# Frações Contínuas, Representações de Números e Aproximações Diofantinas

**Carlos Gustavo T. de A. Moreira**

**I M P A**

**1º Colóquio da Região Sudeste**

**Abril de 2011**

# Sumário


**1 Frações Contínuas** **1**

1.1 Introdução . . . . . 1

1.2 Reduzidas e Boas Aproximações . . . . . 9

1.3 Boas Aproximações são Reduzidas . . . . . 11

1.4 Frações Contínuas Periódicas . . . . . 14

1.5 Problemas Propostos . . . . . 17

**2 Frações Contínuas e Aproximações Diofantinas** **21**

2.1 Introdução . . . . . 21

2.2 O Teorema de Khintchine via frações contínuas . . . . . 23

2.3 O Teorema de Khintchine $n$-dimensional . . . . . 25

2.4 Aproximações diofantinas não-homogêneas . . . . . 28

2.5 Números de Liouville . . . . . 31

2.6 Problemas Propostos . . . . . 32

**3 Os Espectros de Markov e Lagrange** **35**

3.1 Definições e enunciados . . . . . 35

3.2 Problemas Propostos . . . . . 37

**Referências Bibliográficas** **39**

# Capítulo 1

# Frações Contínuas

## 1.1 Introdução

A teoria de frações contínuas é um dos mais belos assuntos da Matemática elementar, sendo ainda hoje tema de pesquisa.

Nas inclusões $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$, a passagem de $\mathbb{Q}$ para $\mathbb{R}$ é sem dúvida a mais complicada conceitualmente e a representação de um número real está diretamente ligada à própria noção de número real.

De fato, o conceito de número natural é quase um conceito primitivo. Já um número inteiro é um número natural com um sinal que pode ser $+$ ou $-$, e um número racional é a razão entre um número inteiro e um natural não nulo. Por outro lado, dizer o que é um número real é tarefa bem mais complicada, mas há coisas que podemos dizer sobre eles. Uma propriedade essencial de $\mathbb{R}$ é que todo número real pode ser bem aproximado por números racionais. Efetivamente, dado $x \in \mathbb{R}$, existe $k = \lfloor x \rfloor \in \mathbb{Z}$ tal que $0 \le x - k < 1$. Podemos escrever a representação decimal de

$$x - k = 0, a_1 a_2 \dots a_n \dots, \qquad a_i \in \{0, 1, \dots, 9\},$$

o que significa que se $r_n = a_n + 10 \cdot a_{n-1} + 100 \cdot a_{n-2} + \cdots + 10^{n-1} \cdot a_1$, então $\frac{r_n}{10^n} \le x - k < \frac{r_n + 1}{10^n}$, e portanto $k + \frac{r_n}{10^n}$ é uma boa aproximação racional de $x$, no sentido de que o erro $\left|x - \left(k + \frac{r_n}{10^n}\right)\right|$ é menor do que $\frac{1}{10^n}$, que é um número bem pequeno se $n$ for grande. A representação decimal de um número real fornece pois uma sequência de aproximações por racionais cujos denominadores são potências de 10.

Vamos lembrar uma notação que nos será muito útil: dado $x \in \mathbb{R}$, definimos a *parte inteira* de $x$ como o único inteiro $\lfloor x \rfloor$ tal que $\lfloor x \rfloor \le x < \lfloor x \rfloor + 1$, e a *parte fracionária* de $x$ como $\{x\} = x - \lfloor x \rfloor \in [0, 1)$.

A representação decimal de números reais está intimamente ligada à função $f : [0, 1) \to [0, 1)$ dada por $f(x) = \{10x\} = 10x - \lfloor 10x \rfloor$ (mais precisamente, à *dinâmica* da função $f$, i.e., ao estudo de suas composições sucessivas). De fato, se $x \in [0, 1)$ tem representação decimal $0, a_1 a_2 a_3 \dots$, então $a_1 = \lfloor 10x \rfloor$ e $f(x) = 0, a_2 a_3 a_4 \dots$. Assim, definindo $f^1 = f$ e $f^{n+1} = f \circ f^n$, temos $f^n(x) = 0, a_{n+1} a_{n+2} a_{n+3} \dots$ para todo $n \ge 1$.

Dado qualquer $x \in \mathbb{R}$ e $q$ natural não nulo existe $p \in \mathbb{Z}$ tal que $\frac{p}{q} \leq x < \frac{p+1}{q}$ (basta tomar $p$ inteiro tal que $p \leq qx < p+1$, i.e., $p = \lfloor qx \rfloor$), e portanto $\left|x - \frac{p}{q}\right| < \frac{1}{q}$ e $\left|x - \frac{p+1}{q}\right| \leq \frac{1}{q}$. Em particular há aproximações de $x$ por racionais com denominador $q$ com erro menor do que $\frac{1}{q}$. A representação decimal de $x$ equivale a dar essas aproximações para os denominadores $q$ que são potências de 10, e tem méritos como sua praticidade para efetuar cálculos que a fazem a mais popular das representações dos números reais. Por outro lado, envolve a escolha arbitrária da base 10, e oculta frequentemente aproximações racionais de $x$ muito mais eficientes do que as que exibe.

Senão vejamos: tomemos um número real totalmente ao acaso, digamos

$$\pi = 3,14159265358979323846264338327950 2884\ldots.$$

Uma aproximação clássica de $\pi$ por um número racional é $22/7 = 3,142857142857\ldots$, devida a Arquimedes. Uma outra aproximação ainda melhor é $355/113 = 3,1415929203539823\ldots$. Note que

$$\left|\pi - \frac{22}{7}\right| < \frac{1}{700} < \left|\pi - \frac{314}{100}\right| \text{ e } \left|\pi - \frac{355}{113}\right| < \frac{1}{3000000} < \left|\pi - \frac{3141592}{1000000}\right|,$$

e portanto $\frac{22}{7}$ e $\frac{355}{113}$ são melhores aproximações de $\pi$ que aproximações decimais com denominadores muito maiores, e de fato são aproximações muito mais espetacularmente boas do que se poderia esperar pelo tamanho dos denominadores envolvidos.

Vamos apresentar uma outra maneira de representar números reais, a representação por *frações contínuas*, que sempre fornece aproximações racionais surpreendentemente boas, e de fato fornece todas as aproximações excepcionalmente boas, além de ser natural e conceitualmente simples.

Definimos recursivamente

$$\alpha_0 = x, \quad a_n = \lfloor \alpha_n \rfloor$$
$$\text{e, se } \alpha_n \notin \mathbb{Z}, \quad \alpha_{n+1} = \frac{1}{\alpha_n - a_n} = \frac{1}{\{\alpha_n\}}, \text{ para todo } n \in \mathbb{N}.$$

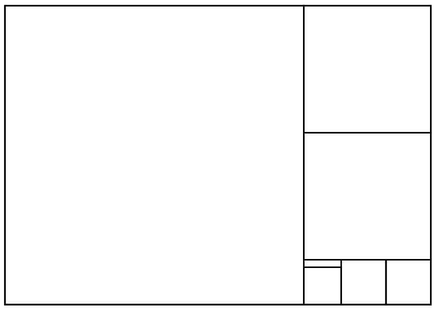
Se, para algum $n$, $\alpha_n = a_n$ temos

$$x = \alpha_0 = [a_0; a_1, a_2, \ldots, a_n] \stackrel{\text{def}}{=} a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}.$$

Se não, denotamos

$$x = [a_0; a_1, a_2, \ldots] \stackrel{\text{def}}{=} a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}}.$$

O sentido dessa última notação ficará claro mais tarde. A representação acima se chama *representação por frações contínuas de $x$*.



A figura dá uma interpretação geométrica para a representação de um número por frações contínuas. Enchemos um retângulo $1 \times x$ com quadrados de forma "gulosa", isto é, sempre colocando o maior quadrado possível dentro do espaço ainda livre. Os coeficientes $a_0, a_1, a_2, \ldots$ indicam o número de quadrados de cada tamanho. Na figura, se os lados do retangulo são $c < d$ então

$$d/c = [1; 2, 2, 1, ...]$$

pois temos $a_0 = 1$ quadrado grande, $a_1 = 2$ quadrados menores, $a_2 = 2$ quadrados ainda menores, $a_3 = 1$ quadrados ainda ainda menores, e um número grande não desenhado de quadrados ainda ainda ainda menores ($a_4$ é grande). Deixamos a verificação de que esta descrição geométrica corresponde à descrição algébrica acima a cargo do leitor.

Do mesmo modo que a representação decimal está ligada à dinâmica da função $f(x) = \{10x\}$, como vimos anteriormente, a representação em frações contínuas está intimamente ligada à dinâmica da função $g : (0,1) \to [0,1)$, dada por $g(x) = \{\frac{1}{x}\} = \frac{1}{x} - \lfloor \frac{1}{x} \rfloor$, também conhecida como *transformação de Gauss*: se $x = [0; a_1, a_2, a_3, \ldots] \in (0,1)$, então $a_1 = \lfloor \frac{1}{x} \rfloor$ e $g(x) = [0; a_2, a_3, a_4, ...]$. Assim, definindo, como antes $g^1 = g$ e $g^{n+1} = g \circ g^n$ para todo $n \geq 1$, temos $g^n(x) = [0; a_{n+1}, a_{n+2}, a_{n+3}, \ldots]$, para todo $n \geq 1$.

Note que, se a representação por frações contínuas de $x$ for finita então $x$ é claramente racional.

Reciprocamente, se $x \in \mathbb{Q}$, sua representação será finita, e seus coeficientes $a_n$ vêm do algoritmo de Euclides: se $x = p/q$ (com $q > 0$) temos

$$\begin{array}{rcll} p & = & a_0 q + r_1, & 0 \leq r_1 < q. \\ q & = & a_1 r_1 + r_2, & 0 \leq r_2 < r_1, \\ r_1 & = & a_2 r_2 + r_3, & 0 \leq r_3 < r_2, \\ & \vdots & \vdots & \\ r_{n-1} & = & a_n r_n, & r_{n+1} = 0 \end{array}$$

Temos então

$$x = p/q = a_0 + r_1/q = a_0 + \frac{1}{a_1 + r_2/r_1} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + r_3/r_2}}$$

$$= \cdots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}} = [a_0; a_1, a_2, \ldots, a_n].$$

Isso já é uma vantagem da representação por frações contínuas (além de não depender de escolhas artificiais de base), pois o reconhecimento de racionais é mais simples que na representação decimal.

Seja $x = [a_0; a_1, a_2, \ldots]$. Sejam $p_n \in \mathbb{Z}$, $q_n \in \mathbb{N}_{>0}$ primos entre si tais que $\frac{p_n}{q_n} = [a_0; a_1, a_2, \ldots, a_n]$, $n \geq 0$. Esta fração $\frac{p_n}{q_n}$ é chamada de $n$-ésima *reduzida* ou *convergente* da fração contínua de $x$. O seguinte resultado será fundamental no que seguirá.

**Proposição 1.1** *Dada uma sequência (finita ou infinita) $t_0, t_1, t_2, \cdots \in \mathbb{R}$ tal que $t_k > 0$, para todo $k \geq 1$, definimos sequências $(x_m)$ e $(y_m)$ por*
*$x_0 = t_0$, $y_0 = 1$, $x_1 = t_0 t_1 + 1$, $y_1 = t_1$,*
*$x_{m+2} = t_{m+2} x_{m+1} + x_m$, $y_{m+2} = t_{m+2} y_{m+1} + y_m$, $\forall m \geq 0$. Temos então*

$$[t_0; t_1, t_2, \ldots, t_n] = t_0 + \cfrac{1}{t_1 + \cfrac{1}{t_2 + \ddots + \cfrac{1}{t_n}}} = \frac{x_n}{y_n}, \forall n \geq 0.$$

*Além disso, $x_{n+1} y_n - x_n y_{n+1} = (-1)^n, \forall n \geq 0$.*

**Demonstração:** A prova será por indução em $n$. Para $n = 0$ temos $[t_0] = t_0 = t_0/1 = x_0/y_0$. Para $n = 1$, temos $[t_0; t_1] = t_0 + 1/t_1 = \frac{t_0 t_1 + 1}{t_1} = x_1/y_1$ e, para $n = 2$, temos

$$[t_0; t_1, t_2] = t_0 + \frac{1}{t_1 + 1/t_2} = t_0 + \frac{t_2}{t_1 t_2 + 1} = \frac{t_0 t_1 t_2 + t_0 + t_2}{t_1 t_2 + 1}$$

$$= \frac{t_2(t_0 t_1 + 1) + t_0}{t_2 t_1 + 1} = \frac{t_2 x_1 + x_0}{t_2 y_1 + y_0} = \frac{x_2}{y_2}.$$

Suponha que a afirmação seja válida para $n$. Para $n + 1$ em lugar de $n$ temos

$$\begin{aligned}
[t_0; t_1, t_2, \ldots, t_n, t_{n+1}] &= [t_0; t_1, t_2, \ldots, t_n + \frac{1}{t_{n+1}}] \\
&= \frac{(t_n + \frac{1}{t_{n+1}}) x_{n-1} + x_{n-2}}{(t_n + \frac{1}{t_{n+1}}) y_{n-1} + y_{n-2}} \\
&= \frac{t_{n+1}(t_n x_{n-1} + x_{n-2}) + x_{n-1}}{t_{n+1}(t_n y_{n-1} + y_{n-2}) + y_{n-1}} \\
&= \frac{t_{n+1} x_n + x_{n-1}}{t_{n+1} y_n + y_{n-1}} = \frac{x_{n+1}}{y_{n+1}}.
\end{aligned}$$

Vamos agora mostrar, por indução, a segunda afirmação. Temos

$$\begin{aligned} x_1y_0 - x_0y_1 &= (t_0t_1 + 1) - t_0t_1 = 1 = (-1)^0 \\ &\text{e, se } x_{n+1}y_n - x_ny_{n+1} = (-1)^n, \\ x_{n+2}y_{n+1} - x_{n+1}y_{n+2} &= (t_{n+2}x_{n+1} + x_n)y_{n+1} - (t_{n+2}y_{n+1} + y_n)x_{n+1} \\ &= -(x_{n+1}y_n - x_ny_{n+1}) = -(-1)^n = (-1)^{n+1}. \end{aligned}$$

□

Nos próximos resultados, $x = [a_0; a_1, a_2, a_3, \ldots]$ será um número real, e $(\frac{p_n}{q_n})_{n\in\mathbb{N}}$, $\frac{p_n}{q_n} = [a_0; a_1, a_2, \ldots, a_n]$ será a sequência de reduzidas da fração contínua de $x$.

**Corolário 1.2** *As sequências $(p_n)$ e $(q_n)$ satisfazem as recorrências*

$$p_{n+2} = a_{n+2}p_{n+1} + p_n \qquad e \qquad q_{n+2} = a_{n+2}q_{n+1} + q_n$$

*para todo $n \geq 0$, com $p_0 = a_0$, $p_1 = a_0a_1 + 1$, $q_0 = 1$ e $q_1 = a_1$. Além disso,*

$$p_{n+1}q_n - p_nq_{n+1} = (-1)^n$$

*para todo $n \geq 0$.*

**Demonstração:** As sequências $(p_n)$ e $(q_n)$ definidas pelas recorrências acima satisfazem, pela proposição anterior, as igualdades

$$\frac{p_n}{q_n} = [a_0; a_1, a_2, \ldots, a_n] \text{ e } p_{n+1}q_n - p_nq_{n+1} = (-1)^n, \forall n \geq 0.$$

Como $p_{n+1}q_n - p_nq_{n+1} = (-1)^n$, para todo $n \in \mathbb{N}$, temos que os $p_n$, $q_n$ dados pelas recorrências acima são primos entre si. Além disso, também segue da recorrência que $q_n > 0, \forall n \geq 0$. Esses fatos implicam que $(\frac{p_n}{q_n})_{n\in\mathbb{N}}$ é a sequência de reduzidas da fração contínua de $x$. □

**Corolário 1.3** *Temos, para todo $n \in \mathbb{N}$,*

$$x = \frac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}} \qquad e \qquad \alpha_n = \frac{p_{n-2} - q_{n-2}x}{q_{n-1}x - p_{n-1}}$$

**Demonstração:** A primeira igualdade segue da proposição anterior pois $x = [a_0; a_1, a_2, \ldots, a_{n-1}, \alpha_n]$ e a segunda é consequência direta da primeira. □

**Proposição 1.4** *Temos*

$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{(\alpha_{n+1} + \beta_{n+1})q_n^2}$$

*onde*

$$\beta_{n+1} = \frac{q_{n-1}}{q_n} = [0; a_n, a_{n-1}, a_{n-2}, \ldots, a_1].$$

*Em particular,*

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

**Demonstração:** Pelo corolário anterior temos

$$x - \frac{p_n}{q_n} = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}} - \frac{p_n}{q_n} = \frac{p_{n-1}q_n - p_nq_{n-1}}{(\alpha_{n+1}q_n + q_{n-1})q_n}$$
$$= \frac{-(p_nq_{n-1} - p_{n-1}q_n)}{(\alpha_{n+1}q_n + q_{n-1})q_n} = \frac{-(-1)^{n-1}}{(\alpha_{n+1}q_n + q_{n-1})q_n} = \frac{(-1)^n}{(\alpha_{n+1}q_n + q_{n-1})q_n}$$
$$= \frac{(-1)^n}{(\alpha_{n+1} + q_{n-1}/q_n)q_n^2} = \frac{(-1)^n}{(\alpha_{n+1} + \beta_{n+1})q_n^2}.$$

Em particular,

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

e, como $\lfloor \alpha_{n+1} \rfloor = a_{n+1}$ e $0 < \beta_{n+1} < 1$, segue que $a_{n+1} < \alpha_{n+1} + \beta_{n+1} < a_{n+1} + 2$, o que implica a última afirmação.

