Como medir a irracionalidade de um número:

a medida de irracionalidade de Liouville-Roth e suas consequências

Marcelo Simis Muniz

26 de novembro de 2025

1 Aproximação por Racionais e Medida de Irracionalidade

Definição 1.1. *Um número real α é dito ser aproximado por racionais por ordem μ se existe uma constante $k(\alpha)$, possivelmente dependendo de α, tal que a inequação*

$$\left|\alpha - \frac{p}{q}\right| < \frac{k(\alpha)}{q^\mu}$$

possui infinitas soluções com p e q primos entre si e $q > 0$.

É importante notar que essa definição implica, como esperamos para qualquer aproximação, que qualquer sequência $\left\{\frac{p_n}{q_n}\right\}_{n\in\mathbb{N}}$ que a satisfaça necessariamente converge para α, uma vez que, para infinitos racionais distintos, é necessário que $|p_n| \to \infty$ ou $q_n \to \infty$. Todavia, se apenas $|p_n| \to \infty$, a inequação não terá infinitas soluções, pois neste caso $\left|\alpha - \frac{p_n}{q_n}\right| \to \infty \Rightarrow \exists n_0 \in \mathbb{N}$ tal que $\left|\alpha - \frac{p_{n_0}}{q_{n_0}}\right| \geq \frac{k(\alpha)}{q_{n_0}^\mu}$. Logo, $q_n \to \infty$ e, por consequência, $\left|\alpha - \frac{p_n}{q_n}\right| \to 0$.

Definição 1.2. *A medida de irracionalidade de Liouville-Roth (ou expoente de irracionalidade) de um número real α é definida como:*

$$\mu_{\mathcal{L}}(\alpha) = \sup\left\{\mu : \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\mu} \text{ tem infinitas soluções com } p \text{ e } q \text{ primos entre si e } q > 0\right\}$$

Observe que o conjunto cujo supremo é o expoente de irracionalidade é necessariamente um intervalo, pois $\forall \mu_1, \mu_2$ tais que $0 \leq \mu_1 < \mu_2$, temos que $\frac{1}{q^{\mu_1}} > \frac{1}{q^{\mu_2}}$ e, portanto, se μ_2 fornece infinitas soluções, as mesmas soluções funcionarão para qualquer número real no intervalo $[0, \mu_2]$.

É evidente a relação entre as definições: a medida de irracionalidade de um número real é necessariamente menor ou igual à maior ordem pela qual este número pode ser aproximado. Além disso, a medida de irracionalidade está diretamente relacionada com a facilidade de aproximar um número real por racionais distintos — quanto maior a medida, "melhores" as aproximações.

A princípio, essa ideia dá a entender que a medida de irracionalidade de um número racional seria infinita, uma vez que um racional pode ser perfeitamente aproximado por números racionais. No entanto, é necessário notar que a definição exige que os racionais que aproximam o número em questão sejam distintos entre si - e aproximar um racional por racionais distintos não é tão eficiente. Disso, decorre a seguinte proposição:

Proposição 1.1. *O expoente de irracionalidade de um número racional $\frac{a}{b}$ é igual a 1.*

Demonstração. Vamos dividir essa demonstração em duas partes: primeiro, provaremos que a medida de irracionalidade de $\frac{a}{b}$ é ≥ 1. Em seguida, provaremos que a medida de irracionalidade é ≤ 1, e, por consequência, tal medida deve ser exatamente igual a 1. Ademais, assumiremos sem perda de generalidade que $b > 0$ e que a e b são primos entre si.

Para a primeira parte, considere a sequência de racionais $\left\{\frac{p_n}{q_n}\right\}_{n\in\mathbb{N}\setminus\{0,1\}}$, definida da seguinte forma:

$$\begin{cases} p_n = n \cdot a - 1 \\ q_n = n \cdot b \end{cases}$$

Note que

$$\left|\frac{a}{b} - \frac{p_n}{q_n}\right| = \left|\frac{a}{b} - \frac{n\cdot a - 1}{n \cdot b}\right| = \left|\frac{a\cdot(n\cdot b) - (n\cdot a + 1)\cdot b}{n \cdot b^2}\right| = \left|\frac{b}{n \cdot b^2}\right|$$

Como $b > 0$, temos:

$$\left|\frac{a}{b} - \frac{p_n}{q_n}\right| = \frac{b}{n \cdot b^2} = \frac{1}{n \cdot b} = \frac{1}{q_n}$$

Ora, como $q_n > 1$ (pois $n > 1$), então $\forall \varepsilon \in (0,1)$ vale que

$$q_n > {q_n}^{\varepsilon} \Rightarrow \frac{1}{q_n} < \frac{1}{{q_n}^{\varepsilon}} \Rightarrow \left|\frac{a}{b} - \frac{p_n}{q_n}\right| < \frac{1}{{q_n}^{\varepsilon}}$$

Observe que, mesmo que p_n e q_n não sejam primos entre si, i.e., se existir $\frac{p'_n}{q'_n} = \frac{p_n}{q_n}$ com $q'_n < q_n$, teremos que $\frac{1}{q'_n} > \frac{1}{q_n}$ e, portanto,

Ora, mas segue da definição 1.1 que $q \to \infty$. Portanto, chegamos em uma contradição ($q^{\mu-1} \to \infty$ e $q^{\mu-1} < b$, ou seja, há apenas uma quantidade finita de soluções se o expoente é maior que 1), e $\mu \leq 1$. Dessa forma, $\mu = 1$. □

A seguir, demonstramos também algumas propriedades fundamentais dessa medida de irracionalidade:

Proposição 1.2. *Se x pode ser aproximado por racionais por ordem μ, então $\forall m \in \mathbb{Z}$, vale o mesmo para $x + m$.*

Demonstração. Ora, se x é aproximado por racionais por ordem μ, então existe uma constante $k(x)$ e uma sequência com infinitos elementos distintos $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ tal que

$$\left|x - \frac{p_n}{q_n}\right| < \frac{k(x)}{{q_n}^{\mu}}$$

para todo $n \in \mathbb{N}$. Trivialmente, temos que

$$\left|(x+m) - \frac{p_n + (m \cdot q_n)}{q_n}\right| < \frac{k(x)}{{q_n}^{\mu}}$$

Dessa forma, mesmo que $p_n + (m \cdot q_n)$ e q_n não sejam primos entre si, basta tomar a forma simplificada $\frac{p'_n}{q'_n}$, com $q'_n < q_n$, e teremos $\left|(x+m) - \frac{p'_n}{q'_n}\right| < \frac{k(x)}{{q_n}^{\mu}} < \frac{k(x)}{{q'_n}^{\mu}}$. Ademais, a sequência $\left(\frac{p_n+(m\cdot q_n)}{q_n}\right)_{n\in\mathbb{N}}$ possui infinitos elementos distintos, uma vez que $\frac{p_a}{q_a} \neq \frac{p_b}{q_b} \Rightarrow \frac{p_a+m\cdot q_a}{q_a} \neq \frac{p_b+m\cdot q_b}{q_b}$. Isso significa que $x + m$ pode ser aproximado por racionais por ordem μ. □

Proposição 1.3. *Se α pode ser aproximado por racionais por ordem μ, então $\mu_{\mathcal{L}}(\alpha) \geq \mu$.*

Demonstração. Queremos provar que, se $|\alpha - p/q| < k(\alpha)/q^{\mu}$ tem infinitas soluções racionais distintas com $q > 0$, então para qualquer $\nu < \mu$, a inequação $|\alpha - p/q| < 1/q^{\nu}$ também terá.

Seja então $\varepsilon > 0$. Mostraremos que a desigualdade

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

possui infinitas soluções. Seja $(p_k, q_k)_{k\in\mathbb{N}}$ uma sequência arbitrária de soluções distintas para

$$\left|\alpha - \frac{p_k}{q_k}\right| < \frac{1}{q_k^{\mu}} \tag{2}$$

Note que a desigualdade (2) implicará (1) se

$$\frac{k(\alpha)}{q_k^{\mu}} \leq \frac{1}{q_k^{r-\varepsilon}} \iff c \leq \frac{q_k^{\mu}}{q_k^{\mu-\varepsilon}} \iff c \leq q_k^{\varepsilon}$$

Como $q_k \to \infty$, para todo $\epsilon > 0$ existe uma subsequência de $(p_k, q_k)_{k\in\mathbb{N}}$ que satisfaz (1). Logo, para todo $\nu < \mu$, $|\alpha - p/q| < 1/q^{\nu}$ tem infinitas soluções distintas, e

$$\sup\left\{\nu : \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{\nu}} \text{ tem infinitas soluções com } p \text{ e } q \text{ primos entre si e } q > 0\right\} \geq \mu$$

□

Teorema 1.4 (Teorema da aproximação de Dirichlet)**.** *O expoente de irracionalidade de um número irracional α é maior ou igual a 2.*

Demonstração. Seja α irracional e N natural. Ora, então para cada $k = 0, 1, ..., N$ podemos escrever $k \cdot \alpha = m_k + x_k$, com m_k inteiro e $x_k \in [0, 1)$. Ao mesmo tempo, é possível dividir $[0, 1)$ em N intervalos de tamanho $\frac{1}{N}$

Note que, como α é irracional, temos $N + 1$ números $x_0, x_1, ..., x_N$, todos distintos. Isso decorre do fato que, se α é irracional, então não existem $(a, b) \in \mathbb{N}^* \times \mathbb{N}$ tais que $a \cdot \alpha - b \in \mathbb{N}$ (se existissem, então existiriam $(a, b, c) \in \mathbb{N}^* \times \mathbb{N} \times \mathbb{N}$ tais que $\alpha = \frac{c+b}{a}$, e α seria racional).

Ao mesmo tempo, temos também N intervalos de tamanho $\frac{1}{N}$. É evidente, portanto, que pelo menos dois destes números estão em um único intervalo, isto é, $\exists i\ \exists j\ (0 \leq i < j \leq N)$ tais que

$$|x_j - x_i| < \frac{1}{N}$$

Voltando à definição de cada x_k, temos:

$$x_k = k \cdot \alpha - m_k \Rightarrow |(j \cdot \alpha - m_j) - (i \cdot \alpha - m_i)| < \frac{1}{N} \text{ , com } m_i \text{ e } m_j \text{ inteiros}$$

Reescrevemos a expressão anterior:

$$|(j - i) \cdot \alpha - (m_j - m_i)| < \frac{1}{N} \Rightarrow \left|\alpha - \frac{m_j - m_i}{j - i}\right| < \frac{1}{(j - i) \cdot N}$$

Note que, por definição, $i < j \leq N$ e, portanto, $0 < (j - i) \leq N$. Logo,

$$\left|\alpha - \frac{m_j - m_i}{j - i}\right| < \frac{1}{(j - i)^2}$$

Resta, todavia, provar que temos infinitas soluções distintas. Ora, como $\alpha \notin \mathbb{Q}$, então

$$\left|\alpha - \frac{m_j - m_i}{j - i}\right| = x > 0$$

Ao mesmo tempo,

$$\left|\alpha - \frac{m_j - m_i}{j - i}\right| = x < \frac{1}{(j - i) \cdot N}$$

Como N é arbitrário, e pode ser escolhido tão grande quanto se queira, temos que $\frac{1}{(j-i)\cdot N} \to 0$. Ora, então se existirem finitas soluções, podemos tomar x_0 como o menor módulo da diferença entre as soluções e α. Teríamos:

$$\begin{cases} x_0 > 0 \\ x_0 < \frac{1}{(j-i)\cdot N} \forall N \end{cases}$$

Que, evidentemente, é uma contradição.

Conseguimos, portanto, infinitos racionais de forma $\frac{m_j - m_i}{j-i}$ (bastando variar N para variar os racionais) que satisfazem à condição para que o número 2 pertença ao conjunto cujo supremo é a medida de irracionalidade. □

Teorema 1.5 (Teorema de Liouville)**.** *Seja x um número algébrico de grau n. Então x pode ser aproximado por racionais por ordem no máximo n.*

Demonstração. Seja x um algébrico irracional, e $f(X) = a_n \cdot X^n + \cdots + a_1 \cdot X + a_0$ o polinômio minimal (i.e., com coeficientes inteiros e de menor grau) que satisfaz $f(x) = 0$. Ora, por definição, f é irredutível sobre $\mathbb{Z}$ e, por consequência, irredutível sobre $\mathbb{Q}$. Em particular, se f é irredutível sobre $\mathbb{Q}$, então f não possui raízes racionais (uma vez que, se possuísse uma raiz racional $\frac{a}{b}$, seria divisível por $X - \frac{a}{b}$)

Sejam agora

$$M = \sup_{|z-x|<1} \{|f'(z)|\} \text{ , e } \frac{p}{q} \text{ um racional tal que } \left|x - \frac{p}{q}\right| < 1 \text{ com } q > 0$$

O Teorema do Valor Médio nos garante que existe c entre x e $\frac{p}{q}$ tal que

$$\left|\frac{f\left(\frac{p}{q}\right)-f(x)}{\frac{p}{q}-x}\right| = |f'(c)| \Rightarrow \left|f\left(\frac{p}{q}\right)-f(x)\right| = \left|f'(c)\left(x-\frac{p}{q}\right)\right|$$

Note que $|c-x|<1$ e, portanto, $|f'(c)|<M$. Logo,

$$\left|f\left(\frac{p}{q}\right)-f(x)\right| \leq M\cdot\left|x-\frac{p}{q}\right|, \text{ sempre que } \frac{p}{q}\in(x-1,x+1) \tag{3}$$

Todavia, sabemos que f não possui raízes racionais. Temos:

$$f\left(\frac{p}{q}\right) = a_n\left(\frac{p}{q}\right)^n+\cdots+a_0 = \frac{a_n\cdot p^n+\cdots+a_1\cdot p\cdot q^{n-1}+a_0\cdot q^n}{q^n} \neq 0 \Rightarrow$$

$$\Rightarrow a_n\cdot p^n+\cdots+a_1\cdot p\cdot q^{n-1}+a_0\cdot q^n \in \mathbb{Z}\backslash\{0\}$$

Ao mesmo tempo, $f(x)=0$ por definição. Logo,

$$\left|f\left(\frac{p}{q}\right)-f(x)\right| = \left|f\left(\frac{p}{q}\right)\right| = \frac{\left|a_n\cdot p^n+\ldots+a_1\cdot p\cdot q^{n-1}+a_0\cdot q^n\right|}{q^n} \geq \frac{1}{q^n} \tag{4}$$

Combinando (1) e (2), temos:

$$M\cdot\left|x-\frac{p}{q}\right| \geq \frac{1}{q^n} \Rightarrow \left|x-\frac{p}{q}\right| \geq \frac{1}{M\cdot q^n} \tag{5}$$

Isso é o suficiente para provar que x pode ser aproximado por racionais por ordem, no máximo n, pois, supondo que não o fosse, teríamos uma sequência infinita $\left\{\frac{p_i}{q_i}\right\}_{i\geq 1}$ e uma constante $k(x)$ tais que

$$\left|x-\frac{p_i}{q_i}\right| < \frac{k(x)}{q_i^{n+\varepsilon}}, \text{ com } \varepsilon>0$$

Ora, a sequência $\left\{\frac{p_i}{q_i}\right\}_{i\geq 1}$ deve convergir a x por definição. Podemos, portanto, tomar $\frac{p_i}{q_i}$ como contida no intervalo $(x-1,x+1)$. Dessa forma, $\frac{p_i}{q_i}$ satisfaz às condições de (1), e vale o resultado de (3):

$$\frac{1}{q_i^n} \leq M\cdot\left|x-\frac{p_i}{q_i}\right| \Rightarrow \frac{1}{M\cdot q_i^n} \leq \left|x-\frac{p_i}{q_i}\right|$$

Combinando estas duas últimas inequações, temos:

$$\frac{1}{M\cdot q_i^n} < \frac{k(x)}{q_i^{n+\varepsilon}} \Rightarrow \frac{1}{k(x)\cdot M\cdot q_i^n} < \frac{1}{q_i^{n+\varepsilon}} \Rightarrow \frac{1}{k(x)\cdot M} < \frac{1}{q_i^{\varepsilon}} \Rightarrow q_i^{\varepsilon} < k(x)\cdot M$$

Ora, mas $q_i\to\infty$ por consequência da definição 1.1. Temos, portanto, uma contradição: existe A fixo tal que $q_i<A$ para todo i, mas q_i tende ao infinito. Por conta disso, x deve ser aproximado por racionais a grau, no máximo, n. □

Uma aplicação particularmente interessante do Teorema 1.5 decorre de notar que, se um número é algébrico, então a maior ordem pela qual ele pode ser aproximado por racionais é finita. Se conseguirmos encontrar um número que pode ser aproximado por racionais a uma ordem tão grande quanto se queira, portanto, este número é necessariamente transcendental.

