = \infty$ .  $\square$

**Theorem 5.1.** *Liouville numbers are transcendental.*

*Proof.* Let  $L$  be algebraic then there exists some  $f \in \mathbb{Z}[X]$  such that  $f(L) = 0$ . However, then  $\mu(L) \leq \deg f$  which is finite so  $\mu(L) < \infty$  and thus  $L$  is not Liouville. Thus, if  $L$  is Liouville, then  $L$  is not algebraic so  $L$  is transcendental.  $\square$

**Theorem 5.2.** *Take  $b \in \mathbb{Z}$  with  $b \geq 2$  and  $a_k \in \{0, 1, 2, \dots, b-1\}$  for every  $k \in \mathbb{N}$ , then, the number,*

$$L = \sum_{k=1}^{\infty} \frac{a_k}{b^{k!}}$$

*is Liouville number and thus transcendental. In particular, we have uncountably many explicit examples of transcendental numbers.*



*Proof.* Let  $q_n = b^{n!}$  and  $p_n = q_n \sum_{k=1}^n \frac{a_k}{b^{k!}}$ . By definition,  $\frac{p_n}{q_n}$  is the  $n^{\text{th}}$ -partial sum of  $L$ ,

$$\frac{p_n}{q_n} = \sum_{k=1}^n \frac{a_k}{b^{k!}}$$

Therefore, the difference  $\alpha - \frac{p_n}{q_n}$  is the sum starting at  $n+1$ ,

$$0 < \left| \alpha - \frac{p}{q} \right| = \sum_{k=n+1}^{\infty} \frac{a_k}{b^{k!}} \leq \sum_{k=n+1}^{\infty} \frac{b-1}{b^{k!}}$$

because each  $a_k \leq b-1$ . By setting  $k' = k!$  we can add in terms  $\frac{b-1}{b^{k'}}$  for the remaining values of  $k' \geq (n+1)!$  to get,

$$\begin{aligned} \sum_{k=n+1}^{\infty} \frac{b-1}{b^{k!}} &< \sum_{k'=(n+1)!}^{\infty} \frac{b-1}{b^{k'}} = \frac{b-1}{b^{(n+1)!}} \sum_{m=0}^{\infty} \frac{1}{b^m} \\ &= \frac{b-1}{b^{(n+1)!}} \frac{b}{b-1} = \frac{b}{b^{(n+1)!}} \leq \frac{b^{n!}}{b^{(n+1)!}} \end{aligned}$$

Now,  $(n+1)! - n! = (n+1) \cdot n! - n! = n \cdot n!$  and thus,

$$0 < \left| \alpha - \frac{p_n}{q_n} \right| < \frac{b^{n!}}{b^{(n+1)!}} = \frac{1}{b^{n \cdot n!}} = \frac{1}{(b^{n!})^n} = \frac{1}{q_n^n}$$

Therefore, the inequality,

$$0 < \left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n^n}$$

has a solution for every integer  $n$ . For any  $k$  we can take an integer  $n > k$  so that,

$$0 < \left| \alpha - \frac{p_n}{q_n} \right| < \frac{1}{q_n^n} < \frac{1}{q_n^k}$$

has a solution. □

## 6 Measure Theory of Approximable Numbers

**Definition:** Let  $\psi : \mathbb{Z}^+ \rightarrow \mathbb{R}^+$  be a function. We say that  $\alpha \in \mathbb{R}$  is  $\psi$ -approximable if the set of  $\psi$ -good Diophantine approximations,

$$G_{\psi}(\alpha) = \left\{ \frac{p}{q} \in \mathbb{Q} \mid 0 < \left| \alpha - \frac{p}{q} \right| < \frac{\psi(q)}{q} \right\}$$

is infinite.

**Theorem 6.1** (Khinchin). *Let  $\psi : \mathbb{Z}^+ \rightarrow \mathbb{R}^+$  be a function such that the series,*

$$\sum_{q=1}^{\infty} \psi(q) < \infty$$

*converges then almost no real  $\alpha \in \mathbb{R}$  is  $\psi$ -approximable in the sense that,*

$$A_\psi = \{\alpha \in \mathbb{R} \mid |G_\psi(\alpha)| = \infty\}$$

*has Lebesgue measure zero.*

*Proof.* Define,

$$B(q) = \bigcup_{p \in \mathbb{Z}} \left( \frac{p}{q} - \frac{\psi(q)}{q}, \frac{p}{q} + \frac{\psi(q)}{q} \right)$$