A expansão de $\beta_{n+1}$ como fração contínua segue de

$$\frac{q_{n-1}}{q_n} = \frac{q_{n-1}}{a_nq_{n-1} + q_{n-2}} \implies \frac{q_{n-1}}{q_n} = \frac{1}{a_n + \frac{q_{n-2}}{q_{n-1}}}$$

aplicado recursivamente. □

**Observação 1.5** Como $\lim_{n\to\infty} q_n = +\infty$ (pois $(q_n)$ é estritamente crescente), segue desta proposição que

$$\lim_{n\to\infty} \frac{p_n}{q_n} = x,$$

o que permite recuperar $x$ a partir de $a_0, a_1, a_2, \ldots$, e dá sentido à igualdade $x = [a_0; a_1, a_2, \ldots]$ quando a fração contínua de $x$ é infinita (i.e., quando $x$ é irracional).

**Observação 1.6** A proposição anterior implica que, para todo $\alpha$ irracional, a desigualdade $|\alpha - p/q| < 1/q^2$ tem infinitas soluções racionais $p/q$. Este fato é conhecido como o *Teorema de Dirichlet*.

É interessante notar que, se $\alpha = r/s \in \mathbb{Q}$, a desigualdade $|\alpha - p/q| < 1/q^2$ tem apenas um número finito de soluções racionais $p/q$. De fato, $|r/s - p/q| < 1/q^2$ equivale a $|qr - ps| < s/q$, o que implica que $q \le s$.

**Curiosidade**: O denominador da $n$-ésima aproximação em base $B$ de um número real é $B^n$. Já o denominador $q_n$ da $n$-ésima aproximação por fração contínua de $x$ depende de $x$. Apesar disso, para quase todo real $x$, $\sqrt[n]{q_n}$ converge a $e^{\pi^2/12\ln 2} = 3,27582291872\ldots$ (um número real bastante simpático!) e $\sqrt[n]{\left|x - \frac{p_n}{q_n}\right|}$ converge a $e^{-\pi^2/6\ln 2} = 0,093187822954\ldots$.

A seguinte proposição mostra que os convergentes pares formam uma sequência crescente, e que os convergentes ímpares formam uma sequência decrescente. Além disso todos os convergentes ímpares são maiores do que todos os convergentes pares.

**Proposição 1.7** *Para todo $k \geq 0$, temos*

$$\frac{p_{2k}}{q_{2k}} \leq \frac{p_{2k+2}}{q_{2k+2}} \leq x \leq \frac{p_{2k+3}}{q_{2k+3}} \leq \frac{p_{2k+1}}{q_{2k+1}}.$$

**Demonstração:** O resultado segue dos seguintes fatos gerais. Para todo $n \geq 0$, temos que

$$\begin{aligned}\frac{p_{n+2}}{q_{n+2}} - \frac{p_n}{q_n} &= \frac{a_{n+2}p_{n+1} + p_n}{a_{n+2}q_{n+1} + q_n} - \frac{p_n}{q_n} \\ &= \frac{a_{n+2}(p_{n+1}q_n - p_n q_{n+1})}{q_n(a_{n+2}q_{n+1} + q_n)} = \frac{(-1)^n a_{n+2}}{q_{n+2}q_n}\end{aligned}$$

é positivo para $n$ par e negativo para $n$ ímpar. Além disso, para todo $n \geq 0$, temos que $x - \frac{p_n}{q_n} = \frac{(-1)^n}{(\alpha_{n+1}q_n + q_{n-1})q_n}$ é positivo para $n$ par e negativo para $n$ ímpar. □

**Proposição 1.8** *Sejam $a_0, a_1, \ldots, a_n$ inteiros com $a_k > 0, \forall k \geq 1$, e seja $(p_k/q_k)_{k\geq 0}$ a sequência de reduzidas da fração contínua $[a_0; a_1, a_2, \ldots, a_n]$. Então o conjunto dos números reais cuja representação por frações contínuas começa com $a_0, a_1, \ldots, a_n$ é o intervalo*

$$\begin{aligned} I(a_0, a_1, \ldots, a_n) &= \left\{\frac{p_n}{q_n}\right\} \cup \{[a_0, a_1, \ldots, a_n, \alpha], \alpha > 1\} \\ &= \begin{cases} \left[\frac{p_n}{q_n}, \frac{p_n + p_{n-1}}{q_n + q_{n-1}}\right) & \text{se } n \text{ é par} \\ \left(\frac{p_n + p_{n-1}}{q_n + q_{n-1}}, \frac{p_n}{q_n}\right] & \text{se } n \text{ é ímpar.} \end{cases} \end{aligned}$$

*Além disso, a função $G : (0, +\infty) \to I(a_0, a_1, \ldots, a_n)$ dada por $G(\alpha) = [a_0; a_1, a_2, \ldots, a_n, \alpha]$ é monótona, sendo crescente para $n$ ímpar e decrescente para $n$ par.*

**Demonstração:** É suficiente notar que, como na prova do corolário anterior, $G(\alpha) = [a_0; a_1, a_2, \ldots, a_n, \alpha] = \frac{\alpha p_n + p_{n-1}}{\alpha q_n + q_{n-1}} = \frac{p_n}{q_n} + \frac{(-1)^n}{(\alpha q_n + q_{n-1})q_n}$, e portanto $G$ é crescente para $n$

ímpar e decrescente para $n$ par. Assim, como $G(1) = \frac{p_n+p_{n-1}}{q_n+q_{n-1}}$ e $\lim_{\alpha\to+\infty} G(\alpha) = \frac{p_n}{q_n}$, temos

$$G((1,+\infty)) = \begin{cases} (\frac{p_n}{q_n}, \frac{p_n+p_{n-1}}{q_n+q_{n-1}}) & \text{se } n \text{ é par} \\ (\frac{p_n+p_{n-1}}{q_n+q_{n-1}}, \frac{p_n}{q_n}) & \text{se } n \text{ é ímpar.} \end{cases}$$

Portanto,

$$I(a_0, a_1, \ldots, a_n) = \left\{\frac{p_n}{q_n}\right\} \cup \{[a_0, a_1, \ldots, a_n, \alpha], \alpha > 1\}$$

$$= \left\{\frac{p_n}{q_n}\right\} \cup G((1,+\infty)) = \begin{cases} \left[\frac{p_n}{q_n}, \frac{p_n+p_{n-1}}{q_n+q_{n-1}}\right) & \text{se } n \text{ é par} \\ \left(\frac{p_n+p_{n-1}}{q_n+q_{n-1}}, \frac{p_n}{q_n}\right] & \text{se } n \text{ é ímpar.} \end{cases}$$

□

**Proposição 1.9** *Dados inteiros $a_0, a_1, a_2, \ldots$, com $a_k > 0, \forall k \geq 1$, existe um único número real $\alpha$ (que é irracional) cuja representação por frações contínuas é $[a_0; a_1, a_2, \ldots]$.*

**Demonstração:** Considere as sequências $(p_n)$ e $(q_n)$ definidas pelas recorrências

$$p_{n+2} = a_{n+2}p_{n+1} + p_n \qquad \text{e} \qquad q_{n+2} = a_{n+2}q_{n+1} + q_n$$

para todo $n \geq 0$, com $p_0 = a_0$, $p_1 = a_0a_1 + 1$, $q_0 = 1$ e $q_1 = a_1$. Temos, como na proposição 1.7,

$$\frac{p_{2k}}{q_{2k}} \leq \frac{p_{2k+2}}{q_{2k+2}} \leq \frac{p_{2k+3}}{q_{2k+3}} \leq \frac{p_{2k+1}}{q_{2k+1}}, \forall k \geq 0.$$

Assim, considerando os intervalos fechados

$$I_k = \left[\frac{p_{2k}}{q_{2k}}, \frac{p_{2k+1}}{q_{2k+1}}\right],$$

temos $I_{k+1} \subset I_k, \forall k \geq 0$, e portanto, como

$$|I_k| = \frac{p_{2k+1}}{q_{2k+1}} - \frac{p_{2k}}{q_{2k}} = \frac{p_{2k+1}q_{2k} - p_{2k}q_{2k+1}}{q_{2k+1}q_{2k}} = \frac{(-1)^{2k}}{q_{2k+1}q_{2k}} = \frac{1}{q_{2k+1}q_{2k}}$$

tende a 0 quando $k$ tende a infinito, existe $\alpha \in \mathbb{R}$ tal que

$$\bigcap_{k\geq 0} I_k = \{\alpha\}.$$

Como, para todo $k \geq 0$,

$$[a_0; a_1, a_2, \ldots, a_{2k}] = \frac{p_{2k}}{q_{2k}} \leq \alpha \leq \frac{p_{2k+1}}{q_{2k+1}} = [a_0; a_1, a_2, \ldots, a_{2k}, a_{2k+1}]$$

e, da proposição anterior, $[a_0; a_1, a_2, \ldots, a_{2k}]$ e $[a_0; a_1, a_2, \ldots, a_{2k}, a_{2k+1}]$ pertencem a $I(a_0; a_1, a_2, \ldots, a_{2k})$, que é um intervalo, segue que $\alpha \in I(a_0; a_1, a_2, \ldots, a_{2k})$, e portanto a fração contínua de $\alpha$ começa com $a_0, a_1, \ldots, a_{2k}$, para todo $k \geq 0$, donde a representação por frações contínuas de $\alpha$ é $[a_0; a_1, a_2, \ldots]$.

Note que, como a representação por frações contínuas de $\alpha$ é infinita, $\alpha$ é irracional.

□

**Exemplo 1.10** Temos

$\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, \dots]$, portanto

$$\frac{p_0}{q_0} = 3, \quad \frac{p_1}{q_1} = \frac{22}{7}, \quad \frac{p_2}{q_2} = \frac{333}{106}, \quad \frac{p_3}{q_3} = \frac{355}{113} \dots$$

$e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \dots, 1, 1, 2n, \dots]$ (veja o exercício 8).

$\sqrt{2} = [1; 2, 2, 2, \dots]$ pois

$$\sqrt{2} = 1 + \frac{1}{\sqrt{2}+1} = 1 + \cfrac{1}{2 + \cfrac{1}{\sqrt{2}+1}} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\sqrt{2}+1}}} = \cdots$$

$\frac{1+\sqrt{5}}{2} = [1; 1, 1, 1, \dots]$ pois

$$\frac{1+\sqrt{5}}{2} = 1 + \frac{1}{\frac{1+\sqrt{5}}{2}} = 1 + \cfrac{1}{1 + \cfrac{1}{\frac{1+\sqrt{5}}{2}}} = \cdots$$

Isto prova em particular que $\sqrt{2}$ e $\frac{1+\sqrt{5}}{2}$ são irracionais, pois suas frações contínuas são infinitas.

## 1.2 Reduzidas e Boas Aproximações

**Teorema 1.11** *Temos, para todo $n \in \mathbb{N}$,*

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

*Além disso,*

$$\left| x - \frac{p_n}{q_n} \right| < \frac{1}{2q_n^2} \qquad ou \qquad \left| x - \frac{p_{n+1}}{q_{n+1}} \right| < \frac{1}{2q_{n+1}^2}.$$

**Demonstração:** O número $x$ sempre pertence ao segmento de extremos $\frac{p_n}{q_n}$ e $\frac{p_{n+1}}{q_{n+1}}$ cujo comprimento é

$$\left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| = \left| \frac{(-1)^n}{q_n q_{n+1}} \right| = \frac{1}{q_n q_{n+1}} \implies \left| x - \frac{p_n}{q_n} \right| \leq \frac{1}{q_n q_{n+1}} < \frac{1}{q_n^2}.$$

Além disso, se

$$\left| x - \frac{p_n}{q_n} \right| \geq \frac{1}{2q_n^2} \qquad \text{e} \qquad \left| x - \frac{p_{n+1}}{q_{n+1}} \right| \geq \frac{1}{2q_{n+1}^2},$$

então
$$\frac{1}{q_nq_{n+1}} = \left|x - \frac{p_n}{q_n}\right| + \left|x - \frac{p_{n+1}}{q_{n+1}}\right| \geq \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2} \implies q_{n+1} = q_n,$$
absurdo. $\square$

**Observação 1.12** De fato $\left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_nq_{n+1}} < \frac{1}{a_{n+1}q_n^2}$. Quanto maior for $a_{n+1}$ melhor será a aproximação $\frac{p_n}{q_n}$ de $x$.

**Teorema 1.13 (Hurwitz, Markov)** *Para todo $\alpha$ irracional e todo inteiro $n \geq 1$, temos*
$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$$
*para pelo menos um racional*
$$\frac{p}{q} \in \left\{\frac{p_{n-1}}{q_{n-1}}, \frac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}\right\}$$
*Em particular, a desigualdade acima tem infinitas soluções racionais $p/q$.*

**Demonstração:** Suponha que o teorema seja falso. Então, pela proposição 1.4, existe $\alpha$ irracional, $n \geq 1$ com $\alpha_n + \beta_n \leq \sqrt{5}$, $\alpha_{n+1} + \beta_{n+1} \leq \sqrt{5}$ e $\alpha_{n+2} + \beta_{n+2} \leq \sqrt{5}$. Devemos portanto ter $a_{n+1} = a_{n+2} = 1$ já que claramente $a_k \leq 2$ para $k = n, n+1, n+2$ e se algum $a_k = 2$ com $k = n+1, n+2$, teríamos $a_k + \beta_k \geq 2 + \frac{1}{3} > \sqrt{5}$, absurdo.

Sejam $x = 1/\alpha_{n+2}$ e $y = \beta_{n+1}$. As desigualdades acima se traduzem em
$$\frac{1}{1+x} + \frac{1}{y} \leq \sqrt{5}, \qquad 1 + x + y \leq \sqrt{5} \qquad \text{e} \qquad \frac{1}{x} + \frac{1}{1+y} \leq \sqrt{5}.$$
Temos
$$\begin{aligned} 1 + x + y \leq \sqrt{5} &\implies 1 + x \leq \sqrt{5} - y \\ &\implies \frac{1}{1+x} + \frac{1}{y} \geq \frac{1}{\sqrt{5} - y} + \frac{1}{y} = \frac{\sqrt{5}}{y(\sqrt{5} - y)} \end{aligned}$$
e portanto $y(\sqrt{5} - y) \geq 1 \implies y \geq \frac{\sqrt{5}-1}{2}$. Por outro lado temos
$$\begin{aligned} x \leq \sqrt{5} - 1 - y \implies \frac{1}{x} + \frac{1}{1+y} &\geq \frac{1}{\sqrt{5} - 1 - y} + \frac{1}{1+y} \\ &= \frac{\sqrt{5}}{(1+y)(\sqrt{5} - 1 - y)} \end{aligned}$$
e portanto $(1+y)(\sqrt{5} - 1 - y) \geq 1 \implies y \leq \frac{\sqrt{5}-1}{2}$, e portanto devemos ter $y = \frac{\sqrt{5}-1}{2}$, o que é absurdo pois $y = \beta_{n+1} = \frac{q_{n-1}}{q_n} \in \mathbb{Q}$.