1.1 Construindo números transcendentais

Definição 1.3. *Se, para todo $n\in\mathbb{N}$ arbitrariamente grande, a inequação $0<\left|\alpha-\frac{p}{q}\right|<\frac{k(\alpha)}{q^n}$ possui uma solução, dizemos que α é aproximado por racionais por ordem infinita. Se $k(\alpha)=1$, então temos que $\mu_{\mathcal{L}}(\alpha)=\infty$. (Note: esta definição é equivalente a dizer que há infinitas soluções para cada n, pois quando $n\to\infty$, $\frac{k(\alpha)}{q^n}\to 0$, mas $0<\left|\alpha-\frac{p}{q}\right|$, resultando em infinitas soluções de forma $\frac{p}{q}$).*

Motivados pelo Teorema 1.5 e também pela definição 1.3, nosso objetivo agora é encontrar um número real que seja aproximado por racionais por ordem infinita, garantindo portanto que este seja transcendental.

Considere a série

$$\sum_{m=1}^{\infty} \frac{1}{10^{m!}}$$

É evidente que a série é convergente, pois $\frac{1}{10^m} \geq \frac{1}{10^{m!}} \; \forall \; m \in \mathbb{N}$. Seja, portanto, $x = \sum_{m=1}^{\infty} \frac{1}{10^{m!}}$. Seja $N \in \mathbb{N}$ fixado e $n > N$. Definimos:

$$\frac{p_n}{q_n} = \sum_{m=1}^{n} \frac{1}{10^{m!}}, \text{ com } p_n, q_n > 0 \text{ e primos entre si.}$$

Note que q_n deve dividir $10^{n!}$, pois

$$\frac{p_n}{q_n} = \frac{1}{10^{1!}} + \frac{1}{10^{2!}} \cdots + \frac{1}{10^{n!}} = \frac{10^{n!-1!}}{10^{n!}} + \frac{10^{n!-2!}}{10^{n!}} + \ldots \frac{1}{10^{n!}} \Rightarrow$$

$$\Rightarrow \exists K \in \mathbb{N} \text{ tal que } \frac{p_n}{q_n} = \frac{K}{10^{n!}}$$

Como p_n, q_n são primos entre si, q_n deve dividir $10^{n!}$ e, portanto,

$$q_n \leq 10^{n!} \tag{6}$$

Além disso, $\left\{\frac{p_n}{q_n}\right\}$ converge monotonicamente em direção a x. Logo, temos:

$$0 < x - \frac{p_n}{q_n} = \sum_{m>n}^{\infty} \frac{1}{10^{m!}} = \frac{1}{10^{(n+1)!}} \left(1 + \frac{1}{10^{n+2}} + \frac{1}{10^{(n+2)(n+3)}} + \ldots\right)$$

Note que

$$1 + \frac{1}{10^{n+2}} + \frac{1}{10^{(n+2)(n+3)}} + \cdots < 1 + \frac{1}{10^1} + \frac{1}{10^2} + \cdots < 2$$

Logo,

$$x - \frac{p_n}{q_n} < \frac{2}{(10^{n!})^{n+1}}$$

Usando (4), temos, portanto, que

$$0 < x - \frac{p_n}{q_n} < \frac{2}{q_n^{n+1}} < \frac{2}{q_n^N}$$

Como N pode ser escolhido arbitrariamente grande, x pode ser aproximado por racionais a uma ordem tão grande quanto se queira, uma vez que $i \neq j \Rightarrow \frac{p_i}{q_i} \neq \frac{p_j}{q_j}$ por definição. Por consequência do Teorema 1.5, x é transcendental.

Considere agora a seguinte família de funções:

$$\begin{aligned} d_n : \mathbb{R} &\longrightarrow \mathbb{N} \\ x &\longmapsto \text{n-ésimo dígito decimal de } x \end{aligned}$$

Por exemplo: $d_1(\pi) = 1$, $d_2(\pi) = 4$ e assim sucessivamente. É evidente que

$$d_n(x) \leq 9 \; \forall \; x \in \mathbb{R} \; \forall \; n \in \mathbb{N}$$

Dessa forma, dado um número real x, considere a seguinte série:

$$\sum_{m=1}^{\infty} \frac{d_m(x)}{10^{m!}}$$

É evidente que trata-se de uma série convergente, pois $d_m(x) \leq 9$, e a série $\sum_{m=1}^{\infty} \frac{1}{10^{m!}}$ é convergente. Seja, então,

$$L_x = \sum_{m=1}^{\infty} \frac{d_m(x)}{10^{m!}}$$

Note que podemos repetir a mesma demonstração que prova que x é transcendental, apenas alterando a constante:

$$0 < L_x - \frac{p'_n}{q'_n} \leq \sum_{m>n}^{\infty} \frac{9}{10^{m!}} = \frac{9}{10^{(n+1)!}} \left(1 + \frac{1}{10^{n+2}} + \frac{1}{10^{(n+2)(n+3)}} + \dots\right) \Rightarrow$$

$$\Rightarrow L_x - \frac{p'_n}{q'_n} < \frac{18}{\left(10^{n!}\right)^{n+1}}$$

E, concluindo da mesma forma,

$$0 < L_x - \frac{p'_n}{q'_n} < \frac{18}{{q'_n}^{n+1}} < \frac{18}{{q'_n}^{N}}$$

O que significa que L_x também é transcendental, pois pode ser aproximado por racionais a uma ordem tão grande quanto se queira. No caso de uma representação decimal finita para x, basta escolher sua representação decimal infinita — ou seja, no lugar de $0,3$, usamos $0,2999\dots$

Além disso, podemos somar a parte inteira de x a L_x, e o número continuará sendo transcendental. Podemos, portanto, notar uma clara bijeção entre o conjunto dos números reais e esse conjunto de números transcendentais, que formam um subconjunto dos chamados Números de Liouville. O número associado a π, por exemplo, seria $3.14000100000000000000000005\dots$, com o próximo digito de π ocorrendo após $5! - 4! - 1$ zeros.

Mais que isso, é possível provar que esses números possuem expoente de irracionalidade infinito, i.e., para N arbitrariamente grande, $\left|L_x - \frac{p}{q}\right| < \frac{1}{q^N}$ possui infinitas soluções com p, q primos entre si. Isso decorre de generalizar a forma destes números para qualquer base b:

Teorema 1.6. *Dado $b \geq 2$, qualquer número de forma $\sum_{k=1}^{\infty} \frac{a_k}{b^{k!}}$, onde $a_k \in \{0, 1, ..., b-1\} \forall k$, com $(a_k)_{k\in\mathbb{N}}$ eventualmente não-nula (i.e., $\exists K$ tal que $\forall k' \geq K$, $a_{k'} \neq 0$), possui expoente de irracionalidade infinito.*

Demonstração. Note que todas as séries de forma $\sum_{k=1}^{\infty} \frac{a_k}{b^{k!}}$ serão convergentes com as condições impostas pelo teorema, pois serão dominadas pela série $\sum_{k=1}^{\infty} \frac{b-1}{b^k} = (b-1) \cdot \sum_{k=1}^{\infty} \frac{1}{b^k}$.

Considere agora, com $n \geq 1$, a sequência $\frac{p_n}{q_n}$, na qual

$$\begin{cases} q_n = b^{n!} \\ p_n = b^{n!} \cdot \sum_{k=1}^{n} \frac{a_k}{b^{k!}} = \sum_{k=1}^{n} a_k \cdot b^{n!-k!} \end{cases}$$

Note que $\frac{p_n}{q_n} = \sum_{k=1}^{n} \frac{a_k}{b^{k!}}$. Ora, então se $x = \sum_{k=1}^{\infty} \frac{a_k}{b^{k!}}$, temos:

$$0 < x - \frac{p_n}{q_n} = x - \sum_{k=1}^{n} \frac{a_k}{b^{k!}} = \sum_{k=1}^{\infty} \frac{a_k}{b^{k!}} - \sum_{k=1}^{n} \frac{a_k}{b^{k!}} = \sum_{k=n+1}^{\infty} \frac{a_k}{b^{k!}} \leq \sum_{k=n+1}^{\infty} \frac{b-1}{b^{k!}} < \sum_{k=(n+1)!}^{\infty} \frac{b-1}{b^k} =$$

$$= \frac{b-1}{b^{(n+1)!}} + \frac{b-1}{b^{(n+1)!+1}} + \dots = \frac{b-1}{b^{(n+1)!}b^0} + \frac{b-1}{b^{(n+1)!}b^1} + \dots =$$

$$= \frac{b-1}{b^{(n+1)!}} \cdot \sum_{k=0}^{\infty} \frac{1}{b^k} = \frac{b-1}{b^{(n+1)!}} \cdot \frac{b}{b-1} = \frac{b}{b^{(n+1)!}} \leq$$

$$\leq \frac{b^{n!}}{b^{(n+1)!}} = \frac{1}{b^{(n+1)!-n!}} = \frac{1}{b^{(n+1)\cdot n!-n!}} = \frac{1}{b^{n\cdot n!+n!-n!}} = \frac{1}{b^{n\cdot n!}} = \frac{1}{(b^{n!})^n} = \frac{1}{{q_n}^n}$$

Ora, então para qualquer $n \in \mathbb{N}$, encontramos infinitos racionais distintos e com denominador e numerador primos entre si, e $\mu_{\mathcal{L}}(x) = \infty$

Note que só podemos garantir $x - \frac{p_n}{q_n} \neq 0$ e que $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ possui infinitos elementos distintos se $(a_n)_{n\in\mathbb{N}}$ não for eventualmente zero, e, por isso, é necessário usar o "truque" da representação decimal infinita descrito na construção acima. □

Como consequência dos Teoremas 1.2 e 1.6, notamos que os números descritos na construção feita no início desta subseção são todos transcendentais e, mais que isso, possuem medida de irracionalidade de Liouville-Roth infinita. Essa segunda propriedade nos revela uma propriedade ainda mais surpreendente deste conjunto de números: sua medida de Lebesgue é igual zero.

Evidentemente, não pretendemos realizar uma explicação detalhada de teoria da medida. De maneira geral, quando tratamos de subconjuntos dos números reais, a medida de Lebesgue busca quantificar seu comprimento: os intervalos $[0, 1]$ e $(0, 1)$ possuem medida igual a 1, por exemplo, mesmo contendo o mesmo número de elementos (i.e., cardinalidade) de $\mathbb{R}$, enquanto pontos "isolados" (i.e., elementos de $\{\{x\} : x \in \mathbb{R}\}$) possuem medida zero. Ademais, qualquer união enumerável de conjuntos de medida de Lebesgue zero possui, também, medida zero — qualquer subconjunto enumerável de $\mathbb{R}$, portanto, possui medida zero. Por fim, algumas propriedades intuitivas são verdadeiras: a medida de Lebesgue é ≥ 0 para qualquer subconjunto mensurável de $\mathbb{R}$; e, se B tem medida de Lebesgue zero, todo subconjunto $A \subset B$ também tem medida de Lebesgue zero. Nem todo conjunto é mensurável — todavia, isso foge ao assunto deste trabalho.

Para provar que o conjunto dos números construídos nesta subseção têm medida de Lebesgue zero, é interessante considerar um conjunto ainda maior: o de todos os números reais com medida de irracionalidade infinita. Isso motiva a seguinte definição:

Definição 1.4. *O conjunto dos números de Liouville, $\mathcal{L}$, é definido da seguinte forma:*

$$\mathcal{L} = \{x \in \mathbb{R} : \mu_{\mathcal{L}}(x) = \infty\}$$

Desta forma, se provarmos que $\mathcal{L}$ possui medida de Lebesgue zero, o conjunto dos números que construímos também terá.

Precisamos, ainda, de uma uma ferramenta para provar que medida de Lebesgue de um conjunto é zero. Por mais que a construção de tal medida em geral seja complexa, as propriedades descritas acima levam, de certa forma, à intuição de que, se conseguirmos cobrir um conjunto com uma união enumerável de intervalos cuja soma dos comprimentos seja tão pequeno quanto se queira, então esse conjunto terá medida de Lebesgue zero. Formalizando essa ideia, temos a seguinte proposição:

Proposição 1.7. *Um conjunto A tem medida de Lebesgue zero se $\forall \varepsilon > 0$ existe uma coleção de intervalos abertos $\{I_n \subset \mathbb{R} : n \in \mathbb{N}\}$ tal que*

$$A \subset \bigcup_{i=1}^{\infty} I_i \ , \ e \ \sum_{i=1}^{\infty} \ell(I_i) < \varepsilon$$

com $\ell(I_i)$ denotando o comprimento de cada intervalo - i.e., $\ell((a, b)) = b - a$.

