UNIVERSIDADE FEDERAL DE ALAGOAS-UFAL
CAMPUS AC SIMÕES

GERSON FERREIRA SANTOS JUNIOR

RELAÇÕES ENTRE ANÁLISE, SISTEMAS DINÂMICOS E GEOMETRIA FRACTAL COM TEORIA DOS NÚMEROS

MACEIÓ
2023

Gerson Ferreira Santos Junior

RELAÇÕES ENTRE ANÁLISE, SISTEMAS DINÂMICOS E GEOMETRIA FRACTAL COM TEORIA DOS NÚMEROS

Trabalho de Conclusão de Curso submetido à Universidade Federal de Alagoas, como requisito necessário para obtenção do grau de Licenciado em Matemática da Universidade Federal de Alagoas - UFAL, Campus AC Simões.

Orientador: Prof. Dr. Davi dos Santos Lima

Maceió
2023

Catalogação na fonte
Universidade Federal de Alagoas
Biblioteca Central
Divisão de Tratamento Técnico
Bibliotecária: Girlaine da Silva Santos – CRB-4 – 1127

S237r Santos Júnior, Gerson Ferreira.
Relações entre análise, sistemas dinâmicos e geometria fractal com teoria dos números / Gerson Ferreira Santos Júnior. – 2024.
123 f. : il.

Orientador: Davi dos Santos Lima.
Monografia (Trabalho de conclusão de curso em Matemática : Licenciatura) - Universidade Federal de Alagoas. Instituto de Matemática. Maceió, 2024.

Bibliografia: f. 123.

1. Geometria. 2. Geometria fractal. 3. Teoria dos números. 4. Desigualdade de Pólya. 5.Teorema de Jarnik. I. Título.

CDU: 514

Gerson Ferreira Santos Junior

RELAÇÕES ENTRE ANÁLISE, SISTEMAS DINÂMICOS E GEOMETRIA FRACTAL COM TEORIA DOS NÚMEROS

Monografia apresentada como requisito parcial para obtenção do grau de Licenciado em Matemática da Universidade Federal de Alagoas - UFAL, Campus AC Simões.

Data de Aprovação: 22/12/2023

Banca Examinadora

Orientador: Prof. Dr. Davi dos Santos Lima
Universidade Federal de Alagoas

Profa. Dra. Elaine Cristine de Souza Silva
Universidade Federal de Alagoas

Prof. Dr. Márcio Cavalcante de Melo
Universidade Federal de Alagoas

Prof. Dr. Rafael Nóbrega de Oliveira Lucena
Universidade Federal de Alagoas

AGRADECIMENTOS

Obrigado à minha família que me deu o suporte necessário para que eu me dedicasse aos estudos e obrigado aos colegas e professores que me ajudaram nesse trajeto.

"Se eu não fizer por mim, não há quem faça." -Kamau

RESUMO

Este trabalho trata de mostrar algumas aplicações de Análise, Geometria Fractal e Sistemas Dinâmicos em Teoria dos Números. Na primeira parte apresentamos funções aritméticas e provamos alguns resultados, evoluindo para o estudo dos caracteres de Dirichlet para provar a Desigualdade de Pólya e o Teorema de Dirichlet para primos em progressões aritméticas. Na segunda parte estudamos conjuntos denominados fractais, calculando suas dimensões e descobrindo suas propriedades e características derivadas. As técnicas desenvolvidas e o conhecimento adquirido nos permitem provar resultados em frações contínuas e o Teorema de Jarnik, na área de aproximações diofantinas.

Palavras-chave: Geometria Fractal. Teoria dos números. Desigualdade de Pólya. Teorema de Jarnik.

ABSTRACT

This work aims to show some applications of Analysis, Fractal Geometry and Dynamic systems in Number Theory. In the first part we present arithmetic functions and prove some results, evolving to the study of Dirichlet characters to prove Pólya's Inequality and Dirichlet's Theorem for primes in arithmetic progressions. In the second part we study sets called fractals, calculating their dimensions and discovering their properties and derived characteristics. The techniques developed and the knowledge acquired allow us to prove results in continued fractions and Jarnik's Theorem, in the area of diophantine approximations.

Keywords: Fractal Geometry. Number theory. Pólya's inequality. Jarnik's theorem.

LISTA DE FIGURAS

Figura 1 – Plano qd - Fonte: autoria própria 30
Figura 2 – Pontos do lática $\mathbb{Z}^2$ - Fonte: autoria própria 34
Figura 3 – Tabelas de caracteres para $k = 3, 4$ e 5 - Fonte: (APOSTOL, 1976) 49
Figura 4 – O Conjunto de Cantor - Fonte: autoria própria 73
Figura 5 – Curva de von Koch - Fonte: autoria própria 75
Figura 6 – Curva floco de neve - Fonte: autoria própria 76
Figura 7 – Triângulo de Sierpinski - Fonte: (FALCONER, 2014) 76
Figura 8 – Poeira de Cantor - Fonte: (FALCONER, 2014) 77
Figura 9 – Passos na construção de uma distribuição de massa μ por divisões repetidas. A massa nos conjuntos $\mathcal{E}_k$ é dividida entre os conjuntos de $\mathcal{E}_{k+1}$, então por exemplo, $\mu(U) = \mu(U_1) + \mu(U_2)$ - Fonte: (FALCONER, 2014). 81
Figura 10 – Um conjunto e duas $\delta-$coberturas possíveis para F. O ínfimo de $\Sigma|U_i|^s$ sobre todas essas $\delta-$coberturas$\{U_i\}$ nos dá $\mathcal{H}^s_\delta(F)$ - Fonte: (FALCONER, 2014). . 83
Figura 11 – Gráfico da medida s-dimensional de Hausdorff em função de s - Fonte: autoria própria 87
Figura 12 – Poeira de Cantor - Fonte: (FALCONER, 2014). 89
Figura 13 – Cubo no δ-látice em $\mathbb{R}^2$ - Fonte: autoria própria. 92
Figura 14 – Cinco maneiras de encontrar a dimensão box de F. O número $N_\delta(F)$ é tomado como: (i) o menor número de bolas fechadas de raio δ que cobrem F; (ii) o menor número de cubos de lado δ que cobrem F; (iii) o número de cubos do δ-látice que intersectam F; (iv) o menor número de conjuntos de diâmetro no máximo δ que cobrem F; (v) o maior número de bolas disjuntas de raio δ com centros em F - Fonte: (FALCONER, 2014). 95
Figura 15 – Um conjunto de Cantor uniforme com $m = 3$ e $r = 4/15$, então $\dim_H F = \dim_B F = \log 3/ - \log 4/15 = 0,831...$ - Fonte: (FALCONER, 2014) . . . 103
Figura 16 – Exemplo de coberturas para conjuntos A e B - Fonte: (FALCONER, 2014) . 106
Figura 17 – Estágios na construção de uma curva fractal de um gerador (E_1). Os comprimentos dos segmentos do gerador são $1/3, 1/4, 1/3, 1/4, 1/3$, e as dimensões de Hausdorff e box de F são dadas por $3(1/3)^s + 2(1/4)^s = 1$ ou $s = 1, 34...$ - Fonte: (FALCONER, 2014) 111
Figura 18 – Uma curva fractal e seu gerador. As dimensões de Hausdorff e box são iguais a $\log 8/ \log 4 = \log 2^3/ \log 2^2 = 3/2$ - Fonte: (FALCONER, 2014) 112
Figura 19 – Uma curva fractal e seu gerador. As dimensões de Hausdorff e box são iguais a $\log 5/ \log 3 = 1, 465...$ - Fonte: (FALCONER, 2014) 113

SUMÁRIO

1 INTRODUÇÃO 13

I APLICAÇÕES DE ANÁLISE EM TEORIA DOS NÚMEROS **14**

2 FUNÇÕES ARITMÉTICAS 15
2.1 Funções Básicas 15
2.2 A função $\mu(n)$ de Möbius 15
2.3 A função totiente de Euler $\varphi(n)$ 16
2.4 Uma relação entre φ e μ 16
2.5 A função φ como um produto 17
2.6 Convolução de Dirichlet (ou produto de Dirichlet) 18
2.7 Inversos de Dirichlet e a fórmula de inversão de Möbius 20
2.8 A função de Mangoldt $\Lambda(n)$ 21
2.9 Funções multiplicativas 22
2.10 Função de Liouville $\lambda(n)$ 24
2.11 As funções divisores $\sigma_\alpha(n)$ 25

3 MÉDIAS DE FUNÇÕES ARITMÉTICAS 26
3.1 Introdução 26
3.2 Notação grande O 26
3.3 Fórmula de soma de Euler 27
3.4 Algumas fórmulas assintóticas elementares 28
3.5 O valor médio das funções divisores $\sigma_\alpha(n)$ 29
3.6 O valor médio de $\varphi(n)$ 32
3.7 Uma aplicação para a distribuição dos pontos do látice $\mathbb{Z}^2$ visíveis da origem. 32

4 ALGUNS TEOREMAS SOBRE A DISTRIBUIÇÃO DE NÚMEROS PRIMOS 36
4.1 Funções de Chebyshev $\psi(x)$ e $\theta(x)$ 36
4.2 Relações entre $\theta(x)$ e $\pi(x)$ 37
4.3 Algumas formas equivalentes do teorema dos números primos 39

5 GRUPOS ABELIANOS FINITOS E SEUS CARACTERES 41
5.1 Algumas definições 41
5.2 Propriedades elementares 41
5.3 Construção de subgrupos 42
5.4 Caracteres de grupos abelianos finitos 43
5.5 O grupo de caracteres 45
5.6 Relação de ortogonalidade para caracteres 46

5.7 Caracteres de Dirichlet 47

6 TEOREMA DE DIRICHLET PARA PRIMOS EM PROGRESSÕES ARITMÉTICAS 50
6.1 Produto de Euler 50
6.2 L-séries de Dirichlet 53
6.3 Prova do teorema 55

7 FUNÇÕES ARITMÉTICAS PERIÓDICAS E SOMAS DE GAUSS . . . 56
7.1 Funções periódicas módulo k 56
7.2 Existência de série de Fourier finita para funções aritméticas periódicas . . . 56
7.3 Somas de Ramanujan e generalizações 58
7.4 Propriedades multiplicativas de $s_k(n)$ 60
7.5 Somas de Gauss associadas a Caracteres de Dirichlet 62
7.6 Caracteres de Dirichlet com somas de Gauss não nulas 63
7.7 Módulo induzido e caracteres primitivos 64
7.8 Propriedades de módulo induzido 65
7.9 O condutor de um caractere 67
7.10 Caracteres primitivos e somas de Gauss separáveis 67
7.11 A série de Fourier finita dos caracteres de Dirichlet 68
7.12 A desigualdade de Pólya 69

II APLICAÇÕES DE GEOMETRIA FRACTAL E SISTEMAS DINÂMICOS EM TEORIA DOS NÚMEROS **71**

8 MOTIVAÇÕES 72

9 PRELIMINARES 78
9.1 Medidas e distribuições de massa 78

10 MEDIDA DE HAUSDORFF E DIMENSÃO 83
10.1 Medida de Hausdorff 83
10.2 Dimensão de Hausdorff 86
10.3 Exemplos de cálculo de dimensão de Hausdorff 89

11 OUTRAS DEFINIÇÕES DE DIMENSÃO 92
11.1 Dimensão box 92
11.2 Propriedades da dimensão box 97

12 TÉCNICAS PARA CALCULAR DIMENSÕES 99

13 SISTEMA ITERADO DE FUNÇÕES 105
13.1 Dimensão de conjuntos autossimilares 108

13.2 Variações 111

14 APLICAÇÕES EM TEORIA DOS NÚMEROS 116
14.1 Frações contínuas 116
14.2 Aproximações diofantinas 118
14.3 O teorema de Jarník 120

REFERÊNCIAS 123

1 INTRODUÇÃO

O presente trabalho tem como objetivo explorar conexões entre diversas áreas da matemática, incluindo análise, sistemas dinâmicos, geometria fractal e teoria dos números. Na primeira parte estudamos algumas funções aritméticas que surgem naturalmente ao investigar as propriedades aritméticas dos números inteiros. Analisar o comportamento médio dessas funções nos permite determinar se existe, de maneira geral, uma grande quantidade de números naturais ou inteiros com uma determinada propriedade. Esse comportamento médio é estudado através de técnicas analíticas não convencionais. Provamos algumas formas equivalentes do teorema dos números primos através de relações com as funções de Chebyshev. Além de explorar identidades clássicas como a identidade de Abel, investigamos o grupo de caracteres de um grupo, resultados sobre somas de Gauss associadas a caracteres de Dirichlet e séries de Fourier finitas para certas funções e como isso implica em desigualdades significativas, como a desigualdade de Pólya. Descrevemos detalhadamente a ideia de Dirichlet para provar a infinitude de números primos em progressões aritméticas e sua relação com L-séries e números complexos.

Na segunda parte, abordamos conceitos de dimensão fractal, que generaliza a definição encontrada em álgebra linear e possivelmente em cursos avançados de geometria diferencial. A dimensão de Hausdorff e a dimensão box frequentemente exigem elementos combinatoriais que surgem naturalmente ao estudar objetos em sistemas dinâmicos. Esses objetos são construídos a partir de funções especiais que permitem estimar a dimensão de conjuntos específicos. Como exemplo, utilizando a aplicação de Gauss, que está intimamente ligada a frações contínuas, estimamos a dimensão de Hausdorff do conjunto dos números reais cuja expansão em fração contínua consiste apenas nos dígitos 1 e 2. Finalmente, fazendo uso de uma análise detalhada de conjuntos fractais construídos de maneira análoga ao conjunto de Cantor ternário, demonstramos um teorema célebre de Jarnik que estima a dimensão de Hausdorff do conjunto dos pontos α-bem aproximáveis. As definições e conceitos necessários são apresentados ao longo do texto, e um entendimento sólido de análise real e teoria elementar dos números é recomendado para uma leitura proveitosa.

Parte I

Aplicações de Análise em Teoria dos Números

2 Funções Aritméticas

2.1 FUNÇÕES BÁSICAS

Uma função real, ou complexa, cujo domínio é o conjunto dos inteiros positivos é chamada de **função aritmética**, i.e., $f : \mathbb{Z}^+ \to \mathbb{R}$ ou $f : \mathbb{Z}^+ \to \mathbb{C}$.

Definição 2.1. Definimos as funções aritméticas N^α como $N^\alpha(n) = n^\alpha$ para todo $n \in \mathbb{Z}^+$ e $\alpha \in \mathbb{R}$. Chamadas de funções potência.

Observação. Em particular, quando $\alpha = 1$, escrevemos $N(n) = n$. E quando $\alpha = 0$ escrevemos $N^0(n) = u(n) = 1$, chamada a função unitária.

2.2 A FUNÇÃO $\mu(n)$ DE MÖBIUS

Definição 2.2. A função piso, ou função parte inteira, é a função definida como $\lfloor x \rfloor = \max\{m \in \mathbb{Z} \mid m \leq x\}$.

Por exemplo, temos $\lfloor \pi \rfloor = 3$, $\lfloor -\pi \rfloor = -4$, $\lfloor e \rfloor = 3$, $\lfloor -e \rfloor = -4$, $\lfloor 4 \rfloor = 4$ e $\lfloor -4 \rfloor = -4$.

Definição 2.3. A função de Möbius μ é definida da seguinte forma:

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } a^2 | n \text{ para algum } a > 1 \\ (-1)^k & \text{se } n \text{ é produto de } k \text{ primos distintos} \end{cases}$$

Por exemplo, temos $\mu(105) = \mu(3 \cdot 5 \cdot 7) = (-1)^3 = -1$ e $\mu(325) = \mu(5^2 \cdot 13) = 0$.

Teorema 2.1. Se $n \geq 1$ temos que

$$\sum_{d|n} \mu(d) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 \text{ se } n = 1, \\ 0 \text{ se } n > 1. \end{cases}$$

Demonstração. A fórmula é fácilmente verificada se $n = 1$. Assuma que $n > 1$ e seja $n = p_1^{a_1} ... p_k^{a_k}$. Na soma $\sum_{d|n} \mu(d)$ os únicos termos diferentes de 0 vêm de $d = 1$ e dos divisores de n que são produtos de primos distintos. Assim

$$\begin{aligned} \sum_{d|n} \mu(d) =& \mu(1) + \mu(p_1) + ... + \mu(p_k) + \mu(p_1 p_2) + ... + \mu(p_{k-1} p_k) \\ & + ... + \mu(p_1 p_2 \cdots p_k) \\ =& 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + ... + \binom{k}{k}(-1)^k = (1-1)^k = 0. \end{aligned}$$

No último passo utilizamos o teorema binomial

$$(x+y)^k = \binom{k}{0} x^k y^0 + \binom{k}{1} x^{k-1} y^1 + \binom{k}{2} x^{k-2} y^2 + \cdots + \binom{k}{k} x^0 y^k.$$

□

2.3 A FUNÇÃO TOTIENTE DE EULER $\varphi(n)$

Definição 2.4. Se $n \geq 1$ a função totiente de Euler $\varphi(n)$ é definida como a quantidade de números inteiros positivos e menores que n que são relativamente primos com n; isto é,

$$\varphi(n) = \sum_{k=1}^{n}{}' 1 \tag{2.1}$$

Onde $'$ indica que a soma percorre os k relativamente primos a n.

Para melhor entendimento, segue uma tabela de valores de $\varphi(n)$:

n:	1	2	3	4	5	6	7	8	9	10
$\varphi(n)$:	1	1	2	2	4	2	6	4	6	4

Teorema 2.2. Se $n \geq 1$ temos que

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

Demonstração. Seja S o conjunto $\{1, 2, ..., n\}$. Distribuiremos os elementos de S em conjuntos disjuntos. Para cada divisor d de n, seja (a, b) o mdc entre a e b e

$$A(d) = \{k : (k, n) = d, 1 \leq k \leq n\} = \{1 \leqslant k \leqslant n; \text{mdc}(k, n) = d\}.$$

Isto é, $A(d)$ contém os elementos k de S que têm mdc d com n. Os conjuntos $A(d)$ formam uma coleção disjunta cuja união é S, i.e., $\bigcup_{d|n} A(d) = S$. Dessa forma se $f(d)$ denota o número de inteiros em $A(d)$ temos que

$$\sum_{d|n} f(d) = n. \tag{2.2}$$

Mas, $(k, n) = d \iff (k/d, n/d) = 1$. Como $k/d \leq n/d$, podemos concluir que k está em $A(d)$ se k/d for relativamente primo com n/d. Logo, em $A(d)$ temos exatamente $\varphi(n/d)$ elementos. Pela equação (2.2), usando que $f(d) = |A(d)| = \varphi(n/d)$ temos

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

O fato de que para cada divisor d de n, n/d é também um divisor de n, significa que quando d percorre o conjunto dos divisores de n, n/d também percorre este mesmo conjunto. Portanto, $\sum_{d|n} \varphi(d) = n$. □

2.4 UMA RELAÇÃO ENTRE φ E μ

As funções aritméticas das seções 2.2 e 2.3 são objetos de estudo por se conectarem com diversos outros problemas em Teoria dos Números, convém obter desde já uma relação entre elas.

Teorema 2.3. Se $n \geq 1$ temos que

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

Demonstração. A soma (2.1) da definição de $\varphi(n)$ pode ser reescrita na forma

$$\varphi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{(n,k)} \right\rfloor$$

onde k agora percorre todos os inteiros $\leq n$. Agora usamos o Teorema 2.1 com n substituído por (n,k) para obter

$$\varphi(n) = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d).$$

Isto nos diz que para um divisor fixo d de n devemos somar para todos os k no intervalo $1 \leq k \leq n$ que são múltiplos de d. Se escrevermos $k = qd$ então $1 \leq k \leq n$ se somente se $1 \leq q \leq n/d$. Assim podemos reescrever a última soma como

$$\varphi(n) = \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d|n} \mu(d)\frac{n}{d}.$$

□

2.5 A FUNÇÃO φ COMO UM PRODUTO

Podemos utilizar a expressão para $\varphi(n)$ provada no Teorema 2.3 para expressar $\varphi(n)$ como um produto estendido sobre os divisores primos distintos de n.

No próximo teorema, para $n = 1$ o produto é vazio, já que não há primos que dividem 1, portanto vamos definir que o produto é 1.

Teorema 2.4. Para $n > 1$ nós temos

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) \tag{2.3}$$

Demonstração. Suponha que $n > 1$ e sejam $p_1, ..., p_r$ os primos distintos divisores de n. O produto pode ser escrito como

$$\begin{aligned} \prod_{p|n} \left(1 - \frac{1}{p}\right) &= \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \\ &= 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k} + ... + \sum \frac{(-1)^r}{p_1 p_2 \cdots p_r}. \end{aligned} \tag{2.4}$$

Note que cada termo à direita da primeira linha é da forma $\pm 1/d$ onde d é um divisor de n que é 1 ou um produto de primos distintos. O númerador ± 1 é exatamente $\mu(d)$. Como $\mu(d) = 0$ se d é divisível pelo quadrado de qualquer p_i vemos que a soma é exatamente igual a

$$\sum_{d|n} \frac{\mu(d)}{d}.$$

E vimos no teorema anterior que $\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$.

□

Proposição 2.1. $\varphi(m \cdot n) = \varphi(m)\varphi(n)$ sempre que mdc$(m, n) = 1$.

Demonstração. Vamos dispor os números de 1 até mn da seguinte forma:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \dots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \dots & (n-1)m+2 \\ 3 & m+3 & 2m+3 & \dots & (n-1)m+3 \\ & & & \vdots & \\ m & 2m & 3m & \dots & nm \end{array}$$

Se na linha r, onde estão os termos $r, m+r, 2m+r, ..., (n-1)m+r$, tivermos $(m, r) = d > 1$, então nenhum termo nesta linha será primo com mn, uma vez que estes termos, sendo da forma $km + r$, $0 \leq k \leq n-1$, são todos divisíveis por d que é o máximo divisor comum de m e r. Logo, para encontrarınos os inteiros desta tabela que são primos com mn, devemos olhar na linha r somente se $(m, r) = 1$. Portanto temos $\varphi(m)$ linhas onde todos os elementos são primos com m.

Devemos, pois, procurar em cada uma dessas $\varphi(m)$ linhas, quantos elementos säo primos com n, uma vez que todos são primos com m. Como $(m, n) = 1$ os elementos $r, m+r, 2m+r, ..., (n-1)m+r$ formam um sistema completo de resíduos módulo n. Logo, cada uma destas linhas possui $\varphi(n)$ elementos primos com n e, portanto, como eles são primos com m, eles säo prinos com mn. Isto nos garante que $\varphi(mn) = \varphi(m)\varphi(n)$. □

Proposição 2.2. Para p primo e k um inteiro positivo temos

$$\varphi(p^k) = p^k - p^{k-1}$$

Demonstração. Observe que $\varphi(p^k)$ é por definição a quantidade de números menores e coprimos com p^k. Como p é primo, os únicos números n tais que mdc$(n, p^k) > 1$ são os múltiplos de p, i.e., $\{1p, 2p, 3p, \dots, p^{k-1}p\}$. Este conjunto tem cardinalidade igual a p^{k-1}, portanto $\varphi(p^k) = p^k - p^{k-1}$. □

Note em particular que as Proposições 2.1 e 2.2 conjuntamente com o Teorema Fundamental da Aritmética fornecem outra prova do Teorema 2.4.

2.6 CONVOLUÇÃO DE DIRICHLET (OU PRODUTO DE DIRICHLET)

Definição 2.5. Se f e g são duas funções aritméticas nós definimos sua convolução de Dirichlet como a função aritmética h determinada pela equação

$$h(n) = \sum_{d|n} f(d)g\left(\frac{n}{d}\right).$$

Escrevemos $f * g$ para h e $(f * g)(n)$ para $h(n)$. Nesta notação, o Teorema 2.3 pode ser escrito da forma

$$\varphi = \mu * N$$
$$\varphi = \sum_{d|n} \mu(d) N\left(\frac{n}{d}\right)$$

Proposição 2.3. A convolução de Dirichlet é comutativa e associativa. Isto é, para quaisquer funções aritméticas f, g, k temos

$$f * g = g * f \quad \text{(propriedade comutativa)}$$

$$(f * g) * k = f * (g * k) \quad \text{(propriedade associativa)}$$

Demonstração. Primeiro note que a definição de $f * g$ pode ser expressa como segue:

$$(f * g)(n) = \sum_{a \cdot b = n} f(a) g(b),$$

onde a e b percorrem todos os inteiros positivos cujo produto é n. Assim a propriedade comutativa sai de imediato. Para provar a propriedade associativa defina $A = g * k$ e considere $f * A = f * (g * k)$. Temos que

$$(f * A)(n) = \sum_{a \cdot d = n} f(a) A(d) = \sum_{a \cdot d = n} f(a) \sum_{b \cdot c = d} g(b) k(c)$$

$$= \sum_{a \cdot b \cdot c = n} f(a) g(b) k(c).$$

Da mesma forma, se definirmos $B = f * g$ e considerarmos $B * k$ somos levados para a mesma fórmula para $(B * k)(n)$. Por isso $f * A = B * k$ que significa que a convolução de Dirichlet é associativa. □

Observação. Podemos definir o monoide das funções aritméticas $(\mathcal{F}, *)$ cuja operação é o produto de Dirichlet.

Definição 2.6. A função aritmética I dada por

$$I(n) = \left\lfloor \frac{1}{n} \right\rfloor = \begin{cases} 1 \text{ se } n = 1, \\ 0 \text{ se } n > 1. \end{cases}$$

É chamada de função identidade.

Proposição 2.4. Para todo f temos $I * f = f * I = f$.

Demonstração. Temos que

$$(f * I)(n) = \sum_{d|n} f(d) I\left(\frac{n}{d}\right) = \sum_{d|n} f(d) \left\lfloor \frac{d}{n} \right\rfloor = f(n)$$

porque $\lfloor d/n \rfloor = 0$ se $d < n$ □

2.7 INVERSOS DE DIRICHLET E A FÓRMULA DE INVERSÃO DE MÖBIUS

Teorema 2.5. Seja $\mathcal{F}$ o conjunto das funções aritméticas f tais que $f(1) \neq 0$, então f pertence ao grupo das unidades do monoide $(\mathcal{F}, *)$, isto é, existe uma função aritmética única g, chamada a inversa de Dirichlet de f, tal que

$$f * g = g * f = I.$$

Ademais, $g = f^{-1}$ é dada pelas fórmulas recursivas

$$f^{-1}(1) = \frac{1}{f(1)}, \quad f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) \quad \text{para } n > 1.$$

Demonstração. Dada f, devemos mostrar que a equação $(f * f^{-1})(n) = I(n)$ tem uma única solução para os valores da função $f^{-1}(n)$. Para $n = 1$ temos que resolver a equação

$$(f * f^{-1})(1) = I(1)$$

que se reduz a

$$f(1)f^{-1}(1) = 1.$$

Como $f(1) \neq 0$ existe uma única solução, a saber $f^{-1}(1) = 1/f(1)$. Por indução suponha que os valores da função $f^{-1}(k)$ foram determinados para todo $k < n$. Agora temos que resolver a equação $(f * f^{-1})(n) = I(n)$, ou

$$\sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0.$$

Que pode ser escrita como

$$f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) = 0.$$

e os valores de $f^{-1}(d)$ são conhecidos para todos os divisores $d < n$, há um único valor determinado para $f^{-1}(n)$, a saber,

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d),$$

como $f(1) \neq 0$. Isto estabelece a existência e unicidade de f^{-1} por indução.

□

Observação. Podemos definir o grupo abeliano $(\mathcal{F}, *, I)$, onde $\mathcal{F}$ é conjunto de todas funções aritméticas f tal que $f(1) \neq 0$ e o elemento identidade é a função I. Discutiremos mais noções de álgebra abstrata no Capítulo 5.

Observação. O Teorema 2.1 nos diz que $\sum_{d|n} \mu(d) = I(n)$. Na notação da convolução de Dirichlet, isso torna-se

$$\mu * u = I.$$

Assim u e μ são inversos de Dirichlet um do outro:

$$u = \mu^{-1} \qquad \text{e} \qquad \mu = u^{-1}.$$

Com isso em mãos, a prova da fórmula de inversão de Möbius fica mais clara:

Teorema 2.6. Fórmula de inversão de Möbius.

$$f(n) = \sum_{d|n} g(d) \Leftrightarrow g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right).$$

Demonstração. ($\Rightarrow$) Suponha que $f = g * u$, multiplicando por μ obtemos $f * \mu = (g * u) * \mu = g * (u * \mu) = g * I = g$. Assim encontramos que $g = f * \mu$, exatamente o que queríamos.
($\Leftarrow$) Supondo $g = f * \mu$ e multiplicando por u achamos $f = g * u$.

□

Exemplo 2.1. A fórmula de inversão de Möbius pode ser usada pra obter o Teorema 2.2 a partir do Teorema 2.3 e vice versa. Usando a notação de convolução de Dirichlet:

$$N = \varphi * u \Longleftrightarrow \varphi = \mu * N$$

Demonstração. ($\Rightarrow$) Basta multiplicar por μ em ambos os lados e usar comutatividade e associatividade.
($\Leftarrow$) Basta multiplicar por u em ambos os lados e usar comutatividade e associatividade. □

2.8 A FUNÇÃO DE MANGOLDT $\Lambda(n)$

Definição 2.7. Para todo inteiro $n \geq 1$ definimos

$$\Lambda(n) = \begin{cases} \log p & \text{se } n = p^m \text{ para algum primo } p \text{ e algum } m \geq 1, \\ 0 & \text{caso contrário} \end{cases}$$

Exemplo 2.2. Segue uma tabela de valores de $\Lambda(n)$:

n:	1	2	3	4	5	6	7	8	9	10
$\Lambda(n)$:	0	$\log 2$	$\log 3$	$\log 2$	$\log 5$	0	$\log 7$	$\log 2$	$\log 3$	0

Teorema 2.7. Se $n \geq 1$ temos que

$$\log n = \sum_{d|n} \Lambda(d). \tag{2.5}$$

Demonstração. Para $n = 1$ é fácil ver a veracidade. Portanto assuma que $n > 1$ e seja

$$n = \prod_{k=1}^{r} p_k^{a_k}.$$

Aplicando logaritmos ficamos com

$$\log n = \sum_{k=1}^{r} a_k \log p_k.$$

Considere a soma à direita de 2.5. Os únicos termos diferentes de 0 vêm dos divisores de d da forma p_k^m com $m = 1, 2, ..., a_k$ e $k = 1, 2, ..., r$. Por isso

$$\sum_{d|n} \Lambda(d) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \Lambda(p_k^m) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \log p_k = \sum_{k=1}^{r} a_k \log p_k = \log n,$$

o que prova o teorema. □

Agora vamos usar a fórmula inversão de Möbius para expressar $\Lambda(n)$ em termos de logaritmo.

Teorema 2.8. Se $n \geq 1$ temos que

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = -\sum_{d|n} \mu(d) \log d.$$

Demonstração. Invertendo 2.5 com a fórmula de inversão de Möbius obtemos

$$\begin{aligned} \Lambda(n) =& \sum_{d|n} \mu(d) \log \frac{n}{d} = \log n \sum_{d|n} \mu(d) - \sum_{d|n} \mu(d) \log d \\ =& I(n) \log n - \sum_{d|n} \mu(d) \log d. \end{aligned}$$

Uma vez que $I(n) \log n = 0$ para todo n a prova está completa. □

2.9 FUNÇÕES MULTIPLICATIVAS

Nesta seção introduziremos uma classe de funções de extrema relevância, a classe de funções multiplicativas e mostraremos que esta classe munida da convolução de Dirichlet forma um subgrupo de $(\mathcal{F}, *, I)$. Comentamos mais sobre aspectos de grupos no capítulo 5.

Definição 2.8. Uma função aritmética f é chamada multiplicativa se f não é nula e se

$$f(mn) = f(m)f(n) \text{ sempre que } (m, n) = 1.$$

e f é chamada completamente multiplicativa se temos

$$f(mn) = f(m)f(n) \text{ para todo } m, n.$$

Exemplo 2.3. A função potência $N^\alpha(n)$ e a função identidade $I(n)$ são completamente multiplicativas.

Exemplo 2.4. A função de Mobius $\mu(n)$ e a função totiente de Euler $\varphi(n)$ (Proposição 2.1) são multiplicativas.

Observação. Se f é multiplicativa, então $f(1) = 1$. A prova não é difícil e fica à cargo do leitor.

Teorema 2.9. Dada f com $f(1) = 1$. Temos:

a) f é multiplicativa se, e somente se,

$$f(p_1^{a_1} \dots p_r^{a_r}) = f(p_1^{a_1}) \dots f(p_r^{a_r})$$

para todo primo p_i e todo inteiro $a_i \geq 1$.

b) Se f é multiplicativa, então f é completamente multiplicativa se, e somente se,

$$f(p^a) = f(p)^a$$

para todo primo p e todo inteiro $a \geq 1$.

Demonstração. a) ($\Rightarrow$) $p_i^{a_i}$ e $p_j^{a_j}$ são coprimos para quaisquer $i \neq j$, como f é multiplicativa, segue que $f(p_1^{a_1} \dots p_r^{a_r}) = f(p_1^{a_1}) \dots f(p_r^{a_r})$.
($\Leftarrow$) Segue pelo teorema fundamental da aritmética e pela definição de função multiplicativa.

b) Segue pelo item anterior.