$\square$

**Observação 1.14** Em particular provamos que $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$ tem infinitas soluções racionais $\frac{p}{q}$, para todo $\alpha$ irracional. O número $\sqrt{5}$ é o maior com essa propriedade. De fato, se

$$\varepsilon > 0, \quad \alpha = \frac{1+\sqrt{5}}{2} \qquad \text{e} \qquad \left|\alpha - \frac{p}{q}\right| < \frac{1}{(\sqrt{5}+\varepsilon)q^2},$$

temos

$$\left|q\left(\frac{1+\sqrt{5}}{2}\right) - p\right| < \frac{1}{(\sqrt{5}+\varepsilon)q}$$

$$\Longrightarrow \left|q\left(\frac{1+\sqrt{5}}{2}\right) - p\right|\left|q\left(\frac{1-\sqrt{5}}{2}\right) - p\right| < \frac{\left|\frac{1-\sqrt{5}}{2} - \frac{p}{q}\right|}{\sqrt{5}+\varepsilon},$$

ou seja,

$$|p^2 - pq - q^2| < \left|\frac{1+\sqrt{5}}{2} - \frac{p}{q} - \sqrt{5}\right| \Big/ (\sqrt{5}+\varepsilon).$$

Se $q$ é grande, $1/q^2$ é pequeno, e $\frac{1+\sqrt{5}}{2} - \frac{p}{q}$ é muito próximo de 0, donde o lado direito da desigualdade é muito próximo de $\frac{\sqrt{5}}{\sqrt{5}+\varepsilon} < 1$, absurdo, pois $|p^2 - pq - q^2| \geq 1$, de fato se $p^2 - pq - q^2 = 0$ teríamos

$$\left(\frac{p}{q}\right)^2 - \left(\frac{p}{q}\right) - 1 = 0 \Longrightarrow \frac{p}{q} \in \left\{\frac{1+\sqrt{5}}{2}, \frac{1-\sqrt{5}}{2}\right\},$$

o que é absurdo, pois $\frac{p}{q} \in \mathbb{Q}$.

Outra maneira de ver que, para todo $\varepsilon > 0$, $\left|\frac{1+\sqrt{5}}{2} - \frac{p}{q}\right| < \frac{1}{(\sqrt{5}+\varepsilon)q^2}$ tem apenas um número finito de soluções $\frac{p}{q} \in \mathbb{Q}$ é observar que as melhores aproximações racionais de $\frac{1+\sqrt{5}}{2}$ são as reduzidas $\frac{p_n}{q_n}$ de sua fração contínua $[1; 1, 1, 1, \dots]$ (ver próxima seção), para as quais temos $\left|\frac{1+\sqrt{5}}{2} - \frac{p_n}{q_n}\right| = \frac{1}{(\alpha_{n+1}+\beta_{n+1})q_n^2}$, com $\alpha_{n+1} + \beta_{n+1}$ se aproximando cada vez mais de

$$[1; 1, 1, 1, \dots] + [0; 1, 1, 1, \dots] = \frac{1+\sqrt{5}}{2} + \frac{\sqrt{5}-1}{2} = \sqrt{5}.$$

## 1.3 Boas Aproximações são Reduzidas

O próximo teorema (e seu corolário 1.17) caracteriza as reduzidas em termos do erro reduzido da aproximação de $x$ por $p/q$, o qual é, por definição, $|qx - p|$, a razão entre $|x - p/q|$ e o erro máximo da aproximação por falta com denominador $q$, que é $1/q$.

**Teorema 1.15** *Para todo $p, q \in \mathbb{Z}$, com $0 < q < q_{n+1}$ temos*

$$|q_n x - p_n| \leq |qx - p|.$$

*Além disso, se $0 < q < q_n$ a desigualdade acima é estrita.*

**Demonstração:** Como $\text{mdc}(p_n, q_n) = 1$, temos que se $\frac{p}{q} = \frac{p_n}{q_n}$ então $p = kp_n$ e $q = kq_n$ para algum inteiro $k \neq 0$ e neste caso o resultado é claro. Assim, podemos supor que $\frac{p}{q} \neq \frac{p_n}{q_n}$ de modo que

$$\left| \frac{p}{q} - \frac{p_n}{q_n} \right| \geq \frac{1}{qq_n} > \frac{1}{q_n q_{n+1}}$$

já que $q < q_{n+1}$. Assim, $\frac{p}{q}$ está fora do intervalo de extremos $\frac{p_n}{q_n}$ e $\frac{p_{n+1}}{q_{n+1}}$ e portanto

$$\left| x - \frac{p}{q} \right| \geq \min \left\{ \left| \frac{p}{q} - \frac{p_n}{q_n} \right|, \left| \frac{p}{q} - \frac{p_{n+1}}{q_{n+1}} \right| \right\} \geq \frac{1}{qq_{n+1}}$$

o que implica

$$|qx - p| \geq \frac{1}{q_{n+1}} \geq |q_n x - p_n|.$$

Além disso, a igualdade só pode ocorrer se $x = \frac{p_{n+1}}{q_{n+1}}$, donde $a_{n+1} \geq 2$, e $q_{n+1} > 2q_n$, pois numa fração contínua finita, como no algoritmo de Euclides, o último coeficiente $a_n$ é sempre maior que 1. Nesse caso, se $q < q_n$, teremos

$$\begin{aligned}
\left| x - \frac{p}{q} \right| &\geq \left| \frac{p}{q} - \frac{p_n}{q_n} \right| - \left| \frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n} \right| \\
&\geq \frac{1}{qq_n} - \frac{1}{q_n q_{n+1}} = \frac{q_{n+1} - q}{qq_n q_{n+1}} > \frac{1}{qq_{n+1}}
\end{aligned}$$

o que implica

$$|qx - p| > \frac{1}{q_{n+1}} \geq |q_n x - p_n|.$$

□

**Corolário 1.16** *Para todo $q < q_n$,*

$$\left| x - \frac{p_n}{q_n} \right| < \left| x - \frac{p}{q} \right|$$

**Corolário 1.17** *Se $|qx - p| < |q'x - p'|$, para todo $p'$ e $q' \leq q$ tais que $\frac{p}{q} \neq \frac{p'}{q'}$, então $p/q$ é uma reduzida da fração contínua de $x$.*

**Demonstração:** Tome $n$ tal que $q_n \leq q < q_{n+1}$. Pelo teorema, $|q_n x - p_n| \leq |qx - p|$, e portanto $p/q = p_n/q_n$.

□

**Teorema 1.18** *Se $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$ então $\frac{p}{q}$ é uma reduzida da fração contínua de $x$.*

**Demonstração:** Seja $n$ tal que $q_n \leq q < q_{n+1}$. Suponha que $\frac{p}{q} \neq \frac{p_n}{q_n}$. Como na demonstração do teorema anterior, $\left|x - \frac{p}{q}\right| \geq \frac{1}{qq_{n+1}}$ e assim $\frac{p}{q}$ está fora do intervalo de extremos $\frac{p_n}{q_n}$ e $\frac{p_{n+1}}{q_{n+1}}$. Temos duas possibilidades:

a) Se $q \geq \frac{q_{n+1}}{2}$ então $\left|x - \frac{p}{q}\right| \geq \frac{1}{qq_{n+1}} \geq \frac{1}{2q^2}$, absurdo.

b) Se $q < \frac{q_{n+1}}{2}$,

$$\begin{aligned}\left|x - \frac{p}{q}\right| &\geq \left|\frac{p_n}{q_n} - \frac{p}{q}\right| - \left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| \\ &\geq \frac{1}{qq_n} - \frac{1}{q_nq_{n+1}} = \frac{q_{n+1} - q}{qq_nq_{n+1}} \\ &> \frac{1}{2qq_n} \geq \frac{1}{2q^2}\end{aligned}$$

o que também é um absurdo.

□

Dado $\alpha \in \mathbb{R}$, definimos a *ordem* de $\alpha$ por

$$\operatorname{ord} \alpha \stackrel{\text{def}}{=} \sup\left\{\nu > 0 \;\middle|\; \left|\alpha - \frac{p}{q}\right| < \frac{1}{q^\nu} \text{ tem infinitas soluções } \frac{p}{q} \in \mathbb{Q}\right\}$$

Observemos que a ordem de todo número irracional pode ser calculado a partir de sua fração contínua.

**Teorema 1.19** *Seja $\alpha$ um número irracional, e sejam $[a_0; a_1, a_2, a_3 \ldots]$ sua fração contínua e $\{\frac{p_n}{q_n}\}$ suas convergentes. Então*

$$\operatorname{ord} \alpha = 1 + \limsup_{n\to\infty} \frac{\ln q_{n+1}}{\ln q_n} = 2 + \limsup_{n\to\infty} \frac{\ln a_{n+1}}{\ln q_n}.$$

**Demonstração:** Sabemos que as melhores aproximações por racionais são obtidas a partir das convergentes da fração contínua, assim para calcular a ordem, basta calcular a ordem gerada pelas convergentes. Seja $s_n > 0$ um número real tal que $\left|\alpha - \frac{p_n}{q_n}\right| = \frac{1}{q_n^{s_n}}$. Como foi provado no Capítulo 3 $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_nq_{n+1}}$ e

$$\left|\alpha - \frac{p_n}{q_n}\right| > \frac{1}{2}\left(\left|\alpha - \frac{p_n}{q_n}\right| + \left|\alpha - \frac{p_{n+1}}{q_{n+1}}\right|\right) = \frac{1}{2}\left|\frac{p_{n+1}}{q_{n+1}} - \frac{p_n}{q_n}\right| = \frac{1}{2q_nq_{n+1}}.$$

Logo temos que

$$\frac{1}{2q_nq_{n+1}} \leq \frac{1}{q_n^{s_n}} \leq \frac{1}{q_nq_{n+1}},$$

e tomando o logaritmo obtemos

$$\ln 2 + \ln q_n + \ln q_{n+1} \geq s_n \ln q_n \geq \ln q_n + \ln q_{n+1}.$$

Portanto $\operatorname{ord} \alpha = \limsup_{n\to\infty} s_n = 1 + \limsup_{n\to\infty} \dfrac{\ln q_{n+1}}{\ln q_n}$. Para mostrar a segunda igualdade, observemos que $q_{n+1} = a_{n+1}q_n + q_{n-1}$, assim

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

agora tomando o logaritmo e dividindo por $\ln q_n$ obtemos

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

portanto $\limsup_{n\to\infty} \dfrac{\ln q_{n+1}}{\ln q_n} = 1 + \limsup_{n\to\infty} \dfrac{\ln a_{n+1}}{\ln q_n}$.

□

Observe que usando a fração contínua de $e$ (ver exercícios), é possível provar que $\operatorname{ord}(e) = 2$.

## 1.4 Frações Contínuas Periódicas

Nesta seção provaremos que os números reais com fração contínua periódica são exatamente as raízes de equações do segundo grau com coeficientes inteiros.

Lembramos que na representação de $x$ por fração contínua, $a_n$, $\alpha_n$ são definidos por recursão por

$$\alpha_0 = x, \quad a_n = \lfloor \alpha_n \rfloor, \quad \alpha_{n+1} = \frac{1}{\alpha_n - a_n}$$

e temos

$$\alpha_n = \frac{p_{n-2} - q_{n-2}x}{q_{n-1}x - p_{n-1}}, \quad \forall n \in \mathbb{N}.$$

Isso dá uma prova explícita do fato de que se a fração contínua de $x$ é periódica, então $x$ é raiz de uma equação do segundo grau com coeficientes inteiros. De fato, se $\alpha_{n+k} = \alpha_n$, $n \in \mathbb{N}$, $k \in \mathbb{N}_{>0}$ segue que

$$\frac{p_{n-2} - q_{n-2}x}{q_{n-1}x - p_{n-1}} = \frac{p_{n+k-2} - q_{n+k-2}x}{q_{n+k-1}x - p_{n+k-1}},$$

então $Ax^2 + Bx + C = 0$, onde

$$\begin{aligned}
A &= q_{n-1}q_{n+k-2} - q_{n-2}q_{n+k-1} \\
B &= p_{n+k-1}q_{n-2} + p_{n-2}q_{n+k-1} - p_{n+k-2}q_{n-1} - p_{n-1}q_{n+k-2} \\
C &= p_{n-1}p_{n+k-2} - p_{n-2}p_{n+k-1}
\end{aligned}$$

Note que o coeficiente de $x^2$ é não-nulo, pois $\frac{q_{n-1}}{q_{n-2}}$ é uma fração irredutível de denominador $q_{n-2}$, pois $p_{n-1}q_{n-2} - p_{n-2}q_{n-1} = (-1)^n$, e $\frac{q_{n+k-1}}{q_{n+k-2}}$ é uma fração irredutível de denominador $q_{n+k-2} > q_{n-2}$, donde $\frac{q_{n-1}}{q_{n-2}} \neq \frac{q_{n+k-1}}{q_{n+k-2}}$, logo $q_{n-1}q_{n+k-2} - q_{n-2}q_{n+k-1} \neq 0$.

Vamos provar agora um resultado devido a Lagrange segundo o qual se $x$ é uma *irracionalidade quadrática*, isto é, se $x$ é um irracional do tipo $r + \sqrt{s}$, $r, s \in \mathbb{Q}$, $s > 0$, então a fração contínua de $x$ é periódica, i.e., existem $n \in \mathbb{N}$ e $k \in \mathbb{N}_{>0}$ com $\alpha_{n+k} = \alpha_n$. Neste caso, existem $a$, $b$, $c$ inteiros tais que $ax^2 + bx + c = 0$, com $b^2 - 4ac > 0$ e $\sqrt{b^2 - 4ac}$ irracional. Como $x = \frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}$, temos

$$\begin{aligned} & ax^2 + bx + c = 0 \\ \Longrightarrow\ & a\left(\frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}\right)^2 + b\left(\frac{p_{n-1}\alpha_n + p_{n-2}}{q_{n-1}\alpha_n + q_{n-2}}\right) + c = 0 \\ \Longrightarrow\ & A_n\alpha_n^2 + B_n\alpha_n + C_n = 0, \end{aligned}$$

onde

$$\begin{aligned} A_n &= ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2 \\ B_n &= 2ap_{n-1}p_{n-2} + b(p_{n-1}q_{n-2} + p_{n-2}q_{n-1}) + 2cq_{n-1}q_{n-2} \\ C_n &= ap_{n-2}^2 + bp_{n-2}q_{n-2} + cq_{n-2}^2. \end{aligned}$$

Note que $C_n = A_{n-1}$. Vamos provar que existe $M > 0$ tal que $0 < |A_n| \leq M$ para todo $n \in \mathbb{N}$, e portanto $0 < |C_n| \leq M$, $\forall n \in \mathbb{N}$:

$$A_n = ap_{n-1}^2 + bp_{n-1}q_{n-1} + cq_{n-1}^2 = aq_{n-1}^2\left(x - \frac{p_{n-1}}{q_{n-1}}\right)\left(\bar{x} - \frac{p_{n-1}}{q_{n-1}}\right),$$

onde $x$ e $\bar{x}$ são as raízes de $aX^2 + bX + c = 0$, mas

$$\begin{aligned} \left|x - \frac{p_{n-1}}{q_{n-1}}\right| < \frac{1}{q_{n-1}^2} \leq 1 \implies |A_n| &= aq_{n-1}^2\left|x - \frac{p_{n-1}}{q_{n-1}}\right|\left|\bar{x} - \frac{p_{n-1}}{q_{n-1}}\right| \\ &\leq a\left(|\bar{x} - x| + \left|x - \frac{p_{n-1}}{q_{n-1}}\right|\right) \\ &\leq M \stackrel{\text{def}}{=} a(|\bar{x} - x| + 1). \end{aligned}$$

Notemos agora que, para qualquer $n \in \mathbb{N}$,

$$B_n^2 - 4A_nC_n = (p_{n-1}q_{n-2} - p_{n-2}q_{n-1})^2(b^2 - 4ac) = b^2 - 4ac$$

Portanto

$$\begin{aligned} & B_n^2 \leq 4A_nC_n + b^2 - 4ac \leq 4M^2 + b^2 - 4ac \\ \Longrightarrow\ & B_n \leq M' \stackrel{\text{def}}{=} \sqrt{4M^2 + b^2 - 4ac} \end{aligned}$$

Provamos assim que $A_n$, $B_n$ e $C_n$ estão uniformemente limitados, donde há apenas um número finito de possíveis equações $A_nX^2 + B_nX + C_n = 0$, e portanto de possíveis valores de $\alpha_n$. Assim, necessariamente $\alpha_{n+k} = \alpha_n$ para alguma escolha de $n \in \mathbb{N}$, $k \in \mathbb{N}_{>0}$.