A demonstração dessa proposição pode ser facilmente encontrada em livros de análise real ou mesmo de cálculo, mas foge ao tema deste trabalho. Dessa forma, o leitor pode tomá-la como uma definição. Com isso, podemos provar o seguinte teorema:

Teorema 1.8. *A medida de Lebesgue de $\mathcal{L}$, $\ell(\mathcal{L})$, é igual a zero.*

Demonstração. Considere a seguinte família de conjuntos, com $(p, q, n) \in \mathbb{Z} \times \mathbb{N}\backslash\{0, 1\} \times \mathbb{N}\backslash\{0, 1, 2\}$:

$$V_{n,q} = \bigcup_{p\in\mathbb{Z}} \left(\frac{p}{q} - \frac{1}{q^n}, \frac{p}{q} + \frac{1}{q^n}\right)$$

Note que, por definição, todo Número de Liouville L,= pertence a $\left(\frac{p}{q} - \frac{1}{q^n}, \frac{p}{q} + \frac{1}{q^n}\right)$ para algum $\frac{p}{q}$ para todo n. Logo, para todo n,

$$\mathcal{L} \subset \bigcup_{q=2}^{\infty} V_{n,q}$$

Consideremos, agora, os conjuntos de elementos L de $\mathcal{L}$ tais que $|L| < m$ para algum $m \in \mathbb{N}$. Cada conjunto desses poderá ser descrito por

$$\mathcal{L} \cap (-m, m) \subset \bigcup_{q=2}^{\infty} V_{n,q} \cap (-m, m)$$

Voltando à definição de $V_{n,q}$, obtemos:

$$\bigcup_{q=2}^{\infty} V_{n,q} \cap (-m, m) = \bigcup_{q=2}^{\infty} \bigcup_{p \in \mathbb{Z}} \left(\frac{p}{q} - \frac{1}{q^n}, \frac{p}{q} + \frac{1}{q^n} \right) \cap (-m, m) \subset \bigcup_{q=2}^{\infty} \bigcup_{p=-m \cdot q}^{m \cdot q} \left(\frac{p}{q} - \frac{1}{q^n}, \frac{p}{q} + \frac{1}{q^n} \right)$$

Seja

$$W_{n,m} = \bigcup_{q=2}^{\infty} V_{n,q} \cap (-m, m)$$

Note que

$$\mathcal{L} \subset \bigcup_{q=2}^{\infty} V_{n,q} \Rightarrow \mathcal{L} \cap (-m, m) \subset \bigcup_{q=2}^{\infty} V_{n,q} \cap (-m, m) = W_{n,m}$$

Note que $\left(\frac{p}{q} + \frac{1}{q^n} \right) - \left(\frac{p}{q} - \frac{1}{q^n} \right) = \frac{2}{q^n}$. Portanto, a soma dos comprimentos dos intervalos contidos em $W_{n,m}$, será menor ou igual a

$$\sum_{q=2}^{\infty} \sum_{p=-m \cdot q}^{m \cdot q} \frac{2}{q^n} = \sum_{q=2}^{\infty} \frac{2(2 \cdot m \cdot q + 1)}{q^n} = \sum_{q=2}^{\infty} \frac{4 \cdot m \cdot q + 2}{q^n}$$

Como $q \geq 2$,

$$\sum_{q=2}^{\infty} \frac{4 \cdot m \cdot q + 2}{q^n} \leq \sum_{q=2}^{\infty} \frac{4 \cdot m \cdot q + q}{q^n} = (4 \cdot m + 1) \sum_{q=2}^{\infty} \frac{1}{q^{n-1}}$$

Note que para todo $n > 2$ a série será convergente, e, como $f(q) = \frac{1}{q^{n-1}}$ é contínua e decrescente, a aproximação com retângulos pela direita será menor que a integral. Se usarmos retângulos de base 1, essa aproximação será justamente a série que analisamos, e portanto $n > 2$ implica

$$\sum_{q=2}^{\infty} \frac{1}{q^{n-1}} < \int_1^{\infty} \frac{dq}{q^{n-1}} = \frac{1}{n-2}$$

Dessa forma, a soma dos tamanhos dos intervalos que pertencem a cada $W_{n,m}$ é menor ou igual a

$$\frac{4 \cdot m + 1}{n - 2}$$

Ora, então quando n tende ao infinito, essa soma obviamente tende a zero, ou seja, $\forall \varepsilon > 0 \ \ \exists n_\varepsilon$ tal que

$$0 < \frac{4 \cdot m + 1}{n_\varepsilon - 2} < \varepsilon$$

Ora, então a restrição de $\mathcal{L}$ ao intervalo $(-m, m)$ possui medida zero, pois é uma união enumerável de intervalos cuja soma dos comprimentos pode ser tão pequena quanto se queira.

Note agora que

$$\mathcal{L} = \bigcup_{m \in \mathbb{N}} (\mathcal{L} \cap (-m, m))$$

Ora, mas cada $\mathcal{L} \cap (-m, m)$ tem medida zero, e $\mathbb{N}$ é enumerável por definição. Segue, portanto, que $\mathcal{L}$ tem medida de Lebesgue zero. □

As propriedades surpreendentes de $\mathcal{L}$, todavia, não param por aí. É possível provar que trata-se de um conjunto denso sobre $\mathbb{R}$ — essa afirmação possui um significado muito mais profundo caso o leitor queira se aprofundar em topologia geral, mas, nesse contexto, é suficiente dizer que um conjunto A é denso sobre $\mathbb{R}$ em todo intervalo aberto e não-nulo há pelo menos um representante de A. Em outras palavras, entre quaisquer dois números reais, há pelo menos um número contido em A. Para provar que $\mathcal{L}$ é denso sobre $\mathbb{R}$, todavia, precisamos provar uma proposição fundamental:

Proposição 1.9. *Se x é um número de Liouville e $\frac{a}{b}$ é um número racional com $b > 0$, então $x + \frac{a}{b} \in \mathcal{L}$.*

Demonstração. Ora, se x é um número de Liouville, existe uma sequência $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ com p_n, q_n relativamente primos tal que

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

Ao mesmo tempo,

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

Seja $y = x + \frac{a}{b}$, $p'_n = p_n \cdot b + q_n \cdot a$ e $q'_n = q_n \cdot b$. Temos:

$$0 < \left| y - \frac{p'_n}{q'_n} \right| < \frac{1}{{q_n}^n}$$

Queremos mostrar que, se a desigualdade acima vale para todo $n \in \mathbb{N}$, então para todo $m \in \mathbb{N}$

$$0 < \left| y - \frac{p'_n}{q'_n} \right| < \frac{1}{(q'_n)^m}$$

Para isso, basta mostrar que para todo m, existe um n tal que

$$\frac{1}{{q_n}^n} < \frac{1}{(q'_n)^m}$$

Ora, trata-se do mesmo que mostrar que, para todo m existe um n tal que

$${q_n}^n > (q'_n)^m = (q_n \cdot b)^m = q^m \cdot b^m$$

Note que isso é equivalente a encontrar, para todo m, um valor para n tal que

$${q_n}^{n-m} > b^m$$

Tome $n > m$. Temos:

$${q_n}^{n-m} > b^m \iff \left({q_n}^{n-m}\right)^{\frac{1}{n-m}} > (b^m)^{\frac{1}{n-m}} \iff q_n > b^{\frac{m}{n-m}}$$

Note agora que, quando $n \to \infty$, $q_n \to \infty$, mas $b^{\frac{m}{n-m}} \to 1$. Dessa forma, deve existir n_0 tal que, para todo $n \geq n_0$, vale:

$$q_n > b^{\frac{m}{n-m}}$$

Dessa forma, para todo m, encontramos n_0 tal que

$$0 < \left| y - \frac{p'_{n_0}}{q'_{n_0}} \right| < \frac{1}{q^{n_0}} < \frac{1}{(q')^m}$$

Como a sequência $\left(\frac{p_n}{q_n}\right)_{n\in\mathbb{N}}$ possui infinitos elementos distintos, a sequência $\left(\frac{p'_n}{q'_n}\right)_{n\in\mathbb{N}}$ também possuirá; e, portanto $y = x + \frac{a}{b}$ é um número de Liouville. □

Munidos dessa proposição, podemos provar facilmente o seguinte teorema:

Teorema 1.10. *Dado $(a, b) \in \mathbb{R}^2$ com $a < b$, $\exists x \in \mathcal{L}$ tal que $a < x < b$.*

Demonstração. Ora, se $a < b$, então uma propriedade conhecida dos números racionais é de que existe um racional $\frac{p}{q}$ (com $q > 0$) tal que $a < \frac{p}{q} < b$. Ao mesmo tempo, um número de Liouville pode ser arbitrariamente pequeno: $\forall \varepsilon > 0$, temos que existe algum n tal que $\frac{1}{2^{n!}} < \varepsilon$. Basta notar que, se definirmos a sequência $(c_k)_{k\in\mathbb{N}}$ como:

$$\begin{cases} c_k = 0 \text{ , se } k \leq n \\ c_k = 1 \text{ , se } k > n \end{cases}$$

teremos que

$$x_\varepsilon = \sum_{k=1}^{\infty} \frac{c_k}{2^{k!}} < \frac{1}{2^{n!}} < \varepsilon$$

Note que x_ε é um número de Liouville, pois satisfaz às hipóteses do Teorema 1.6.

Note, também, que $a < \frac{p}{q} < b \Rightarrow a < \frac{p}{q} < \frac{p}{q} + \frac{b-\frac{p}{q}}{2} < b$. Tomando $\varepsilon = \frac{b-\frac{p}{q}}{2}$ (que obviamente é > 0), teremos que $\frac{p}{q} + x_\varepsilon < \frac{p}{q} + \varepsilon < b$.

Por consequência da proposição 1.9, $\frac{p}{q} + x_\varepsilon$ é um número de Liouville, e, ao mesmo tempo, $a < \frac{p}{q} + x_\varepsilon < b$. □

2 O Teorema de Thue-Siegel-Dyson-Roth

O teorema de Thue-Siegel-Roth é um dos resultados mais importantes no contexto do estudo do expoente de irracionalidade. Essencialmente, o seu resultado prova que, se um número é algébrico de grau $n \geq 2$, seu expoente de irracionalidade é igual a 2. A demonstração desse teorema é muito elaborada, e foi alvo do estudo de diversos matemáticos ao longo da história. Thue, Siegel, e Dyson foram responsáveis por diminuir o limite superior da medida de irracionalidade de números algébricos, até que Roth finalmente conseguiu provar que seria exatamente igual a 2. Nesta seção, trataremos dos precursores ao teorema final.

2.1 O teorema de Thue

Em 1909, Axel Thue provou que há um máximo para a medida de irracionalidade de um número algébrico: se α é algébrico de grau $n \geq 3$, então $\mu_{\mathcal{L}}(\alpha) \leq (n+2)/2$. Isso é equivalente a provar que, para qualquer $\varepsilon > 0$, a inequação

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

possui uma quantidade finita de soluções. A demonstração original feita por Thue é bastante trabalhosa, e pode ser encontrada em [1]. Apresentamos, todavia, uma demonstração mais simplificada, contida em [2], com a contrapartida de que nem todos os lemas e proposições intermediários usados serão demonstrados, sendo exibida apenas a intuição por detrás deles.

O primeiro é o Lema de Siegel, cuja demonstração pode ser encontrada em [3, Lema D.4.1, p. 317-319].

Lema 2.1. *Seja $L : \mathbb{Z}^M \to \mathbb{Z}^N$ uma aplicação linear dada por uma matriz com coeficientes inteiros. Então, se $M > N$, existe $x \in \mathbb{Z}^M \backslash \{0\}$ tal que $Lx = 0$ e $|x|_\infty \leq |L|_{op}^{N/(M-N)} + 1$, em que*

$$|L|_{op} = \sup_{x \in \mathbb{Z}^M \backslash \{0\}} \frac{|Lx|_\infty}{|x|_\infty}$$

Nesse contexto, $|x|_\infty$ é a "norma do supremo" — i.e.,

$$|(x_1, \dots x_n)|_\infty = \sup_{1 \leq i \leq n} |x_i|$$

O que este lema nos garante é que, se tivermos um sistema linear homogêneo com coeficientes inteiros, e o número de equações é maior que o número de incógnitas, então temos um vetor solução x cujas coordenadas são inteiras e, mais que isso, este vetor é pequeno (menor que a chamada norma operador de L, $|L|_{op}$) e fica menor, comparado à norma do próprio sistema, quanto mais equações "sobressalentes" tivermos. Nesse contexto, se L pode ser representado por uma matriz (a_{ij}), então sua norma operador pode ser calculada por

$$|L|_{op} = \max_{1 \leq i \leq N} \sum_{j=1}^{M} |a_{ij}|$$

isto é, a norma-operador de L é igual à maior soma dos valores absolutos de uma das linhas de sua matriz correspondente. Por conta disso, se assumirmos que $(a_{ij}) \leq B \ \forall \ i, j$, teremos que $|L|_{op} \leq MB$, estabelecendo portanto um limite superior conciso para a solução inteira x.

O seguinte lema também será usado na demonstração:

Lema 2.2. *Suponha que $Q(\beta) = 0$, onde $Q \in \mathbb{Z}[x]$ com grau n e coeficiente dominante q_n. Então, para qualquer $m \geq n$, podemos escrever*

$$q_n^m \beta^m = \sum_{k=0}^{n-1} c_{km} \beta^k,$$

onde $c_{km} \in \mathbb{Z}$ e $|c_{km}| \leq (2|Q|)^m$, sendo $|Q| = \max_{0 \leq i \leq n} q_i$

Demonstração. Sejam

$$\begin{cases} Q(x) = q_n x^n + q_{n-1} x^{n-1} + \cdots + q_0 \text{ , com } q_i \in \mathbb{Z} \text{ e } q_n \neq 0 \\ |Q| = \max_{0 \leq i \leq n} q_i \end{cases}$$

Como $q_n \neq 0$, temos que $|Q| \geq q_n \geq 1$ (pois q_n é inteiro). Por hipótese, $Q(\beta) = 0$ e, portanto,

$$q_n \beta^n = -(q_{n-1} \beta^{n-1} + \cdots + q_0) \tag{7}$$

Provaremos por indução em m que, para $m \geq n$,

$$q_n^m \beta^m = \sum_{k=0}^{n-1} c_{km} \beta^k$$

em que $c_{km} \in \mathbb{Z}$ e $c_{km} \leq (2|Q|)^m$.

Caso base: $m = n$.

Multiplicamos (7) por q_n^{n-1}:

$$q_n^{n-1}(q_n \beta^n) = q_n^n \beta^n = q_n^{n-1} \left(- \sum_{k=0}^{n-1} q_k \beta^k \right) = \sum_{k=0}^{n-1} (-q_n^{n-1} q_k) \beta^k$$

Como $m = n$, seja $c_{kn} = (-q_n^{n-1} q_k)$ para $k = 0, 1, ..., n-1$. Vamos comparar as magnitudes de c_{kn} e $(2|Q|)^m$:

Por definição, $|q_i| \leq |Q|$. Então $|c_{kn}| \leq |Q|^{n-1}|Q| = |Q|^n < 2^n |Q|^n = (2|Q|)^n$. Portanto, o caso base vale.