We know that  $\alpha \in A_\psi$  iff  $\alpha \in B(q)$  for infinitely many  $q$ . Thus,  $\alpha \notin A_\psi$  iff there exists a maximum  $q$  such that  $\alpha \in B(q)$  i.e. for some  $N$  and any  $q \geq N$  that  $\alpha \notin B(q)$ . Therefore,

$$A_\psi^C = \bigcup_{N=1}^{\infty} \bigcap_{q=N}^{\infty} B(q)^C$$

and thus we may write,

$$A_\psi = \bigcap_{N=1}^{\infty} \bigcup_{q=N}^{\infty} B(q)$$

Because  $A_\psi$  is translation invariant, it suffices to consider  $\tilde{A}_\psi = A_\psi \cap [0, 1]$ . Furthermore, if  $\psi(q) \geq \frac{1}{2}$  then  $B(q) \cap [0, 1] = [0, 1]$  otherwise,

$$B(q) \cap [0, 1] = [0, \frac{\psi(q)}{q}) \cup (\frac{1}{q} - \frac{\psi(q)}{q}, \frac{1}{q} + \frac{\psi(q)}{q}) \cup \dots \cup (\frac{q-1}{q} - \frac{\psi(q)}{q}, \frac{q-1}{q} + \frac{\psi(q)}{q}) \cup (1 - \frac{\psi(q)}{q}, 1]$$

and thus, in either cases,

$$\mu_{\mathcal{L}}(B(q) \cap [0, 1]) \leq 2\psi(q)$$

Let,

$$W_N = \bigcup_{q=N}^{\infty} B(q) \cap [0, 1]$$

which by subadditivity satisfy,

$$\mu_{\mathcal{L}}(W_N) \leq \sum_{q=N}^{\infty} \mu_{\mathcal{L}}(B(q)) \leq \sum_{q=N}^{\infty} 2\psi(q)$$

Now,

$$\tilde{A}_\psi = \bigcap_{N=1}^{\infty} W_N$$

and therefore we have,

$$\mu_{\mathcal{L}}(\tilde{A}_\psi) \leq \mu_{\mathcal{L}}(W_N) \leq \sum_{q=N}^{\infty} 2\psi(q) \xrightarrow{N \rightarrow \infty} 0$$

because the sum converges and thus,

$$\sum_{q=1}^{\infty} \psi(q) < \infty \implies \sum_{q=N}^{\infty} \psi(q) = \left[ \sum_{q=1}^{\infty} \psi(q) - \sum_{q=1}^{N-1} \psi(q) \right] \rightarrow 0$$

Therefore,

$$\mu_{\mathcal{L}}(\tilde{A}_\psi) = 0$$

which implies by translation invariance and countable additivity that,

$$\mu_{\mathcal{L}}(A_\psi) = 0$$

□

*Remark 6.0.1.* This proof is basically an application of Borel-Cantelli.

**Corollary 6.2.** *Almost all real numbers have  $\mu(\alpha) = 2$  and the set*

$$\{\alpha \in \mathbb{R} \mid \mu(\alpha) > 2\}$$

*has measure zero. In particular, almost all transcendental  $\alpha \in \mathbb{R}$  have  $\mu(\alpha) = 2$ .*

*Proof.* For  $\varepsilon > 0$  let  $\psi(q) = q^{-(1+\varepsilon)}$ . The convergence of,

$$\sum_{q=1}^{\infty} q^{-(1+\varepsilon)} < \infty$$

implies that  $A_{2+\varepsilon} = \{\alpha \in \mathbb{R} \mid |G_{2+\varepsilon}(\alpha)| = \infty\} = \{\alpha \in \mathbb{R} \mid \mu(\alpha) \geq 2 + \varepsilon\}$  has measure zero. Therefore,

$$\{\alpha \in \mathbb{R} \mid \mu(\alpha) > 2\} = \bigcup_{N=1}^{\infty} \{\alpha \in \mathbb{R} \mid \mu(\alpha) \geq 2 + \frac{1}{N}\}$$

has measure zero. In particular, almost all  $\alpha \in \mathbb{R}$  have  $\mu(\alpha) \leq 2$ . However, only countably many  $\alpha \in \mathbb{R}$  have  $\mu(\alpha) < 2$  (exactly the rational ones) so almost all  $\alpha \in \mathbb{R}$  have  $\mu(\alpha) = 2$ . □

**Lemma 6.3.** *For any  $\alpha \in \mathbb{R}$  and  $r \in \mathbb{Q}$  we have  $\mu(\alpha + r) = \mu(r \cdot \alpha) = \mu(\alpha)$ .*