□

Teorema 2.10. Se f e g são multiplicativas, o produto de Dirichlet $f * g$ também é.

Demonstração. Seja $h = f * g$ e m, n inteiros coprimos. Temos

$$h(mn) = \sum_{c|mn} f(c) g\left(\frac{mn}{c}\right).$$

Todo divisor positivo c de mn pode ser expresso da forma $c = ab$ onde $a|m$ e $b|n$. Além disso, $(a, b) = 1$, $(m/a, n/b) = 1$, e existe uma função injetiva entre os o conjunto dos produtos ab e os divisores c de mn. Daí,

$$\begin{aligned} h(mn) &= \sum_{\substack{a|m \\ b|n}} f(ab) g\left(\frac{mn}{ab}\right) = \sum_{\substack{a|m \\ b|n}} f(a) f(b) g\left(\frac{m}{a}\right) g\left(\frac{n}{b}\right) \\ &= \sum_{a|m} f(a) g\left(\frac{m}{a}\right) \sum_{b|n} f(b) g\left(\frac{n}{b}\right) = h(m) h(n). \end{aligned}$$

□

Teorema 2.11. Se g e $f * g$ são multiplicativas, então f também é.

Demonstração. Vamos supor que f não é multiplicativa e provar que $f * g$ também não seria. Seja $h = f * g$. Como f não é multiplicativa existem $m, n \in \mathbb{Z}^+$ com $(m, n) = 1$ tais que

$$f(mn) \neq f(m)f(n).$$

Escolhemos os menores m, n possíveis.
Se $mn = 1$, então $f(1) \neq f(1)f(1)$ e $f(1) \neq 1$. Como $h(1) = f(1)g(1) = f(1) \neq 1$, h não é multiplicativa.
Se $mn > 1$, temos $f(ab) = f(a)f(b)$ para todos $a, b \in \mathbb{Z}^+$ com $(a, b) = 1$ e $ab < mn$. Assim, temos

$$\begin{aligned} h(mn) = &\sum_{\substack{a|m \\ b|n \\ ab<mn}} f(ab)g\left(\frac{mn}{ab}\right) + f(mn)g(1) = \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) + f(mn) \\ =&\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\sum_{b|n} f(b)g\left(\frac{n}{b}\right) - f(m)f(n) + f(mn) \\ =&h(m)h(n) - f(m)f(n) + f(mn) \end{aligned}$$

Como $f(mn) \neq f(m)f(n)$, isso mostra que $h(mn) \neq h(m)h(n)$, ou seja, h não é multiplicativa. Isto completa a prova. □

Teorema 2.12. Se g é multiplicativa, g^{-1} também é.

Demonstração. Direto do teorema anterior, pois g e $g * g^{-1} = I$ são multiplicativas. □

2.10 FUNÇÃO DE LIOUVILLE $\lambda(n)$

Definição 2.9. Definimos $\lambda(1) = 1$, e se $n = p_1^{a_1} \dots p_k^{a_k}$ definimos

$$\lambda(n) = (-1)^{a_1 + \cdots + a_k}.$$

Segue da definição que λ é completamente multiplicativa.

Teorema 2.13. Para todo $n \geq 1$ temos

$$\sum_{d|n} \lambda(d) = \begin{cases} 1 & \text{se } n \text{ é quadrado,} \\ 0 & \text{caso contrário.} \end{cases}$$

Além disso, $\lambda^{-1}(n) = |\mu(n)|$ para todo n.

Demonstração. Seja $g(n) = \sum_{d|n} \lambda(d)$. Note que g é multiplicativa, então para determinar $g(n)$ só precisamos olhar g aplicada em potência de primos. Temos

$$\begin{aligned} g(p^a) = \sum_{d|p^a} \lambda(d) =&1 + \lambda(p) + \lambda(p^2) + \cdots + \lambda(p^a) \\ =&1 - 1 + 1 - \cdots + (-1)^a = \begin{cases} 0 & \text{se a é ímpar,} \\ 1 & \text{se a é par.} \end{cases} \end{aligned}$$

Por isso se $n = \prod_{i=1}^{k} p_i^{a_i}$ temos $g(n) = \prod_{i=1}^{k} g(p_i^{a_i})$. Se qualquer expoente a_i for ímpar, $g(p_i^{a_i}) = 0$, por isso $g(n) = 0$. Se todos expoentes a_i são pares, então $g(p_i^{a_i}) = 1$ para todo i e $g(n) = 1$. Assim provamos a primeira parte, para a segunda, note que $\lambda^{-1}(n) = \mu(n)\lambda(n) = \mu^2(n) = |\mu(n)|$. □

2.11 AS FUNÇÕES DIVISORES $\sigma_\alpha(n)$

Definição 2.10. Para α real ou complexo e qualquer inteiro $n \geq 1$ definimos

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha,$$

a soma das α-ésimas potências dos divisores de n. Vamos falar algumas propriedades destas funções.

São multiplicativas, pois $\sigma_\alpha = u * N^\alpha$, produto de duas funções multiplicativas.

Quando $\alpha = 0$, $\sigma_0(n)$ é o número de divisores de n, muitas vezes denotado por $d(n)$.

Quando $\alpha = 1$, $\sigma_1(n)$ é a soma dos divisores de n, comumente denotado por $\sigma(n)$.

Como $\sigma_\alpha(n)$ é multiplicativa, temos

$$\sigma_\alpha(p_1^{a_1} \dots p_k^{a_k}) = \sigma_\alpha(p_1^{a_1}) \dots \sigma_\alpha(p_k^{a_k})$$

Para computar $\sigma_\alpha(p^a)$ notemos que os divisores de p^a com p primo são

$$1, p, p^2, \dots, p^a,$$

portanto

$$\begin{aligned} \sigma_\alpha(p^a) = 1^\alpha + p^\alpha + p^{2\alpha} + \cdots + p^{a\alpha} &= \frac{p^{\alpha(a+1)} - 1}{p^\alpha - 1} \quad \text{se } \alpha \neq 0 \\ &= a + 1 \qquad\qquad \text{se } \alpha = 0 \end{aligned}$$

Teorema 2.14. Para $n \geq 1$ temos

$$\sigma_\alpha^{-1}(n) = \sum_{d|n} d^\alpha \mu(d) \mu\left(\frac{n}{d}\right).$$

Demonstração. Como $\sigma_\alpha = N^\alpha * u$ e N^α é completamente multiplicativa temos

$$\sigma_\alpha^{-1} = (\mu N^\alpha) * u^{-1} = (\mu N^\alpha) * \mu.$$

□

3 Médias de funções aritméticas

3.1 INTRODUÇÃO

No último capítulo discutimos várias identidades satisfeitas por funções aritméticas como $\mu(n), \varphi(n), \Lambda(n)$, e as funções divisores $\sigma_\alpha(n)$. Uma pergunta natural é sobre o comportamento destas e de outras funções aritméticas $f(n)$ para valores grandes de n.

Por exemplo, considere $d(n)$, o número de divisores de n. Esta função assume o valor 2 infinitamente (quando n é primo) e também assume valores arbitrariamente grandes quando n tem um grande número de divisores. Assim, os valores de $d(n)$ flutuam consideravelmente à medida que n aumenta.

Isto acontece com muitas funções aritméticas, por conta disso é interessante estudar a média aritmética dessas funções

$$\tilde{f}(n) = \frac{1}{n}\sum_{k=1}^{n} f(k)$$

Médias costumam suavizar flutuações, por isso é razoável esperar que as médias $\tilde{f}(n)$ podem se comportar mais regularmente do que $f(n)$. Para estudar a média de uma função arbitrária f precisamos conhecer suas somas parciais $\sum_{k=1}^{n} f(k)$. Às vezes é conveniente substituir o índice superior n por um número real positivo arbitrário x e considerar somas da forma

$$\sum_{k\leq x} f(k).$$

Aqui entende-se que o índice k varia de 1 a $\lfloor x \rfloor$, o maior inteiro menor ou igual a x. Se $0 < x < 1$ a soma é vazia e atribuímos a ela o valor 0. Nosso objetivo é determinar o comportamento desta soma em função de x, especialmente para x grandes.

3.2 NOTAÇÃO GRANDE O

Definição 3.1. Se $g(x) > 0$ para todo $x \geq a$, escrevemos

$$f(x) = O(g(x))$$

para dizer que o quociente $f(x)/g(x)$ é limitado para $x \geq a$; isto é, existe uma constante $M > 0$ tal que

$$|f(x)| \leq Mg(x) \text{ para todo } x \geq a$$

Uma equação da forma

$$f(x) = h(x) + O(g(x))$$

significa que $f(x) - h(x) = O(g(x))$.

Definição 3.2. Se

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

dizemos que $f(x)$ é assintótico a $g(x)$ quando $x \to +\infty$, e escrevemos

$$f(x) \sim g(x) \text{ quando } x \to +\infty.$$

A notação O é comumente usada para representar o "erro" na aproximação de uma equação quando temos termos que crescem pouco comparados com outras parcelas.

3.3 FÓRMULA DE SOMA DE EULER

$\zeta(s)$ é a função zeta de Riemann, definida como

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \text{ se } \mathrm{Re}(s) > 1$$

isto é, se a parte real do número complexo $s = a + ib$ é maior que 1. Para definir esta função em toda parte é usada uma ferramenta de análise complexa chamada continuação analítica, e não faremos isto neste texto.

Definimos $\{t\} = t - \lfloor t \rfloor$, $\{t\}$ é chamada **parte fracionária** de t.

Teorema 3.1 (Fórmula da Soma de Euler)**.** Se $f : [x, y] \to \mathbb{R}$ é de classe C^1 (tem derivada contínua f') no intervalo $[y, x]$, onde $0 < y < x$, então

$$\begin{aligned} \sum_{y<n\leq x} f(n) = &\int_y^x f(t)dt + \int_y^x (t - \lfloor t \rfloor) f'(t)dt \\ &+ f(x)(\lfloor x \rfloor - x) - f(y)(\lfloor y \rfloor - y). \end{aligned} \tag{3.1}$$

Onde $\int$ é a integral de Riemann. Frequentemente tomamos $y = 1$, e neste caso

$$\sum_{n\leq x} f(n) = \int_1^x f(t)dt + \int_1^x \{t\} f'(t)dt - \{x\} f(x) + f(1)$$

Demonstração. Seja $m = \lfloor y \rfloor$, $k = \lfloor x \rfloor$. Para inteiros n e $n - 1$ em $[y, x]$ temos

$$\begin{aligned} \int_{n-1}^{n} \lfloor t \rfloor f'(t)dt = &\int_{n-1}^{n} (n-1) f'(t)dt = (n-1)(f(n) - f(n-1)) \\ =&(nf(n) - (n-1)f(n-1)) - f(n). \end{aligned}$$

Somando de $n = m + 2$ até $n = k$ descobrimos que a primeira soma é telescópica, e portanto

$$\begin{aligned} \int_{m+1}^{k} \lfloor t \rfloor f'(t)dt) =&kf(k) - (m+1)f(m+1) - \sum_{n=m+2}^{k} f(n) \\ =&kf(k) - mf(m+1) - \sum_{y<n\leq x} f(n). \end{aligned}$$

Dessa forma

$$\begin{aligned} \sum_{y<n\leq x} f(n) = &- \int_{m+1}^{k} \lfloor t \rfloor f'(t)dt + kf(k) - mf(m+1) \\ = &- \int_y^x \lfloor t \rfloor f'(t)dt + kf(x) - mf(y). \end{aligned} \tag{3.2}$$

Integrando por partes conseguimos

$$\int_y^x f(t)dt = xf(x) - yf(y) - \int_y^x tf'(t)dt,$$

combinando isto com (3.2) obtemos (3.1). □

3.4 ALGUMAS FÓRMULAS ASSINTÓTICAS ELEMENTARES

Teorema 3.2. Se $x \geq 1$ temos:

(a) $\sum_{n\leq x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right)$.

(b) $\sum_{n\leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O(x^{-s})$ se $s > 0, s \neq 1$.

(c) $\sum_{n>x} \frac{1}{n^s} = O(x^{1-s})$ se $s > 1$.

(d) $\sum_{n\leq x} n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha)$ se $\alpha \geq 0$.

Demonstração. Para (a) tome $f(t) = 1/t$ na formula de soma de Euler, obtendo

$$\begin{aligned}\sum_{n\leq x} \frac{1}{n} &= \int_1^x \frac{dt}{t} - \int_1^x \frac{\{t\}}{t^2}dt - \frac{\{x\}}{x} + 1 \\ &= \ln x - \int_1^\infty \frac{\{t\}}{t^2} + \int_x^\infty \frac{\{t\}}{t^2} + 1 + O\left(\frac{1}{x}\right)\end{aligned}$$

observe que

$$\int_x^\infty \frac{\{t\}}{t^2} \leq \int_x^\infty \frac{1}{t^2}dt = \frac{1}{x}$$

que também é limitada por M/x, com $M > 1$, assim

$$\sum_{n\leq x} \frac{1}{n} = \log x + 1 - \int_1^\infty \frac{\{t\}}{t^2}dt + O(1/x)$$

que é a letra (a) com $C = 1 - \int_1^\infty \frac{\{t\}}{t^2}dt$.

Para a letra (b) usamos os mesmo argumento com $f(x) = x^{-s}$, onde $s > 0, s \neq 1$. A fórmula da soma de Euler nos dá

$$\begin{aligned}\sum_{n\leq x} \frac{1}{n^s} &= \int_1^x \frac{dt}{t^s} - s\int_1^\infty \frac{\{t\}}{t^{s+1}}dt + 1 - \frac{\{x\}}{x^s} \\ &= \frac{x^{1-s}}{1-s} - \frac{1}{1-s} + 1 - s\int_1^\infty \frac{\{t\}}{t^{s+1}}dt + O(x^{-s}).\end{aligned}$$

Portanto

$$\sum_{n\leq x} \frac{1}{n^s} = \frac{x^{1-s}}{1-s} + C(s) + O(x^{-s}), \tag{3.3}$$

onde

$$C(s) = 1 - \frac{1}{1-s} - s\int_1^\infty \frac{\{t\}}{t^{s+1}}dt.$$

Se $s > 1$, o lado esquerdo de (3.3) se aproxima de $\zeta(s)$ quando $x \to +\infty$ e os termos x^{1-s} e x^{-s} se aproximam de 0. Por isso $C(s) = \zeta(s)$ se $s > 1$. Se $0 < s < 1$, $x^{-s} \to 0$ e (3.3) mostra que

$$\lim_{x\to\infty}\left(\sum_{n\leq x}\frac{1}{n^s} - \frac{x^{1-s}}{1-s}\right) = C(s).$$

Portanto $C(s)$ também é igual a $\zeta(s)$ se $0 < s < 1$. Assim provamos (b).

Para a letra (c) usamos (b) com $s > 1$ e obtemos

$$\sum_{n>x}\frac{1}{n^s} = \zeta(s) - \sum_{n\leq x}\frac{1}{n^s} = \frac{x^{1-s}}{s-1} + O(x^{-s}) = O(x^{1-s})$$

desde que $x^{-s} \leq x^{1-s}$

Finalmente, para a letra (d) usamos a fórmula da soma de Euler com $f(t) = t^\alpha$:

$$\begin{aligned}\sum_{n\leq x} n^\alpha =& \int_1^x t^\alpha dt + \alpha\int_1^x t^{\alpha-1}\{t\}dt + 1 - \{x\}x^\alpha \\ =& \frac{x^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1} + O\left(\alpha\int_1^x t^{\alpha-1}dt\right) + O(x^\alpha) \\ =& \frac{x^{\alpha+1}}{\alpha+1} + O(x^\alpha).\end{aligned}$$

□

3.5 O VALOR MÉDIO DAS FUNÇÕES DIVISORES $\sigma_\alpha(n)$

Teorema 3.3. Para todo $x \geq 1$ temos

$$\sum_{n\leq x} d(n) = x\log x + (2C-1)x + O(\sqrt{x}), \tag{3.4}$$

onde $C = \lim_{n\to\infty}\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\right)$. chamada de constante de Euler.

Demonstração. Como $d(n) = \sum_{d|n} 1$ temos

$$\sum_{n\leq x} d(n) = \sum_{n\leq x}\sum_{d|n} 1.$$

Isso é uma soma dupla estendida sobre d e n. Como $d|n$, escrevemos $n = qd$ e mudamos a soma para

$$\sum_{n\leq x} d(n) = \sum_{\substack{q,d \\ qd\leq x}} 1. \tag{3.5}$$

Isto pode ser interpretado como uma soma sobre certos pontos de coordenadas inteiras numa região hiperbólica no plano qd, chamados pontos do látice $\mathbb{Z}^2$.

Vamos utilizar a simetria na região sobre a reta $q = d$. O número total de pontos do látice na região é igual ao dobro dos números abaixo da linha $q = d$ somados aos números na reta.

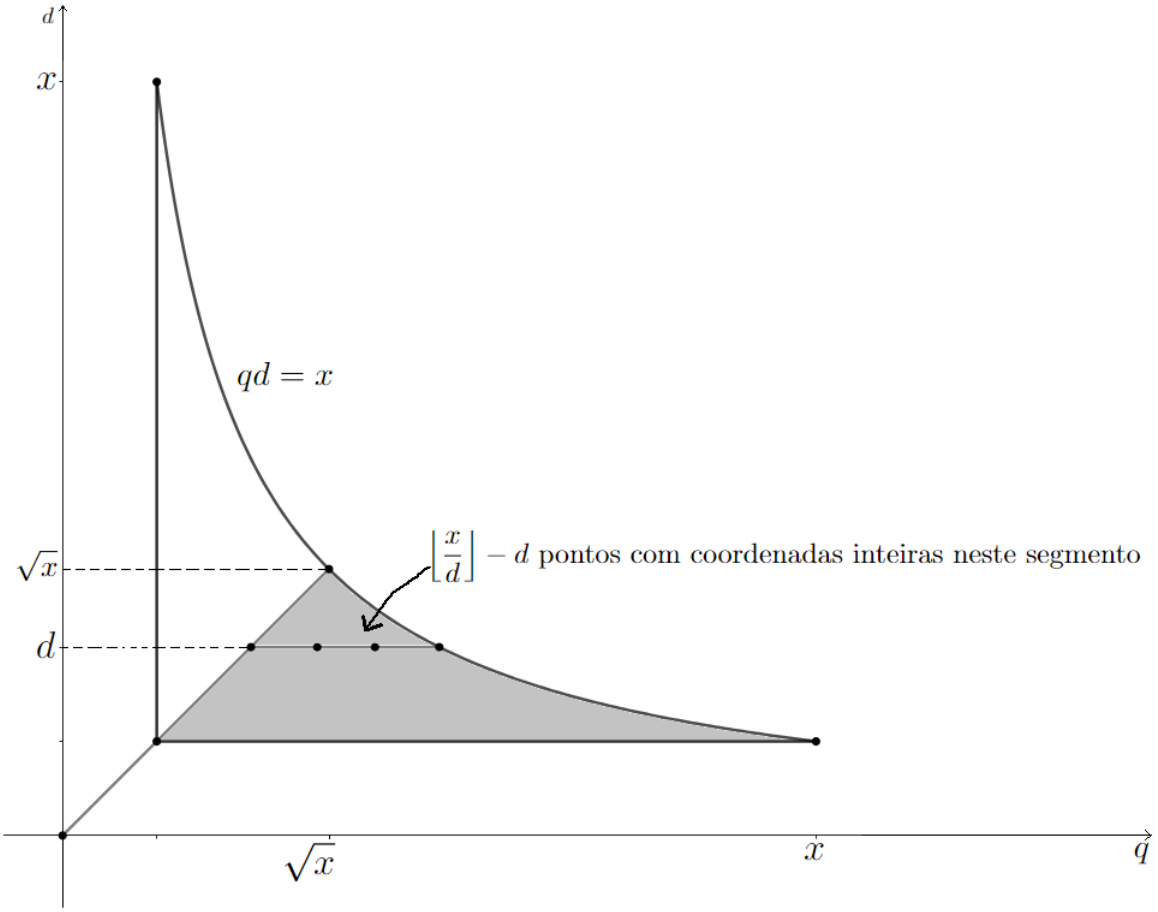


Figura 1 – Plano qd - Fonte: autoria própria

Observando a figura, percebemos que

$$\sum_{n\leq x} d(n) = 2\sum_{d\leq\sqrt{x}} \{\lfloor x/d\rfloor - d\} + \lfloor\sqrt{x}\rfloor$$

Usando a relação $\lfloor y\rfloor = y + O(1)$ e partes a) e d) do Teorema 3.2 obtemos

$$\begin{aligned}\sum_{n\leq x} d(n) =& 2\sum_{d\leq\sqrt{x}} \left\{\frac{x}{d} - d + O(1)\right\} + O(\sqrt{x})\\ =& 2x\sum_{d\leq\sqrt{x}} \frac{1}{d} - 2\sum_{d\leq\sqrt{x}} d + O(\sqrt{x})\\ =& 2x\left\{\log\sqrt{x} + C + O\left(\frac{1}{\sqrt{x}}\right)\right\} - 2\left\{\frac{x}{2} + O(\sqrt{x})\right\} + O(\sqrt{x})\\ =& x\log x + (2C-1)x + O(\sqrt{x}).\end{aligned}$$

□

Teorema 3.4. Para todo $x \geq 1$ temos

$$\sum_{n\leq x} \sigma_1(n) = \frac{1}{2}\zeta(2)x^2 + O(x\log x). \tag{3.6}$$

Demonstração. Usando as partes a) e b) do Teorema 3.2, temos:

$$\begin{aligned}\sum_{n\leq x}\sigma_1(n) =& \sum_{n\leq x}\sum_{q|n} q = \sum_{\substack{q,d\\ qd\leq x}} q = \sum_{d\leq x}\sum_{q\leq x/d} q\\ =& \sum_{d\leq x}\left\{\frac{1}{2}\left(\frac{x}{d}\right)^2 + O\left(\frac{x}{d}\right)\right\} = \frac{x^2}{2}\sum_{d\leq x}\frac{1}{d^2} + O\left(x\sum_{d\leq x}\frac{1}{d}\right)\\ =& \frac{x^2}{2}\left\{-\frac{1}{x} + \zeta(2) + O\left(\frac{1}{x^2}\right)\right\} + O(x\log x) = \frac{1}{2}\zeta(2)x^2 + O(x\log x).\end{aligned}$$

□

O próximo teorema apenas enunciaremos sem demonstração, pois a prova é análoga. Para a prova, use as letras b) e d) do Teorema 3.2.

Teorema 3.5. Se $x \geq 1$ e $\alpha > 0$, $\alpha \neq 1$, temos

$$\sum_{n\leq x}\sigma_\alpha(n) = \frac{\zeta(\alpha+1)}{\alpha+1}x^{\alpha+1} + O(x^\beta),$$

onde $\beta = \max\{1, \alpha\}$.

Para encontrar o valor médio de $\sigma_\alpha(n)$ para α negativo escrevemos $\alpha = -\beta$, com $\beta > 0$.

Teorema 3.6. Se $\beta > 0$ seja $\delta = \max\{0, 1-\beta\}$. Então se $x > 1$ temos

$$\begin{aligned}\sum_{n\leq x}\sigma_{-\beta}(n) &= \zeta(\beta+1)x + O(x^\delta) \text{ se } \beta \neq 1,\\ &= \zeta(2)x + O(\log x) \text{ se } \beta = 1.\end{aligned}$$

Demonstração. Usando a definição de $\sigma_{-\beta}(n) = \sum_{d|n} d^{-\beta}$ e o fato que se $d|n$ então existe q tal que $n = qd$,

$$\begin{aligned}\sum_{n\leq x}\sigma_{-\beta}(n) =& \sum_{n\leq x}\sum_{d|n}\frac{1}{d^\beta} = \sum_{qd\leq x}\sum_{n=qd}\frac{1}{d^\beta} =\\ & \text{podemos comutar as somas pois elas são finitas}\\ =& \sum_{d\leq x}\frac{1}{d^\beta}\sum_{q\leq x/d} 1, \text{ usando a letra d) do Teorema 3.2, temos}\\ =& \sum_{d\leq x}\frac{1}{d^\beta}\left\{\frac{x}{d} + O(1)\right\} = x\sum_{d\leq x}\frac{1}{d^{\beta+1}} + O\left(\sum_{d\leq x}\frac{1}{d^\beta}\right).\end{aligned}$$

O último termo é $O(\log x)$ se $\beta = 1$ e $O(x^\delta)$ se $\beta \neq 1$. Uma vez que

$$x\sum_{n\leq x}\frac{1}{d^{\beta+1}} = \frac{x^{1-\beta}}{-\beta} + \zeta(\beta+1)x + O(x^{-\beta}) = \zeta(\beta+1)x + O(x^{1-\beta}).$$

□

3.6 O VALOR MÉDIO DE $\varphi(n)$

Para analisar o valor médio de $\varphi(n)$, precisamos da série

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Vamos assumir isto como hipótese e note que

$$\begin{aligned}\sum_{n\leq x} \frac{\mu(n)}{n^2} =& \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2} - \sum_{n>x} \frac{\mu(n)}{n^2} \\ =& \frac{6}{\pi^2} + O\left(\sum_{n>x} \frac{1}{n^2}\right) = \frac{6}{\pi^2} + O(1/x)\end{aligned}$$

Onde usamos a parte c) do Teorema 3.2.

Teorema 3.7. Para $x > 1$ temos

$$\sum_{n\leq x} \varphi(n) = \frac{3}{\pi^2}x^2 + O(x\log x) \tag{3.7}$$

Demonstração. Sabemos do Teorema 2.3 que

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

com isso, usando $n = qd$ temos

$$\begin{aligned}\sum_{n\leq x} \varphi(n) =& \sum_{n\leq x}\sum_{d|n} \mu(d)\frac{n}{d} = \sum_{\substack{q,d \\ qd\leq x}} \mu(d)q = \sum_{d\leq x} \mu(d) \sum_{q\leq x/d} q \\ =& \sum_{d\leq x} \mu(d)\left\{\frac{1}{2}\left(\frac{x}{d}\right)^2 + O\left(\frac{x}{d}\right)\right\} \\ =& \frac{1}{2}x^2 \sum_{d\leq x} \frac{\mu(d)}{d^2} + O\left(x\sum_{d\leq x}\frac{1}{d}\right) \\ =& \frac{1}{2}x^2\left\{\frac{6}{\pi^2} + O\left(\frac{1}{x}\right)\right\} + O(x\log x) = \frac{3}{\pi^2}x^2 + O(x\log x).\end{aligned}$$

□

3.7 UMA APLICAÇÃO PARA A DISTRIBUIÇÃO DOS PONTOS DO LÁTICE $\mathbb{Z}^2$ VISÍVEIS DA ORIGEM.

Definição 3.3. Dois pontos de coordenadas inteiras P e Q são chamados mutuamente visíveis se o segmento ligando-os não contém nenhum ponto do látice além de P e Q.

Teorema 3.8. Dois pontos do látice $\mathbb{Z}^2$ (a, b) e (m, n) são mutuamente visíveis se, e somente se, $a - m$ e $b - n$ são relativamente primos.

Demonstração. Primeiro, observe que (a, b) e (m, n) são mutuamente visíveis se, e somente se, $(a - m, b - n)$ é visível da origem. Por isso vamos provar o teorema para $(m, n) = (0, 0)$.
Suponha que (a, b) é visível da origem e seja $mdc(a, b) = d$, queremos mostrar que $d = 1$. Se $d > 1$, então $a = da'$ e $b = db'$ e o ponto do lática (a', b') está no segmento ligando a origem a (a, b), esta contradição prova que $d = 1$.
Reciprocamente, suponha que $mdc(a, b) = 1$. Se um ponto do lática (a', b') está no segmento ligando $(0, 0)$ a (a, b) teríamos

$$a' = ta, \qquad b' = tb, \qquad \text{onde } 0 < t < 1.$$

Daí, t é racional e temos $t = r/s$, onde $r, s \in \mathbb{Z}^+$ e $mdc(r, s) = 1$. Disso

$$sa' = ar \qquad \text{e} \qquad sb' = br,$$

Isso indica que $s|ar$ e $s|br$, e como $mdc(a, b) = 1$, $s = 1$. Isso contradiz a desigualdade $0 < t < 1$. Assim fica claro que o ponto (a, b) é visível da origem. □

Existem infinitos pontos do lática e é natural nos perguntarmos como eles estão distribuídos no plano.

Considere uma área quadrada no plano xy definida pelas desigualdades

$$|x| \leq r, \qquad |y| \leq r.$$

Seja $N(r)$ o número de pontos do lática nesse quadrado, e seja $N'(r)$ o número de pontos visíveis da origem. O quociente $N'(r)/N(r)$ mede a fração de pontos desses pontos do lática que são visíveis da origem.

Teorema 3.9. O conjunto dos pontos do lática visíveis da origem tem densidade $6/\pi^2$.

Demonstração. Provaremos que

$$\lim_{r\to\infty} \frac{N'(r)}{N(r)} = \frac{6}{\pi^2}.$$

Todos os 8 pontos do lática mais próximos da origem são visíveis da origem, veja na figura abaixo. Por simetria, vemos que $N'(r)$ é igual a 8, mais 8 vezes o número de pontos visíveis na região (pois dividimos o plano em 8 partes)

$$\{(x, y) : 2 \leq x \leq r, \quad 1 \leq y \leq x\},$$

que é a região escura na figura. Este número é

$$N'(r) = 8 + 8 \sum_{2\leq n\leq r} \sum_{\substack{1\leq m<n \\ (m,n)=1}} 1 = 8 \sum_{1\leq n\leq r} \varphi(n).$$

Usando o Teorema 3.7 temos

$$N'(r) = \frac{24}{\pi^2} r^2 + O(r \log r).$$

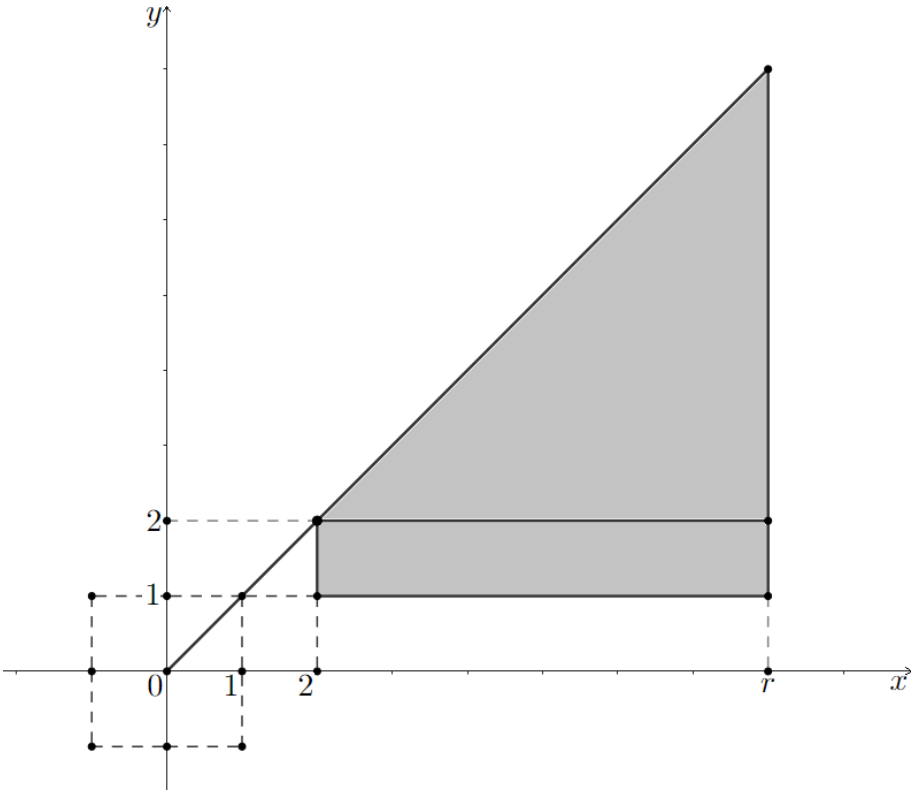


Figura 2 – Pontos do látice $\mathbb{Z}^2$ - Fonte: autoria própria

Mas, o número total de pontos do látice no quadrado é

$$N(r) = (2\lfloor r \rfloor + 1)^2 = (2r + O(1))^2 = 4r^2 + O(r)$$

então

$$\frac{N'(r)}{N(r)} = \frac{\frac{24}{\pi^2}r^2 + O(r \log r)}{4r^2 + O(r)} = \frac{\frac{6}{\pi^2} + O\left(\frac{\log r}{r}\right)}{1 + O(1/r)}$$

Portanto quando $r \to \infty$ encontramos $N'(r)/N(r) \to 6/\pi^2$. □

Este resultado que acabamos de provar é equivalente a dizer que **ao escolher dois números inteiros aleatoriamente, a probabilidade de eles serem primos entre si é igual a** $6/\pi^2 \approx 60\%$. Abaixo apresentamos uma prova mais direta, que usa argumentos probabilísticos e de teoria dos números, assumindo que sabemos o valor de $\zeta(2)$.