Hipótese de indução: assuma que, para algum $m \geq n$, $q_n^m \beta^m = \sum_{k=0}^{n-1} c_{km} \beta^k$, com $c_{km} \in \mathbb{Z}$ e $|c_{km}| \leq (2|Q|)^m$. Queremos demonstrar que o mesmo vale para $m+1$, i.e.: $q_n^{m+1} \beta^{m+1} = \sum_{k=0}^{n-1} c_{k,m+1} \beta^k$, com $c_{k,m+1} \in \mathbb{Z}$ e $|c_{k,m+1}| \leq (2|Q|)^{m+1}$

Note que $q_n^{m+1} \beta^{m+1} = q_n \beta (q_n^m \beta^m)$. Usando a hipótese de indução, isso significa que:

$$q_n^{m+1} \beta^{m+1} = q_n \beta \left(\sum_{k=0}^{n-1} c_{km} \beta^k \right) = \sum_{k=0}^{n-1} q_n c_{km} \beta^{k+1}$$

Separando o termo de $k = n-1$:

$$q_n^{m+1} \beta^{m+1} = q_n c_{n-1,m} \beta^n + \sum_{k=0}^{n-2} q_n c_{km} \beta^{k+1}$$

Usando novamente (7), teremos:

$$q_n^{m+1} \beta^{m+1} = c_{n-1,m}(q_n \beta^n) + \sum_{k=0}^{n-2} q_n c_{km} \beta^{k+1} = c_{n-1,m} \left(- \sum_{k=0}^{n-1} q_k \beta^k \right) + \sum_{k=0}^{n-2} q_n c_{km} \beta^{k+1} =$$

$$\sum_{k=0}^{n-1} (-c_{n-1,m} q_k) \beta^k + \sum_{k=1}^{n-1} (q_n c_{k-1,m}) \beta^k$$

Simplificando a notação da segunda somatória:

$$q_n^{m+1} \beta^{m+1} = \sum_{k=0}^{n-1} (-c_{n-1,m} q_k) \beta^k + \sum_{k=1}^{n-1} (q_n c_{k-1,m}) \beta^k$$

Os coeficientes $c_{k,m+1}$ são:

$$\begin{cases} k = 0 : c_{0,m+1} = -c_{n-1,m} q_0 \\ 1 \leq k \leq n-1 : c_{k,m+1} = -c_{n-1,k} q_k + c_{k-1,m} q_n \end{cases}$$

Vamos checar suas magnitudes: Para $k = 0$: $|c_{0,m+1}| = |c_{n-1,m}||q_0|$. Pela hipótese de indução e pela definição de $|Q|$, portanto, $|c_{0,m+1}| \leq (2|Q|)^m|Q| = \frac{|2Q|}{2}|(2|Q|)^m = \frac{(2|Q|)^{m+1}}{2} < (2|Q|)^{m+1}$

Para $1 \leq k \leq n-1$: $|c_{k,m+1}| = |-c_{n-1,m}q_k + c_{k-1,m}q_n| \leq |-c_{n-1,m}q_k| + |c_{k-1,m}q_n| = |c_{n-1,m}||q_k| + |c_{k-1,m}||q_n|$. Novamente usando a definição de $|Q|$ e a hipótese de indução, temos $|c_{k,m+1}| \leq (2|Q|)^m|Q| + (2|Q|)^m|Q| = 2|Q|(2|Q|)^m = (2|Q|)^{m+1}$ e, portanto, a afirmação inicial valerá para todo $m \geq n$. □

É evidente que, da forma como definimos a norma do polinômio, que o enunciado também vale para a norma $|Q| = \sum_i |q_i|$. Em essência, o que esse lema demonstra é que, se β é uma raiz de um polinômio Q de grau n e com coeficientes inteiros, então $m \geq n$ implica que $q_n^m\beta^m$ pode ser expressado como uma combinação linear de elementos de $\{1, \beta, ..., \beta^{n-1}\}$, e que os coeficientes dessa combinação linear deverão ser limitados por $(2|Q|)^m$. Estes dois lemas podem ser usados para provar a seguinte proposição:

Proposição 2.3. *Seja $\beta \in \mathbb{R}$ um algébrico de grau n. Suponha $\varepsilon > 0$. Para qualquer inteiro suficientemente grande m, existe um polinômio $P \in \mathbb{Z}[x_1, x_2]$ de forma $P(x_1, x_2) = P_1(x_1)x_2 + P_0(x_1)$ tal que:*

- $\partial_1^j P(\beta, \beta) = 0$ *para* $0 \leq j \leq m-1$.
- $\deg P \leq \frac{1+\varepsilon}{2}nm + 2$.
- $|P| \leq C(\beta)^{m/\varepsilon}$.

Demonstração. Queremos encontrar um polinômio $P(x_1, x_2) = P_1(x_1)x_2 + P_0(x_1)$ com coeficientes inteiros que satisfaça as condições dadas. Escreveremos:

$$P_0(x_1) = \sum_{k=0}^{D_0} b_k x_1^k \text{ , e } P_1(x_1) = \sum_{k=0}^{D_1} a_k x_1^k$$

em que a_k, b_k são os coeficientes inteiros a serem determinados. O grau de P é $\max(D_1 + 1, D_0)$. Para simplificar a notação, escolheremos $D_0 = D_1 = D$, com a contrapartida que a_D ou b_D podem ser iguais a zero. A primeira condição é que $\partial_1^j P(\beta, \beta) = 0$ para $j = 0, 1, ..., m-1$. Vamos calcular as derivadas:

$$\partial_1^j P(\beta, \beta) = (\partial_1^j P_1)(\beta)\beta + (\partial_1^j P_0)(\beta) =$$
$$= \beta\left(\sum_{k=j}^{D} a_k \frac{k!}{(k-j)!}\beta^{k-j}\right) + \sum_{k=j}^{D} b_k \frac{k!}{(k-j)!}\beta^{k-j} =$$
$$= \sum_{k=j}^{D} a_k \frac{k!}{(k-j)!}\beta^{k-j+1} + \sum_{k=j}^{D} b_k \frac{k!}{(k-j)!}\beta^{k-j} = 0$$

Como há uma equação para cada $j = 0, ..., m-1$, temos um total de m equações. Note, contudo, que $\frac{k!}{(k-j)!}$ é divisível por $j!$, pois $\frac{k!}{(k-j)!j!} = \binom{k}{j}$. A equação se torna:

$$\frac{1}{j!}\partial_1^j P(\beta, \beta) = \sum_{k=j}^{D} a_k \binom{k}{j}\beta^{k-j+1} + \sum_{k=j}^{D} b_k \binom{k}{j}\beta^{k-j} = 0 \tag{8}$$

Escolheremos $D \leq nm$, e portanto os coeficientes $\binom{k}{j}$ são tais que

$$\binom{k}{j} \leq 2^k \leq 2^D$$

Ora, mas β é um algébrico de grau n. Portanto, qualquer potência de β pode ser reescrita como combinação linear de $\{1, \beta, \ldots, \beta^{n-1}\}$ com coeficientes racionais. Portanto, para cada $j = 0, \ldots, m-1$ podemos converter (8) para a forma

$$\sum_{k=j}^{D} a_k \binom{k}{j}\beta^{k-j+1} + \sum_{k=j}^{D} b_k \binom{k}{j}\beta^{k-j} = \sum_{i=0}^{n-1} \beta^i \left(\sum_{k=j}^{D} \binom{k}{j} A_{i,j,k} \cdot a_k + \sum_{k=j}^{D} \binom{k}{j} B_{i,j,k} \cdot b_k\right) = 0$$

em que $A_{i,j,k}$ e $B_{i,j,k}$ são racionais.

Ora, mas $\{1, \beta, \ldots, \beta^{n-1}\}$ é precisamente a base de $\mathbb{Q}(\beta)$. Portanto, é linearmente independente, e, para cada $i = 0, \ldots, n-1$ fixado, isso quer dizer que

$$\sum_{k=j}^{D} \binom{k}{j} A_{i,j,k} \cdot a_k + \sum_{k=j}^{D} \binom{k}{j} B_{i,j,k} \cdot b_k = 0 \tag{9}$$

Portanto, para cada $j = 0, \ldots, m-1$, temos n equações de coeficientes racionais. Dessa forma, o total de equações N é igual a mn. Para converter estes racionais para inteiros, notamos que a maior potência de β que aparece em (8) é β^{D+1}. Dessa forma, definindo $Q(x) = q_0 + q_1 x + \cdots + q_n x^n$ como o polinômio minimal de β, podemos multiplicar (8) por q_n^{D+1}, obtendo

$$\sum_{k=j}^{D} a_k \binom{k}{j} q_n^{D+1} \beta^{k-j+1} + \sum_{k=j}^{D} b_k \binom{k}{j} q_n^{D+1} \beta^{k-j} =$$

$$= \sum_{i=0}^{n-1} q_n^{D+1} \beta^i \left(\sum_{k=j}^{D} \binom{k}{j} A_{i,j,k} \cdot a_k + \sum_{k=j}^{D} \binom{k}{j} B_{i,j,k} \cdot b_k \right) = 0$$

Nesse caso, podemos invocar o Lema 2.2 para garantir que $q_n^{D+1} A_{i,j,k}$ e $q_n^{D+1} B_{i,j,k}$ são inteiros e, mais que isso, que $A_{i,j,k}$ e $B_{i,j,k}$ são menores ou iguais a $(2q_n)^{D+1}$. Ora, com essa multiplicação, cada equação da forma de (9) se torna:

$$\sum_{k=j}^{D} q^{D+1} \binom{k}{j} A_{i,j,k} \cdot a_k + \sum_{k=j}^{D} q^{D+1} \binom{k}{j} B_{i,j,k} \cdot b_k = 0$$

Note, então, que $\binom{k}{j} \leq 2^D$ e $A_{i,j,k}, B_{i,j,k} \leq (2q_n)^{D+1}$. Dessa forma, as entradas na matriz que representa os coeficientes inteiros desta equação serão menores ou iguais a

$$2^D (2q_n)^{D+1} \leq 2^{nm} (2q_n)^{nm+1} \leq 2^{nm} (2q_n)^{nm+m} = (2^n q_n^{n+1})^m$$

As variáveis são $a_0, \ldots a_D, b_0, \ldots b_D$. Temos, portanto, $2D+2$ variáveis. A norma operador da matriz que representa os coeficientes da equação, portanto é menor ou igual a

$$(2D+2)(2^n q_n^{n+1})^m \leq (2mn+2)(2^n q_n^{n+1})^m \leq m(2n+2)(2^n q_n^{n+1})^m \leq m((2n+2)2^n q_n^{n+1})^m$$

Note que q_n e n são constantes em relação a β. Definindo $C_1(\beta) = (2n+2)2^n q_n^{n+1}$, a norma operador da matriz é menor ou igual a $mC_1(\beta)^m$. Podemos simplificar mais ainda:

$$mC_1(\beta)^m \leq 2^m C_1(\beta)^m = (2C_1(\beta))^m$$

Portanto, definindo $C_2(\beta) = 2C_1(\beta)$, a norma operador da matriz será menor ou igual a $C_2(\beta)^m$.

Agora vamos aplicar o Lema 2.1: temos $N = mn$ equações e $D = 2D + 2$ variáveis. Como m é suposto como suficientemente grande, podemos escolher D para satisfazer a segunda condição da proposição, de forma que

$$D \leq \frac{1+\varepsilon}{2} nm$$

mas, ao mesmo tempo,

$$M = 2D + 2 \geq (1 + \frac{\varepsilon}{2})nm = (1 + \frac{\varepsilon}{2})N$$

Vamos calcular o expoente da estimativa dada pelo Lema 2.1:

$$\frac{N}{M-N} = \frac{N}{(1+\frac{\varepsilon}{2})N - N} = \frac{N}{\frac{\varepsilon}{2}N} = \frac{2}{\varepsilon}$$

Com isso, a estimativa dada pelo Lema de Siegel nos garante que

$$\max\{a_0, \ldots a_D, b_0, \ldots b_D\} = (C_2(\beta)^m)^{2/\varepsilon} + 1 = (C_2(\beta)^2)^{m/\varepsilon} + 1 \leq (2C_2(\beta)^2)^{m/\varepsilon}.$$

Por fim, definindo $C(\beta) = 2C_2(\beta)^2$, notamos que $|P| = \max\{a_0, \ldots a_D, b_0, \ldots b_D\} \leq C(\beta)^{m/\varepsilon}$, e conseguimos todas as condições exigidas pela proposição.

□

O que essa proposição nos garante é que, para cada número algébrico, teremos um polinômio de coeficientes inteiros com uma forma específica $(P_1(x_1)x_2 + P_0(x_1)$, que pode ser interpretado como um polinômio de grau 1 em x_2 com coeficientes que são outros polinômios) que se anula de ordem m em (β, β) (i.e., além da própria função se anular, todas as suas derivadas parciais na primeira coordenada até a m-ésima são 0 quando avaliadas em (β, β)) e, mais que isso, que o grau e a norma deste polinômio são limitados pelos valores de m, β e ε.

Para esta demonstração do teorema de Thue, também é interessante lembrar o teorema de Taylor:

Teorema 2.4 (Teorema de Taylor)**.** *Se f é uma função infinitamente derivável em um intervalo, então $f(x+h)$ pode ser aproximada pela sua expansão de Taylor em torno de x:*

$$f(x+h) = \sum_{j=0}^{m-1} \frac{1}{j!} \partial^j f(x) h^j + E$$

onde o termo de erro E é limitado por

$$|E| \leq \frac{1}{m!} \sup_{y \in [x, x+h]} |\partial^m f(y)| h^m$$

Um corolário do Teorema de Taylor é o seguinte:

Corolário 2.5. *Dado Q um polinômio de grau n de uma variável que se anula de ordem $m \geq 1$ em x se $|h| \leq 1$, então*

$$|Q(x+h)| \leq C(x)^n |Q| |h|^m.$$

Demonstração. Ora, se Q se anula em x em ordem $m \geq 1$, então temos:

$$\begin{cases} \partial^1 Q(x) = 0 \\ \cdots \\ \partial^{m-1} Q(x) = 0 \end{cases}$$

Ademais, como Q é um polinômio, podemos realizar sua expansão de Taylor em torno de x:

$$Q(x+h) = \sum_{j=0}^{m-1} \frac{1}{j!} \partial^j Q(x) h^j + E$$

Como as $m-1$ primeiras derivadas são zero por hipótese, temos $Q(x+h) = E$ e, portanto, $|Q(x+h)| = |E|$. Ao mesmo tempo, denotando $[x, x+h]$ como o segmento de x a $x+h$ (mesmo em caso de h ser negativo), temos:

$$|E| \leq \frac{1}{m!} \sup_{y \in [x, x+h]} |\partial^m Q(y)| |h|^m$$

Seja $Q(t) = \sum_{k=0}^{n} a_k t^k$. Assim como fizemos na última demonstração, definimos $|Q|$ como $\max_{0 \leq k \leq n} |a_k|$. A m-ésima derivada de $Q(t)$ é

$$\partial^m Q(t) = \sum_{k=m}^{n} a_k \frac{k!}{(k-m)!} t^{k-m}$$

uma vez que, para $k < m$, a derivada é igual a zero por hipótese. Seja então y um ponto qualquer do segmento $[x, x+h]$. Ora, então $|y| \leq |x| + 1$. Seja então $Y_0 = |x| + 1$. Ora, então $|y| \leq Y_0$. Consideremos $|\partial^m Q(y)|$:

$$\begin{aligned} |\partial^m Q(y)| &= \left| \sum_{k=m}^{n} a_k \frac{k!}{(k-m)!} y^{k-m} \right| \\ &\leq \sum_{k=m}^{n} |a_k| \frac{k!}{(k-m)!} |y|^{k-m} \\ &\leq |Q| \sum_{k=m}^{n} \frac{k!}{(k-m)!} |y|^{k-m} \quad \text{(como } |a_k| \leq |Q|\text{)} \\ &\leq |Q| \sum_{k=m}^{n} \frac{k!}{(k-m)!} Y_0^{k-m} \quad \text{(como } |y| \leq Y_0 \text{ e } Y_0 \geq 1\text{)} \end{aligned}$$

Como essa limitação vale para qualquer y no segmento, temos:

$$\sup_{y\in[x,x+h]} |\partial^m Q(y)||h|^m \leq |Q| \sum_{k=m}^{n} \frac{k!}{(k-m)!} Y_0^{k-m}$$