**Aplicação:** A equação de Pell.

Seja $A$ um inteiro positivo. Estamos interessados na equação $x^2 - Ay^2 = 1$, com $x$ e $y$ inteiros. Se $A$ é um quadrado perfeito, digamos $a = k^2$, temos que $x^2 - Ay^2 = (x - ky)(x + ky) = 0$ admite apenas as soluções triviais $y = 0$, $x = \pm 1$, pois teríamos $x - ky = x + ky = \pm 1$. o caso itneressante é quando $A$ não é um quadrado pergeito, e portanto $\sqrt{A}$ é um irracional (de fato, se $\sqrt{A} = \frac{p}{q}$, com $\mathrm{mdc}(p, q) = 1$ e $q > 1$, teríamos $A = \frac{p^2}{q^2}$ o que é um absurdo, pois $\mathrm{mdc}(p, q) = 1 \Rightarrow \mathrm{mdc}(p^2, q^2) = 1$, donde $p^2/q^2$ não pode ser inteiro). nesse caso, a equação $x^2 - Ay^2 = 1$ é conhecida como uma *equação de Pell*. Nosso resultado principal é o seguinte:

**Teorema 1.20** *A equação $x^2 - Ay^2 = 1$ tem infinitas soluções inteiras $(x, y)$. Além disso, as soluções com $x$ e $y$ inteiros positivos podem ser enumeradas por $(x_n, y_n)$, $n \geq 0$ de modo que, para todo $n$, $x_n + y_n\sqrt{A} = (x_1 + y_1\sqrt{A})^n$, e portanto*

$$x_n = \frac{(x_1 + y_1\sqrt{A})^n + (x_1 - y_1\sqrt{A})^n}{2} \quad e \quad y_n = \frac{(x_1 + y_1\sqrt{A})^n + (x_1 - y_1\sqrt{A})^n}{2\sqrt{A}}.$$

**Observação 1.21** As seqüências $(x_n)$ e $(y_n)$ acma satisfazem a recorrência $u_{n+2} = 2x_0u_{n+1} - u_n$, $\forall\ n \geq 1$.

**Demonstração:** Observemos inicialmente que, se $D = \{x + y\sqrt{A} \mid x, y \in \mathbb{Z}\}$ então $N\colon D \to D$, $N(x + y\sqrt{A}) = x^2 - Ay^2$ é uma função multiplicativa, isto é,

$$N((x + y\sqrt{A})(u + v\sqrt{A})) = N(x + y\sqrt{A})N(u + v\sqrt{A}),\ \forall\, x, y, u, v \in \mathbb{Z}.$$

De fato,

$$\begin{aligned} N((x + y\sqrt{A})(u + v\sqrt{A})) &= N((xu + ayv) + (xv + yu)\sqrt{A}) \\ &= (xu + Ayv)^2 - A(xv + yu)^2 \\ &= x^2u^2 + A^2y^2v^2 - A(x^2v^2 + y^2u^2) \\ &= (x^2 - Ay^2)(u^2 - Av^2). \end{aligned}$$

Usaremos agora o fato de que, como $\sqrt{A}$ é irracional, a desigualdade $|\sqrt{A} - \frac{p}{q}| < \frac{1}{q^2}$ tem infinitas soluções racionais $p/q$. Note que se $|\sqrt{A} - \frac{p}{q}| < \frac{1}{q^2}$ então

$$\begin{aligned} |p^2 - Aq^2| &= |p - q\sqrt{A}||p + q\sqrt{A}| = q|\sqrt{A} - \frac{p}{q}||p + q\sqrt{A}| < q \cdot \frac{1}{q^2} \cdot |p + q\sqrt{A}| \\ &= |\frac{p}{q} + \sqrt{A}| \leq 2\sqrt{A} + |\sqrt{A} - \frac{p}{q}| < 2\sqrt{A} + 1. \end{aligned}$$

Considerando infinitos pares de inteiros positivos $(p_n, q_n)$ com $|\sqrt{A} - \frac{p_n}{q_n}| < \frac{1}{q_n^2}$, teremos sempre $|p_n - Aq_n^2| < 2\sqrt{A} + 1$, e portanto temos um número finito de possibilidades para o valor (inteiro) de $p_n - Aq_n^2$. consequentemente, existe um inteiro $k \neq 0$ tal que $p_n - Aq_n^2 = k$ para infinitos valores de $n$. Obtemos portanto duas seqüências crescentes de pares de inteiros positivos $u_r), (v_r)$, $r \in \mathbb{N}$ tais que $u_r^2 - kv_r^2 = k$ para todo $r$.

Como há apenas $|k|^2$ possibilidades para os pares $(\overline{u}_r(\text{mod } |k|), \overline{v}_r(\text{mod } |k|))$, axistem inteiros $a$ e $b$ e infinitos valores de $r$ tais que $u_r \equiv a(\text{mod } |k|)$ e $v_r \equiv b(\text{mod } |k|)$. Tomamos então $r < s$ com as propriedades acima. Seja

$$x + y\sqrt{A} = \frac{u_s + v_s\sqrt{A}}{u_r + v_r\sqrt{A}} = \frac{(u_s + v_s\sqrt{A})(u_r - v_r\sqrt{A})}{u_r^2 - Av_r^2}$$
$$= \frac{u_s u_r - Av_s v_r}{k} + \left(\frac{u_r v_s - u_s v_r}{k}\right)\sqrt{A}.$$

Temos $u_s u_r - Av_s V_r \equiv u_r^2 - Av_r^2 = k \equiv 0(\text{mod } |k|)$ e $u_r v_s - u_s v_r \equiv ab - ab = 0(\text{mod } |k|)$, e portanto $x = \frac{u_s u_r - Av_s v_r}{k}$ e $y = \frac{u_r v_s - u_s v_r}{k}$ são inteiros. Por outro lado, $(x + y\sqrt{A})(u_r + v_r\sqrt{A}) = u_s + v_s\sqrt{A}$, donde $N(x + y\sqrt{A})N(u_r + v_r\sqrt{A}) = N(u_s + v_s\sqrt{A})$. Como $N(u_r + v_r\sqrt{A}) = N(u_s + v_s\sqrt{A}) = k$, segue que $N(x + y\sqrt{A}) = x^2 - Ay^2 = 1$. Além disso, como $s > r$, $u_s + v_s\sqrt{A} > u_r + v_r\sqrt{A}$, donde $x + y\sqrt{A} = \frac{u_s + v_s\sqrt{A}}{u_r + v_r\sqrt{A}} > 1$.

Sejam agora $x_1, y_1 \in \mathbb{Z}$ tais que $x_1 + y_1\sqrt{A} > 1$ e $x_1^2 - Ay_1^2 = 1$ com $x_1 + y_1\sqrt{A}$ mínimo. Temos então $(x_1 + y_1\sqrt{A})^{-1} = x_1 - y_1\sqrt{A}$. Vamos mostrar que, se $\tilde{x} + \tilde{y}\sqrt{A} > 1$ e $\tilde{x}^2 - A\tilde{y}^2 = 1$ (com $\tilde{x}$ e $\tilde{y}$ inteiros) então $\tilde{x} + \tilde{y}\sqrt{A} = (x_1 + y_1\sqrt{A})^n$ para algum inteiro positivo $n$. Para isso, tome $n \geq 1$ tal que $(x_1 + y_1\sqrt{A})^n \leq \tilde{x} + \tilde{y}\sqrt{A} < (x_1 + y_1\sqrt{A})^{n+1}$. Temos então $1 \leq (\tilde{x} + \tilde{y}\sqrt{A})(x_1 - y_1\sqrt{A})^n < x_1 + y_1\sqrt{A}$. Se $u + v\sqrt{A} = (\tilde{x} + \tilde{y}\sqrt{A})(x_1 - y_1\sqrt{A})^n$, com $u$ e $v$ inteiros, temos

$$u^2 - Av^2 = N(u + v\sqrt{A}) = N(\tilde{x} + \tilde{y}\sqrt{A})N(x_1 - y_1\sqrt{A})^n = 1,$$

donde $u + v\sqrt{A} = 1$, pela minimalidade de $x_1 + y_1\sqrt{A}$, pois $1 \leq u + v\sqrt{A} < x_1 + y_1\sqrt{A}$. Note finalmente que se $x$ e $y$ são inteiros e $x^2 - Ay^2 = 1$ então $x + y\sqrt{A} > 1$ equivale a termos $x$ e $y$ positivos, pois temos $0 < (x + y\sqrt{A})^{-1} = x - y\sqrt{A} < 1$, donde $x = \frac{(x+y\sqrt{A}) + (x-y\sqrt{A})}{2}$ e $y = \frac{(x+y\sqrt{A}) - (x-y\sqrt{A})}{2\sqrt{A}}$ são positivos. □

## 1.5 Problemas Propostos

**1** Seja

$$\frac{p_n}{q_n} = \cfrac{1}{1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{\ddots\, 2 + \cfrac{(2n-3)^2}{2}}}}}$$

a $n$-ésima convergente da fração contínua

$$\cfrac{1}{1+\cfrac{1^2}{2+\cfrac{3^2}{2+\cfrac{5^2}{2+\cfrac{7^2}{\ddots}}}}}$$

Demonstrar que $\frac{p_n}{q_n} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \cdots + (-1)^{n-1}\frac{1}{2n-1}$.

**2** Demonstrar que, para todo inteiro positivo $a$, temos as seguintes expansões em frações contínuas periódicas:

a) $\sqrt{a^2+1} = [a, \overline{2a}]$.

b) $\sqrt{a^2-1} = [a-1, \overline{1, 2a-2}]$.

c) $\sqrt{a^2-2} = [a-1, \overline{1, a-2, 1, 2a-2}]$.

d) $\sqrt{a^2-a} = [a-1, \overline{2, 2a-2}]$.

**3** Encontrar as frações contínuas de $\sqrt{a^2+4}$ e $\sqrt{a^2-4}$.

**4** Seja $\alpha = [a_0; a_1, a_2, \dots] \in \mathbb{R}$. Prove que, se $q_n \le q < q_{n+1}, \mathrm{mdc}(p,q) = 1$ e $p/q \ne p_n/q_n$ então $|\alpha - p/q| \le |\alpha - p_n/q_n|$ se, e somente se, $\frac{p}{q} = \frac{p_{n+1}-rp_n}{q_{n+1}-rq_n}$, onde $r \in \mathbb{N}$ é tal que $0 < r < a_{n+1}/2$ ou ($r = a_{n+1}/2$ e $\alpha_{n+2}\beta_{n+1} \ge 1$).

**5** Seja $\alpha = [a_0; a_1, a_2, \dots] \in \mathbb{R}$. Prove que, se $q_n \le q < q_{n+1}, \mathrm{mdc}(p,q) = 1$ e $p/q \ne p_n/q_n$ então $|\alpha - p/q| < 1/q^2$ se, e somente se, $a_{n+1} \ge 2$ e $\frac{p}{q} = \frac{p_{n+1}-p_n}{q_{n+1}-q_n}$ ou ($\frac{p}{q} = \frac{p_n+p_{n-1}}{q_n+q_{n-1}}$ e $(\alpha_{n+1}-2)\beta_{n+1} < 1$).

**6** Seja $\alpha = [a_0; a_1, a_2, \dots]$ um número real.

a) Prove que, se $\operatorname{ord}\alpha > 2$ então existe $\lambda > 1$ tal que, para infinitos inteiros positivos $n$, temos $a_n \ge \lambda^n$.

b) Prove que $\operatorname{ord}\alpha \ge 1 + \exp(\limsup_{n\to\infty} \frac{\log\log(a_n+1)}{n})$.

c) Mostre que, para todo $c \ge 2$, existe $\alpha \in \mathbb{R}$ tal que $\operatorname{ord}\alpha = 1 + \exp(\limsup_{n\to\infty} \frac{\log\log(a_n+1)}{n}) = c$.

d) Determine $\operatorname{ord}\alpha$ se $a_n = 2^n, \forall n \ge 0$.

**7** Prove que, para todo $\alpha \in \mathbb{R}$, $\limsup_{n\to+\infty} \cos^n(n\alpha) = 1$.

**8** Este exercício, baseado em [Cohn], tem como objetivo calcular a fração contínua de $e$.

a) São dadas as sequências $\{A_n\}$, $\{B_n\}$ e $\{C_n\}$ definidas por

$$\begin{aligned} A_n &= \int_0^1 \frac{x^n(x-1)^n}{n!} e^x\,dx, \\ B_n &= \int_0^1 \frac{x^{n+1}(x-1)^n}{n!} e^x\,dx, \\ C_n &= \int_0^1 \frac{x^n(x-1)^{n+1}}{n!} e^x\,dx. \end{aligned}$$

Mostrar que para todo $n \geq 1$ se cumprem as relações

(i) $A_n + B_{n-1} + C_{n-1} = 0$,

(ii) $B_n - 2nA_n + C_{n-1} = 0$,

(iii) $A_n - B_n + C_n = 0$.

b) Dadas as sequências $\{p_n\}$ e $\{q_n\}$ definidas recursivamente como $p_0 = q_0 = p_1 = 1$, $q_1 = 0$ e

$$\begin{aligned} p_{3n} &= p_{3n-1} + p_{3n-2}, & q_{3n} &= q_{3n-1} + q_{3n-2} \\ p_{3n+1} &= 2np_{3n} + p_{3n-1}, & q_{3n+1} &= 2nq_{3n} + q_{3n-1} \\ p_{3n+2} &= p_{3n+1} + p_{3n}, & q_{3n+2} &= q_{3n+1} + q_{3n} \end{aligned}$$

Mostrar por indução que para todo $n \geq 0$ se cumprem as relações

$$A_n = q_{3n}e - p_{3n}, \quad B_n = p_{3n+1} - q_{3n+1}e, \quad \text{e} \quad C_n = p_{3n+2} - q_{3n+2}e.$$

c) Mostrar que

$$e = \lim_{n\to\infty} \frac{p_n}{q_n} = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots, 1, 1, 2n, \ldots].$$

**9** Prove que

$$|e - \frac{p}{q}| < \frac{\log\log q}{2q^2 \log q} \text{ tem infinitas soluções } \frac{p}{q} \in \mathbb{Q}, \text{ mas, para todo } \varepsilon > 0,$$

$$|e - \frac{p}{q}| < \frac{\log\log q}{(2+\varepsilon)q^2 \log q} \text{ tem apenas um número finito de soluções } \frac{p}{q} \in \mathbb{Q}.$$

# Capítulo 2

# Propriedades Estatísticas de Frações Contínuas e Aproximações Diofantinas: O Teorema de Khintchine

## 2.1 Introdução

O problema básico da teoria de aproximações diofantinas é o de estudar boas aproximações de números reais por números racionais. Uma extensão natural desse problema é o estudo de aproximações simultâneas de $n$ números reais por números racionais com o mesmo denominador.

Dado um número irracional $\alpha$, um resultado clássico de Dirichlet (que já provamos usando frações contínuas) afirma que existem infinitos racionais $\frac{p}{q}$ tais que $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$ (vejamos outra prova simples: dado $N \in \mathbb{N}$, consideramos os $N+1$ elementos de $[0,1)$ da forma $j\alpha - \lfloor j\alpha \rfloor$, com $0 \leq j \leq N$. Como $[0,1) = \bigcup_{k=0}^{N-1} \left[\frac{k}{N}, \frac{k+1}{N}\right)$, existem dois desses elementos, digamos $j_1\alpha - \lfloor j_1\alpha \rfloor$ e $j_2\alpha - \lfloor j_2\alpha \rfloor$ num mesmo intervalo $\left[\frac{k}{N}, \frac{k+1}{N}\right)$, e portanto, se $j_1 < j_2$, $q = j_2 - j_1$ e $p = \lfloor j_2\alpha \rfloor - \lfloor j_1\alpha \rfloor$, temos $0 < |q\alpha - p| < \frac{1}{N} \Rightarrow |\alpha - \frac{p}{q}| < \frac{1}{qN} \leq \frac{1}{q^2}$). Hurwitz e Markov provaram que de fato $|\alpha - \frac{p}{q}| < \frac{1}{\sqrt{5}q^2}$ tem infinitas soluções $\frac{p}{q} \in \mathbb{Q}$, para todo irracional $\alpha$, e que $\sqrt{5}$ é a maior constante com essa propriedade. Markov ([Mar1] e [Mar2]) provou que, para todo $c < 3$, o conjunto dos $\alpha \in \mathbb{R}$ tais que $|\alpha - \frac{p}{q}| < \frac{1}{cq^2}$ tem apenas um número finito de soluções $\frac{p}{q} \in \mathbb{Q}$ é enumerável, mas o conjunto dos $\alpha \in \mathbb{R}$ tais que $|\alpha - \frac{p}{q}| < \frac{1}{3q^2}$ tem apenas um número finito de soluções tem o mesmo cardinal que $\mathbb{R}$.