Demonstração. A probabilidade de um número qualquer ser divisível por um primo p é $1/p$. Se tivermos s números, a probabilidade de todos serem divisíveis por p, pelo princípio fundamental da contagem, é $1/p^s$. Por conseguinte, a probabilidade de pelo menos um deles não ser divisível por p é $1 - 1/p^s$.

Para primos distintos estes eventos são independentes entre si, pois um número é divisível por dois números coprimos m e n se, e somente se, ele é divisível pelo produto $m \cdot n$. Logo, a probabilidade de s números serem coprimos é:

$$\prod_{p \text{ primo}} \left(1 - \frac{1}{p^s}\right) = \left(\prod_{p \text{ primo}} \frac{1}{1 - p^{-s}}\right)^{-1} = \frac{1}{\zeta(s)}.$$

Como $\zeta(2) = \pi^2/6$, encontramos o mesmo resultado. □

Para esta demonstração utilizamos um resultado que é provado num capítulo vindouro, a saber, a Proposição 6.1.

4 Alguns teoremas sobre a distribuição de números primos

Se $x > 0$, $\pi(x)$ denota a quantidade de números primos menores ou iguais a x. Claramente $\pi(x) \to \infty$ quando $x \to \infty$. Gauss e Legendre conjecturaram que

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

Isto foi provado em 1896 por Hadamard e de la Vallée Poussin usando técnicas de análise complexa e é conhecido como o teorema dos números primos. Vamos mostrar que o teorema dos números primos pode ser expresso de várias formas equivalentes.

4.1 FUNÇÕES DE CHEBYSHEV $\psi(x)$ E $\theta(x)$

Definição 4.1. Para $x > 0$ definimos a função ψ de Chebyshev pela fórmula

$$\psi(x) = \sum_{n\leq x} \Lambda(n).$$

Como $\Lambda(n) = 0$ quando n não é uma potência de primo, escrevemos como segue:

$$\psi(x) = \sum_{n\leq x} \Lambda(n) = \sum_{\substack{m=1 \\ p^m\leq x}}^{\infty} \sum_{p} \Lambda(p^m) = \sum_{m=1}^{\infty} \sum_{p\leq x^{1/m}} \log p.$$

A soma em m é uma soma finita. De fato, a soma em p é vazia se $x^{1/m} < 2$, isto é, se $(1/m)\log x < \log 2$, ou se

$$m > \frac{\log x}{\log 2} = \log_2 x$$

Dessa forma temos

$$\psi(x) = \sum_{m\leq log_2 x} \sum_{p\leq x^{1/m}} \log p.$$

Podemos escrever isto de uma forma diferente utilizando outra função de Chebyshev.

Definição 4.2. Se $x > 0$ definimos a função θ de Chebyshev pela equação

$$\theta(x) = \sum_{p\leq x} \log p$$

onde p percorre todos os primos $\leq x$. Daí, a última fórmula para $\psi(x)$ pode ser escrita como:

$$\psi(x) = \sum_{m\leq \log_2 x} \theta(x^{1/m}). \tag{4.1}$$

Teorema 4.1. Para $x > 0$ temos

$$0 \leq \frac{\psi(x)}{x} - \frac{\theta(x)}{x} \leq \frac{(\log x)^2}{2\sqrt{x}\log 2}.$$

Observação. Essa desigualdade implica

$$\lim_{x\to\infty}\left(\frac{\psi(x)}{x}-\frac{\theta(x)}{x}\right)=0.$$

Em outras palavras, se um dos $\psi(x)/x$ ou θ/x tende a um limite, o outro também, e os limites são iguais.

Demonstração. De (4.1) temos

$$0\leq\psi(x)-\theta(x)=\sum_{2\leq m\leq\log_2 x}\theta(x^{1/m}).$$

Mas, da definição de $\theta(x)$ temos a desigualdade trivial

$$\theta(x)\leq\sum_{p\leq x}\log x\leq x\log x$$

daí

$$\begin{aligned}0\leq\psi(x)-\theta(x)\leq&\sum_{2\leq m\leq\log_2} x^{1/m}\log(x^{1/m})\leq(\log_2 x)\sqrt{x}\log\sqrt{x}\\=&\frac{\log x}{\log 2}\cdot\frac{\sqrt{x}}{2}\log x=\frac{\sqrt{x}(\log x)^2}{2\log 2}.\end{aligned}$$

Divindo por x encontramos o teorema. □

4.2 RELAÇÕES ENTRE $\theta(x)$ E $\pi(x)$

Teorema 4.2 (Identidade de Abel)**.** Para qualquer função aritmética $a(n)$ seja

$$A(x)=\sum_{n\leq x}a(n),$$

onde $A(x)=0$ se $x<1$. Assuma que $f\in C^1$ no intervalo $[y,x]$, onde $0<y<x$. Então temos

$$\sum_{y<n\leq x}a(n)f(n)=A(x)f(x)-A(y)f(y)-\int_y^x A(t)f'(t)dt \tag{4.2}$$

Como $A(t)=0$ se $t<1$, quando $y<1$ a equação (4.2) toma a forma

$$\sum_{n\leq x}a(n)f(n)=A(x)f(x)-\int_1^x A(t)f'(t)dt. \tag{4.3}$$

Demonstração. Seja $k = \lfloor x \rfloor$ e $m = \lfloor y \rfloor$, então $A(x) = A(k)$ e $A(y) = A(m)$. Daí

$$\begin{aligned}
\sum_{y<n\leq x} a(n)f(n) &= \sum_{n=m+1}^{k} a(n)f(n) = \sum_{n=m+1}^{k} \{A(n) - A(n-1)\}f(n) \\
&= \sum_{n=m+1}^{k} A(n)f(n) - \sum_{n=m}^{k-1} A(n)f(n+1) \\
&= \sum_{n=m+1}^{k-1} A(n)\{f(n) - f(n+1)\} + A(k)f(k) - A(m)f(m+1) \\
&= -\sum_{n=m+1}^{k-1} A(n) \int_{n}^{n+1} f'(t)dt + A(k)f(k) - A(m)f(m+1) \\
&= -\sum_{n=m+1}^{k-1} \int_{n}^{n+1} A(t)f'(t)dt + A(k)f(k) - A(m)f(m+1) \\
&= -\int_{m+1}^{k} A(t)f'(t)dt + A(x)f(x) - \int_{k}^{x} A(t)f'(t)dt \\
&\quad - A(y)f(y) - \int_{y}^{m+1} A(t)f'(t)dt \\
&= A(x)f(x) - A(y)f(y) - \int_{y}^{x} A(t)f'(t)dt. \quad \square
\end{aligned}$$

Observação. Podemos provar a fórmula da soma de Euler utilizando a identidade de Abel. Se $a(n) = 1$ para todo $n \geq 1$ achamos $A(x) = \lfloor x \rfloor$ e (4.2) implica

$$\sum_{y<n\leq x} f(n) = f(x)\lfloor x \rfloor - f(y)\lfloor y \rfloor - \int_{y}^{x} \lfloor t \rfloor f'(t)dt.$$

Combinando isto com integração por partes temos

$$\int_{y}^{x} tf'(t)dt = xf(x) - yf(y) - \int_{y}^{x} f(t)dt$$

E obtemos a Fórmula da Soma de Euler.

Teorema 4.3. Para $x \geq 2$ temos

$$\theta(x) = \pi(x)\log x - \int_{x}^{2} \frac{\pi(t)}{t}dt \tag{4.4}$$

e

$$\pi(x) = \frac{\theta(x)}{\log x} + \int_{2}^{x} \frac{\theta(t)}{t\log^2 t}dt. \tag{4.5}$$

Demonstração. Seja $a(n)$ a função característica dos primos, isto é,

$$a(n) = \begin{cases} 1 & \text{se } n \text{ é primo} \\ 0 & \text{caso contrário} \end{cases}$$

Assim temos

$$\pi(x) = \sum_{p \le x} 1 = \sum_{1 < n \le x} a(n) \qquad \text{e} \qquad \theta(x) = \sum_{p \le x} \log p = \sum_{1 < n \le x} a(n) \log n.$$

Tomando $f(x) = \log x$ em (4.2) com $y = 1$ obtemos

$$\theta(x) = \sum_{1 < n \le x} a(n) \log n = \pi(x) \log x - \pi(1) \log 1 - \int_1^x \frac{\pi(t)}{t} dt,$$

o que prova (4.4) desde que $\pi(t) = 0$ para $t < 2$. Em seguida, seja $b(n) = a(n) \log n$ e escreva

$$\pi(x) = \sum_{3/2 < n \le x} b(n) \frac{1}{\log n}, \qquad \theta(x) = \sum_{n \le x} b(n).$$

Tomando $f(x) = 1/\log x$ em (4.2) com $y = 3/2$ obtemos

$$\pi(x) = \frac{\theta(x)}{\log x} - \frac{\theta(3/2)}{\log 3/2} + \int_{3/2}^x \frac{\theta(t)}{t \log^2 t} dt,$$

o que prova (4.5) pois $\theta(t) = 0$ se $t < 2$. □

4.3 ALGUMAS FORMAS EQUIVALENTES DO TEOREMA DOS NÚMEROS PRIMOS

Teorema 4.4. As seguintes relações são equivalentes:

$$\lim_{x \to \infty} \frac{\pi(x) \log x}{x} = 1. \tag{4.6}$$

$$\lim_{x \to \infty} \frac{\theta(x)}{x} = 1. \tag{4.7}$$

$$\lim_{x \to \infty} \frac{\psi(x)}{x} = 1. \tag{4.8}$$

Demonstração. De (4.4) e (4.5) obtemos, respectivamente,

$$\frac{\theta(x)}{x} = \frac{\pi(x) \log x}{x} - \frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt$$

e

$$\frac{\pi(x) \log x}{x} = \frac{\theta(x)}{x} + \frac{\log x}{x} \int_2^x \frac{\theta(t) dt}{t \log^2 t}.$$

Para mostrar que (4.6) implica (4.7) só precisamos mostrar que (4.6) implica:

$$\lim_{x \to \infty} \frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt = 0.$$

Mas, repare que (4.6) implica $\dfrac{\pi(t)}{t} = O\left(\dfrac{1}{\log t}\right)$ para $t \ge 2$ então

$$\frac{1}{x} \int_2^x \frac{\pi(t)}{t} dt = O\left(\frac{1}{x} \int_2^x \frac{dt}{\log t}\right).$$

Daí

$$\int_2^x \frac{dt}{\log t} = \int_2^{\sqrt{x}} \frac{dt}{\log t} + \int_{\sqrt{x}}^x \frac{dt}{\log t} \leq \frac{\sqrt{x}}{\log 2} + \frac{x - \sqrt{x}}{\log \sqrt{x}}$$

então

$$\frac{1}{x} \int_2^{\sqrt{x}} \frac{dt}{\log t} \to 0 \quad \text{quando } x \to \infty.$$

Isso mostra que (4.6) implica (4.7).

Para mostrar que (4.7) implica (4.6) só precisamos mostrar que (4.7) implica

$$\lim_{x \to \infty} \frac{\log x}{x} \int_2^x \frac{\theta(t)dt}{t \log^2 t} = 0.$$

Mas (4.7) implica $\theta(t) = O(t)$ então

$$\frac{\log x}{x} \int_2^x \frac{\theta(t)dt}{t \log^2 t} = O\left(\frac{\log x}{x} \int_2^x \frac{dt}{\log^2 t} \right).$$

Agora

$$\int_2^x \frac{dt}{\log^2 t} = \int_2^{\sqrt{x}} \frac{dt}{\log^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\log^2 t} \leq \frac{\sqrt{x}}{\log^2 2} + \frac{x - \sqrt{x}}{\log^2 \sqrt{x}}$$

por isso

$$\frac{\log x}{x} \int_2^x \frac{dt}{\log^2 t} \to 0 \quad \text{quando } x \to \infty.$$

Isso prova que (4.7) implica (4.6), então (4.6) e (4.7) são equivalentes. Já sabemos pelo Teorema (4.1) que (4.7) e (4.8) são equivalentes. □

5 Grupos abelianos finitos e seus caracteres

5.1 ALGUMAS DEFINIÇÕES

Definição 5.1. Um grupo G é um conjunto não vazio munido de uma operação $\cdot$ que satisfaz as seguintes propriedades:

a) Fechamento. Se $a, b \in G$ então $a \cdot b \in G$.

b) Associatividade. Para todo $a, b, c \in G$, temos $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

c) Identidade. Existe um único elemento $e \in G$ tal que $a \cdot e = e \cdot a$ para todo $a \in G$.

d) Inverso. Para todo $a \in G$, existe um único elemento $b \in G$ tal que $a \cdot b = b \cdot a = e$. Denotamos esse b por a^{-1} e o chamamos de inverso de a.

Definição 5.2. Um **grupo abeliano** é um grupo cuja operação é comutativa, isto é $ab = ba$ para todos $a, b \in G$.

Definição 5.3. Um **grupo é finito** se G é um conjunto finito. O número de elementos de G será denotado por $|G|$ e chamado de **ordem** de G.

Exemplo 5.1. Um exemplo clássico de conjunto finito é o conjunto das permutações num conjunto de n símbolos, comumente chamado de grupo simétrico S_n. Os elementos são considerados como funções injetivas e a operação usada é a composição. Este é um grupo de ordem $n!$.

Definição 5.4. Um **subgrupo** é um subconjunto G' de G que também é um grupo.

Exemplo 5.2. $(\mathbb{Z}+, 0)$ é um subgrupo de $(\mathbb{Q}, +, 0)$.

5.2 PROPRIEDADES ELEMENTARES

Os teoremas desta seção, relacionados a propriedades de grupos, serão enunciados sem demonstração. O leitor interessado pode consultar o livro (JACOBSON, 2012)

Teorema 5.1. Se os elementos $a, b, c \in G$ satisfazem

$$ac = bc \qquad \text{ou} \qquad ca = cb,$$

então $a = b$.

Teorema 5.2. Em qualquer grupo G temos

a) $e^{-1} = e$

b) Para todo $a \in G$, $(a^{-1})^{-1} = a$.

c) Para todo $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

d) Para todo $a, b \in G$, a equação $ax = b$ tem a solução única $x = a^{-1}b$; a equação $ya = b$ tem a solução única $y = ba^{-1}$.

Definição 5.5. Se $a \in G$, definimos a^n para qualquer inteiro n pelas seguintes relações:

$$a^0 = e, \qquad a^n = aa^{n-1}, \qquad a^{-n} = (a^{-1})^n \qquad \text{para } n > 0$$

Teorema 5.3. Se $a \in G$, quaisquer potências de a comutam, e para todos inteiros m, n temos

$$a^m a^n = a^{m+n} = a^n a^m \qquad \text{e} \qquad (a^m)^n = a^{mn} = (a^n)^m$$

Além disso, se a e b comutam temos

$$a^n b^n = (ab)^n.$$

Teorema 5.4. Se G' é um subconjunto de G, então G' é um subgrupo se, e somente se, satisfaz as propriedades $a)$ e $d)$:

a) Fechamento. Se $a, b \in G$ então $a \cdot b \in G$.

d) Inverso. Para todo $a \in G$, existe um único elemento $b \in G$ tal que $a \cdot b = b \cdot a = e$. Denotamos esse b por a^{-1} e o chamamos de inverso de a.

5.3 CONSTRUÇÃO DE SUBGRUPOS

Um subgrupo de um dado grupo G pode sempre ser construído escolhendo qualquer elemento $a \in G$ e formando o conjunto de todas as suas potências $a^n, n = 0, \pm 1, \pm 2, \ldots$ Este conjunto claramente satisfaz os postulados (a) e (d), então é um subgrupo de G. Ele é chamado o subgrupo cíclico gerado por a e é denotado por $\langle a \rangle$.
Note que pelo Teorema 5.3, $\langle a \rangle$ é abeliano, mesmo que G não seja.
Se $a^n = e$ par algum $n \in \mathbb{N}$, pelo princípio da boa ordenação, existe um elemento mínimo k com essa propriedade e o subgrupo $\langle a \rangle$ será um grupo finito de ordem k.

$$\langle a \rangle = \{a, a^2, \ldots, a^k = e\}$$

O inteiro k é chamado **ordem do elemento** a.

Teorema 5.5. Se G é finito e $a \in G$, então existe um inteiro positivo $n \leq |G|$ tal que $a^n = e$, i.e., a ordem de qualquer elemento não é maior que a ordem do grupo.

Demonstração. Suponha $|G| = g$, então pelo menos dois dos seguintes elementos devem ser iguais:

$$e, a, a^2, \ldots, a^g$$

suponha $a^r = a^s$, onde $0 \leq s < r \leq g$. Daí temos

$$e = a^r (a^s)^{-1} = a^{r-s}.$$

Então o teorema é válido para $n = r - s$. □

Observação. Se G' é um subgrupo de um grupo finito G, então para qualquer elemento a em G existe um inteiro n tal que $a^n \in G'$. Se a já estiver em G', simplesmente tomamos $n = 1$. Se $a \notin G'$ podemos tomar n como sendo a ordem de a, pois $a^n = e \in G'$. No entanto, pode haver uma potência positiva menor que a que se encontra em G'. Pelo princípio da boa ordenação existe um menor inteiro positivo n tal que $a^n \in G'$. Chamamos esse inteiro de **indicador de** a **em** G'.

Teorema 5.6. Seja G' um subgrupo de um grupo abeliano finito G, onde $G' \neq G$. Escolha um elemento a em G, $a \notin G'$, e seja h o indicador de a em G'. Então o conjunto de produtos

$$G'' = \{xa^k : x \in G' \text{ e } k = 0, 1, 2, \ldots, h-1\}$$

é um subgrupo de G que contém G'. Além disso

$$|G''| = h|G'|.$$

Demonstração. Para verificar que G'' é subgrupo apenas precisamos testar se a operação é fechada e existência de inverso. Deixamos isso a cargo do leitor.
Em seguida, determinamos a ordem de G''. Seja $m = |G'|$. Quando x percorre o elementos de G' e k percorre os h inteiros $0, 1, 2, \ldots, h-1$ obtemos mh produtos xa^k. Se mostrarmos que todos são distintos, então G'' tem ordem mh. Considere dois desses produtos, digamos xa^k e ya^j e suponha que

$$xa^k = ya^j \quad \text{com } 0 \leq j \leq k < h.$$

Então $a^{k-j} = x^{-1}y$ e $0 \leq k - j < h$. Como $x^{-1}y \in G'$ devemos ter a^{k-j} em G' e isso só é possível se $k = j$ e, portanto, $x = y$. Isso completa a prova. □

5.4 CARACTERES DE GRUPOS ABELIANOS FINITOS

Definição 5.6. Seja G um grupo qualquer. Uma função complexa f definida em G tomando valores em $\mathbb{C}$ é chamada um **caractere** de G se f possui a propriedade multiplicativa

$$f(ab) = f(a)f(b)$$

Para todo $a, b \in G$.

Teorema 5.7. Se f é um caractere de um grupo finito G com identidade e, então $f(e) = 1$ e cada valor da função $f(a)$ é uma raiz da unidade. De fato, se $a^n = e$ então $f(a)^n = 1$.

Demonstração. Escolha $c \in G$ tal que $f(c) \neq 0$. Como $ce = c$ temos

$$f(ce) = f(c)f(e) = f(c)$$

então $f(e) = 1$. Em seguida, se $a^n = e$, $f(a)^n = f(a^n) = f(e) = 1$. □

Definição 5.7. Todo grupo G tem pelo menos um caractere, a saber, o caractere que é identicamente igual a 1 para todo elemento de G. Este é chamado o **caractere principal**.

Teorema 5.8. Um grupo abeliano finito G de ordem n tem exatamente n caracteres distintos.

Demonstração. No Teorema 5.6 aprendemos como construir, a partir de um dado subgrupo $G' \neq G$, um novo subgrupo G'' contendo G' e pelo menos mais um elemento a que não pertence a G'. Usaremos o símbolo $\langle G'; a\rangle$ para denotar o subgrupo G'' construído naquele teorema. Assim

$$\langle G'; a\rangle = \{xa^k : x \in G' \text{ e } 0 \leq k < h\}$$

onde h é o indicador de a em G'.
Agora aplicamos esta construção repetidamente, começando com o subgrupo $\{e\}$ que denotamos por G_1. Se $G_1 \neq G$ seja a_1 um elemento de G diferente de e e defina $G_2 = \langle G_1; a_1\rangle$. Se $G_2 \neq G$ Seja a_2 um elemento de G que não pertence a G_2 e defina $G_3 = \langle G_2; a_2\rangle$. Continue o processo para obter um conjunto de elementos finitos $a_1, a_2, \ldots, a_t$, e um conjunto correspondente de subgrupos $G_1, G_2, \ldots, G_{t+1}$ tal que

$$G_{r+1} = \langle G_r; a_r\rangle$$

com

$$G_1 \subset G_2 \subset \cdots \subset G_{t+1} = G$$

Este processo deve terminar em algum momento, pois G é um grupo finito e cada subgrupo posterior tem mais elementos que o seu predecessor. Agora, vamos provar o teorema por indução.

É claro que G_1 tem apenas um caractere, a saber, a função $f(n) = 1$ para todo n. Suponha que G_r tem ordem m e que há exatamente m caracteres distintos para G_r. Considere $G_{r+1} = \langle G_r; a_r\rangle$ e seja h o indicador de a_r em G_r. Vamos mostrar que há exatamente h maneiras diferentes de estender cada caractere de G_r para obter um caractere de G_{r+1} e que cada caracter de G_{r+1} é uma extensão de algum caractere de G_r. Isto provará que G_{r+1} tem exatamente mh caracteres, e como mh é a ordem de G_{r+1}, o teorema estará provado por indução. Um elemento qualquer de G_{r+1} tem a forma

$$xa_r^k, \quad \text{onde } x \in G_r \text{ e } 0 \leq k < h$$

Suponha que é possível estender um caractere de G_r para G_{r+1}. Chame esta extensão de $\tilde{f}$ e vamos analisar o que se sabe sobre $\tilde{f}(xa_r^k)$. Pela propriedade multiplicativa temos

$$\tilde{f}(xa_r^k) = \tilde{f}(x)\tilde{f}(a_r)^k.$$

como $x \in G_r$, $\tilde{f}(x) = f(x)$, entao a equação acima implica

$$\tilde{f}(xa_r^k) = f(x)\tilde{f}(a_r^k)$$

Precisamos, então, definir quais são os possíveis valores de $\tilde{f}(a_r^k)$. Suponha $c = a_r^h$. Como $c \in G_r$, $f(c) = \tilde{f}(c)$. Como $\tilde{f}$ é multiplicativa, $\tilde{f}(c) = \tilde{f}(a_r)^h$. Consequentemente

$$\tilde{f}(a_r) = \sqrt[h]{f(c)}$$

Daí, $\tilde{f}(a_r)$ é uma das raízes h-ésimas da unidade de $f(c)$. Portanto existem no máximo h opções para $\tilde{f}(a_r)$.

Com essas observações podemos definir $\tilde{f}$. Se f é um caractere de G_r, escolhemos uma das h-ésimas raizes da unidade de $f(c)$, onde $c = a_r^h$ e definimos $\tilde{f}(a_r)$ como sendo esta raiz. Daí, definimos $\tilde{f}$ no restante de G_{r+1} pela equação

$$\tilde{f}(xa_r^k) = f(x)\tilde{f}(a_r)^k \tag{5.1}$$

As h escolhas para $\tilde{f}(a_r)$ são todas diferentes, então isso nos dá h formas diferentes de definir $\tilde{f}(xa_r^k)$. Agora verificamos se a função $\tilde{f}$ como foi definida tem a propriedade multiplicativa. De (5.1) achamos

$$\begin{aligned}\tilde{f}(xa_r^k ya_r^j) =& \tilde{f}(xy \cdot a_r^{k+j}) = f(xy)\tilde{f}(a_r)^{k+j} \\ =& f(x)f(y)\tilde{f}(a_r)^k\tilde{f}(a_r)^j \\ =& \tilde{f}(xa_r^k)\tilde{f}(ya_r^j).\end{aligned}$$

Então $\tilde{f}$ é um caractere de G_{r+1}. Não podemos ter duas extensões $\tilde{f}$ e $\tilde{g}$ iguais em G_{r+1} porque as funções f e g das quais elas são estendidas também seriam iguais em G_r. Portanto, cada um dos m caracteres de G_r pode ser estendido de h formas diferentes para produzir um caractere de G_{r+1}. Além disso, se β é um caractere qualquer de G_{r+1}, a sua retrição a G_r também é um caractere em G_r, então o processo de extensão produz todos os caracteres de G_{r+1}. Isto completa a prova. □

5.5 O GRUPO DE CARACTERES

Definição 5.8. Nesta seção G é um grupo abeliano de ordem n. O caractere principal é denotado por $f_1 \equiv 1$. Os outros caracteres, denotados por $f_2, \ldots, f_n$, são chamados caracteres não-principais. Eles têm a propriedade de que $f(a) \neq 1$ para algum $a \in G$.

Teorema 5.9. Se a multiplicação de caracteres é definida pela relação

$$(f_i f_j)(a) = f_i(a)f_j(a)$$

para cada a em G, então o conjunto de caracteres de G forma um grupo abeliano de ordem n. Denotamos este grupo por G. O elemento identidade de G é o caractere principal f_1. O inverso de f_i é $1/f_i$.

Demonstração. Basta verificar os postulados de grupo.

Observação. Para cada caractere f temos $|f(a)| = 1$. Daí o recíproco $1/f(a)$ é igual ao conjugado complexo $\overline{f(a)}$. Assim, a função $\bar{f}$ definida por $\bar{f}(a) = \overline{f(a)}$ também é um caractere de G. Além disso, temos

$$\bar{f}(a) = \frac{1}{f(a)} = f(a^{-1})$$

para todo $a \in G$.

5.6 RELAÇÃO DE ORTOGONALIDADE PARA CARACTERES

Observação. Denotamos por $A = [a_{ij}]_{i,j=1}^{n} = A(G)$ a matriz cujos elementos a_{ij} na linha i e coluna j são

$$a_{ij} = f_i(a_j)$$

Vamos provar que a matriz A tem uma inversa e então usar este fato para deduzir as chamadas relações de ortogonalidade para caracteres. Nós primeiro determinaremos a soma das entradas em cada linha de A.

Teorema 5.10. A soma das entradas na i-ésima linha de A é dada por

$$\sum_{r=1}^{n} f_i(a_r) = \begin{cases} n & \text{se } f_i \text{ é o caractere principal } (i = 1), \\ 0 & \text{caso contrário.} \end{cases}$$

Demonstração. Vamos denotar por S a soma em questão. Se $f_i = f_1$ cada termo da soma é 1 e $S = n$. Se $f_i \neq f_1$ existe um elemento b em G para o qual $f_i(b) \neq 1$. Quando a_r percorre os elementos de G o mesmo acontece com o produto ba_r. Daí

$$S = \sum_{r=1}^{n} f_i(ba_r) = f_i(b) \sum_{r=1}^{n} f_i(a_r) = f_i(b)S.$$

Portanto $S(1 - f_i(b)) = 0$. Como $f_i(b) \neq 1$ segue que $S = 0$. □

Teorema 5.11. Seja A^* o conjugado transposto da matriz A. Temos

$$AA^* = nI,$$

onde I é a matriz identidade $n \times n$. Portanto $n^{-1}A^*$ é o inverso de A.

Demonstração. Seja $B = AA^*$. A entrada b_{ij} é dada por

$$b_{ij} = \sum_{r=1}^{n} f_i(a_r)\bar{f}_j(a_r) = \sum_{r=1}^{n} (f_i\bar{f}_j)(a_r) = \sum_{r=1}^{n} f_k(a_r),$$

onde $f_k = f_i\bar{f}_j = f_i/f_j$. Observe que $f_i/f_j = f_1$ se, e somente se, $i = j$. Daí, pelo Teorema 5.10 temos

$$b_{ij} = \begin{cases} n & \text{se } i = j, \\ 0 & \text{se } i \neq j \end{cases}$$

Em outras palavras, $B = nI$. □

Agora vamos usar o fato que uma matriz comuta com seu inverso para demonstrar relação de ortonogonalidade para caracteres.

Teorema 5.12. Relação de ortogonalidade para caracteres.

$$\sum_{r=1}^{n} \bar{f}_r(a_i) f_r(a_j) = \begin{cases} n & \text{se } a_i = a_j, \\ 0 & \text{se } a_i \neq a_j \end{cases} \tag{5.2}$$

Demonstração. A relação $AA^* = nI$ implica $A^*A = nI$. Mas o elemento na i-ésima linha e j-ésima coluna de A^*A é a soma à esquerda de (5.2). Isto completa a prova. □

Observação. Como $\bar{f}_r(a_i) = f_r(a_i)^{-1} = f_r(a_i^{-1})$, o termo geral da soma em (5.2) é igual a $f_r(a_i^{-1})f_r(a_j) = f_r(a_i^{-1}a_j)$. Portanto a relação de ortogonalidade pode ser expressa como segue:

$$\sum_{r=1}^{n} f_r(a_i^{-1}a_j) = \begin{cases} n & \text{se } a_i = a_j, \\ 0 & \text{se } a_i \neq a_j. \end{cases}$$

Quando a_i é a identidade obtemos:

Corolário 5.1. A soma das entradas na j-ésima coluna de A é dada por

$$\sum_{r=1}^{n} f_r(a_j) = \begin{cases} n & \text{se } a_j = e, \\ 0 & \text{caso contrário.} \end{cases} \tag{5.3}$$

5.7 CARACTERES DE DIRICHLET

Nas seções anteriores tratamos de caracteres de um grupo G abeliano finito arbitrário. Agora denotaremos G como o grupo de classes reduzidas de resíduos módulo um inteiro positivo fixo k. Primeiro provamos que essas classes de resíduos formam um grupo se a multiplicação é definida adequadamente.

Definição 5.9. Um sistema reduzido de resíduos módulo k é um conjunto de $\varphi(k)$ inteiros $\{a_1, \ldots, a_{\varphi(k)}\}$ incongruentes módulo k, e cada um relativamente primo a k. Para cada inteiro a a classe residual correspondente $\hat{a}$ é o conjunto de todos os inteiros congruentes a $a \bmod k$:

$$\hat{a} = \{x : x \equiv a \pmod{k}\}$$

a multiplicação de classes residuais é definida como

$$\hat{a} \cdot \hat{b} = \widehat{ab} \tag{5.4}$$

Ou seja, o produto de duas classes de resíduos $\hat{a}$ e $\hat{b}$ é a classe de resíduos do produto ab.

Teorema 5.13. Com a multiplicação definida por (5.4), o conjunto de classes reduzidas de resíduos módulo k é um grupo abeliano finito de ordem $\varphi(k)$. A identidade é a classe de resíduos $\hat{1}$. O inverso de $\hat{a}$ é a classe de resíduos $\hat{b}$ onde $ab \equiv 1 \pmod{k}$.

Demonstração. A propriedade de fechamento é automaticamente satisfeita devido à forma como a multiplicação de classes de resíduos foi definida. A classe $\hat{1}$ é claramente o elemento de identidade. Se $(a, k) = 1$ existe um único b tal que $ab \equiv 1 \pmod{k}$. Portanto, o inverso de $\hat{a}$ é $\hat{b}$. Finalmente, fica claro que o grupo é abeliano e que sua ordem é $\varphi(k)$, onde usamos propriedades de congruência à vontade. □

Definição 5.10. Seja G o grupo de classes reduzidas de resíduos módulo k. Correspondendo a cada caractere f de G definimos uma função aritmética $\chi = \chi_f$ como segue:

$$\chi(n) = f(\hat{n}) \quad \text{se } (n,k) = 1,$$
$$\chi(n) = 0 \qquad \text{se } (n,k) > 1.$$

A função χ é chamada de **caractere de Dirichlet** módulo k. O caractere principal é o que tem as propriedades

$$\chi_1(n) = \begin{cases} 1 & \text{se } (n,k) = 1, \\ 0 & \text{se } (n,k) > 1, \end{cases}$$

Teorema 5.14. Existem $\varphi(k)$ caracteres de Dirichlet distintos módulo k, cada um deles completamente multiplicativo e periódico com período k. Ou seja, nós temos

$$\chi(mn) = \chi(m)\chi(n) \quad \text{para todo } m, n \tag{5.5}$$

e

$$\chi(n+k) = \chi(n) \quad \text{para todo } n.$$

Reciprocamente, se χ é completamente multiplicativa e periódica com período k, e se $\chi(n) = 0$ quando $(n,k) > 1$, então χ é um dos caracteres de Dirichlet mod k.