E, portanto,

$$|Q(x+h) \leq \frac{1}{m!}\left(|Q| \sum_{k=m}^{n} \frac{k!}{(k-m)!} Y_0^{k-m}\right)|h|^m = \left(\sum_{k=m}^{n} \frac{k!}{m!(k-m)!} Y_0^{k-m}\right)|Q||h|^m =$$

$$= \left(\sum_{k=m}^{n} \binom{k}{m} Y_0^{k-m}\right)|Q||h|^m$$

Vamos analisar apenas $K = \sum_{k=m}^{n} \binom{k}{m} Y_0^{k-m}$. Se substituirmos $j = k - m$, teremos:

$$K = \sum_{j=0}^{n-m} \binom{j+m}{m} Y_0^j$$

Como $Y_0 \geq 1$ $Y_0^j, \leq Y_0^{n-m}$ para $j \leq n - m$. Portanto,

$$K \leq \sum_{j=0}^{n-m} \binom{j+m}{m} Y_0^{n-m} = Y_0^{n-m} \sum_{j=0}^{n-m} \binom{j+m}{m}$$

Lembrando da identidade $\sum_{i=r}^{n} \binom{i}{r} = \binom{N+1}{r+1}$, temos:

$$K \leq Y_0^{n-m} \sum_{j=0}^{n-m} \binom{j+m}{m} = Y_0^{n-m} \binom{n+1}{m+1} = \binom{n+1}{m+1}(|x|+1)^{n-m}$$

E, portanto,

$$|Q(x+h)| \leq \binom{n+1}{m+1}(|x|+1)^{n-m}|Q||h|^m$$

Para provar o corolário, portanto, resta encontrar uma função $C(x)$ tal que

$$\binom{n+1}{m+1}(|x|+1)^{n-m} \leq (C(x))^n$$

Note que

$$\binom{n+1}{m+1}(|x|+1)^{n-m} < \binom{n+1}{m+1}(|x|+1)^n \leq 2^{n+1}(|x|+1)^n$$

Definindo $C(x) = 2^{n+1/n}(|x|+1)$, temos $C(x)^n \geq \binom{n+1}{m+1}(|x|+1)^{n-m}$, concluindo a demonstração. □

Assim como em 2.2, a norma escolhida para o polinômio poderia ser também a soma do valor absoluto de seus coeficientes. Esse corolário nos permitirá usar uma versão Proposição 2.3 com números racionais:

Proposição 2.6. *Seja β é um algébrico de grau $n \geq 3$, s um número real tal que $s > (n+2)/2$, e $r_1 = p_1/q_1$ e $r_2 = p_2/q_2$ racionais que satisfazem a desigualdade $|\beta - r_i| \leq q_i^{-s}$. Assumindo $q_1 < q_2$, e definindo m como o inteiro tal que $q_1^m \leq q_2 < q_1^{m+1}$ e que, dados β e s, temos q_1 e m suficientemente grandes. Então, existe um polinômio $P \in \mathbb{Z}[x_1, x_2]$ da forma $P(x_1, x_2) = P_1(x_1)x_2 + P_0(x_1)$, e constantes $c(\beta, s) > 0$ e $C(\beta, s) > 0$ tais que:*

- $\partial_1^j P(r_1, r_2) = 0$ *para* $0 \leq j < c(\beta, s)m$.
- $|P| \leq C(\beta, s)^m$.
- $\deg P \leq C(\beta, s)m$.

A demonstração dessa proposição pode ser encontrada em [2, pp. 263-265] e essencialmente envolve utilizar a Proposição 2.3 para construir um polinômio que satisfaz a segunda e a terceira condições usando $\varepsilon = (1/10n)(s - (n+2)/2)$, e então usar o Corolário 2.5 para mostrar que o valor absoluto das derivadas deste polinômio em (r_1, r_2) deve ser tão pequeno quanto se queira, e, portanto, que estas se anulam.

Outro lema utilizado na demonstração é o Lema de Gauss:

Lema 2.7 (Lema de Gauss)**.** *Seja $r = p/q$ um número racional (com p e q primos entre si) e $P \in \mathbb{Z}[x]$ tal que $\partial^j P(r) = 0$ para $j = 0, ..., l-1$. Então existe $P_1 \in \mathbb{Z}[x]$ tal que $P(x) = (qx-p)^l P_1(x)$*

Demonstração. A condição de que as l primeiras derivadas de $P(x)$ se anulam em $r = p/q$ significa que r é uma raiz de $P(x)$ com multiplicidade de pelo menos l. Isso quer dizer que $(x-r)^l$ divide $P(x)$.

Reescrevendo $(x-r)^l$:

$$(x-r)^l = \left(x - \frac{p}{q}\right)^l = \left(\frac{qx-p}{q}\right)^l = \frac{1}{q^l}(qx-p)^l$$

Como $P(x)$ é um múltiplo de $(x-r)^l$, podemos escrever $P(x) = (qx-p)^l \cdot P_2(x)$ para algum polinômio $P_2(x)$.

$P(x)$ tem coeficientes inteiros, e o fator $(qx-p)^l$ também tem coeficientes inteiros (pois p e q são inteiros). Portanto, ao realizar a divisão de polinômios, temos $P_2(x) = \frac{P(x)}{(qx-p)^l}$, em que o resultado será um polinômio com coeficientes racionais. Portanto, $P_2(x) \in \mathbb{Q}[x]$.

Queremos provar que os coeficientes são, na verdade, inteiros.

Como $P_2(x)$ tem coeficientes racionais, podemos escrever todos os seus coeficientes com um denominador comum, M. Assim, podemos expressar $P_2(x)$ como:

$$P_2(x) = \frac{1}{M}\tilde{P}_2(x),$$

onde $\tilde{P}_2(x)$ é um polinômio com coeficientes inteiros, e escolhemos M de forma que os coeficientes de $\tilde{P}_2(x)$ não todos divisíveis pelo mesmo fator primo.

Substituindo na equação original, obtemos: $P(x) = \frac{1}{M}(qx-p)^l \tilde{P}_2(x)$

Multiplicando ambos os lados por M:

$$M \cdot P(x) = (qx-p)^l \tilde{P}_2(x)$$

Suponha que $|M| \neq 1$. Isso significa que M deve ter pelo menos um fator primo. Vamos chamar esse fator primo de s.

Agora, vamos analisar a equação $M \cdot P(x) = (qx-p)^l \tilde{P}_2(x)$ "módulo s":

Como s é um fator de M, temos que $M \equiv 0 \pmod{s}$. Portanto, o lado esquerdo se torna:

$$M \cdot P(x) \equiv 0 \cdot P(x) \equiv 0 \pmod{s}$$

O lado direito é $(qx-p)^l \tilde{P}_2(x)$. Note que o fator $(qx-p)$ não é nulo módulo s: se fosse, teríamos $q \equiv 0 \pmod{s}$ e $p \equiv 0 \pmod{s}$. Isso implicaria que s é um fator comum de p e q. Mas $r = p/q$ é uma fração irredutível, então p e q são primos entre si e não têm fatores primos em comum. Logo, $(qx-p) \not\equiv 0 \pmod{s}$.

Ao mesmo tempo, $\tilde{P}_2(x)$ também não é nulo por construção, pois o definimos de forma que não há nenhum primo que divida todos os seus coeficientes. Como s é um primo, ele não pode dividir todos os coeficientes de $\tilde{P}_2(x)$. Logo, $\tilde{P}_2(x) \not\equiv 0 \pmod{s}$.

Chegamos, portanto, a uma contradição, e M não pode ter fatores primos. Logo, $\tilde{P}_2 \in \mathbb{Z}[x]$, e, definindo $P_1 = \tilde{P}_2$, temos o resultado desejado. □

Essencialmente, o que este lema nos garante é que, se temos um polinômio de coeficientes inteiros com uma raiz racional p/q na qual o polinômio se anula de ordem l, então ao "retirar" essa raiz do polinômio, o polinômio resultante também terá coeficientes inteiros. Mais que isso, é notável é que q^l deve dividir o coeficiente líder de P: se $P(x) = a_0 + ... + a_n x^n$ e $P_1(x) = b_0 + ... + b_m x^m$, com $a_i, b_j \in \mathbb{Z}$, temos

$$a_0 + \cdots + a_n x^n = (qx-p)^l(b_0 + \cdots + b_m x^m) = (q^l x^l + \dots)(b_0 + \dots b_m x^m) \implies$$
$$\implies a_n x^n = q^l x^l b_m x^m \implies a_n = q^l b_m$$

Portanto, $|P| \geq q^l$. Com esse lema, podemos provar a última proposição necessária para provar o Teorema de Thue:

Proposição 2.8. *Sejam* $P(x_1, x_2) = P_q(x_1)x_2 + P_0(x_1) \in \mathbb{Z}[x_1, x_2]$ *e* $(r_1, r_2) = (p_1/q_1, p_2/q_2) \in \mathbb{Q}^2$. *Se* $\partial_1^j P(r_1, r_2) = 0$ *para* $j = 0, ..., l-1$ *e* $l \geq 2$, *então*

$$|P| \geq min\left(\frac{q_1^{(l-1)/2}}{2 \cdot \deg P}, q_2\right)$$

Demonstração. Nossa hipótese é que

$$\partial_1^j P_1(r_1)r_2 + \partial_1^j P_0(r_1) = 0, \quad \text{para} \quad 0 \leq j \leq l-1$$

Seja $V(x)$ o vetor $(P_1(x), P_0(x))$. Então a hipótese é que, para $0 \leq j \leq l-1$, as derivadas $\partial^j V(r_1)$ todas pertencem à reta $V \cdot (r_2, 1) = 0$. Em particular, isso quer dizer que quaisquer duas dessas derivadas são linearmente dependentes. Isso nos diz que muitos determinantes se anulam. Denotando, para $V, W \in \mathbb{R}^2$, $[V, W]$ como a matriz 2×2 com a primeira coluna V e a segunda coluna W, temos

$$\det[\partial^{j_1} V, \partial^{j_2} V](r_1) = 0, \text{ para quaisquer } 0 \leq j_1, j_2 \leq l-1$$

Como o determinante é um funcional multilinear, temos a regra de Leibniz $\partial \det[V, W] = \det[\partial V, W] + \det[V, \partial W]$, que vale para quaisquer funções vetoriais $V, W : \mathbb{R} \to \mathbb{R}^2$. Usando isso, temos:

$$\partial^j \det[V, \partial V](r_1) = 0, \text{ para quaisquer } 0 \leq j \leq l-2$$

Note que $\det[V, \partial V]$ é um polinômio de coeficientes inteiros; e, se esse polinômio é não-nulo, então o corolário do Lema 2.7 nos garante que

$$|\det[V, \partial V]| \geq q_1^{l-1}$$

Analisando $|\det[V, \partial V]|$, notamos que:

$$|\det[V, \partial V]| = |(\partial P_0)P_1 - P_0(\partial P_1)| \leq |(\partial P_0)P_1| + |P_0(\partial P_1)| \leq \deg P |P|^2 + \deg P |P|^2 \leq 2(\deg P |P|)^2$$

e, portanto,

$$q_1^{l-1} \leq 2(\deg P |P|)^2 \implies |P| \geq \frac{q_1^{(l-1)/2}}{2 \cdot \deg P}$$

Caso o polinômio $\det[V, \partial V]$ seja identicamente nulo, então

$$\partial\left(\frac{P_0}{P_1}\right) = \frac{(\partial P_0)P_1 - P_0(\partial P_1)}{{P_1}^2} = 0,$$

pois seu numerador (que é justamente o determinante de $[V, \partial V]$) é zero. Portanto, a razão entre P_1 e P_0 deve ser uma constante. Logo, existe $A \in \mathbb{R}$ tal que

$$P_0 = A \cdot P_1 \implies P(x_1, x_2) = (x_2 + A)P_1(x_1)$$

Voltando à condição de que P se anula de ordem l em (r_1, r_2), temos que:

$$\partial_1^j P(r_1, r_2) = (r_2 + A)\partial_1^j P_1(r_1) = 0, \quad \text{para} \quad j = 0, \ldots, l-1$$

Nesse caso, temos duas possibilidades:
Se $r_2 + A = 0$, a constante A é $-r_2 = -p_2/q_2$. O polinômio se torna:

$$P(x_1, x_2) = (x_2 - p_2/q_2)P_1(x_1) = \frac{1}{q_2}(q_2 x_2 - p_2)P_1(x_1)$$

Como P e P_1 têm coeficientes inteiros, o Lema 2.7 garante que podemos encontrar $\tilde{P}(x_1)$ tal que

$$P(x_1, x_2) = (q_2 x_2 - p_2)\tilde{P}(x_1),$$

onde $\tilde{P}(x_1)$ também tem coeficientes inteiros. Dessa forma, $|P| \geq q_2$.
Se $(r_2 + A) \neq 0$, temos que

$$\partial_1^j P_1(r_1) = 0, \quad \text{para} \quad j = 0, \ldots, l-1$$

Usando mais uma vez o Lema 2.7, temos que

$$|P| \geq q_1^l \geq \frac{q_1^{(l-1)/2}}{2 \cdot \deg P},$$

concluindo assim a demonstração.

□

Essa proposição estabelece um limite inferior para a norma de um polinômio que se anula em ordem alta, enquanto a Proposição 2.3 estabelece um limite superior. Podemos, portanto, encontrar uma contradição caso o limite inferior seja maior que o superior.

Com esses lemas e proposições, podemos facilmente provar o Teorema de Thue:

Teorema 2.9 (Teorema de Thue)**.** *Seja β um algébrico de grau n. Então a inequação*

$$\left|\beta - \frac{p}{q}\right| \leq \frac{1}{q^\mu}$$

possui apenas uma quantidade finita de soluções se $\mu > (n+2)/2$ (ou, em outras palavras, $\mu_{\mathcal{L}}(\beta) \leq (n+2)/2$).

Demonstração. Suponha que existam infinitas soluções. Então existe uma sequência $\left\{\frac{p_n}{q_n}\right\}_{n\in\mathbb{N}}$ que satisfaça

$$\left|\beta - \frac{p}{q}\right| \leq \frac{1}{q^\mu}$$

com $\mu > (n+2)/2$. Lembrando que $q_n \to \infty$, podemos tomar q_1 e q_2 tão grandes quanto se queira. Escolheremos o valor de m de forma que

$$q_1{}^m \leq q_2 \leq q_1{}^{m+1}$$

A Proposição 2.6 nos garante que existe um polinômio $P \in \mathbb{Z}[x_1, x_2]$ de forma $P(x_1, x_2) = P_1(x_1)x_2 + P_0(x_1)$ e constantes $c(\beta, s) > 0$ e $C(\beta, s) > 0$ tais que:

- $\partial_1^j P(r_1, r_2) = 0$ para $0 \leq j < c(\beta, s)m$.
- $|P| \leq C(\beta, s)^m$.
- $\deg P \leq C(\beta, s)m$.

Por outro lado, a Proposição 2.8 nos garante que

$$|P| \geq min\left(\frac{q_1^{(c(\beta,s)m-1)/2}}{2 \cdot C(\beta, s)m}, q_2\right)$$

Deve, portanto, existir uma constante $c_1(\beta, s)$ tal que

$$|P| \geq \frac{q_1^{c_0(\beta,s)m}}{m}$$

Comparando os dois limites, temos

$$\frac{q_1^{c_0(\beta,s)m}}{m} \leq |P| \leq C(\beta, s)^m \implies \frac{q_1^{c_0(\beta,s)m}}{m} \leq C(\beta, s)^m$$

Portanto, deve existir uma constante $C_0(\beta, s, m)$ independente de q_1 tal que

$$q_1 \leq C_0(\beta, s, m)$$

Ora, mas q_1 pode ser tomado tão grande quanto se queira, não podendo, portanto, ser limitado. Por contradição, a inequação deve possuir uma quantidade finita de soluções. □

O Teorema de Thue, apesar de parecer insignificante perto do resultado obtido por Roth (de que a medida de irracionalidade de todos os números algébricos é igual a 2) representou um avanço significativo em pelo menos dois sentidos: por um lado, cortou pela metade a distância entre o limite superior obtido pelo Teorema de Liouville (1.5, que implica que a medida de irracionalidade de um algébrico é menor ou igual a seu grau) e a verdadeira medida de irracionalidade; por outro, estabeleceu a ideia geral que seria usada por Siegel, Dyson e Roth para melhorar as estimativas — usando o que chamamos hoje do método de polinômios auxiliares.

