# Introdução à Teoria dos Números

**(com ênfase em Aproximações Diofantinas)**


Carlos Gustavo T. de A. Moreira

I M P A

*Estrada Dona Castorina 110, Jardim Botânico*

*Rio de Janeiro-RJ*

CEP 22.460-320 - Brasil

Correio eletrônico: gugu@impa.br

Página na internet: www.impa.br/∼ gugu

# Conteúdo

## PARTE II: APROXIMAÇÕES DIOFANTINAS

# Introdução

Estas são as notas de um mini-curso que fui convidado a dar no IMCA em novembro de 2001. Boa parte do material aqui contido foi adaptado das notas dos cursos "Primos de Mersenne (e outros primos muito grandes)", em colaboração com Nicolau Saldanha e "Conjuntos de Cantor, Dinâmica e Aritmética", que dei no XXII Colóquio Brasileiro de Matemática, em 1999, e do artigo "Propriedades Estatísticas de Frações Contínuas e Aproximações Diofantinas", publicado na Revista Matemática Universitária.

O objetivo dessas notas é ser uma referência introdutória sobre teoria dos números e aproximações diofantinas, destinada a alunos de graduação ou mestrado em matemática. Boa parte do material é totalmente elementar, sendo acessível a bons alunos do ensino médio (em particular aos olímpicos...). Agradeço aos Professores Cesar Camacho e Roger Metzger pelo convite e a oportunidade de visitar o Peru e dar aulas sobre esse assunto tão fascinante.

Rio de Janeiro, 26 de outubro de 2001.

# PARTE I

# CONGRUÊNCIAS E NÚMEROS PRIMOS

# CAPÍTULO 1

## Divisibilidade e Congruências

Neste primeiro capítulo veremos os tópicos básicos de teoria dos números, como divisibilidade, congruências e aritmética módulo $n$.

## 1 Divisão euclidiana e o teorema fundamental da aritmética

A divisão euclidiana, ou divisão com resto, é uma das quatro operações que toda criança aprende na escola. Sua formulação precisa é: dados $a \in \mathbb{Z}$, $b \in \mathbb{Z}^*$ existem $q, r \in \mathbb{Z}$ com $0 \le r < |b|$ e $a = bq + r$. Tais $q$ e $r$ estão unicamente determinados e são chamados o *quociente* e *resto* da divisão de $a$ por $b$. Se $b > 0$ podemos definir $q = \lfloor a/b \rfloor$ e se $b < 0$, $q = \lceil a/b \rceil$; em qualquer caso, $r = a - bq$. O resto $r$ é às vezes denotado por $a \bmod b$; definimos $a \bmod 0 = a$. Lembramos que $\lfloor x \rfloor$ denota o único inteiro $k$ tal que $k \le x < k+1$ e $\lceil x \rceil$ o único inteiro $k$ tal que $k - 1 < x \le k$.

Dados dois inteiros $a$ e $b$ (em geral com $b \neq 0$) dizemos que $b$ *divide* $a$, ou que $a$ é um *múltiplo* de $b$, e escrevemos $b|a$, se existir $q \in \mathbb{Z}$ com $a = qb$. Se $a \neq 0$, também dizemos que $b$ é um *divisor* de $a$. Assim, $b|a$ se e somente se $a \bmod b = 0$.

**Proposição 1.1:** Dados $a, b \in \mathbb{Z}$ existe um único $d \in \mathbb{N}$ tal que $d|a$, $d|b$ e, para todo $c \in \mathbb{N}$, se $c|a$ e $c|b$ então $c|d$. Além disso existem $x, y \in \mathbb{Z}$ com $d = ax + by$.

Esse natural $d$ é chamado o *máximo divisor comum*, ou mdc, entre $a$ e $b$. Escrevemos $d = \mathrm{mdc}(a, b)$ ou (se não houver possibilidade de confusão) $d = (a, b)$.

**Dem:** O caso $a = b = 0$ é trivial (temos $d = 0$). Nos outros casos, seja $I(a, b) = \{ax + by; x, y \in \mathbb{Z}\}$ e seja $d = ax_0 + by_0$ o menor elemento positivo de $I(a, b)$. Como $d \in \mathbb{N}^*$, existem $q, r \in \mathbb{Z}$ com $a = dq + r$ e $0 \le r < d$. Temos $r = a - dq = a(1 - qx_0) + b(-qy_0) \in I(a, b)$; como $r < d$ e

$d$ é o menor elemento positivo de $I(a, b)$, $r = 0$ e $d|a$. Analogamente, $d|b$. Suponha agora que $c|a$ e $c|b$; temos $c|ax + by$ para quaisquer valores de $x$ e $y$ donde, em particular, $c|d$. ■

O *algoritmo de Euclides* para calcular o mdc baseia-se nas seguintes observações simples. Se $a = bq + r$, $0 \leq r < b$, temos (com a notação da demonstração acima) $I(a, b) = I(b, r)$, donde $(a, b) = (b, r)$. Definindo $a_0 = a$, $a_1 = b$ e $a_n = a_{n+1}q_{n+2} + a_{n+2}$, $0 \leq a_{n+2} < a_{n+1}$ (ou seja, $a_{n+2}$ é o resto da divisão de $a_n$ por $a_{n+1}$) temos $(a, b) = (a_0, a_1) = (a_1, a_2) = (a_2, a_3) = \cdots = (a_n, a_{n+1})$ para qualquer valor de $n$. Seja $N$ o menor natural para o qual $a_{N+1} = 0$: temos $(a, b) = (a_N, 0) = a_N$.

**Lema 1.2:** *Se $(a, b) = 1$ e $a|bc$ então $a|c$.*

**Dem:** Como $(a, b) = 1$, existem $x, y \in \mathbb{Z}$ com $ax + by = 1$, logo $a|c = acx + bcy$. ■

Quando $(a, b) = 1$ dizemos que $a$ e $b$ são *primos entre si*. Um natural $p > 1$ é chamado *primo* se os únicos divisores positivos de $p$ são 1 e $p$. Um natural $n > 1$ é chamado *composto* se admite outros divisores além de 1 e $n$.

Claramente, se $p$ é primo e $p \nmid a$ temos $(p, a) = 1$. Usando o lema anterior e indução temos o seguinte resultado:

**Corolário 1.3:** *Sejam $p$ um número primo e sejam $a_1, \ldots a_m \in \mathbb{Z}$. Se $p|a_1 \cdots a_m$ então $p|a_i$ para algum $i$, $1 \leq i \leq n$.*

Estamos agora prontos para enunciar e provar o teorema que diz que todo inteiro admite fatoração única como produto de primos.

**Teorema 1.4:** (Teorema fundamental da aritmética) Seja $n \geq 2$ um número natural. Podemos escrever $n$ de uma única forma como um produto

$$n = p_1 \cdots p_m$$

onde $m \geq 1$ é um natural e $p_1 \leq \ldots \leq p_m$ são primos.

**Dem:** Mostramos a existencia da fatoração por indução. Se $n$ é primo não há o que provar (escrevemos $m = 1$, $p_1 = n$). Se $n$ é composto podemos escrever $n = ab$, $a, b \in \mathbb{N}$, $1 < a < n$,

$1 < b < n$. Por hipótese de indução, $a$ e $b$ se decompõem como produto de primos. Juntando as fatorações de $a$ e $b$ (e reordenando os fatores) obtemos uma fatoração de $n$.

Vamos agora mostrar a unicidade, também por indução. Suponha que

$$n = p_1 \cdots p_m = q_1 \cdots q_{m'},$$

com $p_1 \leq \ldots \leq p_m$, $q_1 \leq \ldots \leq q_{m'}$. Como $p_1 | q_1 \cdots q_{m'}$ temos $p_1 | q_i$ para algum valor de $i$, donde, como $q_i$ é primo, $p_1 = q_i$ e $p_1 \geq q_1$. Analogamente temos $q_1 \leq p_1$, donde $p_1 = q_1$. Mas por hipótese de indução

$$n/p_1 = p_2 \cdots p_m = q_2 \cdots q_{m'}$$

admite uma única fatoração, donde $m = m'$ e $p_i = q_i$ para todo $i$. ■

Outra forma de escrever a fatoração é

$$n = p_1^{e_1} \cdots p_m^{e_m},$$

com $p_1 < \cdots < p_m$, $e_i > 0$. Ainda outra formulação é escrever

$$n = 2^{e_2} 3^{e_3} 5^{e_5} \cdots p^{e_p} \cdots$$

onde o produto é tomado sobre *todos* os primos mas apenas um número finito de expoentes é maior do que zero.

Segue deste teorema o outro algoritmo comum para calcular o mdc de dois números: fatoramos os dois números e tomamos os fatores comuns com os menores expoentes. Este algoritmo é bem menos eficiente do que o de Euclides para inteiros grandes (que em geral não sabemos fatorar) mas é instrutivo saber que os dois algoritmos dão o mesmo resultado.

**Corolário 1.5:** *Se* $(a, n) = (b, n) = 1$ *então* $(ab, n) = 1$.

**Dem:** Evidente a partir do algoritmo descrito acima. ■

**Teorema 1.6:** (Euclides) *Existem infinitos números primos.*

**Dem:** Suponha por absurdo que $p_1, p_2, ..., p_m$ fossem *todos* os primos. O número $N = p_1 \cdot p_2 \cdots p_m + 1 > 1$ não seria divisível por nenhum primo, o que contradiz o teorema fundamental da aritmética. ■

Observe que *não* provamos que $p_1 \cdot p_2 \cdots p_m + 1$ é primo para algum conjunto finito de primos (por exemplo, os $m$ primeiros primos). Aliás, $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \cdot 509$, $2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209 = 11 \cdot 19$, $4! + 1 = 25 = 5^2$ e $8! - 1 = 40319 = 23 \cdot 1753$ não são primos. Não existe nenhuma fórmula simples conhecida que gere sempre números primos. Veja a seção 3.1.

# 2 Congruências

Sejam $a, b, n \in \mathbb{Z}$. Dizemos que *$a$ é congruente a $b$ módulo $n$*, e escrevemos $a \equiv b \pmod{n}$, se $n | b - a$. Como a congruência módulo 0 é a igualdade e quaisquer inteiros são côngruos módulo 1, em geral estamos interessados em $n > 1$.

**Proposição 2.1:** *Para quaisquer $a, a', b, b', c, n \in \mathbb{Z}$ temos:*

(a)

*1.* $a \equiv a \pmod{n}$*;*

*2. se* $a \equiv b \pmod{n}$ *então* $b \equiv a \pmod{n}$*;*

*3. se* $a \equiv b \pmod{n}$ e $b \equiv c \pmod{n}$ *então* $a \equiv c \pmod{n}$*;*

*4. se* $a \equiv a' \pmod{n}$ *e* $b \equiv b' \pmod{n}$ *então* $a + b \equiv a' + b' \pmod{n}$*;*

*5. se* $a \equiv a' \pmod{n}$ *então* $-a \equiv -a' \pmod{n}$*;*

*6. se* $a \equiv a' \pmod{n}$ *e* $b \equiv b' \pmod{n}$ *então* $a \cdot b \equiv a' \cdot b' \pmod{n}$.

**Dem:** Para o item (a) basta observar que $n | a - a = 0$. Em (b), se $n | b - a$ então $n | a - b = -(b - a)$. Em (c), se $n | b - a$ e $n | c - b$ então $n | c - a = (c - b) + (b - a)$. Em (d), se $n | a' - a$ e $n | b' - b$ então $n | (a' + b') - (a + b) = (a' - a) + (b' - b)$. Em (e), se $n | a' - a$ então $n | (-a') - (-a) = -(a' - a)$. Em (f), se $n | a' - a$ e $n | b' - b$ então $n | a'b' - ab = a'(b' - b) + b(a' - a)$. ∎

Os itens (a), (b) e (c) da proposição acima dizem, nesta ordem, que a relação $\equiv \pmod{n}$ ("ser côngruo módulo $n$") é uma relação reflexiva, simétrica e transitiva. Relações satisfazendo estas três propriedades são chamadas *relações de equivalência*. Dada uma relação de equivalência $\sim$ sobre um conjunto $X$ e um elemento $x \in X$ definimos a *classe de equivalência* $\overline{x}$ de $x$ como

$$\overline{x} = \{y \in X | y \sim x\};$$

observe que $x \sim y$ se e somente se $\overline{x} = \overline{y}$. As classes de equivalência formam uma partição de $X$, i.e., uma coleção de subconjuntos não vazios e disjuntos de $X$ cuja união é $X$. O conjunto $\{\overline{x} | x \in X\}$ das classes de equivalência é chamado o *quociente* de $X$ pela relação de equivalência $\sim$ e é denotado por $X/\sim$.

Aplicando esta construção geral ao nosso caso, definimos o quociente $\mathbb{Z}/(\equiv \pmod{n})$, chamado por simplicidade de notação de $\mathbb{Z}/(n)$, $\mathbb{Z}/n\mathbb{Z}$ ou às vezes $\mathbb{Z}_n$. Dado $a \in \mathbb{Z}$, a definição de $\overline{a}$ como um subconjunto de $\mathbb{Z}$ raramente será importante: o importante é sabermos que $\overline{a} = \overline{a'}$ se e somente se $a \equiv a' \pmod{n}$. Se $n > 0$, a divisão euclidiana diz que todo inteiro $a$ é côngruo a um único inteiro $a'$ com $0 \leq a' < n$; podemos reescrever este fato na nosso nova linguagem como

$$\mathbb{Z}/(n) = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}.$$

Quando não houver possibilidade de confusão omitiremos as barras e chamaremos os elementos de $\mathbb{Z}/(n)$ simplesmente de $0, 1, \ldots, n-1$.

Os itens (d), (e) e (f) da proposição dizem que as operações de soma, diferença e produto são compatíveis com a relação de congruência. É esta propriedade que torna congruências tão úteis, nos possibilitando fazer contas módulo $n$. Podemos por exemplo escrever

$$\begin{aligned}
196883 &= 1 \cdot 10^5 + 9 \cdot 10^4 + 6 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10^1 + 3 \cdot 10^0 \\
&\equiv 1 \cdot 1^5 + 9 \cdot 1^4 + 6 \cdot 1^3 + 8 \cdot 1^2 + 8 \cdot 1^1 + 3 \cdot 1^0 \\
&= 1 + 9 + 6 + 8 + 8 + 3 \\
&= 35 \\
&\equiv 8 \pmod{9},
\end{aligned}$$

já que $10 \equiv 1 \pmod 9$ (mostrando assim porque funciona o conhecido critério de divisibilidade por 9). Uma formulação mais abstrata da mesma idéia é dizer que as operações $+$ e $\cdot$ *passam ao quociente*, i.e., que podemos definir

$$+ : \mathbb{Z}/(n) \times \mathbb{Z}/(n) \to \mathbb{Z}/(n), \qquad \cdot : \mathbb{Z}/(n) \times \mathbb{Z}/(n) \to \mathbb{Z}/(n)$$

por $\overline{a} + \overline{b} = \overline{a+b}$ e $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$. A dúvida à primeira vista seria se a escolha de $a$ e $b$ não afeta a resposta: afinal existem infinitos inteiros $a'$ e $b'$ com $\overline{a} = \overline{a'}$ e $\overline{b} = \overline{b'}$. Os itens (d) e (f) da proposição são exatamente o que precisamos: eles nos dizem que nestas condições $\overline{a+b} = \overline{a'+b'}$ e $\overline{a \cdot b} = \overline{a' \cdot b'}$.

**Proposição 2.2:** *Sejam $a, n \in \mathbb{Z}$, $n > 0$. Então existe $b \in \mathbb{Z}$ com $ab \equiv 1 \pmod n$ se e somente se $(a, n) = 1$.*

**Dem:** Se $ab \equiv 1 \pmod n$ temos $nk = 1 - ab$ para algum $k$, donde $(a, n) | ab + nk = 1$ e $(a, n) = 1$. Se $(a, n) = 1$ temos $ax + ny = 1$ para certos inteiros $x$ e $y$, donde $ax \equiv 1 \pmod n$. ∎

Dizemos portanto que $a$ é *invertível* [1] módulo $n$ quando $(a, n) = 1$ e chamamos $b$ com $ab \equiv 1 \pmod n$ de *inverso* de $a$ módulo $n$. O inverso é sempre único módulo $n$: se $ab \equiv ab' \equiv 1 \pmod n$ temos $b \equiv ab^2 \equiv abb' \equiv b' \pmod n$.

**Corolário 2.3:** *Se $(a, n) = 1$ e $ab \equiv ab' \pmod n$ então $b \equiv b' \pmod n$.*

**Dem:** Basta escrever $b \equiv abc \equiv ab'c \equiv b' \pmod n$ onde $c$ é o inverso de $a$ módulo $n$. ∎

Definimos $(\mathbb{Z}/(n))^* \subset \mathbb{Z}/(n)$ por

$$(\mathbb{Z}/(n))^* = \{\overline{a}; (a, n) = 1\}.$$

Observe que o produto de elementos de $(\mathbb{Z}/(n))^*$ é sempre um elemento de $(\mathbb{Z}/(n))^*$ (corolário 1.5).

[1] Alguns autores preferem escrever *inversível*. Os interessados em discutir esta questão ortográfica devem escrever para o Prof. Zoroastro Azambuja, IMPA, Estr. D. Castorina 110, Rio de Janeiro, RJ

**Teorema 2.4:** (Teorema Chinês dos restos) *Se* $(m, n) = 1$ *então*

$$f : \mathbb{Z}/(mn) \to \mathbb{Z}/(m) \times \mathbb{Z}/(n)$$
$$\overline{a} \mapsto (\overline{a}, \overline{a})$$

*é uma bijeção. Além disso, a imagem por* $f$ *de* $(\mathbb{Z}/(mn))^*$ *é* $(\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*$.

Note que cada $\overline{a}$ na definição de $f$ é tomado em relação a um módulo diferente. A função está bem definida pois $a \bmod mn$ determina $a \bmod m$ e $a \bmod n$.

**Dem:** Como $\mathbb{Z}/(mn)$ e $\mathbb{Z}/(m) \times \mathbb{Z}/(n)$ têm $mn$ elementos cada, para provar que $f$ é bijetiva basta verificar que $f$ é injetiva. E, de fato, se $a \equiv a' \pmod{m}$ e $a \equiv a' \pmod{n}$ então $m|(a - a')$ e $n|(a - a')$, donde $mn|(a - a')$ e $a \equiv a' \pmod{mn}$. A imagem de $(\mathbb{Z}/(mn))^*$ é $(\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*$ pois $(a, mn) = 1$ se e somente se $(a, m) = (a, n) = 1$. ■

Dados inteiros $m_1, m_2, \ldots, m_r$, dizemos que estes inteiros são *primos entre si* se $(m_i, m_j) = 1$ para quaiquer $i \neq j$.

**Corolário 2.5:** *Se* $m_1, m_2, \ldots, m_r$ *são inteiros primos entre si. Então*

$$f : \mathbb{Z}/(m_1 m_2 \cdots m_r) \to \mathbb{Z}/(m_1) \times \mathbb{Z}/(m_2) \cdots \mathbb{Z}/(m_r)$$
$$\overline{a} \mapsto (\overline{a}, \overline{a}, \ldots, \overline{a})$$

*é uma bijeção.*

**Dem:** Basta aplicar o teorema anterior $r$ vezes. ■

A aplicação mais comum deste teorema é para garantir que existe $a$ com $a \equiv a_i \pmod{m_i}$ onde $a_i$ são inteiros dados quaisquer.

**Problema resolvido:** Prove que dado $n \in \mathbb{N}$ existe um conjunto de $n$ elementos $A \subset \mathbb{N}$ tal que para todo $B \subset A$, $B \neq \varnothing$, $\sum_{x \in B} x$ é uma potência não trivial (isto é, um número da forma $m^k$, onde $m, k$ são inteiros maiores ou iguais a 2), ou seja, $A = \{x_1, x_2, \ldots x_n\}$ tal que $x_1, x_2, \ldots x_n, x_1 + x_2, x_1 + x_3, \ldots, x_{n-1} + x_n, \ldots, x_1 + x_2 + \ldots x_n$ são todos potências não triviais.

**Solução:** $A = \{4\}$ é solução para $n = 1$, $A = \{9, 16\}$ é solução para $n = 2$. Vamos provar a existência de um tal conjunto por indução em $n$. Suponha que $A = \{x_1, \ldots, x_n\}$ é um conjunto com $n$ elementos e para todo $B \subset A$, $B \neq \varnothing$, $\sum\limits_{x \in B} x = m_B^{k_B}$. Vamos mostrar que existe $c \in \mathbb{N}$ tal que o conjunto $\tilde{A} = \{cx_1, cx_2, \ldots, cx_n, c\}$ satisfaz o enunciado.

Seja $\ell = \text{mmc}\{k_b, B \subset A,\ B \neq \varnothing\}$ o mínimo múltiplo comum de todos os exponentes $k_B$.

Para cada $B \subset A$, $B \neq \varnothing$ associamos um número primo $p_B > \ell$, de forma que $B_1 \neq B_2 \Rightarrow p_{B_1} \neq p_{B_2}$, e associamos um natural $r$ com $r_B \equiv 0$ (módulo $p_x$), $\forall\, X \neq B$, $\ell r_B + 1 \equiv 0$ (módulo $p_B$) (tal $r_B$ existe pelo teorema chinês dos restos), e tomamos

$$c = \prod_{\substack{B \subset A \\ B \neq \varnothing}} (1 + m_B^{k_B})^{\ell r_B}.$$

Como $c$ é uma potência $\ell$-ésima, $c$ é uma potência $k_B$-ésima para todo $B \subset A$, $B \neq \varnothing$, portanto, para $B' \subset \{cx_1, cx_2, \ldots, cx_n\}$, $B' \neq \varnothing$, teremos $B' = \{cx \mid x \in B\}$ para algum $B \subset A$, $B \neq \varnothing$. Logo $\sum\limits_{x \in B'} x$ será uma potência $k_B$-ésima.

Além disso,

$$\sum_{X \in B' U \{c\}} x = c(1 + m_B^{K_B}) = \left[ \prod_{\substack{X \subset A \\ X \neq \varnothing, B}} (1 + m_X^{K_X})^{\ell r_X} \right] \cdot (1 + m_B^{K_B})^{\ell r_B + 1},$$

que é uma potência $p_B$-ésima, pois $r_X$ é múltiplo de $p_B$ para $X \neq B$ e $\ell r_B + 1$ é múltiplo de $p_B$. ■

# 3 A função de Euler e o pequeno teorema de Fermat

Definimos $\varphi(n) = |(\mathbb{Z}/(n))^*|$ (onde $|X|$ denota o número de elementos de $X$). A função $\varphi$ é conhecida como a *função de Euler*. Temos $\varphi(1) = \varphi(2) = 1$, e, para $n > 2$, $1 < \varphi(n) < n$. Se $p$ é primo, $\varphi(p) = p - 1$; mais geralmente $\varphi(p^k) = p^k - p^{k-1}$ pois $(a, p^k) = 1$ se e somente se $a$ não é múltiplo de $p$ e há $p^{k-1}$ múltiplos de $p$ no intervalo $0 \leq a < p^k$.

Dizemos que os $n$ números inteiros $a_1, a_2, \ldots, a_n$ formam um *sistema completo de resíduos* (ou s.c.r.) módulo $n$ se $\{\overline{a_1}, \overline{a_2}, \ldots \overline{a_n}\} = \mathbb{Z}/(n)$, isto é, se os $a_i$ representam todas as classes de congruência módulo $n$. Por exemplo, 0, 1, 2, $\ldots$ $n-1$ formam um s.c.r. módulo $n$. Equivalentemente, podemos dizer que $a_1, a_2, \ldots, a_n$ formam um s.c.r. módulo $n$ se e somente se $a_i \equiv a_j \pmod n$ implicar $i = j$. Os $\varphi(n)$ números inteiros $b_1, b_2, \ldots, b_{\varphi(n)}$ formam um *sistema completo de invertíveis* (s.c.i.) módulo $n$ se

$$\{\overline{b_1}, \overline{b_2}, \ldots \overline{b_{\varphi(n)}}\} = (\mathbb{Z}/(n))^*,$$

isto é, se os $b_i$ representam todas as classes de congruências invertíveis módulo $n$. Também equivalentemente, $b_1, b_2, \ldots, b_{\varphi(n)}$ formam um s.c.i. módulo $n$ se e somente se $(b_i, n) = 1$ para todo $i$ e $a_i \equiv a_j \pmod n$ implicar $i = j$.

**Proposição 3.1:** *Sejam $q, r, n \in \mathbb{Z}$, $n > 0$, $q$ invertível módulo $n$, $a_1, a_2, \ldots, a_n$ um s.c.r. módulo $n$ e $b_1, b_2, \ldots, b_{\varphi(n)}$ um s.c.i. módulo $n$. Então $qa_1 + r, qa_2 + r, \ldots, qa_n + r$ formam um s.c.r. módulo $n$ e $qb_1, qb_2, ...qb_{\varphi(n)}$ formam um s.c.i. módulo n.*

**Dem:** Se $qa_i + r \equiv qa_j + r \pmod n$ então $n | q(a_i - a_j)$ e $a_i \equiv a_j \pmod n$, donde $i = j$; com isto provamos que $qa_1 + r, qa_2 + r, \ldots, qa_n + r$ formam um s.c.r..