Demonstração. Existem $\varphi(k)$ caracteres f para o grupo G de classes reduzidas de resíduos módulo k, e consequentemente $\varphi(k)$ caracteres χ_f módulo k. A propriedade multiplicativa (5.5) de χ_f vem de f quando m e n são relativamente primos a k. Se m ou n não é relativamente primo a k, então mn também não é, portanto, ambos os membros de (5.5) são zero.
A propriedade de periodicidade decorre do fato de que $\chi_f(n) = f(\hat{n})$ e que $a \equiv b \pmod{k}$ implica $(a,k) = (b,k)$. Para provar a recíproca notamos que a função f definida no grupo G pela equação

$$f(\hat{n}) = \chi(n) \qquad (n,k) = 1$$

é um caractere de G, então χ é um caractere de Dirichlet mod k. □

Exemplo 5.3. Quando $k = 1$ ou $k = 2$ então $\varphi(k) = 1$ e o único caractere de Dirichlet é o caractere principal χ_1. Para $k \geq 3$, existem ao menos dois caracteres de Dirichlet, pois $\varphi(k) \geq 2$. As seguintes tabelas mostram os caracteres de Dirichlet para $k = 3, 4$ e 5.

n	1	2	3
$\chi_1(n)$	1	1	0
$\chi_2(n)$	1	−1	0

$k = 3, \varphi(k) = 2$

n	1	2	3	4
$\chi_1(n)$	1	0	1	0
$\chi_2(n)$	1	0	−1	0

$k = 4, \varphi(k) = 2$

n	1	2	3	4	5
$\chi_1(n)$	1	1	1	1	0
$\chi_2(n)$	1	−1	−1	1	0
$\chi_3(n)$	1	i	$-i$	−1	0
$\chi_4(n)$	1	$-i$	i	−1	0

$k = 5, \varphi(k) = 4$

Figura 3 – Tabelas de caracteres para $k = 3, 4$ e 5 - Fonte: (APOSTOL, 1976)

Para preenchê-las usamos o fato que $\chi(n)^{\varphi(k)} = 1$ sempre que $(n, k) = 1$, então $\chi(n)$ é uma $\varphi(k)$-ésima raiz da unidade. Também notamos que se χ é um caractere mod k, $\overline{\chi}$ também é. Com isto preenchemos a tabela para $k = 3$ e $k = 4$.

Quando $k = 5$, $\varphi(5) = 4$, então os possiveis valores para $\chi(n)$ são ± 1 e $\pm i$ quando $(n, 5) = 1$. Também, $\chi(2)\chi(3) = \chi(6) = \chi(1) = 1$ então $\chi(2)$ e $\chi(3)$ são inversos. Como $\chi(4) = \chi(2)^2$, conseguimos preencher a tabela para $k = 5$.

Para checar se a tabela está correta, podemos usar o Teorema 5.10 e o Corolário 5.1 que nos dizem que a soma das linhas e colunas é sempre igual a 0, exceto a primeira linha e primeira coluna.

Teorema 5.15. Sejam $\chi_1, \ldots, \chi_{\varphi(k)}$ os $\varphi(k)$ caracteres de Dirichlet módulo k. Sejam m e n dois inteiros, com $(n, k) = 1$. Então temos

$$\sum_{r=1}^{\varphi(k)} \chi_r(m)\overline{\chi}_r(n) = \begin{cases} \varphi(k) & \text{se } m \equiv n \pmod{k}, \\ 0 & \text{se } m \not\equiv n \pmod{k}. \end{cases}$$

Demonstração. Se $(m, k) = 1$ tome $a_i = \hat{n}$ e $a_j = \hat{m}$ no Teorema 5.12 e observe que $\hat{m} = \hat{n}$ se, e somente se, $m \equiv n$ (mod k). Se $(m, k) > 1$ cada termo na soma desaparece e $m \not\equiv n \pmod{k}$. □

6 Teorema de Dirichlet para primos em progressões aritméticas

Teorema 6.1 (Teorema de Dirichlet para Primos em Progressões Aritméticas)**.** Se $\mathrm{mdc}(a, m) = 1$, existem infinitos primos na progressão aritmética

$$\{a + nm \mid n \geq 1\} = \{a + m, a + 2m, a + 3m, \dots\}.$$

Neste capítulo iremos apresentar ideias da prova do teorema acima. Para isso precisamos de alguns resultados.

6.1 PRODUTO DE EULER

Teorema 6.2 (Produto de Euler)**.** Seja $f : \mathbb{N} \to \mathbb{C}$ uma função aritmética completamente multiplicativa tal que $\sum_{n=1}^{\infty} f(n)$ converge absolutamente, então

$$\sum_{n=1}^{\infty} f(n) = \prod_{\text{p primo}} \frac{1}{1 - f(p)}.$$

Demonstração. Seja p um número primo. Note que

$$\sum_{k=0}^{\infty} |f(p^k)| \leq \sum_{n \in \mathbb{N}} |f(n)| < +\infty.$$

Logo, para cada p primo, $\sum_{k=0}^{\infty} f(p^k)$ converge absolutamente. Como f é completamente multiplicativa, devemos ter $|f(p)| < 1$, pois se fosse maior ou igual a 1, divergiria por comparação com a série $\sum 1 = +\infty$. Assim,

$$\frac{1}{1 - f(p)} = \sum_{k=0}^{\infty} f(p)^k = \sum_{k=0}^{\infty} f(p^k).$$

Pela convergência absoluta e pelo Teorema Fundamental da Aritmética,

$$\prod_{p \text{ primo}} \frac{1}{1 - f(p)} = \prod_{p \text{ primo}} \left(\sum_{k=0}^{\infty} f(p^k) \right) = \sum_{n=1}^{\infty} f(n).$$

Proposição 6.1. Lembre que a **Função Zeta de Riemann** é uma função de variável complexa definida como

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \dots.$$

Vamos assumir que ela é absolutamente convergente para $\mathrm{Re}(s) > 1$. Pelo teorema anterior, temos

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ primo}} \left(1 - \frac{1}{p^s} \right)^{-1}.$$

Proposição 6.2. $\zeta(s) = \dfrac{1}{s-1} + O(1)$, para $s > 1$, $s \in \mathbb{R}$

Demonstração. Seja $f(x) = \frac{1}{x^s}$, f é decrescente para $s > 1$ e $x > 0$. Seja $s > 1$ e $n \leq x \leq n+1$. Assim, $f(n+1) \leq f(x) \leq f(n)$. Logo,

$$\begin{aligned}
\frac{1}{(n+1)^s} \leq \frac{1}{x^s} \leq \frac{1}{n^s} \Rightarrow \int_n^{n+1} \frac{1}{(n+1)^s} dx \leq \int_n^{n+1} \frac{1}{x^s} \leq \int_n^{n+1} \frac{1}{n^s} dx \\
\Rightarrow \frac{1}{(n+1)^s}(n+1-n) \leq \int_n^{n+1} \frac{1}{x^s} dx \leq \frac{1}{n^s}(n+1-n) \\
\Rightarrow \sum_{n=1}^{\infty} \frac{1}{(n+1)^s} \leq \sum_{n=1}^{\infty} \int_n^{n+1} \frac{1}{x^s} dx \leq \sum_{n=1}^{\infty} \frac{1}{n^s} \\
\Rightarrow \zeta(s) - 1 \leq \int_1^{\infty} \frac{1}{x^s} dx \leq \zeta(s)
\end{aligned}$$

Observe que $\int_1^{\infty} \frac{1}{x^s} dx = \lim_{a\to\infty} \int_1^a \frac{1}{x^s} dx = \lim_{a\to\infty} \frac{x^{-s+1}}{-s+1}\Big|_1^a = \lim_{a\to\infty} \frac{\cancelto{0}{a^{-s+1}}}{-s+1} - \frac{1}{1-s} = \frac{1}{s-1}$, $s > 1$. Com isso temos $\zeta(s) - 1 \leq \frac{1}{s-1} \leq \zeta(s)$ o que implica $\zeta(s) = \frac{1}{s-1} + O(1)$, $s > 1$. □

Proposição 6.3. $\sum_{n\geq 2} \frac{\Lambda(n) n^{-s}}{\log n} = \log \zeta(s)$, $s \geq 1$.

Demonstração.

$$\begin{aligned}
\sum_{n\geq 2} \frac{\Lambda(n) n^{-s}}{\log n} &= \sum_p \sum_{k\geq 1} \frac{\Lambda(p^k) p^{-ks}}{\log p^k} \\
&= \sum_p \sum_{k\geq 1} \frac{(\log p) p^{-ks}}{k(\log p)} \\
&= \sum_p \left(\sum_{k\geq 1} \frac{(p^{-s})^k}{k} \right) \\
&= \sum_p \log((1-p^{-s})^{-1}) \\
&= \log \left(\prod_p (1-p^{-s})^{-1} \right) = \log \zeta(s).
\end{aligned}$$

Onde usamos que $\log(1-z)^{-1} = \sum_{k=1}^{\infty} \frac{z^k}{k}$, $|z| < 1$. □

Lema 6.1. Se $0 < x \leq 1/2$ então $-\log(1-x) < x + x^2$

Demonstração. Defina $f[0,1) \to \mathbb{R}$ como $f(x) = x + x^2 + \log(1-x)$, observe que $f(0) = 0$, $f'(x) = 1 + 2x - \frac{1}{1-x}$ e $f'(x) > 0$ em $(0, 1/2)$. Logo, f é crescente em $(0, 1/2)$ e daí $f(x) > 0$ em $(0, 1/2)$, o que implica que $x + x^2 > -\log(1-x)$.

Teorema 6.3. $\sum_{p \text{ primo}} \frac{1}{p} = +\infty$.

Demonstração. Vamos provar que esta série diverge comparando com a função ζ. Pela Proposição 6.2,

$$\begin{aligned}\zeta(s) =& \frac{1}{s-1} + O(1) = \frac{1 + (s-1)O(1)}{s-1} \\ =& \frac{1 + O(s-1)}{s-1} = \frac{O(1)}{s-1} \text{ (quando } s \to 1^+).\end{aligned}$$

Daí,

$$\log \zeta(s) = \log\left(\frac{O(1)}{s-1}\right) = \log\left(\frac{1}{s-1}\right) + \log(O(1))$$

Pela Proposição 6.3,

$$\log \zeta(s) = \sum_p \sum_{k\geq 1} \frac{p^{-ks}}{k} = \sum_p p^{-s} + \sum_p \sum_{k\geq 2} \frac{p^{-ks}}{k}.$$

Assim,

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + O(1).$$

Com isso conseguimos uma cota inferior, agora vamos trabalhar para encontrar uma cota superior. Pelo lema acima, temos que

$$\begin{aligned}\log \zeta(s) &= -\sum_{p \text{ primo}} \log\left(1 - \frac{1}{p^s}\right) \\ &< \sum_{p \text{ primo}} \frac{1}{p^s} + \sum_{p \text{ primo}} \frac{1}{p^{2s}} \\ &< \sum_{p \text{ primo}} \frac{1}{p^s} + \sum_{n=1}^{\infty} \frac{1}{n^{2s}} \\ &< \sum_{p \text{ primo}} \frac{1}{p^s} + \sum_{n=1}^{\infty} \frac{1}{n^2} = \sum_{p \text{ primo}} \frac{1}{p^s} + \frac{\pi^2}{6}\end{aligned}$$

Onde usamos o fato de que $\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$. Lembre que já usamos isto no início do Capítulo 3.6. Assim provamos que

$$\sum_{p \text{ primo}} \frac{1}{p^s} < \log \zeta(s) < \sum_{p \text{ primo}} \frac{1}{p^s} + \frac{\pi^2}{6} \tag{6.1}$$

Tomando $s \to 1^+$, observe que $\zeta(s)$ se aproxima da série harmônica, ou seja, diverge. Por conseguinte, $\lim_{s\to 1^+} \log \zeta(s)$ também diverge. Dessa forma, usando as desigualdades (6.1) acima, temos

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

pelo critério de comparação.

□

Com isso grosseiramente podemos dizer que os números primos são mais densos nos naturais do que os quadrados perfeitos, no sentido de que a série dos recíprocos dos quadrados perfeitos convergem ($\zeta(2) = \sum 1/n^2 = \pi^2/6$) enquanto a série dos recíprocos dos primos diverge.

6.2 L-SÉRIES DE DIRICHLET

Denotamos as L-séries de Dirichlet por

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}, s > 1$$

Como os caracteres de Dirichlet são completamente multiplicativos, suas somas também têm uma representação em produto de Euler 6.2.

$$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_{p \text{ primo}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \tag{6.2}$$

Observe que utilizando χ como o caractere principal ($f(n) = 1 \; \forall \; n$) teríamos a função ζ, logo isto é uma generalização da função zeta de Riemann.

As próximas proposições são necessárias para a prova do Teorema de Dirichlet.

Proposição 6.4. $\lim_{x \to 1^+} L(s,\chi_1) = +\infty$

Demonstração. Por (6.2) temos

$$L(s,\chi_1) = \sum_{n=1}^{\infty} \frac{\chi_1(n)}{n^s} = \prod_{p} \left(1 - \frac{\chi_1(p)}{p^s}\right)^{-1}$$

lembre que $\chi_1(p) = 0$ se mdc$(p,m) > 1$ e $\chi_1(p) = 1$ se mdc$(p,m) = 1$. Logo, o fator do produto é igual a 1 se, e somente se, $p|m$, pois teríamos $(1 - \chi_1(p)/p^s)^{-1} = (1 - 0/p^s)^{-1} = 1$. Assim, temos

$$L(s,\chi_1) = \prod_{\substack{p \text{ primo} \\ p \nmid m}} \left(1 - \frac{1}{p^s}\right)^{-1}$$

Note que todos fatores são maiores que 1 e $\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$, donde segue que $L(s,\chi_1) < \zeta(s)$ por uma quantidade pequena, pois a quantidade de primos p que dividem m é finita, logo eles não contribuem significativamente para a divergência.

Dessa forma, como $\lim_{s \to 1^+} \zeta(s) = +\infty$, segue que $\lim_{s \to 1^+} L(s,\chi_1) = +\infty$. □

Lema 6.2. Se $A_n = \sum_{k=1}^{n} a_k$ é limitada, i.e., $|A_n| \leq c$, para todo $n \in \mathbb{N}$, então a série $\sum_{n=1}^{\infty} |a_n| n^s$ converge para $s > 0$.

Demonstração. Fixe $\delta > 0$. Dado $\varepsilon > 0$, existe $n \in \mathbb{N}$ tal que $\frac{1}{n^\delta} < \frac{\varepsilon}{4c}$ para todo $n \geq n_0$. Assim, para $s > \delta$, temos

$$\frac{1}{n^s} \leq \frac{1}{n^\delta} < \frac{\varepsilon}{4c}, \; \forall \; n \geq n_0.$$

Dados $M > N \geq n_0$, temos:

$$\sum_{k=N}^{M} \frac{a_k}{k^s} = \sum_{k=N}^{M} \frac{A_k - A_{k-1}}{k^s} = \sum_{k=N}^{M} \frac{A_k}{k^s} - \sum_{k=N}^{M} \frac{A_{k-1}}{k^s} =$$
$$= \sum_{k=N}^{M} \frac{A_k}{k^s} - \sum_{k=N-1}^{M-1} \frac{A_k}{(k+1)^s} =$$
$$= \frac{A_M}{M^s} + \sum_{k=N}^{M-1} \left(\frac{A_k}{k^s} - \frac{A_k}{(k+1)^s} \right) - \frac{A_{N-1}}{N^s}.$$

Assim,

$$\left| \sum_{K=N}^{M} \frac{a_k}{k^s} \right| \leq \left| \frac{A_M}{M^s} \right| + \sum_{K=N}^{M-1} \left| \frac{A_k}{k^s} - \frac{A_k}{(k+1)^s} \right| + \left| \frac{A_{N+1}}{N^s} \right|$$
$$\leq \frac{c}{M^s} + \sum_{K=N}^{M-1} |A_k| \left| \frac{1}{k^s} - \frac{1}{(k+1)^s} \right| + \frac{c}{N^s}$$
$$\leq \frac{c}{M^s} + \frac{c}{N^s} - \frac{c}{M^s} + \frac{c}{N^s}$$
$$= \frac{2c}{N^s} < 2c \cdot \frac{\varepsilon}{4c} = \frac{\varepsilon}{2} < \varepsilon.$$

Portanto, dado $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que, se $M > N \geq n_0$ então

$$|x_M - x_N| < \varepsilon,$$

com $x_n = \sum_{k=1}^{n} \frac{a_k}{k^s}$. Logo, pelo teste de Cauchy, segue o resultado. □

Proposição 6.5. Se $\chi \neq \chi_1 \Rightarrow L(s, \chi)$ é contínua para $s > 0$.

Demonstração. Dado $\chi \neq \chi_1$ e $n \in \mathbb{N}$, podemos dividir N por q, de modo que $N = qm + r$, com $m, r \in \mathbb{Z}$ e $0 \leq r \leq q$. Assim,

$$\left| \sum_{n=1}^{N} \chi(n) \right| = \left| \sum_{n=1}^{r} \chi(n) \right| \leq \sum_{n=1}^{r} |\chi(n)| \leq \sum_{n=1}^{q-1} |\chi(n)| = \varphi(q), \text{ que não depende de } N.$$

E o resultado segue pelo lema acima. □

Apenas enunciaremos a próxima proposição, pois seria necessário apresentar muitas outras definições e proposições para demonstrar, mas é interessante falar que a ideia de Dirichlet foi provar para caracteres complexos e reais separadamente. Para caracteres complexos é possível provar por contradição, e para caracteres reais podemos usar somatório ao longo de hipérboles. O leitor interessado pode procurar uma prova detalhada em (LI, 2012).

Proposição 6.6. Se $\chi \neq \chi_1 \Rightarrow L(1, \chi) \neq 0$.

6.3 PROVA DO TEOREMA

Teorema 6.4 (Teorema de Dirichlet para primos em progressões aritméticas)**.** Se a e q são inteiros positivos relativamente primos, então existe uma infinidade de primos da forma $a + qk$, com $k \in \mathbb{Z}$.

Demonstração. Seja $n \in \mathbb{Z}$, denotaremos $C_n = \{n + qm \mid m \geq 0\}$. Basta mostrar que existem infinitos primos em C_a. Sejam $\chi_1, \chi_2, \ldots, \chi_{\varphi(q)}$ caracteres em I_q, onde I_q é o conjunto dos caráteres mod q. Dado $i \in \{1, \ldots, \varphi(q)\}$, temos

$$\log L(s, \chi_i) = \sum_p \frac{\chi_i(p)}{p^s} + O(1) \tag{6.3}$$

onde "p" no somatório indica todo p primo. Observe que

$$\sum_p \frac{\chi_i(p)}{p^s} = \sum_{n=1}^{\infty} \sum_{p \in C_n} \frac{\chi_i(p)}{p^s} = \sum_{n=1}^{\infty} \left(\chi_i(n) \sum_{p \in C_n} \frac{1}{p^s} \right).$$

Agora, denote $\sum_{p \in C_n} \dfrac{1}{p^s} = f(s, n)$ para facilitar a notação. Assim,

$$\sum_p \frac{\chi_i(p)}{p^s} = \sum_{n \in \mathbb{N}} \chi_i(n) f(s, n)$$

Substituindo em (6.3),

$$\log L(s, \chi_i) = \sum_{n \in \mathbb{N}} \chi_i(n) f(s, n) + O(1)$$

Seja a^{-1} o inverso de $a \pmod q$. Vamos multiplicar ambos os lados da igualdade por $\chi_i(a^{-1})$ e somá-los:

$$\sum_{i=1}^{\phi(q)} \chi(a^{-1}) \log L(s, \chi_i) = \sum_{n \in \mathbb{N}} \sum_{i=1}^{\phi(q)} \chi_i(a^{-1} n) f(s, n) + O(1).$$

Sabemos que $\sum_{\chi \in I_q} \chi(t) = \phi(q)$ se $t = 1$ e 0 caso contrário, assim, temos

$$\chi_1(a^{-1}) \log L(s, \chi_1) + \sum_{\substack{\chi \in I_q \\ \chi \neq \chi_1}} \log L(s, \chi) = \phi(q) f(s, a) + O(1).$$

Agora, observe que $\lim_{s \to 1^+} L(s, \chi_1) = +\infty$ e $\sum_{\substack{\chi \in I_q \\ \chi \neq \chi_1}} \log L(s, \chi) < +\infty$, o que implica

$$\lim_{s \to 1^+} f(s, a) = +\infty$$

para a igualdade ser verdadeira. Ou seja, a série

$$\sum_{p \in C_a} \frac{1}{p} = f(1, a)$$

diverge, o que implica que há infinitos primos da forma $a + qm$. □

7 Funções Aritméticas Periódicas e Somas de Gauss

7.1 FUNÇÕES PERIÓDICAS MÓDULO k

Definição 7.1. Seja k um inteiro positivo. Uma função aritmética f é dita periódica com periodo k (ou periódica módulo k) quando

$$f(n+k) = f(n)$$

para todo inteiro n. O menor período de f é chamado **período fundamental**.

Exemplo 7.1. A função máximo divisor comum é periódica módulo k já que $(n+k, k) = (n, k)$.

Exemplo 7.2. A função $f(n) = e^{2\pi imn/k}$ também é periódica módulo k. O número $e^{2\pi im/k}$ é uma k-ésima raiz da unidade e $f(n)$ é a sua n-ésima potência. Qualquer combinação linear destas funções, digamos

$$\sum_m c(m)e^{2\pi imn/k}$$

também é periódica mod k para cada escolha de coeficientes $c(m) \in \mathbb{C}$.

Teorema 7.1. Para $k \geq 1$ fixo seja

$$g(n) = \sum_{m=0}^{k-1} e^{2\pi imn/k}.$$

Então

$$g(n) = \begin{cases} 0 & \text{se } k \nmid n, \\ k & \text{se } k|n. \end{cases}$$

Demonstração. Como $g(n)$ é soma dos termos em uma progressão geométrica

$$g(n) = \sum_{m=0}^{k-1} x_m,$$

onde $x = e^{2\pi in/k}$, temos

$$g(n) = \begin{cases} \dfrac{x^k - 1}{x - 1} & \text{if } x \neq 1, \\ k & \text{if } x = 1. \end{cases}$$

Mas $x^k = 1$, e $x = 1$ se e somente se $k|n$, então o teorema está provado. □

7.2 EXISTÊNCIA DE SÉRIE DE FOURIER FINITA PARA FUNÇÕES ARITMÉTICAS PERIÓDICAS

Usaremos o polinômio de Lagrange para mostrar que toda função aritmética periódica tem uma expansão de Fourier finita.

Teorema 7.2 (Teorema de interpolação de Lagrange)**.** Sejam $z_0, \ldots, z_{k-1}$ k números complexos distintos, e sejam $w_0, w_1, \ldots, w_{k-1}$ k números complexos distintos ou não. Existe um único polinômio $P(z)$ de grau $\leq k-1$ tal que

$$P(z_m) = w_m \text{ para } m = 0, 1, \ldots, k-1$$

Demonstração. Construímos o polinômio $P(z)$, chamado o polinômio interpolador de Lagrange como segue. Seja

$$A(z) = (z - z_0)(z - z_1) \cdots (z - z_{k-1})$$

e seja

$$A_m(z) = \frac{A(z)}{z - z_m}.$$

Então $A_m(z)$ é um polinômio de grau $k-1$ com as seguintes propriedades:

$$A_m(z_m) \neq 0, \qquad A_m(z_j) = 0 \text{ if } j \neq m$$

Daí $A_m(z)/A_m(z_m)$ é um polinômio de grau $k-1$ que se anula para cada z_j com $j \neq m$ e tem valor 1 em z_m. Portanto a combinação linear

$$P(z) = \sum_{m=0}^{k-1} w_m \frac{A_m(z)}{A_m(z_m)}$$

é um polinômio de grau $\leq k-1$ com $P(z_j) = w_j$ para cada j. Se existisse outro polinômio $Q(z)$ da mesma forma, a diferença $P(z) - Q(z)$ se anularia em k pontos distintos, daí $P(z) = Q(z)$ desde que ambos os polinômios têm grau $\leq k-1$.

Definimos os números $z_0, \ldots, z_{k-1}$ como as k-ésimas raízes da unidade e obtemos:

Teorema 7.3. Dados k números complexos $w_0, \ldots, w_{k-1}$, existem k números complexos únicos $a_0, a_1, \ldots, a_{k-1}$ tais que

$$w_m = \sum_{n=0}^{k-1} a_n e^{2\pi i m n/k} \tag{7.1}$$

para $m = 0, 1, \ldots, k-1$. Ademais, os coeficientes a_n são dados pela fórmula

$$a_n = \frac{1}{k} \sum_{m=0}^{k-1} w_m e^{-2\pi i m n/k} \text{ para } n = 0, 1, 2, \ldots, k-1. \tag{7.2}$$

Demonstração. Seja $z_m = e^{2\pi i m/k}$. Os números $z_0, z_1, \ldots, z_{k-1}$ são distintos, então existe um polinômio de Lagrange único

$$P(z) = \sum_{n=0}^{k-1} a_n z^n$$

tal que $P(z_m) = w_m$ para cada $m = 0, 1, 2, \ldots, k-1$. Isto mostra que existem a_n unicamente determinados satisfazendo (7.1). Para deduzir a fórmula (7.2) multiplicamos ambos os lados de

(7.1) por $e^{-2\pi imr/k}$, onde m e r são inteiros não negativos menores que k, e somamos em m para obter

$$\sum_{m=0}^{k-1} w_m e^{-2\pi imr/k} = \sum_{n=0}^{k-1} a_n \sum_{m=0}^{k-1} e^{2\pi i(n-r)m/k}.$$

Pelo Teorema 7.1, a soma em m é 0 a não ser que $k|(n-r)$. Mas $|n-r| \leq k-1$ então $k|(n-r)$ se, e somente se, $n = r$. Portanto o único termo não nulo na direita ocorre quando $n = r$ e achamos

$$\sum_{m=0}^{k-1} w_m e^{-2\pi imr/k} = ka_r.$$

Esta equação nos dá (7.2). □

Teorema 7.4. Seja f uma função aritmética periódica módulo k. Então existe uma função aritmética g únicamente determinada e periódica módulo k tal que

$$f(m) = \sum_{n=0}^{k-1} g(n) e^{2\pi imn/k}.$$

e g é dado pela fórmula

$$g(n) = \frac{1}{k} \sum_{m=0}^{k-1} f(m) e^{-2\pi imn/k}.$$

Demonstração. Seja $w_m = f(m)$ para $m = 0, 1, \ldots, k-1$ e aplique o Teorema 7.3 para determinar os números $a_0, a_1, \ldots, a_{k-1}$. Defina a função g pelas relações $g(m) = a_m$ para $m = 0, 1, 2, \ldots, k-1$ e amplie a definição de $g(m)$ para todos os inteiros m por periodicidade mod k. Daí f está relacionado com g pelas equações no teorema. □

Observação. Como f e g são periódicas, reescrevemos o Teorema 7.4 como segue:

$$f(m) = \sum_{n \bmod k} g(n) e^{2\pi imn/k} \tag{7.3}$$

e

$$g(n) = \frac{1}{k} \sum_{m \bmod k} f(m) e^{-2\pi imn/k.} \tag{7.4}$$

Em cada caso a soma pode ser estendida sobre qualquer sistema completo de resíduos módulo k. A soma em (7.3) é chamada **expansão finita de Fourier** de f e os números $g(n)$ são chamados **coeficientes de Fourier** de f.

7.3 SOMAS DE RAMANUJAN E GENERALIZAÇÕES

Teorema 7.5. Seja μ a função μ de Mobius. Então $\mu(n)$ é a soma das n-ésimas raizes primitivas da unidade.

Demonstração.

$$\sum_{\substack{k=1\\(k,n)=1}}^{n} e^{2\pi ik/n} = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) e^{2\pi ik/n}$$

onde usamos o Teorema 2.1. Lembre que a soma das n raízes da unidade é sempre igual a 0 e vamos rearranjar os somatórios

$$\sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) e^{2\pi ik/n} = \sum_{d|n} \mu(d) \sum_{j=1}^{n/d} e^{2\pi idj/n}$$

Repare que este último somatório é igual a 0 em toda parte, a não ser quando $d = n$. Assim provamos que

$$\sum_{\substack{k=1\\(k,n)=1}}^{n} e^{2\pi ik/n} = \mu(n).$$

Agora vamos generalizar este resultado.

Definição 7.2. Seja n um inteiro positivo fixo e considere a soma das n-ésimas potências das k-ésimas raizes da unidade primitivas. Esta soma é conhecida como **soma de Ramanujan** e é denotada por $c_k(n)$:

$$c_k(n) = \sum_{\substack{m \bmod k\\(k,m)=1}} e^{2\pi imn/k}$$

Provamos no teorema anterior que essa soma é igual a $\mu(k)$ quando $n = 1$.

$$\mu(k) = c_k(1).$$

Teorema 7.6. Seja $s_k(n) = \sum_{d|(n,k)} f(d)g(k/d)$. Então $s_k(n)$ tem a expansão em série de Fourier

$$s_k(n) = \sum_{m \bmod k} a_k(m) e^{2\pi imn/k} \tag{7.5}$$

onde

$$a_k(m) = \sum_{d|(m,k)} g(d) f(k/d) \frac{d}{k}. \tag{7.6}$$

Demonstração. Pelo Teorema 7.4 os coeficientes $a_k(m)$ são dados por

$$\begin{aligned} a_k(m) =& \frac{1}{k} \sum_{n \bmod k} s_k(n) e^{-2\pi inm/k} \\ =& \frac{1}{k} \sum_{n=1}^{k} \sum_{\substack{d|n\\d|k}} f(d)g(k/d) e^{-2\pi imn/k} \end{aligned}$$

Escrevemos $n = cd$, note que para cada d fixado, o índice c vai de 1 até k/d e obtemos

$$a_k(m) = \frac{1}{k} \sum_{d|k} f(d)g(k/d) \sum_{c=1}^{k/d} e^{-2\pi icdm/k}.$$

Substituímos d por k/d na soma à direita e obtemos

$$a_k(m) = \frac{1}{k}\sum_{d|k} f(k/d)g(d)\sum_{c=1}^{d} e^{-2\pi icm/d}.$$

Pelo Teorema 7.1, a soma em c é 0 a não ser que $d|m$, e nesse caso a soma vale d. Por isso

$$a_k(m) = \frac{1}{k}\sum_{\substack{d|k\\ d|m}} f(k/d)g(d)d$$

□

Teorema 7.7. Temos

$$c_k(n) = \sum_{d|(n,k)} d\mu(k/d).$$

Demonstração. Tomando $f(k) = k$ e $g(k) = \mu(k)$ no teorema anterior nos dá

$$\sum_{d|(n,k)} d\mu(k/d) = \sum_{m \bmod k} a_k(m)e^{2\pi imn/k}$$

onde

$$a_k(m) = \sum_{d|(m,k)} \mu(d) = \left\lfloor \frac{1}{(m,k)} \right\rfloor = \begin{cases} 1 & \text{se } (m,k) = 1, \\ 0 & \text{se } (m,k) > 1. \end{cases}$$

Portanto

$$\sum_{d|(n,k)} d\mu(k/d) = \sum_{\substack{m \bmod k\\ (m,k)=1}} e^{2\pi imn/k} = c_k(n).$$

□

7.4 PROPRIEDADES MULTIPLICATIVAS DE $s_k(n)$

Lema 7.1. (a, b) denota o $mdc(a, b)$. Temos que

$$(ah, bk) = (a, b)(h, k)\left(\frac{a}{(a, b)}, \frac{k}{(h, k)}\right)\left(\frac{b}{(a, b)}, \frac{h}{(h, k)}\right).$$

Em particular isso mostra que $(ah, bk) = (a, k)(b, h)$ sempre que $(a, b) = (h, k) = 1$.