2.2 Os Teoremas de Siegel, Dyson e Roth

Com a finalidade de melhorar o limite superior para a medida de irracionalidade estabelecido por Thue, Carl Ludwig Siegel usa um método semelhante ao que mostramos na subseção anterior para demonstrar o seguinte teorema:

Teorema 2.10 (Teorema de Siegel)**.** *Seja α um número algébrico de grau $n \geq 3$. Se μ é um número real positivo tal que*

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

possui infinitas soluções, então

$$\mu \leq \frac{n}{s+1} + s$$

onde $s = 1, 2, ..., n-1$.

É fácil provar que isso implica diretamente que $\mu_{\mathcal{L}}(\alpha) \leq 2\sqrt{n}$. A maior diferença na demonstração de Siegel é a classe de polinômios utilizada: enquanto o Teorema de Thue utiliza polinômios específicos de duas variáveis, o Teorema de Siegel utiliza polinômios gerais de duas variáveis, i.e., da forma

$$P(x, y) = \sum_{i=0}^{a} \sum_{j=0}^{b} c_{ij} x^i y^j$$

Em 1947, Freeman John Dyson usa a ideia da demonstração feita por Siegel, mas de maneira mais sofisticada (introduzindo uma série de notações novas e analisando as matrizes wronskianas dos polinômios), e consegue provar o seguinte teorema:

Teorema 2.11 (Teorema de Dyson)**.** *Seja α um número algébrico de grau $n \geq 3$. Se μ é um número real positivo tal que*

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

possui infinitas soluções, então

$$\mu \leq \sqrt{2n}.$$

É curioso notar que o limite superior estabelecido por Dyson é justamente a média geométrica entre o grau do algébrico dado e sua verdadeira medida de irracionalidade (2), enquanto o limite superior estabelecido por Thue é a média aritmética. Podemos notar, portanto, uma diminuição rápida para o limite superior: o Teorema de Liouville foi provado em 1844; o de Thue, em 1909; e, o de Dyson, em 1947. Por fim, em 1955, Klaus Friedrich Roth prova o seguinte teorema, dando fim à discussão:

Teorema 2.12 (Teorema de Roth)**.** *Seja α um número algébrico de grau $n \geq 3$. Se μ é um número real positivo tal que*

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

possui infinitas soluções, então

$$\mu \leq 2.$$

A demonstração do teorema de Roth também segue as ideias dos teoremas anteriores: garantira a existência um polinômio que anula um algébrico α e mostrar que, se houvessem infinitas soluções para a equação, este polinômio se anula "demais", levando a um limite inferior menor do que o superior. Todavia, a principal diferença dessa demonstração é o número de variáveis: enquanto nos demais teoremas analisamos polinômios de no máximo 2 variáveis, agora analisamos polinômios de n variáveis, o que dificulta significativamente o trabalho. Todavia, o ganho também é imenso: a medida de irracionalidade de números algébricos passa a ser constante, limitando portanto a "qualidade"das aproximações de qualquer número algébrico. Em razão dos avanços estabelecidos com suas demonstrações, o Teorema de Roth costuma carregar também os nomes de Thue e Siegel, e, em alguns textos, também carrega o nome de Dyson.

2.3 Aplicações do Teorema de Thue-Siegel-Dyson-Roth

Uma aplicação particular do Teorema de Thue diz respeito às chamadas equações de Thue:

Teorema 2.13. *Seja m um inteiro diferente de zero. Então, a equação*

$$f(x,y) = a_0x^n + a_1x^{n-1}y + \cdots + a_ny^n = m,$$

em que $n \geq 3$ e $f(x,y)$ é um polinômio irredutível de coeficientes inteiros, possui apenas um número finito de soluções inteiras.

Demonstração. Note que, se $y = 0$, a equação se torna $a_0x^n = m$, que possui no máximo duas soluções inteiras. Suponhamos, sem perda de generalidade, que $y > 0$. Considere

$$\frac{f(x,y)}{y^n} = a_o\left(\frac{x}{y}\right)^n + a_1\left(\frac{x}{y}\right)^{n-1} + \cdots + a_n = \frac{m}{y^n}$$

Definindo $z = x/y$, o polinômio anterior se torna $f(z,1)$. Pelo Teorema Fundamental da Álgebra, podemos fatorar $f(z,1)$ como

$$f(z,1) = a_0(z-\alpha_1)\dots(z-\alpha_n)$$

em que $\alpha_1, ..., \alpha_n$ são as raízes de $f(z,1)$. Portanto,

$$f(x,y) = y^n \cdot f(z,1) = a_0(x-\alpha_1y)\dots(x-\alpha_ny)$$

e podemos reescrever a equação original como

$$\left|a_0\prod_{i=0}^{n}(x-\alpha_iy)\right| = |m|$$

então, para pelo menos algum i, temos que existe B_1 tal que

$$|x-\alpha_1y| \leq |m/a_0|^{1/n} = B_1$$

pois, se todos fossem maiores, o produto seria maior. Sem perda de generalidade, tomaremos este "i" como sendo 1. Então, para $i \neq 1$,

$$|x-\alpha_iy| = |x-\alpha_1y+(\alpha_1-\alpha_i)y| \geq |\alpha_1-\alpha_i|y - |x-\alpha_1y|$$

Definindo B_2 como

$$\min_{i=2,\dots,n}|\alpha_1-\alpha_i|,$$

temos:

$$|x-\alpha_iy| \geq B_2y - B_1 \geq \frac{B_2y}{y}, \quad \forall \quad y > \frac{2B_1}{b_2}$$

Logo,

$$\left|a_0(x-\alpha_1y)\left(\frac{B_2y}{2}\right)^{n-1}\right| < |m|$$

ou seja, temos que

$$\left|\frac{x}{y}-\alpha_1\right| < \frac{1}{y^n}\left|\frac{m}{a_0}\right|\left(\frac{2}{B_2}\right)^{n-1} \leq \frac{1}{y^{n-1/4}}, \quad \forall \quad y^{1/4} > \frac{|m|}{|a_0|}\left(\frac{2}{B_2}\right)^{n-1}$$

Ora, mas α_1 é um algébrico de grau n, pois f é irredutível e α_1 é raiz de $f(z,1)$, que também é irredutível. Ora, mas o Teorema de Thue nos garante que, como $n - 1/4 > (n+2)/2$, a inequação

$$\left|\frac{x}{y}-\alpha_1\right| = \left|\alpha_1-\frac{x}{y}\right| \leq \frac{1}{y^{n-1/4}}$$

só pode ter uma quantidade finita de soluções. □

A próxima aplicação considera uma classe específica de funções: definindo f_r, com $r \in \mathbb{R}$, $r > 2$ como

$$f_r(x) = \begin{cases} \frac{1}{q^r}, \text{ se x é uma fração irredutível } \frac{p}{q} \text{ com } p \neq 0 \\ 0, \text{ se } x = 0 \text{ ou } x \notin \mathbb{Q} \end{cases}$$

queremos saber em que pontos f_r é contínua e em quais desses pontos é diferenciável.

Proposição 2.14. *Para cada $r > 2$, f_r é contínua no zero e em todos os irracionais, mas descontínua nos racionais não-nulos.*

Demonstração. Dado um racional não nulo $x = p/q$, podemos sempre encontrar uma sequência $(x_n)_{n\in\mathbb{N}}$ de irracionais que converge para p/q (por exemplo, $x_n = p/q + \sqrt{2}/n$). Nesse caso, notamos que $f_r(x_n) = 0 \quad \forall\, n \in \mathbb{N}$ e portanto $\lim_{n\to\infty} f_r(x_n) = 0$, mas $x_n \to x$ e $\lim_{n\to\infty} f_r(x_n) \neq f_r(x)$. Portanto, f_r é descontínua em todo racional não-nulo.

Tomemos agora α como um irracional ou igual a zero. Tome então $(y_k)_{k\in\mathbb{N}}$ como uma sequência que converge para α. Vale que:

$$f_r(y_k) = \begin{cases} \frac{1}{{q_k}^r} \text{ para algum } q_k, \text{ se } y_k \text{ é racional e diferente de zero} \\ 0, \text{ caso contrário} \end{cases}$$

Dessa forma, vale que, para todo y_k, existe q_k inteiro tal que

$$|\alpha - y_k| < \delta \implies |f_r(\alpha) - f_r(y_k)| \leq \frac{1}{{q_k}^r}$$

Ao mesmo tempo, dado $\varepsilon > 0$, podemos escolher n grande o suficiente para que $0 < 1/n^r < \varepsilon$. Neste caso, note que para todo $n \in \mathbb{N}$, existe $\delta > 0$ tal que, se

$$\left|\alpha - \frac{p}{q}\right| < \delta,$$

então $q > n$. Para observar que isso é verdade, basta tomar

$$\delta = \frac{1}{2} \min_{p\in\mathbb{Z},\, p\neq 0,\, q\in\mathbb{N},\, q\leq n} \left\{\left|\alpha - \frac{p}{q}\right|\right\}$$

e, então, notar que o mínimo existe (pois o há apenas uma quantidade finita de denominadores) e que é maior que zero (uma vez que α é irracional ou igual a zero). Portanto, tendo escolhido n, podemos escolher δ de forma que

$$|\alpha - y_k| < \delta \implies q_k > n$$

Dessa forma, notamos que

$$|\alpha - y_k| < \delta \implies |f_r(\alpha) - f_r(y_k)| \leq \frac{1}{{q_k}^r} < \frac{1}{n^r} < \varepsilon,$$

concluindo a demonstração. □

Agora, vamos analisar os pontos onde f_r é diferenciável:

Proposição 2.15. *Seja $r > 2$. Se definirmos*

$$S = \{\alpha \in \mathbb{R} : \alpha \notin \mathbb{Q} \text{ e } f_r \text{ não é diferenciável em } \alpha\}$$

e

$$\mathcal{L}(x) = \{\alpha \in \mathbb{R} : \mu_{\mathcal{L}}(\alpha) > x\},$$

então $S \subset \mathcal{L}(2)$.

Demonstração. Queremos provar que, para todo $\alpha \in S$, $\mu_{\mathcal{L}}(\alpha) > 2$, i.e., que a desigualdade

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

possui infinitas soluções se $r > 2$.

Seja então S_n o conjunto dos irracionais tais que, para todo $\delta > 0$ existe $x \in (\alpha - \delta, \alpha + \delta)$ tal que

$$\left|\frac{f_r(x) - f_r(\alpha)}{x - \alpha}\right| = \left|\frac{f_r(x)}{x - \alpha}\right| > \frac{1}{n}.$$

Note que $S = \bigcup_{n=1}^{\infty} S_n$ e que, além disso, todo ponto x que satisfaz a desigualdade acima deve ser racional. Substituindo $x = p/q$, obtemos

$$\left|\frac{1/q^r}{p/q - \alpha}\right| > \frac{1}{n}$$

Como q^r é positivo, podemos reescrever como:

$$\frac{1}{q^r|\alpha - p/q|} > \frac{1}{n},$$

e, reorganizando os termos, obtemos

$$\left|\alpha - \frac{p}{q}\right| < \frac{n}{q^r} \tag{10}$$

Como podemos encontrar $x \in (\alpha - \delta, \alpha + \delta)$ para qualquer valor de δ, e α é irracional, então há infinitas soluções racionais para (10). Dessa forma, a proposição 1.3 nos garante que $\mu_{\mathcal{L}}(\alpha) > 2$ (pois $r > 2$) e, por fim, $S \subset \mathcal{L}(2)$. □

Essa proposição nos diz que f_r é diferenciável no zero e no conjunto dos números reais cuja medida de irracionalidade é igual a 2 (ou seja, todos os algébricos de grau $n \geq 2$ e também "quase todos" os números transcendentais).

É interessante notar que o conjunto dos pontos onde f_r não é diferenciável tem medida nula, em decorrência da seguinte proposição:

Proposição 2.16. *A medida de Lebesgue de $\mathcal{L}(2)$ é igual a zero.*

A demonstração dessa proposição é muito parecida com a da proposição 1.8 (na qual provamos que a medida de Lebesgue de $\mathcal{L}(\infty)$ é zero) e, por isso, não a incluiremos. O leitor interessado pode encontrá-la em [1, p. 99]. Dessa forma, apesar de ser descontínua em todos os racionais não-nulos e não-diferenciável um conjunto de números transcendentais (pois todo número com medida de irracionalidade maior que 2 é transcendental), f_r ainda é diferenciável na "maioria" dos pontos, sob a ótica da medida de Lebesgue.

3 Exemplos e Generalização

Definição 3.1. *Seja a_0 um inteiro, e $\{a_n\}_{n\in\mathbb{N}}$ uma sequência (finita ou infinita) de inteiros positivos. Definimos:*

1. *Uma fração contínua finita é uma expressão da forma*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}$$

   que denotamos por $[a_0; a_1, a_2, \ldots, a_n]$. Os termos a_i são chamados de denominadores parciais, e essa expressão é (evidentemente) um número racional.

2. *Uma fração contínua infinita, denotada por $[a_0; a_1, a_2, \ldots]$, é definida como o limite de suas aproximações finitas. Para cada $k \geq 0$, o número racional*

$$c_k = [a_0; a_1, a_2, \ldots, a_k]$$

   é chamado de k-ésimo convergente da fração. O valor da fração contínua infinita, portanto, é definido como

$$[a_0; a_1, a_2, \ldots] := \lim_{k\to\infty} c_k$$

Dado um irracional α, existe um algoritmo para calcular seus denominadores parciais: definimos $\alpha_0 = \alpha$. Então, definimos a sequência $\{\alpha_n\}_{n\in\mathbb{N}}$ indutivamente:

$$\alpha_{n+1} = \frac{1}{\alpha_n - a_n},$$

em que $a_n = \lfloor \alpha_n \rfloor$.

Teorema 3.1. *A sequência dos convergentes p_n/q_n obtida pelo algoritmo acima converge para α. Ademais, vale:*

$$\frac{1}{2q_{n+1}} < \frac{1}{q_{n+1}+q_n} < |q_n\alpha - p_n| < \frac{1}{q_{n+1}},$$

o que implica

$$\frac{1}{2q_{n+1}q_n} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_{n+1}q_n}$$

A demonstração desse teorema foge do escopo deste trabalho, mas pode ser encontrada em [4, p. 7-8].

Definição 3.2. *Dizemos que a/b aproxima α melhor que c/d se vale*

$$\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{c}{d}\right|$$

Se a/b é o racional que melhor aproxima α com denominador menor ou igual a b, dizemos que a/b é uma melhor aproximação de α. Note que isso é equivalente a dizer que

$$|b\alpha - a| < |d\alpha - c| \quad \forall d < b$$

.