Neste capítulo, vamos estudar desigualdades do tipo

$$|\alpha - \frac{p}{q}| < \frac{f(q)}{q}, \tag{1}$$

onde $f\colon \mathbb{N} \to \mathbb{R}^+$ é uma função decrescente, do ponto de vista da teoria da medida. Vamos provar o teorema de Khintchine, segundo o qual, se $\sum_{q=1}^{\infty} f(q) = +\infty$ então (1) tem infinitas soluções $\frac{p}{q} \in \mathbb{Q}$, para quase todo $\alpha \in \mathbb{R}$, mas se $\sum_{q=1}^{\infty} f(q) < +\infty$ então (1) tem apenas um número finito de soluções $\frac{p}{q} \in \mathbb{Q}$, para quase todo $\alpha \in \mathbb{R}$.

Note que do ponto de vista topológico a situação é diferente: qualquer que seja a função positiva $f$, (1) tem infinitas soluções $\frac{p}{q} \in \mathbb{Q}$ para $\alpha \in R_f$, onde $R_f$ é um conjunto residual, i.e. contém (de fato é) uma interseção enumerável de abertos densos.

A principal técnica usada para estudar aproximações de números reais por números racionais são as frações contínuas, que fornecem todas as boas aproximações de um irracional $\alpha$ por racionais. Lembramos os seguintes resultados a seguir sobre frações contínuas.

Dado $\alpha \in \mathbb{R}$, definimos $\alpha_0 = \alpha$, $a_n = \lfloor \alpha_n \rfloor$ e, se $\alpha_n \notin \mathbb{Z}$, $\alpha_{n+1} = \frac{1}{\alpha_n - a_n}$, para todo $n \in \mathbb{N}$. Para cada $n \in \mathbb{N}$ tomamos $p_n \in \mathbb{Z}$ e $q_n \in \mathbb{N}^*$ primos entre si tais que

$$\frac{p_n}{q_n} = [a_0; a_1, a_2, \dots, a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots + \cfrac{1}{a_n}}}.$$

Temos

$$\frac{1}{(a_{n+1}+2)q_n^2} < |\alpha - \frac{p_n}{q_n}| < \frac{1}{a_{n+1}q_n^2} \le \frac{1}{q_n^2}, \quad \text{para todo } n \in \mathbb{N}.$$

As seqüências $p_n$ e $q_n$ satisfazem $p_{n+1}q_n - p_nq_{n+1} = (-1)^n$, $\forall\, n \ge 0$. Se $|\alpha - \frac{p}{q}| < \frac{1}{2q^2}$ então $\frac{p}{q} = \frac{p_n}{q_n}$, para algum $n \in \mathbb{N}$. Por outro lado, para todo $n \in \mathbb{N}$ vale $|\alpha - \frac{p_n}{q_n}| < \frac{1}{2q_n^2}$ ou $|\alpha - \frac{p_{n+1}}{q_{n+1}}| < \frac{1}{2q_{n+1}^2}$.

Temos

$$p_{n+2} = a_{n+2}p_{n+1} + p_n,\; q_{n+2} = a_{n+2}q_{n+1} + q_n \text{ e } \alpha = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}, \text{ para todo } n \in \mathbb{N}.$$

A prova que apresentaremos na Seção 1, baseada no estudo de propriedades estatísticas de frações contínuas, é inspirada em conversas que tive há uns 9 anos com o Prof. Nicolau Corção Saldanha sobre o tema.

O problema básico de aproximações simultâneas é o seguinte: dado $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{R}$ queremos encontrar números racionais $\frac{p_1}{q}, \frac{p_2}{q}, \dots, \frac{p_n}{q}$ tais que $|\alpha_j - \frac{p_j}{q}|$ seja pequeno para todo $j \le n$. Em geral sempre é possível encontrar racionais tais que $|\alpha_j - \frac{p_j}{q}| < \frac{1}{q^{1+1/n}}$, o que estende o teorema de Dirichlet e pode ser provado de modo análogo: dado $N \in \mathbb{N}$ consideramos os $N^n + 1$ pontos

$$p_j = (\alpha_1 j - \lfloor \alpha_1 j \rfloor, \alpha_2 j - \lfloor \alpha_2 j \rfloor, \dots, \alpha_n j - \lfloor \alpha_n j \rfloor), \quad 0 \le j \le N^n$$

no hipercubo $[0,1)^n$. Dividimos $[0,1)^n$ como $\left(\bigcup_{k=0}^{N-1} \left[\frac{k}{N}, \frac{k+1}{N}\right)\right)^n$ em $N^n$ cubos de lado $\frac{1}{N}$. Haverá necessariamente dois pontos $p_{j_1}$ e $p_{j_2}$ num mesmo cubo dessa decomposição, e, se $j_1 < j_2$, $q = j_2 - j_1$, $p_j = \lfloor j_2\alpha_j \rfloor - \lfloor j_1\alpha_j \rfloor$, teremos $|\alpha_j - \frac{p_j}{q_j}| < \frac{1}{Nq_j} \le \frac{1}{q_j^{1+1/n}}$, para todo $j \le n$.

Infelizmente não há um substituto satisfatório para a teoria de frações contínuas em dimensão maior que um, mas é possível provar uma versão $n$-dimensional do Teorema de Khinchine (provada originalmente em [K]), o que faremos na Seção 2.

Para maiores informações sobre aproximações diofantinas, veja [Ca1] e [S].

## 2.2 O Teorema de Khintchine via frações contínuas

**Teorema 2.1 (Khintchine)** *Seja $f\colon \mathbb{N} \to \mathbb{R}^+$ uma função decrescente tal que $h(n) = nf(n)\colon \mathbb{N} \to \mathbb{R}^+$ também seja decrescente.*

*a) Se $\sum_{n=1}^{\infty} f(n) < +\infty$ então a equação $|\alpha - \frac{p}{q}| < \frac{f(q)}{q}$ tem apenas um número finito de soluções racionais $p/q$, para quase todo $\alpha \in \mathbb{R}/\mathbb{Q}$*

*b) Se $\sum_{n=1}^{\infty} f(n) = +\infty$ então a equação $|\alpha - \frac{p}{q}| < \frac{f(q)}{q}$ tem um número infinito de soluções racionais $p/q$, para quase todo $\alpha \in \mathbb{R}/\mathbb{Q}$.*

**Observação 2.2** A condição de $nf(n)$ ser decrescente não é de fato necessária, como veremos na seção 2, mas simplifica a prova. Por outro lado, não podemos retirar a hipótese de $f$ ser decrescente (veja [Ca2]).

**Lema 2.3** *Sejam $n, k \in \mathbb{N}$, e seja $[0, a_1, a_2, \dots]$ a fração contínua de um número $\alpha \in [0, 1]$. A probabilidade de um termo $a_{n+1}$ ser igual a k dado que $a_1 = k_1$, $a_2 = k_2, \dots, a_n = k_n$ está entre $1/(k+1)(k+2)$ e $2/k(k+1)$, $\forall\ k_1, k_2, \dots, k_n \in \mathbb{N}^*$.*

**Demonstração:** Sejam

$$p_{n-1}/q_{n-1} = [0; a_1, a_2, \dots, a_{n-1}] \quad \text{e} \quad p_n/q_n = [0; a_1, a_2, \dots, a_{n-1}, a_n].$$

Se $\alpha \in [0, 1]$, $\alpha = [0; a_1, a_2, \dots, a_n, \alpha_{n+1}]$, $\alpha_{n+1} \in [1, +\infty)$ então $\alpha \in \left[\frac{p_n+p_{n-1}}{q_n+q_{n-1}}, \frac{p_n}{q_n}\right)$, e, se além disso $a_{n+1} = k$, temos $\alpha \in \left[\frac{kp_n+p_{n-1}}{kq_n+q_{n-1}}, \frac{(k+1)p_n+p_{n-1}}{(k+1)q_n+q_{n-1}}\right]$, e valem as recíprocas (as ordens dos extremos dos intervalos podem estar trocadas). Os comprimentos dos referidos intervalos são, respectivamente, $\frac{1}{q_n(q_n+q_{n-1})}$ e $\frac{1}{(kq_n+q_{n-1})((k+1)q_n+q_{n-1})}$ (pois $|p_n q_{n-1} - p_{n-1} q_n| = 1$), e portanto a razão entre seus comprimentos é $\frac{q_n(q_n+q_{n-1})}{(kq_n+q_{n-1})((k+1)q_n+q_{n-1})} = \frac{1+\beta}{(k+\beta)(k+1+\beta)}$, onde $\beta = q_{n-1}/q_n \in [0, 1]$. Portanto, a razão pertence a $[1/(k+1)(k+2), 2/k(k+1)]$.

□

**Corolário 2.4** *A probabilidade de $a_{n+1} \geq k$, nos termos do Lema acima, pertence a $[1/(k+1), 2/k]$.*

**Lema 2.5** *Para quase todo $\alpha \in \mathbb{R}$ existe $c \in \mathbb{R}$ tal que $q_n \leq c^n$, para todo $n \in \mathbb{N}$.*

Antes de provar o Lema 2.4 vamos mostrar como termina a prova do Teorema de Khintchine.

**Demonstração do Teorema de Kintchine:** Suponhamos que $\Sigma f(n) < \infty$. Seja $\gamma = \frac{1+\sqrt{5}}{2}$. Se a aproximação $p_n/q_n$ de $\alpha$ é tal que $|\alpha - \frac{p_n}{q_n}| < \frac{f(q_n)}{q_n}$ então $a_{n+1} + 2 > \frac{1}{q_n f(q_n)} > \frac{1}{\gamma^{n-1} f(\gamma^{n-1})}$ (pois para todo $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ vale $q_n > \gamma^{n-1}$, $\forall\, n \in \mathbb{N}$). $\Rightarrow a_{n+1} > \frac{1}{\gamma^{n-1} f(\gamma^{n+1})} - 2$. A probabilidade de $a_{n+1} \leq \frac{1}{\gamma^{n-1} f(\gamma^{n-1})} - 2 =: A(n)$ é pelo menos $1 - \frac{2}{A(n)}$, $\forall\, n \in \mathbb{N}$ (pelo corolário do Lema 1.2), e a hipótese de $\sum_{n=1}^{\infty} f(n) < \infty$ implica que $\sum_{n=1}^{\infty} \frac{2}{A(n)} < \infty$, por comparação com

$$\sum_{k=1}^{\infty} \gamma^k f(\gamma^k) < \frac{\gamma}{\gamma - 1} \sum_{k=0}^{\infty} (\gamma^{k+1} - \gamma^k) f(\gamma^{k+1}) < \sum_{n=1}^{\infty} f(n) < +\infty.$$

Temos portanto $\prod_{n=1}^{\infty}(1 - \frac{2}{A(n)}) > 0 \Rightarrow$ para cada $\varepsilon > 0$ existe $n_0 \in \mathbb{N}$ tal que $\prod_{n=n_0}^{\infty}(1 - \frac{2}{A_n}) > 1 - \varepsilon$, donde com probabilidade total $a_{n+1} \leq A(n)$ para todo $n$ suficientemente grande $\Rightarrow |\alpha - \frac{p}{q}| < \frac{f(q)}{q}$ tem apenas um número finito de soluções.

Suponhamos agora que $\Sigma f(n) = +\infty$, fixemos $c > 0$ e vamos nos restringir ao conjunto $X_c$ dos $\alpha \in [0,1]$ tais que $q_n < c^n$ para todo $n \in \mathbb{N}$ (a união dos conjuntos $X_c$ para todo $c \in \mathbb{N}$ tem probabilidade total em $[0,1]$, pelo Lema 1.4).

Se $a_{n+1} > \frac{1}{q_n f(q_n)}$ teremos $|\alpha - \frac{p_n}{q_n}| < \frac{f(q_n)}{q_n}$. Como $q_n < c^n$, $\frac{1}{q_n f(q_n)} < \frac{1}{c^n f(c^n)}$. Vamos mostrar que com probabilidade total temos $a_{n+1} \geq \frac{1}{c^n f(c^n)}$ para infinitos valores de $n \in \mathbb{N}$. Isso segue de $\prod_{n=1}^{\infty}\left(1 - \frac{1}{B(n)+1}\right) = 0$, onde $B(n) = \frac{1}{c^n f(c^n)}$, que por sua vez segue de $\sum_{n=1}^{\infty} c^n f(c^n) \geq c^{-1} \sum_{n=1}^{\infty}(c^{n+1} - c^n) f(c^n) = +\infty$. Portanto, para todo $n_0 \in \mathbb{N}$ temos $\prod_{n=n_0}^{\infty}\left(1 - \frac{1}{B(n)+1}\right) = 0$, e, com probabilidade total, existe $n \geq n_0$ com $a_{n+1} \geq \frac{1}{c^n f(c^n)}$, donde a equação $|\alpha - \frac{p_n}{q_n}| < \frac{f(q_n)}{q_n}$ é satisfeita com probabilidade total para infinitos valores de $n \in \mathbb{N}$.

□

**Prova do Lema 2.4:** Sejam $n, k \in \mathbb{N}$. A probabilidade de que $k$ apareça pelo menos $4n/k(k+1)$ vezes entre $a_1, a_2, \ldots, a_n$ é limitada por $\sum_{j=sn}^{n} C_n^j (\frac{s}{2})^j (1 - \frac{s}{2})^{n-j}$, onde $s = \frac{4}{k(k+1)}$, que é menor que $(\frac{3}{4})^{\frac{n}{k(k+1)}}$ para $\frac{n}{k(k+1)}$ grande (de fato, $\frac{C_n^{j+1}(\frac{s}{2})^{j+1}(1-\frac{s}{2})^{n-j-1}}{C_n^j(\frac{s}{2})^j(1-\frac{s}{2})^{n-j}} = \frac{n-j}{j+1} \cdot \frac{s}{2-s} < \frac{4-3s}{3s} \cdot \frac{s}{2-s} = \frac{4-3s}{6-3s} < \frac{2}{3}$, se $j \geq \frac{3sn}{4}$, logo, como $\sum_{j=0}^{n} C_n^j (\frac{s}{2})^j (1 - \frac{s}{2})^{n-j} = 1$, para $j = \frac{3sn}{4}$, $C_n^j (\frac{s}{2})^j (1 - \frac{s}{2})^{n-j} \leq 1$, donde $C_n^{sn} (\frac{s}{2})^{sn} (1 - \frac{s}{2})^{(1-s)n} \leq (\frac{2}{3})^{sn/4}$ e $\sum_{j=sn}^{n} C_n^j (\frac{s}{2})^j (1 - \frac{s}{2})^{n-j} \leq (\frac{2}{3})^{sn/4} \sum_{k=0}^{\infty} (\frac{2}{3})^k = 3(\frac{2}{3})^{sn/4} = 3(\frac{2}{3})^{n/k(k+1)} < (\frac{3}{4})^{n/k(k+1)}$, se $n/k(k+1)$ é suficientemente grande). A probabilidade disso acontecer pra algum $k < [\sqrt[3]{n}]$ é no máximo $\sqrt[3]{n} \cdot (\frac{3}{4})^{\sqrt[3]{n}}$, que converge a zero quando $n \to +\infty$. Por outro lado, com probabilidade total, $a_n < n^2$ para todo $n$ suficientemente grande $\Rightarrow q_n < \prod_{k=1}^{n}(a_k + 1) < \left(\prod_{r=1}^{\sqrt[3]{n}} (r+1)^{\frac{4n}{r(r+1)}}\right) \cdot (n^2)^{4n/\sqrt[3]{n}}$ com probabilidade total para todo $n$ grande, pois também com probabilidade total o número de termos maiores ou iguais a $\sqrt[3]{n}$ entre $a_1, a_2, \ldots, a_n$ é no máximo $4n/\sqrt[3]{n}$, para $n$ suficientemente grande.