Demonstração. Vamos utilizar livremente que $(n, m) = g \iff (n/g, m/g) = 1$. Seja $a_1 = a/(a, b), b_1 = b/(a, b), h_1 = h/(h, k), k_1 = k/(h, k)$. Temos

$$\begin{aligned} &(ah, bk) = (a, b)(h, k)\left(\frac{a}{(a, b)}, \frac{k}{(h, k)}\right)\left(\frac{b}{(a, b)}, \frac{h}{(h, k)}\right) \\ \iff &(a_1h_1, b_1k_1) = (a_1, k_1)(b_1, h_1) \\ \iff &\left(\frac{a_1}{(a_1, k_1)}\frac{h_1}{(b_1, h_1)}, \frac{b_1}{(b_1, h_1)}\frac{k_1}{(a_1, k_1)}\right) = 1. \end{aligned}$$

Agora defina $\alpha = (a_1, k_1), \gamma = \frac{h_1}{(b_1,h_1)}, \beta = \frac{b_1}{(b_1,h_1)}, \delta = \frac{k_1}{(a_1,k_1)}$. Temos que $(\alpha, \delta) = 1$ e $(\gamma, \beta) = 1$. Além disso, note que

$$\alpha = \frac{a}{d_1(a,b)} \quad \text{and} \quad \beta = \frac{b}{d_2(a,b)}$$

para algum d_1 e algum d_2, então segue que $(\alpha, \beta) = 1$ e analogamente $(\gamma, \delta) = 1$. Isso significa que $\alpha\gamma$ e $\beta\delta$ não podem compartilhar divisores positivos além de 1, isto é $(\alpha\gamma, \beta\delta) = 1$. □

Teorema 7.8. Seja

$$s_k(n) = \sum_{d|(n,k)} f(d)g(k/d)$$

onde f e g são multiplicativas. Então temos

$$s_{mk}(ab) = s_m(a)s_k(b) \quad \text{sempre que } (a,k) = (b,m) = 1. \tag{7.7}$$

Em particular, temos

$$s_m(ab) = s_m(a) \quad \text{se } (b,m) = 1, \tag{7.8}$$

e

$$s_{mk}(a) = s_m(a)g(k) \quad \text{se } (a,k) = 1. \tag{7.9}$$

Demonstração. Pelo lema anterior, as relações $(a,k) = (b,m) = 1$ implicam

$$(ab, km) = (a,m)(k,b)$$

com (a,m) e (b,k) coprimos. Portanto

$$s_{mk}(ab) = \sum_{d|(mk,ab)} f(d)g(mk/d) = \sum_{d|(a,m)(b,k)} f(d)g(mk/d).$$

Escrevendo $d = d_1d_2$ na última soma nos dá

$$\begin{aligned} s_{mk}(ab) &= \sum_{d_1|(a,m)} \sum_{d_2|(b,k)} f(d_1d_2)g\left(\frac{mk}{d_1d_2}\right) \\ &= \sum_{d_1|(a,m)} f(d_1)g(m/d_1) \sum_{d_2|(b,k)} f(d_2)g(k/d_2) = s_m(a)s_k(b). \end{aligned}$$

Isso prova (7.7). Tomando $k = 1$ em (7.7) nos dá

$$s_m(ab) = s_m(a)s_1(b) = s_m(a)$$

desde que $s_1(b) = f(1)g(1) = 1$. Assim provamos (7.8). Tomando $b = 1$ em (7.7):

$$s_{mk}(a) = s_m(a)s_k(1) = s_m(a)g(k)$$

desde que $s_k(1) = f(1)g(k) = g(k)$. Com isso provamos (7.9). □

7.5 SOMAS DE GAUSS ASSOCIADAS A CARACTERES DE DIRICHLET

Definição 7.3. Para qualquer caractere de Dirichlet $\chi \bmod k$ a soma

$$G(n,\chi) = \sum_{m=1}^{k} \chi(m) e^{2\pi i m n/k}$$

é chamada a **Soma de Gauss** associada a χ. Se χ é χ_1, o caractere principal mod k, temos $\chi_1(m) = 1$ se $(m,k) = 1$ e $\chi_1(m) = 0$ caso contrário. Neste caso a soma de Gauss se reduz à soma de Ramanujan:

$$G(n,\chi_1) = \sum_{\substack{m=1 \\ (m,k)=1}}^{k} e^{2\pi i m n/k} = c_k(n).$$

Assim, as somas de Gauss $G(n,\chi)$ podem ser consideradas como generalizações da soma de Ramanujan. Passamos agora a um estudo detalhado de suas propriedades.

Teorema 7.9. Se χ é qualquer caractere de Dirichlet mod k então

$$G(n,\chi) = \bar{\chi}(n) G(1,\chi) \quad \text{sempre que } (n,k) = 1.$$

Demonstração. Quando $(n,k) = 1$ os números nr percorrem um sistema completo de resíduos mod k com r. Além disso, $|\chi(n)|^2 = \chi(n)\bar{\chi}(n) = 1$ então

$$\chi(r) = \bar{\chi}(n)\chi(n)\chi(r) = \bar{\chi}(n)\chi(nr)$$

Portanto a soma definindo $G(n,\chi)$ pode ser escrita como segue:

$$\begin{aligned} G(n,\chi) &= \sum_{r \bmod k} \chi(r) e^{2\pi i n r/k} = \bar{\chi}(n) \sum_{r \bmod k} \chi(nr) e^{2\pi i n r/k} \\ &= \bar{\chi}(n) \sum_{m \bmod k} \chi(m) e^{2\pi i m/k} = \bar{\chi}(n) G(1,\chi). \end{aligned}$$

Isto prova o teorema. □

Definição 7.4. A soma de Gauss $G(n,\chi)$ é dita **separável** se

$$G(n,\chi) = \bar{\chi}(n) G(1,\chi) \tag{7.10}$$

O Teorema 7.9 nos disse que $G(n,\chi)$ é separável sempre que n é relativamente primo ao módulo k. Para o restante temos o seguinte teorema:

Teorema 7.10. Se χ é um caractere de Dirichlet mod k a soma de Gauss $G(n,\chi)$ é separável para todo n se, e somente se

$$G(n,\chi) = 0 \quad \text{sempre que } (n,k) > 1$$

Demonstração. A separabilidade é sempre válida se $(n,k) = 1$. Se $(n,k) > 1$ temos $\bar{\chi}(n) = 0$ então a equação (7.10) é válida se e somente se $G(n,\chi) = 0$. □

Teorema 7.11. Se $G(n,\chi)$ é separável para todo n então

$$|G(1,\chi)|^2 = k. \tag{7.11}$$

Demonstração.

$$\begin{aligned}|G(1,\chi)|^2 =& G(1,\chi)\overline{G(1,\chi)} = G(1,\chi)\sum_{m=1}^{k}\bar{\chi}(m)e^{-2\pi im/k}\\ =& \sum_{m=1}^{k} G(m,\chi)e^{-2\pi im/k} = \sum_{m=1}^{k}\sum_{r=1}^{k}\chi(r)e^{2\pi imr/k}e^{-2\pi im/k}\\ =& \sum_{r=1}^{k}\chi(r)\sum_{m=1}^{k}e^{2\pi im(r-1)/k} = k\chi(1) = k.\end{aligned}$$

Desde que a última soma sobre m é uma soma geométrica que se anula em todo ponto menos em $r = 1$.

7.6 CARACTERES DE DIRICHLET COM SOMAS DE GAUSS NÃO NULAS

Para cada caractere χ mod k vimos que $G(n,\chi)$ é separável se $(n,k) = 1$, e que a separabilidade de $G(n,\chi)$ é equivalente a $G(n,\chi)$ ser nula para $(n,k) > 1$. Agora descrevemos outras propriedades desses caracteres, tais que $G(n,\chi) = 0$ sempre que $(n,k) > 1$. Na verdade, é mais simples estudar o conjunto complementar. O próximo teorema dá uma condição necessária para que $G(n,\chi)$ seja diferente de zero para $(n,k) > 1$.

Teorema 7.12. Seja χ um caractere de Dirichlet mod k e assuma que $G(n,\chi) \neq 0$ para algum n satisfazendo $(n,k) > 1$. Então existe um divisor próprio d de k, de tal modo que

$$\chi(a) = 1 \quad \text{sempre que } (a,k) = 1 \text{ e } a \equiv 1 \pmod{d} \tag{7.12}$$

Demonstração. Para o n dado, seja $q = (n,k)$ e seja $d = k/q$. Então $d|k$ e, já que $q > 1$, temos $d < k$. Escolha qualquer a satisfazendo $(a,k) = 1$ e $a \equiv 1 \pmod{d}$. Vamos provar que $\chi(a) = 1$.

Como $(a,k) = 1$, na soma definindo $G(n,\chi)$ podemos substituir o índice m da soma por am e encontramos

$$\begin{aligned}G(n,\chi) =& \sum_{m \bmod k}\chi(m)e^{2\pi inm/k} = \sum_{m \bmod k}\chi(am)e^{2\pi inam/k}\\ =& \chi(a)\sum_{m \bmod k}\chi(m)e^{2\pi inam/k}.\end{aligned}$$

Como $a \equiv 1 \pmod{d}$ e $d = k/q$ podemos escrever $a = 1 + (bk/q)$ para algum inteiro b, e temos

$$\frac{anm}{k} = \frac{nm(\frac{kb}{q}+1)}{k} = \frac{nmkb}{kq} + \frac{nm}{k} = \frac{nmb}{q} + \frac{nm}{k}$$

Como $(n,k)=q$, $q|n$, então

$$\frac{nmb}{q}+\frac{nm}{k}\equiv\frac{nm}{k}\pmod 1$$

Daí $e^{2\pi inam/k}=e^{2\pi inm/k}$ e a soma para $G(n,\chi)$ torna-se

$$G(n,\chi)=\chi(a)\sum_{m \bmod k}\chi(m)e^{2\pi inm/k}=\chi(a)G(n,\chi).$$

Como $G(n,\chi)\neq 0$, isto implica $\chi(a)=1$, como afirmado. □

7.7 MÓDULO INDUZIDO E CARACTERES PRIMITIVOS

Definição 7.5. Seja χ um caractere de Dirichlet mod k e seja d qualquer divisor positivo de k. O número d é chamado de **módulo induzido** para χ se tivermos

$$\chi(a)=1 \quad \text{sempre que } (a,k)=1 \text{ e } a\equiv 1 \pmod d \tag{7.13}$$

Em outras palavras, d é um módulo induzido se o caractere χ mod k age como um caractere mod d nos representantes da classe de restos $\hat{1}$ mod d que são relativamente primos a k. Observe que o próprio k é sempre um módulo induzido para χ.

Teorema 7.13. Seja χ um caractere de Dirichlet mod k. Então 1 é um módulo induzido para χ se, e somente se, $\chi=\chi_1$.

Demonstração. Se $\chi=\chi_1$ então $\chi(a)=1$ para todo a relativamente primo a k. Mas como todo a satisfaz $a\equiv 1 \pmod 1$, o número 1 é um módulo induzido.
Por outro lado, se 1 é um módulo induzido, então $\chi(a)=1$ sempre que $(a,k)=1$, então $\chi=\chi_1$ já que χ se anula nos números não relativamente primos a k. □

Definição 7.6. Um caractere de Dirichlet χ mod k é dito **primitivo mod** k se não possui módulo induzido $d<k$. Em outras palavras, χ é primitivo mod k se, e somente se, para todo divisor d de k, $0<d<k$, existe um inteiro $a\equiv 1 \pmod d$, $(a,k)=1$, tal que $\chi(a)\neq 1$.
Se $k>1$ o caractere principal χ_1 não é primitivo, pois tem 1 como módulo induzido. A seguir mostramos que se o módulo é primo todo caractere não principal é primitivo.

Teorema 7.14. Todo caractere não-principal χ módulo um primo p é um caractere primitivo mod p.

Demonstração. Os únicos divisores de p são 1 e p, então estes são os únicos candidatos a módulos induzidos. Mas se $\chi\neq\chi_1$ o divisor 1 não é um módulo induzido, então χ não tem módulo induzido $<p$. Portanto, χ é primitivo.

Agora podemos reafirmar os resultados dos Teoremas 7.10 a 7.12 na terminologia de caracteres primitivos

Teorema 7.15. Seja χ um caractere de Dirichlet mod k primitivo. Então nós temos:

a) $G(n,\chi) = 0$ para todo n com $(n,k) > 1$.

b) $G(n,\chi)$ é separável para todo n.

c) $|G(1,\chi)|^2 = k$.

Demonstração. Se $G(n,\chi) \neq 0$ para algum n com $(n,k) > 1$ então o Teorema 7.12 mostra que χ tem um módulo induzido $d < k$, assim χ não pode ser primitivo. Isso prova (a). A parte (b) segue de (a) e do Teorema 7.10. Parte (c) segue da parte (b) e Teorema 7.11.

7.8 PROPRIEDADES DE MÓDULO INDUZIDO

Teorema 7.16. Seja χ um caractere de Dirichlet mod k e suponha $d|k$, $d > 0$. Então d é um módulo induzido para χ se, e somente se,

$$\chi(a) = \chi(b) \quad \text{sempre que } (a,k) = (b,k) = 1 \text{ e } a \equiv b \pmod{d}. \tag{7.14}$$

Demonstração. Se (7.14) é verdadeiro, d é um módulo induzido pois podemos escolher $b = 1$ e usar a equação (7.13). Agora provemos o contrário.

Escolha a e b tal que $(a,k) = (b,k) = 1$ e $a \equiv b \pmod{d}$. Vamos mostrar que $\chi(a) = \chi(b)$. Seja a' o inverso de $a \bmod k$, $aa' \equiv 1 \pmod{k}$. O inverso existe porque $(a,k) = 1$. Agora $aa' = 1 \pmod{d}$ desde $d|k$. Portanto, $\chi(aa') = 1$, pois d é um módulo induzido. Mas $aa' \equiv ba' \equiv 1 \pmod{d}$ porque $a \equiv b \pmod{d}$, portanto $\chi(aa') = \chi(ba')$, então

$$\chi(a)\chi(a') = \chi(b)\chi(a').$$

Mas $x(a') \neq 0$ já que $x(a)x(a') = 1$. Cancelando $\chi(a')$ encontramos $\chi(a) = \chi(b)$, e isso completa a prova.

A Equação (7.14) nos diz que χ é periódico módulo inteiros relativamente primos a k. Assim, χ age de forma parecida a um caractere módulo d. Para explorar mais essa relação vale a pena considerar alguns exemplos.

Exemplo 7.3. A seguinte tabela descreve um dos caracteres $\chi \pmod{9}$.

n	1	2	3	4	5	6	7	8	9
$\chi(n)$	1	-1	0	1	-1	0	1	-1	0

Note que esta tabela é periódica módulo 3, então 3 é um módulo induzido para χ· Na verdade, χ se comporta como o seguinte caractere ψ módulo 3:

n	1	2	3
$\psi(n)$	1	-1	0

Como $\chi(n) = \psi(n)$ para todo n, chamamos χ uma extensão de ψ. É claro que sempre que χ é uma extensão de um caractere ψ módulo d então d será um módulo induzido para χ.

Exemplo 7.4. Agora examinemos um dos caracteres χ módulo 6:

n	1	2	3	4	5	6
$\chi(n)$	1	0	0	0	-1	0

Neste caso, o número 3 é um módulo induzido porque $\chi(n) = 1$ para todo $n \equiv 1 \pmod 3$ com $(n, 6) = 1$. (Existe apenas um tal n, a saber, $n = 1$.)
No entanto, χ não é uma extensão de nenhum caractere ψ módulo 3, pois os únicos caracteres módulo 3 são o caractere principal ψ_1, dado pela tabela:

n	1	2	3
$\psi_1(n)$	1	1	0

e o caractere ψ mostrado no primeiro exemplo. Como $\chi(2) = 0$, não pode ser extensão de ψ nem ψ_1.

O seguinte lema será útil para provar o próximo Teorema.

Lema 7.2. Sejam n, a, d inteiros com $(a, d) = 1$. Seja $m = a + qd$ onde q é o produto (possívelmente vazio) de todos os primos que dividem n, mas não dividem a. Prove que

$$m \equiv a \pmod d \quad \text{e } (m, n) = 1$$

Demonstração. Como $m = a + qd$, por definição $m \equiv a \pmod d$. Suponha $p|n$ para algum primo p. Se $p|a$, por definição $p \nmid qd$ e por linearidade, $p \nmid m$. Se $p \nmid a$ então novamente pela definição $p|qd$ e por linearidade $p \nmid m$. O que nos dá $(m, n) = 1$. □

Teorema 7.17. Seja χ um caractere de Dirichlet mod k e suponha $d|k$, $d > 0$. Então as duas afirmações são equivalentes:

a) d é um módulo induzido para χ.

b) Existe um caractere ψ módulo d tal que

$$\chi(n) = \psi(n)\chi_1(n) \quad \text{para todo n,} \tag{7.15}$$

onde χ_1 é o caractere principal módulo k.

Demonstração. ($\Leftarrow$) Supondo b) verdadeiro, escolha n satisfazendo $(n, k) = 1$, $n \equiv 1 \pmod d$. Então $\chi_1(n) = \psi(n) = 1$ e dai $\chi(n) = 1$ e portando d é um módulo induzido para χ.
($\Rightarrow$) Suponha $(n, d) = 1$, pelo lema anterior, existe m com $m \equiv n \pmod d$ e $(m, k) = 1$. Defina

$$\psi(n) = \chi(m)$$

O número $\psi(n)$ está bem definido porque χ toma valores iguais em números que são congruentes módulo d e relativamente primos a k. Observe que, de fato, χ é um caractere mod d e temos que

se $(n,k)=1$ então $(n,d)=1$ e daí $\psi(n)=\chi(m)$ para algum $m \equiv n \pmod{d}$. Portanto, pelo teorema anterior,

$$\chi(n)=\chi(m)=\psi(n)=\psi(n)\chi_1(n)$$

desde que $\chi_1(n)=1$.

Se $(n,k)>1$, então $\chi(n)=\chi_1(n)=0$ e ambos os membros de (7.15) são 0. Assim, (7.15) vale para todo n. □

7.9 O CONDUTOR DE UM CARACTERE

Definição 7.7. Seja χ um caractere de Dirichlet mod k. O menor módulo induzido d de χ é chamado **o condutor de** χ.

Teorema 7.18. Todo caractere de Dirichlet χ mod k pode ser expresso como um produto

$$\chi(n)=\psi(n)\chi_1(n) \quad \text{para todo n,} \tag{7.16}$$

onde χ_1 é o caractere principal mod k e ψ é um caractere primitivo módulo o condutor de χ.

Demonstração. Seja d o condutor de χ. Do teorema anterior sabemos que χ pode ser expresso como um produto da forma (7.16), onde ψ é um caractere mod d. Agora vamos provar que ψ é primitivo mod d.

Assumimos que ψ não é primitivo mod d e chegamos a uma contradição. Se ψ não é primitivo mod d existe um divisor q de d, $q<d$, que é um módulo induzido para ψ. Vamos provar que este q, que divide k, é também um módulo induzido para χ, contrariando o fato de que d é o menor módulo induzido para χ.

Escolha $n \equiv 1 \pmod{q}$, $(n,k)=1$. Então

$$\chi(n)=\psi(n)\chi_1(n)=\psi(n)=1$$

porque q é um módulo induzido para ψ. Portanto, q também é um módulo induzido para χ e isso é uma contradição. □

7.10 CARACTERES PRIMITIVOS E SOMAS DE GAUSS SEPARÁVEIS

Para provar o teorema desta seção precisamos de um Lema, que enunciaremos sem prova.

Lema 7.3. Seja S um sistema reduzido de resíduos mod k, e seja $d>0$ um divisor de k. Então temos as seguintes decomposições de S:

a) S é a união de $\varphi(k)/\varphi(d)$ conjuntos disjuntos, cada um dos quais é um sistema reduzido de resíduos mod d.

b) S é a união de $\varphi(d)$ conjuntos disjuntos, cada um dos quais consiste em $\varphi(k)/\varphi(d)$ números congruentes entre si mod d.

Teorema 7.19. Seja χ um caractere mod k. Então χ é primitivo mod k se, e somente se, a soma de Gauss

$$G(n,\chi) = \sum_{m \bmod k} \chi(m) e^{2\pi i m n/k}$$

é separável para todo n.

Demonstração. Se χ é primitivo, então $G(n,\chi)$ é separável pelo Teorema 7.15. Agora provamos a recíproca.

Por causa dos Teorema 7.9 e Teorema 7.10 é suficiente provar que se χ não é primitivo mod k então para algum r satisfazendo $(r,k) > 1$ teríamos $G(r,\chi) \neq 0$. Suponha, então, que χ não é primitivo mod k. Isso implica $k > 1$. Então χ tem um condutor $d < k$. Seja $r = k/d$. Então $(r,k) > 1$ e provaremos que $G(r,\chi) \neq 0$ para este r. Pelo Teorema 7.18 existe um caractere primitivo $\psi \pmod d$ tal que $\chi(n) = \psi(n)\chi_1(n)$ para todo n. Dessa forma podemos escrever

$$\begin{aligned} G(r,\chi) &= \sum_{m \bmod k} \psi(m)\chi_1(m) e^{2\pi i r m/k} = \sum_{\substack{m \bmod k \\ (m,k)=1}} \psi(m) e^{2\pi i r m/k} \\ &= \sum_{\substack{m \bmod k \\ (m,k)=1}} \psi(m) e^{2\pi i m/d} = \frac{\varphi(k}{\varphi(d)} \sum_{\substack{m \bmod k \\ (m,k)=1}} \psi(m) e^{2\pi i m/d}, \end{aligned}$$

onde no último passo utilizamos o lema anterior. Portanto temos

$$G(r,\chi) = \frac{\varphi(k)}{\varphi(d)} G(1,\psi).$$

Mas $G(1,\psi)|^2 = d$ pelo Teorema 7.15 (ψ não é primitivo mod d), daí $G(r,\chi) \neq 0$. Isto finaliza a prova. □

7.11 A SÉRIE DE FOURIER FINITA DOS CARACTERES DE DIRICHLET

Como cada caractere de Dirichlet $\chi \pmod k$ é periódico mod k, ele tem uma expansão de Fourier

$$\chi(m) = \sum_{n=1}^{k} a_k(n) e^{2\pi i m n/k}, \tag{7.17}$$

e o Teorema 7.4 nos diz que os coeficientes são dados pela fórmula

$$a_k(n) = \frac{1}{k} \sum_{m=1}^{k} \chi(m) e^{-2\pi i m n/k}.$$

a soma à direita é uma soma de Gauss $G(-n,\chi)$ então temos

$$a_k(n) = \frac{1}{k} G(-n,\chi) \tag{7.18}$$

Quando χ é primitivo a expansão de Fourier de (7.17) pode ser expressa como segue:

Teorema 7.20. A expansão de Fourier finita de um caractere de Dirichlet $\chi \pmod k$ primitivo tem a forma

$$\chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{k} \bar{\chi}(n) e^{-2\pi imn/k} \tag{7.19}$$

onde

$$\tau_k(\chi) = \frac{G(1,\chi)}{\sqrt{k}} = \frac{1}{\sqrt{k}} \sum_{m=1}^{k} \chi(m) e^{2\pi im/k}. \tag{7.20}$$

E os números $\tau_k(\chi)$ têm valor absoluto 1.

Demonstração. Como χ é primitivo, $G(-n,\chi) = \bar{\chi}(n)G(1,\chi)$ e (7.18) implica $a_k(n) = \bar{\chi}(-n)G(1,\chi)/k$. Portanto (7.17) pode ser escrito como

$$\chi(m) = \frac{G(1,\chi)}{k} \sum_{n=1}^{k} \bar{\chi}(-n) e^{2\pi imn/k} = \frac{G(1,\chi)}{k} \sum_{n=1}^{k} \bar{\chi}(n) e^{-2\pi imn/k}$$

que é o mesmo que (7.19). Pelo Teorema 7.11, $\tau_k(\chi)$ tem valor absoluto 1. □

7.12 A DESIGUALDADE DE PÓLYA

Lema 7.4. $\sin t \geq 2t/\pi$ em $0 \leq t \leq \pi/2$.

Demonstração. $\sin x$ é côncava em $[0, \pi/2]$ e $g(t) = 2t/\pi$ é o segmento de reta que vai de $(0,0)$ a $(\pi/2, 1)$ □

Teorema 7.21 (A desigualdade de Pólya)**.** Se χ é um caractere mod k primitivo então para todo $x \geq 1$ temos

$$\left| \sum_{m \leq x} \chi(m) \right| < \sqrt{k} \log k. \tag{7.21}$$

Demonstração. Expressamos $\chi(m)$ pela sua expansão em série de Fourier finita, usando o Teorema anterior.

$$\chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{k} \bar{\chi}(n) e^{-2\pi imn/k}$$

e somamos para todo $m \leq x$ para obter

$$\sum_{m \leq x} \chi(m) = \frac{\tau_k(\chi)}{\sqrt{k}} \sum_{n=1}^{k-1} \bar{\chi}(n) \sum_{m \leq x} e^{-2\pi imn/k}$$

pois $\chi(k) = 0$. Tomando o módulo e multiplicando por $\sqrt{k}$ obtemos

$$\sqrt{k} \left| \sum_{m \leq x} \chi(m) \right| \leq \sum_{n=1}^{k-1} \left| \sum_{m \leq x} e^{-2\pi imn/k} \right| = \sum_{n=1}^{k-1} |f(n)| \tag{7.22}$$

onde $f(n) = \sum_{m \leq x} e^{-2\pi imn/k}$. observe que

$$f(k-n) = \sum_{m \leq x} e^{-2\pi im(k-n)/k} = \sum_{m \leq x} e^{2\pi imn/k} = \overline{f(n)}$$

então $|f(k-n)| = |f(n)|$. Daí (7.22) pode ser escrito como

$$\sqrt{k}\left|\sum_{m\leq x}\chi(m)\right| \leq 2\sum_{n<k/2}|f(n)| + \left|f\left(\frac{k}{2}\right)\right|, \tag{7.23}$$

onde o termo $|f(k/2)|$ só aparece se k é par. Note que $f(n)$ é uma soma geométrica da forma

$$f(n) = \sum_{m=1}^{r} y^m$$

onde $r = \lfloor x \rfloor$ e $y = e^{-2\pi i n/k}$. Aqui $y \neq 1$ uma vez que $1 \leq n \leq k-1$. Escrevendo $z = e^{-\pi i n/k}$, temos $y = z^2$ e $z^2 \neq 1$ pois $n \leq k/2$. Portanto

$$f(n) = y\frac{y^r - 1}{y-1} = z^2\frac{z^{2r}-1}{z^2-1} = \frac{\not{z}\cdot z\cdot z^r(z^r - z^{-r})}{\not{z}(z - z^{-1})} = z^{r+1}\frac{z^r - z^{-r}}{z - z^{-1}}$$

então

$$|f(n)| = \left|\frac{z^r - z^{-r}}{z - z^{-1}}\right| = \left|\frac{e^{-\pi i r n/k} - e^{\pi i r n/k}}{e^{-\pi i n/k} - e^{\pi i n/k}}\right| = \frac{\left|\sin\dfrac{\pi r n}{k}\right|}{\left|\sin\dfrac{\pi n}{k}\right|} \leq \frac{1}{\sin\dfrac{\pi n}{k}} \tag{7.24}$$

Agora usamos o Lema 7.4 com $t = \pi n/k$ para achar

$$|f(n)| \leq \frac{1}{\dfrac{2}{\pi}\dfrac{\pi n}{k}} = \frac{k}{2n}.$$

Se k é ímpar, (7.23) torna-se

$$\sqrt{k}\left|\sum_{m\leq x}\chi(m)\right| \leq k\sum_{n<k/2}\frac{1}{n} < k\log k.$$

Mas, se k é par, $|f(k/2)| \leq 1$ e (7.23) nos dá

$$\sqrt{k}\left|\sum_{m\leq x}\chi(m)\right| \leq k\left\{\sum_{n<k/2}\frac{1}{n} + \frac{1}{k}\right\} < k\log k,$$

E isto prova o teorema, basta dividir por $\sqrt{k}$ em ambos os lados da desigualdade. □

Parte II

Aplicações de Geometria Fractal e Sistemas Dinâmicos em Teoria dos Números

8 Motivações

(FALCONER, 2014) dá algumas explicações sobre o que é um fractal. Muitos fractais têm algum grau de autossemelhança - eles são feitos de partes que se assemelham ao todo de alguma forma.

Basicamente, uma dimensão fornece uma descrição de quanto espaço um conjunto preenche. É uma medida da proeminência das irregularidades de um conjunto quando visto em escalas muito pequenas. Uma dimensão contém muitas informações sobre as propriedades geométricas de um conjunto, como veremos. É possível definir a "dimensão" de um conjunto de muitas maneiras. É importante perceber que diferentes definições podem dar diferentes valores de dimensão para o mesmo conjunto e também podem ter propriedades muito diferentes. O uso inconsistente às vezes leva à confusão.

Em seu artigo original, (MANDELBROT; NESS, 1968) definiu um fractal como sendo um conjunto com dimensão de Hausdorff estritamente maior que sua dimensão topológica. Essa definição provou ser insatisfatória porque excluiu um número de conjuntos que deveriam ser considerados como fractais. Várias outras definições foram propostas, mas todas parecem ter a mesma desvantagem.

Parece melhor considerar um fractal como um conjunto que tem propriedades como as listados abaixo, em vez de procurar uma definição precisa que quase certamente excluirá alguns casos interessantes. Quando nos referimos a um conjunto F como um fractal, portanto, normalmente temos o seguinte em mente:

1. F tem uma estrutura fina, ou seja, detalhes em escalas arbitrariamente pequenas.
2. F é muito irregular para ser descrito na linguagem geométrica tradicional, tanto local quanto globalmente.
3. Frequentemente F tem alguma forma de autossimilaridade, talvez aproximada ou estatística.
4. Normalmente, a "dimensão fractal" de F (definida de alguma forma) é maior do que sua dimensão topológica.
5. Na maioria dos casos de interesse, F é definido de forma muito simples, talvez recursivamente.

Vamos ver alguns exemplos de fractais, e analisar algumas de suas propriedades.

Exemplo 8.1 (O conjunto de Cantor do terço médio)**.** Também chamado de Conjunto de Cantor ternário ou simplesmente Conjunto de Cantor, este é um dos fractais mais conhecidos.

É construído a partir de um intervalo unitário por uma sequência de operações de eliminação. Seja E_0 o intervalo $[0, 1]$. Seja E_1 o conjunto obtido excluindo o terço médio de E_0, de modo que E_1 consiste nos dois intervalos $\left[0, \frac{1}{3}\right]$ e $\left[\frac{2}{3}, 1\right]$. Excluir os terços médios desses

intervalos nos dá E_2; assim, E_2 compreende os quatro intervalos $\left[0, \frac{1}{9}\right]$, $[\frac{2}{9}, \frac{1}{3}]$, $[\frac{2}{3}, \frac{7}{9}]$ e $\left[\frac{8}{9}, 1\right]$. Continuamos desta forma, com E_k obtido por eliminar o terço médio de cada intervalo em E_{k-1}. Assim, E_k consiste em 2^k intervalos cada um com comprimento 3^{-k}. O conjunto de Cantor F consiste nos números que estão em E_k para todo k; matematicamente, F é a interseção $\bigcap_{k=0}^{\infty} E_k$.

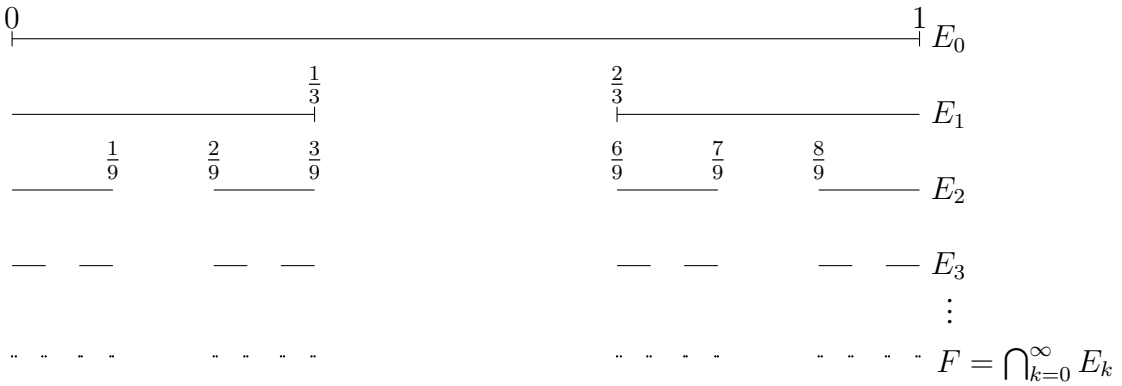


Figura 4 – O Conjunto de Cantor - Fonte: autoria própria

O conjunto de Cantor F pode ser pensado como o limite da sequência de conjuntos E_k quando k tende ao infinito. É obviamente impossível desenhar o próprio conjunto F, então representações de F normalmente são imagens de um dos E_k, que são uma boa aproximação de F quando k é razoavelmente grande.

Observe que se definirmos $f(x) = 3x \pmod 1 = 3x - \lfloor 3x \rfloor$ em $[0, 1]$, temos por indução que $f^n(x) = 3^n x \pmod 1$. Assim, o conjunto de Cantor é o maximal invariante de f restrita aos intervalos $[0, 1/3]$ e $[2/3, 1]$, isto é, $F = \bigcap_{n\geq 0} f^{-n}([0, 1/3] \cup [2/3, 1])$.

Pode parecer que removemos tantos pedaços do intervalo $[0, 1]$ que sobram poucos pontos, mas na verdade, F é um conjunto não enumerável. Para entender isso, perceba que se escrevermos os números em $[0, 1]$ na expansão em base 3, isto é, $a = a_1 3^{-1} + a_2 3^{-2} + a_3 3^{-3} + \cdots = (a_1 a_2 a_3 \ldots)_3$, em cada passo k da construção, estamos removendo os números em que $a_k = 1$. Ou seja, os números do Conjunto de Cantor são os números pertencentes a $[0, 1]$ cuja representação em base 3 não contém o dígito 1, com exceção dos números que são bordas dos intervalos fechados, como $1/3 = (0, 1)_2$ e $1/9 = (0, 01)_2$, mas se utilizarmos que $(0, 1)_2 = (0, 022222...)_2$ e $(0, 01)_2 = (0, 002222...)_2$, podemos nos livrar desse problema. Daí, como já sabemos que o conjunto das sequências infinitas de dois dígitos é não enumerável, segue que o conjunto de Cantor também é.

Vamos pontuar e provar algumas propriedades deste conjunto:

(i) F é autossimilar. É claro que a parte de F no intervalo $[0, \frac{1}{3}]$ e a parte de F em $[\frac{2}{3}, 1]$ são ambos geometricamente semelhantes a F em uma escala $\frac{1}{3}$. Novamente, as partes de F em cada um dos quatro intervalos de E_2 são semelhantes a F, mas a uma escala $\frac{1}{9}$ e assim por diante. O conjunto de Cantor contém cópias de si mesmo em muitas escalas diferentes

(ii) O conjunto F possui uma estrutura fina; isto é, contém detalhes arbitrariamente pequenos. Quanto mais ampliamos a imagem do conjunto de Cantor, mais lacunas aparecem.