É possível provar que os convergentes p_n/q_n da expansão em frações contínuas de um número real α são precisamente suas melhores aproximações (e que, portanto, a expansão em frações contínuas é única). Mais que isso, é possível provar que p_n/q_n é o racional com menor denominador que satisfaz $|\alpha q_n - p_n| < |\alpha q_{n-1} - p_{n-1}|$. A demonstração deste fato também está contida em [4, p. 9-10].

A expansão em frações contínuas está intimamente conectada com a medida de irracionalidade de Liouville-Roth. Essa conexão começa a ser evidenciada com o seguinte lema, que é corolário do fato enunciado acima:

Lema 3.2. *Seja α um número real. Se p, q satisfazem a desigualdade*

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

Então o racional p/q é um convergente da expansão em frações contínuas de α.

Demonstração. Suponha que temos p/q que satisfaz:

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

.

Logo,

$$|q\alpha - p| < \frac{1}{2q} \tag{11}$$

Tome a/b que aproxima melhor α:

$$\left|\alpha - \frac{a}{b}\right| < \left|\alpha - \frac{p}{q}\right|$$

Temos 2 casos: $b > q$ ou $b \leq q$. Se $b > q$, demonstramos o que queríamos. Se $b \leq q$, então:

$$|b\alpha - a| = \left|\alpha - \frac{a}{b}\right| \cdot b < \left|\alpha - \frac{p}{q}\right| \cdot b \leq \left|\alpha - \frac{p}{q}\right| \cdot q = |q\alpha - p|$$

Logo:

$$|b\alpha - a| < |q\alpha - p| \implies |b\alpha - a| < \frac{1}{2q}$$

.

O que implica:

$$\left|\alpha - \frac{a}{b}\right| < \frac{1}{2bq} \tag{12}$$

Note que:

$$\frac{1}{qb} \leq \left|\frac{a}{b} - \frac{p}{q}\right| \leq \left|\alpha - \frac{a}{b}\right| + \left|\alpha - \frac{p}{q}\right|$$

Portanto, substituindo (11) e (12) na desigualdade de $|\frac{a}{b} - \frac{p}{q}|$:

$$\frac{1}{qb} < \frac{1}{2bq} + \frac{1}{2q^2} = \frac{q+b}{2q^2b}$$

E, concluindo,

$$1 < \frac{q+b}{2q} \implies b > q$$

□

Para números irracionais cujos denominadores parciais possuem uma fórmula conhecida, é possível usar uma fórmula para calcular sua medida de irracionalidade:

Teorema 3.3. *Seja $\alpha = [a_0; a_1, a_2, ...]$ um irracional cujos convergentes são p_n/q_n. Então*

$$\mu_{\mathcal{L}}(\alpha) = 1 + \limsup_{n\to\infty} \frac{\ln(q_{n+1})}{\ln(q_n)} = 2 + \limsup_{n\to\infty} \frac{\ln(a_{n+1})}{\ln(q_n)}$$

Demonstração. Primeiro, demonstraremos que qualquer sequência de racionais $\{p_k/q_k\}_{k\in\mathbb{N}}$ cujas aproximações são "boas" o suficiente para influenciar o valor de $\mu_{\mathcal{L}}(\alpha)$ (i.e., que aproxime α por ordem > 2) possui necessariamente uma subsequência cujos termos são os convergentes de α. Como consequência disso, a maior ordem pela qual α pode ser aproximado por seus convergentes é também a maior ordem pela qual pode ser aproximado por racionais.

Seja $\{p_k/q_k\}_{k\in\mathbb{N}}$ uma sequência que aproxima α por ordem $\nu > 2$. Então, quando $k \to \infty$, vale que $q_k \to \infty$. Mas, como $\nu > 2$, isso significa que para todo $a \in \mathbb{N}$ existe k_a tal que para todo $k' \geq k_a$,

$$q_{k'}{}^{\nu} > a q_{k'}{}^2 \implies \frac{1}{q_{k'}{}^{\nu}} < \frac{1}{a q_{k'}{}^2}$$

Em particular, para $a = 2$,

$$\frac{1}{q_{k'}{}^{\nu}} < \frac{1}{2q_{k'}{}^2}.$$

Nesse caso, note que a sequência

$$\{p_k/q_k\}_{k\geq k_2}$$

será composta exclusivamente por convergentes de α pelo lema 3.2, e podemos restringir nossa "procura" para calcular a medida de irracionalidade exclusivamente à sequência de convergentes.

Definimos, então, como λ_n o número real que, para cada convergente p_n/q_n satisfaz

$$\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n{}^{\lambda_n}}.$$

Pela definição, $\mu_{\mathcal{L}}(\alpha)$ é o supremo do conjunto de números reais μ tais que a desigualdade $|\alpha - p/q| < q^{-\mu}$ admite infinitas soluções racionais p/q. Como mostramos que para $\mu > 2$ basta considerar os convergentes, buscamos o supremo dos valores ρ tais que

$$\left|\alpha - \frac{p_n}{q_n}\right| < q_n^{-\rho}$$

para infinitos n. Substituindo $|\alpha - p_n/q_n| = q_n^{-\lambda_n}$, a desigualdade equivale a $q_n^{-\lambda_n} < q_n^{-\rho}$, o que implica $\lambda_n > \rho$. Assim,

$$\mu_{\mathcal{L}}(\alpha) = \sup\{\rho \in \mathbb{R} : \lambda_n > \rho \text{ para infinitos } n\}$$

Esta é precisamente a definição de limite superior da sequência (λ_n). Logo:

$$\mu_{\mathcal{L}}(\alpha) = \limsup_{n\to\infty} \lambda_n.$$

Para chegar na fórmula dada, aplicamos o Teorema 3.1 para notar que

$$\frac{1}{2q_{n+1}q_n} < \frac{1}{{q_n}^{\lambda_n}} < \frac{1}{q_{n+1}q_n} \implies 2q_{n+1}q_n > {q_n}^{\lambda_n} > q_{n+1}q_n$$

Aplicando o logaritmo, obtemos

$$\ln(2q_{n+1}q_n) > \ln({q_n}^{\lambda_n}) > \ln(q_{n+1}q_n) \implies \frac{\ln(2q_{n+1}q_n)}{\ln(q_n)} > \lambda_n > \frac{\ln(q_{n+1}q_n)}{\ln(q_n)} \implies$$

$$\implies 1 + \frac{\ln(q_{n+1})}{\ln(q_n)} < \lambda_n < \frac{\ln(2)}{\ln(q_n)} + 1 + \frac{\ln(q_{n+1})}{\ln(q_n)}$$

Tomando o limite superior, obtemos:

$$\limsup_{n\to\infty}\left(1 + \frac{\ln(q_{n+1})}{\ln(q_n)}\right) \le \limsup_{n\to\infty} \lambda_n \le \limsup_{n\to\infty}\left(\frac{\ln(2)}{\ln(q_n)} + 1 + \frac{\ln(q_{n+1})}{\ln(q_n)}\right)$$

Como $q_n \to \infty$, os limites superiores nas extremidades são iguais. Portanto, temos

$$\mu_{\mathcal{L}}(\alpha) = 1 + \limsup_{n\to\infty} \frac{\ln(q_{n+1})}{\ln(q_n)} \tag{13}$$

Para a segunda fórmula, utilizamos a seguinte relação de recorrência, demonstrada em [4, p. 2]:

$$q_{n+1} = a_{n+1}q_n + q_{n-1} \tag{14}$$

Como $0 \le q_{n-1} < q_n$, temos as seguintes desigualdades:

$$a_{n+1}q_n < q_{n+1} \le a_{n+1}q_n + q_n = (a_{n+1}+1)q_n$$

Tomando o logaritmo em toda a desigualdade:

$$\ln(a_{n+1}) + \ln(q_n) < \ln(q_{n+1}) \le \ln(a_{n+1}+1) + \ln(q_n)$$

Dividindo por $\ln(q_n)$ (que é positivo para n suficientemente grande):

$$\frac{\ln(a_{n+1})}{\ln(q_n)} + 1 < \frac{\ln(q_{n+1})}{\ln(q_n)} \le \frac{\ln(a_{n+1}+1)}{\ln(q_n)} + 1$$

Note que $\ln(a_{n+1}+1) = \ln(a_{n+1}(1+\frac{1}{a_{n+1}})) = \ln(a_{n+1}) + \ln(1+\frac{1}{a_{n+1}})$. Como $a_{n+1} \ge 1$, temos $0 < \ln(1+\frac{1}{a_{n+1}}) \le \ln(2)$. Assim:

$$\frac{\ln(a_{n+1})}{\ln(q_n)} + 1 < \frac{\ln(q_{n+1})}{\ln(q_n)} \le \frac{\ln(a_{n+1})}{\ln(q_n)} + \frac{\ln(2)}{\ln(q_n)} + 1$$

Tomando o limite superior quando $n \to \infty$, e observando que $\frac{\ln(2)}{\ln(q_n)} \to 0$, obtemos:

$$1 + \limsup_{n\to\infty} \frac{\ln(a_{n+1})}{\ln(q_n)} \le \limsup_{n\to\infty} \frac{\ln(q_{n+1})}{\ln(q_n)} \le 1 + \limsup_{n\to\infty} \frac{\ln(a_{n+1})}{\ln(q_n)}$$

Logo, pela equação (13), concluímos:

$$\mu_{\mathcal{L}}(\alpha) = 1 + \left(1 + \limsup_{n\to\infty} \frac{\ln(a_{n+1})}{\ln(q_n)}\right) = 2 + \limsup_{n\to\infty} \frac{\ln(a_{n+1})}{\ln(q_n)} \tag{15}$$

□

Com a fórmula estabelecida, podemos aplicá-la para calcular a medida de irracionalidade de números cujas expansões em frações contínuas seguem padrões conhecidos. O exemplo mais notável é o número de Euler e, para o qual a regularidade dos denominadores parciais permite um cálculo direto.

Teorema 3.4. *A medida de irracionalidade do número de Euler e é igual a 2.*

Demonstração. Para demonstrar este resultado, utilizaremos a fórmula estabelecida no Teorema 3.3:

$$\mu_{\mathcal{L}}(e) = 2 + \limsup_{n\to\infty} \frac{\ln(a_{n+1})}{\ln(q_n)}$$

A expansão em frações contínuas simples para o número de Euler e segue um padrão regular bem conhecido, cuja demonstração pode ser encontrada em [5]:

$$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots, 1, 1, 2k, \ldots]$$

Para índices $m \geq 1$, os denominadores parciais a_m seguem a estrutura: $a_m = 2k$ se $m = 3k - 1$, e $a_m = 1$ caso contrário.

Note que a subsequência de $\{a_n\}$ com os maiores valores ocorre quando $n + 1 \equiv 2 \pmod 3$, bastando então considerá-la para o limite superior. Se $n + 1 = 3k - 1$, então $k = (n + 2)/3$, e o denominador parcial é $a_{n+1} = 2(n + 2)/3 < n + 2$. Para todos os outros casos, $a_{n+1} = 1$. Portanto, para todo $n \geq 1$, temos a estimativa:

$$1 \leq a_{n+1} < n + 2$$

Tomando o logaritmo, obtemos $0 \leq \ln(a_{n+1}) < \ln(n + 2)$, o que indica que o numerador da fórmula do limite cresce logaritmicamente em relação a n.

Por outro lado, os denominadores dos convergentes q_n são definidos pela relação de recorrência (14): $q_n = a_n q_{n-1} + q_{n-2}$, com $q_0 = 1$ e $q_1 = a_1$. Como $a_n \geq 1$ para todo n, os denominadores crescem pelo menos tão rápido quanto a sequência de Fibonacci (F_n). Usando a aproximação de forma fechada para os números de Fibonacci, sabemos que $F_n \approx \phi^n/\sqrt{5}$, onde ϕ é a proporção áurea. Assim, q_n cresce exponencialmente. Tomando o logaritmo natural, obtemos uma estimativa linear: $\ln(q_n) \geq \ln(F_{n+1}) \approx n \ln(\phi)$. Portanto, existe uma constante $C > 0$ tal que, para n suficientemente grande, $\ln(q_n) > C \cdot n$.

Substituindo essas estimativas no termo dentro do limite superior:

$$0 \leq \frac{\ln(a_{n+1})}{\ln(q_n)} < \frac{\ln(n + 2)}{C \cdot n}$$

Calculando o limite quando $n \to \infty$ (notando que, se o limite existe, é igual ao limite superior), e observando que o crescimento logarítmico é mais lento que o linear, temos:

$$\lim_{n\to\infty} \frac{\ln(n + 2)}{C \cdot n} = 0$$

Concluímos que $\limsup_{n\to\infty} \frac{\ln(a_{n+1})}{\ln(q_n)} = 0$. Aplicando este resultado à fórmula original, obtemos:

$$\mu_{\mathcal{L}}(e) = 2 + 0 = 2$$

□

Uma demonstração semelhante também garante que $\mu_{\mathcal{L}}(\tan(1)) = 2$, pois sua expansão em frações contínuas é $[1; 1, 1, 3, 1, 5, 1, 7, 1, \ldots]$, na qual o crescimento linear dos denominadores parciais a_n também será dominado pelo crescimento exponencial dos numeradores dos convergentes q_n. Mais que isso, é possível provar que o mesmo vale para qualquer número real da forma $\tan(1/k)$, para $k \in \mathbb{N}$ (a demonstração deste fato pode ser encontrada em [6, p. 212]).

Apesar de a medida de irracionalidade de Liouville-Roth fornecer uma classificação importante para os números reais, distinguindo algébricos de alguns transcendentais (como os números de Liouville), ela pode ser insuficiente para distinguir a "qualidade" da aproximação entre números que possuem a mesma medida. Por exemplo, sabemos que quase todos os números reais possuem medida de irracionalidade igual a 2. Isso motiva a seguinte definição, encontrada em [7].

Definição 3.3. *Uma medida de irracionalidade generalizada é uma função $f(x, \lambda)$, definida para $x \geq 1$ e $\lambda > 0$, que assume valores nos reais positivos e é estritamente decrescente tanto em x quanto em λ (isto é, para todo λ fixo, $x_1 < x_2 \implies f(x_1, \lambda) > f(x_2, \lambda)$, e para todo x fixo, $\lambda_1 < \lambda_2 \implies f(x, \lambda_1) > f(x, \lambda_2)$). Se existe $\lambda > 0$ com a propriedade de que, para qualquer $\varepsilon > 0$, existe um inteiro positivo $q(\varepsilon)$ tal que*

$$\left|\alpha - \frac{p}{q}\right| > f(q, \lambda+\varepsilon), \quad \textit{para todos os inteiros } p, q, \textit{ com } q \geq q(\varepsilon),$$

então denotamos por $\lambda(\alpha)$ o menor tal λ, e dizemos que α tem medida de irracionalidade $f(x, \lambda(\alpha))$. Caso contrário, se tal λ não existir, escrevemos $\lambda(\alpha) = \infty$.

Se tomarmos $f(x, \lambda) = x^{-\lambda}$, obtemos a medida de irracionalidade de Liouville-Roth. Um outro exemplo é a chamada base de irracionalidade, que consegue distinguir alguns números de Liouville:

Definição 3.4. *A base de irracionalidade de um número real α, denotada por $\mu_{\mathcal{B}}(\alpha)$, é definida como o menor número real $\beta \geq 1$ tal que, para todo $\varepsilon > 0$, existe um $q(\varepsilon)$ tal que a desigualdade*

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{(\beta+\varepsilon)^q} \tag{16}$$

vale para todos os inteiros p, q com $q \geq q(\varepsilon)$. Isso corresponde a tomar a medida de irracionalidade generalizada com a função $f(x, \lambda) = \lambda^{-x}$.