Como $\lim_{n\to\infty} 8\log n/\sqrt[3]{n} = 0$, temos com probabilidade total

$$\limsup_{n\to\infty} \sqrt[n]{q_n} \leq \exp\left(\sum_{r=1}^{\infty} \frac{4\log(r+1)}{r(r+1)}\right) < +\infty.$$

□

**Observação 2.6** Pode-se provar com métodos de teoria ergódica que para quase todo $\alpha \in \mathbb{R}$ vale

$$\lim_{n\to\infty} \sqrt[n]{q_n} = e^{\pi^2/12\ln 2} \simeq 3,2758229\ldots$$

Pretendemos discutir este e outros resultados finos ligados a propriedade estatísticas de frações contínuas num próximo artigo.

**Corolários do Teorema de Khintchine:**

i) *Para quase todo $\alpha \in \mathbb{R}$, $|\alpha - \frac{p}{q}| < \frac{1}{q^2\log^2 q}$ tem apenas um número finito de soluções $\frac{p}{q} \in \mathbb{Q}$, e portanto $|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\varepsilon}}$ tem apenas um número finito de soluções racionais $\frac{p}{q}$, para todo $\varepsilon > 0$. Em particular ord $\alpha = 2$ para quase todo $\alpha \in \mathbb{R}$ (onde ord $\alpha := \inf\{\nu > 0 \,|\, |\alpha - \frac{p}{q}| < \frac{1}{q^\nu}$ tem infinitas soluções $\frac{p}{q} \in \mathbb{Q}\}$).*

ii) *Para quase todo $\alpha \in \mathbb{R}$, $|\alpha - \frac{p}{q}| < \frac{1}{q^2\log q}$ tem infinitas soluções racionais $p/q$, e portanto, para todo $k \in \mathbb{R}$, $|\alpha - \frac{p}{q}| < \frac{1}{kq^2}$ tem infinitas soluções $\frac{p}{q} \in \mathbb{Q}$.*

## 2.3 O Teorema de Khintchine $n$-dimensional

**Teorema 2.7** *Sejam $f_1, f_2, \ldots, f_n \colon \mathbb{N} \to \mathbb{R}^+$ funções decrescentes e $F \colon \mathbb{N} \to \mathbb{R}^+$ dada por $F(k) = f_1(k)f_2(k)\ldots f_n(k)$. Seja $\alpha = (\alpha_1, \ldots, \alpha_2, \ldots, \alpha_n) \in \mathbb{R}^n$. O sistema de aproximação simultâneas*

$$|\alpha - \frac{p_i}{q}| < \frac{f_i(q)}{q}, \quad 1 \leq i \leq n \text{ é tal que} \qquad (*)$$

*a) Se $\sum_{q=1}^{\infty} F(q) < +\infty$ então (*) tem apenas um número finito de soluções $\left(\frac{p_1}{q}, \frac{p_2}{q}, \ldots, \frac{p_n}{q}\right) \in \mathbb{Q}^n$, para quase todo $\alpha \in \mathbb{R}^n$.*

*b) Se $\sum_{q=1}^{\infty} F(q) = +\infty$ então (*) tem infinitas soluções $\left(\frac{p_1}{q}, \ldots, \frac{p_n}{q}\right) \in \mathbb{Q}^n$ para quase todo $\alpha \in \mathbb{R}^n$.*

**Demonstração:** Dado $q_0 \in \mathbb{N}$, consideremos o conjunto

$$S(q_0) = \bigcup_{q \geq q_0} \bigcup_{0 \leq p_1, \ldots, p_n < q} \prod_{i=1}^{n} \left( \frac{p_i}{q} - \frac{f_i(q)}{q}, \frac{p_i}{q} + \frac{f_i(q)}{q} \right),$$

que é o conjunto dos $\alpha \in [0,1)^n$ tais que a desigualdade (*) do enunciado do Teorema tem alguma solução com $q \geq q_0$ (e logo $\bigcap_{q_0 \in \mathbb{N}} S(q_0)$ é o conjunto dos $\alpha \in \mathbb{R}^n$ tais que (*) tem infinitas soluções $(\frac{p_i}{q}, \ldots, \frac{p_n}{q}) \in \mathbb{Q}^n$). Temos $m(S(q_0)) \leq \sum_{q=q_0}^{\infty} q^n (\frac{2^n F(q)}{q^n}) = 2^n \sum_{q=q_0}^{\infty} F(q)$, que tende a 0 quando $q$ tende a $\infty$, pois $\sum_{q=1}^{\infty} F(q)$ converge. Portanto, $m(\bigcap_{q_0 \in \mathbb{N}} S(q_0)) = 0$, o que completa a prova de a).

Primeiro obtemos funções decrescentes $g_1, g_2, \ldots, g_n \colon \mathbb{N} \to \mathbb{R}^+$ tais que $\lim\limits_{q \to s_0} \frac{g_i(q)}{f_i(q)} = 0$ e $G = g_1, g_2, \ldots, g_n \colon \mathbb{N} \to \mathbb{R}^+$ satisfaz $\lim\limits_{q \to \infty} qG(q) = 0$ e $\sum_{q=1}^{\infty} G(q) = +\infty$ (podemos tomar $G_1(k) = (F(1) + F(2) + \cdots + F(k))^{-1} \cdot F(k)$ e $G(k) = (G_1(1) + G_1(2) + \cdots + G_1(k))^{-1} G_1(k)$, $\forall\, k \in \mathbb{N}$. Teremos $G_1$ e $G$ decrescentes, $G_1(k) \leq 1/k$, $kG(k) \to 0$, $\Sigma G_1(k) = \infty$, $\Sigma G(k) = \infty$, e definimos $g_i(q) = f_i(q) \cdot (G(q)/F(q))^{1/n}$).

Fixemos agora $q_0 \in \mathbb{N}$ grande e definimos $s_0 = s_0(q_0) = \min\{s \in \mathbb{N} | G(q_0) + G(q_0 + 1) + \cdots + G(s) \geq \tilde{c}\}$, onde $\tilde{c}$ é uma constante que escolheremos posteriormente. Note que $\lim_{q \to \infty} \frac{s_0(q)}{q} = +\infty$.

Para cada $s$ com $q_0 \leq s \leq s_0$ vamos estimar o número de $\left(\frac{r_1}{s}, \frac{r_2}{s}, \ldots, \frac{r_n}{s}\right) \in \mathbb{Q}^n$ com $r_i \in \mathbb{Z}$, $1 \leq i \leq n$, $0 \leq r_i < s$ tais que existem $q$ com $q_0 \leq q < s$, $p_1, p_2, \ldots, p_n \in \mathbb{Z}$, $0 \leq p_i < q$ satisfazendo

$$|\frac{r_i}{s} - \frac{p_i}{q}| < \frac{g_i(q)}{q} + \frac{g_i(s)}{s}, \quad \forall\, i = 1, 2, \ldots, n. \qquad (**)$$

Temos que, como cada $g_i$ é decrescente, (**) implica

$$|r_i q - p_i s| < 2qs \frac{g_i(q)}{q} = 2s g_i(q), \quad i = 1, 2, \ldots, n.$$

Para um tal $\left(\frac{r_1}{s}, \ldots, \frac{r_n}{s}\right)$ que não satisfaz (**) para nenhum $q$ com $q_0 \leq q < s$, $p_1, \ldots, p_n$ o bloco $\prod_{i=1}^{n} \left(\frac{r_i}{s} - \frac{g_i(s)}{s}, \frac{r_i}{s} + \frac{g_i(s)}{s}\right)$ será disjunto de todos os blocos associados a $\left(\frac{p_1}{q}, \ldots, \frac{p_n}{q}\right)$, $\forall\, q$ com $q_0 \leq q < s$, $\forall\, p_1, \ldots, p_n \in \mathbb{Z}$ com $0 \leq p_i < q$.

Para completarmos a prova de b), aplicaremos:

**Lema 2.8** *Para todo $k \in \mathbb{N}$ existe $c_k > 0$ tal que $\sum_{j=1}^{n} \left(\frac{\varphi(j)}{j}\right)^k \geq c_k n$.*

**Demonstração:** Para $k = 1$ segue de

$$\lim_{n \to \infty} \frac{1}{n} \sum_{j=1}^{n} \frac{\varphi(j)}{j} = \lim_{n \to \infty} \frac{1}{n} \sum_{q=1}^{n} \sum_{d|q} \frac{\mu(d)}{d} = \lim_{n \to \infty} \frac{1}{n} \sum_{d=1}^{n} \lceil \frac{n}{d} \rceil \frac{\mu(d)}{d}$$
$$= \sum_{d=1}^{\infty} \frac{\mu(d)}{d^2} = \frac{6}{\pi^2}$$

pois $\sum_{r=1}^{\infty}\frac{\mu(m)}{m^2}\sum_{k=1}^{\infty}\frac{1}{k^2}=\sum_{n=1}^{\infty}\frac{\sum_{m|n}\mu(m)}{n^2}=1$, e $\sum_{k=1}^{\infty}\frac{1}{k^2}=\frac{\pi^2}{6}$. Como $h(x)=x^k$ é convexa para $k\geq 1$, temos $\frac{1}{n}\sum_{j=1}^{n}\left(\frac{\varphi(j)}{j}\right)^k\geq\left(\frac{1}{n}\sum_{j=1}^{n}\frac{\varphi(j)}{j}\right)^k$, donde segue o resultado (com $C_k=\left(\frac{6}{\pi^2}\right)^k$).

□

**Final da demonstração de b):** Se $q_0\leq q<s$, o número de soluções de $|r_iq-p_is|<2sg_i(q)$ com $0\leq p_i<q$, $0\leq r_i<s$ é no máximo $4sg_i(q)$ desde que $\mathrm{mdc}(r_i,s)=1$. De fato, nessas condições $r_iq-p_is$ não se anula, senão teríamos $\frac{p_i}{q}=\frac{r_i}{s}$, que é uma fração irredutível de denominador $s>q$, absurdo. Seja $d=\mathrm{mdc}(s,q)$. Dado $k\in\mathbb{Z}$, a equação diofantina $rq-ps=k$ só tem solução de $d|k$, quando tem $d$ soluções com $0\leq r<s$. Portanto, $0<rq-ps<x$ (resp. $-x<rq-ps<0$) tem no máximo $d\lfloor\frac{x}{d}\rfloor\leq x$ soluções $(p,r)$ com $0\leq r<s$, o que claramente implica a afirmação. Portanto, o número de soluções da desigualdade acima para todo $i$ com $1\leq i\leq n$ é no máximo $4^ns^nG(q)$. Por outro lado há $\varphi(s)^n$ pontos $\left(\frac{r_i}{s},\ldots,\frac{r_n}{s}\right)$, $0\leq r_i<s$, $\mathrm{mdc}(r_i,s)=1$, $1\leq i\leq n$. Isso nos dá a estimativa do número de novos blocos disjuntos dos anteriormente considerados que têm denominador $s$ de pelo menos $\varphi(s)^n-4^ns^n\sum_{q=q_0}^{s-1}G(q)$, e para o volume da união dos blocos disjuntos adicionados até o denominador $s_0$ de pelo menos

$$\sum_{s=q_0}^{s_0}(\varphi(s)^n-4^ns^n\sum_{q=q_0}^{s-1}G(q))\frac{2^nG(s)}{s^n}$$
$$=2^k\sum_{s=q_0}^{s_0}\left(\frac{\varphi(s)}{s}\right)^nG(s)-8^n\sum_{s=q_0}^{s_0}\left(\sum_{q=q_0}^{s-1}G(q)\right)G(s).$$

Por outro lado, com $s_0=\min\{s\geq q_o|\sum_{q=q_0}^{s}G(q)\geq\tilde{c}\}$, temos

$$\begin{aligned}\sum_{s=q_0}^{s_0}\left(\frac{\varphi(s)}{s}\right)^nG(s)&=\sum_{s=q_0}^{s_0-1}(G(s)-G(s+1))\sum_{j=q_0}^{s}\left(\frac{\varphi(j)}{j}\right)^n+G(s_0)\sum_{j=q_0}^{s_0}\left(\frac{\varphi(j)}{j}\right)^n\\&\geq\sum_{s=q_0}^{s_0-1}(G(s)-G(s+1))(c_ns-q_0)+G(s_0)(c_ns_0-q_0)\\&=c_n\sum_{s=q_0+1}^{s_0}G(s)-(1-c_n)q_0G(q_0)\\&=c_n\tilde{c}+\varepsilon_1\quad\text{onde }\varepsilon_1\to 0\text{ quando }q_0\to\infty\end{aligned}$$

(pois $\lim_{q_0\to\infty}q_0G(q_0)=0$).

Por outro lado, $8^n\sum_{s=q_0}^{s_0}\left(\sum_{q=q_0}^{s-1}G(q)\right)G(s)\leq 8^n\tilde{c}\sum_{s=q_0}^{s_0}G(s)\leq 8^n\tilde{c}(\tilde{c}+\varepsilon_2)$ onde $\varepsilon_2=G(s_0)\to 0$ quando $q_0\to\infty$. Assim, nosso volume é, pelo menos, $2^n(c_n\tilde{c}+\varepsilon_1)-8^n\tilde{c}(\tilde{c}+\varepsilon_2)$. Tomando $\tilde{c}=\frac{c_n}{4^{n+1}}$ temos que, se $q_0$ é suficientemente grande (e logo $\varepsilon_1$ e $\varepsilon_2$ suficientemente pequenos), o volume de $A(q_0)$ é pelo menos $c_n^2/2^{n+3}$, onde

$$A(q_0)=\bigcup_{q\geq q_0}\bigcup_{0\leq p_1,\ldots,p_n<q}\prod_{i=1}^{n}\left(\frac{p_i}{q}-\frac{g_i(q)}{q},\frac{p_i}{q}+\frac{g_i(q)}{q}\right).$$

Como $A(q) \supset A(q+1), \forall\, q \in \mathbb{N}$, temos $m(A_\infty) \geq \frac{1}{15 \cdot 2^n} > 0$, onde $A_\infty = \bigcap_{q \in \mathbb{N}} A(q)$. Se $\beta = (\beta_1, \beta_2, \ldots, \beta_n) \in A_\infty$, $|\beta_i - \frac{p_i}{q}| < \frac{g_i(q)}{q}$, $i = 1, 2, \ldots, n$ tem infinitas soluções $(\frac{p_1}{q}, \frac{p_1}{q}, \ldots, \frac{p_n}{q}) \in \mathbb{Q}^n$. Como $m(A_\infty) > 0$, dado $\varepsilon > 0$ existe cubo $Q = \prod_{i=1}^{n} [\frac{b_i}{C}, \frac{b_i+1}{C}]$, $C \in \mathbb{N}$, $b_i \in \mathbb{Z}$, $0 \leq b_i < C$ tal que $m(A_\infty \cap Q) \geq (1-\varepsilon) m(Q)$. Se $T \colon \mathbb{R}^n \to \mathbb{R}^n$ é dada por

$$T(X_1, \ldots, X_n) = (CX_1 - b_1, CX_2 - b_2, \ldots, CX_n - b_n),$$

temos $T(Q) = [0,1]^n$ e $m(T(Q \cap A_\infty)) \geq 1 - \varepsilon$. Além disso, se $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in T(Q \cap A_\infty)$, $\alpha = T(\beta)$, $\beta = (\beta_1, \ldots, \beta_n) \in A_\infty \cap Q$, e portanto $|\beta_i - \frac{p_i}{q}| < \frac{g_i(q)}{q}$, para todo $i = 1, 2, \ldots, n$ tem infinitas soluções $(\frac{p_1}{q}, \frac{p_2}{q}, \ldots, \frac{p_n}{q}) \in \mathbb{Q}^n$, donde $|\alpha_i - \frac{r_i}{q}| < \frac{C g_i(q)}{q}$ (e logo $|\alpha_i - \frac{r_i}{q}| < \frac{f_i(q)}{q}$) tem infinitas soluções

$$\left(\frac{r_1}{q}, \frac{r_2}{q}, \ldots, \frac{r_n}{q}\right) = \left(\frac{Cp_1 - b_1}{q}, \frac{Cp_1 - b_2}{q}, \ldots, \frac{Cp_n - b_n}{q}\right) \in \mathbb{Q}^n,$$

e como $\varepsilon > 0$ pode ser feito arbitrariamente pequeno está provado o item b).