(iii) Embora F tenha uma estrutura complexamente detalhada, a definição real de F é bem direta.

(iv) F é obtido por um procedimento recursivo. Nossa construção consistiu em remover repetidamente os terços médios dos intervalos. Etapas sucessivas fornecem aproximações cada vez mais boas E_k para o conjunto F.

(v) A geometria de F não é facilmente descrita em termos clássicos: não é o lugar geométrico dos pontos que satisfazem alguma condição geométrica simples, nem é o conjunto de soluções de alguma equação simples.

(vi) É estranho descrever a geometria local de F − perto de cada um de seus pontos há um grande número de outros pontos, separados por lacunas de comprimentos variados. De fato, todo ponto de F é um ponto de acumulação (Proposição 8.1).

(vii) Embora F seja, em alguns aspectos, um conjunto bastante grande, seu tamanho não é percebido por medidas usuais. Por várias definições razoáveis, F tem comprimento zero.

(viii) Se indicarmos com $I_1, I_2, \ldots, I_n, \ldots$ os intervalos abertos omitidos na construção, veremos que $A = \mathbb{R} \setminus \bigcup I_n$ é um conjunto fechado, logo $F = [0,1] \cap A$ é fechado e limitado, ou seja, é compacto.

(ix) F não contém intervalos. Observamos que depois da n-ésima etapa de sua construção restam apenas intervalos de comprimento $1/3^n$. Portanto, dado qualquer intervalo $J \subset [0,1]$ de comprimento $c > 0$, se tomarmos n tal que $1/3^n < c$, o intervalo J estará mutilado depois da n-ésima etapa da formação de F. Assim, F nào contém intervalos.

Proposição 8.1. Todo ponto do conjunto de Cantor F é ponto de acumulação.

Demonstração. Seja $c \in F$ extremidade de algum intervalo, digamos (c, b), omitido de $[0,1]$ para formar F. Quando (c, b) foi retirado, restou um certo intervalo $[a, c]$. Nas etapas seguintes da construção de F, restarão sempre terços finais de intervalo, do tipo $[a_n, c]$, com $a_n \in F$. O comprimento $c - a_n$ tende a zero, logo $a_n \to c$ e assim c não é ponto isolado de F. Suponha agora que $c \in F$ não é extremo de intervalo retirado de $[0,1]$ durante a construção de F. Vamos provar que c não é ponto isolado em F. Para todo $n \in \mathbb{N}$, c pertence ao interior de um intervalo $[x_n, y_n]$ que restou depois da n-ésima etapa da construção de F. Temos $x_n < c < y_n$ e $y_n - x_n = 1/3^n$. Logo $c = \lim x_n = \lim y_n$ é ponto de acumulação de F. □

Veja a Proposição 9.1 para outra propriedade interessante deste conjunto.

Exemplo 8.2 (Curva de von Koch)**.** Esta curva é construída da seguinte forma: Seja E_0 um segmento unitário, E_1 consiste de 4 segmentos, onde retiramos o terço médio de E_0 e o substituímos

pelos outros dois lados do triângulo equilátero cuja base seria o terço médio do segmento. E_2 é construído da mesma forma, aplicando em cada um dos quatro segmentos de E_1 e assim por diante.

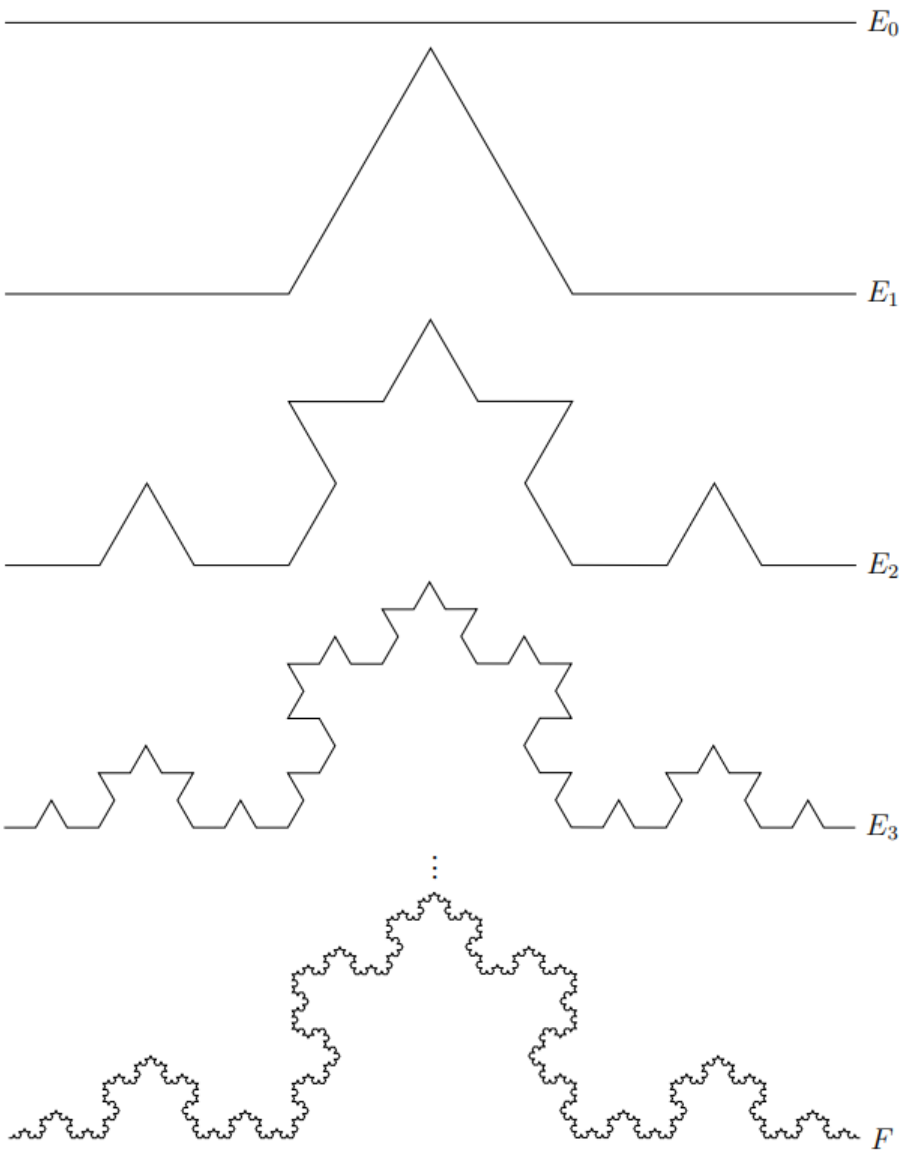


Figura 5 – Curva de von Koch - Fonte: autoria própria

A curva de von Koch tem várias características semelhantes às listadas para o conjunto de Cantor. É composto de quatro "quartos", cada um semelhante ao todo, mas dimensionado por um fator $\frac{1}{3}$. Tem uma estrutura fina, no entanto, esta estrutura complexa decorre de uma construção basicamente simples. Um cálculo simples mostra que E_k tem comprimento $\left(\frac{4}{3}\right)^k$; fazendo k tender ao infinito implica que F tem comprimento infinito. Por outro lado, F ocupa zero área no plano, portanto nem o comprimento nem a área fornecem uma descrição muito útil do tamanho de F.

Juntando três curvas de von Koch conseguimos formar uma curva floco de neve:

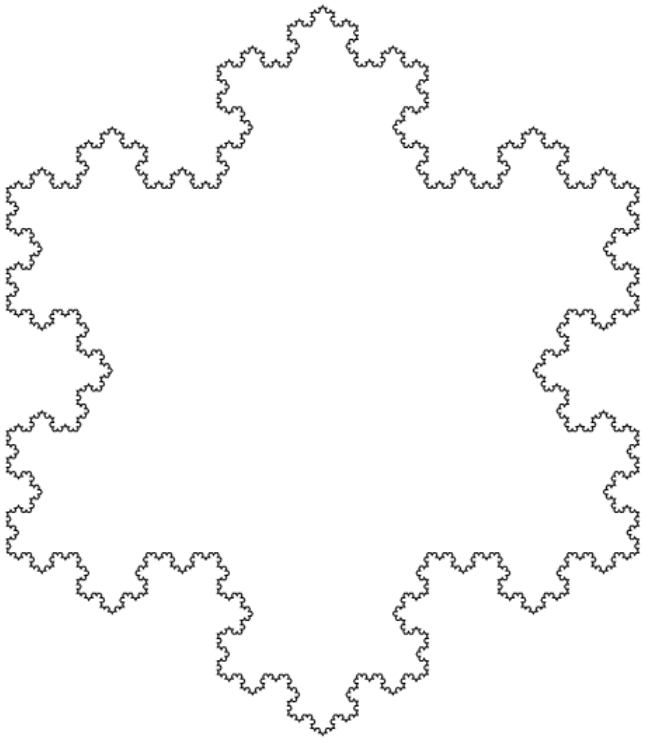


Figura 6 – Curva floco de neve - Fonte: autoria própria

Exemplo 8.3 (Triângulo de Sierpinski)**.** O triângulo de Sierpinski é obtido removendo repetidamente triângulos equiláteros (invertidos) de um triângulo equilátero inicial de lado com comprimento unitário. Também é útil pensar neste procedimento como a substituição repetida de um triângulo equilátero por três triângulos com metade da altura.

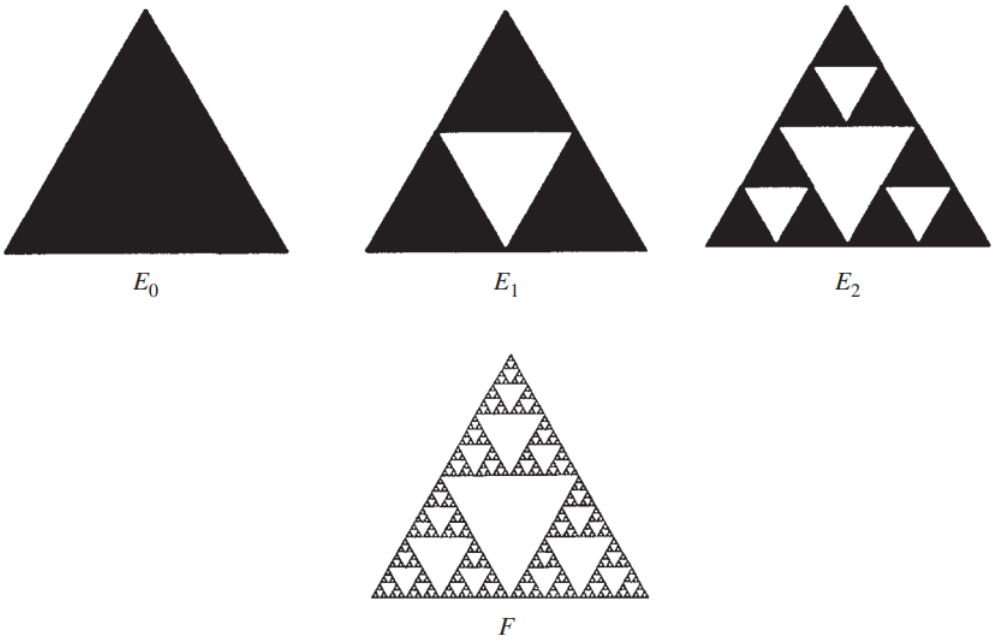


Figura 7 – Triângulo de Sierpinski - Fonte: (FALCONER, 2014)

Exemplo 8.4. Um análogo ao Conjunto de Cantor, chamado de “Poeira de Cantor” está ilustrado abaixo. Em cada estágio, cada quadrado restante é dividido em 16 quadrados menores, e apenas 4 são mantidos.

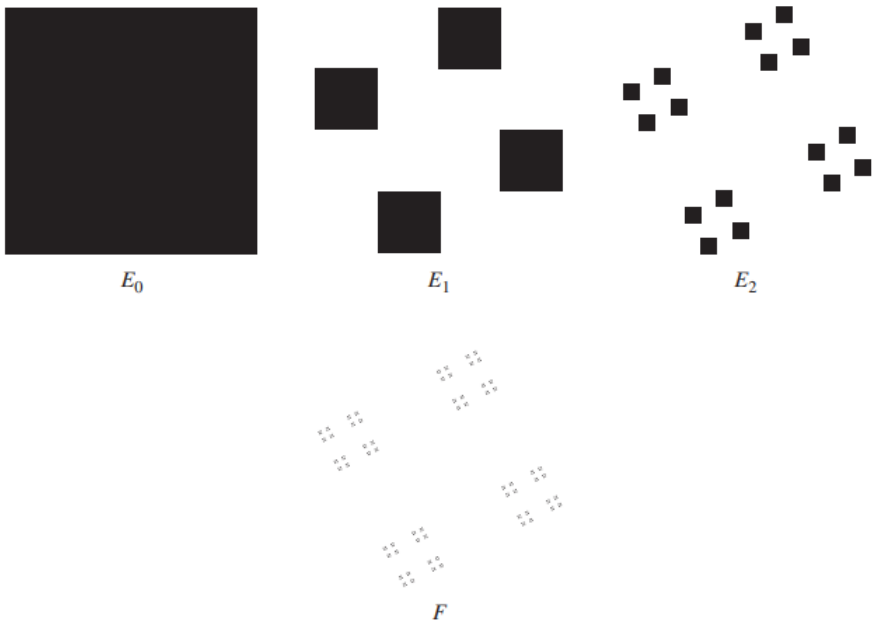


Figura 8 – Poeira de Cantor - Fonte: (FALCONER, 2014)

Estes exemplos têm propriedades semelhantes ao do conjunto de Cantor e da curva de von Koch.

9 Preliminares

É interessante enunciar e/ou provar alguns resultados de teoria da medida que usaremos bastante daqui em diante.

9.1 MEDIDAS E DISTRIBUIÇÕES DE MASSA

Uma família $\mathcal{X}$ de subconjuntos de um conjunto X é considerada uma σ-álgebra se:

1. $\varnothing$, X pertencem a $\mathcal{X}$.
2. Se A pertence a $\mathcal{X}$, então o complementar $A^{\complement} = X \setminus A$ pertence a $\mathcal{X}$.
3. Se (A_n) é uma sequência de conjuntos em $\mathcal{X}$, então a união $\bigcup_{n=1}^{\infty} A_n$ pertence a $\mathcal{X}$.

Dada uma σ-algebra $\mathcal{M}$ em X. Uma medida em $\mathcal{M}$ é uma função $\mu : \mathcal{M} \to [0, +\infty]$ tal que

1. $\mu(\varnothing) = 0$;
2. $\mu(A) \geq 0$ para todo $A \in \mathcal{M}$;
3. Se $\{E_j\}_1^{\infty}$ é uma sequência enumerável de conjuntos disjuntos em $\mathcal{M}$, então

$$\mu(\bigcup_{1}^{\infty} E_j) = \sum_{1}^{\infty} \mu(E_j).$$

Por enquanto, vamos nos concentrar apenas em medidas em subconjuntos de $\mathbb{R}^n$, basta considerar a σ-álgebra como o conjunto das partes de $\mathbb{R}^n$. Basicamente, uma medida é apenas uma forma de atribuir um "tamanho" a conjuntos, de modo que se um conjunto for decomposto em um número finito ou enumerável de pedaços de uma forma razoável, então tamanho do todo é a soma dos tamanhos dos pedaços.

Definição 9.1. Pensamos no **suporte** de uma medida como o conjunto no qual a medida se concentra. Formalmente, o suporte de μ, escrito spt μ, é o menor conjunto fechado X tal que $\mu(\mathbb{R}^n \setminus X) = 0$. Assim, x está no suporte se e somente se $\mu(B(x, r)) > 0$ para todo $r > 0$. Dizemos que μ é uma medida em um conjunto A se A contém o suporte de μ.

Definição 9.2. Uma medida em um subconjunto limitado de $\mathbb{R}^n$ para o qual $0 < \mu(\mathbb{R}^n) < \infty$ será chamada de **distribuição de massa**, e pensamos em $\mu(A)$ como a massa do conjunto A. Muitas vezes pensamos nisso de forma intuitiva: pegamos uma massa finita e a "espalhamos" de alguma forma por um conjunto X para obter uma distribuição de massa em X; as condições para uma medida serão então satisfeitas.

Vejamos agora alguns exemplos de medidas e distribuições de massa.

Exemplo 9.1 (Medida de contagem)**.** Para cada subconjunto A de $\mathbb{R}^n$, seja $\mu(A)$ o número de pontos em A se A é finito e ∞ caso contrário. Então μ é uma medida em $\mathbb{R}^n$:

1. $\mu(\varnothing) = 0$; pois não há nenhum elemento no conjunto vazio.

2. Tome $\{E_j\}_1^\infty$ uma sequência de conjuntos disjuntos em $\mathbb{R}^n$. Se $\mu(E_j) = \infty$ para algum $j \in \mathbb{N}$, a igualdade segue. Agora, suponha que todos os subconjuntos têm medida finita. Dados E_{k_1} e E_{k_2} subconjuntos de $\mathbb{R}^n$ quaisquer, como eles são disjuntos, temos que $\mu(E_{k_1} \cup E_{k_2}) = \mu(E_{k_1}) + \mu(E_{k_2})$. Suponha por indução forte que

$$\mu(\bigcup_{j=1}^{n} E_{k_j}) = \sum_{j=1}^{n} \mu(E_{k_j})$$

   Então

$$\mu(\bigcup_{j=1}^{n} E_{k_j} \cup E_{k_{n+1}}) = \mu(\bigcup_{j=1}^{n+1} E_{k_j}) = \sum_{j=1}^{n+1} \mu(E_{k_j})$$

   pois, $E_{k_j} \cap E_{k_l}$ sempre que $j \neq l$ implica $\bigcup E_{k_j} \cap E_{k_{n+1}} = \varnothing$. Por indução temos que

$$\mu(\bigcup_{j=1}^{\infty} E_j) = \sum_{j=1}^{\infty} E_j.$$

□

Exemplo 9.2 (Massa pontual)**.** Seja a um ponto em $\mathbb{R}^n$, defina $\mu_a(A) = 1$ se A contém a e 0 caso contrário. μ é uma distribuição de massa.

Exemplo 9.3 (Medida de Lebesgue em $\mathbb{R}$)**.** A medida de Lebesgue $\mathcal{L}^1$ estende a ideia de "comprimento" para uma coleção maior de subconjuntos de $\mathbb{R}$ que inclui os conjuntos de Borel. Para intervalos abertos e fechados, tomamos $\mathcal{L}^1(a, b) = \mathcal{L}^1[a, b] = b - a$. Se $A = \bigcup_i [a_i, b_i]$ é uma união finita ou enumerável de intervalos disjuntos, definimos $\mathcal{L}^1(A) = \sum(b_i - a_i)$ como o comprimento de A considerado como a soma do comprimento dos intervalos. Isso nos leva à definição da medida de Lebesgue $\mathcal{L}^1(A)$ de um conjunto arbitrário A.

$$\mathcal{L}^1(A) = \inf \left\{ \sum_{i=1}^{\infty} (b_i - a_i) : A \subset \bigcup_{i=1}^{\infty} [a_i, b_i] \right\},$$

isto é, olhamos para todas as coberturas de A por coleções enumeráveis de intervalos e tomamos o menor comprimento total de intervalo possível. Não é difícil ver que $\mathcal{L}(\varnothing) = 0$, mas é difícil mostrar σ-aditividade para conjuntos de Borel disjuntos A_i , o leitor pode ver a prova em (FOLLAND, 1999). A medida de Lebesgue em $\mathbb{R}$ é geralmente considerada como "comprimento", e frequentemente escrevemos $\mathrm{comprimento}(A)$ para $\mathcal{L}^1(A)$ quando desejamos enfatizar este significado intuitivo.

Proposição 9.1. O conjunto de Cantor F tem medida de Lebesgue igual a zero.

Demonstração. Seja $\mathcal{L}$ a medida de Lebesgue. O conjunto F é obtido removendo um intervalo aberto de tamanho $1/3$, depois dois intervalos de tamanhao $1/9$, em seguida quatro de tamanho $1/27$, e assim por diante. Logo

$$\mathcal{L}(F) = 1 - \sum_{n=0} \frac{2^n}{3^{n+1}} = 1 - 1/3 \sum_{n=0} \left(\frac{2}{3}\right)^n = 1 - \frac{1}{3}\left(\frac{1}{1-\frac{2}{3}}\right) = 1 - 1 = 0$$

Exemplo 9.4 (Medida de Lebesgue em $\mathbb{R}^n$)**.** Chamamos um conjunto da forma $A = \{(x_1, \ldots, x_n) \in \mathbb{R}^n : a_i \leqslant x_i \leqslant b_i\}$ um paralelepípedo coordenado em $\mathbb{R}^n$, seu volume n-dimensional A é dado por

$$\mathrm{vol}^n(A) = (b_1 - a_1)(b_2 - a_2) \cdots (b_n - a_n).$$

(Claro, se $n = 1$, um paralelepípedo coordenado é apenas um intervalo com vol^1 como comprimento; se $n = 2$, é um retângulo com vol^2 como área, e se $n = 3$, é um cuboide com vol^3 (o volume tridimensional usual.) Então a medida de Lebesgue n-dimensional $\mathcal{L}^n$ pode ser pensada como a extensão do volume n-dimensional para uma grande classe de conjuntos. Obtemos uma medida em $\mathbb{R}^n$ definindo

$$\mathcal{L}^n(A) = \inf \left\{ \sum_{i=1}^{\infty} \mathrm{vol}^n(A_i) : A \subset \bigcup_{i=1}^{\infty} A_i \right\}$$

onde o ínfimo é tomado sobre todas as coberturas de A por paralelepípedos coordenados A_i. Temos que $\mathcal{L}^n(A) = \mathrm{vol}^n(A)$ se A é um paralelepípedo coordenado ou, na verdade, qualquer conjunto para o qual o volume pode ser determinado pelas regras usuais de medição. Novamente, para ajudar a intuição, às vezes escrevemos area(A) no lugar de $\mathcal{L}^2(A), \mathrm{vol}(A)$ para $\mathcal{L}^3(A)$ e $\mathrm{vol}^n(A)$ para $\mathcal{L}^n(A)$.

Exemplo 9.5 (Distribuição de massa uniforme em um segmento)**.** Seja L um segmento de reta de comprimento unitário no plano. Defina $\mu(A) = \mathcal{L}^1(L \cap A)$ ou seja, o "comprimento" da interseção de A com L. Então μ é uma distribuição de massa com suporte em L, já que $\mu(A) = 0$ se $A \cap L = \varnothing$. Podemos pensar em μ como uma massa unitária espalhada uniformemente ao longo do segmento L.

Exemplo 9.6 (Restrição de medida)**.** Seja μ uma medida em $\mathbb{R}$ e E um subconjunto boreliano de $\mathbb{R}$. Podemos definir uma medida ν em $\mathbb{R}$, chamada de restrição de μ em E, por $\nu(A) = \mu(E \cap A)$ para cada conjunto A. Então ν é uma medida em $\mathbb{R}$ com suporte contido em $\overline{E}$.

O método a seguir é frequentemente usado para construir uma distribuição de massa em um subconjunto de $\mathbb{R}^n$. Envolve subdivisão repetida de uma massa entre partes de um conjunto de Borel E limitado. Suponha $\mathcal{E}_0 = E$. Para $k = 1, 2, \ldots$ seja $\mathcal{E}_k$ uma coleção de subconjuntos de E borelianos e disjuntos tais que cada conjunto U em $\mathcal{E}_k$ esteja contido em um dos conjuntos de $\mathcal{E}_{k-1}$ e contém um número finito de conjuntos em $\mathcal{E}_{k+1}$. Assumimos que o diâmetro máximo dos conjuntos em $\mathcal{E}_k$ tende a 0 quando $k \to \infty$. Definimos uma distribuição de massa em E por subdivisão repetida; veja a figura abaixo.

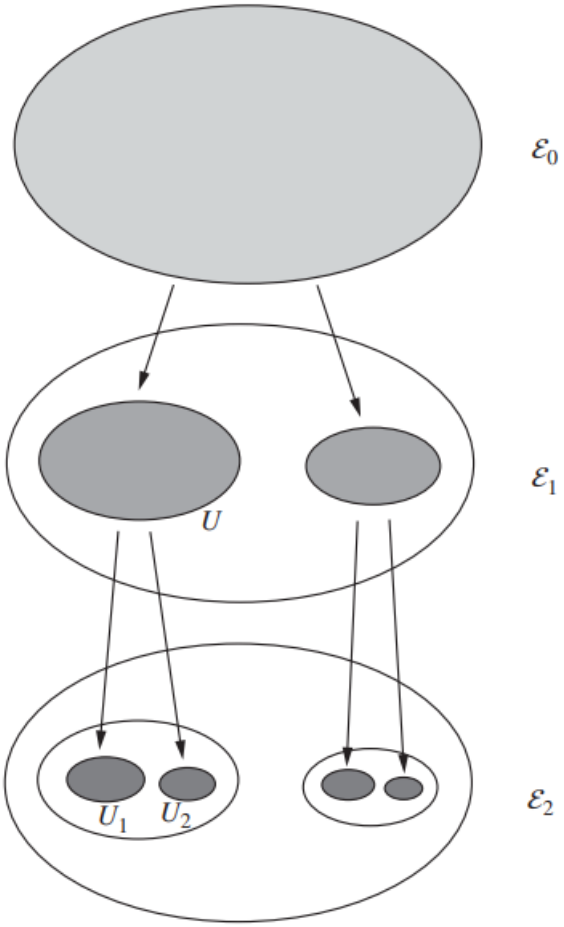


Figura 9 – Passos na construção de uma distribuição de massa μ por divisões repetidas. A massa nos conjuntos $\mathcal{E}_k$ é dividida entre os conjuntos de $\mathcal{E}_{k+1}$, então por exemplo, $\mu(U) = \mu(U_1) + \mu(U_2)$ - Fonte: (FALCONER, 2014).

Suponha que $0 < \mu(E) < \infty$ e divida essa massa entre os conjuntos $U_1, \ldots, U_m$ em $\mathcal{E}_1$ definindo $\mu(U_i)$ de tal forma que $\sum_{i=1}^{m} \mu(U_i) = \mu(E)$. Da mesma forma, atribuímos massas aos conjuntos de $\mathcal{E}_2$ de modo que se $U_1, \ldots, U_m$ são os conjuntos de $\mathcal{E}_2$ contidos em um conjunto U de $\mathcal{E}_1$, então $\sum_{i=1}^{m} \mu(U_i) = \mu(U)$. Em geral, atribuímos massas de modo que

$$\sum_i \mu(U_i) = \mu(U) \tag{9.1}$$

para cada conjunto U de $\mathcal{E}_k$, onde $\{U_i\}$ são os conjuntos disjuntos em $\mathcal{E}_{k+1}$ contidos em U. Para cada k, definimos E_k como a união dos conjuntos em $\mathcal{E}_k$ e definimos $\mu(A) = 0$ para todo A com $A \cap E_k = \varnothing$.

Denote $\mathcal{E}$ como a coleção de conjuntos que pertencem a $\mathcal{E}_k$ para algum k junto com os subconjuntos do $\mathbb{R}^n \setminus E_k$. O procedimento acima define a massa $\mu(A)$ de cada conjunto A em $\mathcal{E}$, e deve parecer razoável que, ao construir conjuntos a partir dos conjuntos em $\mathcal{E}$, ele especifique o suficiente sobre a distribuição da massa μ através de $\mathcal{E}$ para determinar $\mu(A)$para qualquer conjunto A boreliano. Este é de fato o caso, como afirma a seguinte proposição.

Proposição 9.2. Seja μ definido em uma coleção de conjuntos $\mathcal{E}$ como acima. Então a definição de μ pode ser estendida a todos os subconjuntos de $\mathbb{R}^n$ de modo que μ se torne uma medida. O valor de $\mu(A)$ é unicamente determinado se A for um conjunto de Borel. O suporte de μ está contido em $E_\infty = \bigcap_{k=1}^{\infty} \overline{E}_k$.

Demonstração. Se A é qualquer subconjunto de $\mathbb{R}^n$, seja

$$\mu(A) = \inf \left\{ \sum_{i=1}^{\infty} \mu(U_i) \ : A \cap E_\infty \subset \bigcup_{i=1}^{\infty} U_i \text{ e } U_i \in \mathcal{E} \right\}. \tag{9.2}$$

Assim, pegamos o menor valor possível de $\sum_{i=1}^{\infty} \mu(U_i)$ onde os conjuntos U_i estão em $\mathcal{E}$ e cobrem $A \cap E_\infty$; já definimos $\mu(U_i)$ para tais U_i.)

Não é difícil ver que se A é um dos conjuntos em $\mathcal{E}$, então 9.2 se reduz à massa $\mu(A)$ especificada na construção. A prova completa de que μ satisfaz todas as condições de uma medida e que seus valores nos conjuntos de $\mathcal{E}$ determinam seus valores nos conjuntos de Borel é bastante complicada e pode ser consultada em (RANA, 2002). Como $\mu(\mathbb{R}^n \backslash E_k) = 0$, temos $\mu(A) = 0$ se A é um conjunto aberto que não intersecta E_k para algum k, então o suporte de μ está em $\overline{E}_k$ para todo k. □

Exemplo 9.7 (Medida de Lebesgue por subdivisão repetida)**.** Defina $\mathcal{E}_k$ como a coleção de "intervalos binários" de comprimento 2^{-k}, que é da forma $[r2^{-k}, (r+1)2^{-k})$ onde $0 \leqslant r \leqslant 2^k - 1$. Se tomarmos $\mu([r2^{-k}, (r+1)2^{-k}]) = 2^{-k}$ na construção acima, obtemos que μ é a medida de Lebesgue em $[0, 1]$.

Para ver isso, observe que se I é um intervalo em $\mathcal{E}_k$ de comprimento 2^{-k} e I_1, I_2 são os dois subintervalos de I em $\mathcal{E}_{k+1}$ de comprimento 2^{-k-1}, temos $\mu(I) = \mu(I_1) + \mu(I_2)$ que é (9.1). Pela Proposição 9.2, μ se estende para uma distribuição de massa em $[0, 1]$. Temos $\mu(I) = \text{comprimento}(I)$ para I em $\mathcal{E}$, e é possível demonstrar que isso implica que μ coincide com a medida de Lebesgue em qualquer conjunto.

10 Medida de Hausdorff e dimensão

10.1 MEDIDA DE HAUSDORFF

Lembre-se de que se U é qualquer subconjunto não vazio do espaço euclidiano n-dimensional, $\mathbb{R}^n$, o diâmetro de U é definido como $|U| = \sup\{|x-y| : x, y \in U\}$, ou seja, a maior distância de qualquer par de pontos em U. Se $\{U_i\}$ é uma coleção enumerável (ou finita) de conjuntos de diâmetro no máximo δ que cobrem F, ou seja, $F \subset \bigcup_{i=1}^{\infty} U_i$ com $0 \leqslant |U_i| \leqslant \delta$ para cada i, dizemos que $\{U_i\}$ é uma $\delta-$cobertura de F.

Suponha que F é um subconjunto de $\mathbb{R}^n$ e seja s um número não negativo. Para qualquer $\delta > 0$ nós definimos

$$\mathcal{H}^s_\delta(F) = \inf\left\{\sum_{i=1}^{\infty} |U_i|^s : \{U_i\} \text{ é uma } \delta\text{-cobertura de } F\right\}. \tag{10.1}$$

Assim, olhamos para todas as coberturas de F por conjuntos de diâmetro no máximo δ e procuramos minimizar a soma das s-ésimas potências dos diâmetros. À medida que δ diminui, a classe de coberturas admissíveis de F é reduzida. Portanto, o ínfimo $\mathcal{H}^s_s(F)$ aumenta, e assim se aproxima de um limite quando $\delta \to 0$. Escrevemos

$$\mathcal{H}^s(F) = \lim_{\delta \to 0} \mathcal{H}^s_\delta(F). \tag{10.2}$$

Figura 10 – Um conjunto e duas $\delta-$coberturas possíveis para F. O ínfimo de $\Sigma|U_i|^s$ sobre todas essas $\delta-$coberturas$\{U_i\}$ nos dá $\mathcal{H}^s_\delta(F)$ - Fonte: (FALCONER, 2014).

Este limite existe para qualquer subconjunto F de $\mathbb{R}^n$, embora o valor do limite possa ser (e geralmente é) 0 ou ∞. Chamamos de $\mathcal{H}^s(F)$ a medida s-dimensional de Hausdorff de F.

Definição 10.1. Uma medida exterior em um conjunto não vazio X é uma função $\mu^* : \mathcal{P}(X) \to [0, +\infty]$ que satisfaz

- $\mu^*(\varnothing) = 0$,
- $\mu^*(A) \leq \mu^*(B)$ se $A \subset B$,
- $\mu^*(\bigcup_1^\infty A_j) \leq \sum_1^\infty (A_j)$.

Proposição 10.1. $\mathcal{H}^s$ é medida exterior.

Demonstração. De fato, $\mathcal{H}^s(\varnothing) = 0$ por vacuidade.