Como $(q, n) = (b_i, n) = 1$, temos $(qb_i, n) = 1$. Por outro lado, se $qb_i \equiv qb_j \pmod n$ temos $b_i \equiv b_j \pmod n$ (como no parágrafo anterior) e $i = j$. Isto conclui a demonstração. ∎

**Teorema 3.2:** (Euler) *Sejam $a, n \in \mathbb{Z}$, $n > 0$, tais que $(a, n) = 1$. Então $a^{\varphi(n)} \equiv 1 \pmod n$.*

**Dem:** Seja

$$b_1, b_2, \ldots .b_{\varphi(n)}$$

um s.c.i. módulo $n$. Pela proposição anterior,

$$ab_1, ab_2, \ldots ab_{\varphi(n)}$$

também formam um s.c.i. módulo $n$. Assim,

$$b_1 \cdot b_2 \cdots b_{\varphi(n)} \equiv ab_1 \cdot ab_2 \cdots ab_{\varphi(n)} \pmod n$$

pois módulo $n$ os dois lados têm os mesmos fatores a menos de permutação. Mas isto pode ser reescrito como

$$a^{\varphi(n)}(b_1 \cdot b_2 \cdots b_{\varphi(n)}) \equiv 1 \cdot (b_1 \cdot b_2 \cdots b_{\varphi(n)}) \pmod n$$

e pelo corolário 1.9 isto implica $a^{\varphi(n)} \equiv 1 \pmod n$. ∎

**Corolário 3.3:** (Pequeno Teorema de Fermat) *Se $p$ é primo então, para todo inteiro $a$, $a^p \equiv a \pmod{p}$.*

**Dem:** Se $p|a$, então $a^p \equiv a \equiv 0 \pmod{p}$. Caso contrário, $\varphi(p) = p-1$, $a^{p-1} \equiv 1 \pmod{p}$ e novamente $a^p \equiv a \pmod{p}$. ∎

Outra demonstração do pequeno teorema de Fermat é por indução em $a$ usando o binômio de Newton e algumas propriedades de números binomiais. Se $0 < i < p$ temos

$$\binom{p}{i} = \frac{p!}{i!(p-i)!} \equiv 0 \pmod{p}$$

pois há um fator $p$ no numerador que não pode ser cancelado com nada que apareça no denominador. Os casos $a = 0$ e $a = 1$ do teorema são triviais. Supondo válido o teorema para $a$, temos

$$\begin{aligned}(a+1)^p &= a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + 1\\ &\equiv a^p + 1\\ &\equiv a + 1 \pmod{p}\end{aligned}$$

e a indução está completa.

**Corolário 3.4:** *Se $(m,n) = 1$ então $\varphi(mn) = \varphi(m)\varphi(n)$.*

**Dem:** Construimos uma bijeção entre $(\mathbb{Z}/(mn))^*$ e $(\mathbb{Z}/(m))^* \times (\mathbb{Z}/(n))^*$, o que garante que estes conjuntos têm o mesmo número de elementos. ∎

**Corolário 3.5:** *Se*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m}$$

*com $p_1 < p_2 < \ldots < p_m$ e $e_i > 0$ para todo $i$ então*

$$\begin{aligned}\varphi(n) &= (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \cdots (p_m^{e_m} - p_m^{e_m-1})\\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_m}\right).\end{aligned}$$

**Dem:** Isto segue da fórmula que já vimos para $\varphi(p^e)$ e do corolário anterior. ∎

Em particular, se $n > 2$ então $\varphi(n)$ é par.

**Problema resolvido:** Exiba $n \in \mathbb{N}$ tal que $2^n$ tenha mais de duas mil casas decimais e tenha entre suas 2000 últimas casas decimais 1000 zeros consecutivos.

**Solução:** $2^{\varphi(5^{2000})} \equiv 1$ (módulo $5^{2000}$), pelo Teorema de Euler. Portanto, existe $b \in \mathbb{N}$ com $2^{\varphi(5^{2000})} = 5^{2000}b + 1$, e teremos $2^{2000+\varphi(5^{2000})} = 10^{2000}b + 2^{2000}$, e portanto os 2000 últimos dígitos de $2^{2000+\varphi(5^{2000})}$ coincidem com a representação decimal de $2^{2000}$, que tem no máximo 667 dígitos, pois $2^3 < 10 \Rightarrow 2^{2000} < 2^{3.667} < 10^{667}$. Desta forma, $2^{2000+\varphi(5^{2000})}$ tem pelo menos $2000 - 667 = 1333$ zeros consecutivos dentre as 2000 últimas casas decimais, de modo que $n = 4.5^{1999} + 2000$ satisfaz as condições do enunciado (pois $\varphi(5^{2000}) = 4.5^{1999}$). ■

Mais adiante estudaremos equações do segundo grau em $\mathbb{Z}/(p)$; vejamos desde já um pequeno resultado deste tipo que garante que os únicos $a$ que são seus próprios inversos módulo $p$ são 1 e $-1$.

**Lema 3.6:** *Se $p$ é primo então as únicas soluções de $x^2 = 1$ em $\mathbb{Z}/(p)$ são 1 e $-1$. Em particular,se $x \in (\mathbb{Z}/(p))^* - \{1, -1\}$ então $x^{-1} \neq x$ em $\mathbb{Z}/(p)$.*

**Dem:** Podemos reescrever a equação como $(x-1)(x+1) = 0$, o que torna o resultado trivial. ■

**Teorema 3.7:** (Wilson) *Seja $n > 4$. Então $(n-1)! \equiv -1 \pmod{n}$ se $n$ é primo e $(n-1)! \equiv 0 \pmod{n}$ se $n$ é composto.*

**Dem:** Se $n$ é composto mas não é o quadrado de um primo podemos escrever $n = ab$ com $1 < a < b < n$: neste caso tanto $a$ quanto $b$ aparecem em $(n-1)!$ e $(n-1)! \equiv 0 \pmod{n}$. Se $n = p^2$, $p > 2$, então $p$ e $2p$ aparecem em $(n-1)!$ e novamente $(n-1)! \equiv 0 \pmod{n}$; isto demonstra que para todo $n$ composto, $n > 4$, temos $(n-1)! \equiv 0 \pmod{n}$.

Se $n$ é primo podemos escrever $(n-1)! \equiv -(2 \cdot 3 \cdots n-2) \pmod{n}$; mas pelo lema anterior podemos juntar os inversos aos pares no produto do lado direito, donde $(n-1)! \equiv -1 \pmod{n}$. ■

# 4 A função de Möbius

Vejamos inicialmente uma propriedade da função $\varphi$.

**Teorema 4.1:** *Para todo natural $n$,*

$$\sum_{d|n} \varphi(d) = n.$$

Este teorema segue facilmente da fórmula que provamos para $\varphi(n)$ na seção anterior. Daremos entretanto uma demonstração *bijetiva*.

**Dem:** Considere as $n$ frações

$$\frac{0}{n}, \frac{1}{n}, \ldots, \frac{n-1}{n}$$

e simplifique cada uma delas: obtemos assim, para cada $d|n$, $\varphi(d)$ frações com denominador $d$, donde segue a identidade do enunciado.

Mais formalmente, dado $\overline{a} \in \mathbb{Z}/(n)$, sejam $d = n/(n,a)$ e $a' = a/(n,a)$. Claramente $\overline{a'} \in (\mathbb{Z}/(d))^*$ e definimos assim uma função de $\mathbb{Z}/(n)$ para a união disjunta dos conjuntos $(\mathbb{Z}/(d))^*$, onde $d$ varia sobre os divisores de $n$. A inversa desta função leva $\overline{a'} \in (\mathbb{Z}/(d))^*$ em $\overline{a}$, $a = na'/d$, donde a função é uma bijeção. ∎

O processo de construir $g$ a partir de $f$ como

$$g(n) = \sum_{d|n} f(d)$$

é bastante comum em teoria dos números. Seria interessante poder inverter esta identidade para escrever $f$ a partir de $g$. O teorema anterior nos mostra que se fazemos $f = \varphi$ na equação acima temos $g(n) = n$; invertendo esta identidade teríamos uma fórmula para $\varphi$. O objetivo desta seção é mostrar como fazer este tipo de inversão.

Definimos a *função de Möbius* $\mu : \mathbb{N}^* \to \mathbb{Z}$ por

$$\mu(n) = \begin{cases} (-1)^m, & \text{se } n = p_1 p_2 \cdots p_m, \text{ com } p_1, p_2, \cdots, p_m \text{ primos distintos,} \\ 0, & \text{se } n \text{ tem algum fator primo repetido em sua fatoração.} \end{cases}$$

Assim, $\mu(1) = \mu(6) = \mu(10) = 1$, $\mu(2) = \mu(3) = \mu(5) = \mu(7) = -1$ e $\mu(4) = \mu(8) = \mu(9) = 0$.

**Lema 4.2:** *Para todo inteiro positivo $n$ temos*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \text{se } n = 1, \\ 0, & \text{se } n > 1. \end{cases}$$

**Dem:** O caso $n = 1$ é trivial. Se $n > 1$, seja $p$ um divisor primo de $n$ e seja $n = p^e n'$ com $p \nmid n'$. Temos

$$\begin{aligned} \sum_{d|n} \mu(d) &= \sum_{d|n, p\nmid d} \mu(d) + \sum_{d|n, p|d, p^2\nmid d} \mu(d) + \sum_{d|n, p^2|d} \mu(d) \\ &= \sum_{d|n'} \mu(d) + \sum_{d'|n'} \mu(pd') + 0 \\ &= \sum_{d|n'} \mu(d) - \sum_{d'|n'} \mu(d') \\ &= 0. \end{aligned}$$

■

**Teorema 4.3:** (Fórmula de inversão de Möbius) *Se para todo $n > 0$ temos*

$$g(n) = \sum_{d|n} f(d)$$

*então*

$$f(n) = \sum_{d|n} \mu(n/d) g(d).$$

Observe que a fórmula do corolário 1.16 para $\varphi(n)$ segue facilmente dos dois teoremas acima.

**Dem:** Basta provar que

$$f(n) = \sum_{d|n} \mu(n/d) \left( \sum_{d'|d} f(d') \right).$$

Mas, escrevendo $d'' = n/d$ e $m = n/d'$ temos

$$\sum_{d|n} \mu(n/d) \left( \sum_{d'|d} f(d') \right) = \sum_{m|n} \left( \sum_{d''|m} \mu(d'') \right) f(n/m) = f(n).$$

■

**Teorema 4.4:** (Segunda fórmula de inversão de Möbius) *Sejam $f$ e $g$ funções reais com domínio $(0,+\infty)$ tais que $f(t)=g(t)=0$ para todo $t<1$. Se*

$$g(x)=\sum_{k=1}^{\infty} f\left(\frac{x}{k}\right)=\sum_{1=k}^{\lfloor x\rfloor} f\left(\frac{x}{k}\right)$$

*para todo $x$ então então*

$$f(x)=\sum_{k=1}^{\infty}\mu(k)g\left(\frac{x}{k}\right)=\sum_{1=k}\lfloor x\rfloor\mu(k)g\left(\frac{x}{k}\right).$$

**Dem:** Basta provar que

$$f(x)=\sum_{k=1}^{\infty}\mu(k)\left(\sum_{r=1}^{\infty} f\left(\frac{x}{kr}\right)\right),$$

mas, tomando $m=kr$ a última soma é igual a

$$\sum_{m=1}^{\infty}\left(\left(\sum_{k|m}\mu(k)\right)f\left(\frac{x}{m}\right)\right)$$

que pelo lema é igual a $f(x)$. ■

Apesar de não estar relacionada com o resto da nossa discussão, não podemos deixar de mencionar a seguinte conjectura.

**Conjectura 4.5:** (Hipótese de Riemann) *Se $\alpha>1/2$ então*

$$\lim_{n\to\infty}\frac{1}{n^{\alpha}}\sum_{1\leq m}^{n}\mu(m)=0.$$

Esta é uma das formulações da famosa hipótese de Riemann, um dos problemas em aberto mais importantes da matemática.

Podemos reenunciar esta conjectura assim: seja $f:(0,+\infty)\to\mathbb{R}$ definida por $f(t)=0$ se $t<1$ e

$$\sum_{k=1}^{\infty} f(t/k)=1, \quad \text{se } t\geq 1$$

então, para todo $\alpha > 1/2$,

$$\lim_{t\to\infty} \frac{f(t)}{t^\alpha} = 0.$$

De fato, pela segunda fórmula de inversão de Möbius temos

$$f(t) = \sum_{m=1}^{\lfloor t \rfloor} \mu(m).$$

# 5 Bases

A notação usual para naturais é a chamada base 10, com algarismos $0, \ldots, 9$. Isto significa, por exemplo, que

$$196883 = 1 \cdot 10^5 + 9 \cdot 10^4 + 6 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10^1 + 3 \cdot 10^0.$$

O teorema abaixo mostra como escrever qualquer natural em qualquer base $d$.

**Teorema 5.1:** *Seja $n \geq 0$ e $d > 1$. Então existe uma única seqüência $a_0, \ldots, a_k, \ldots$ com as seguintes propriedades:*

(a)

1. *para todo $k$, $0 \leq a_k < d$,*

2. *existe $m$ tal que se $k \geq m$ então $a_k = 0$,*

3. *$n = \sum_k a_k d^k$.*

**Dem:** Escrevemos $n = n_0 = n_1 d + a_0$, $0 \leq a_0 < d$, $n_1 = n_2 d + a_1$, $0 \leq a_1 < d$, e em geral $n_k = n_{k+1} d + a_k$, $0 \leq a_k < d$. Nossa primeira afirmação é que $n_k = 0$ para algum valor de $k$. De fato, se $n_0 < d^m$ então $n_1 < d^{m-1}$ e mais geralmente, por indução, $n_k < d^{m-k}$; fazendo $k \geq m$ temos $n_k < 1$ donde $n_k = 0$. Segue daí que $a_k = 0$ para $k \geq m$. A identidade do item (c) é facilmente demonstrada por indução.

Para a unicidade, suponha $\sum_k a_k d^k = \sum_k b_k d^k$. Se as seqüências $a_k$ e $b_k$ são distintas existe um menor índice, digamos $j$, para o qual $a_j \neq b_j$. Podemos escrever $a_j + \sum_{k>j} a_k d^{k-j} = b_j + \sum_{k>j} b_k d^{k-j}$ donde $a_j \equiv b_j \pmod{d}$, o que é uma contradição. ■

Às vezes é interessante considerar expansões não apenas em outras bases mas com outros conjuntos de algarismos (veremos um exemplo disso no último capítulo). Por exemplo, podemos preferir algarismos negativos pequenos a algarismos positivos grandes e assim um bom conjunto de algarismos na base 10 seria

$$-4, -3, -2, -1, 0, 1, 2, 3, 4, 5.$$

Desta forma, escrevemos $13 = 1 \cdot 10 + 3$ mas escrevemos $9 = 1 \cdot 10 - 1$ e $64 = 1 \cdot 10^2 - 4 \cdot 10 + 4$. Generalizando, os algarismos na base $d$ seriam os inteiros $a$ com $-d/2 < a \leq d/2$, ou seja,

$$a = -\lfloor (d-1)/2 \rfloor, -\lfloor (d-1)/2 \rfloor + 1, \ldots, -1, 0, 1, \ldots, \lfloor d/2 \rfloor - 1, \lfloor d/2 \rfloor.$$

Este conjunto de algarismos nos permite enunciar um teorema análogo ao anterior, com a diferença que agora números negativos não precisam ser tratados em separado.

**Teorema 5.2:** *Seja $n \in \mathbb{Z}$ e $d > 2$. Então existe uma única seqüência $a_0, \ldots, a_k, \ldots$ com as seguintes propriedades:*

(a)

1. *para todo $k$, $-d/2 < a_k \leq d/2$,*
2. *existe $m$ tal que se $k \geq m$ então $a_k = 0$,*
3. *$n = \sum_k a_k d^k$.*

**Dem:** Escrevemos $n = n_0 = n_1 d + a_0$, $-d/2 < a_0 \leq d/2$, $n_1 = n_2 d + a_1$, $-d/2 < a_1 \leq d/2$, e em geral $n_k = n_{k+1} d + a_k$, $-d/2 < a_k \leq d/2$. Novamente, nossa primeira afirmação é que $n_k = 0$ para algum valor de $k$. De fato, se

$$-d^m/2 < n_0 \leq d^m/2$$

então, por indução,

$$-d^{m-k}/2 < n_k \leq d^{m-k}/2;$$

fazendo $k \geq m$ temos $n_k = 0$. Segue daí que $a_k = 0$ para $k \geq m$. A identidade do item (c) e a unicidade são demonstradas como no teorema anterior. ■

Pode-se estudar representações na base $d$ com outros conjuntos $X$ de algarismos. Algumas condições mínimas para que $X$ seja um conjunto de algarismos interessante são que $0 \in X$, que $X$ seja um sistema completo de resíduos e que o mdc dos elementos de $X$ seja 1.

# 6 Corpos e polinômios

Um *grupo* é um conjunto $G$ munido de uma operação $* : G \times G \to G$ e um elemento $e \in G$ com as seguintes propriedades:

1. para quaisquer $a, b, c \in G$, $a * (b * c) = (a * b) * c$.
2. para qualquer $a \in G$, $a * e = e * a = a$,
3. para qualquer $a \in G$ existe $b \in G$ com $a * b = b * a = e$.

Se além disso tivermos $a * b = b * a$ para quaisquer $a, b \in G$ dizemos que o grupo é *comutativo* ou *abeliano*. Quando a operação $*$ se chama $+$ dizemos que $G$ é um grupo aditivo e chamamos o elemento neutro $e$ de 0. Se a operação se chama $\cdot$ chamamos $G$ de grupo multiplicativo e denotamos o elemento neutro $e$ por 1. Assim, $\mathbb{Z}/(n)$ é um grupo abeliano aditivo e $(\mathbb{Z}/(n))^*$ é um grupo abeliano multiplicativo.

Um *anel comutativo com unidade* é um grupo abeliano aditivo $A$ munido de uma segunda operação $\cdot : A \times A \to A$ satisfazendo $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, $a \cdot b = b \cdot a$ para quaisquer $a, b, c \in A$ e um elemento $1 \in A$ com $1 \cdot a = a$ para todo $a \in A$. Assim, $\mathbb{Z}/(n)$ é um anel comutativo com unidade.

Um *corpo* é um anel comutativo com unidade onde para todo $a \in K$ com $a \neq 0$ existe $b \in K$ com $a \cdot b = 1$. Repetindo então, $K$ é munido de duas operações $+ : K \times K \to K$ e $\cdot : K \times K \to K$, de uma função $- : K \to K$ e dois elementos especiais distintos chamados 0 e 1 satisfazendo as seguintes propriedades:

$$a + (b + c) = (a + b) + c$$

$$a + 0 = a$$

$$a + (-a) = 0$$
$$a + b = b + a$$
$$a(b + c) = ab + ac$$
$$a(bc) = (ab)c$$
$$a1 = a$$
$$ab = ba$$

e onde para todo $a \in K$, $a \neq 0$ existe $b \in K$ com

$$ab = 1.$$

Os exemplos mais conhecidos de corpos são $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$. Vimos no capítulo anterior que $\mathbb{Z}/(p)$ também é um corpo se $p$ é primo; veremos a seguir outros exemplos de corpos finitos.

Dado um corpo $K$, definimos o anel comutativo com unidade $K[x]$ como sendo o conjunto das expressões da forma $P = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, chamados de *polinômios* com coeficientes em $K$. Observe que $x$ é um símbolo formal e não um elemento de $K$; apesar disso, cada polinômio define uma *função polinomial*

$$P : K \to K$$
$$c \mapsto P(c) = a_0 + a_1c + a_2c^2 + \cdots + a_nc^n$$

também chamada de $P$. A distinção entre um polinômio e uma função polinomial é bem ilustrada pelo polinômio $P = x^p - x \in (\mathbb{Z}/(p))[x]$: este polinômio é não nulo pois seus coeficientes são não nulos mas para todo $x \in \mathbb{Z}/(p)$ temos $P(x) = 0$ pelo pequeno teorema de Fermat.

Se $P = \sum a_ix^i$ e $Q = \sum b_ix^i$ são polinômios definimos $P + Q = \sum(a_i + b_i)x^i$ e $PQ = \sum c_ix^i$ onde $c_k = \sum_{i+j=k} a_ib_j$. Definimos o *grau* $\deg P$ de um polinômio $P = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ como sendo $n$ se $a_n \neq 0$ mas $a_m = 0$ para $m > n$; definimos ainda o grau do polinômio 0 como sendo $-\infty$.

**Lema 6.1:** *Para quaisquer polinômios $P$ e $Q$ temos* $\deg(PQ) = \deg(P) + \deg(Q)$ *e* $\deg(P + Q) \leq \max\{\deg(P), \deg(Q)\}$.

**Dem:** Fácil. ■

Observe que definimos $-\infty < n$ e $(-\infty) + (-\infty) = -\infty + n = -\infty$ para todo $n$. Temos uma forma de divisão com resto em $K[x]$.

**Teorema 6.2:** *Sejam $A, B \in K[x]$, $B \neq 0$. Então existem únicos polinômios $Q, R \in K[x]$ com $A = QB + R$ e $\deg R < \deg B$.*

**Dem:** A demonstração é feita por indução no grau de $A$. Se $\deg(A) < \deg(B)$, tomamos $Q = 0$, $R = A$. Caso contrário, sejam $n$ e $m$ os graus de $A$ e $B$ e sejam $a$ e $b$ os coeficientes de mais alto grau destes polinômios. Podemos escrever $A = (a/b)x^{n-m}B + A_1$, com $\deg(A_1) < \deg(A)$. Pela hipótese de indução, temos $A_1 = Q_1 B + R$, com $\deg(R) < \deg(B)$. Fazendo $Q = (a/b) + x^{n-m} + Q_1$ temos $A = QB + R$. A unicidade segue facilmente do lema anterior.

■

A demonstração acima nada mais é do que o algoritmo usual de divisão usual. Um polinômio $P$ tem *raiz* $a$ (i.e., $P(a) = 0$) se e somente se $(x - a)|P$. Mais geralmente, $P(a)$ é o resto da divisão de $P$ por $x - a$.

**Proposição 6.3:** *Um polinômio $P$ não nulo de grau $n$ tem no máximo $n$ raízes.*

**Dem:** A demonstração é feita por indução em $n = \deg(P)$; os casos $n = 0$ e $n = 1$ são triviais. Se $P$ tivesse $n + 1$ raízes distintas $a_1, \ldots, a_{n+1}$ então $P$ seria múltiplo de $(x - a_{n+1})$; $P/(x - a_{n+1})$ teria grau $n - 1$ e raízes $a_1, \ldots, a_n$, contradizendo a hipótese de indução. ■

A partir da divisão com resto podemos repetir muitas das construções feitas para $\mathbb{Z}$ no capítulo anterior; dizemos que $K[x]$ (assim como $\mathbb{Z}$) é um *domínio euclidiano*. Daremos um esboço desta teoria; estes resultados não serão necessários para acompanhar o resto do livro.

Definimos $A|B$ se existe $C$ com $AC = B$ e dizemos que um polinômio $P$ de grau maior que $n > 0$ é *irredutível* se seus divisores todos têm grau $0$ ou $n$ (assim generalizando o conceito de número primo). O conceito de mdc também se generaliza, como indicado na proposição abaixo.

**Proposição 6.4:** *Dados polinômios não nulos $A, B \in K[x]$ existe um único $D \in K[x]$ (a menos de multiplicação por constante) tal que $D|A$, $D|B$ e, para todo $C \in K[x]$, se $C|A$ e $C|B$ então $C|D$. Além disso existem $E, F \in \mathbb{Z}$ com $D = AE + BF$.*

**Dem:** Definimos $I(A,B) = \{AE + BF; E, F \in K[x]\}$ e tomamos $D$ de grau mínimo dentre os elementos não nulos de $I(A,B)$; o resto da demonstração é análoga à da proposição 1.1. ■

Polinômios irredutíveis são como números primos: um produto de polinômios só é múltiplo de um polinômio irredutível se um dos fatores o for.

**Proposição 6.5:** *Sejam $P$ um polinômio irredutível e sejam $A_1, \dots A_m \in K[x]$. Se $P | (A_1 \cdots A_m)$ então $P | A_i$ para algum $i$, $1 \leq i \leq n$.*

**Dem:** Análoga à do corolário 1.3. ■

Temos também um teorema de fatoração única.

**Teorema 6.6:** *Todo polinômio pode ser fatorado como um produto de polinômios irredutíveis; esta fatoração é única a menos da ordem dos fatores.*

**Dem:** Análoga à do teorema fundamental da aritmética, usando a proposição acima e fazendo indução no grau do polinômio. ■

Os exemplos mais evidentes de polinômios irredutíveis são os da forma $x - a$, $a \in K$. Quando estes são os *únicos* polinômios irredutíveis dizemos que o corpo é *algebricamente fechado*. Polinômios de grau 2 e 3 são irredutíveis se e somente se não têm raízes.

O pequeno teorema de Fermat também admite uma formulação em termos de polinômios.

**Teorema 6.7:** *Seja $p$ primo; em $(\mathbb{Z}/(p))[x]$ temos*

$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)).$$

**Dem:** Os dois polinômios dos dois lados da equação têm grau $p$ e o coeficiente de $x^p$ é 1 nos dois casos. Assim, a diferença tem grau menor do que $p$ mas se anula em $p$ pontos: 0, 1, ... $p-1$. Pelo corolário anterior, esta diferença deve ser o polinômio zero. ■

A partir do teorema acima temos uma nova prova do teorema de Wilson: $x^{p-1} - 1 = (x-1)(x-2)\cdots(x-(p-1))$ em $(\mathbb{Z}/(p))[x]$, mas o coeficiente independente é $-1$ do lado esquerdo e $(p-1)!$ do lado direito.

Podemos definir congruências em $K[x]$:

$$A \equiv B \pmod{P} \iff P|(B-A).$$

As propriedades básicas de congruências podem ser traduzidas para este novo contexto e podemos definir um quociente $K[x]/(P)$ da mesma forma como definimos $\mathbb{Z}/(n)$; demonstra-se que $K[x]/(P)$ é um corpo exatamente quando $P$ é irredutível.