Caso não exista tal β (ou seja, se a desigualdade falhar para β arbitrariamente grande), definimos $\mu_{\mathcal{B}}(\alpha) = \infty$ e dizemos que α é um número super Liouville.

Alternativamente, podemos defini-la de maneira análoga ao expoente de irracionalidade:

$$\mu_{\mathcal{B}}(\alpha) = \sup\left\{\beta \in \mathbb{R} : \left|\alpha - \frac{p}{q}\right| < \frac{1}{\beta^q} \textit{ admite infinitas soluções}\right\}$$

Proposição 3.5. *As duas definições de base de irracionalidade são equivalentes.*

Demonstração. Seja μ_1 o valor de $\mu_{\mathcal{B}}(\alpha)$ dado pela primeira definição e μ_2 o valor dado pela definição alternativa.

A primeira definição estabelece que μ_1 é o menor número real $\beta \geq 1$ tal que, para todo $\varepsilon > 0$, a desigualdade

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{(\beta+\varepsilon)^q}$$

vale para todos os inteiros p, q com q suficientemente grande ($q \geq q(\varepsilon)$).

Essa condição implica que, para qualquer $\varepsilon > 0$, a desigualdade inversa

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{(\beta+\varepsilon)^q}$$

é satisfeita por apenas um número finito de valores de q. Consequentemente, a desigualdade estrita

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{(\beta+\varepsilon)^q}$$

também admite apenas um número finito de soluções.

Considere agora a segunda definição::

$$\mu_2 = \sup(S), \text{ com } S = \left\{\beta \in \mathbb{R} : \left|\alpha - \frac{p}{q}\right| < \frac{1}{\beta^q} \text{ admite infinitas soluções}\right\}$$

Primeiro, provamos que $\mu_2 \leq \mu_1$. Da análise da primeira definição, sabemos que para qualquer $\varepsilon > 0$, o valor $\beta = \mu_1 + \varepsilon$ resulta em apenas um número finito de soluções. Portanto, $\mu_1 + \varepsilon$ não pode pertencer ao conjunto S (que exige infinitas soluções). Além disso, se algum $x > \mu_1 + \varepsilon$ estivesse em S, então $|\alpha - p/q| < x^{-q}$ teria infinitas soluções. Como $x^{-q} < (\mu_1 + \varepsilon)^{-q}$, isso implicaria infinitas soluções para $\mu_1 + \varepsilon$, o que é falso. Logo, todo elemento de S deve ser menor ou igual a $\mu_1 + \varepsilon$. Como isso vale para todo $\varepsilon > 0$, o supremo de S não pode exceder μ_1. Portanto, $\mu_2 \leq \mu_1$.

A seguir, provamos que $\mu_1 \leq \mu_2$. Devemos mostrar que μ_2 satisfaz a condição exigida pela primeira definição. Seja $\varepsilon > 0$ arbitrário. Suponha, por contradição, que a condição falhe para μ_2. Isso significaria que a desigualdade

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{(\mu_2+\varepsilon)^q}$$

não vale para todo q grande. Em outras palavras, sua negação vale para infinitos q:

$$\left|\alpha - \frac{p}{q}\right| \leq \frac{1}{(\mu_2+\varepsilon)^q}$$

Note que para qualquer δ tal que $0 < \delta < \varepsilon$, temos $(\mu_2 + \varepsilon) > (\mu_2 + \delta)$, o que implica $(\mu_2 + \varepsilon)^{-q} < (\mu_2 + \delta)^{-q}$. Portanto, se a desigualdade acima vale infinitas vezes, então

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{(\mu_2 + \delta)^q}$$

também admite infinitas soluções. Isso implica que $\mu_2 + \delta$ pertence ao conjunto S. No entanto, como $\delta > 0$, isso significa que existe um elemento em S estritamente maior que μ_2. Isso contradiz a definição de μ_2 como o supremo de S. Assim, a suposição é falsa, e μ_2 satisfaz a condição da primeira definição. Como μ_1 é definido como o *menor* número satisfazendo essa condição, devemos ter $\mu_1 \leq \mu_2$.

Como $\mu_2 \leq \mu_1$ e $\mu_1 \leq \mu_2$, concluímos que $\mu_1 = \mu_2$. □

Tendo verificado a equivalência, podemos provar algumas propriedades da base de irracionalidade. A primeira é a existência de números super Liouville, que faremos através da construção de um exemplo.

Proposição 3.6. *A soma da seguinte série é um número super Liouville:*

$$S = \frac{1}{1} + \frac{1}{2^1} + \frac{1}{4^{2^1}} + ...$$

Demonstração. Escrevemos $S = \sum_{n=1}^{\infty} \frac{1}{b_n}$. Como b_{n-1} divide b_n para todo $n > 1$, a n-ésima soma parcial da série pode ser escrita como a_n/b_n para algum inteiro a_n.

Analisando o erro da aproximação, temos:

$$0 < S - \frac{a_n}{b_n} = \sum_{k=n+1}^{\infty} \frac{1}{b_k} < \frac{2}{b_{n+1}}$$

Substituindo a definição de b_{n+1}, obtemos:

$$\frac{2}{b_{n+1}} = \frac{2}{(2^{n+1})^{b_n}}$$

Para $n \geq 2$, temos que $2 < 2^{b_n}$, o que nos permite refinar a cota superior:

$$\frac{2}{(2^{n+1})^{b_n}} < \frac{1}{(2^n)^{b_n}}$$

Combinando as desigualdades, obtemos para $n \geq 2$:

$$\left|S - \frac{a_n}{b_n}\right| < \frac{1}{(2^n)^{b_n}}$$

Se considerarmos a definição alternativa de base de irracionalidade, estamos interessados no supremo dos valores β tais que $|\alpha - p/q| < \beta^{-q}$ possui infinitas soluções.

Neste caso, para qualquer $B > 0$, podemos escolher um inteiro n tal que $2^n > B$. A desigualdade acima mostra que a_n/b_n é uma solução para $\beta = 2^n$. Como podemos fazer isso para infinitos n, concluímos que o conjunto de tais β não é limitado superiormente.

Portanto, $\mu_{\mathcal{B}}(S) = \infty$, e S é um número super Liouville. □

Com esse resultado, podemos ter a intuição de que obter uma cota superior para a base de irracionalidade é uma condição muito mais fraca (uma vez que a série que usamos para obter base infinita converge muito mais rapidamente que a que usamos para a medida de irracionalidade infinita) do que obter uma cota superior para a medida de irracionalidade de Liouville-Roth. De fato, se reescrevermos a desigualdade (16) como

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

vemos que o expoente de q no lado direito é $-\frac{q}{\log q}\log(\beta + \varepsilon)$, que tende a $-\infty$ conforme $q \to \infty$. Em contraste, para uma medida de irracionalidade finita μ, a cota inferior é da ordem de $q^{-\mu}$, onde o expoente é constante.

Como a função $q^{-\frac{q}{\log q}C}$ decresce muito mais rapidamente do que $q^{-\mu}$ para qualquer constante μ, a cota inferior imposta pela base de irracionalidade é muito menor (ou seja, mais próxima de

zero). Uma cota inferior menor significa que a desigualdade é mais fácil de ser satisfeita, pois permite que as aproximações racionais p/q estejam muito mais próximas de α sem violar a condição. Especificamente, uma base de irracionalidade finita permite aproximações exponencialmente boas (como as que ocorrem para números de Liouville), enquanto uma medida de irracionalidade finita restringe as aproximações a serem apenas polinomialmente boas.

Portanto, a classe de números com base de irracionalidade finita é muito mais ampla e inclui números com medida de irracionalidade infinita (como o número super Liouville construído na Proposição 3.6). De fato, qualquer número com medida de irracionalidade finita μ possui automaticamente base de irracionalidade $\mu_{\mathcal{B}}(\alpha) = 1$:

Proposição 3.7. *Um irracional α que não é de Liouville (i.e., $\mu_{\mathcal{L}}(\alpha) \neq \infty$) possui base de irracionalidade $\mu_{\mathcal{B}}(\alpha) = 1$.*

Demonstração. Se $\mu = \mu_{\mathcal{L}}(\alpha)$ é finita, então para qualquer $\varepsilon > 0$ sabemos que existe q_0 tal que, para todo $q > q_0$:

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{q^{\mu+\varepsilon}}$$

Note que, para q suficientemente grande, a função exponencial $(1+\varepsilon)^q$ cresce muito mais rapidamente que a função polinomial $q^{\mu+\varepsilon}$. Portanto, existe q_1 tal que para $q > q_1$:

$$q^{\mu+\varepsilon} < (1+\varepsilon)^q \implies \frac{1}{q^{\mu+\varepsilon}} > \frac{1}{(1+\varepsilon)^q}$$

Combinando as desigualdades para $q > \max(q_0, q_1)$, temos:

$$\left|\alpha - \frac{p}{q}\right| > \frac{1}{(1+\varepsilon)^q}$$

Portanto, para qualquer $\beta > 1$, podemos escolher ε tal que $1 + \varepsilon < \beta$, e a desigualdade $|\alpha - p/q| > \beta^{-q}$ valerá para todo q suficientemente grande. Logo, $\mu_{\mathcal{B}}(\alpha)$ deve ser igual a 1. □

Também é possível encontrar uma fórmula análoga a 3.3 para a base de irracionalidade:

Teorema 3.8. *Seja α um irracional cuja expansão em frações contínuas é $[a_0; a_1, a_2, ...]$. Então:*

$$\ln(\mu_{\mathcal{B}}(\alpha)) = \limsup_{n\to\infty} \frac{\ln q_{n+1}}{q_n} = \limsup_{n\to\infty} \frac{\ln a_{n+1}}{q_n}$$

Demonstração. De maneira análoga à demonstração do Teorema 3.3, definimos λ_n pela equação

$$\left|\alpha - \frac{p_n}{q_n}\right| = \lambda_n^{-q_n} \tag{17}$$

Pela definição alternativa de base de irracionalidade (Definição 3.4), $\mu_{\mathcal{B}}(\alpha)$ é o supremo dos valores β tais que a desigualdade $|\alpha - p/q| < \beta^{-q}$ admite infinitas soluções.

Primeiramente, justificamos que basta considerar os convergentes para essa análise. Suponha que $\beta > 1$. Note que a função exponencial β^q cresce muito mais rapidamente que a função polinomial $2q^2$. Portanto, para q suficientemente grande, temos $\beta^q > 2q^2$, o que implica $\beta^{-q} < \frac{1}{2q^2}$.

Assim, se um racional p/q (com q grande o suficiente) satisfaz $|\alpha - p/q| < \beta^{-q}$, ele necessariamente satisfaz:

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

Pelo Lema 3.2, isso garante que p/q é um convergente da expansão em frações contínuas de α. Logo, para calcular o supremo dos β (que certamente será ≥ 1 para irracionais), podemos restringir nossa busca à subsequência dos convergentes.

A desigualdade $|\alpha - p_n/q_n| < \beta^{-q_n}$ equivale a $\lambda_n^{-q_n} < \beta^{-q_n}$, o que implica $\lambda_n > \beta$. Portanto:

$$\mu_{\mathcal{B}}(\alpha) = \limsup_{n\to\infty} \lambda_n$$

Utilizando as desigualdades do Teorema 3.1:

$$\frac{1}{2q_nq_{n+1}} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_nq_{n+1}}$$

Substituindo a definição de λ_n:

$$\frac{1}{2q_nq_{n+1}} < \lambda_n^{-q_n} < \frac{1}{q_nq_{n+1}}$$

Tomando o logaritmo natural e multiplicando por -1 (invertendo as desigualdades):

$$\ln(2q_nq_{n+1}) > q_n \ln \lambda_n > \ln(q_nq_{n+1})$$

Dividindo por q_n:

$$\frac{\ln 2 + \ln q_n + \ln q_{n+1}}{q_n} > \ln \lambda_n > \frac{\ln q_n + \ln q_{n+1}}{q_n}$$

Reorganizando os termos:

$$\frac{\ln q_{n+1}}{q_n} + \frac{\ln q_n}{q_n} + \frac{\ln 2}{q_n} > \ln \lambda_n > \frac{\ln q_{n+1}}{q_n} + \frac{\ln q_n}{q_n}$$

Note que $\frac{\ln q_n}{q_n} \to 0$ (pois $q_n \to \infty$). O termo $\frac{\ln 2}{q_n}$ também tende a zero quando n tende ao infinito. Portanto:

$$\limsup_{n\to\infty} \ln \lambda_n = \limsup_{n\to\infty} \frac{\ln q_{n+1}}{q_n}$$

Como a função logaritmo é contínua e crescente, e $\lambda_n \geq 1$, vale que

$$\ln(\limsup \lambda_n) = \limsup(\ln \lambda_n).$$

Logo:

$$\ln(\mu_{\mathcal{B}}(\alpha)) = \limsup_{n\to\infty} \frac{\ln q_{n+1}}{q_n}$$

Isso prova a primeira igualdade. Para a segunda, usamos novamente a relação $q_{n+1} = a_{n+1}q_n + q_{n-1}$.

$$a_{n+1}q_n < q_{n+1} < (a_{n+1}+1)q_n$$

Tomando o logaritmo:

$$\ln a_{n+1} + \ln q_n < \ln q_{n+1} < \ln(a_{n+1}+1) + \ln q_n$$

Dividindo por q_n:

$$\frac{\ln a_{n+1}}{q_n} + \frac{\ln q_n}{q_n} < \frac{\ln q_{n+1}}{q_n} < \frac{\ln(a_{n+1}+1)}{q_n} + \frac{\ln q_n}{q_n}$$

Novamente, $\frac{\ln q_n}{q_n} \to 0$. Além disso, $\ln(a_{n+1}+1) - \ln a_{n+1} = \ln(1 + 1/a_{n+1}) \leq \ln 2$. Portanto, a diferença entre o termo da direita e o da esquerda tende a zero. Assim:

$$\limsup_{n\to\infty} \frac{\ln q_{n+1}}{q_n} = \limsup_{n\to\infty} \frac{\ln a_{n+1}}{q_n}$$

O que conclui a demonstração. □

Referências

[1] Ragognette, Luis Fernando: *Uma demonstração do teorema de Thue-Siegel-Dyson-Roth*. Dissertação de mestrado, Universidade de São Paulo, 2012.

[2] Guth, Larry: *Polynomial Methods in Combinatorics*, volume 64 de *University Lecture Series*. American Mathematical Society, 2016.

[3] Hindry, Marc e Silverman, Joseph H.: *Diophantine Geometry: An Introduction*, volume 201 de *Graduate Texts in Mathematics*. Springer-Verlag, 2000, ISBN 978-0387989815.

[4] Lang, Serge: *Introduction to Diophantine Approximations*. Springer-Verlag, 1995, ISBN 978-1461287001.

[5] Cohn, Henry: *A Short Proof of the Simple Continued Fraction Expansion of e*. The American Mathematical Monthly, 113(1):57–62, 2006.

[6] Walters, R. F. C.: *Alternative Derivation of Some Regular Continued Fractions*. Journal of the Australian Mathematical Society, 8:205–212, 1968.

[7] Sondow, Jonathan: *Irrationality Measures, Irrationality Bases, and a Theorem of Jarnik*. arXiv preprint math/0406300, 2004.