Dados $A \subset B$, $\mathcal{H}^s(A) \leq \mathcal{H}^s(B)$, pois toda δ-cobertura de B também é δ-cobertura de A, mas o contrário nem sempre é válido.

Temos $\mathcal{H}^s\left(\bigcup_i^\infty A_j\right) \leq \sum_i^\infty \mathcal{H}^s(A_j)$, pois para todo j existe $\{U_j^k\}_{k=1}^\infty$ tal que $A_j \subset \bigcup_{k=1}^\infty U_j^k$ e $\sum_{k=1}^\infty |U_j^k| \leq \mathcal{H}^s(A_j) + \varepsilon/2^j$, tomando $A = \bigcup_1^\infty A_j$, temos $A \subset U_{j,k=1}^\infty U_j^k$ e $\sum_{j,k} |U_j^k| \leq \sum_j \mathcal{H}^s(A_j) + \varepsilon$, o que implica $\mathcal{H}^s(A) \leq \sum_j \mathcal{H}^s(A_j) + \varepsilon$. Como ε é arbitrário, o resultado segue. □

Definição 10.2. Uma metric outer measure é uma medida exterior μ^* definida num espaço métrico (X, d) tal que

$$\mu^*(A \cup B) = \mu^*(A) + \mu^*(B)$$

para todo A, B tal que $d(A, B) > 0$, onde $d(A, B) = \inf\{d(a, b) | a \in A, b\}$.

Proposição 10.2. $\mathcal{H}^s$ é uma metric outer measure.

Demonstração. Sejam A e B conjuntos com $d(A, B) = \varepsilon > 0$. Para qualquer $\delta < \varepsilon/3$, as coberturas de A e B são disjuntas e portanto não há uma "contagem dupla". Disso segue que $\mathcal{H}^s(A \cup B) \geq \mathcal{H}^s(A) + \mathcal{H}^s(B)$, pela σ-aditividade provada acima segue que $\mathcal{H}^s(A \cup B) = \mathcal{H}^s(A) + \mathcal{H}^s(B)$. □

Enunciamos o seguinte teorema sem a demonstração, o leitor pode vê-la em (FOLLAND, 1999).

Teorema 10.1 (Critério de Carathéodory)**.** Se μ^* é uma medida exterior em X, a coleção $\mathcal{M}$ de conjuntos μ^*-mensuráveis é uma σ-álgebra, e a restrição de μ^* a $\mathcal{M}$ é uma medida completa (uma medida cujo domínio contém todos os subconjuntos de conjuntos com medida nula).

Segue do Critério de Carathéodory e da proposição anterior que $\mathcal{H}^s$ é uma medida quando restrita aos borelianos.

As medidas de Hausdorff generalizam as ideias familiares de comprimento, área, volume, etc. O leitor pode conferir nos trabalhos de (FALCONER, 1985), (FALCONER et al., 1999), (FEDERER, 2014), (ROGERS, 1998) as demonstrações que, para subconjuntos de $\mathbb{R}^n$, a medida de Hausdorff n-dimensional é, a menos de uma constante, apenas a medida de Lebesgue n-dimensional, ou seja, o volume n-dimensional usual. Mais precisamente, se F é um subconjunto Boreliano de $\mathbb{R}^n$, então

$$\mathcal{H}^n(F) = c_n^{-1} \mathrm{vol}^n(F) \tag{10.3}$$

onde c_n é o volume de uma bola n-dimensional de diâmetro l, de modo que $c_n = \pi^{n/2}/2^n(n/2)!$ se n é par e $c_n = \pi^{(n-1)/2}((n-1)/2)!/n!$ se n é ímpar.

De forma similar, para subconjuntos de menor dimensão de $\mathbb{R}^n$, temos que $\mathcal{H}^0(F)$ é o número de pontos em F; $\mathcal{H}^1(F)$ dá o comprimento de uma curva suave F; $\mathcal{H}^2(F) = (4/\pi) \times \text{area}(F)$ se F é uma superfície suave; $\mathcal{H}^3(F) = (6/\pi) \times \text{vol}(F)$; e $\mathcal{H}^m(F) = c_m^{-1} \times \text{vol}^m(F)$ se F é uma subvariedade m-dimensional suave de $\mathbb{R}^n$ (ou seja, uma superfície m-dimensional no sentido clássico).

As propriedades de escala de comprimento, área e volume são bem conhecidas. Na homotetia por um fator λ, o comprimento de uma curva é multiplicado por λ, a área de uma região plana é multiplicada por λ^2 e o volume de um objeto tridimensional é multiplicado por λ^3. Tais propriedades de escala são fundamentais para a teoria dos fractais.

Proposição 10.3. Seja S uma transformação de similaridade de razão $\lambda > 0$, i.e., $|S(x)-S(y)| = \lambda|x-y|$, $S : \mathbb{R}^n \to \mathbb{R}^n$. Se $F \subset \mathbb{R}^n$ então

$$\mathcal{H}^s(S(F)) = \lambda^s \mathcal{H}^s(F). \tag{10.4}$$

Demonstração. Se $\{U_i\}$ é uma δ-cobertura de F então $\{S(U_i)\}$ é uma $\lambda\delta$-cobertura de $S(F)$, então

$$\Sigma|S(U_i)|^s = \lambda^s \Sigma|U_i|^s$$

e

$$\mathcal{H}^s_{\lambda\delta}(S(F)) \leqslant \lambda^s \mathcal{H}^s_\delta(F)$$

ao tomar o ínfimo. Fazendo $\delta \to 0$ dá que $\mathcal{H}^s(S(F)) \leqslant \lambda^s \mathcal{H}^s(F)$. Substituindo S por S^{-1}, λ por $1/\lambda$, e F por $S(F)$ dá a desigualdade oposta necessária. □

Definição 10.3. Uma função $f : F \subset \mathbb{R}^n \to \mathbb{R}^m$ é chamada (c, α)-Holder se obedece

$$|f(x) - f(y)| \leqslant c|x-y|^\alpha \quad (x, y \in F) \tag{10.5}$$

para constantes $c > 0$ e $\alpha > 0$. É fácil ver que toda função Holder é uniformemente contínua.

Proposição 10.4. Seja $F \subset \mathbb{R}^n$ e $f : F \to \mathbb{R}^m$ um mapa (c, α)-Holder. Então para cada s, temos

$$\mathcal{H}^{s/\alpha}(f(F)) \leqslant c^{s/\alpha} \mathcal{H}^s(F). \tag{10.6}$$

Demonstração. Se $\{U_i\}$ é uma $\delta-$cobertura de F, então, já que $|f(F \cap U_i)| \leqslant c|F \cap U_i|^\alpha \leqslant c|U_i|^\alpha$, segue que $\{f(F \cap U_i)\}$ é uma ε-cobertura de $f(F)$, onde $\varepsilon = c\delta^\alpha$. Assim $\sum_i |f(F \cap U_i)|^{s/\alpha} \leqslant c^{s/\alpha} \sum_i |U_i|^s$, de modo que $\mathcal{H}^{s/\alpha}_\varepsilon(f(F)) \leqslant c^{s/\alpha} \mathcal{H}^s_\delta(F)$. Quando $\delta \to 0$, $\varepsilon \to 0$ também. □

Observação. Quando $\alpha = 1$, i. e.

$$|f(x) - f(y)| \leq c|x-y| \quad (x, y \in F) \tag{10.7}$$

f é chamada de Lipschitz, e

$$\mathcal{H}^s(f(F)) \leqslant c^s \mathcal{H}^s(F). \tag{10.8}$$

Proposição 10.5 (Propriedade de escala)**.** Seja $f : \mathbb{R}^n \to \mathbb{R}^n$ uma transformação de similaridade de razão $\lambda > 0$. Se $F \subset \mathbb{R}^n$, então

$$\mathcal{H}^s(f(F)) = \lambda^s \mathcal{H}^s(F). \tag{10.9}$$

Demonstração. Como

$$|f(x) - f(y)| = \lambda|x - y| \text{ logo } |f^{-1}(x) - f^{-1}(y)| = \lambda^{-1}|x - y| \quad (x, y \in F), \tag{10.10}$$

aplicando a proposição anterior a f^{-1} conseguimos o resultado. □

Em particular, (10.8) vale para qualquer função diferenciável e contínua com derivada limitada, pois tais funções são necessariamente Lipschitz pelo Teorema do Valor Médio. Se f é uma isometria, isto é, $|f(x) - f(y)| = |x - y|$, então $\mathcal{H}^s(f(F)) = \mathcal{H}^s(F)$. Assim, as medidas de Hausdorff são invariantes para translações (i.e. $\mathcal{H}^s(F + z) = \mathcal{H}^s(F)$, onde $F + z = \{x + z : x \in F\}$), e invariante para rotações.

10.2 DIMENSÃO DE HAUSDORFF

Vamos utilizar a definição de medida de Hausdorff para encontrar um ponto crítico de F.

Proposição 10.6. Se $\delta < 1$, então $\mathcal{H}^s(F)$ é não crescente com s para todo $F \subset \mathbb{R}^n$.

Demonstração. De fato, tome $\{U_i\}$ uma $\delta-$cobertura qualquer. Como $\delta < 1$, $\sum_{i=1}^{\infty} |U_i|^t \leq \sum_{i=1}^{\infty} |U_i|^s$ com $s \leq t$. Tomando o ínfimo em todas as $\delta-$coberturas, segue que $\mathcal{H}^s_\delta(F) \geq \mathcal{H}^t_\delta(F)$, ou seja, $\mathcal{H}^s_\delta(F)$ é não crescente em s. Como $\mathcal{H}^s(F) = \lim_{\delta \to 0} \mathcal{H}^s_\delta(F)$, obtemos o resultado. □

Além disso, se $t > s$ e $\{U_i\}$ é δ-cobertura de F temos

$$\sum_i |U_i|^t \leq \sum_i |U_i|^{t-s} |U_i|^s \leq \delta^{t-s} \sum_i |U_i|^s. \tag{10.11}$$

Tomando o ínfimo, temos $\mathcal{H}^t_\delta(F) \leq \delta^{t-s} \mathcal{H}^s_\delta(F)$. Fazendo $\delta \to 0$, se $\mathcal{H}^s(F) < \infty$, então $\mathcal{H}^t(F) = 0$ para $t > s$. Colocando isso num gráfico, temos o seguinte

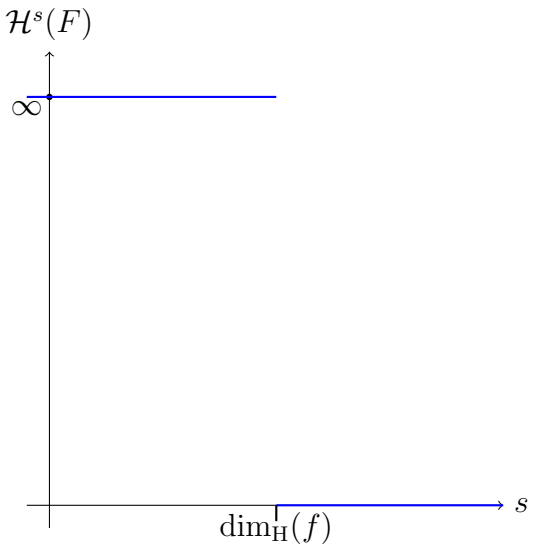


Figura 11 – Gráfico da medida s-dimensional de Hausdorff em função de s - Fonte: autoria própria

Ou seja, existe um valor crítico de s no qual $\mathcal{H}^s(F)$ "pula" de ∞ para 0. Este valor crítico é chamado **Dimensão de Hausdorff** de F, e escreve-se $\dim_H(F)$. Formalmente, temos

$$\dim_H(F) = \inf\{s \geq 0 : \mathcal{H}^s(F) = 0\} = \sup\{s : \mathcal{H}^s(F) = \infty\} \tag{10.12}$$

$$\mathcal{H}^s(F) = \begin{cases} \infty & \text{se } 0 \leqslant s < \dim_{\mathrm{H}} F \\ 0 & \text{se } s > \dim_{\mathrm{H}} F. \end{cases} \tag{10.13}$$

Se $s = \dim_H(F)$, então $0 \leq \mathcal{H}^s(F) \leq \infty$, a depender do conjunto. A dimensão de Hausdorff satisfaz as seguintes propriedades (que podem ser esperadas para qualquer definição razoável de dimensão).

- Monotonicidade. Se $E \subset F$ então $\dim_{\mathrm{H}} E \leqslant \dim_{\mathrm{H}} F$. Pois se $E \subset F$, então $\mathcal{H}^s(E) \leqslant \mathcal{H}^s(F)$ para cada s por propriedades de medida.

- Estabilidade enumerável. Se $F_1, F_2, \ldots$ é uma sequência enumerável de conjuntos então $\dim_H \bigcup_{i=1}^{\infty} F_i = \sup_{1 \leqslant i < \infty}\{\dim_{\mathrm{H}} F_i\}$. Certamente, $\dim_H \bigcup_{i=1}^{\infty} F_i \geqslant \dim_{\mathrm{H}} F_j$ para cada j pela propriedade de monotonicidade. Por outro lado, se $s > \dim_H F_i$ para todo i, então $\mathcal{H}^s(F_i) = 0$, de modo que $\mathcal{H}^s(\bigcup_{i=1}^{\infty} F_i) = 0$, dando a desigualdade oposta.

- Conjuntos enumeráveis. Se F é enumerável então $\dim_{\mathrm{H}} F = 0$. Pois se F_i é um único ponto $\mathcal{H}^0(F_i) = 1$ e $\dim_{\mathrm{H}} F_i = 0$, então por estabilidade enumerável, $\dim_H \bigcup_{i=1}^{\infty} F_i = 0$.

- Conjuntos abertos. Se $F \subset \mathbb{R}^n$ é aberto, então $\dim_{\mathrm{H}} F = n$. Pois F contém uma bola de volume n-dimensional positivo, $\dim_H F \geqslant n$, mas como F está contido em uma quantidade enumerável de bolas, $\dim_H F \leqslant n$ usando estabilidade enumerável e monotonicidade.

- Conjuntos suaves. Uma variedade de dimensão m é um espaço topológico em que cada ponto tem uma vizinhança que é homeomorfa ao espaço euclidiano de dimensão m. Uma subvariedade é um subconjunto de uma variedade que possui ele próprio a estrutura de uma variedade. Se F é uma subvariedade m-dimensional suave (i.e. continuamente diferenciável) de $\mathbb{R}^n$, então $\dim_{\mathrm{H}} F = m$. Em particular, curvas suaves têm dimensão l e superfícies suaves têm dimensão 2. Essencialmente, isso pode ser deduzido da relação entre as medidas de Hausdorff e Lebesgue.

Proposição 10.7. Seja $F \subset \mathbb{R}^n$ e suponha que $f : F \to \mathbb{R}^m$ é $(c, \alpha)-$Holder

$$|f(x) - f(y)| \leqslant c|x - y|^{\alpha} \quad (x, y \in F).$$

Então $\dim_{\mathrm{H}} f(F) \leqslant (1/\alpha)\dim_{\mathrm{H}} F$.

Demonstração. Se $s > \dim_{\mathrm{H}} F$ então pela proposição 10.4, $\mathcal{H}^{s/\alpha}(f(F)) \leqslant c^{s/\alpha}\mathcal{H}^s(F) = 0$, implicando que $\dim_{\mathrm{H}} f(F) \leqslant s/\alpha$ para todos $s > \dim_{\mathrm{H}} F$. □

Corolário 10.1. (a) Se $f : F \to \mathbb{R}^m$ é uma transformação Lipschitz então $\dim_{\mathrm{H}} f(F) \leqslant \dim_H F$.

(b) Se $f : F \to \mathbb{R}^m$ é uma transformação bi-Lipschitz, ou seja,

$$c_1|x - y| \leqslant |f(x) - f(y)| \leqslant c_2|x - y| \quad (x, y \in F) \tag{10.14}$$

onde $0 < c_1 \leqslant c_2 < \infty$, então $\dim_{\mathrm{H}} f(F) = \dim_{\mathrm{H}} F$.

Demonstração. (a) segue da proposição anterior tomando $\alpha = 1$. Em breve provaremos que f^{-1} existe (Proposição 10.8). Por enquanto assumimos como verdade e aplicamos isso a $f^{-1} : f(F) \to F$ que nos dá a outra desigualdade necessária para (b). □

Este corolário revela uma propriedade fundamental da dimensão de Hausdorff: a dimensão de Hausdorff é invariante sob transformações bi-Lipschitz. Assim, se dois conjuntos têm dimensões diferentes, não pode haver um mapa bi-Lipschitz de um para o outro.

Em topologia, dois conjuntos são considerados "iguais" se houver um homeomorfismo entre eles. Uma abordagem da geometria fractal é considerar dois conjuntos como "iguais" se houver um mapa bi-Lipschitz entre eles. Como as transformações bi-Lipschitz são necessariamente homeomorfismos (Proposição 10.8), os parâmetros topológicos fornecem um ponto de partida nessa direção, e dimensão de Hausdorff (e outras definições de dimensão) fornecem mais características distintivas para os fractais.

Proposição 10.8. Toda transformação bi-Lipschitz é um homeomorfismo com a sua imagem.

Demonstração. Seja $f : X \to Y$ uma transformação bi-Lipschitz. Então existem c_1 e c_2 reais não nulos tais que $c_1|x - y| \leq |f(x) - f(y)| \leq c_2|x - y|$ para todo $x, y \in X$. Observe que se $f(x) = f(y)$, então $c_1|x - y| \leq 0 \leq c_2|x - y| \iff x = y$, logo f é injetiva. Tome $f^{-1} : f(X) \to X$.

Para todo $y_1, y_2 \in f(X)$, existem $x_1, x_2 \in X$ únicos tais que $f(x_1) = y_1$ e $f(x_2) = y_2$. Daí,

$$c_1|x_1 - x_2| \leq |f(x_1) - f(x_2)| \leq c_2|x_1 - x_2|$$

isso nos dá

$$c_1|f^{-1}(y_1) - f^{-1}(y_2)| \leq |y_1 - y_2|$$

e

$$|y_1 - y_2| \leq c_2|f^{-1}(y_1) - f^{-1}(y_2)|$$

ou seja, f^{-1} também é bi-lipschitz. Logo f é homeomorfismo. □

Em geral, a dimensão de um conjunto por si só nos diz pouco sobre suas propriedades topológicas. No entanto, qualquer conjunto de dimensão menor que 1 é necessariamente tão esparso que é totalmente desconexo; isto é, dois de seus pontos não estão na mesma componente conexa:

Proposição 10.9. Um conjunto $F \subset \mathbb{R}^n$ com $\dim_H F < 1$ é totalmente desconexo.

Demonstração. Sejam x e y pontos distintos de F. Defina um mapa $f : \mathbb{R}^n \to [0, \infty)$ por $f(z) = |z-x|$. Como $|f(z)-f(w)| = ||z-x| - |w-x|| \leqslant |(z-x)-(w-x)| = |z-w|$ segue que f não aumenta distâncias. Pela parte (a) do corolário anterior, $\dim_H f(F) \leqslant \dim_{\mathrm{H}} F < 1$. Assim, $f(F)$ é um subconjunto de $\mathbb{R}$ de medida $\mathcal{H}^1$ igual a zero e, portanto, possui um complementar denso. Escolhendo r com $r \notin f(F)$ e $0 < r < f(y)$ segue que

$$F = \{z \in F : |z - x| < r\} \cup \{z \in F : |z - x| > r\}.$$

Assim, F está contido em dois conjuntos abertos disjuntos com x em um conjunto e y no outro, de modo que x e y estão em diferentes componentes conexas de F. □

10.3 EXEMPLOS DE CÁLCULO DE DIMENSÃO DE HAUSDORFF

Exemplo 10.1. Seja F a poeira de Cantor construída a partir do quadrado unitário como na figura abaixo. (A cada estágio da construção os quadrados são divididos em 16 quadrados com um quarto do comprimento do lado, dos quais o mesmo padrão de quatro quadrados são retidos.) Então $1 \leqslant \mathcal{H}^1(F) \leqslant \sqrt{2}$, daí $\dim_{\mathrm{H}} F = 1$.

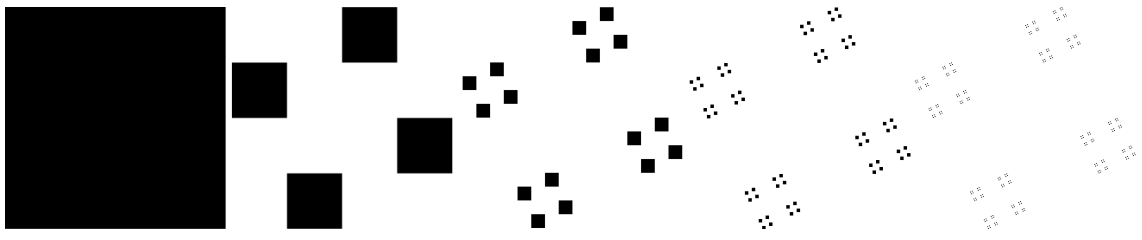


Figura 12 – Poeira de Cantor - Fonte: (FALCONER, 2014).

Observe que E_k, o k-ésimo estágio da construção, consiste em 4^k quadrados de lado 4^{-k} e, portanto, de diâmetro $4^{-k}\sqrt{2}$. Tomando os quadrados de E_k como uma δ-cobertura de F onde $\delta = 4^{-k}\sqrt{2}$, obtemos uma estimativa $\mathcal{H}^1_\delta(F) \leqslant 4^k 4^{-k}\sqrt{2}$ para o ínfimo em 10.1. Quando $k \to \infty$, $\delta \to 0$ nos dando $\mathcal{H}^1(F) \leqslant \sqrt{2}$.

Para estimar por baixo, denotamos proj como a projeção ortogonal no eixo x. A projeção ortogonal preserva distâncias, ou seja, $|\mathrm{proj}x - \mathrm{proj}y| \leqslant |x - y|$ se $x, y \in \mathbb{R}^2$, então proj é um mapa Lipschitz. Pela construção de F, a projeção ou "sombra" de F no eixo x é o intervalo unitário $[0, 1]$, pois sempre deixamos um quadrado em cada coluna. Usando a propriedade 10.8 para mapas lipschitz, temos:

$$1 = \mathrm{comprimento}(\,[0,\,1]) = \mathcal{H}^1([0,\,1]) = \mathcal{H}^1(\mathrm{proj}\,F) \leqslant \mathcal{H}^1(F).$$

□

É possível deduzir que este método de usar projeção ortogonal só funciona em casos específicos. Vamos aprender outros métodos.

Exemplo 10.2. Seja F o Conjunto de Cantor ternário. Se $s = \log 2/\log 3 = 0.6309\ldots$ então $\dim_{\mathrm{H}} F = s$ e $\frac{1}{2} \leq \mathcal{H}^s(F) \leqslant 1$.

Demonstração. Chamamos os intervalos que compõem os conjuntos E_k na construção de F de intervalos de nível k ou intervalos de k-ésimo nível. Assim E_k consiste de 2^k intervalos de nível k cada um de comprimento 3^{-k}. Tomando os intervalos de E_k como uma 3^k-cobertura de F nos dá que $\mathcal{H}^s_{3^k}(F) \leqslant 2^k 3^{-ks} = 1$ se $s = \log 2/\log 3$. Fazendo $k \to \infty$ resulta em $\mathcal{H}^s(F) \leqslant 1$ Para provar que $\mathcal{H}^s(F) \geqslant \frac{1}{2}$ mostraremos que

$$\sum_i |U_i|^s \geqslant \frac{1}{2} = 3^{-s} \tag{10.15}$$

para qualquer cobertura $\{U_i\}$ de F. Pela compacidade de F, podemos facilitar nossos cálculos. Assumindo que $\{U_i\}$ são intervalos, podemos aumentar seus diâmetros levemente e tomar uma subcobertura finita. Logo, precisamos apenas verificar a desigualdade acima se $\{U_i\}$ é uma coleção finita de subintervalos fechados de $[0, 1]$. Para cada U_i, seja k o inteiro tal que

$$3^{-(k+1)} \leqslant |U_i| < 3^{-k}. \tag{10.16}$$

Então U_i pode intersectar no máximo um intervalo de nível k desde que a separação desses intervalos de nível k seja de pelo menos 3^{-k}. Se $j \geqslant k$ então, por construção, U_i intersecta no máximo $2^{j-k} = 2^j 3^{-sk} \leqslant 2^j 3^s |U_i|^s$ intervalos de nível j de E_j, usando $3^{-(k+1)} \leqslant |U_i| < 3^{-k}$. Se escolhermos j grande o suficiente para que $3^{-(j+1)} \leqslant |U_i|$ para todos U_i, então, como os $\{U_i\}$ intersectam todos os 2^j intervalos básicos de comprimento 3^j, contar intervalos nos dá

$$\begin{aligned} 2^j &\leq \sum_i 2^j 3^s |U_i|^s \\ 2^j &\leq 2^j 3^s \sum_i |U_i|^s \\ 3^{-s} &\leq \sum_i |U_i|^s. \end{aligned}$$

□

Veremos mais a frente outras técnicas que nos ajudam a calcular ou estimar a dimensão de Hausdorff de certos conjuntos.

11 Outras definições de dimensão

11.1 DIMENSÃO BOX

Seja F qualquer subconjunto limitado não vazio de $\mathbb{R}^n$ e seja $N_\delta(F)$ o menor número de conjuntos de diâmetro no máximo δ que cobrem F. As dimensões box inferior e superior de F são definidas respectivamente como

$$\underline{\dim}_B F = \lim_{\delta \to 0} \frac{\log N_\delta(F)}{-\log \delta} \tag{11.1}$$

$$\overline{\dim}_B F = \lim_{\delta \to 0} \frac{\log N_\delta(F)}{-\log \delta} \tag{11.2}$$

Se estes forem iguais, nos referimos ao valor comum como dimensão box de F

$$\dim_{\mathrm{B}} F = \lim_{\delta \to 0} \frac{\log N_\delta(F)}{-\log \delta}. \tag{11.3}$$

Assumimos que $\delta > 0$ é suficientemente pequeno para garantir que $-\log \delta$ e quantidades semelhantes sejam estritamente positivas. Para evitar problemas com $'\log 0'$ ou $'\log \infty'$, geralmente consideramos a dimensão box apenas para conjuntos limitados não vazios. Ao desenvolver a teoria geral das dimensões box, assumimos que os conjuntos considerados são limitados e não vazios.

Existem diversas definições equivalentes de dimensão box que às vezes são mais convenientes de usar. Considere a coleção de cubos no δ-látice de $\mathbb{R}^n$, ou seja, cubos da forma

$$[m_1\delta, (m_1+1)\delta] \times \cdots \times [m_n\delta, (m_n+1)\delta]$$

onde $m_1, \ldots, m_n$ são inteiros. (Lembre-se de que um "cubo" é um intervalo em $\mathbb{R}$ e um quadrado em $\mathbb{R}^2$.) Observe o cubo em $\mathbb{R}^2$:

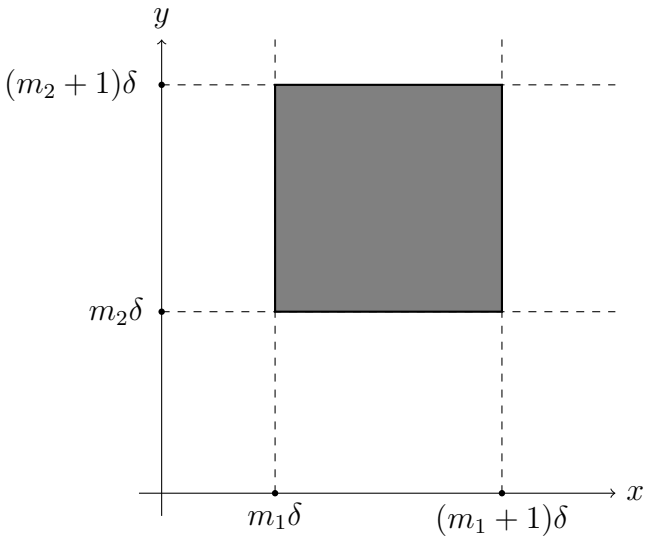


Figura 13 – Cubo no δ-látice em $\mathbb{R}^2$ - Fonte: autoria própria.

Seja $N'_\delta(F)$ o número de cubos do δ-látice que intersectam F. Eles obviamente fornecem uma coleção de $N'_\delta(F)$ conjuntos de diâmetro $\delta\sqrt{n}$ que cobrem F, então

$$N_{\delta\sqrt{n}}(F) \leqslant N'_\delta(F).$$

Se $\delta\sqrt{n} < 1$ então

$$\frac{\log N_{\delta\sqrt{n}}(F)}{-\log(\delta\sqrt{n})} \leqslant \frac{\log N'_\delta(F)}{-\log\sqrt{n} - \log\delta}$$

então tomando limite com $\delta \to 0$

$$\underline{\dim}_{\mathrm{B}} F \leqslant \underline{\lim}_{\delta\to 0} \frac{\log N'_\delta(F)}{-\log\delta} \tag{11.4}$$

e

$$\overline{\dim}_{\mathrm{B}} F \leqslant \overline{\lim}_{\delta\to 0} \frac{\log N'_\delta(F)}{-\log\delta}. \tag{11.5}$$

Por outro lado, qualquer conjunto de diâmetro no máximo δ está contido em 3^n cubos de látice de lado δ (escolhendo um cubo contendo algum ponto do conjunto junto com seus cubos vizinhos). Por isso

$$N'_\delta(F) \leqslant 3^n N_\delta(F)$$

tomando logaritmos e limites quando $\delta \to 0$ leva às desigualdades opostas.

Portanto, para encontrar as dimensões box, podemos também considerar $N_\delta(F)$ como o número de cubos de látice de lado δ que intersectam F.

Segundo (FALCONER, 1985). esta versão das definições são amplamente utilizadas empiricamente. Para encontrar a dimensão box de um conjunto plano F desenhamos uma malha de quadrados ou caixas (boxes em inglês) de lado δ e contamos o número $N_\delta(F)$ que se sobrepõem ao conjunto para vários δ pequenos. A dimensão é a taxa logarítmica na qual $N_\delta(F)$ aumenta à medida que $\delta \to 0$, e pode ser estimada pelo gradiente do gráfico de $\log N_\delta(F)$ contra $-\log\delta$.

Esta definição dá uma interpretação do significado da dimensão box. O número de cubos de lado δ que interceptam um conjunto é uma indicação de quão espalhado ou irregular o conjunto é quando examinado em escala δ. A dimensão reflete a rapidez com que as irregularidades se desenvolvem quando $\delta \to 0$. A seguir, vamos citar várias definições equivalentes para a dimensão box aqui creditadas a (FALCONER; HOWROYD, 1997).

Outra definição frequentemente usada de dimensão box é obtida tomando-se $N_\delta(F)$ como o menor número de cubos arbitrários de lado δ necessários para cobrir F. A equivalência desta definição segue como no caso da malha de cubos, observando que qualquer cubo de lado δ tem diâmetro $\delta\sqrt{n}$, e que qualquer conjunto de diâmetro no máximo δ está contido em um cubo de lado δ.

Da mesma forma, obteremos exatamente os mesmos valores se tomarmos $N_\delta(F)$ como o menor número de bolas fechadas de raio δ que cobrem F.

Uma formulação equivalente menos óbvia de dimensão box é com o maior número de bolas disjuntas de raio δ com centros em F. Seja este número $N'_\delta(F)$ e sejam $B_1, \ldots, B_{N'_\delta(F)}$

bolas disjuntas centradas em F e de raio δ. Se x pertence a F então x deve estar distante δ ou menor de um dos B_i, caso contrário a bola de centro x e raio δ pode ser adicionada para formar uma coleção maior de bolas disjuntas. Assim, as $N'_\delta(F)$ bolas concêntricas com as B_i mas de raio 2δ (diâmetro 4δ) cobrem F, resultando em

$$N_{4\delta}(F) \leqslant N'_\delta(F). \tag{11.6}$$

Suponha também que $B_1, \ldots, B_{N'_\delta(F)}$ são bolas disjuntas de raios δ com centros em F. Seja $U_1, \ldots, U_k$ qualquer coleção de conjuntos de diâmetro no máximo δ que cubram F. Como os U_j devem cobrir os centros das B_i, cada B_i deve conter pelo menos um dos U_j. Como as B_i são disjuntas, existem pelo menos tantos U_j quanto B_i. Por isso

$$N'_\delta(F) \leqslant N_\delta(F). \tag{11.7}$$

Tomando logaritmos e limites em ambas as inequações acima mostra que os valores das dimensões box ficam inalterados se $N_\delta(F)$ é substituído por este $N'_\delta(F)$.

Resumindo, temos o seguinte:

Definição 11.1. As dimensões box inferior e superior de um subconjunto F de $\mathbb{R}^n$ são dadas por

$$\underline{\dim}_{\mathrm{B}} F = \underline{\lim}_{\delta \to 0} \frac{\log N_\delta(F)}{-\log \delta} \tag{11.8}$$

$$\overline{\dim}_{\mathrm{B}} F = \overline{\lim_{\delta \to 0}} \frac{\log N_\delta(F)}{-\log \delta} \tag{11.9}$$

e a dimensão box de F por

$$\dim_{\mathrm{B}} F = \lim_{\delta \to 0} \frac{\log N_\delta(F)}{-\log \delta} \tag{11.10}$$

(se este limite existir), onde $N_\delta(F)$ é qualquer um dos seguintes:

(i) o menor número de bolas fechadas de raio δ que cobrem F;

(ii) o menor número de cubos de lado δ que cobrem F;

(iii) o número de cubos do δ-látice que intersectam F;

(iv) o menor número de conjuntos de diâmetro no máximo δ que cobrem F;

(v) o maior número de bolas disjuntas de raio δ com centros em F.