Prometemos que veríamos outros exemplos de corpos finitos além de $\mathbb{Z}/(p)$: o parágrafo acima ensina que podemos construir tais corpos como $(\mathbb{Z}/(p))[x]/(P)$ onde $P \in (\mathbb{Z}/(p))[x]$ é irredutível. Por exemplo, o polinômio $x^2+x+1$ é irredutível em $(\mathbb{Z}/(2))[x]$ o que nos permite construir um corpo de 4 elementos: $0$, $1$, $x$ e $x+1$. As operações em $\mathbb{Z}/(2)$ e a relação $x^2 = x+1$ definem as operações neste corpo (denotamos $x+1$ por $x'$):

| + | 0 | 1 | x | x′ |
|---|---|---|---|---|
| 0 | 0 | 1 | x | x′ |
| 1 | 1 | 0 | x′ | x |
| x | x | x′ | 0 | 1 |
| x′ | x′ | x | 1 | 0 |

| * | 0 | 1 | x | x′ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | x | x′ |
| x | 0 | x | x′ | 1 |
| x′ | 0 | x′ | 1 | x |

De fato existem em $(\mathbb{Z}/(p))[x]$ polinômios irredutíveis de qualquer grau e todo corpo finito pode ser construido desta forma. Enunciaremos sem demonstração um teorema que classifica os corpos finitos.

**Teorema 6.8:** *Existe um corpo finito com $q$ elementos se e somente se $q$ é da forma $p^n$ para algum primo $p$ e algum inteiro positivo $n$. Além disso, dados dois corpos finitos $K_1$ e $K_2$ com o mesmo número de elementos existe uma única bijeção $f : K_1 \to K_2$ com $f(a+b) = f(a)+f(b)$ e $f(ab) = f(a)f(b)$ para quaisquer $a, b \in K_1$.*

Uma bijeção como a descrita acima é chamada de *isomorfismo* e dois corpos são ditos *isomorfos* se existe entre eles um isomorfismo; a idéia é que corpos isomorfos são iguais a menos dos nomes dos elementos. Veremos mais tarde outras formas mais concretas de construir corpos finitos.

# 7 Ordens e raízes primitivas

Dados $n, a \in \mathbb{Z}$ com $n > 0$ e $(a, n) = 1$, definimos a *ordem de a módulo* $n$, denotada por $\operatorname{ord}_n a$, como sendo o menor inteiro positivo $t$ com $a^t \equiv 1 \pmod{n}$. Analogamente, se $K$ for um corpo finito e $a \in K$, $a \neq 0$, definimos a *ordem de a em* $K$, denotada por $\operatorname{ord}_K a$, como sendo o menor inteiro positivo $t$ com $a^t = 1 \in K$; temos $\operatorname{ord}_p a = \operatorname{ord}_{\mathbb{Z}/(p)} a$.

Claramente $a^e \equiv a^{e'} \pmod{n}$ se e somente se $e \equiv e' \pmod{\operatorname{ord}_n a}$; pelo teorema de Euler, $\operatorname{ord}_n a | \varphi(n)$.

Dizemos que $a$ é uma *raiz primitiva módulo* $n$ se $\operatorname{ord}_n a = \varphi(n)$. Analogamente, dizemos que $a$ é uma *raiz primitiva em* $K$ se $\operatorname{ord}_K a = q - 1$, onde $q = |K|$ é o número de elementos de $K$. Por exemplo, 2 é raiz primitiva módulo 5 mas 2 não é raiz primitiva módulo 7 ($2^3 \equiv 1 \pmod{7}$). Também é fácil verificar que não existe raiz primitiva módulo 8 pois se $x$ é ímpar então $x^2 \equiv 1 \pmod{8}$. Podemos também dizer que $a$ é raiz primitiva se a função

$$\begin{aligned} \mathbb{Z}/(\varphi(n)) &\to (\mathbb{Z}/(n))^* \\ r &\mapsto a^r \end{aligned}$$

ou

$$\begin{aligned} \mathbb{Z}/(q-1) &\to K^* \\ r &\mapsto a^r \end{aligned}$$

é injetora. Como o domínio e contradomínio são conjuntos finitos com o mesmo número de elementos, a função é injetora se e somente se ela é sobrejetora. Podemos assim dizer que $a$ é uma raiz primitiva módulo $n$ se e somente se para todo $b \in (\mathbb{Z}/(n))^*$ (ou para todo $b \in K^*$) existe $r$ com $a^r = b$.

Um corolário desta caracterização de raízes primitivas é que se $a$ é raiz primitiva módulo $n$ e $m|n$ então $a$ é raiz primitiva módulo $m$. O objetivo da próxima seção é caracterizar os valores de $n$ para os quais existe uma raiz primitiva módulo $n$. Nesta seção mostraremos que todo corpo finito admite raiz primitiva; em particular existe raiz primitiva módulo $p$ para qualquer primo $p$.

Precisamos primeiro de uma versão do pequeno teorema de Fermat para corpos finitos:

**Teorema 7.1:** *Se $K$ é um corpo finito e $q = |K|$ então $a^q - a = 0$ para todo $a \in K$.*

**Dem:** Se $a = 0$ o teorema vale; vamos supor a partir de agora $a \neq 0$. Sejam $b_1, \ldots b_{q-1}$ os elementos não nulos de $K$. Os elementos $ab_1, \ldots ab_{q-1}$ são todos não nulos e distintos, logo são os *próprios* $b_1, \ldots b_{q-1}$, apenas permutados. Assim

$$\begin{aligned} b_1 \cdot b_2 \cdots b_{q-1} &= (ab_1)(ab_2) \cdots (ab_{q-1}) \\ &= a^{q-1}(b_1 \cdot b_2 \cdots b_{q-1}) \end{aligned}$$

e $a^{q-1} = 1$. ■

Segue deste teorema que $\operatorname{ord}_K a | q-1$, analogamente ao que já sabiamos para $\mathbb{Z}/(n)$. A partir do que vimos sobre polinômios temos também que

$$x^q - x = x(x - b_1) \cdots (x - b_{q-1})$$

em $K[x]$.

**Teorema 7.2:** *Se $K$ é um corpo finito então existe raiz primitiva em $K$.*

**Dem:** Seja $d$ um divisor de $q-1$: definimos $N(d)$ como o número de elementos de $K^*$ de ordem $d$. Claramente $\sum_{d|q-1} N(d) = q-1$.

Se $N(d) > 0$, seja $a_d$ um elemento de $K$ com $\operatorname{ord}_K a_d = d$: os elementos $1, a_d, a_d^2, \ldots a_d^{d-1}$ são raízes do polinômio $x^d - 1 = 0$. Como este polinômio tem no máximo $d$ raízes, estas são todas as raízes. Assim, os elementos de $K$ de ordem $d$ são precisamente $a_d^r$, $r \in (\mathbb{Z}/(d))^*$. Assim os únicos valores possíveis para $N(d)$ são 0 e $\varphi(d)$. Mas como $\sum_{d|q-1} N(d) = \sum_{d|q-1} \varphi(d) = q-1$, temos $N(d) = \varphi(d)$ para todo $d|q-1$. Em particular $N(q-1) > 0$ e existem raízes primitivas. ■

Apesar de existirem raízes primitivas módulo $p$ para todo primo $p$ não existe uma fórmula simples para obter uma raiz primitiva. Por outro lado, conjectura-se que todo inteiro que não é um quadrado é raiz primitiva para infinitos valores de $p$ (conjectura de Artin).

**Corolário 7.3:** *Dados $x \in K^*$ e um inteiro positivo $k$ existe $y \in K^*$ com $y^k = x$ se e somente se $x^{(q-1)/\operatorname{mdc}(k,q-1)} = 1$, onde $q = |K|$.*

**Dem:** Se $x = y^k$ então $x^{(q-1)/\operatorname{mdc}(k,q-1)} = (y^{q-1})^{k/\operatorname{mdc}(k,q-1)} = 1$ pois $y^{q-1} = 1$. Suponha agora que $x^{(q-1)/\operatorname{mdc}(k,q-1)} = 1$. Sejam $a$ uma raiz primitiva de $K$ e $r \in \mathbb{Z}$ com $x = a^r$. Temos $(a^r)^{(q-1)/\operatorname{mdc}(k,q-1)} = 1$ donde $\operatorname{mdc}(k, q-1) \mid r$ e portanto existem inteiros $u, v$ com $ku + (q-1)v = r$. Assim $x = a^r = a^{ku+(q-1)v} = (a^u)^k \cdot (a^{q-1})^v = y^k$ onde $y = a^u$. ∎

# 8 Raízes primitivas em $\mathbb{Z}/(n)$

Nesta seção caracterizaremos os inteiros $n$ para os quais existe raiz primitiva módulo $n$.

**Lema 8.1:** *Sejam $p$ um número primo e $a \in \mathbb{Z}$ uma raiz primitiva módulo $p$. Então $a$ ou $a' = a + p$ é raiz primitiva módulo $p^2$.*

**Dem:** Pelo binômio de Newton, $a'^p = (a+p)^p \equiv a^p \pmod{p^2}$. Sem perda de generalidade, podemos supor $a^p \not\equiv a \pmod{p^2}$ ou $a^{p-1} \not\equiv 1 \pmod{p^2}$, donde $\operatorname{ord}_{p^2} a \neq p-1$. Como $p - 1 = \operatorname{ord}_p a \mid \operatorname{ord}_{p^2} a \mid \varphi(p^2) = p(p-1)$ isto implica em $\operatorname{ord}_{p^2} a = p(p-1)$. ∎

**Lema 8.2:** *Se $p$ é um número primo ímpar e $a$ é raiz primitiva módulo $p^2$ então $a$ é raiz primitiva módulo $p^k$ para todo $k > 2$, $k \in \mathbb{Z}$.*

**Dem:** Temos $a^{p-1} \equiv 1 \pmod{p}$, mas $a^{p-1} \not\equiv 1 \pmod{p^2}$, donde $a^{p-1} = 1 + b_0 p$ com $b_0 \not\equiv 0 \pmod{p}$. Vamos mostrar por indução que $a^{p^j(p-1)} = 1 + b_j p^{j+1}$ com $b_j \equiv b_0 \pmod{p}$. Podemos escrever

$$\begin{aligned}
a^{p^{j+1}(p-1)} &= (a^{p^j(p-1)})^p \\
&= (1 + b_j p^{j+1})^p \\
&= 1 + p b_j p^{j+1} + \binom{p}{2} b_j^2 p^{2j+2} + \cdots + b_j^p p^{pj+p} \\
&= 1 + b_j (1 + \binom{p}{2} b_j p^j + \cdots b_j^{p-1} p^{(p-1)j+p-2}) p^{j+2} \\
&= 1 + b_{j+1} p^{j+2}
\end{aligned}$$

com $b_{j+1} \equiv b_j \pmod{p}$ pois o parêntesis na penúltima linha é da forma $1+$ um múltiplo de $p$. Esta última afirmação segue da positividade dos expoentes de $p$ *exceto* no caso $j = 0$; neste caso o expoente do primeiro termo não trivial é zero mas temos $\binom{p}{2} \equiv 0 \pmod{p}$ pois $p > 2$

(é neste ponto que precisamos da hipótese de $p$ ser ímpar). O lema segue de $a^{(p-1)p^{k-2}} \not\equiv 1 \pmod{p^k}$ por indução, pois teremos $(p-1)p^{k-2} = \text{ord}_{p^{k-1}} a \mid \text{ord}_{p^k} a \mid \varphi(p^k) = (p-1)p^{k-1}$, donde $\text{ord}_{p^k} a = (p-1)p^{k-1}$. ■

**Exemplo:** 2 é raiz primitiva módulo $5^k$, $\forall\, k \in \mathbb{N}$. De fato, 2 é raiz primitiva módulo 5, e, como $2^4 = 16 \neq 1$ (módulo 25), 2 é raiz primitiva módulo $25 = 5^2$ (como no Lema 8.1). Portanto, pelo Lema 8.2, 2 é rais primitiva módulo $5^k$, $\forall\, k \in \mathbb{N}$.

**Problema resolvido:** Mostre que existe $n$ natural tal que os mil últimos dígitos de $2^n$ pertencem a $\{1, 2\}$.

**Solução:** Observamos inicialmente que para todo $k \in \mathbb{N}$ existe um número $m_k$ de $k$ algarismos, todos 1 ou 2, divisível por $2^k$. De fato, $m_1 = 2$ e $m_2 = 12$ satisfazem o enunciado.

Seja $m_k = 2^k \cdot r_k$, $r_k \in \mathbb{N}$. Se $r_k$ é par, tome $m_{k+1} = 2 \cdot 10^k + m_k = 2^{k+1}(5^k + r_k/2)$, e se $r_k$ é ímpar, tome $m_{k+1} = 10^k + m_k = 2^{k+1}(5^k + r_k)/2$.

Como $m_{1000} \equiv 2$ (módulo 10), 5 não divide $r_{1000} = m_{1000}/2^{1000}$. Como 2 é raiz primitiva módulo $5^{1000}$, existe $k \in \mathbb{N}$ com $2^k \equiv r_{1000}$ (módulo $5^{1000}$). Logo $2^k = b \cdot 5^{1000} + r_{1000}$, para algum $b \in \mathbb{N}$. Portanto, $2^{k+1000} = b \cdot 10^{1000} + 2^{1000} \cdot r_{1000} = b \cdot 10^{1000} + m_{1000}$, e as 1000 últimas casas de $2^{k+1000}$ são as 1000 casas de $m_{1000}$, que pertencem todas a $\{1, 2\}$. ■

**Lema 8.3:** *Seja $n > 1$. O número de soluções para a congruência $x^2 \equiv 1 \pmod{n}$ é:*

1. *1 se $n = 2$,*
2. *2 se $n = 4$,*
3. *4 se $n = 2^k$, $k > 2$,*
4. *2 se $n = p^k$, $p$ um primo ímpar,*
5. *$2^{m+i}$ se $n = 2^k p_1^{e_1} \cdots p_m^{e_m}$, onde $i = 0$ se $k \leq 1$, $i = 1$ se $k = 2$ e $i = 2$ se $k > 2$.*

**Dem:** Os itens (a) e (b) são verificáveis diretamente. As quatro soluções no item (c) são 1, $2^{k-1} - 1$, $2^{k-1} + 1$ e $2^k - 1$. De fato, é fácil verificar que estes quatro valores são soluções da congruência. Por outro lado, para que $a$ seja solução da congruência devemos ter $2^k | (a+1)(a-1) = a^2 - 1$; portanto $a$ deve ser ímpar. Um dentre $a-1$ e $a+1$ deve ser da forma $2b$, $b$ ímpar. Assim o outro deve ser múltiplo de $2^{k-1}$, o que diz que $a$ deve ter um dos quatro valores acima. Analogamente para o item (d), apenas um dentre $a-1$ e $a+1$ é múltiplo de $p$, o que só permite as soluções 1 e $n-1$.

Para o item (e) usamos os itens anteriores e o teorema chinês dos restos: $a$ é solução da congruência acima se e somente se $a$ satisfaz $a^2 \equiv 1 \pmod{2^k}$ e $a^2 \equiv 1 \pmod{p_i^{e_i}}$ para cada $i$. Assim, o número de soluções módulo $n$ é o produto do número de soluções módulo $2^k$, $p_1^{e_1}, \ldots,$ $p_m^{e_m}$, o que nos dá a fórmula do item (e). ■

**Teorema 8.4:** *Um inteiro $n > 1$ admite raiz primitiva se e somente se $n = 2$, $n = 4$ ou $n$ é da forma $p^k$ ou $2p^k$, onde $p$ é um primo ímpar, admite raiz primitiva.*

**Dem:** Os casos $n = 2$ e $n = 4$ podem ser verificados diretamente. A existência de uma raiz primitiva módulo $p^k$ ($p$ um primo ímpar) segue dos dois primeiros lemas desta seção. Para o caso $2p^k$, seja $a$ uma raiz primitiva módulo $p^k$: $a$ ou $a + p^k$, aquele que for ímpar, será uma raiz primitiva módulo $2p^k$ pois $\varphi(2p^k) = \varphi(p^k)$.

Se $n$ não for de uma destas formas, o lema anterior garante que a congruência $x^2 \equiv 1 \pmod{n}$ admite mais de duas soluções. Por outro lado, a existência de uma raiz primitiva $a$ módulo $n$ garante que a congruência $x^2 \equiv 1 \pmod{n}$ só tem as soluções 1 e $n-1$. De fato, qualquer solução pode ser escrita da forma $a^k$ para algum $k$ e nossa congruência torna-se $a^{2k} \equiv 1 \pmod{n}$ ou $2k \equiv 0 \pmod{\varphi(n)}$, que só tem as soluções $k = 0$ ($a^k = 1$) e $k = (\varphi(n))/2$ ($a^k \equiv n-1 \pmod{n}$).

Outra demonstração, sem usar o lema anterior, consiste em observar que se $n$ não for de uma destas duas formas então $n = n_1 n_2$, com $n_1, n_2 \geq 3$ e $\mathrm{mdc}(n_1, n_2) = 1$. Temos então $a^{\varphi(n)/2} \equiv 1 \pmod{n}$ para todo $a$ inteiro com $\mathrm{mdc}(a, n) = 1$, pois $\varphi(n_1) \mid \varphi(n)/2$ e $\varphi(n_2) \mid \varphi(n)/2$. ■

# 9 A lei da reciprocidade quadrática

A lei de Gauss de reciprocidade quadrática afirma que se $p$ e $q$ são primos há uma relação direta entre $p$ ser quadrado módulo $q$ e $q$ ser quadrado módulo $p$. Este teorema fornece um rápido algoritmo para determinar se $a$ é quadrado módulo $p$ onde $a$ é um inteiro e $p$ um número primo.

**Definição 9.1:** *Seja $p$ um primo e $a$ um inteiro. Definimos o símbolo de Lagrange $(\frac{a}{p})$ por*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{se } p \text{ divide } a \\ -1 & \text{se } a \text{ não é quadrado módulo } p \\ 1 & \text{se } p \nmid a \text{ e } a \text{ é quadrado módulo } p. \end{cases}$$

**Proposição 9.2:** *Seja $p$ um primo ímpar e $a \in \mathbb{Z}$ tal que $p \nmid a$. Então $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.*

**Dem:** Sabemos que se $p \nmid a$ então $a^{p-1} \equiv 1 \pmod p$, ou seja, $X^{p-1} - 1$ tem como raízes $1, 2, \ldots, p-1$ em $\mathbb{Z}/(p)$. Por outro lado, $X^{p-1} - 1 = (X^{\frac{p-1}{2}} - 1)(X^{\frac{p-1}{2}} + 1)$. Se existe $b \in \mathbb{Z}$ tal que $a \equiv b^2 \pmod p$ então $a^{\frac{-1}{2}} \equiv b^{p-1} \equiv 1 \pmod p$; ou seja, $\left(\frac{a}{p}\right) = 1 \equiv a^{\frac{p-1}{2}} \pmod p$. Como $X^2 \equiv Y^2 \pmod p \Leftrightarrow X \equiv \pm Y \pmod p$, há pelo menos $\frac{p-1}{2}$ quadrados em $(\mathbb{Z}/(p))^*$, logo os quadrados são exatamente as raízes de $X^{\frac{p-1}{2}} - 1$ em $\mathbb{Z}/(p)$, donde os não quadrados são exatamente as raízes de $X^{\frac{p-1}{2}} + 1$, ou seja, se $(\frac{b}{p}) = -1$ então $b^{\frac{p-1}{2}} \equiv -1 \pmod p$. ■

**Corolário 9.3:** *Se $p$ é primo ímpar então $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.*

Vamos agora reinterpretar a Proposição 1. Seja $a \in (\mathbb{Z}/(p))^*$. Para cada $j = 1, 2, \ldots, \frac{p-1}{2}$ escrevemos $a \cdot j$ como $\varepsilon_j m_j$ com $\varepsilon_j \in \{-1, 1\}$ e $m_j \in \{1, 2, \ldots, \frac{p-1}{2}\}$. Se $m_i \neq m_j$ temos $a \cdot i = a \cdot j$ ou $a \cdot i = -a \cdot j$; a primeira possibilidade implica $i = j$ e a segunda é impossível. Assim, se $i \neq j$ temos $m_i \neq m_j$ donde $\{m_1, m_2, \ldots, m_{\frac{p-1}{2}}\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. Assim

$$\begin{aligned} \left(\frac{a}{p}\right) &\equiv a^{\frac{p-1}{2}} \\ &= \frac{(a\cdot 1)(a \cdot 2)\cdots(a \cdot \frac{p-1}{2})}{1 \cdot 2 \cdots \frac{p-1}{2}} \\ &\equiv \frac{\varepsilon_1 \varepsilon_2 \cdots \varepsilon_{\frac{p-1}{2}} m_1, m_2, \ldots, m_{\frac{p-1}{2}}}{1 \cdot 2 \cdots \frac{p-1}{2}} \\ &= \varepsilon_1 \varepsilon_2 \cdots \varepsilon_{\frac{p-1}{2}} \pmod p \end{aligned} \tag{1}$$

donde $(\frac{a}{p}) = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_{\frac{p-1}{2}}$, pois ambos pertencem a $\{-1, 1\}$. Assim, $(\frac{a}{p}) = (-1)^m$ onde $m$ é o número de elementos $j$ de $\{1, 2, \ldots, \frac{p-1}{2}\}$ tais que $\varepsilon_j = -1$. Como primeira conseqüência deste fato temos o seguinte resultado.

**Proposição 9.4:** *Se $p$ é um primo ímpar então*

$$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \textit{se } p \equiv \pm 1 \pmod 8, \\ -1, & \textit{se } p \equiv \pm 3 \pmod 8. \end{cases}$$

**Dem:** Se $p \equiv 1 \pmod 4$, digamos $p = 4k+1$, temos $\frac{p-1}{2} = 2k$. Como $1 \leq 2j \leq \frac{p-1}{2}$ para $j \leq k$ e $\frac{p-1}{2} < 2j \leq p-1$ para $k+1 \leq j \leq 2k$, temos

$$(\frac{a}{p}) = (-1)^k = \begin{cases} 1, & \text{se } p \equiv 1 \pmod 8, \\ -1, & \text{se } p \equiv 5 \pmod 8. \end{cases}$$

Se $p \equiv 3 \pmod 4$, digamos $p = 4k+3$, temos $\frac{p-1}{2} = 2k+1$. Para $1 \leq j \leq k$ temos $1 \leq 2j \leq \frac{p-1}{2}$ e para $k+1 \leq j \leq 2k+1$ temos $\frac{p-1}{2} < 2j \leq p-1$, donde

$$(\frac{a}{p}) = (-1)^{k+1} = \begin{cases} -1, & \text{se } p \equiv 3 \pmod 8, \\ 1, & \text{se } p \equiv 7 \pmod 8. \end{cases}$$

■

**Teorema 9.5:** (Lei de reciprocidade quadrática) *Sejam $p$ e $q$ primos ímpares. Então $(\frac{p}{q}) = (-1)^{(p-1)(q-1)/4}(\frac{q}{p})$.*

**Dem:** Na notação acima, com $a = q$, para cada $j \in P$, onde

$$P = \{1, 2, \ldots, (p-1)/2\},$$

temos que $\varepsilon_j = -1$ se e só se existe $y \in \mathbb{Z}$ tal que $-(p-1)/2 \leq qj - py < 0$. Tal $y$ deve pertencer a $Q$, onde

$$Q = \{1, 2, \ldots, (q-1)/2\}.$$

Assim, temos que $(\frac{q}{p}) = (-1)^m$ onde $m = |X|$ e

$$X = \{(x, y) \in P \times Q \mid -(p-1)/2 \leq qx - py < 0\};$$

note que $qx - py$ nunca assume o valor 0. Analogamente, $(\frac{p}{q}) = (-1)^n$, onde $n = |Y|$ e

$$Y = \{(x, y) \in P \times Q \mid 0 < qx - py \leq (q-1)/2\}.$$

Daí segue que $(\frac{p}{q})(\frac{q}{p}) = (-1)^k$ onde $k = m + n = |Z|$ onde

$$Z = \{(x, y) \in P \times Q \mid -(p-1)/2 \leq qx - py \leq (q-1)/2\}$$

pois $qx - py$ nunca assume o valor 0. Temos $k = |C| - |A| - |B|$ onde $C = P \times Q$,

$$A = \{(x, y) \in C \mid qx - py < -(p-1)/2\},$$
$$B = \{(x, y) \in C \mid qx - py > (q-1)/2\}.$$

Como $|C| = (p-1)(q-1)/4$, basta mostrar que $|A| = |B|$. Mas $f : C \to C$ definida por $f(x, y) = (((p+1)/2) - x, ((q+1)/2) - y)$ define uma bijeção entre $A$ e $B$. ■

# 10 Extensões quadráticas de corpos finitos

Sejam $p$ primo e $d$ um inteiro que não seja quadrado perfeito. O anel $(\mathbb{Z}/(p))[\sqrt{d}]$ é o conjunto

$$\{a + b\sqrt{d},\ a, b \in \mathbb{Z}/(p)\}$$

onde

$$(a + b\sqrt{d}) + (\tilde{a} + \tilde{b}\sqrt{d}) = (a + \tilde{a}) + (b + \tilde{b})\sqrt{d}$$
$$(a + b\sqrt{d})(\tilde{a} + \tilde{b}\sqrt{d}) = (a\tilde{a} + db\tilde{b}) + (a\tilde{b} + \tilde{a}b)\sqrt{d}.$$

Por definição,

$$a + b\sqrt{d} = \tilde{a} + \tilde{b}\sqrt{d} \Leftrightarrow a = \tilde{a}, b = \tilde{b}.$$

Como grupo aditivo, $(\mathbb{Z}/(p))[\sqrt{d}] = \mathbb{Z}/(p) \times \mathbb{Z}/(p)$. Vamos investigar a estrutura multiplicativa de $(\mathbb{Z}/(p))[\sqrt{d}]$. Observemos inicialmente que, se $d$ é um quadrado módulo $p$ então $(\mathbb{Z}/(p))[\sqrt{d}]$ não pode ser um corpo, pois se $a^2 = d$ em $\mathbb{Z}/(p)$ então $(a + \sqrt{d})(a - \sqrt{d}) = 0$ em $(\mathbb{Z}/(p))[\sqrt{d}]$. A próxima proposição é uma recíproca deste fato:

**Proposição 10.1:** *Se* $(\frac{d}{p}) = -1$ *então* $(\mathbb{Z}/(p))[\sqrt{d}]$ *é um corpo.*

**Dem:** De fato, se $(a,b) \neq (0,0)$, $(a+b\sqrt{d})^{-1} = (a-b\sqrt{d})/(a^2-db^2)$. Temos que $a^2-db^2 \in (\mathbb{Z}/(p))^*$, pois $d$ não é quadrado mod $p$, logo, se $b \neq 0$, $a^2-db^2=0$, que equivale a $d=(a/b)^2$ seria uma contradição e, se $b=0$, $a^2-db^2=a^2 \neq 0$ pois $(a,b) \neq (0,0) \Rightarrow a \neq 0 \Rightarrow a^2 \neq 0$.