□

## 2.4 Aproximações diofantinas não-homogêneas

**Proposição 2.9** *Se $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ então $X = \{m + n\alpha \,|\, m, n \in \mathbb{Z}\}$ é denso em $\mathbb{R}$.*

**Demonstração:** Dado $\varepsilon > 0$ existem $p, q$ inteiros com $> 1/\varepsilon$ tais que $|\alpha - \frac{p}{q}| < \frac{1}{q^2} \Rightarrow 0 < |q\alpha - p| < \frac{1}{q} < \varepsilon$. Dado $x \in \mathbb{R}$ existe $k \in \mathbb{Z}$ tal que $x$ está entre $k(q\alpha - p)$ e $(k+1)(q\alpha - p)$, donde $|x - k(q\alpha - p)| \leq \varepsilon$. Como $k(q\alpha - p) = -pk + qk\alpha \in X$, o resultado está provado.

□

O próximo resultado, devido a Kronecker, estende a proposição anterior para dimensão qualquer.

**Proposição 2.10** *Seja $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n) \in \mathbb{R}^n$. Suponha que $1, \alpha_1, \ldots, \alpha_n$ sejam linearmente inependentes sobre $\mathbb{Q}$ (isto é, $k + m_1\alpha_1 + m_2\alpha_2 + \cdots + m_n\alpha_n = 0$ com $k, m_1, \ldots, m_n \in \mathbb{Z}$ implica $k = m_1 = \cdots = m_n = 0$). Então $X = \{k\alpha + m_1 e_1 + m_2 e_2 + \cdots + m_n e_n | k, m_1, \ldots, m_n \in \mathbb{Z}\}$ é denso em $\mathbb{R}^n$, onde $e_1 = (1, 0, \ldots, 0), \ldots, e_n = (0, \ldots, 0, 1)$ são os elementos da base canônica de $\mathbb{R}^n$.*

**Demonstração:** Seja $\overline{X} \subset \mathbb{R}^n$ o fecho de $X$, e $V \subset \overline{X}$ um subespaço vetorial maximal de $\mathbb{R}^n$ contido em $\overline{X}$. Suponhamos por absudo que $V \neq \mathbb{R}^n$. Seja $f$ um funcional linear não nulo de $\mathbb{R}^n$.

Seja $V^\perp$ o complemento ortogonal de $V$, e seja $\pi\colon \mathbb{R}^n \to V^\perp$ a projeção ortogonal sobre $V^\perp$. Para todo $x \in \overline{X}$, $\pi(x) \in \overline{X}$, pois $\pi(x) = x + (\pi(x) - x)$, $\pi(x) - x \in C \subset \overline{X}$ e $\overline{X}$ é invariante por adição (pois $X$ também é).

Seja $k = \dim V^\perp$. Escolhemos vetores $e_{i_1}, e_{i_2}, \ldots, e_{i_k}$ tais que $\pi(e_{i_1}), \pi(e_{i_2}), \ldots, \pi(e_{i_k})$ geram $V^\perp$. Se fizermos $e_0 = \alpha$, para todo $i = 0, 1, \ldots, n$ escrevemos $\pi(e_i) = \sum_{j=1}^k \lambda_{ij}\pi(e_{i_j})$. Não podemos ter $\lambda_{i1} \in \mathbb{Q}$ para todo $i$, senão podemos definir um funcional linear $f$ da seguinte forma: dado $x \in \mathbb{R}^n$ escrevemos $\pi(x)$ como $\sum_{j=1}^k \beta_j \pi(e_{i_j})$, e tomamos $f(x) = \beta_1$. Se $\lambda_{i1} = f(e_i) \in \mathbb{Q}$ para todo $i$, teríamos $\lambda_{01} = f(\alpha) = \sum_{i=1}^n \alpha_i f(e_i) = \sum_{i=1}^n \lambda_{i1}\alpha_i \in \mathbb{Q}$, contradizendo a hipótese da proposição.

Seja então $i_0$ tal que $\lambda_{i_0 1} \notin \mathbb{Q}$. Tomamos $\gamma = (\lambda_{i_0 1}, \ldots, \lambda_{i_0 k}) \in \mathbb{R}^k$. Como observamos na introdução deste artigo, existem $x_n = q_n\gamma - (p_{1n}, p_{2n}, \ldots, p_{kn}) \neq 0$, com $q_n, p_{1n}, \ldots, p_{kn} \in \mathbb{Z}$ e $\lim\limits_{n\to\infty} |x_n| \leq \lim\limits_{n\to\infty} |q_n|^{-1/k} = 0$, e portanto, se $w_n = q_n\pi(e_{i_0}) - \sum_{j=1}^k p_{jn}\pi(e_{i_j})$, $\lim\limits_{n\to\infty} w_n = 0$ (e $w_n \neq 0, \forall\, n$). Passando a uma subseqüência, se necessário, podemos supor que $\lim\limits_{n\to\infty} \frac{w_n}{|w_n|} = \tilde{w} \in S^{n-1} \cap V^\perp$. Para todo $t \in \mathbb{R}$, temos que $t\tilde{w} = \lim\limits_{n\to\infty} \lfloor \frac{t}{w_n} \rfloor w_n \in \overline{X}$, $\forall\, n \in \mathbb{N}$. Portanto, como $\overline{X}$ é invariante por adição, o subespaço $\tilde{V} = \{v + t\tilde{w} | v \in V,\ t \in \mathbb{R}\}$ é tal que $\tilde{V} \subset \overline{X}$ e $\tilde{V}$ contém propriamente $V$, absurdo.

$\square$

**Observação 2.11** A hipótese da Proposição A.2 é necessária, pois se existem inteiros $k, m_1, \ldots, m_n$ não todos nulos tais que $k + m_1\alpha_1 + \cdots + m_n\alpha_n = 0$ então $\overline{X} \subset \{(x_1, \ldots, x_n) \in \mathbb{R}^n | m_1x_1 + m_2x_2 + \cdots + m_nx_n \in \mathbb{Z}\}$, que é um fechado com interior vazio.

O teorema de Kronecker possui a seguinte generalização, devida a Weyl. Antes necessitamos de uma

**Definição 2.12** *Uma sequência $(a_n)_{n\geq 0}$ com $a_n \in [0,1]^d$ é dita* uniformemente distribuída *se para qualquer paralelepípedo retangular $C \subset [0,1]^d$, temos*

$$\lim_{n\to\infty} \frac{\#\{j \mid 1 \leq j \leq n \text{ e } a_j \in C\}}{n} = m(C),$$

*onde $m(C)$ é o volume de $C$.*

**Observação 2.13** Caso uma seqüência $(a_n)_{n\geq 0}$ com $a_n \in [0,1]^d$ seja uniformemente distribuída, então a propriedade da definição valerá não somente para paralelepípedos retangulares, mas também para qualquer conjunto $C \subset [0,1]^d$ com volume (*à la* Riemann) bem definido (o que requer que o conjunto seja J-mensurável, i.e., que sua fronteira tenha medida nula).

**Teorema 2.14 (Weyl)** *Seja $\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{R}^d$ onde as coordenadas são tais que $1, \alpha_1, \ldots, \alpha_d$ são linearmente independentes sobre $\mathbb{Q}$. Então a sequência*

$$\{n\alpha\} \stackrel{\text{def}}{=} (n\alpha_1 - \lfloor n\alpha_1 \rfloor, \ldots, n\alpha_d - \lfloor n\alpha_d \rfloor)$$

*é uniformemente distribuída no cubo $[0,1]^d$.*

**Demonstração:** Sejam $C_1, C_2 \subset [0,1)^d$ dois cubos abertos tais que o lado de $C_2$ é menor que o lado de $C_1$. Então o fecho $\overline{C}_2$ de $C_2$ está contido em um transladado de $C_1$ ($\overline{C}_2 \subset C_1 + v$, $\exists v \in \mathbb{R}^d$). Como existem vetores $\tilde{v}$ arbitrariamente próximos de $v$, com $\tilde{v} = (q\alpha_1 + p_1, \ldots, q\alpha_d + p_d)$, $q, p_1, \ldots, p_d \in \mathbb{Z}$, tomando um tal $\tilde{v}$ de modo que sua distância a $v$ seja menor que a distância de $\overline{C}_2$ à fronteira de $C_1 + v$, temos que

$$\{m\alpha\} \in \overline{C}_2 \implies \{(m-q)\alpha\} \in \overline{C}_2 - \tilde{v} \subset C_1.$$

Se definirmos, para cada paralelepípedo retangular $C$, $\mathcal{N}(n, \alpha, C) := \#\{j \mid 1 \leq j \leq n \text{ e } \{j\alpha \in C\}$, teremos então $\mathcal{N}(n, \alpha, C_2) \leq \mathcal{N}(n, \alpha, C_1) + |q|$ para todo $n \in \mathbb{N}$.

Seja então $N$ um número natural grande dado e $C$ um cubo dado de lado $1/N$. Considere a decomposição $[0,1)^d = (\bigcup_{k=0}^{N} \left[\frac{k}{N+1}, \frac{k+1}{N+1}\right))^d$ como a união de $(N+1)^d$ cubos de lado $\frac{1}{N+1}$. Seja $\mathcal{C}$ a coleção desses cubos. Para cada cubo $\tilde{C} \in \mathcal{C}$ dessa coleção, existe um inteiro $q^{(\tilde{C})}$ tal que $\mathcal{N}(n, \alpha, \tilde{C}) \leq \mathcal{N}(n, \alpha, C) + |q^{(\tilde{C})}|$ para todo $n \in \mathbb{N}$. Se $\hat{q}$ é o máximo dos números $|q^{(\tilde{C})}|$, podemos usar o fato de que, para todo $n \in \mathbb{N}$, existe um cubo $\tilde{C} \in \mathcal{C}$ com $\mathcal{N}(n, \alpha, \tilde{C}) \geq \frac{n}{(N+1)^d}$ para concluir que $\mathcal{N}(n, \alpha, C) \geq \frac{n}{(N+1)^d} - \hat{q}, \forall n \in \mathbb{N}$, de onde obtemos $\liminf\limits_{n\to\infty} \mathcal{N}(n, \alpha, C)/n \geq \frac{1}{(N+1)^d}$.

Analogamente (considerando a decomposição $[0,1)^d = (\bigcup_{k=0}^{N-2} \left[\frac{k}{N-1}, \frac{k+1}{N-1}\right))^d$ como a união de $(N-1)^d$ cubos de lado $\frac{1}{N-1}$, podemos provar que $\limsup\limits_{n\to\infty} \mathcal{N}(n, \alpha, C)/n \leq \frac{1}{(N-1)^d}$.

Seja agora $B = \Pi_{i=1}^d [a_i, b_i)$ um paralelepípedo retangular dado. Para cada número natural grande $N$, $B$ contém uma união disjunta de $\Pi_{i=1}^d \lfloor N(b_i - a_i) \rfloor$ cubos de lado $1/N$. Assim, da discussão acima, segue que

$$\liminf_{n\to\infty} \frac{\mathcal{N}(n, \alpha, B)}{n} \geq \frac{1}{(N+1)^d} \Pi_{i=1}^d \lfloor N(b_i - a_i) \rfloor \geq (\frac{N}{N+1})^d \Pi_{i=1}^d (b_i - a_i - \frac{1}{N}),$$

e, fazendo $N$ tender a infinito, obtemos $\liminf\limits_{n\to\infty} \mathcal{N}(n, \alpha, B)/n \geq \Pi_{i=1}^d (b_i - a_i) = m(B)$. Por outro lado, $B$ está contido numa união de $\Pi_{i=1}^d \lceil N(b_i - a_i) \rceil$ cubos de lado $1/N$, donde, pela discussão acima, $\limsup\limits_{n\to\infty} \mathcal{N}(n, \alpha, B)/n \geq \frac{1}{(N-1)^d} \Pi_{i=1}^d \lceil N(b_i - a_i) \rceil \geq (\frac{N}{N-1})^d \Pi_{i=1}^d (b_i - a_i + 1/N)$, e, fazendo $N$ tender a infinito, obtemos $\limsup\limits_{n\to\infty} \mathcal{N}(n, \alpha, B)/n \leq \Pi_{i=1}^d (b_i - a_i) = m(B)$. Portanto $\lim\limits_{n\to\infty} \mathcal{N}(n, \alpha, B)/n = \Pi_{i=1}^d (b_i - a_i) = m(B)$. $\square$

**Observação 2.15** É possível provar o teorema anterior com técnicas de análise de Fourier. Dizemos que uma sequência $(w_n)_{n\geq 0}$ com $w_n \in \mathbb{R}^d$ é dita *uniformemente distribuída módulo 1* se $(\{w_n\})_{n\geq 0}$ é uniformemente distribuída em $[0,1]^d$, onde, para $w = (w_1, w_2, \ldots, w_d) \in \mathbb{R}^d$, $\{w\} := (\{w_1\}, \{w_2\}, \ldots, \{w_d\})$. É possível provar que $(w_n)_{n\geq 0}$ é uniformemente distribuída módulo 1 se, e somente se, para todo vetor $v \in \mathbb{Z}^d$ com $v \neq (0, 0, \ldots, 0)$,

$$\lim_{n\to\infty} \frac{1}{n} \sum_{1\leq j\leq n} \exp(2\pi i \langle w_n, v\rangle) = 0$$

(onde $\langle u, v\rangle$ denota o produto interno dos vetores $u$ e $v$). Não é difícil verificar esta condição para a sequência $w_n = n\alpha$, onde $\alpha = (\alpha_1, \ldots, \alpha_d) \in \mathbb{R}^d$ é tal que $1, \alpha_1, \ldots, \alpha_d$ são linearmente independentes sobre $\mathbb{Q}$.

Esta caracterização de sequências uniformemente distribuídas módulo 1 pode ser usada para provar o seguinte fato: uma condição suficiente (mas não necessária) para que uma sequência $(w_n)_{n\geq 0}$ com $w_n \in \mathbb{R}$ seja uniformemente distribuída módulo 1 é que, para todo inteiro positivo $h$, a sequência $(w_{n+h} - w_n)_{n\in\mathbb{N}}$ seja uniformemente distribuída. Este fato, por sua vez, pode ser usado para provar (por indução no grau) que, para todo polinômio $p(x) = \alpha_d x^d + \alpha_{d-1}x^{d-1} + \cdots + \alpha_0$ que tenha algum coeficiente não constante $\alpha_j, j \geq 1$ irracional, a sequência $(p(n))_{n\in\mathbb{N}}$ é uniformemente distribuída módulo 1.

Veja o capítulo IV de [C1] ou [StSa], páginas 105-113 para mais detalhes.

## 2.5 Números de Liouville

Vimos no corolário i) do teorema de Khintchine que $\operatorname{ord}\alpha = 2$ para quase todo $\alpha \in \mathbb{R}$. Dado $\alpha \in \mathbb{R}\setminus\mathbb{Q}$, dizemos que $\alpha$ é um *número de Liouville* se $\operatorname{ord}\alpha = \infty$, isto é, se para todo $n > 0$ existem infinitos racionais $\frac{p}{q}$ com $|\alpha - \frac{p}{q}| < \frac{1}{q^n}$. O conjunto dos número de Liouville é portanto dado por

$$L = \bigcap_{n\in\mathbb{N}} \bigcup_{q\geq 2} \bigcup_{p\in\mathbb{Z}} \Big(\frac{p}{q} - \frac{1}{q^n}, \frac{p}{q} + \frac{1}{q^n}\Big).$$

Assim, $L$ é uma interseção enumerável de abertos densos e portanto é um conjunto genérico no sentido de Baire, embora, como vimos, tenha medida nula.

Uma parte do interesse dos números de Liouville é motivado pelo seguinte resultado, que implica que todo número de Liouville é transcendente (a recíproca entretanto é falsa, já que o conjunto dos números algébricos é enumerável e portanto o conjunto dos números transcendentes tem medida total).

**Proposição 2.16** *Seja $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ um número algébrico de grau $n$, isto é, $\alpha$ é raiz de um polinômio não nulo de grau $n$ com coeficientes inteiros. Então existe $c > 0$ tal que*

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

*para todo $p/q \in \mathbb{Q}$. Em particular,* $\operatorname{ord}\alpha \leq n$.