*Proof.* Let  $r = \frac{a}{b} \in \mathbb{Q}$  and  $s = \mu(\alpha)$  then  $\forall \varepsilon > 0$  then  $|G_{s-\varepsilon}(\alpha)| = \infty$  thus there are infinitely many  $\frac{p}{q} \in \mathbb{Q}$  such that,

$$0 < \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^{s-\varepsilon}}$$

and therefore,

$$0 < \left| \left( \alpha + \frac{a}{b} \right) - \left( \frac{a}{b} + \frac{p}{q} \right) \right| < \frac{1}{q^{s-\varepsilon}} = \frac{1}{q^\varepsilon q^{s-2\varepsilon}}$$

Now choose  $q$  sufficiently large such that  $q^\varepsilon > b^s$ . Because there are infinitely many solutions we will still have infinitely many solutions with this additional requirement and then,

$$0 < \left| \left( \alpha + \frac{a}{b} \right) - \frac{aq + pb}{bq} \right| < \frac{1}{q^\varepsilon q^{s-2\varepsilon}} < \frac{1}{b^s q^{s-2\varepsilon}} < \frac{1}{(bq)^{s-2\varepsilon}}$$

Therefore,  $|G_{s-2\varepsilon}(\alpha + r)| = \infty$  so  $\mu(\alpha + r) \geq s - 2\varepsilon$  for any  $\varepsilon > 0$ . Thus,  $\mu(\alpha + r) \geq \mu(\alpha)$ . Since rational addition is inevitable we must have  $\mu(\alpha + r) = \mu(\alpha)$ . Furthermore, consider,

$$0 < \left| \frac{a}{b}\alpha - \frac{ap}{bq} \right| < \frac{a}{bq^{s-\varepsilon}} = \frac{a}{b} \frac{1}{q^\varepsilon} \frac{1}{q^{s-2\varepsilon}}$$

Again choose  $q$  sufficiently large such that  $q^\varepsilon > ab^{s-1}$ . Since there are infinitely many solutions we will still have infinitely many solutions with this additional requirement and then,

$$0 < \left| \frac{a}{b}\alpha - \frac{ap}{bq} \right| < \frac{a}{b} \frac{1}{q^\varepsilon} \frac{1}{q^{s-2\varepsilon}} < \frac{1}{b^s} \frac{1}{q^{s-2\varepsilon}} < \frac{1}{(bq)^{s-2\varepsilon}}$$

Therefore,  $|G_{s-2\varepsilon}(r \cdot \alpha)| = \infty$  so  $\mu(r \cdot \alpha) \geq s - 2\varepsilon$  for any  $\varepsilon > 0$  which implies that  $\mu(r \cdot \alpha) \geq \mu(\alpha)$  as before  $\mu(r \cdot \alpha) = \mu(\alpha)$  by inversion.  $\square$

**Corollary 6.4.** *For any  $m \in \text{Im } \mu$  the set  $\mu^{-1}(m) = \{\alpha \in \mathbb{R} \mid \mu(\alpha) = m\}$  is dense.*

*Proof.* Since  $m \in \text{Im } \mu$  the preimage is nonempty. Choose any nonzero  $\alpha \in \mu^{-1}(m)$  (zero is only in preimage of 1 which also includes all rational numbers). Take any interval  $(a, b) \subset \mathbb{R}$ . Then consider the interval  $(a/|\alpha|, b/|\alpha|) \subset \mathbb{R}$  which must contain a rational:  $r \in (a/|\alpha|, b/|\alpha|) \cap \mathbb{Q}$ . Then by the above,  $r \cdot \alpha \in (a, b)$  and  $\mu(r \cdot \alpha) = \mu(\alpha) = m$  so  $\mu^{-1}(m) \cap (a, b) \neq \emptyset$ . Thus,  $\mu^{-1}(m)$  is dense.  $\square$

**Theorem 6.5.** *Liouville numbers form a dense uncountable measure zero transcendental subset of  $\mathbb{R}$ .*

*Remark 6.0.2.* The Hausdorff (fractal) dimension of  $A_{1+c}$  is  $1/c$  showing that  $A_2$  which includes almost all numbers has the dimension of the real line. The Hausdorff dimension then decreases as we look at better approximable sets. Finally the Hausdorff dimension of the Liouville numbers is zero showing that they are measure theoretically point-like. However, the Hausdorff dimension of the very well-approximable numbers i.e. those with  $\mu(\alpha) > 2$  is also one. Finally, almost every number is well-approximable but the Hausdorff dimension of the badly-approximable numbers is one.