$\blacksquare$

**Problemas:**

1) Sejam $a, n > 1$ inteiros. Prove que

   i) Se $a^n - 1$ é primo então $a = 2$ e $n$ é primo.

   ii) Se $a^n + 1$ é primo então $n = 2^k$ para algum inteiro $k$.

2) Prove que existem infinitos números primos congruentes a 3 módulo 4.

3) Determine todos os $n$ naturais tais que $(2^n - 1)/n$ é inteiro.

4) Determine todos os $n$ naturais que $(2^n + 1)/n^2$ é inteiro.

5) Prove que se $a$ e $b$ são naturais e $(a^2+b^2)/(ab+1)$ é inteiro então $(a^2+b^2)/(ab+1)$ é quadrado perfeito.

6) Sejam $a, n \in \mathbb{N}^*$. Considere a seqüência $(x_n)$ definida por $x_1 = a$, $x_{k+1} = a^{x_k}$, $\forall\, k \in \mathbb{N}$. Mostre que existe $N \in \mathbb{N}$ tal que $x_{k+1} \equiv x_k$ (módulo $n$), para todo $k \geq N$.

**Obs.:** Os Problemas 4 e 5 foram propostos na 31ª e na 29ª Olimpíada Internacional de Matemática (1990 e 1988) respectivamente.

# CAPÍTULO 2

# Números Primos

## 1 Sobre a distribuição dos números primos

Já vimos que existem infinitos primos; o teorema dos números primos dá uma estimativa de quantos primos existem até um inteiro $x$, ou seja, descreve a distribuição dos primos. Defina $\pi(x)$ como sendo o número de primos $p$ com $2 \leq p \leq x$.

**Teorema 1.1:** (Teorema dos números primos)

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Observe que aqui e em todo o livro log denota o logaritmo natural. Este resultado foi conjecturado por vários matemáticos, inclusive por Legendre e Gauss, mas a demonstração completa só foi encontrada em 1896, por de la Vallée Poussin e Hadamard (independentemante). Não demonstraremos este teorema: as demonstrações elementares conhecidas são todas bastante difíceis (lembramos que uma demonstração é dita *elementar* quando não usa ferramentas avançadas: muitas demonstrações elementares são longas e sofisticadas). Daremos uma demonstração da seguinte proposição (devida a Tchebycheff) que é claramente uma versão fraca do teorema dos números primos.

**Proposição 1.2:** *Existem constantes positivas $c < C$ tais que*

$$c\frac{x}{\log x} < \pi(x) < C\frac{x}{\log x}$$

*para todo $x \geq 2$.*

**Dem:** Observemos inicialmente que $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ é múltiplo de todos os primos $p$ que satisfazem $n < p \leq 2n$. Como

$$\binom{2n}{n} < \sum_{0 \leq k \leq 2n} \binom{2n}{k} = 2^{2n},$$

segue que o produto dos primos entre $n$ e $2n$ é menor do que $2^{2n}$. Como há $\pi(2n)-\pi(n)$ primos como esses segue que $n^{\pi(2n)-\pi(n)} < 2^{2n}$ (pois todos esses primos são maiores que $n$), donde $(\pi(2n)-\pi(n))\log n < 2n\log 2$ e

$$\pi(2n)-\pi(n) < \frac{2n\log 2}{\log n}.$$

Isso implica facilmente, por indução, que

$$\pi(2^{k+1}) \leq \frac{5\cdot 2^k}{k}$$

(começando com $k=5$; até $k=5$ segue de $\pi(n)\leq n/2$). Daí segue que se $2^k < x \leq 2^{k+1}$ então

$$\pi(x) \leq \frac{5\cdot 2^k}{k} \leq \frac{5x\log 2}{\log x}$$

pois $f(x) = x\log 2/\log x$ é uma função crescente para $x \geq 3$.

Vamos agora provar a outra desigualdade. O expoente do primo $p$ na fatoração de $n!$ é

$$\begin{aligned} w_p(n) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots \\ &= \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \end{aligned}$$

(esta é uma soma finita pois se $k > \log_p n = \log n/\log p$ então $\lfloor \frac{n}{p^k} \rfloor = 0$). De fato, $\lfloor \frac{n+1}{p^j} \rfloor - \lfloor \frac{n}{p^k} \rfloor$ é sempre 0 ou 1, e é igual a 1 se e só se $p^j$ divide $n+1$. Assim, $w_p(n+1)-w_p(n)$ é igual ao expoente de $p$ na fatoração de $n+1$, o que fornece uma prova por indução do fato acima.

Assim, o expoente de $p$ em $\binom{2n}{n} = (2n)!/n!^2$ é

$$\sum_{k=1}^{\infty}\left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2\left\lfloor \frac{n}{p^k} \right\rfloor\right).$$

Temos agora que $\lfloor \frac{2n}{p^k} \rfloor - 2\lfloor \frac{n}{p^k} \rfloor$ é sempre 0 ou 1 (pois $0 \leq x - \lfloor x \rfloor < 1$ para todo $x$), donde o expoente de $p$ em $\binom{2p}{p}$ é no máximor $\log_p n = \log n/\log p$ para todo primo $p$. Por outro lado, se $n < p \leq 2n$, o expoente de $p$ em $\binom{2p}{p}$ é 1. Assim, se $\binom{2n}{n} = \prod_{p<2n} p^{\alpha_p}$ é a fatoração de $\binom{2n}{n}$

então

$$\begin{aligned}\log\binom{2n}{n} &= \sum_{p<2n}\alpha_p\log p \\ &= \sum_{p\le n}\alpha_p\log p + \sum_{n<p\le 2n}\log p \\ &\le \pi(n)\log n + (\pi(2n)-\pi(n))\log(2n) \\ &\le \pi(2n)\log(2n)\end{aligned}$$

donde

$$\pi(2n) \ge \log\binom{2n}{n}/\log(2n) \ge n\log 2/\log(2n)$$

pois

$$\binom{2n}{n} = \frac{2n}{n}\cdot\frac{2n-1}{n-1}\cdots\frac{n+1}{1} \ge 2^n,$$

donde

$$\pi(x) \ge \frac{x\log 2}{\log x}$$

para todo $x$ par, o que implica na mesma estimativa para todo $x$ inteiro, pois $\pi(2k-1) = \pi(2k)$.

■

**Corolário 1.3:** *Seja $f : \mathbb{N} \to [0, +\infty)$ uma função decrescente. A série*

$$\sum_{p\ primo} f(p)$$

*converge se e somente se a série*

$$\sum_{n=2}^{\infty}\frac{f(n)}{\log n}$$

*converge. Em particular,*

$$\sum_{p\ primo}\frac{1}{p} = +\infty.$$

Deixamos a demonstração deste corolário como exercício.

Uma aproximação mais precisa para $\pi(x)$ é dada por

$$\mathrm{Li}(x) = \int_0^x \frac{dt}{\log t},$$

onde tomamos o valor principal desta integral, ou seja,

$$\mathrm{Li}(x) = \lim_{\varepsilon \to 0} \int_\varepsilon^{1-\varepsilon} \frac{dt}{\log t} + \int_{1+\varepsilon}^x \frac{dt}{\log t};$$

claramente

$$\lim_{x \to \infty} \frac{\mathrm{Li}(x)}{\log(x)/x} = 1.$$

Sabe-se entretanto que

$$|\pi(x) - \mathrm{Li}(x)| \leq Cxe^{-a(\log x)^{3/5}(\log\log x)^{-1/5}}$$

para algum valor das constantes $a$ e $C$ (independente de $x$). Em particular, para qualquer $k > 0$ existe $C > 0$ tal que,para todo x,

$$|\pi(x) - \mathrm{Li}(x)| \leq C\frac{x}{(\log x)^k},$$

o que mostra que $\mathrm{Li}(x)$ (e mesmo $x/(\log x - 1)$) é uma aproximação de $\pi(x)$ bem melhor do que $x/\log x$.

A hipótese de Riemann, já mencionada, equivale a dizer que para todo $\varepsilon > 0$ existe $C$ com

$$|\pi(x) - \mathrm{Li}(x)| \leq Cx^{1/2+\varepsilon};$$

ninguém sabe demonstrar que esta estimativa seja correta sequer para algum valor de $\varepsilon < 1/2$. A hipótese de Riemann também implica que existe $C$ com

$$|\pi(x) - \mathrm{Li}(x)| \leq Cx^{1/2}\log x,$$

o que daria uma estimativa para o tamanho deste erro muito melhor de que as que se sabe demonstrar. Por outro lado, sabe-se demonstrar que não pode existir nenhuma estimativa muito melhor do que esta para $|\pi(x) - \mathrm{Li}(x)|$: existe uma constante $C > 0$ e inteiros $x_1$ e $x_2$ arbitrariamente grandes com

$$\pi(x_1) - \mathrm{Li}(x_1) < -C\frac{\sqrt{x_1}\log\log\log x_1}{\log x_1},$$
$$\pi(x_2) - \mathrm{Li}(x_2) > C\frac{\sqrt{x_2}\log\log\log x_2}{\log x_2}.$$

## 2 Outros resultados e conjecturas sobre primos

Nesta seção veremos o enunciado de alguns resultados clássicos sobre números primos. Também veremos vários problemas em aberto famosos.

**Teorema 2.1:** (Dirichlet) *Dados naturais $a, d$ com $\operatorname{mdc}(a, d) = 1$, existem infinitos primos da forma $a + dn$ (com $n$ natural).*

A demonstração usual deste teorema usa variáveis complexas. Muitos casos particulares admitem demonstrações elementares mais ou menos simples. O leitor não deve ter dificuldade em demonstrar, por exemplo, que existem infinitos primos da forma $4n + 3$ ou $6n + 5$.

Existem vários refinamentos conhecidos do teorema de Dirichlet. Definimos $\pi_{d,a}(x)$ como sendo o número de primos da forma $a + dn$ no intervalo $[2, x]$. De la Vallée Poussin provou que

$$lim_{x\to+\infty}\frac{\pi_{d,a}(x)}{\pi(x)} = \frac{1}{\varphi(d)},$$

isto é, todas as possíveis classes módulo $d$ têm aproximadamente a mesma proporção de primos.

Por outro lado, Tchebycheff observou que para valores pequenos de $x$ $\pi_{3,2}(x) - \pi_{3,1}(x)$ e $\pi_{4,3}(x) - \pi_{4,1}(x)$ são positivos. Um teorema de Littlewood, entretanto, demonstra que estas funções mudam de sinal infinitas vezes. Em 1957, Leech demonstrou que o menor valor de $x$ para o qual $\pi_{4,3}(x) - \pi_{4,1}(x) = -1$ é 26861 e em 1978 Bays e Hudson demonstraram que o menor valor de $x$ para o qual $\pi_{3,2}(x) - \pi_{3,1}(x) = -1$ é 608981813029.

Seja $p(d, a)$ o menor primo da forma $a + dn$, $n$ inteiro e

$$p(d) = \max\{p(d, a) \mid 0 < a < d, \operatorname{mdc}(a, d) = 1\}.$$

Linnik (1944) provou que existe $L > 1$ com $p(d) < d^L$ para todo $d$ suficientemente grande. A melhor estimativa conhecida para $L$ é $L \leq 5,5$, devida a Heath-Brown (1992), que também conjecturou que

$$p(d) \leq Cd(\log d)^2.$$

Por outro lado, não se sabe demonstrar que existam infinitos primos da forma $n^2 + 1$; aliás, não existe nenhum polinômio $P$ em uma variável e de grau maior que 1 para o qual se saiba demonstrar que existem infinitos primos da forma $P(n)$, $n \in \mathbb{Z}$. Por outro lado, existem muitos polinômios em mais de uma variável que assumem infinitos valores primos: por exemplo, prova-se facilmente que todo primo da forma $4n+1$ pode ser escrito também na forma $a^2+b^2$, $a, b \in \mathbb{Z}$. Por outro lado, Friedlander e Iwaniec provaram recentemente um resultado muito mais difícil: que existem infinitos primos da forma $a^2 + b^4$.

Um dos problemas em aberto mais famosos da matemática é a conjectura de Goldbach: todo número par maior ou igual a 4 é a soma de dois primos. Chen demonstrou que todo número par suficientemente grande é a soma de um primo com um número com no máximo dois fatores primos. Vinogradov demonstrou que todo ímpar suficientemente grande (por exemplo, maior do que $3^{3^{15}}$) é uma soma de três primos.

Quando $p$ e $p+2$ são ambos primos, dizemos que eles são *primos gêmeos*. Conjectura-se, mas não se sabe demonstrar, que existem infinitos primos gêmeos. Brun, por outro lado, provou que primos gêmeos são escassos no seguinte sentido: se $\pi_2(x)$ é o número de pares de primos gêmeos até $x$ então

$$\pi_2(x) < \frac{100x}{(\log x)^2}$$

para $x$ sufientemente grande. Em particular,

$$\sum_{p \text{ primo gêmeo}} \frac{1}{p} < +\infty.$$

Acredita-se que $\pi_2(x)$ seja assintótico a $Cx/(\log x)^2$ para alguma constante positiva $C$. Deixamos como exercício provar a seguinte caracterização de primos gêmeos devida a Clement. Seja $n \geq 2$; os inteiros $n$ e $n+2$ são ambos primos se e somente se

$$4((n-1)!+1) + n \equiv 0 \pmod{n(n+2)}.$$

Seja $p_n$ o $n$-ésimo número primo. O teorema dos números primos equivale a dizer que

$$\lim_{n\to\infty} \frac{p_n}{n \log n} = 1.$$

Por outro lado, sabe-se muito pouco sobre o comportamento da função $d_n = p_{n+1} - p_n$. Por exemplo, a conjectura de que existem infinitos primos gêmeos equivale a dizer que $\liminf d_n = 2$.

Não se sabe provar nem que

$$L = \liminf \frac{d_n}{\log p_n} = 0;$$

Erdös provou que $L < 1$ e Maier que $L \leq 0,248$. Erdös também provou que o conjunto dos pontos de acumulação de $d_n/\log p_n$ tem medida positiva. Por outro lado, é um teorema clássico, conhecido como postulado de Bertrand, que sempre existe pelo menos um primo entre $m$ e $2m$, ou seja, $d_n < p_n$. Em 1931, Westzynthius provou que

$$\limsup \frac{d_n}{\log p_n} = \infty,$$

e em 1963 Rankin, completando um trabalho de Erdös, mostrou que

$$\limsup \frac{d_n(\log\log\log p_n)^2}{\log p_n \log\log p_n \log\log\log\log p_n} \geq e^\gamma \approx 1,78107$$

onde $\gamma$ é a constante de Euler-Mascheroni,

$$\gamma = \lim_{n\to\infty}\left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n\right) \approx 0,5772156649;$$

este resultado foi melhorado posteriormente por Pomerance e Pintz, que provou que o lado esquerdo é maior ou igual a $2e^\gamma$ ([**Pintz**]). Conjectura-se que

$$\limsup \frac{d_n}{(\log p_n)^2} = C$$

para alguma constante positiva $C$. Outra conjectura famosa é que sempre há pelo menos um primo entre $n^2$ e $(n+1)^2$. Observamos que a primeira vez que $d_n > 1000$ ocorre para $p_n = 1693182318746371$, quando $d_n = 1132$, o que foi descoberto recentemente por T. Nicely e D. Nyman.

Sierpinski provou que existem infinitos números naturais $k$ tais que $k \cdot 2^n + 1$ é composto para todo natural $n$ e Riesel provou o mesmo resultado para $k \cdot 2^n - 1$. Conjectura-se que os menores valores de $k$ com as propriedades acima são respectivamente 78557 e 509203. Há um projeto cooperativo, que consiste em procurar primos grandes, para demonstrar estas conjecturas (veja `http://vamri.xray.ufl.edu/proths/`).

O leitor interessado em aprender mais sobre problemas em aberto em teoria dos números pode consultar [**Guy**].

# 3 Fórmulas para primos e testes de primalidade

Mencionamos na introdução deste capítulo que não se conhece nenhuma fórmula simples para gerar primos arbitrariamente grandes. Uma palavra imprecisa mas importante nesta frase é "simples". Existem fórmulas que geram números primos, mas que são tão complicadas que não ajudam muito nem a gerar números primos explicitamente nem a responder perguntas teóricas sobre a distribuição dos primos. Um exemplo de fórmula para $p_n$, o $n$-ésimo primo, é

$$p_n = \left\lfloor 1 - \frac{1}{\log 2} \log \left( -\frac{1}{2} + \sum_{d \mid P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right\rfloor,$$

onde $P_{n-1} = p_1 p_2 \cdots p_{n-1}$; deixamos a demonstração a cargo do leitor. Outra fórmula é

$$p_n = \lfloor 10^{2^n} c \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} c \rfloor,$$

onde

$$c = \sum_{n=1}^{\infty} \frac{p_n}{10^{2^n}} = 0.0203000500000007\ldots.$$

A inutilidade desta última fórmula vem do fato que para calcular $c$ devemos encontrar todos os primos; a fórmula se tornaria mais interessante se existisse outra interpretação para o número real $c$, o que parece muito improvável. Por outro lado, existe um número real $a > 1$ tal que $\lfloor a^{3^n} \rfloor$ é sempre primo.

Um tipo de fórmula para primos, de certa forma mais intrigante, são polinômios de coeficientes inteiros em $S$ variáveis com a seguinte propriedade quase mágica: a interseção da imagem de $\mathbb{N}^S$ com $\mathbb{N}$ é exatamente o conjunto dos números primos. Note que se tomarmos um ponto de $\mathbb{N}^S$ "ao acaso", o valor do polinômio neste ponto quase certamente será negativo; assim, é difícil usar o polinômio para gerar primos. A título de curiosidade, vejamos um exemplo de polinômio com estas propriedades; aqui $N = 26$, o valor do polinômio é $P$, as variáveis chamam-se $a, b, \ldots, z$ e $A, B, \ldots, N$ são expressões auxiliares:

$$
\begin{aligned}
P &= (k+2)(1 - A^2 - B^2 - C^2 - \cdots - N^2),\\
A &= wz + h + j - q,\\
B &= (gk + 2g + k + 1)(h + j) + h - z,\\
C &= 16(k+1)^3(k+2)(n+1)^2 + 1 - f^2,\\
D &= 2n + p + q + z - e,\\
E &= e^3(e+2)(a+1)^2 + 1 - o^2,\\
F &= (a^2-1)y^2 + 1 - x^2,\\
G &= 16r^2y^4(a^2-1) + 1 - u^2,\\
H &= ((a + u^2(u^2-a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2,\\
I &= (a^2-1)l^2 + 1 - m^2,\\
J &= ai + k + 1 - l - i,\\
K &= n + l + v - y,\\
L &= p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m,\\
M &= q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x,\\
N &= z + pl(a - p) + t(2ap - p^2 - 1) - pm.
\end{aligned}
$$

Algumas observações simples: a única forma de $P$ ser positivo é se $A = B = \cdots = N = 0$; neste caso seu valor será $k + 2$. Vemos assim que para produzir um número primo $P$ com este polinômio devemos antes de mais nada tomar $k = P - 2$. As expressões auxiliares viram equações: como $A = 0$ temos $q = wz + h + j$. Assim, dado $k$ para o qual $k + 2$ é primo, precisamos procurar valores para as outras letras que satisfaçam estas equações. Estes valores de certa forma *encodificam* uma demonstração de que $P = k + 2$ é primo.

# 4 Testes de primalidade baseados em fatorações de $n - 1$

**Proposição 4.1:** *Seja $n > 1$. Se para cada fator primo $q$ de $n - 1$ existe um inteiro $a_q$ tal que $a_q^{n-1} \equiv 1 \pmod{n}$ e $a_q^{(n-1)/q} \not\equiv 1 \pmod{n}$ então $n$ é primo.*

**Dem:** Seja $q^{k_q}$ a maior potência de $q$ que divide $n-1$. A ordem de $a_q$ em $(\mathbb{Z}/(n))^*$ é um múltiplo de $q^{k_q}$, donde $\varphi(n)$ é um múltiplo de $q^{k_q}$. Como isto vale para todo fator primo $q$ de $n-1$, $\varphi(n)$ é um múltiplo de $n-1$ e $n$ é primo. ■

**Proposição 4.2:** (Pocklington) *Se $n-1 = q^k R$ onde $q$ é primo e existe um inteiro $a$ tal que $a^{n-1} \equiv 1 \pmod n$ e $\mathrm{mdc}(a^{(n-1)/q} - 1, n) = 1$ então qualquer fator primo de $n$ é congruo a 1 módulo $q^k$.*

**Dem:** Se $p$ é um fator primo de $n$ então $a^{n-1} \equiv 1 \pmod p$ e $p$ não divide $a^{(n-1)/q} - 1$, donde $\mathrm{ord}_p\, a$, a ordem de $a$ módulo $p$, divide $n-1$ mas não divide $(n-1)/q$. Assim, $q^k \mid \mathrm{ord}_p\, a | p-1$, donde $p \equiv 1 \pmod q)^k$. ■

**Corolário 4.3:** *Se $n-1 = FR$, com $F > R$ e para todo fator primo $q$ de $F$ existe $a > 1$ tal que $a^{n-1} \equiv 1 \pmod n$ e $\mathrm{mdc}(a^{(n-1)/q} - 1, n) = 1$ então $n$ é primo.*

**Dem:** Seja $q$ um fator primo de $F$ e $q^k$ a maior potência de $q$ que divide $F$; pela proposição anterior, todo fator primo de $n$ deve ser côngruo a 1 módulo $q^k$. Como isto vale para qualquer fator primo de $F$, segue que qualquer fator primo de $n$ deve ser côngruo a 1 módulo $F$. Como $F > \sqrt{n}$, isto implica que $n$ é primo. ■

De fato, basta conhecer um conjunto de fatores primos cujo produto seja maior do que $(n-1)^{1/3}$ para, usando o resultado de Pocklington, tentar demonstrar a primalidade de $n$ (o que deixamos como exercício). Os seguintes critérios clássicos são conseqüências diretas das proposições acima.

Fermat conjecturou que todo número da forma $F_n = 2^{2^n} + 1$ fosse primo e verificou a conjectura para $n \leq 4$. Observe que $2^n + 1$ (e em geral $a^n + 1$ com $a \geq 2$) *não* é primo se $n$ não é uma potência de 2: se $p$ é um fator primo ímpar de $n$, podemos escrever $a^n + 1 = b^p + 1 = (b+1)(b^{p-1} - b^{p-2} + \cdots + b^2 - b + 1)$ onde $b = a^{n/p}$. Euler mostraria mais tarde que $F_5$ não é primo (temos $F_5 = 4294967297 = 641 \cdot 6700417$) e já se demonstrou que $F_n$ é composto para vários outros valores de $n$; nenhum outro primo da forma $F_n = 2^{2^n} + 1$ é conhecido, mas se conhecem muitos primos (alguns bastante grandes) da forma $a^{2^n} + 1$, que são conhecidos como primos de Fermat generalizados. O teste a seguir mostra como testar eficientemente a primalidade de $F_n$.

**Corolário 4.4:** (Teste de Pépin) *Seja* $F_n = 2^{2^n} + 1$*;* $F_n$ *é primo se e somente se* $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

**Dem:** Se $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$ então a primalidade de $F_n$ segue da Proposição 4.1. Por outro lado, se $F_n$ é primo então $3^{(F_n-1)/2} \equiv (\frac{3}{F_n}) = (\frac{F_n}{3}) = (\frac{2}{3}) = -1 \pmod{F_n}$. ∎

**Corolário 4.5:** (Teorema de Proth; 1878) *Seja* $n = h \cdot 2^k + 1$ *com* $2^k > h$*. Então* $n$ *é primo se e somente se existe um inteiro* $a$ *com* $a^{(n-1)/2} \equiv -1 \pmod{n}$.

**Dem:** Se $n$ é primo, podemos tomar $a$ qualquer com $(\frac{a}{n}) = -1$; ou seja, metade dos inteiros entre 1 e $n-1$ serve como $a$. A recíproca segue do Corolário 4.3 com $F = 2^k$. ∎

**Corolário 4.6:** *Se* $n = h \cdot q^k + 1$ *com* $q$ *primo e* $q^k > h$*. Então* $n$ *é primo se e somente se existe um inteiro* $a$ *com* $a^{n-1} \equiv 1 \pmod{n}$ *e* $\mathrm{mdc}(a^{(n-1)/q} - 1, n) = 1$.

**Dem:** Se $n$ é primo, podemos tomar $a$ qualquer que não seja da forma $x^q$ módulo $n$; ou seja, uma proporção de $(q-1)/q$ dentre inteiros entre 1 e $n-1$ serve como $a$. A recíproca segue do Corolário 4.3 com $F = q^k$. ∎

Uma expressiva maioria entre os 100 maiores primos conhecidos estão nas condições do teorema de Proth (ver tabelas). Isto se deve ao fato de primos desta forma serem freqüentes (mais freqüentes do que, por exemplo, primos de Mersenne) e que sua primalidade é facilmente demonstrada usando este resultado.

# 5 Primos de Mersenne

Um número de Mersenne é um número da forma $M_p = 2^p - 1$. Os 5 maiores números primos conhecidos atualmente são primos de Mersenne. O maior deles é $2^{13466917} - 1$, descoberto em 14/11/2001. Este é um dos dois primos conhecidos com mais de um milhão de dígitos. O outro é $2^{6972593} - 1$ (também primo de Mersenne). Ambos foram descobertos pelo GIMPS (veja `www.mersenne.org`). O critério de Lucas-Lehmer, que apresentaremos nesta seção, é um dos fatores para que isso ocorra pois fornece um teste de primalidade bastante rápido para números de Mersenne. Vejamos primeiramente que $2^p - 1$ só tem chance de ser primo quando $p$ é primo.