**Demonstração:** Seja $P(x)$ um polinômio de grau $n$ com coeficientes inteiros tal que $P(\alpha) = 0$. Existe um $d > 0$ tal que $P(x) \neq 0$ para todo $0 < |x - \alpha| < d$. Sejam

$$k = \max_{|x-\alpha|\leq 1} |P'(x)| \qquad \text{e} \qquad c = \min\left\{1, d, \frac{1}{k}\right\}$$

Se $|\alpha - \frac{p}{q}| < \frac{c}{q^n}$, com $p, q \in \mathbb{N}_{>0}$, teríamos $|\alpha - \frac{p}{q}| < c \leq d$, donde $P(\frac{p}{q}) \neq 0$. Assim, como $q^n \cdot P(\frac{p}{q}) \in \mathbb{Z}$, $\left|q^n \cdot P(\frac{p}{q})\right| \geq 1 \iff \left|P(\frac{p}{q})\right| \geq \frac{1}{q^n}$. Por outro lado,

$$\left|P\left(\frac{p}{q}\right)\right| = \left|P\left(\frac{p}{q}\right) - P(\alpha)\right| = \left|P'(y) \cdot \left(\frac{p}{q} - \alpha\right)\right|,$$

para algum $y$ estritamente entre $\alpha$ e $\frac{p}{q}$, pelo teorema do valor médio, mas $|y - \alpha| < |\alpha - \frac{p}{q}| < c \leq 1$ implica $|P'(y)| \leq k$, logo

$$\frac{1}{q^n} \leq \left|P\left(\frac{p}{q}\right)\right| \leq k\left|\alpha - \frac{p}{q}\right| < \frac{kc}{q^n} \leq \frac{1}{q^n}$$

o que é absurdo. □

Um teorema não trivial devido a Roth (e que lhe rendeu uma medalha Fields) mostra que, de fato, ord $\alpha = 2$, para *todo* $\alpha$ algébrico (veja por exemplo [Leq]).

Lembramos que, usando a fração contínua de $e$, é possível provar que $\operatorname{ord}(e) = 2$ (veja o capítulo 3), isto é, o número $e$ é transcendente, mas "não muito".

## 2.6 Problemas Propostos

**1** Mostre que a sequência $(a_n)$ com $a_n \in [0,1]^d$ é uniformemente distribuída se, e só se, para qualquer função contínua $f\colon [0,1]^d \to \mathbb{R}$, temos

$$\lim_{n\to\infty} \frac{f(a_1) + f(a_2) + \cdots + f(a_n)}{n} = \int_{[0,1]^d} f.$$

**2** Prove que $\alpha = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ é um número de Liouville e, portanto, é transcendente.

**3** Mostrar que se $\alpha$ e $\beta$ são números irracionais positivos satisfazendo $\frac{1}{\alpha} + \frac{1}{\beta} = 1$, então as sequências

$$\lfloor\alpha\rfloor, \lfloor 2\alpha\rfloor, \lfloor 3\alpha\rfloor, \cdots \qquad \text{e} \qquad \lfloor\beta\rfloor, \lfloor 2\beta\rfloor, \lfloor 3\beta\rfloor, \cdots$$

juntas contém todo inteiro positivo exatamente uma vez.

**4** Mostrar que se $a$ e $b$ são números inteiros positivos arbitrários, então

$$|a\sqrt{2} - b| > \frac{1}{2(a+b)}.$$

**5** Construa uma sequência infinita limitada $x_0, x_1, x_2, \ldots$ tal que para todos os números naturais $i$ e $j$ com $i \neq j$ se tenha

$$|x_i - x_j||i - j| \geq 1.$$

**Obs.**: Uma consequência imediata deste fato é que, dado um real $a > 1$, existe uma sequência infinita limitada $x_0, x_1, x_2, \ldots$ tal que para todos os números naturais $i$ e $j$ com $i \neq j$ se tenha

$$|x_i - x_j||i - j|^a \geq 1.$$

O problema 6 da IMO de 1991 consistiu em provar esta última afirmação.

**6** Sejam $a, b, c$ inteiros não todos nulos. Mostrar que

$$\frac{1}{4a^2 + 3b^2 + 2c^2} \leq |\sqrt[3]{4}a + \sqrt[3]{2}b + c|.$$

**7** Mostrar que a sequência $\{a_n\}_{n \geq 1}$ definida por $a_n = \lfloor n\sqrt{2} \rfloor$ contém um número infinito de termos que são potências de 2.

**8** Seja $\{a_n\}$ uma sequência crescente de inteiros positivos tais que para todo $K$ existe um $n \in \mathbb{N}$ tal que $a_{n+1} > Ka_n$. Mostrar que $\sum_{n=1}^{\infty} 2^{-a_n}$ é um número de Liouville (e portanto é transcendente).

**9** a) Prove que existe $n \in \mathbb{N}$ tal que os 2010 primeiros dígitos de $2^n$ são iguais a 1.

b) Prove que existe $n \in \mathbb{N}$ tal que os 2010 primeiros dígitos de $2^n$ são iguais a 1 e os 2010 primeiros dígitos de $3^n$ são iguais a 2.

**10** Prove que, para todo inteiro $a$ com $1 \leq a \leq 9$ temos

$$\lim_{n \to \infty} \frac{\#\{j \mid 1 \leq j \leq n \text{ e o primeiro dígito de } 2^j \text{ é } a\}}{n} = \frac{\log(a+1) - \log a}{\log 10}.$$

# Capítulo 3

# Os Espectros de Markov e Lagrange

## 3.1 Definições e enunciados

Seja $\alpha$ um número irracional. De acordo com o teorema de Dirichlet, a desigualdade $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$ tem uma infinidade de soluções racionais $p/q$. Markov e Hurwitz melhoraram este resultado, provando que, para todo irracional $\alpha$, a desigualdade $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5} \cdot q^2}$ tem uma infinidade de soluções racionais, e que $\sqrt{5}$ é a melhor constante com esta propriedade: para $\alpha = \frac{1+\sqrt{5}}{2}$, e para qualquer $\varepsilon > 0$, a desigualdade $\left|\alpha - \frac{p}{q}\right| < \frac{1}{(\sqrt{5}+\varepsilon)q^2}$ tem apenas um número finito de soluções (ver apêndice). Entretanto, fixado $\alpha$ irracional, pode-se esperar resultados melhores, o que nos leva a associar a cada $\alpha$ a sua constante de melhor aproximação $k(\alpha) = \sup\{k > 0 \mid \left|\alpha - \frac{p}{q}\right| < \frac{1}{kq^2}$ tem uma infinidade de soluções racionais $p/q\} = \limsup_{p,q\in\mathbb{Z}} \left(|q(q\alpha - p)|^{-1}\right) \in \mathbb{R} \cup \{+\infty\}$. Nossa discussão inicial mostra que $k(\alpha) \geq \sqrt{5}$ para todo $\alpha \in \mathbb{R}$, e $k\left(\frac{1+\sqrt{5}}{2}\right) = \sqrt{5}$. Não é difícil provar que $k(\alpha) = +\infty$ para quase todo $\alpha \in \mathbb{R}$. Estaremos interessados nos $\alpha \in \mathbb{R}$ tais que $k(\alpha) < +\infty$, e, mais particularmente, na imagem da função $k$, isto é, no conjunto $L = \{k(\alpha) \mid \alpha \in \mathbb{R}\backslash\mathbb{Z} \text{ e } k(\alpha) < +\infty\}$. Este conjunto é conhecido como o *espectro de Lagrange*.

Provamos no apêndice uma fórmula para $k(\alpha)$: escrevemos $\alpha$ em fração contínua, $\alpha = [a_0, a_1, a_2, \ldots]$ e definimos, para $n \in \mathbb{N}$, $\alpha_n = [a_n, a_{n+1}, a_{n+2}, \ldots]$ e $\beta_n = [0, a_{n-1}, a_{n-2}, \ldots]$. Temos então $k(\alpha) = \limsup_{n\to\infty} (\alpha_n + \beta_n)$. Isto segue dos resultados do Capítulo 3.

É interessante observar que se mudássemos um pouco as funções envolvidas na definição do espectro de Lagrange ele seria um conjunto bastante trivial: se para $f\colon \mathbb{R} \to \mathbb{R}_+$ considerarmos o conjunto $k_f(\alpha) := \sup\{k > 0 \mid |\alpha - \frac{p}{q}| < \frac{f(q)}{k}$ tem infinitas soluções racionais $p/q\}$ então, caso tenhamos $\lim_{q\to+\infty} q^2 f(q) = 0$ então a imagem de $k_f$ seria $(0,+\infty]$ (ou $[0,+\infty]$, se consideramos $\sup(\varnothing)=0$ neste contexto) e, caso $\lim_{q\to+\infty} q^2 f(q)=+\infty$, então a imagem de $k_f$ seria $\{+\infty\}$.

O conjunto $L$ encodifica uma série de propriedades diofantinas de números reais, e vem sendo estudado há bastante tempo. Talvez o primeiro resultado não-trivial sobre ele se deva a Markov, que provou em 1879 (ver [Mar1] e [Mar2]) que $L\cap(-\infty,3)=\{k_1=\sqrt{5}<k_2=2\sqrt{2}<k_3=\frac{\sqrt{221}}{5}<\cdots\}$, onde $(k_n)$ é uma seqüência convergente a 3 tal que $k_n^2\in\mathbb{Q}$ para todo $n$. Assim, o "começo" do espectro de Lagrange é discreto. Essa afirmação não é verdadeira para todo o conjunto $L$. Marshall Hall prova em 1947 ([H]) que $L$ contém toda uma semi-reta (por exemplo $[6,+\infty)$), e G. Freiman determinou em 1975 a maior semi-reta que está contida em $L$, que é $\left[4+\frac{253589820+283748\sqrt{462}}{491993569},+\infty\right)$. Estes dois últimos resulados baseam-se fortemente no estudo de somas de conjuntos de Cantor regulares, cuja relação com o espectro de Lagrange tem origem na fórmula que apresentamos para $k(\alpha)$, e é o tema principal deste capítulo. Por exemplo, o resultado que M. Hall enuncia em seu artigo [H] é o seguinte: se $C(4)$ é o conjunto de Cantor regular dos reais de $[0,1]$ em cuja fração contínua aparecem apenas os coeficientes 1, 2, 3 e 4 então $C(4)+C(4)=[\sqrt{2}-1,4(\sqrt{2}-1)]$, do qual não é difícil deduzir que $L\supset[6,+\infty)$ via a fórmula para $k(\alpha)$.

De $k(\alpha)=\limsup_{n\to\infty}(\alpha_n+\beta_n)$ podemos obter a seguinte caracterização do espectro de Lagrange: seja $\Sigma=\left(\mathbb{N}^*\right)^{\mathbb{N}}$, o conjunto das seqüências bi-infinitas de inteiros positivos, e $\sigma\colon\Sigma\to\Sigma$ o shift definido por $\sigma((a_n)_{n\in\mathbb{Z}})=(a_{n+1})_{n\in\mathbb{Z}}$. Se $f\colon\Sigma\to\mathbb{R}$ é definida por $f((a_n)_{n\in\mathbb{Z}})=\alpha_0+\beta_0=[a_0,a_1,a_2,\ldots]+[0;a_{-1},a_{-2},\ldots]$ então $L=\{\limsup_{n\to+\infty} f(\sigma^n\underline{\theta}),\underline{\theta}\in\Sigma\}$. Outro conjunto de números reais que será de nosso interesse é o *espectro de Markov* $M$, que é igual a $\{\sup_{n\to\infty} f(\sigma^n\underline{\theta}),\underline{\theta}\in\Sigma\}$. O espectro de Markov tem a seguinte interpretação aritmética: $M=\{(\inf_{(x,y)\in\mathbb{Z}^2\setminus(0,0)}|f(x,y)|)^{-1};\ f(x,y)=ax^2+bxy+cy^2,\ b^2-4ac=1\}$. São fatos conhecidos que $L$ e $M$ são subconjuntos fechados da reta e que $L\subset M$. Provamos em [M] os seguintes resultados:

**Teorema 3.1** *Para todo $t\in\mathbb{R}$, as dimensões de Hausdorff de $L\cap(-\infty,t)$ e de $M\cap(-\infty,t)$ são iguais. Se denotarmos essas dimensões por $d(t)$, temos os seguintes fatos:*

*a)* $d\colon\mathbb{R}\to[0,1]$ *é contínua e sobrejetiva.*

*b)* $d(t)=\min\{1,2\cdot HD(k^{-1}(-\infty,t))\}$

*c)* $\max\{t\in\mathbb{R}\mid d(t)=0\}=3$

*d)* $d(\sqrt{12})=1$

(As afirmações c) e d) são consequências simples de b)).

**Teorema 3.2** *O conjunto dos pontos de acumulação de $L$ é perfeito, isto é, $L'=L''$.*

**Teorema 3.3** $0<HD(M\backslash L)<1$.

Estes teoremas são baseados na ideia de aproximar partes de $M$ e de $L$ por dentro e por fora por somas de conjuntos de Cantor regulares de dimensões próximas. A prova do Teorema 1.1 depende de modo essencial de um resultado sobre dimensões de Hausdorff de somas aritméticas de conjuntos de Cantor regulares, cuja prova depende do lema de recorrência de escala de [MY].

## 3.2 Problemas Propostos

**1** Dizemos que dois números irracionais $\alpha$ e $\beta$ são $GL_2(\mathbb{Z})$-equivalentes se existem inteiros $a, b, c, d$ com $|ad - bc| = 1$ tais que $\beta = \frac{a\alpha+b}{c\alpha+d}$.

Mostre que, se as frações contínuas de $\alpha$ e $\beta$ são $\alpha = [a_0; a_1, a_2, \dots]$ e $\beta = [b_0; b_1, b_2, \dots]$ então $\alpha$ e $\beta$ são $GL_2(\mathbb{Z})$-equivalentes se, e somente se, existem $r \in \mathbb{Z}$ e $n_0 \in \mathbb{N}$ tais que $b_n = a_{n+r}, \forall n \geq n_0$.

Conclua que $k(\alpha) = k(\beta)$ sempre que $\alpha$ e $\beta$ são $GL_2(\mathbb{Z})$-equivalentes.

**2** Mostre que se $f : \mathbb{R} \to \mathbb{R}_+$ decrescente e

$$k_f(\alpha) := \sup \left\{ k > 0 \ \middle| \ \left| \alpha - \frac{p}{q} \right| < \frac{f(q)}{k} \text{ tem infinitas soluções racionais } \frac{p}{q} \right\}$$

então, caso tenhamos $\lim_{q \to +\infty} q^2 f(q) = 0$, a imagem de $k_f$ é $(0, +\infty]$ (ou $[0, +\infty]$, se consideramos $\sup(\varnothing) = 0$ neste contexto) e, caso $\lim_{q \to +\infty} q^2 f(q) = +\infty$, então a imagem de $k_f$ é $\{+\infty\}$.

**3** Use o fato de que $C(4) + C(4) = [\sqrt{2} - 1, 4(\sqrt{2} - 1)]$ e a fórmula para $k(\alpha)$ para mostrar que $L \supset [6, +\infty)$.

# Referências Bibliográficas


[C1] J. W. S. Cassels, *An introduction to Diophantine approximation*, Cambridge Tracts in Mathematics and Mathematical Physics 45, Hafner Publishing Co. (1972)

[C2] J. W. S. Cassels, *Some metrical theorems in Diophantine approximation I*, Proc. Camb. Phil. Soc. 46 (1950), 209–218.

[Cohn] H. Cohn, *A short proof of the simple continued fraction expansion of e*, Am. Math. Monthly 113, 57–62 (2006).

[H] M. Hall, *On the sum and product of continued fractions*, Annals of Math., Vol. **48**, (1947), pp. 966–993.

[K] A. Khintchine: *Zur metrischen Theorie der diophantischen Approximationen*, Math. Z. **24** (1926), 706–714.

[Leq] Y. Lequain, *Aproximação de um número real por números racionais*, 19° Colóquio Brasileiro de Matemática (1993).

[M1] C.G. Moreira, *Geometric properties of the Markov and Lagrange spectra*. Preprint - IMPA - 2009.

[M2] C.G. Moreira, *Propriedades estatísticas de frações contínuas e aproximações diofantinas:o teorema de Khintchine*, Revista Matemática Universitária número **29**, pp. 125-137

[M3] C.G. Moreira, *Frações contínuas, representações de números e aproximações*, Eureka **3** (1998), 44–55.

[Mar1] A. Markoff, *A new sequence of minima in the geometry of numbers,* Math. Ann. **15** (1879), 381–406.

[Mar2] A. Markov, *Sur les formes quadratiques binaires indéfinies*, Math. Ann. **15** (1879), 381–406.

[MN] C.G. Moreira e Nicolau Saldanha, *Primos de Mersenne (e outros primos muito grandes)*, 22.o Colóquio Brasileiro de Matemática

[MY] C. G. Moreira and J.-C. Yoccoz, *Stable intersections of regular Cantor sets with large Hausdorff dimensions*, Annals of Math., 154 (2001), 45-96.

[StSa] E. M. Stein, e R. Shakarchi, *Fourier analysis, an introduction*, Princeton University Press (2003).