**Proposição 5.1:** *Se* $2^n - 1$ *é primo então* $n$ *é primo.*

**Dem:** Se $n = ab$ com $a, b \geq 2$ então $1 < 2^a - 1 < 2^n - 1$ e $2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 \equiv 1^b - 1 = 0 \pmod{2^a - 1}$ e $2^n - 1$ é composto. ∎

Por outro lado, não se sabe demonstrar nem que existam infinitos *primos de Mersenne* nem que existem infinitos primos $p$ para os quais $M_p$ é composto. Conjectura-se, entretanto, que existam infinitos primos $p$ para os quais $M_p$ é primo e que, se $p_n$ é o $n$-ésimo primo deste tipo, temos

$$0 < A < \frac{\log p_n}{n} < B < +\infty$$

para constantes $A$ e $B$. Existem algumas conjecturas mais precisas quanto ao valor de

$$\lim_{n \to \infty} \sqrt[n]{p_n};$$

Eberhart conjectura que este limite exista e seja igual a $3/2$; Wagstaff por outro lado conjectura que o limite seja

$$2^{e^{-\gamma}} \approx 1,4757613971$$

onde $\gamma$ é a já mencionada constante de Euler-Mascheroni.

Primos de Mersenne são interessantes também por causa de *números perfeitos*. Dado $n \in \mathbb{N}^*$, definimos

$$\sigma(n) = \sum_{d \mid n} d,$$

a soma dos divisores (positivos) de $n$. Pelo teorema fundamental da aritmética demonstramos facilmente que se

$$n = p_1^{e_1} p_2^{e_2} \cdots p_m^{e_m},$$

com $p_1 < p_2 < \cdots < p_m$ então

$$\begin{aligned}\sigma(n) &= (1 + p_1 + \cdots + p_1^{e_1}) \cdots (1 + p_m + \cdots + p_m^{e_m}) \\ &= \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdots \frac{p_m^{e_m+1} - 1}{p_m - 1}.\end{aligned}$$

Em particular, se $(a, b) = 1$ então $\sigma(ab) = \sigma(a)\sigma(b)$. Um inteiro positivo $n$ é dito *perfeito* se $\sigma(n) = 2n$; os primeiros números perfeitos são 6, 28 e 496. Nosso próximo resultado caracteriza os números perfeitos pares.

**Proposição 5.2:** *Se $M_p$ é um primo de Mersenne então $2^{p-1}M_p$ é perfeito. Além disso, todo número perfeito par é da $2^{p-1}M_p$ para algum primo $p$, sendo $M_p$ um primo de Mersenne.*

**Dem:** Se $M_p$ é primo então

$$\sigma(2^{p-1}M_p) = (2^p - 1)(M_p + 1) = 2 \cdot 2^{p-1}M_p.$$

Por outro lado seja $n = 2^k b$, com $k > 0$ e $b$ ímpar, um número perfeito par. Temos $\sigma(n) = 2n = \sigma(2^k)\sigma(b)$ donde $2^{k+1}b = (2^{k+1}-1)\sigma(b) \geq (2^{k+1}-1)(b+1)$, valendo a igualdade apenas se $b$ for primo. Desta desigualdade temos $b \leq 2^{k+1} - 1$. Por outro lado, como $(2^{k+1}-1)|2^{k+1}b$ e $(2^{k+1}-1, 2^{k+1}) = 1$, temos $(2^{k+1}-1)|b$ e $2^{k+1} - 1 \leq b$. Assim $b = 2^{k+1} - 1$ e $2^{k+1}b = (2^{k+1}-1)(b+1)$, donde $b$ é primo. Pela proposição 3.9, $p = k+1$ é primo, $b = M_p$ e $n = 2^{p-1}M_p$. ■

Por outro lado, um dos problemas em aberto mais antigos da matemática é o da existência de números perfeitos ímpares. Sabe-se apenas que um número perfeito ímpar, se existir, deve ser muito grande (mais de 300 algarismos) e satisfazer simultaneamente várias condições complicadas.

**Conjectura 5.3:** *Não existe nenhum número perfeito ímpar.*

Nosso próximo resultado é o critério de Lucas-Lehmer, a base dos algoritmos que testam para grandes valores de $p$ se $2^p - 1$ é ou não primo:

**Teorema 5.4:** *Seja $S$ a seqüência definida por $S_0 = 4$, $S_{k+1} = S_k^2 - 2$ para todo natural $k$. Seja $n > 2$; $M_n = 2^n - 1$ é primo se e somente se $S_{n-2}$ é múltiplo de $M_n$.*

**Dem:** Observemos inicialmente que

$$S_n = (2+\sqrt{3})^{2^n} + (2-\sqrt{3})^{2^n}$$

para todo natural $n$. A demonstração por indução é simples: claramente $S_0 = 4 = (2+\sqrt{3})^{2^0} + (2-\sqrt{3})^{2^0}$ e

$$\begin{aligned}
S_{k+1} = S_k^2 - 2 &= ((2+\sqrt{3})^{2^k} + (2-\sqrt{3})^{2^k})^2 - 2 \\
&= ((2+\sqrt{3})^{2^k})^2 + 2 \cdot (2+\sqrt{3})^{2^k} \cdot (2-\sqrt{3})^{2^k} + ((2-\sqrt{3})^{2^k})^2 - 2 \\
&= (2+\sqrt{3})^{2^{k+1}} + (2-\sqrt{3})^{2^{k+1}}.
\end{aligned}$$

Suponha por absurdo que $M_n|(2+\sqrt{3})^{2^{n-2}}+(2-\sqrt{3})^{2^{n-2}}$ e que $M_n$ seja composto, com um fator primo $q$ com $q^2 < M_n$. Teremos $(2+\sqrt{3})^{2^{n-2}}+(2-\sqrt{3})^{2^{n-2}} \equiv 0 \pmod q$ donde, no grupo multiplicativo $G = (\mathbb{Z}/(q)[\sqrt{3}])^*$, temos $(2+\sqrt{3})^{2^{n-2}} = -(2-\sqrt{3})^{2^{n-2}}$. Como $2-\sqrt{3} = (2+\sqrt{3})^{-1}$ esta equação pode ser reescrita como $(2+\sqrt{3})^{2^{n-1}} = -1$ (ainda em $G$), o que significa que a ordem de $2+\sqrt{3}$ em $G$ é exatamente $2^n$. Isto é um absurdo, pois o número de elementos de $G$ é apenas $q^2-1 < 2^n$. Fica portanto demonstrado que se $S_{n-2}$ é múltiplo de $M_n$ então $M_n$ é primo.

Suponha agora $M_n$ primo, $n > 2$. Lembramos que $n$ é um primo ímpar. Por reciprocidade quadrática temos $(\frac{3}{M_n}) = -(\frac{M_n}{3}) = -1$, pois $3 \equiv M_n \equiv -1 \pmod 4$ e $M_n \equiv 1 \pmod 3$. Assim, 3 não é um quadrado em $\mathbb{Z}/(M_p)$ e $K = \mathbb{Z}/(M_p)[\sqrt{3}]$ é um corpo de ordem $M_n^2$. Além disso, $3^{\frac{m_n-1}{2}} = (\frac{3}{M_n}) = -1$ em $K$. Queremos provar que $(2+\sqrt{3})^{2^{n-2}} + (2-\sqrt{3})^{2^{n-2}} \equiv 0$ $(\bmod\ M)_p$, ou seja, que é igual a 0 em $K$. Isto equivale a demonstrarmos que temos $(2+\sqrt{3})^{2^{n-2}} = -(2-\sqrt{3})^{2^{n-2}}$ em $K$, o que pode ser reescrito como $(2+\sqrt{3})^{2^{n-1}} = -1$; devemos portanto provar que a ordem de $2+\sqrt{3}$ é exatamente $2^n$. Note que $2^n = M_n + 1$ donde $(2+\sqrt{3})^{2^n} = (2+\sqrt{3})^{M_n}(2+\sqrt{3}) = (2-\sqrt{3})(2+\sqrt{3}) = 1$ (note que, em $K$, $(2+\sqrt{3})^{M_n} = (2^{M_n}+\sqrt{3})^{M_n} = 2 + 3^{\frac{M_n-1}{2}} \cdot \sqrt{3} = 2-\sqrt{3}$); assim é claro que a ordem de $2+\sqrt{3}$ é um divisor de $2^n$.

Como $K^*$ tem $M_n^2 - 1 = 2^{n+1}(2^{n-1}-1)$ elementos, devemos provar que $2+\sqrt{3}$ não é uma quarta potência em $K$. Note que $(2+\sqrt{3})^{2^n} = 1$ demonstra que $2+\sqrt{3}$ é um quadrado, o que aliás pode ser visto mais diretamente: $2+\sqrt{3} = (1+\sqrt{3})^2/2$ e $2 = 2^{n+1} = 2^{(n+1)^2}$ é uma quarta potência em $K$. Resta-nos assim demonstrar que $\pm(1+\sqrt{3})$ não são quadrados em $K$. Suponha por absurdo que $\epsilon(1+\sqrt{3}) = (a+b\sqrt{3})^2$, com $\epsilon = \pm 1$; temos $\epsilon(1-\sqrt{3}) = (a-b\sqrt{3})^2$ e, multiplicando, $-2 = (a^2-3b^2)^2$, o que significa que $-2$ é um quadrado módulo $M_n$ (pois $a$ e $b$ são inteiros). Isto, entretanto, é claramente falso: $(\frac{-2}{M_n}) = (\frac{-1}{M_n})(\frac{2}{M_n}) = -1 \cdot 1 = -1$, pois $M_n \equiv 3 \pmod 4$ e já vimos que 2 é um quadrado módulo $M_p$. Isto conclui a demonstração.

$\blacksquare$

Mesmo quando $M_p$ não é primo, podemos garantir que seus fatores primos serão de certas formas especiais. Isto é muito útil quando procuramos primos de Mersenne pois podemos eliminar alguns expoentes encontrando fatores primos de $M_p$. Isto também pode ser útil para conjecturarmos quanto à "probabilidade" de $M_p$ ser primo, ou, mais precisamente, quanto à distribuição dos primos de Mersenne.

**Proposição 5.5:** *Sejam $p > 2$ e $q$ primos com $q$ um divisor de $M_p$. Então $q \equiv 1 \pmod{p}$ e $q \equiv \pm 1 \pmod{8}$.*

**Dem:** Se $q$ divide $M_p$ então $2^p \equiv 1 \pmod{q}$, o que significa que a ordem de 2 módulo $q$ é $p$ (pois $p$ é primo). Isto significa que $p$ é um divisor de $q-1$, ou seja, que $q \equiv 1 \pmod{p}$. Por outro lado, $2 \equiv 2^{p+1} = (2^{(p+1)/2})^2 \pmod{q}$, donde $\left(\frac{2}{q}\right) = 1$, o que significa que $q \equiv \pm 1 \pmod{8}$. ∎

Os vários valores de $p$ para os quais a primalidade de $M_p$ foi testada sugerem que para a ampla maioria dos valores de $p$, $M_p$ *não* é primo. Isto é apenas uma conjectura: não se sabe demonstrar sequer que existem infinitos primos $p$ para os quais $M_p$ seja composto. Vamos agora ver uma proposição que serve para garantir que para certos valores especiais de $p$, alguns muito grandes, $M_p$ *não* é primo.

**Proposição 5.6:** *Seja $p$ primo, $p \equiv 3 \pmod{4}$. Então $2p+1$ é primo se e somente se $2p+1$ divide $M_p$.*

**Dem:** Se $q$ é primo então $M_p = 2^p - 1 = 2^{(q-1)/2} - 1 \equiv \left(\frac{2}{q}\right) - 1 \pmod{q}$. Mas $p \equiv 3 \pmod{4}$ significa que $q \equiv 7 \pmod{8}$, donde $\left(\frac{2}{q}\right) = 1$. Assim, $M_p \equiv 0 \pmod{q}$, o que demonstra uma das implicações da proposição.

Por outro lado, se $2p+1$ não é primo tem fatores primos $r$ com $r \not\equiv 1 \pmod{p}$ (pois $r < p$). Se $2p+1$ dividisse $M_p$, $r$ seria um fator primo de $M_p$, contrariando a proposição anterior. ∎

Os primos $p$ para os quais $2p+1$ é primo são chamados de *primos de Sophie Germain*. Alguns primos de Sophie Germain bastante grandes são conhecidos, como $p_0 = 18458709 \cdot 2^{32611} - 1$; assim, pela proposição anterior, $M_{p_0}$ é composto. Sabe-se também que se $\pi_{\mathrm{SG}}(x)$ denota o número de primos de Sophie Germain menores do que $x$ então existe $C$ tal que para todo $x$

$$\pi_{\mathrm{SG}}(x) < C \frac{x}{(\log x)^2}.$$

Acredita-se que $\pi_{\mathrm{SG}}(x)$ seja assintótico a $cx/(\log x)^2$ para algum $c > 0$ mas não se sabe demonstrar sequer que existem infinitos primos de Sophie Germain.

# PARTE II

# APROXIMAÇÕES DIOFANTINAS

# CAPÍTULO 3

## Frações Contínuas, Representações de Números e Aproximações

## Introdução

A teoria de frações contínuas é um dos mais belos temas da matemática elementar, sendo ainda hoje assunto de pesquisa recente (incluindo a do autor destas linhas). O objetivo deste artigo é servir como referência didática em português a nível secundário sobre o assunto.

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 no ensino secundário. 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 $k \in \mathbb{Z}$ $(k = [x])$ tal que $0 \leq x - k < 1$. Podemos escrever a representação decimal de $x - k = 0, a_1 a_2 \dots a_n \dots$, $\quad a_i \in \{0, 1, \dots, 9\}$, o que significa que se $r_n = a_n + 10 \cdot a_{n-1} + 100 \cdot a_{n-2} + \dots + 10^{n-1} \cdot a_1$, então $\dfrac{r_n}{10^n} \leq x - k < \dfrac{r_n + 1}{10^n}$, e portanto $k + \dfrac{r_n}{10^n}$ é uma boa aproximação racional de $x$, no sentido que o erro $\left| x - \left(k + \dfrac{r_n}{10^n}\right) \right|$ é menor que $\dfrac{1}{10^n}$, que é um número bem pequeno se $n$ for grande. A representação decimal de um número real fornece pois uma seqüência de aproximações por racionais cujos denominadores são potências de 10.

Dado qualquer $x \in \mathbb{R}$ e $q$ natural não nulo existe $p \in \mathbb{Z}$ tal que $\dfrac{p}{q} \leq x < \dfrac{p+1}{q}$, e portanto $\left| x - \dfrac{p}{q} \right| < \dfrac{1}{q}$ e $\left| x - \dfrac{p+1}{q} \right| \leq \dfrac{1}{q}$. Em particular há aproximações de $x$ por racionais com denominador $q$ com erro menor que $\dfrac{1}{q}$. 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 freqüentemente aproximações racionais de $x$ muito mais eficientes do que as que exibe. Por exemplo,

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

mostram que $\dfrac{22}{7}$ e $\dfrac{355}{113}$ são melhores aproximações de $\pi$ que aproximações decimais com denominadores muito maiores, e de fato são aproximações muito mais espetaculares do que se podia esperar.

O objetivo deste artigo é apresentar uma outra maneira de representar números reais, que sempre fornece aproximações racionais surpreendentemente boas, e de fato fornece todas essas aproximações excepcionalmente boas, além de ser natural e conceitualmente simples: a representação por frações contínuas.

Dado $x \in \mathbb{R}$, definimos $[x]$ como o único inteiro tal que $[x] \leq x < [x] + 1$. Definimos recursivamente

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

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

$$x = \alpha_0 = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_n}}} =: [a_0; a_1, a_2, \ldots, a_n].$$

Senão denotamos

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots}} =: [a_0; a_1, a_2, \ldots].$$

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

*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 $e^{\pi^2/12\ln 2} = 3,27582291872\ldots$ (meu número real preferido!) e $\sqrt[n]{\left|x - \frac{p_n}{q_n}\right|}$ converge a $e^{-\pi^2/6\ln 2} = 0,093187822954\ldots$.

**Observação**: Os $\alpha_n$ (como funções de $x$) são funções distintas do tipo $\dfrac{ax+b}{cx+d}$ com $a, b, c, d$ inteiros. Se a fração contínua de $x$ é periódica, ou seja, se $\alpha_{n+k} = \alpha_n$, $n \in \mathbb{N}$, $k \in \mathbb{N}^*$, então $x$ será raiz de uma equação do segundo grau com coeficientes inteiros, ou seja, será um irracional da forma $r + \sqrt{s}$, $r, s \in \mathbb{Q}$. A recíproca é verdadeira (de fato já foi enunciada no artigo de José Paulo Carneiro na RPN, ver referências), mas sua prova é mais difícil, e será apresentada no Apêndice.

Se $x \in \mathbb{Q}$, sua representação será finita, e seus coeficientes $a_n$ vêm do algoritmo de Euclides:

$$\begin{array}{llll} x = \dfrac{p}{q}, & q > 0 & p = a_0 q + r_0 & 0 \leq r_0 < q \\ & & q = a_1 r_0 + r_1 & 0 \leq r_1 < r_0 \\ & & r_0 = a_2 r_1 + r_2 & 0 \leq r_2 < r_1 \\ & & \vdots & \vdots \\ & & r_{n-2} = a_n r_{n-1} & \end{array}$$

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.

# 1 Reduzidas e boas aproximações

Seja $x = [a_0; a_1, a_2, \ldots]$. Sejam $p_n \in \mathbb{Z}$, $q_n \in \mathbb{N}^*$ primos entre si tais que $\dfrac{p_n}{q_n} = [a_0; a_1, a_2, \ldots, a_n]$, $n \geq 0$. O seguinte resultado será fundamental no que seguirá.

**Proposição 1.1:** $(p_n)$ e $(q_n)$ satisfazem a recorrência $p_{n+2} = a_{n+2} p_{n+1} + p_n$, e $q_{n+2} = a_{n+2} q_{n+1} + q_n$, para todo $n \geq 0$. Temos ainda $p_0 = a_0$, $p_1 = a_0 a_1 + 1$, $q_0 = 1$, $q_1 = a_1$.

Além disso, $p_{n+1}\,q_n - p_n\,q_{n+1} = (-1)^n$, $\forall\, n \geq 0$.

**Dem:** Por indução em $n$, provaremos que se $t_k > 0$, para $k > 1$ então $[t_0; t_1, t_2, \ldots, t_n] = \dfrac{x_k}{y_k}$ onde as seqüências $(x_m)$ e $(y_m)$ são definidas por $x_0 = t_0$, $y_0 = 1$, $x_1 = t_0 t_1 + 1$, $y_1 = t_0$ $x_{n+2} = t_{n+2}\,x_{n+1} + x_n$, $y_{n+2} = t_{n+2}\,y_{n+1} + y_n$, $\forall\, n$. Suponha que a afirmação seja válida para $k = n$. Para $k = n + 1$ temos

$$[t_0; t_1, t_2, \ldots, t_n, t_{n+1}] = [t_0; t_1, t_2, \ldots, t_n + \frac{1}{t_{n+1}}] =$$

$$= \frac{(t_n + \frac{1}{t_{n+1}})x_{n-1} + x_{n-2}}{(t_n + \frac{1}{t_{n+1}})y_{n-1} + y_{n-2}} = \frac{t_{n+1}(t_n x_{n-1} + x_{n-2}) + x_{n-1}}{t_{n+1}(t_n y_{n-1} + y_{n-2}) + y_{n-1}} = \frac{t_{n+1}x_n + x_{n-1}}{t_{n+1}y_n + y_{n-1}}\ .$$

Por outro lado as igualdades

- $p_1 q_0 - p_0 q_1 = (a_0 a_1 + 1) - a_0 a_1 = 1$
- $p_{n+2}q_{n+1} - p_{n+1}q_{n+2} = (a_{n+2}p_{n+1} + p_n)q_{n+1}$

  $-(a_{n+2}\,q_{n+1} + q_n)p_{n+1} = -(p_{n+1}q_n - p_n q_{n+1})$

mostram que $p_{n+1}\,q_n - p_n\,q_{n+1} = (-1)^n$, $\forall\, n \in \mathbb{N}$, o que implica em particular que os $p_n$ , $q_n$ dados pelas recorrências acima são primos entre si. ■

**Corolário 1.2:** $x = \dfrac{\alpha_n p_{n-1} + p_{n-2}}{\alpha_n q_{n-1} + q_{n-2}}$ e $\alpha_n = \dfrac{p_{n-2} - q_{n-2}\alpha}{q_{n-1}\alpha - p_{n-1}}$, $\forall\, n \in \mathbb{N}$.

**Dem:** A primeira igualdade é conseqüência direta da prova, e a segunda é conseqüência direta da primeira pois $x = [a_0; a_1, a_2, \ldots, a_{n-1}, \alpha_n]$.

Note que as reduzidas de ordem par são menores e as de ordem ímpar maiores que $x = [a_0; a_1, \ldots]$.

**Teorema 1.3:** $\left|x - \dfrac{p_n}{q_n}\right| \leq \dfrac{1}{q_n q_{n+1}} < \dfrac{1}{q_n^2}$, $\forall\, n \in \mathbb{N}$.

Além disso, $\left|x - \dfrac{p_n}{q_n}\right| < \dfrac{1}{2q_n^2}$ ou $\left|x - \dfrac{p_{n+1}}{q_{n+1}}\right| < \dfrac{1}{2q_{n+1}^2}$, $\forall\, n \in \mathbb{N}$.

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

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

Além disso, se
$$\left|x - \frac{p_n}{q_n}\right| \geq \frac{1}{2q_n^2} \text{ e } \left|x - \frac{p_{n+1}}{q_{n+1}}\right| > \frac{1}{2q_{n+1}^2},$$
então
$$\frac{1}{q_n q_{n+1}} = \left|x - \frac{p_n}{q_n}\right| + \left|x - \frac{p_{n+1}}{q_{n+1}}\right| \geq \frac{1}{2q_n^2} + \frac{1}{2q_{n+1}^2} \Rightarrow q_{n+1} = q_n \text{ , absurdo.}$$

■

**Observação**: De fato $\left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} < \frac{1}{a_{n+1}q_n^2}$. Quanto maior for $a_{n+1}$ melhor será a aproximação $\frac{p_n}{q_n}$ de $x$. O próximo resultado nos dá explicitamente o erro da aproximação de $x$ por $\frac{p_n}{q_n}$.

**Proposição 1.4:**
$$x - \frac{p_n}{q_n} = \frac{(-1)^n}{(\alpha_{n+1} + \beta_{n+1})q_n^2}, \text{ onde } \beta_{n+1} = \frac{q_{n-1}}{q_n} = [0; a_n, a_{n-1}, a_{n-2}, \ldots, a_1].$$

**Dem:** Temos $\alpha_{n+1} = \frac{p_{n-1} - q_{n-1}x}{q_n x - p_n}$. Portanto,
$$\alpha_{n+1} + \beta_{n+1} = \frac{p_{n-1} - q_{n-1}x}{q_n x - p_n} + \frac{q_{n-1}}{q_n} = \frac{p_{n-1}q_n - p_n q_{n-1}}{q_n(q_n x - p_n)} = \frac{(-1)^n}{q_n(q_n x - p_n)} \Rightarrow x - \frac{p_n}{q_n} =$$
$$= \frac{q_n(q_n x - p_n)}{q_n^2} = \frac{(-1)^n}{(\alpha_{n+1} + \beta_{n+1})q_n^2}.$$

■

Como aplicação podemos provar o seguinte.

**Teorema 1.5:** (Hurwitz, Markov). Para todo $\alpha$ irracional, $n \geq 1$ 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 $\left|\alpha - \frac{p}{q}\right| < \frac{1}{\sqrt{5}q^2}$ tem infinitas soluções racionais $p/q$.

**Dem:** Suponha que o teorema seja falso. Então existe $\alpha$ irracional, $n \geq 1$ com $\alpha_n + \beta_n \leq \sqrt{5}$, $\alpha_{n+1} + \beta_{n+1} \leq \sqrt{5}$ e $\alpha_{n+2} + \beta_{n+2} \leq 5$. Devemos portanto ter $a_n = a_{n+1} = a_{n+2} = 1$ (todos são claramente no máximo 2, e se algum $a_k$ é igual a 2 com $k \in \{n, n+1, n+2\}$, teríamos $a_k + \beta_k \geq 2 + \frac{1}{3} > \sqrt{5}$, absurdo.)

Seja $x = 1/\alpha_{n+2}$ e $y = \beta_{n+1}$. As desigualdades acima se traduzem em

$$\frac{1}{1+x} + \frac{1}{y} \leq \sqrt{5}, \;\; 1+x+y \leq \sqrt{5} \text{ e } e\frac{1}{x} + \frac{1}{1+y} \leq \sqrt{5}.$$

Temos

$$1+x+y \leq \sqrt{5} \Rightarrow 1+x \leq \sqrt{5} - y \Rightarrow \frac{1}{1+x} + \frac{1}{y} \geq \frac{1}{\sqrt{5}-y} + \frac{1}{y} = \frac{\sqrt{5}}{y(\sqrt{5}-y)}$$

e portanto $y(\sqrt{5}-y) \geq 1 \Rightarrow y \geq \dfrac{\sqrt{5}-1}{2}\cdot$ Por outro lado temos

$$x \leq \sqrt{5} - 1 - y \Rightarrow \frac{1}{x} + \frac{1}{1+4} \geq \frac{1}{\sqrt{5}-1-y} + \frac{1}{1+4} = \frac{\sqrt{5}}{(1+y)(\sqrt{5}-1-y)}$$

e portanto $(1+y)(\sqrt{5}-1-y) \geq 1 \Rightarrow y \leq \dfrac{\sqrt{5}-1}{2}$, e portanto devemos ter $y = \dfrac{\sqrt{5}-1}{2}$, o que é absurdo pois $y = \beta_{n+1} = \dfrac{q_{n-1}}{q_n} \in \mathbb{Q}$.

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

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

temos

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

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 $\dfrac{1+\sqrt{5}}{2} - \dfrac{p}{q}$ é muito próximo de 0, donde $\left|\dfrac{1+\sqrt{5}}{2} - \dfrac{p}{q} - \sqrt{5}\right| \Big/ (\sqrt{5}+\varepsilon)$ é muito próximo de $\dfrac{\sqrt{5}}{\sqrt{5}+\varepsilon} < 1$, absurdo, pois $|p^2 - pq - q^2| \geq 1$ (de fato $p^2 - pq - q^2$ é um inteiro não nulo, pois se $p^2 - pq - q^2 = 0$ teríamos

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

absurdo, pois $\dfrac{p}{q} \in \mathbb{Q}$.)

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

$$[1; 1, 1, 1, \ldots] + [0; 1.1.1.\ldots] = \frac{1+\sqrt{5}}{2} + \frac{\sqrt{5}-1}{2} = \sqrt{5}.$$

**Exemplos:**

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

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

- $e = [2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, \ldots, 1, 1, 2n, \ldots]$ (isso não é fácil de provar.)

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

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

$$\frac{1+\sqrt{5}}{2} = [1; 1, 1, 1, \ldots] \text{ pois } \frac{1+\sqrt{5}}{2} = 1 + \cfrac{1}{\cfrac{1+\sqrt{5}}{2}} = 1 + \cfrac{1}{1 + \cfrac{1}{\cfrac{1+\sqrt{5}}{2}}} = \cdots$$

  Isto prova em particular que $\sqrt{2}$ e $\dfrac{1+\sqrt{5}}{2}$ são irracionais, pois sua fração contínua é infinita.

## 2 Boas aproximações são reduzidas

O próximo teorema (e seu Corolário 2) caracteriza as reduzidas em termo do erro reduzido da aproximação de $x$ por $p/q$, o qual é, por definição, a razão entre $|x - p/q|$ e o erro máximo da aproximação por falta com denominador $q$, que é $1/q$. Assim, o erro reduzido da aproximação de $x$ por $p/q$ é $|qx-p|$.

**Teorema 2.1:** $|q_n x - p_n| < |qx-p|$, $\forall\, p,q \in \mathbb{Z}$, $0 < q < q_n$ $\dfrac{p}{q} \neq \dfrac{p_n}{q_n}$·. Além disso, $|q_n x - p_n| \le |qx-p|$, $\forall\, p,q \in \mathbb{Z}$, $0 < q < q_{n+1}$.

**Dem:** $\left|\dfrac{p}{q} - \dfrac{p_n}{q_n}\right| \ge \dfrac{1}{qq_n} > \dfrac{1}{q_n q_{n+1}}$ se $q < q_{n+1}$, e assim $\dfrac{p}{q}$ está fora do intervalo $\left(\dfrac{p_n}{q_n}, \frac{p_{n+1}}{q_{n+1}}\right)$. Portanto

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

Além disso, se vale a igualdade, então $x = \dfrac{p_{n+1}}{q_{n+1}}$, donde $a_{n+1} \ge 2$, 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

$$\left|x-\frac{p}{q}\right| \ge \left|x-\frac{p_n}{q_n}\right| - \left|\frac{p_{n+1}}{q_{n+1}}-\frac{p_n}{q_n}\right| \ge \frac{1}{qq_n} - \frac{1}{q_n q_{n+1}} = \frac{q_{n+1}-q}{qq_nq_{n+1}}$$
$$> \frac{1}{qq_{n+1}} \Rightarrow |qx-p| > \frac{1}{q_{n+1}} \ge |q_n x - p_n|.$$

**Corolário 2.2:** $\left|x-\dfrac{p_n}{q_n}\right| < \left|x-\dfrac{p}{q}\right|$, $\forall\, q < q_n$.

**Corolário 2.3:** Se $|qx-p| < |q'x-p'|$, $\forall\, q' \le q$, $\dfrac{p}{q} \neq \dfrac{q'}{q'}$ então $p/q$ é uma reduzida da fração contínua de $x$.

**Dem:** Tome $n$ tal que $q_n \le q < q_{n+1}$.

Teremos $|q_n x - p_n| \le |qx-p|$, e portanto $p/q = p_n/q_n$. ∎

**Teorema 2.4:** Se $\left|x-\dfrac{p}{q}\right| < \dfrac{1}{2q^2}$ então $\dfrac{p}{q}$ é uma reduzida da fração contínua de $x$.

**Dem:** Seja $n$ tal que $q_n < q \le q_{n+1}$. Suponha que $\dfrac{p}{q} \neq \dfrac{p_{n+1}}{q_{n+1}}$. Então, temos duas possibilidades:

a) $\quad q \geq \dfrac{q_{n+1}}{2} \Rightarrow \left| x - \dfrac{p}{q} \right| \geq \dfrac{1}{q q_{n+1}} \geq \dfrac{1}{2q^2}$.

b) $\quad q < \dfrac{q_{n+1}}{2} \Rightarrow q_{n+1} > 2q_n \Rightarrow \left| x - \dfrac{p}{q} \right| \geq \left| \dfrac{p_n}{q_n} - \dfrac{p}{q} \right| - \left| \dfrac{p_{nm}}{q_{nm}} - \dfrac{p_n}{q_n} \right| \geq \dfrac{1}{q q_n} - \dfrac{1}{q_n q_{n+1}} =$
$\dfrac{q_{n+1} - q}{q q_n q_{n+1}} > \frac{1}{2qq_n} > \frac{1}{2q^2}$.

# 3 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

$$\alpha_0 = x, \quad a_n = [\alpha_n], \quad \alpha_{n+1} = \frac{1}{\alpha_n - a_n}.$$

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 $\alpha_{n+k} = \alpha_n$ , $n \in \mathbb{N}$, $k \in \mathbb{N}^*$ então

$$\begin{aligned} &\frac{p_{n-2} - q_{n-2}x}{q_{n-1}x - p_{n-1}} = \frac{p_{n+k-2} - q_{n+k-2}x}{q_{n+k-1}x - p_{n+k-1}} \quad \Rightarrow (q_{n-1}\, q_{n+k-2} - q_{n-2}\, q_{n+k-1})x^2 \\ &+ (p_{n+k-1}\, q_{n-2} + p_{n-2}\, q_{n+k-1} - p_{n+k-2}\, q_{n-1} - p_{n-1}\, q_{n+k-2})x \\ &+ p_{n-1}\, p_{n+k-2} - p_{n-2}\, p_{n+k-1} = 0. \end{aligned}$$

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

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 $n \in \mathbb{N}$, $k \in \mathbb{N}^*$ 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 vimos na seção 1,

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

e portanto

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

onde

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

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

$$A_n=a\,p_{n-1}^2+b\,p_{n-1}q_{n-1}+c\,q_{n-1}^2=a\,q_{n-1}^2\left(x-\frac{p_{n-1}}{q_{n-1}}\right)\left(\bar{x}-\frac{p_{n-1}}{q_{n-1}}\right),$$

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

$$\begin{aligned} \left|x-\frac{p_{n-1}}{q_{n-1}}\right|<\frac{1}{q_{n-1}^2}\le 1 \Rightarrow |A_n| &= a\,q_{n-1}^2\left|x-\frac{p_{n-1}}{q_{n-1}}\right|\,\left|\bar{x}-\frac{p_{n-1}}{q_{n-1}}\right|\\ &\le a\left(|\bar{x}-x|+\left|x-\frac{p_{n-1}}{q_{n-1}}\right|\right)\le a(|\bar{x}-x|+1)=:M. \end{aligned}$$

Notemos agora que $B_n^2-4A_nC_n=b^2-4ac,\ \ \forall\, n\in\mathbb{N}$. De fato, $B_n^2-4A_nC_n=(p_{n-1}q_{n-2}-p_{n-2}q_{n-1})^2(b^2-4ac)=b^2-4ac$. Portanto, $B_n^2\le 4A_nC_n+b^2-4ac=4M^2+b^2-4ac\Rightarrow B_n\le M'=\sqrt{4M^2+b^2-4ac},\quad \forall\, n\in\mathbb{N}$.

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 $n\in\mathbb{N}$, $k\in\mathbb{N}^*$.

**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 3.1:** 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

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

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

**Dem:** 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

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

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. ■

# CAPÍTULO 4

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

### 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 $0 \le j \le N$. 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 $0 < |q\alpha - p| < \frac{1}{N} \Rightarrow |\alpha - \frac{p}{q}| < \frac{1}{qN} \le \frac{1}{q^2}$). 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 ([Ma]) 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 artigo, 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. As definições e provas dos resultados a seguir sobre frações contínuas podem ser encontradas em [Mo].

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

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

Temos

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

As seqüências $p_n$ e $q_n$ satisfazem $p_{n+1}q_n - p_n q_{n+1} = (-1)^n$, $\forall\, n \geq 0$. 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 $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{R}$ queremos encontrar números racionais $\frac{p_1}{q}, \frac{p_2}{q}, \ldots, \frac{p_n}{q}$ tais que $|\alpha_j - \frac{p_j}{q}|$ seja pequeno para todo $j \leq n$. 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

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

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 $|\alpha_j - \frac{p_j}{q_j}| < \frac{1}{Nq_j} \leq \frac{1}{q_j^{1+1/n}}$, para todo $j \leq n$.

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 [C1] e [S].

# 1 O Teorema de Khintchine via frações contínuas

**Teorema 1.1:** (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:** 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 [C2]).

**Dem:**

**Lema 1.2:** *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 $2/k(k+1)$, $\forall\ k_1, k_2, \dots, k_n \in \mathbb{N}^*$.*

**Dem:** Sejam $p_{n-1}/q_{n-1} = [0; a_1, a_2, \dots, a_{n-1}]$ e $p_n/q_n = [0; a_1, a_2, \dots, a_{n-1}, a_n]$. 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 $|p_nq_{n-1} - p_{n-1}q_n| = 1$), 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 1.3:** A probabilidade de $a_{n+1} \geq k$, nos termos do Lema acima, pertence a $[1/(k+1), 2/k]$.

**Lema 1.4:** *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 1.4 vamos mostrar como termina a prova do Teorema de Khintchine. 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 1.4:** 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 $\lim\limits_{n\to\infty} 8 \log n/\sqrt[3]{n} = 0$, 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:** 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 O Teorema de Khintchine $n$-dimensional

**Teorema 2.1:** Sejam $f_1, f_2, \dots, f_n\colon \mathbb{N} \to \mathbb{R}^+$ funções decrescentes e $F\colon \mathbb{N} \to \mathbb{R}^+$ dada por $F(k) = f_1(k)f_2(k)\dots f_n(k)$. Seja $\alpha = (\alpha_1, \dots, \alpha_2, \dots, \alpha_n) \in \mathbb{R}^n$. O sistema de aproximação simultâneas

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

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

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

**Dem:**

**Dem. de a):** Dado $q_0 \in \mathbb{N}$, consideremos o conjunto

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

que é o conjunto dos $\alpha \in [0,1)^n$ tais que a desigualdade (*) do enunciado do Teorema tem alguma solução com $q \ge q_0$ (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 $(\frac{p_i}{q}, \dots, \frac{p_n}{q}) \in \mathbb{Q}^n$). Temos $m(S(q_0)) \le \sum_{q=q_0}^{\infty} q^n (\frac{2^n F(q)}{q^n}) = 2^n \sum_{q=q_0}^{\infty} F(q)$, que tende a 0 quando $q$ tende a $\infty$, pois $\sum_{q=1}^{\infty} F(q)$ converge. Portanto, $m(\bigcap_{q_0 \in \mathbb{N}} S(q_0)) = 0$.

**Dem. de b):** Primeiro obtemos funções decrescentes $g_1, g_2, \dots, g_n\colon \mathbb{N} \to \mathbb{R}^+$ tais que $\lim\limits_{q \to s_0} \frac{g_i(q)}{f_i(q)} = 0$ e $G = g_1, g_2, \dots, g_n\colon \mathbb{N} \to \mathbb{R}^+$ satisfaz $\lim\limits_{q \to \infty} qG(q) = 0$ e $\sum_{q=1}^{\infty} G(q) = +\infty$ (podemos tomar $G_1(k) = (F(1) + F(2) + \dots + F(k))^{-1} \cdot F(k)$ e $G(k) = (G_1(1) + G_1(2) + \dots + G_1(k))^{-1} G_1(k)$, $\forall\, k \in \mathbb{N}$. Teremos $G_1$ e $G$ decrescentes, $G_1(k) \le 1/k$, $kG(k) \to 0$, $\Sigma G_1(k) = \infty$, $\Sigma G(k) = \infty$, 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 $s_0 = s_0(q_0) = \min\{s \in \mathbb{N} | G(q_0) + G(q_0+1) + \dots + G(s) \ge \tilde{c}\}$, 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 $q_0 \le s \le s_0$ 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 $r_i \in \mathbb{Z}$, $1 \le i \le n$, $0 \le r_i < s$ tais que existem $q$ com $q_0 \le q < s$, $p_1, p_2, \ldots, p_n \in \mathbb{Z}$, $0 \le p_i < q$ 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

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

Para um tal $\left(\frac{r_1}{s}, \ldots, \frac{r_n}{s}\right)$ que não satisfaz (**) para nenhum $q$ com $q_0 \le q < s$, $p_1, \ldots, p_n$ 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 $q_0 \le q < s$, $\forall\, p_1, \ldots, p_n \in \mathbb{Z}$ com $0 \le p_i < q$.

**Lema 2.2:** Para todo $k \in \mathbb{N}$ existe $c_k > 0$ tal que $\sum_{j=1}^{n}\left(\frac{\varphi(j)}{j}\right)^k \ge c_k n$.

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

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

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 $k \ge 1$, temos $\frac{1}{n}\sum_{j=1}^{n}\left(\frac{\varphi(j)}{j}\right)^k \ge \left(\frac{1}{n}\sum_{j=1}^{n}\frac{\varphi(j)}{j}\right)^k$, donde segue o resultado (com $C_k = \left(\frac{6}{\pi^2}\right)^k$).

■

Se $q_0 \le q < s$, o número de soluções de $|r_i q - p_i s| < 2sg_i(q)$ com $0 \le p_i < q$, $0 \le r_i < s$ é no máximo $4sg_i(q)$ desde que $\text{mdc}(r_i, s) = 1$. De fato, nessas condições $r_i q - p_i s$ não se anula, senão teríamos $\frac{p_i}{q} = \frac{r_i}{s}$, que é uma fração irredutível de denominador $s > q$, absurdo. Seja $d = \text{mdc}(s, q)$. Dado $k \in \mathbb{Z}$, a equação diofantina $rq - ps = k$ só tem solução de $d|k$, quando tem $d$ soluções com $0 \le r < s$. Portanto, $0 < rq - ps < x$ (resp. $-x < rq - ps < 0$) tem no máximo $d\lfloor\frac{x}{d}\rfloor \le x$ soluções $(p, r)$ com $0 \le r < s$, o que claramente implica a afirmação.

Portanto, o número de soluções da desigualdade acima para todo $i$ com $1 \le i \le n$ é no máximo $4^n s^n G(q)$. Por outro lado há $\varphi(s)^n$ pontos $\left(\frac{r_i}{s}, \dots, \frac{r_n}{s}\right)$, $0 \le r_i < s$, $\mathrm{mdc}(r_i, s) = 1$, $1 \le i \le n$. Isso nos dá a estimativa do número de novos blocos disjuntos dos anteriormente considerados que têm denominador $s$ de pelo menos $\varphi(s)^n - 4^n s^n \sum_{q=q_0}^{s-1} G(q)$, e para o volume da união dos blocos disjuntos adicionados até o denominador $s_0$ de pelo menos

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

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

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

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

Por outro lado, $8^n \sum_{s=q_0}^{s_0}\left(\sum_{q=q_0}^{s-1} G(q)\right) G(s) \le 8^n \tilde{c} \sum_{s=q_0}^{s_0} G(s) \le 8^n \tilde{c}(\tilde{c} + \varepsilon_2)$ 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

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

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

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

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 $|\alpha_i - \frac{r_i}{q}| < \frac{Cg_i(q)}{q}$ (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). ∎

# Apêndice: Aproximações diofantinas não-homogêneas

**Proposição A.1:** Se $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ então $X = \{m + n\alpha | m, n \in \mathbb{Z}\}$ é denso em $\mathbb{R}$.

**Dem:** 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 A.1 para dimensão qualquer.

**Proposição A.2:** 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 $X = \{k\alpha + m_1e_1 + m_2e_2 + \cdots + m_ne_n | k,\, m_1, \ldots, m_n \in \mathbb{Z}\}$ 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 $\mathbb{R}^n$.

**Dem:** 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 $t\tilde{w} = \lim_{n\to\infty} \lfloor \frac{t}{w_n} \rfloor w_n \in \overline{X}$, $\forall\, n \in \mathbb{N}$. 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. ■

**Observação:** 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.

Deixamos para o leitor a prova do seguinte fato: Dado $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{R}^n$ satisfazendo a condição da Proposição 2, e $m \in \mathbb{N}$, definimos $\{m\alpha\} = (m\alpha_1 - \lfloor m\alpha_1 \rfloor, \ldots, m\alpha_n - \lfloor m\alpha_n \rfloor) \in [0,1)^n$. A seqüência $\{m\alpha\}$ é uniformemente distribuida, isto é, para todo aberto $A \subset [0,1)^n$, se $f_A(k) = \#\{m \leq k | \{m\alpha\} \in A\}$, então $\lim_{k\to\infty} f_A(k)/k = m(A)$, onde $m(A)$ é a medida de Lebesgue de $A$. (*Sugestão*: sejam $C_1, C_2 \subset [0,1)^n$ dois cubos abertos tais que $\overline{C}_2$ está contido em um transladado de $C_1$ ($\overline{C}_2 \subset C_1 + v,\ v \in \mathbb{R}^n$). Use o fato de que existem vetores $\tilde{v}$ arbitrariamente próximos de $v$, com $\tilde{v} = (q\alpha_1 + p_1, \ldots, q\alpha_n + p_n),\ q, p_1, \ldots, p_n \in \mathbb{Z}$, e que $\{m\alpha\} \in C_2 \Rightarrow \{(m-q)\alpha\} \in C_2 - \tilde{v} \subset C_1$, se $\tilde{v}$ está suficientemente próximo de $v$, donde $f_{C_2}(k) \leq f_{C_1}(k) + |q| \Rightarrow \limsup_{k\to\infty} f_{C_2}(k)/k \leq \liminf_{k\to\infty} f_{C_1}(k)/k$).

CAPÍTULO 5

# Os Espectros de Markov e Lagrange

## 1 Definições e enunciados

Seja $\alpha$ um número irracional. De acordo com o teorema de Dirichlet, a desigualdade $\left|\alpha - \dfrac{p}{q}\right| < \dfrac{1}{q^2}$ tem uma infinidade de soluções racionais $p/q$. Markov e Hurwitz melhoraram este resultado, provando que, para todo irracional $\alpha$, a desigualdade $\left|\alpha - \dfrac{p}{q}\right| < \dfrac{1}{\sqrt{5}\cdot q^2}$ tem uma infinidade de soluções racionais, e que $\sqrt{5}$ é a melhor constante com esta propriedade: para $\alpha = \dfrac{1+\sqrt{5}}{2}$, e para qualquer $\varepsilon > 0$, a desigualdade $\left|\alpha - \dfrac{p}{q}\right| < \dfrac{1}{(\sqrt{5}+\varepsilon)q^2}$ 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 $k(\alpha) = \sup\{k > 0 \mid \left|\alpha - \dfrac{p}{q}\right| < \dfrac{1}{kq^2}$ 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 $k\left(\dfrac{1+\sqrt{5}}{2}\right) = \sqrt{5}$. 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 $L = \{k(\alpha) \mid \alpha \in \mathbb{R}\backslash\mathbb{Z}$ 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 $k_f(\alpha) := \sup\big\{k > 0 \mid |\alpha - \dfrac{p}{q}| < \dfrac{f(q)}{k}$ tem infinitas soluções racionais $p/q\big\}$ 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 [Ma]) que $L\cap(-\infty,3)=\{k_1=\sqrt{5}<k_2=2\sqrt{2}<k_3=\dfrac{\sqrt{221}}{5}<\cdots\}$, 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 $\left[4+\dfrac{253589820+283748\sqrt{462}}{491993569},+\infty\right)$. 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 $f((a_n)_{n\in\mathbb{Z}})=\alpha_0+\beta_0=[a_0,a_1,a_2,\dots]+[0;a_{-1},a_{-2},\dots]$ 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 [M2] os seguintes resultados, que pretendemos discutir neste capítulo:

**Teorema 1.1:** 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:

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

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

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

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

(As afirmações iii) e iv) são conseqüências simples de ii)).

**Teorema 1.2:** O conjunto dos pontos de acumulação de $L$ é perfeito, isto é, $L' = L''$.

**Teorema 1.3:** $0 < HD(M \backslash L) < 1$.

Estes teoremas são baseados na idéia 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, que será discutido na próxima seção, e cuja prova depende do lema de recorrência de escala de [MY].

# 2 Dimensões de Hausdorff e somas aritméticas de conjuntos de Cantor de frações contínuas

Vimos no capítulo anterior que, se $K_1$ e $K_2$ são conjuntos de Cantor $C^2$ que satisfazem as hipóteses do lema de recorrência de escalas, então vale a fórmula $HD(K_1+K_2) = \min\{1, HD(K_1)+HD(K_2)\}$.

Iremos aplicar este resultado a conjuntos de Cantor regulares definidos por restrições da função de Gauss $g\colon (0,1] \to (0,1]$ definida por $g(x) = \dfrac{1}{x} - \lfloor \dfrac{1}{x} \rfloor$ (cuja relação com frações contínuas é evidente) a determinados domínios de Markov (que serão uniões finitas de intervalos cujos extremos serão irracionalidades quadráticas). Para isso, precisamos provar que tais conjuntos de Cantor satisfazem as hipóteses do lema de recorrência de escalas, isto é, que não são essencialmente afins.

Observemos inicialmente que qualquer conjunto de Cantor regular de Gauss (nome que atribuiremos aos conjuntos de Cantor descritos no parágrafo anterior) contém um conjunto de Cantor *completo* de Gauss, nome que atribuímos ao seguinte tipo de conjunto de Cantor: A cada conjunto finito de seqüências finitas de inteiros positivos $B$ associamos o conjunto $K(B) = \{[0; \beta_1, \beta_2, \ldots] \mid \beta_i \in B,\ \forall\, i \in \mathbb{N}\}$, que, excetuando os casos triviais onde $K(B)$ é um ponto, é um conjunto de Cantor regular completo de Gauss. Este fato pode ser provado do seguinte mod: tomamos duas palavras finitas admissíveis $\gamma_1 = b_1 b_2 \ldots b_n b_1$ e $\gamma_2 = b_1 \tilde{b}_2 \tilde{b}_3 \ldots \tilde{b}_m b_1$ começando e terminado em $b_1$ que não sejam ambas cópias múltiplas do mesmo bloco de símbolos (aqui os símbolos $b_i$ são inteiros positivos corespondentes a ramos $\dfrac{1}{x} - b_i$ da função de Gauss $g$, que aparecem na construção do Cantor regular de Gauss em questão $K$). Se $\tilde{\gamma}_1 = b_1 b_2 \ldots b_n$ e $\tilde{\gamma}_2 = b_1 \tilde{b}_2 \ldots \tilde{b}_m$ então o Cantor completo de Gauss $K(\{\tilde{\gamma}_1, \tilde{\gamma}_2\})$ está contido em $K$.

Basta provar agora que nenhum Cantor completo de Gauss é essencialmente afim. Observemos que $K(B)$ é definido por $\psi\colon \bigcup_{\beta \in B} I_\beta \to I$, onde $I = [0,1]$ e, para cada $\beta \in B$, $I_\beta = \{[0; \beta, \alpha], \alpha \geq 1\}$ e $\psi_\beta = \psi|_{I_\beta}$ é o iterado de $g$ definido por $\psi_\beta([0; \beta, \alpha]) = 1/\alpha$.

Seja $x_\beta = [0; \beta, \beta, \beta, \ldots]$ o ponto fixo de $\psi_\beta$. Se $\beta = (b_1, b_2, \ldots, b_n)$ e $p_k/q_k = [0; b_1, b_2, \ldots, b_k]$ são as reduzidas de $[0; \beta]$, então $\psi_\beta(x) = \dfrac{q_{n-1}x - p_{n-1}}{p_n - q_n x}$, e os pontos fixos de $\psi_\beta$ (estendido à reta pela sua fórmula) são as raízes de $q_n x^2 + (q_{n-1} - p_n)x - p_{n-1} = 0$ (ver Seção 3 do Apêndice).

Existe um difeomorfismo $\alpha_\beta\colon I \to I$ tal que $\alpha_\beta(x_\beta) = x_\beta \quad \alpha'_\beta(x_\beta) = 1$ e $\alpha_\beta \circ \psi_\beta \circ \alpha_\beta^{-1}$ é afim. Além disso, podemos tomar um tal $\alpha_\beta$ da forma $\alpha_\beta(x) = \dfrac{a_\beta x + b_\beta}{c_\beta x + d_\beta}$ (isto é um exercício sobre triangularização de matrizes...). Não há perda de generalidade em supor que $B$ contém dois elementos $\beta$ de $\gamma$ do mesmo tamanho (i.e., com o mesmo número de símbolos), pois, se não for esse o caso, podemos considerar etapas mais avançada da construção de $K(B)$ onde hja tais elementos. É suficiente agora mostrar que se $\alpha_\beta \circ \alpha_\varepsilon^{-1}$ é afim e $\gamma$ tem o mesmo número de elementos que $\beta$ então $\gamma = \beta$, pois isso implicaria que $\alpha_\beta \circ \psi_\gamma \circ \alpha_\beta^{-1}$ não é afim, donde é uma transformação da forma $\dfrac{Ax + B}{Cx + D}$, cuja derivada segunda é zero apenas num conjunto finito, ou seja, $\alpha_\beta \circ \psi \circ \alpha_\beta^{-1}$ tem uma componente afim (a de $\psi_\beta$), e outra componente cuja derivada segunda é não-nula em muitos pontos de $K(B)$ (a de $\psi_\gamma$), o que implica que $K(B)$ não é essencialmente afim. Se $\alpha_\beta \circ \psi_\gamma \circ \alpha_\beta^{-1}$ é afim então $\infty$ é um ponto fixo comum de $\alpha_\beta \circ \alpha_\beta^{-1}$ e $\alpha_\beta \circ \psi_\beta \circ \alpha_\beta^{-1}$, e portanto $\alpha_\beta^{-1}(\infty)$ é ponto fixo comum de $\psi_\beta(x) = \dfrac{q_{n-1}x - p_{n-1}}{p_n - q_n x}$ e $\psi_\gamma = \dfrac{\tilde{q}_{n-1}x - \tilde{p}_{n-1}}{\tilde{p}_n - \tilde{q}_n x}$, donde é raiz comum dos polinômios $q_n x^2 + (q_{n-1} - p_n)x - p_{n-1}$ e $\tilde{q}_n x^2 + (\tilde{q}_{n-1} - \tilde{p}_n)x - \tilde{p}_{n-1}$, donde esses dois polinômios são iguais (pois são irredutíveis em $\mathbb{Z}[x]$), donde suas outras raízes coincidem, ou seja, $x_\beta = x_\gamma$ e portanto $\beta = \gamma$.

Provamos assim o seguinte resultado:

**Proposição 2.1:** Se $K_1$ e $K_2$ são conjuntos de Cantor regulares de Gauss então $HD(K_1+K_2) = \min\{1, HD(K_1) + HD(K_2)\}$. ■

Outro fato importante na prova de nossos resultados sobre dimensões de Hausdorff de partes dos espectros de Markov e Lagrange será discutido a seguir:

**Definição 2.2:** Se $\beta = (b_1, b_2, \dots, b_n)$ então $\beta^t = (b_n, b_{n-1}, \dots, b_2, b_1)$, e se $B$ é um conjunto de seqüências finitas então $B^t = \{\beta^t, \beta \in B\}$.

Se $q_n(\beta)$ é o denominador da fração contínua $[0; \beta] = [0, b_1, \dots, b_n]$ então $q_n(\beta) = q_n(\beta^t)$. Este é um fator já conhecido por Euler, e uma boa referência sobre sua prova (que também pode ser considerada como um exercício para o leitor) está no apêndice 2 de [CF]. Como conseqüência deste restulado e do fato de que os comprimentos dos intervalos da construção de um conjunto de Cantor completo de Gauss dependerem essencialmente dos denominadores das frações contínuas finitas envolvidas, prova-se a seguinte

**Proposição 2.3:** $HD(K(B)) = HD(K(B^t))$ para todo conjunto finito $B$ de seqüências finitas de inteiros positivos. ■

**Corolário 2.4:** $HD(K(B) + K(B^t)) = \min\{1, 2 \cdot HD(K(B))\}$. ■

# 3 Idéias das demonstrações dos resultados sobre os espectros

Seja $\Sigma = \mathbb{Z}_+^{\mathbb{Z}}$, $\ell \colon \Sigma \to \mathbb{R}$ definida por $\ell(\underline{\theta}) = \limsup_{n\to\infty} (\alpha_n + \beta_n)$, onde, se $\underline{\theta} = (a_k)_{k\in\mathbb{Z}}$ então $\alpha_n = [a_n; a_{n+1}, a_{n+2}, \dots]$ e $\beta_n = [0; a_{n-1}, a_{n-2}, \dots]$ e $m \colon \Sigma \to \mathbb{R}$ definida por $m(\underline{\theta}) =$

$\sup_{n\in\mathbb{Z}}(\alpha_n+\beta_n)$. Então, como observamos no início deste capítulo, o espectro de Lagrange é o conjunto $L=\{\ell(\underline{\theta}),\underline{\theta}\in\Sigma\}$ e o espectro de Markov é o conjunto $M=\{m(\underline{\theta}),\underline{\theta}\in\Sigma\}$.

A prova dos resultados sobre a função $d(t)$ baseia-se, como mencionamos no início deste capítulo, no fato de que podemos aproximar por dentro e por fora pedaços dos espectros de Markov e Lagrange por somas de conjuntos de Cantor regulares de Gauss com dimensões de Hausdorff próximas (em geral essas somas serão do tipo $K(B)+K(B^t)$, e usaremos a proposição acima). A principal ferramenta que usaremos na construção de tais aproximações será o seguinte lema técnico, cuja prova (assim como os detalhes da prova dos teoremas deste capítulo) se encontra em [M2]:

**Lema 3.1:** Para cada $t>0$ e $\varepsilon>0$, seja $\Sigma(t)=\{\underline{\theta}\in\Sigma\mid m(\underline{\theta})\le t\}$, e seja $N_\varepsilon(t)$ o número de seqüências finitas $\alpha$ tais que o intervalo $I(\alpha)=\{x\in[0,1]\mid x=[0;\alpha,y],\ y\ge 1\}$ tem comprimento maior ou igual a $\varepsilon$ e $\alpha$ aparece como subseqüência de algum elemento de $\Sigma(t)$. Definimos $D(t)=\lim_{\varepsilon\to 0}-\dfrac{\log N_\varepsilon(t)}{\log\varepsilon}$ (o limite existe pois existe $C>0$ tal que $N_{\varepsilon\delta}(t)\le C\,N_\varepsilon(t)N_\delta(t)$, $\forall\,\varepsilon,\delta>0$). Então, dado $\tau>0$ existe $\delta>0$ e um shift completo $\widetilde{\Sigma}\subset\Sigma(t-\delta)$ com $HD(\widetilde{\Sigma}_+,d)\ge D(t)-\tau$, onde $\Sigma_+=\mathbb{Z}_+^{\mathbb{Z}}$, $\widetilde{\Sigma}_+=\widetilde{\Sigma}\cap\Sigma_+$, e $d\colon\Sigma_+\times\Sigma_+\to\mathbb{R}$ é a distância definida por $d(\underline{\theta},\underline{\theta}')=|I(\underline{\theta}\wedge\underline{\theta}')|$. ∎

A idéia da prova de que $L'=L''$ é criar conjuntos de Cantor regulares de Gauss usando seq"uências finits que aparecem infinitas vezes nas frações contínuas das preimagem por $k$ de uma seqüência convergente de pontos de $L$. A imagem por $k$ do Cantor de Gauss gerado por, digamos, duas seqüências dessas fornecerá um conjunto de Cantor contido em $L$ próximo ao limiteda tal seqüência. Aumentando o comprimento das seqüências finitas consideradas obtemos o resultado.

Para estudar o complementar do espectro de Lagrange em relação ao espectro de Markov, primeiro mostramos que $M\backslash L$ contém conjuntos de Cantor regulares próximos a $\alpha_\infty=[2;\overline{1,1,2,2,2,1,2}]+[0;1,2,2,2,1,1,2,1,\overline{2}]\cong 3,293044265\ldots$, que Freiman provou ser um ponto de acumulação de $M\backslash L$ (ver Capítulo 3 de [CF]) (as barras superiores indicam período nas frações contínuas pré-periódicas acima), com um argumento semelhante à prova de $L'=L''$. A prova de $HD(M\backslash L)<1$ é mais técnica e delicada, e depende da análise de restrições à seqüências finitas que podem aparecer nas frações contínuas de elementos de conjuntos de Cantor cuja imagem por $k$ esteja contida em $M \backslash L$. Veja [M2] para detalhes.

# 4 Espectros de Markov e Lagrange dinâmicos

As caracterizações em termos de shift $\Sigma$ e das funções $\ell$ e $m$ dos espectros de Markov e Lagrange admitem uma generalização natural no contexto de dinâmica hiperbólica: seja $\varphi\colon M^2 \to M^2$ um difeomorfismo, $\Lambda \subset M^2$ um conjunto hiperbólico para $\varphi$ e $f\colon M^2 \to \mathbb{R}$ uma função real de classe $C^2$. Podemos definir espectros de Markov e Lagrange dinâmicos associados ao par $(f, \Lambda)$ como segue: $L(f, \Lambda) = \{\limsup_{n\to+\infty} f(\varphi^n(x)), x \in \Lambda\}$ e $M(f, \Lambda) = \{\sup_{n\in\mathbb{Z}} f(\varphi^n(x)), x \in \Lambda\}$. É possível provar de um modo análogo ao que descrevemos neste capítulo que para conjuntos abertos de $(f, \varphi)$ (que contém abertos densos de $\{(f, \varphi) \mid \varphi$ preserva área $\}$ a função $d(t) = d_{f,\Lambda}(t) = HD(L(f, \Lambda) \cap (-\infty, t))$ coincide com $HD(M(f, \Lambda) \cap (-\infty, t))$, é contínua e sua imagem é o intervalo $[0, \min\{1, HD(\Lambda)\}]$. Genericamente, nesses casos, o ponto $t_1 = \inf\{t \in \mathbb{R} \mid d(t) = 1\}$ pertence ao fecho do interior de $L(f, \Lambda) \subset M(f, \Lambda)$.

Vale notar que o resultado não é verdade em geral para $\varphi$ dissipativo, pois há conjuntos abertos de contraexemplos onde $d(t)$ tem um número finito de descontinuidades, e sua imagem é uma união finita de intervalos não-degenerados.

As demonstrações desses últimos resultados aparecerão em [M3].

# Apêndice: Conjuntos de Cantor Regulares e Dimensões Fractais

## 1.0 Conjuntos de Cantor

Normalmente as pessoas ouvem falar no "Conjunto de Cantor" antes de ouvir falar em "conjuntos de Cantor" em geral. O conjunto de Cantor é um engenhoso exemplo de um subconjunto da reta que é compacto, não-enumerável e totalmente desconexo, que serve como fonte de exemplos interessantes em análise e topologia. O Conjunto de Cantor, que denotaremos por $K$, pode ser definido de várias maneiras. Por exemplo, $K$ é o conjunto de todos os números do intervalo $[0,1]$ que podem ser escritos em base 3 utilizando apenas os algarismos 0 e 2, ou seja, $K = \left\{ \sum\limits_{n-1}^{\infty} \dfrac{\sigma_n}{3^n},\ \sigma_n \in \{0,2\},\ \forall\, n \in \mathbb{N} \right\}$. Outra maneira de descrever o conjunto $K$ é descrevendo explicitamente seu complementar: tomamos o intervalo $[0,1]$, retiramos seu terço central $\left(\dfrac{1}{3}, \dfrac{2}{3}\right)$ e obtemos dois intervalos fechados: $\left[0, \dfrac{1}{3}\right]$ e $\left[\dfrac{2}{3}, 1\right]$. Retiramos os terços centrais desses intervalos e obtemos quatro intervalos fechados: $\left[0, \dfrac{1}{9}\right]$, $\left[\dfrac{2}{9}, \dfrac{1}{3}\right]$, $\left[\dfrac{2}{3}, \dfrac{7}{9}\right]$ e $\left[\dfrac{8}{9}, 1\right]$. Continuamos o processo, sempre retirando os terços centrais dos intervalos restantes. Os pontos do intervalo $[0,1]$ que não pertencem a nenhum dos intervalos retirados formam o conjunto de Cantor $K$. Notemos que, na $n$-ésima etapa da construção de $K$ sobram $2^n$ intervalos de comprimento $1/3^n$ cada, cuja união contém $K$. Isso implica que $K$ tem medida nula.

A terceira construção do conjunto $K$ que mostraremos a seguir é de particular importância para nós, pois será generalizada para definir conjuntos de Cantor *regulares* ou dinamicamente definidos. Consideremos a função $\psi\colon \left[0, \dfrac{1}{3}\right] \cup \left[\dfrac{2}{3}, 1\right] \to [0,1]$ definida por $\psi(x) = \begin{cases} 3x \text{ se } \left[0, \dfrac{1}{3}\right] \\ 3x - 2 \text{ se } x \in \left[\dfrac{2}{3}, 1\right] \end{cases}$. O domínio da função $\psi$ é a primeira etapa da construção anterior do conjunto $K$. Se denotarmos

$\underbrace{\psi \circ \psi \circ \cdots \circ \psi}_{n \text{ vezes}}$ por $\psi^n$, temos que $\psi^n$ não está definida para todo $x$. Por exemplo, se $n = 2$ e $x = 0,2$, temos que $\psi(x) = 3x = 0,6$, que não pertence ao domínio de $\psi$, donde $\psi^2(0,2)$ não está definido. Podemos caracterizar o Conjunto de Cantor $K$ como o conjunto dos $x \in [0,1]$ tais que $\psi^n(x)$ está definido para todo natural $n$, ou seja, $K = \bigcup_{n=0}^{\infty} \psi^{-n}([0,1])$. Podemos observar que $\psi^{-n}([0,1])$, ou seja, o domínio de $\psi^n$ coincide com o conjunto obtido na $n$-ésima etapa da construção anterior.

$K$ é claramente compacto, pois pela segunda construção, por exemplo, seu complementar é aberto. Além disso, $K$ é não-enumerável, o que segue do fato de que a primeira construção fornece uma bijeção entre $K$ e $\{0,2\}^{\mathbb{N}}$, que de fato é um homeomorfismo, se dotarmos $\{0,2\}^{\mathbb{N}}$ da topologia produto.

Em geral dizemos que um conjunto de Cantor é um espaço topológico homeomorfo a $K$. Nosso principal interesse será nos conjuntos de Cantor contidos na reta real, que podem ser caracterizados como os compactos de interior vazio sem pontos isolados.

Em geral, espaços métricos (ou metrizáveis) compactos, totalmente desconexos (i.e., cujas componentes conexas são os pontos) e sem pontos isolados são conjuntos de Cantor (i.e., são homeomorfos a $K$). Deixamos a prova deste fato como exercício para o leitor. (Sugestão: dado um conjunto como acima, tente decompô-lo como uma união disjunta de abertos e fechados com diâmetro menor que a metade do diâmetro original, repetir o processo e usar isso para reduzir o problema ao caso de subconjuntos da reta. no qual é possível construir homeomorfismos monótonos razoavelmente explícitos).

## 1.1 Conjuntos de Cantor regulares

Mencionamos que a terceira construção que exibimos para o conjunto $K$, que o caracteriza como o maximal invariante pela função $\psi$ no intervalo $[0,1]$ é de particular interesse, pois caracteriza $K$ como um conjunto de Cantor dinamicamente definido. Vamos discutir informalmente algumas propriedades dos conjuntos de Cantor dinamicamente definidos, ou regulares (que serão nosso assunto principal) antes de defini-los mais precisamente. Uma propriedade fundamental do conjunto de Cantor $K$ é a sua *auto-semelhança*: pequenas partes de $K$ são cópias reduzidas de todo o conjunto $K$. De fato, dado $x \in K$ e $\varepsilon > 0$ existe um subconjunto aberto e fechado de $K$ contendo $x$ e de diâmetro menor que $\varepsilon$ que é semelhante ao conjunto $K$ (por exemplo uma peça de uma etapa avançada da construção de $K$ que contenha o ponto $x$). Esta semelhança será dada por um certo iterado da função afim expansora $\psi$.

Os conjuntos de Cantor dinamicamente definidos, ou regulares, sempre apresentam um certo tipo de auto-semelhança: pequenas partes deles são difeomorfas ao conjunto todo, ou a partes grandes dele, com distorção uniformemente limitada. Assim, aspectos locais desses conjuntos não diferem muito de aspectos globais. Este tipo de propriedade é a principal característica dos conjuntos de Cantor regulares, e está ligada ao fato desses conjuntos, por definição, serem caracterizados como maximais invariantes de funções diferenciáveis expansoras (as quais suporemos de classe pelo menos $C^{1+\varepsilon}$).

Vamos passar a definições mais precisas:

Sejam $I, I_1, I_2, \ldots, I_k \subset \mathbb{R}$ intervalos fechados tais que os intervalos $I_j$, $1 \leq j \leq k$ são disjuntos e $I$ é o fecho convexo de $I_1 \cup I_2 \cup \cdots \cup I_k$, e seja $\psi\colon I_1 \cup I_2 \cup \cdots \cup I_k \to I$ uma função expansora de classe $C^{1+\varepsilon}$ para um certo $\varepsilon > 0$, isto é, $\psi$ é de classe $C^1$, $|\psi'(x)| > 1$ para todo $x \in I_1 \cup I_2 \cup \cdots \cup I_k$ e existe $C > 0$ tal que $|\psi'(x) - \psi'(y)| \leq C|x-y|^\varepsilon \quad \forall\, x, y \in I_1 \cup I_2 \cup \cdots \cup I_k$. Suponhamos ainda que para todo $j$ com $1 \leq j \leq k$, $\psi(I_j)$ é o fecho convexo de uma união de intervalos $I_i$, e que, para $n \in \mathbb{N}$ suficientemente grande, $\psi^n(I_j) \supset I_1 \cup I_2 \cup \cdots \cup I_k$.

Dizemos que o conjunto de Cantor regular $K = K_\psi$ associado à função $\psi$ e à *partição de Markov* $(I_1, I_2, \ldots, I_k)$ é o conjunto dos $x \in I$ tais que $\psi^n(x)$ está definido para todo $n \in \mathbb{N}$, isto é $K_\psi = \bigcap_{n\in\mathbb{N}} \psi^{-n}(I_1 \cup \cdots \cup I_k)$. Se $\psi$ é de classe $C^r$, com $1 < r \leq \infty$, dizemos que $K$ é um (conjunto de) Cantor regular de classe $C^r$.

Como indicamos na definição acima, o conjunto dos intervalos $I_j$ com $1 \leq j \leq k$ é denominado a partição de Markov de $K$. O conjuntos $I_1 \cup I_2 \cup \cdots \cup I_k$ será chamado de *domínio de Markov* de $K$, e pode ser visto como a etapa inicial da construção de $K$.

Para entender melhor a estrutura do conjunto $K$ podemos considerar a *matriz de transição* $B = (b_{ij})_{k\times k}$ associada a uma partição de Markov $(I_1, \ldots, I_k)$ e a uma função $\psi$ como acima definida por $b_{ij} = \begin{cases} 1, \text{ se } \psi(I_i) \supset I_j \\ 0, \text{ se } \psi(I_i) \cap I_j = \varnothing \end{cases}$. A condição diz que $\psi^n(I_j) \supset I_1 \cup \cdots \cup I_k$ para todo $n$ grande equivale a todos os termos de $B^n$ serem estritamente positivos se $n$ é grande. A uma tal matriz $B$ podemos associar um *shift de Markov mixing de tipo finito*, isto é, o conjunto

$\Sigma_B = \{\underline{\theta} = (\theta_1, \theta_2, \dots) \subset \{1, 2, \dots, k\}^{\mathbb{N}} \mid b_{\theta_i \theta_{i+1}} = 1, \ \forall\, i \in \mathbb{N}\}$, no qual está definida a função *shift unilateral* $\sigma\colon \Sigma_B \to \Sigma_B$ , por $\sigma((\theta_1, \theta_2, \theta_3, \dots)) = (\theta_2, \theta_3, \dots)$, isto é, $\sigma((\theta_i)_{i\in\mathbb{N}}) = (\theta_{i+1})_{i\in\mathbb{N}}$ .

Veremos que há uma identificação natural entre o par $(K, \psi)$ e o par $(\Sigma_B, \sigma)$ (de fato um homeomorfismo que conjuga as dinâmicas). Para cada palavra finita $\underline{a} = (a_1, a_2, \dots, a_n) \in \{1, 2, \dots, k\}^n$ dizemos que $\underline{a}$ é uma palavra de $\Sigma_B$ se existe algum elemento de $\Sigma_B$ que começa por $\underline{a}$, ou, equivalentemente, se $b_{a_i a_{i+1}} = 1$ para $i = 1, 2, \dots, n-1$. A uma tal palavra $\underline{a}$ associamos o intervalo $I_{\underline{a}} = I_{a_1} \cap \psi^{-1}(I_{a_2}) \cap \psi^{-2}(I_{a_3}) \cap \dots \cap \psi^{-(n-1)}(I_{a_n})$, e a condição $\underline{a}$ ser uma palavra de $\Sigma_B$ equivale a $I_{\underline{a}}$ ser não-vazio. Por outro lado, a expansividade de $\psi$ faz com que o comprimento $|I_{\underline{a}}|$ do intervalo $I_{\underline{a}}$ seja exponencialmente pequeno se $n$ é grande, isto é, existe $\lambda < 1$ tal que para todo $\underline{a} \in \{1, 2, \dots, k\}^n$ que é uma palavra de $\Sigma_B$ (de tamanho $n$), $|I_{\underline{a}}| < \lambda^n |I|$.

Dado $\underline{\theta} = (\theta_1, \theta_2, \dots) \in \Sigma_B$, para cada $n$ definimos $\underline{\theta}^{(n)} = (\theta_1, \theta_2, \dots, \theta_n)$. Note que $\underline{\theta}^{(n)}$ é sempre uma palavra de $\Sigma_B$ . Podemos definir uma função $h\colon \Sigma_B \to K$ definida por $\{h(\underline{\theta})\} = \bigcap_{n\in\mathbb{N}} I_{\underline{\theta}^{(n)}}$, isto é, $h(\underline{\theta})$ é o único ponto que pertence a $I_{\underline{\theta}^{(n)}}$ para todo $n \in \mathbb{N}$. Não é difícil verificar que $h$ é um homeomorfismo, e que $\psi \circ h = h \circ \sigma$, isto é, $h$ é uma conjugação entre $\sigma$ e $\psi$. Se $x = h(\underline{\theta})$, dizemos que $\underline{\theta}$ é o endereço do ponto $x$.

## 1.2 Distorção limitada e geometrias limite

Vamos agora provar uma proposição de grande importância, segundo a qual conjuntos de Cantor regulares têm a propriedade de *distorção limitada*:

**Proposição A.1:** Seja $K \subset \mathbb{R}$ um conjunto de Cantor regular, definido por uma função expansora $\psi \in C^{1+\varepsilon}$ como acima. Dado $\delta > 0$ existe $C(\delta) > 0$ função decrescente de $\delta$ com $\lim_{\delta\to 0} C(\delta) = 0$ tal que para todo $x, y \in K$ satisfazendo

i) $|\psi^n(x) - \psi^n(y)| \leq \delta$

ii) O intervalo $[\psi^j(x), \psi^j(y)]$ está contido no domínio de Markov $I_1 \cup \dots \cup I_k$ para $0 \leq j \leq n$ temos $\log |(\psi^n)'(y)| - \log |(\psi^n)'(x)| \leq C(\delta)$.

**Dem:** Se $\sigma > 1$ é tal que $|\psi'(t)| > \sigma$ para todo $t$ no domínio de Markov, teremos $|\psi^j(y) - \psi^j(x)| \leq \sigma^{1-n} \cdot \delta$ para $0 \leq j \leq n$, donde

$$|\log|(\psi^n)'(y)| - \log|(\psi^n)'(x)| \leq \sum_{j=0}^{n-1} |\log|\psi'(\psi^j(y))| - \log|\psi'(\psi^j(x))||,$$

e, como $\psi'$ (e também $\log|\psi'|$) é de classe $C^\varepsilon$, existe $C > 0$ tal que $|\log|\psi'(s)| - \log|\psi'(t)| \leq C|s-t|^\varepsilon$ para $s$, $t$ no domínio de Markov, donde as expressões acima são majoradas por

$$c\sum_{j=0}^{n-1}(\sigma^{j-n} \cdot \delta)^\varepsilon < c\dot{\delta}^\varepsilon \cdot \sum_{m=1}^{\infty} \sigma^{-m\varepsilon} = c\delta^\varepsilon \cdot \frac{\sigma^{-\varepsilon}}{1-\sigma^{-\varepsilon}} \cdot$$

■

Uma maneira de reformular a proposição acima com significado geométrico mais evidente é dizer que se $x$, $y$ e $z$ pertencem a um mesmo intervalo $I_{\underline{\theta}^{(n)}}$ da $n$-ésima etapa da construção de $K$ então

$$e^{-c}\frac{|z-x|}{|y-x|} \leq \frac{|\psi^n(z) - \psi^n(x)|}{|\psi^n(y) - \psi^n(x)|} \leq e^c \frac{|z-x|}{|y-x|}$$

onde $c = c(|I|)$ é uma constante. Além disso, se $\psi^n(x)$, $\psi^n(y)$ e $\psi^n(z)$ estão próximos, $c$ pode ser tomada pequena. Isto significa que distâncias relativas numa escala microscópica são no máximo distorcidas por um fator constante em relação a distâncias relativas correspondentes numa escala maior, e cada vez menos distorcidas se diminuimos o tamanho da escala maior.

Vamos agora introduzir o conceito de *geometrias limite* de um conjunto de Cantor regular, que dão informações mais precisas sobre a estrutura local de um conjunto de Cantor regular.

Para isto, seja $K$ um conjunto de Cantor regular e $\Sigma_B$ seu shift de Markov associado. Vamos considerar o shift dual associado a $\Sigma_B$, denotado por $\Sigma_B^-$, dado por $\Sigma_B^- - \{\underline{\theta} = (\theta_n)_{n \leq 0},\ f_{\theta_i \theta_{i+1}} = 1, \forall\, i < 0\} \subset \{1, 2, \ldots, k\}^{\mathbb{Z}^-}$.

Dados $\underline{\theta} \neq \underline{\tilde{\theta}}$ em $\Sigma_B^-$, definimos $\underline{\theta} \wedge \underline{\tilde{\theta}}$ como $(\theta_{-n}, \theta_{1-n}, \ldots, \theta_0) \in \{1, 2, \ldots, k\}^{n+1}$, onde $n$ é tal que $\tilde{\theta}_{-j} = \theta_{-j}$ para $0 \leq j \leq n$ e $\tilde{\theta}_{-n-1} \neq \theta_{-n-1}$, e equipamos $\Sigma_B^-$ com a seguinte distância:

$$d(\underline{\theta}, \underline{\tilde{\theta}}) = \begin{cases} 1 & \text{se} \quad \theta_0 \neq \tilde{\theta}_0 \\ |I_{\underline{\theta} \wedge \underline{\tilde{\theta}}}|, & \text{caso contrário} \end{cases}$$

Dado $\underline{\theta} \in \Sigma_B^-$ e $n > 0$, definimos $\underline{\theta}^n = (\theta_{-n}, \ldots, \theta_0)$, e $B(\underline{\theta}^n)$ como sendo a função afim que leva $I_{\underline{\theta}^n}$ em $I_{\theta_0}$ tal que o difeomorfismo $k_n^{\underline{\theta}} = B(\underline{\theta}^n) \circ f_{\underline{\theta}^n}$ preserva orientação, onde $f_{\underline{\theta}^n} := \left(\psi^n|_{I_{\underline{\theta}^n}}\right)^{-1}$.

Com essas definições, $k_n^{\underline{\theta}}$ é um difeomorfismo de $I_{\theta_0}$ em $I_{\theta_0}$, e a imagem de $K \cap I_{\theta_0}$ por $k_n^{\underline{\theta}}$ é uma cópia ampliada de $K \cap I_{\underline{\theta}^n}$.

Com essas notações, temos o seguinte resultado, que caracteriza as geometrias limite de um Cantor regular (ver [Su]):

**Proposição A.2:** Seja $r \in (1, +\infty)$, e $K$ um conjunto de Cantor regular de classe $C^r$ como acima, então:

i) Para cda $\underline{\theta} \in \Sigma_B^-$ existe um difeomorfismo de classe $C^r$ que preserva orientação $k^{\underline{\theta}} = I_{\theta_0} \to I_{\theta_0}$ tal que $k_n^{\underline{\theta}}$ converge a $k^{\underline{\theta}}$ na topologia $C^\alpha$ para todo $\alpha < r$. A convergência é uniforme numa $C^r$-vizinhança de $\psi$.

ii) Se $r \geq 2$ é um inteiro então $k_n^{\underline{\theta}}$ converge a $k^{\underline{\theta}}$ em $\mathrm{Diff}_+^r(I_{\theta_0})$. Além disso, existe $C > 0$ tal que $||k_n^{\underline{\theta}} - k^{\underline{\theta}}||_{C^{r-1}} \leq C|I_{\underline{\theta}^n}|$.

Do item ii) segue que $\underline{\theta} \to k^{\underline{\theta}}$ é Lipschitziana: $||k^{\underline{\theta}} - k^{\underline{\tilde{\theta}}}||_{C^{r-1}} \leq C \cdot d(\underline{\theta}, \underline{\tilde{\theta}}),\ \forall\, \underline{\theta}, \underline{\tilde{\theta}} \in \Sigma_B^-$. Além disso, se $r = 1 + \alpha$, com $0 < \alpha < 1$, então, para

$$||k^{\underline{\theta}} - k^{\underline{\tilde{\theta}}}||_{C^1} \leq C \cdot d(\underline{\theta}, \underline{\tilde{\theta}})^\beta,\ \forall\, \underline{\theta}, \underline{\tilde{\theta}} \in \Sigma_B^-.$$

Esta proposição diz que conjuntos de Cantor regulares têm a seguinte propriedade: se ampliarmos a interseção de um conjunto de Cantor regular $K$ com intervalos pequenos de sua construção, obtemos conjuntos de Cantor difeomorfos a partes fixas de todo o conjunto $K$ (as interseções $K \cap I_a$, com $a \in \{1, 2, \ldots, k\}$), estando esses difeomorfismos muito próximos da família compacta $\{k^{\underline{\theta}}, \underline{\theta} \in \Sigma_B^-\}$ que tem dimensão de Hausdorff finita por exemplo na métrica $C^1$ (ver a próxima seção sobre dimensão de Hausdorff).

Definimos, para $\underline{\theta} \in \Sigma_B^-$, o conjunto de Cantor $K^{\underline{\theta}} := k^{\underline{\theta}}(K)$. Os conjuntos $K^{\underline{\theta}}$ são conjuntos de Cantor regulares tão diferenciáveis quanto $K$, e são conhecidos como as *geometrias limite* de $K$.

**Dem:** A prova da Proposição A.2 não é muito difícil. De fato, $k_n^{\underline{\theta}} = B(\underline{\theta}^n) \circ f_{\underline{\theta}^n}$, onde $f_{\underline{\theta}^n} = \left(\psi|_{I_{\underline{\theta}^n}}\right)^{-1}$ pode ser escrito como $g_n \circ g_{n-1} \circ \cdots \circ g_1$, onde, para $1 \le k \le n$, $\quad g_k = g_k^{\underline{\theta}} \colon I_{\theta_0} \to I_{\theta_0}$ é dada por $g_k = A_k \circ \left(\psi|_{I_{\underline{\theta}}^k}\right)^{-1} \circ A_{k-1}^{-1}$, e os $A_k \colon I_{\underline{\theta}^k} \to I_{\theta_0}$ são difeomorfismos afins tais que $A_0$ é a identidade e $g_k$ preserva orientação para todo $K$.

O resultado segue do fato de que os difeomorfismos $g_k$, para $K$ grande, estão exponencialmente perto da identidade (de modo uniforme em $\underline{\theta}$), nas topologias indicadas no enunciado da proposição, e portanto a composição deles converge exponencialmente nessas topologias. Os detalhes ficam como exercício para o leitor. ■

## 1.3 Dimensões fractais

### 1.3.1 - A dimensão de Hausdorff

Quase todos os conjuntos de Cantor que consideramos neste livro têm medida de Lebesgue nula. Entretanto, há medidas mais finas do tamanho de subconjuntos da reta (e, em geral, de um espaço métrico). Começaremos pelo conceito que será mais importante para nós: a dimensão de Hausdorff:

Se $X$ é um espaço métrico compacto e $\mathcal{U} = \{U_1, U_2, \ldots, U_n\}$ é uma cobertura finita de $X$, definimos a medida de Hausdorff de dimensão $\alpha > 0$ associada à cobertura $\mathcal{U}$ por $m_\alpha(\mathcal{U}) = \sum\limits_{i=1}^{n} \operatorname{diam}(U_i)^\alpha$, onde

$$\operatorname{diam}(U_i) = \sup_{x,y \in U_i} d(x,y) \quad \text{é o diâmetro de } U_i\,,$$

e definimos a medida de Hausdorff de dimensão $\alpha$ de $X$ por $m_\alpha(X) = \liminf_{||\mathcal{U}|| \to 0} m_\alpha(\mathcal{U})$, onde $U$ denota uma cobertura finita de $X$ e $||\mathcal{U}|| = \max_{U \in \mathcal{U}} (\operatorname{diam} U)$ é a norma da partição $\mathcal{U}$. É fácil mostrar que existe um único $h$ em $[0, +\infty]$ tal que se $\alpha < h$ então $m_\alpha(X) = +\infty$ e se $\alpha > h$ então $m_\alpha(X) = 0$. Esse número $h$ é, por definição, a *dimensão de Hausdorff* de $X$. A dimensão de Hausdorff tem algumas propriedades importantes. Uma delas é que, se $f \colon X \to X$ é Lipschitziana e $K \subset X$ tem dimensão de Hausdorff $d$ então $f(K)$ tem dimensão de Hausdorff menor ou igual a $d$. Em particular, se $X$ e $Y$ são intervalos fechados e $f$ é um difeomorfismo então as dimensões de Hausdorff de $K$ e $f(K)$ são iguais. Outra observação simples é que se $K \subset \mathbb{R}^n$ tem dimensão de Hausdorff menor que $n$ então tem medida de Lebesgue nula.

É possível provar que a dimensão de Hausdorff de conjuntos de Cantor regulares da reta depende continuamente da dinâmica que os define (mesmo na topologia $C^1$), e, no caso da dinâmica ser pelo menos $C^{1+\varepsilon}$, está sempre estritamente entre 0 e 1, e a medida de Hausdorff correspondente é finita e positiva no conjunto de Cantor (ver [PT2]).

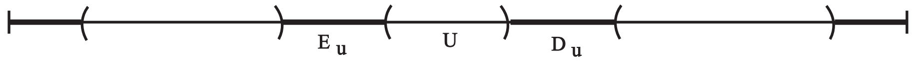
Podemos definir outra dimensão fractal, a *capacidade limite*, como segue: Se $K$ é um espa co métrico compacto, definimos $N_\varepsilon(K)$ como sendo o número mínimo de conjuntos de Diâmetro menor ou igual a $\varepsilon$ necessários para cobrir $K$. A capacidade limite de $K$ é, por definição, $d(K) = \limsup_{\varepsilon\to 0} -\dfrac{\log N_\varepsilon(K)}{\log \varepsilon}\cdot$ É possível provar que, se $K$ é um conjunto de Cantor regular (mesmo que apenas de classe $C^1$) então sua dimensão de Hausdorff coincide com sua capacidade limite (ver [PT2]). Também é verdade que, se $f\colon X \to Y$ é Lipschitziana e $K \subset X$ então $d(f(K)) \leq d(K)$ e que $d(K_1 \times K_2) \leq d(K_1) + d(K_2)$. Além disso, em geral a dimensão de Hausdorff de $K$ é sempre menor ou igual a $d(K)$ (às vezes a desigualdade é estrita, como por exemplo se $K = \{0\} \cup \{1/n,\ n \text{ inteiro positivo}\}$, que tem dimensão de Hausdorff 0 e capacidade limite $1/2$).

Deixamos a prova destas últimas afirmações como exercício para o leitor.

### 1.3.2 - Espessuras

**Definição A.3:** Um *gap* de um conjunto de Cantor é uma componente conexa de seu complementar.

Dado um gap $U$ de um conjunto de Cantor $K$, associamos a ele os intervalos $E_U$ e $D_U$, que são os intervalos à sua esquerda e à sua direita que o separam dos gaps maiores que ele mais próximos:



Definimos
$\tau_D(U) = \dfrac{|D_U|}{|U|}$, $\tau_E(U) = \dfrac{|E_U|}{|U|}$,

$\tau_D(K) = \inf\{\tau_D(U)|U$ gap limitado de $K\}$, a *espessura direita* de $K$;

$\tau_E(K) = \inf\{\tau_E(U)|U$ gap limitado de $K\}$, a *espessura esquerda* de $K$, e

$\tau(K) = \min\{\tau_D(K), \tau_E(K)\}$, a *espessura* de $K$.

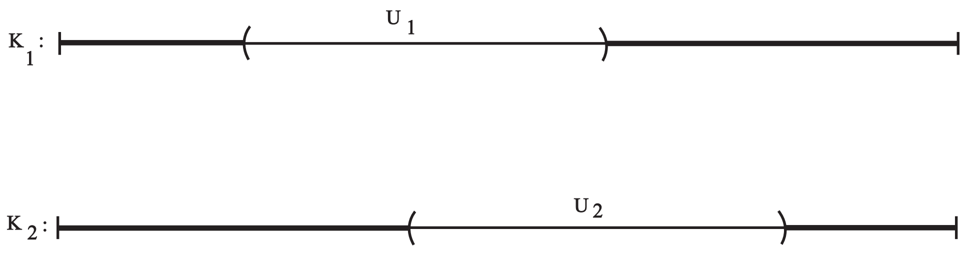
**Observação:** Dado um conjunto de Cantor $K$, uma apresentação de $K$ é uma enumeração $\{U_1, U_2, \dots\}$ de seus gaps limitados. Podemos definir os intervalos $E_U$ e $D_U$ como sendo os intervalos entre $U$ e os gaps de índice menor que o de $U$ mais próximos. No nosso caso estamos usando a apresentação pela ordem de tamanho dos gaps, o que maximiza a espessura $\tau(K)$. Veja [PT2].

A importância das espessuras reside no seguinte resultado, que é uma adaptação do "gap lemma".

**Afirmação:** Dados $K_1$ e $K_2$ conjuntos de Cantor, se $\tau_D(K_1) \cdot \tau_E(K_2) > 1$ e $\tau_E(K_1) \cdot \tau_D(K_2) > 1$, então ou $K_1$ está contido num gap de $K_2$ ou $K_2$ está contido num gap de $K_1$ ou $K_1 \cap K_2 \neq \varnothing$.

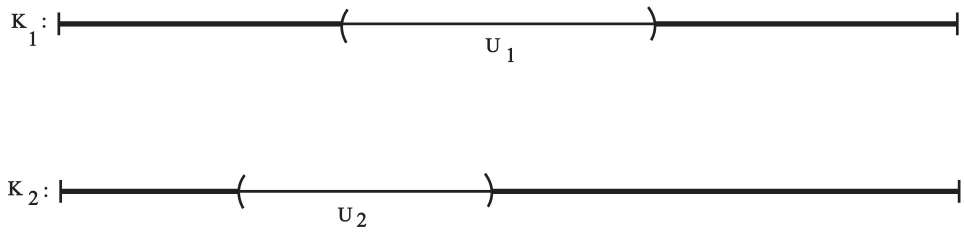
**Observação:** Isso vale em particular se $\tau(K_1) \cdot \tau(K_2) > 1$, que é a hipótese do "gap lemma" clássico. O gap lemma tal como enunciado aqui fornece mais informação, como veremos adiante.

**Dem:** Considere o caso em que nenhum dos $K_i$'s está contido num gap do outro. Então existe um par de gaps encaixados, como nas figuras abaixo (dizemos nesse caso que $K_1$ e $K_2$ estão *intercalados*) a)




Como $\tau_D(U_1)\tau_E(U_2) > 1$, ou $|D_{U_1}| > |U_2|$ ou $|E_{U_2}| > |U_1| \Rightarrow$ existe novo par de gaps como em b) menor que o par $(U_1, U_2)$

b)




Como $\tau_E(U_1)\tau_D(U_2) > 1$, ou $|E_{U_1}| > |U_2|$ ou $|D_{U_2}| > |U_1| \Rightarrow$ existe novo par de gaps como em a) menor que o par $(U_1, U_2)$.

Em qualquer caso obtemos um par de gaps menor, por exemplo no sentido de que a soma dos comprimentos dos gaps dos pares decresce, e reaplicando o argumento obtemos uma seqüência de pares de gaps convergindo a um ponto que necessariamente pertence a $K_1 \cap K_2$. ■

Podemos definir, para $p \in K$, $\tau_{\text{loc}}(K,p) = \limsup_{\varepsilon \to 0} \tau(\overline{K \cap (p-\varepsilon, p+\varepsilon)})$, e analogamente $(\tau_D)_{\text{loc}}(K,p)$ e $(\tau_E)_{\text{loc}}(K,p)$. Para conjuntos de Cantor dinamicamente definidos, $\tau_{\text{loc}}(K,p)$ não depende de $p$ (ver [PT2]), e a mesma prova mostra que $(\tau_D)_{\text{loc}}(K,p)$ e $(\tau_E)_{\text{loc}}(K,p)$ também não dependem de $p$. Vamos, portanto, denotá-los por $\tau_{\text{loc}}(K)$, $(\tau_D)_{\text{loc}}(K)$ e $(\tau_E)_{\text{loc}}(K)$ (as *espessuras locais* de $K$).

A afirmação acima implica que se $(\tau_D)(K_1) \cdot (\tau_E)(K_2) \geq 1$ e se $(\tau_E)(K_1) \cdot (\tau_D)(K_2) \geq 1$ então $K_1 - K_2$ contém intervalo.

Como conseqüência, se $(\tau_D)_{\text{loc}}(K_1) \cdot (\tau_E)_{\text{loc}}(K_2) > 1$ e $(\tau_E)_{\text{loc}}(K_1) \cdot (\tau_D)_{\text{loc}}(K_2) > 1$ então $K_1 - K_2$ contém intervalo. Para este último resultado necessitamos desigualdades estritas.

De fato, no exemplo de Sannami de um conjunto de Cantor dinamicamente definido $K$ com $\lambda(K - K) > 0$ e $\text{int}(K - K) = \varnothing$ temos $\tau_{\text{loc}}(K) = 1$.

# Referências


[AGP] W. R. Alford, A. Granville e C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math., **140** (1994) 703-722.

[APR] L. M. Adleman, C. Pomerance e R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. Math. (2) **117** (1983) 173-206.

[B] N. Beskin, Frações contínuas - Iniciação à Matemática - Editora Mir.

[Bach] Eric Bach, *Explicit bounds for primality testing and related problems*, Math. of Comp. **55**, (1990), pp. 355-380.

[BCR] R. P. Brent, G. L. Cohen e H. J. J. te Riele, *Improved techniques for lower bounds for odd perfect numbers*, Math. Comp., **57** (1991) 857-868 (MR 92c:11004).

[BLS] J. Brillhart, D. H. Lehmer e J. L. Selfridge, *New primality criteria and factorizations of* $2m \pm 1$, Math. Comp., **29** (1975) 620-647.

[BPMV] R. Bamón, S. Plaza, C.G. Moreira and J. Vera, *Differentiable structures of central Cantor sets*, Ergod. Th. and Dynam. Syst. **17** (1997), pp. 1027–1042.

[BPV] R. Bamón, S. Plaza and J. Vera, *On Central Cantor Sets with self-arithmetic difference of positive Lebesgue measure*, J. London Math. Soc. **51** (1995), pp. 137–146.

[Br] J. W. Bruce, *A really trivial proof of the Lucas-Lehmer test*, Amer. Math. Monthly, April (1993) 370-371.

[C] José Paulo Q. Carneiro, *Um processo finito para a raiz quadrada*, RPM **34**, (1997), pp. 36–44.

[Ca1] J.W.S. Cassels, *An introduction to diophantine approximation*, Cambridge Univ. Pres, (1957).

[Ca2] J.W.S. Cassels, *Some metrical theorems in Diophantine approximation I*, Proc. Camb. Phil. Soc. **46** (1950), 209–218.

[CB] M. Clausen e U. Baum, *Fast Fourier Transforms*, BI-Wiss.-Verl., (1993).

[Cipolla] M. Cipolla, *Sui numeri composti $P$, che verificano la congruenza di Fermat* $a^{P-1} \equiv 1 \pmod{P}$, Annali di Matematica, (3), **9**, (1904), 139-160.

[CF] R. Crandall e B. Fagin, *Discrete weighted transforms and large-integer arithmetic*, Math. Comp., **62:205** (1994) 305-324.

[CF] T.W. Cusick and M.E. Flahive, *The Markoff and Lagrange spectra*, Math. Surveys and Monographs, no. **30**, A.M.S. (1989).

[E] P. Erdös, *On a new method in elementary number theory which leads to an elementary proof of the prime number theorem*, Proc. Nat. Acad. Sci. (Washington) **35** (1949) 374-384.

[EP] P. Erdös e Carl Pomerance, *On the number of false witnesses for a composite number*, Math. Comp., **46** (1986) 259-279.

[F] G.A. Freiman, *Diophantine approximation and geometry of numbers (The Markoff spectrum)*, Kalininskii Gosudarstvennyi Universitet, Moscow, (1975).

[GK] S. Goldwasser e J. Kilian, *Almost all primes can be quickly certified*, Proc. 18th STOC (Berkeley, May 28-30, 1986), ACM, New York, (1986), 316-329.

[Guy] R. K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag, New York, (1994) (QA241.G87, ISBN 3-540-94289-0).

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

[HW] G. H. Hardy e E. M. Wright, *An Introduction to the Theory of Numbers 5e*, Oxford University Press, (1979).

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

[KP] Su Hee Kim e Carl Pomerance, *The probability that a random probable prime is composite*, Math. Comp., **53:188** (1989) 721-741.

[Per] L., Per, *L'ensemble difference de deux ensembles de Cantor aleatoires*, C.R. Acad. Sci. Paris Sér. I Math. **310** (1990), no. 10, 735–738.

[Le] D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. Math. 31 (1930) 419-448. Reprinted in *Selected Papers* (ed. D. McCarthy), Vol **1**, Ch. Babbage Res. Center, St. Pierre, Manitoba Canada, 11-48, (1981).

[Lu] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, Amer. J. Math., **1**, (1878), 184-240 e 289-321.

[M1] C.G. Moreira, *Stable intersections of Cantor sets and homoclinic bifurcations*, Ann. Inst. H. Poincaré Anal. Non Linéaire **13** (1996), no. 6, pp. 741–781.

[M2] C.G. Moreira, *Geometric properties of the Markov and Lagrange spectra.* Preprint-IMPA.

[M3] C.G. Moreira, *Geometric properties of dynamical spectra.* To appear

[M4] C.G. Moreira, *Conjuntos de Cantor,bifurcações dinâmicas e aproximações diofantinas*, 22.o Colóquio Brasileiro de Matemática.

[M5] C.G. Moreira, *Propriedades estatísticas de frações contínuas e aproximações diofantinas:o teorema de Khintchine*, Revista Matemática Universitária número **29**, pp. 125-137

[M6] C.G. Moreira, *Frações contínuas, representações de números e aproximações*, Eureka **3** (1998), 44–55.

[Mai] H. Maier, *Primes in short intervals*, Michigan math. J., **32** (1985) 221-225.

[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.

[Mi] W. H. Mills, *A prime representing function*, Bull. Amer. Math. Soc., 53 604.

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

[Mo] , R. A. Mollin, *Prime-producing polynomials*, Amer. Math. Monthly **104** (June-July 1997) 529-544.

[MO] P. Mendes and F. Oliveira, *On the topological structure of the arithmetic sum of two Cantor sets*, Nonlinearity, Vol. **7**, (1994), pp. 329–343.

[MY] C.G. Moreira and J.-C. Yoccoz, *Stable intersections of regular Cantor sets with large Hausdorff dimensions*. Preprint - IMPA, (1998).

[MY2] C.G. Moreira and J.-C. Yoccoz, *Tangences homoclines stables pour les ensembles hyperboliques de grande dimension fractale*. To appear.

[N1] S. Newhouse, *Non density of Axiom $A(a)$ on $S^2$*, Proc. A.M.S. Symp. Pure Math., Vol. **14**, (1970), pp. 191–202.

[N2] S. Newhouse, *Diffeomorphisms with infinitely many sinks*, Topology, Vol. **13**, (1974), pp. 9–18.

[N3] S. Newhouse, *The abundance of wild hyperbolic sets and nonsmooth stable sets for diffeomorphisms*, Publ. Math. IHES, Vol. **50**, (1979), pp. 101–151.

[O] C.D. Olds, *Continued Fractions*, New Mathematical Library, Random House.

[P] J. Palis, *Homoclinic orbits, hyperbolic dynamics and fractional dimension of Cantor sets*, Contemporary Mathematics **58**, (1987), pp. 203–216.

[P1] J. Palis, *Homoclinic bifurcations, sensitive chaotic dynamics and strange attractors*, Dynamical Syst. and Related Topics. World Scientific, (1991), pp. 466-473.

[Pi] J. Pintz, *Very large gaps between consecutive primes*, J. Number Theory **63** (1997), no. 2, 286-301.

[Po] C. Pomerance, *A new lower bound for the pseudoprimes counting function*, Illinois J. Math, **26**, (1982), 4-9.

[PSW] C. Pomerance, J. L. Selfridge e S. S. Wagstaff Jr., *The pseudoprimes to 25.109*, Math. Comp., **35** (1980) 1003-1026.

[PT] J. Palis and F. Takens, *Cycles and measure of bifurcation sets for two-dimensional diffeomorphisms*, Invent. Math., Vol. **82**, (1985), pp. 379–442.

[PT1] J. Palis and F. Takens, *Hyperbolicity and the creation of homoclinic orbits*, Annals of Math., Vol. **125**, (1987), pp. 337–374.

[PT2] J. Palis and F. Takens, *Hyperbolicity and sensitive chaotic dynamics at homoclinic bifurcations: fractal dimensions and infinitely many attractors*, Cambridge Univ. Press, (1992).

[PY] J. Palis and J.C. Yoccoz, *Homoclinic Tangencies for Hyperbolic sets of large Hausdorff Dimension Bifurcations*, Acta Mathematica, Vol. **172**, (1994), pp. 91–136.

[PY1] J. Palis and J.C. Yoccoz, *On the arithmetic sum of regular Cantor sets*, Ann. Inst. H. Poincaré Anal. Non Linéaire **14** (1997), pp. 439–456.

[R] A.M. Rockett, P. Szüsz, *Continued Fractions*, World Scientific.

[Ri1] P. Ribenboim, *The New Book of Prime Number Records*, 3ed., Springer-Verlag, New York, (1995) (QA246 .R47 ISBN 0-387-94457-5).

[Ri2] P. Ribenboim, *Vendendo primos*, Rev. Mat. Univ., 22/23, 1997, 1-13 (tradução de *Selling primes*, Math. Mag., **68** (1995) 175-182).

[Rie1] H. Riesel, *Naagra stora primtal* (Sueco: *Alguns primos grandes*), Elementa **39** (1956) 258-260.

[Rie2] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, Progress in Mathematics, Birkhauser Boston, vol. **57**, (1985); and vol. 126, 1994.

[S] A. Sannami, *An example of a regular Cantor set whose difference set is a Cantor set with positive measure*, Hokkaido Math. Journal, Vol. **XXI** (I), (1992), pp. 7–23.

[Sc] W.M. Schmidt: *Diophantine approximations*, Lecture Notes in Mathematics **785**, Springer Verlag, (1980).

[Se] A. Selberg, *An elementary proof of the prime number theorem*, Annals of Math. **50** (1949) 305-13.

[Si] W. Sierpinski, *Sur un problème concernant les nombres* $k \cdot 2n+1$, Elem. Math., **15** (1960) 73-74. Corrigendum: Elem. Math., **17** (1963) 85.

[Su] D. Sullivan, *Differentiable structures on fractal-like sets, determined by intrinsic scaling functions on dual Cantor sets*, The mathematical heritage of Hermann Weyl (Durham, NC, 1987), 15–223, Proc. Sympos. Pure Math. **48**, Amer. Math. Soc., Providence, RI, (1988).

[WD] H. C. Williams e H. Dubner, *The primality of R1031*, Math. Comp., **47** (1986) 703-711.

[We] E. Westzynthius, *Über die Verteilung der Zahlen die zu den* $n$ *ersten Primzahlen teilerfremd sind*, Comm. Phys. math. Helsingfors, 5:5 (1931) 1-37.

[Wi] H. Wilf, *What is an answer?* Am. Math. Monthly, **89** (1982), 289-292.

[YP] J. Young e A. Potler, *First occurence of primes gaps*, Math. Comp., **52** (1989) 221-224.