Segue uma ilustração de um conjunto F e das coberturas possíveis:

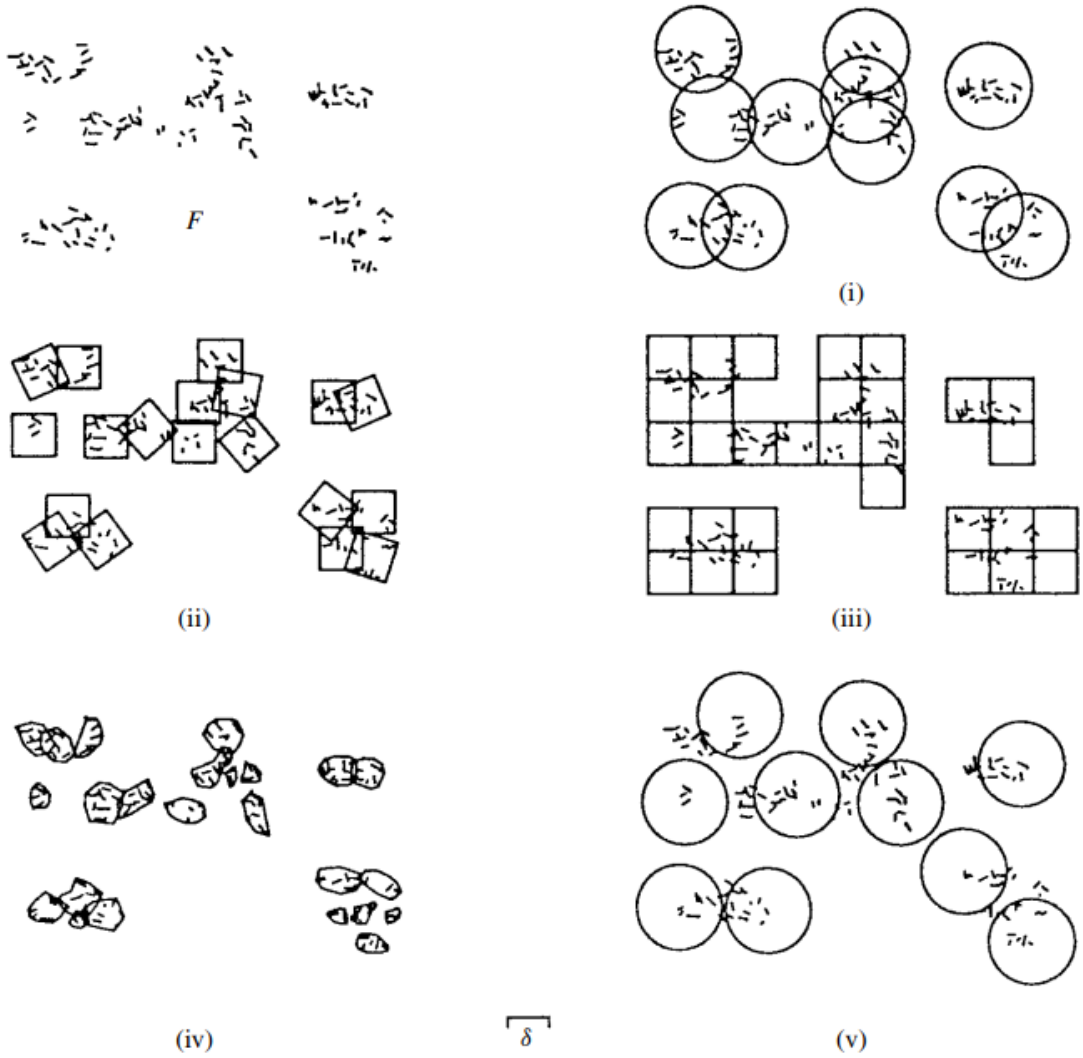


Figura 14 – Cinco maneiras de encontrar a dimensão box de F. O número $N_\delta(F)$ é tomado como: (i) o menor número de bolas fechadas de raio δ que cobrem F; (ii) o menor número de cubos de lado δ que cobrem F; (iii) o número de cubos do δ-látice que intersectam F; (iv) o menor número de conjuntos de diâmetro no máximo δ que cobrem F; (v) o maior número de bolas disjuntas de raio δ com centros em F - Fonte: (FALCONER, 2014).

Observação. É importante notar que é suficiente considerar limites quando δ tende a 0 através de qualquer sequência decrescente δ_k tal que $\delta_{k+1} \geqslant c\delta_k$ para alguma constante $0 < c < 1$; em particular para $\delta_k = c^k$. Para enxergar isso, observe que se $\delta_{k+1} \leqslant \delta < \delta_k$, então, com $N_\delta(F)$ sendo o menor número de conjuntos em uma δ-cobertura de F,

$$\frac{\log N_\delta(F)}{-\log \delta} \leqslant \frac{\log N_{\delta_{k+1}}(F)}{-\log \delta_k} = \frac{\log N_{\delta_{k+1}}(F)}{-\log \delta_{k+1} + \log(\delta_{k+1}/\delta_k)} \leqslant \frac{\log N_{\delta_{k+1}}(F)}{-\log \delta_{k+1} + \log c}$$

e então

$$\varlimsup_{\delta \to 0} \frac{\log N_\delta(F)}{-\log \delta} \leqslant \varlimsup_{k \to \infty} \frac{\log N_{\delta_k}(F)}{-\log \delta_k}. \tag{11.11}$$

A desigualdade oposta é trivial e o caso de limites inferiores pode ser tratado da mesma forma.

Há uma outra definição para dimensão box que vale a pena mencionar. Lembre-se que a δ-vizinhança F_δ de um subconjunto F de $\mathbb{R}^n$ é

$$F_\delta = \{x \in \mathbb{R}^n : |x - y| \leqslant \delta \text{ para alguns } y \in F\} \tag{11.12}$$

ou seja, o conjunto de pontos distantes δ de F. Consideramos a taxa na qual o volume n-dimensional de F_δ encolhe quando $\delta \to 0$. Em $\mathbb{R}^3$, se F é um único ponto então F_δ é uma bola com $\mathrm{vol}(F_\delta) = \frac{4}{3}\pi\delta^3$, e se F é um segmento de comprimento l então F_δ é semelhante a uma salsicha com $\mathrm{vol}(F_\delta) \sim \pi l\delta^2$, e se F for um conjunto plano de área a então F_δ é essencialmente um espessamento de F com $\mathrm{vol}(F_\delta) \sim 2a\delta$. Em cada caso, $\mathrm{vol}(F_\delta) \sim c\delta^{3-s}$ onde o inteiro s é a dimensão de F, então esse expoente de δ é indicativo da dimensão. O coeficiente c de δ^{3-s}, conhecido como **conteúdo de Minkowski** de F é uma medida de comprimento, área ou volume do conjunto, conforme apropriado.

Essa ideia se estende a dimensões fracionárias. Se F é um subconjunto de $\mathbb{R}^n$ e, para alguns s, $\mathrm{vol}^n(F_\delta)/\delta^{n-s}$ tende a um limite finito positivo quando $\delta \to 0$ onde vol^n denota volume n-dimensional, então faz sentido considerar F como s-dimensional. O limite é chamado de conteúdo s-dimensional de F, um conceito de uso ligeiramente restrito, uma vez que não é necessariamente aditivo em subconjuntos disjuntos, ou seja, não é uma medida. Mesmo que este limite não exista, poderemos extrair o expoente crítico de A e isto acaba por estar relacionado com a dimensão box.

Proposição 11.1. Se F é um subconjunto de $\mathbb{R}^n$, então

$$\underline{\dim}_{\mathrm{B}} F = n - \varliminf_{\delta \to 0} \frac{\log \mathrm{vol}^n(F_\delta)}{\log \delta}$$

$$\overline{\dim}_{\mathrm{B}} F = n - \varlimsup_{\delta \to 0} \frac{\log \mathrm{vol}^n(F_\delta)}{\log \delta}$$

onde F_δ é a δ-vizinhança de F. No contexto desta proposição, a dimensão box é às vezes chamada de dimensão de Minkowski ou dimensão de Minkowski-Bouligand.

Demonstração. Se F pode ser coberto por $N_\delta(F)$ bolas de raio $\delta < 1$ então F pode ser coberto pelas bolas concêntricas de raio 2δ. Portanto

$$\mathrm{vol}^n(F_\delta) \leqslant N_\delta(F) c_n (2\delta)^n$$

onde c_n é o volume da bola unitária em $\mathbb{R}^n$. Tomando logaritmos,

$$\frac{\log \mathrm{vol}^n(F_\delta)}{-\log \delta} \leqslant \frac{\log 2^n c_n + n \log \delta + \log N_\delta(F)}{-\log \delta},$$

aqui, $\varliminf_{\delta \to 0} \log 2^n c_n / \log \delta = 0$, pois $\log \delta \to -\infty$ quando $\delta \to 0$, daí

$$\lim_{\delta \to 0} \frac{\log \mathrm{vol}^n(F_\delta)}{-\log \delta} \leqslant -n + \underline{\dim}_{\mathrm{B}} F \tag{11.13}$$

com uma desigualdade semelhante para os limites superiores. Por outro lado se houver $N_\delta(F)$ bolas disjuntas de raio δ com centros em F, então somando seus volumes,

$$N_\delta(F)c_n\delta^n \leqslant \mathrm{vol}^n(F_\delta).$$

Tomando logaritmos e fazendo $\delta \to 0$ nos dá

$$\begin{aligned}\underline{\lim}_{\delta\to 0}\frac{\log \mathrm{vol}^n(F_\delta)}{-\log\delta} &\geq \underline{\lim}_{\delta\to 0}\frac{N_\delta(F)}{-\log\delta} - n \\ &\geq \underline{\dim}_B F - n\end{aligned}$$

que é a desigualdade oposta, e usando a quinta definição equivalente de dimensão box. □

Proposição 11.2. Para todo $F \subset \mathbb{R}^n$ limitado e não vazio temos

$$\dim_{\mathrm{H}} F \leq \underline{\dim}_B F \leq \overline{\dim}_B F \tag{11.14}$$

Demonstração. Suponha que $1 < \mathcal{H}^s(F) = \lim_{\delta\to 0}\mathcal{H}^s(F)$ para algum $s \geq 0$. Então, para todo $\delta > 0$ suficientemente pequeno,

$$1 < \mathcal{H}^s_\delta(F) \leqslant N_\delta(F)\delta^s.$$

Onde $N_\delta(F)$ é o menor número de conjuntos de diâmetro δ que podem cobrir F, usando 10.1. Tomando logaritmos, $0 < \log N_\delta(F) + s\log\delta$, e segue que $s \leq \underline{\lim}_{\delta\to 0}\log N_\delta(F)/-\log\delta$. A segunda desigualdade vem de propriedades de limite inferior e superior. □

Exemplo 11.1. Seja F o conjunto de Cantor ternário. Então $\underline{\dim}_{\mathrm{B}}F = \overline{\dim}_{\mathrm{B}}F = \log 2/\log 3$.

Demonstração. A cobertura usual pelos 2^k intervalos de nível-k de E_k de comprimento 3^{-k} nos dá que $N_\delta(F) \leqslant 2^k$ se $3^{-k} < \delta \leqslant 3^{-k+1}$. De 11.2

$$\overline{\dim}_{\mathrm{B}}F = \overline{\lim}_{\delta\to 0}\frac{\log N_\delta(F)}{-\log\delta} \leqslant \overline{\lim}_{k\to\infty}\frac{\log 2^k}{\log 3^{k-1}} = \frac{\log 2}{\log 3}.$$

Por outro lado, qualquer intervalo de comprimento δ com $3^{-k-1} \leqslant \delta < 3^{-k}$ intersecta no máximo um dos intervalos de nível k de comprimento 3^{-k} usados na construção de F. Existem 2^k tais intervalos, então pelo menos 2^k intervalos de comprimento δ são necessários para cobrir F. Portanto, $N_\delta(F) \geqslant 2^k$ levando a $\underline{\dim}_B F \geq \log 2/\log 3$. □

Assim, pelo menos para o conjunto de Cantor, $\dim_{\mathrm{H}} F = \dim_{\mathrm{B}} F$.

11.2 PROPRIEDADES DA DIMENSÃO BOX

Proposição 11.3. Seja $F \subset \mathbb{R}^n$. Então

$$\underline{\dim}_{\mathrm{B}}\overline{F} = \underline{\dim}_{\mathrm{B}}F$$

e

$$\overline{\dim}_{\mathrm{B}}\overline{F} = \overline{\dim}_{\mathrm{B}}F.$$

Demonstração. seja $B_1, \ldots, B_k$ uma coleção finita de bolas fechadas de raios δ. O conjunto fechado $\bigcup_{i=1}^{k} B_i$ contém F se e somente se também contém $\overline{F}$. Portanto, o menor número de bolas fechadas de raio δ que cobrem F é igual ao menor número necessário para cobrir o conjunto maior F. O resultado segue. □

Uma consequência imediata disso é que se F for um subconjunto denso de um conjunto aberto de $\mathbb{R}^n$, então $\underline{\dim}_B F = \overline{\dim}_B F = n$. Por exemplo, seja F o conjunto (enumerável) de números racionais entre 0 e 1. Então $\overline{F}$ é o intervalo inteiro [0,1], de modo que $\underline{\dim}_{\mathrm{B}} F = \overline{\dim}_{\mathrm{B}} F = 1$. Assim, conjuntos enumeráveis, que são muito pequenos comparados aos números reais, podem ter dimensão box diferente de zero.

Além disso, a dimensão box de cada número racional considerado como um conjunto unitário é claramente zero, mas a união enumerável desses conjuntos unitários tem dimensão 1. Consequentemente, geralmente não é verdade que $\dim_{\mathrm{B}} \bigcup_{i=1}^{\infty} F_i = \sup_i \{\dim_{\mathrm{B}} F_i\}$.

Isto limita severamente a utilidade da box - introduzir um conjunto enumerável pode causar estragos na dimensão. Poderíamos esperar melhorar algo restringindo a atenção a conjuntos fechados, mas as dificuldades ainda permanecem, como mostra o seguinte exemplo de um conjunto "esparso" com dimensão diferente de zero.

Exemplo 11.2. $F = \{0, 1, \frac{1}{2}, \frac{1}{3}, \ldots\}$ é um subconjunto compacto de $\mathbb{R}$ com $\dim_B F = \frac{1}{2}$.

Demonstração. Tome $0 < \delta < \frac{1}{2}$. Observe que $\dfrac{1}{k-1} - \dfrac{1}{k} = \dfrac{1}{k(k-1)}$, então seja k satisfazendo $\dfrac{1}{k(k-1)} > \delta \geq \dfrac{1}{k(k+1)}$. Se $|U| \leq \delta$, U pode cobrir no máximo um dos pontos de $\{1, 1/2, \ldots, 1/k\}$. Assim, precisamos de k conjuntos de diâmetro δ para cobrir F, daí $N_\delta(F) \geq k$.

$$\frac{\log N_\delta(F)}{-\log \delta} \geqslant \frac{\log k}{\log k(k+1)} \text{ é uma indeterminação do tipo } \infty/\infty$$

$$\underline{\lim}_{\delta \to 0} \frac{\log k}{\log k(k+1)} \overset{\text{l'hospital}}{=} \underline{\lim}_{\delta \to 0} \frac{k+1}{2k+1} = \frac{1}{2}.$$

pois $k \to \infty$ quando $\delta \to 0$, então $\underline{\dim}_{\mathrm{B}} F \geqslant \dfrac{1}{2}$.

Por outro lado, se $0 < \delta < 1/2$, tome k tal que $\dfrac{1}{k(k-1)} > \delta \geq \dfrac{1}{k(k+1)}$. Então $\delta(k+1) \geq 1/k$, ou seja, $k+1$ intervalos de tamanho δ cobrem $[-, 1/k]$, sobrando $k-1$ pontos de F que podem ser cobertos por $k-1$ intervalos. Assim, $N_\delta(F) \leq 2k$, e

$$\frac{\log N_\delta(F)}{-\log \delta} \leqslant \frac{\log(2k)}{\log k(k-1)}$$

analogamente ao anterior, chegamos em

$$\overline{\dim}_{\mathrm{B}} F \leqslant \frac{1}{2}.$$

□

12 Técnicas para calcular dimensões

Como regra geral, obtemos limites superiores para medidas e dimensões de Hausdorff ao encontrar coberturas eficazes através de pequenos conjuntos, e limites inferiores, colocando medidas ou distribuições de massa no conjunto. Para a maioria dos fractais, estimativas superiores naturais podem ser obtidas utilizando coberturas naturais por pequenos conjuntos.

Proposição 12.1. Suponha que F possa ser coberto por n_k conjuntos de diâmetro no máximo δ_k com $\delta_k \to 0$ quando $k \to \infty$. Então

$$\dim_{\mathrm{H}} F \leqslant \underline{\dim}_{\mathrm{B}} F \leqslant \underline{\lim}_{k\to\infty} \frac{\log n_k}{-\log \delta_k}.$$

Além disso, se $n_k \delta_k^s$ permanecer limitado quando $k \to \infty$, então $\mathcal{H}^s(F) < \infty$. Se $\delta_k \to 0$ mas $\delta_{k+1} \geq c\delta_k$ para algum $0 < c < 1$, então

$$\overline{\dim}_{\mathrm{B}} F \leqslant \overline{\lim}_{k\to\infty} \frac{\log n_k}{-\log \delta_k}.$$

Demonstração. As desigualdades para a dimensão box são imediatas a partir das definições e da observação em 11.11. A desigualdade $\dim_{\mathrm{H}} F \leqslant \underline{\dim}_{\mathrm{B}} F$ está em 11.14, e se $n_k \delta_k^s$ é limitado, então $\mathcal{H}^s_{\delta_k}(F) \leqslant n_k \delta_k^s$, daí $\mathcal{H}^s_{\delta_k}(F)$ tende a um limite finito $\mathcal{H}^s(F)$ quando $k \to \infty$. □

Com surpreendente frequência, o limite superior "óbvio" para a dimensão de Hausdorff de um conjunto acaba sendo o valor real. No entanto, demonstrar isso pode ser difícil. Para obter um limite superior, é suficiente avaliar somas da forma $\sum |U_i|^s$ para coberturas específicas $\{U_i\}$ de F, enquanto para um limite inferior, devemos mostrar que $\sum |U_i|^s$ é maior do que alguma constante positiva para todas as δ-coberturas de F.

Claramente, um grande número de tais coberturas está disponível. Em particular, ao trabalhar com a dimensão de Hausdorff, em oposição à dimensão box, é necessário considerar coberturas em que alguns dos U_i são muito pequenos e outros têm diâmetros relativamente grandes - isso impede estimativas generalizadas para $\sum |U_i|^s$, como as disponíveis para limites superiores.

Uma maneira de contornar essas dificuldades é mostrar que nenhum conjunto individual U pode cobrir muito de F em comparação com o seu tamanho medido como $|U|^s$. Então, se $\{U_i\}$ cobre F inteiro, a soma $\sum |U_i|^s$ não pode ser muito pequena. A maneira usual de fazer isso é concentrar uma distribuição de massa adequada μ em F e comparar a massa $\mu(U)$ coberta por U com $|U|^s$ para cada U.

Proposição 12.2 (Princípio de distribuição de massa)**.** Seja μ uma distribuição de massa em F e suponha que, para algum s, existam números $c > 0$ e $\varepsilon > 0$ tais que:

$$\mu(U) \leqslant c|U|^s \tag{12.1}$$

para todos os conjuntos U com $|U| \leq \varepsilon$. Então, $\mathcal{H}^s(F) \geq \mu(F)/c$ e

$$s \leqslant \dim_{\mathrm{H}} F \leqslant \underline{\dim}_{\mathrm{B}} F \leqslant \overline{\dim}_{\mathrm{B}} F.$$

Demonstração. Se $\{U_i\}$ for qualquer cobertura de F, então

$$0 < \mu(F) \leqslant \mu\left(\bigcup_i U_i\right) \leqslant \sum_i \mu(U_i) \leqslant c\sum_i |U_i|^s \tag{12.2}$$

usando propriedades de uma medida e a hipótese da proposição. Tomando ínfimos, $\mathcal{H}^s(F) \geq \frac{\mu(F)}{c}$ se δ for suficientemente pequeno, então $\mathcal{H}^s(F) \geq \frac{\mu(F)}{c}$. Como $\mu(F) > 0$, obtemos $\dim_{\mathrm{H}} F \geq s$. □

Observe que a conclusão $\mathcal{H}^s(F) \geq \frac{\mu(F)}{c}$ permanece verdadeira se μ for uma distribuição de massa em $\mathbb{R}^n$ e F for qualquer subconjunto.

Exemplo 12.1. Seja $F_1 = F \times [0,1] \subset \mathbb{R}^2$ o produto do conjunto de Cantor ternário F e o intervalo unitário. Em seguida, definindo $s = 1 + \log 2/\log 3$, temos $\dim_B F_1 = \dim_{\mathrm{H}} F_1 = s$, com $0 < \mathcal{H}^s(F_1) < \infty$.

Demonstração. Para cada k, existe uma cobertura de F por 2^k intervalos de comprimento 3^k. Uma coluna de 3^k quadrados de lado 3^{-k} (diâmetro $3^{-k}\sqrt{2}$) cobre a parte de F_1 acima de cada intervalo desses, então, juntando todos esses, F_1 pode ser coberto por $2^k 3^k$ quadrados de lado 3^{-k}. Portanto,

$$\mathcal{H}^s_{3-k\sqrt{2}}(F_1) \leqslant 3^k 2^k (3^{-k}\sqrt{2})^s = (3 \cdot 2 \cdot 3^{-1-\log 2/\log 3})^k 2^{s/2} = 2^{s/2},$$

então $\mathcal{H}^s(F_1) \leqslant 2^{s/2}$ e $\dim_{\mathrm{H}} F_1 \leq \underline{\dim}_B F_1 \leq \overline{\dim}_B F_1 \leq s$. Para o limite inferior, definimos uma distribuição de massa μ em F_1 ao considerar a distribuição natural de massa em F descrita acima (cada intervalo no passo k de F de lado 3^{-k} tem massa 2^{-k}) e "espalhando-a" uniformemente ao longo dos intervalos acima de F.

Assim, se U for um retângulo, com lados paralelos aos eixos coordenados, de altura $h \leqslant 1$, em cima de um intervalo de nível k de F, então $\mu(U) = h2^{-k}$. Qualquer conjunto U está contido em um quadrado de lado $|U|$ com lados paralelos aos eixos coordenados. Se $3^{-(k+1)} \leq |U| < 3^{-k}$ então U está em cima de no máximo um intervalo do passo k de F de lado 3^{-k}, então

$$\mu(U) \leqslant |U|2^{-k} \leqslant |U|3^{-k\log 2/\log 3} \leqslant |U|(3|U|)^{\log 2/\log 3} = 3^{\log 2/\log 3}|U|^s = 2|U|^s.$$

Pelo princípio de distribuição de massa, $\mathcal{H}^s(F_1) > \frac{1}{2}$. □

O procedimento usado para encontrar dimensões no exemplo acima, tomando uma cobertura natural para obter um limite superior e usar o princípio de distribuição de massa para o limite inferior, é a base de muitos cálculos de dimensão. Iremos aplicá-lo a uma ampla classe de fractais autossimilares no Teorema 13.3. Por enquanto consideramos uma construção geral de subconjuntos fractais de $\mathbb{R}$ que pode ser pensada como uma generalização do conjunto de Cantor do terço médio.

Seja $[0,1] = E_0 \supset E_1 \supset E_2 \supset \ldots$ uma sequência decrescente de conjuntos, com cada E_k uma união de um número finito de intervalos fechados disjuntos chamados intervalos básicos

de k-ésimo nível, com cada intervalo de E_k contendo pelo menos dois intervalos de E_{k+1}, e o comprimento máximo dos intervalos de k-ésimo nível tendendo a quando $k \to \infty$. Então o conjunto

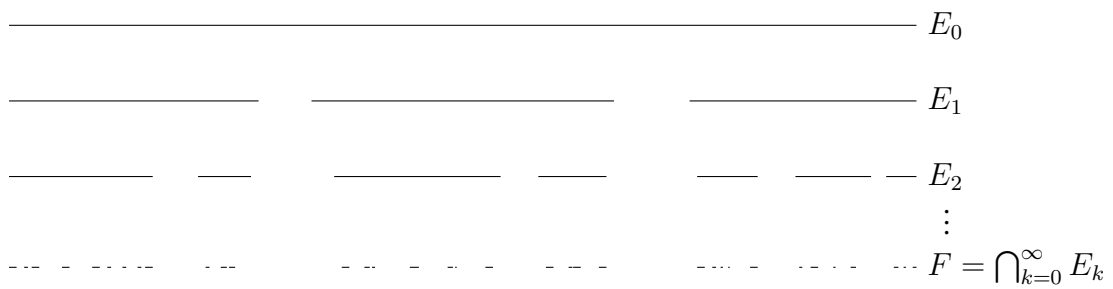
$$F = \bigcap_{k=0}^{\infty} E_k \tag{12.3}$$

é um subconjunto totalmente desconexo de $[0, 1]$ que geralmente é um fractal.

Limites superiores naturais para a dimensão de F estão disponíveis tomando o intervalos de cada E_k como intervalos de cobertura, mas, como sempre, é mais difícil encontrar limites inferiores que sejam iguais aos limites superiores. Observe que nos exemplos a seguir, as estimativas superiores para $\dim_{\mathrm{H}}(F)$ dependem do número e tamanho dos intervalos básicos, enquanto as estimativas inferiores dependem do seu espaçamento. Para que sejam iguais, os intervalos de nível $(k + 1)$ devem ser "quase uniformemente distribuídos" dentro dos intervalos de k-ésimo nível.

Exemplo 12.2. Seja s um número com $0 < s < 1$. Suponha que na construção geral 12.3, para cada intervalo I de k-ésimo nível, os intervalos de $(k + 1)$-ésimo nível $I_1, \ldots, I_m$ $(m \geq 2)$ contidos em I são de mesmo comprimento e igualmente espaçados, sendo os comprimentos dados por

$$|I_i|^s = \frac{1}{m}|I|^s \quad (1 \leqslant i \leqslant m) \tag{12.4}$$



Exemplo da construção geral de um subconjunto de $\mathbb{R}$ - Fonte: autoria própria

com as extremidades esquerdas de I_1 e I coincidentes, e as extremidades direitas de I_m e I coincidindo. Então $\dim_{\mathrm{H}} F = s$ e $0 < \mathcal{H}^s(F) < \infty$. (Observe que m pode ser diferente para diferentes intervalos I na construção, de modo que os intervalos de k-ésimo nível podem ter comprimentos muito diferentes.)

Demonstração. Com I e I_i como dito acima,

$$|I|^s = \sum_{i=1}^{m} |I_i|^s. \tag{12.5}$$

Aplicando isso indutivamente aos intervalos de nível k para k sucessivos e lembrando que E_0 é um intervalo de comprimento 1, temos para cada k, que $1 = \sum_{I_i \in E_k} |I_i|^s$, onde somamos sobre todos os intervalos I_i de nível k. Os intervalos do passo k cobrem F; uma vez que o comprimento máximo do intervalo tende a 0 conforme $k \to \infty$, segue que $\mathcal{H}^s_\delta(F) \leq 1$ para δ suficientemente pequeno, nos dando $\mathcal{H}^s(F) \leqslant 1$.

Agora distribua uma massa μ em F de tal forma que $\mu(I) = |I|^s$ sempre que I for qualquer intervalo do passo k. Assim, começando com massa unitária em $[0, 1]$ dividimos isso igualmente entre cada intervalo de nível 1, a massa em cada um desses intervalos sendo dividida igualmente entre cada subintervalo de nível 2 e assim por diante; veja a Proposição 9.2. A equação (12.5) garante que obteremos uma distribuição de massa em F com $\mu(I) = |I|^s$ para cada intervalo básico. Agora vamos estimar $\mu(U)$ para um intervalo U com extremidades em F. Seja I o menor intervalo básico que contém U; suponha que I seja um intervalo de k-ésimo nível, e sejam $I_i, \ldots, I_m$ os intervalos de nível $(k + 1)$ contidos em I. Então U intersecta um número $j \geqslant 2$ dos I_i, caso contrário U estaria contido em um intervalo básico menor. O espaçamento entre I_i consecutivos é

$$\begin{aligned}(|I| - m|I_i|)/(m-1) &= |I|(1 - m|I_i|/|I|)/(m-1 \\ &= |I|(1 - m^{1-1/s})/(m-1) \\ &\geqslant c_s|I|/m,\end{aligned}$$

onde $c_s = (1 - 2^{1-1/s})$, usando que $m \geq 2$ e $0 < s < 1$. Por isso

$$|U| \geqslant \frac{j-1}{m} c_s|I| \geqslant \frac{j}{2m} c_s|I|.$$

Por (12.4),

$$\begin{aligned}\mu(U) &\leqslant j\mu(I_i) = j|I_i|^s = \frac{j}{m}|I|^s \\ &\leqslant 2^s c_s^{-s} \left(\frac{j}{m}\right)^{1-s} |U|^s \leqslant 2^s c_s^{-s}|U|^s. \end{aligned} \tag{12.6}$$

Isso é verdade para qualquer intervalo U com pontos finais em F e, portanto, para qualquer conjunto U ao aplicar (12.6) para o menor intervalo contendo $U \cap F$. Pelo princípio da distribuição de massa, $\mathcal{H}^s(F) > 0$. □

Chamamos os conjuntos obtidos quando m é mantido constante durante a construção do Exemplo anterior de **conjuntos de Cantor uniformes**. Eles proporcionam uma generalização natural do conjunto de Cantor do terço médio.

Exemplo 12.3 (Conjuntos de Cantor uniformes)**.** Seja $m \geq 2$ um inteiro e $0 < r < 1/m$. Seja F o conjunto obtido pela construção em que cada intervalo básico I é substituído por m subintervalos igualmente espaçados de comprimento $r|I|$, as extremidades de I coincidem com as extremidades dos subintervalos extremos. Então $\dim_{\mathrm{H}} F = \dim_{\mathrm{B}} F = \log m/ - \log r$, e $0 < \mathcal{H}^{\log m/-\log r}(F) < \infty$.

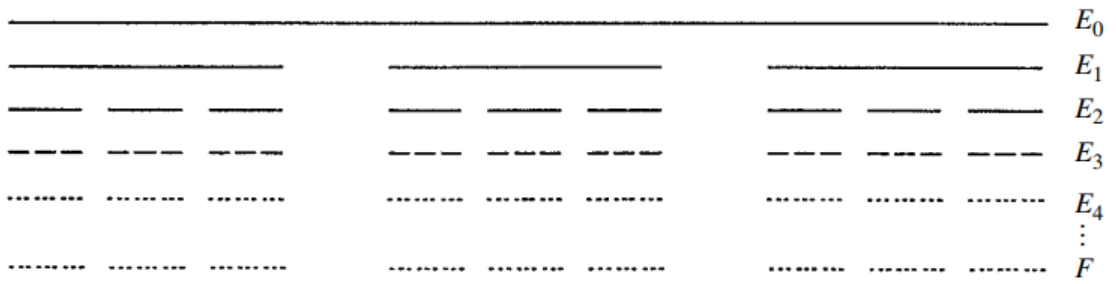


Figura 15 – Um conjunto de Cantor uniforme com $m = 3$ e $r = 4/15$, então $\dim_H F = \dim_B F = \log 3/ - \log 4/15 = 0,831...$ - Fonte: (FALCONER, 2014)

Demonstração. O conjunto F é obtido tomando m constante e $s = \log m/(-\log r)$ no Exemplo 12.2. A equação (12.4) torna-se $(r|I|)^s = (1/m)|I|^s$, que é satisfeita de forma idêntica, então $\dim_{\mathrm{H}} F = s$. Para a dimensão box, observe que F é coberto pelos m^k intervalos de nível k de comprimento r^{-k} para cada k, levando a $\overline{\dim}_B F \leq \log m/ - \log r$ da maneira usual. □

Exemplo 12.4. Suponha que na construção geral 12.3 cada intervalo de nível $k-1$ contém pelo menos $m_k \geqslant 2$ intervalos de k-ésimo nível $(k = 1, 2, \ldots)$ que são separados por lacunas de pelo menos ε_k, onde $0 < \varepsilon_{k+1} < \varepsilon_k$ para cada k. Então

$$\dim_{\mathrm{H}} F \geqslant \underline{\lim}_{k\to\infty} \frac{\log(m_1 \cdots m_{k-1})}{-\log(m_k \varepsilon_k)}. \tag{12.7}$$

Demonstração. Podemos assumir que o lado direito da equação acima é positivo, senão o resultado seria óbvio, pois a dimensão é sempre não-negativa. Suponha que cada intervalo de nível $(k-1)$ contém exatamente m_k intervalos de nível k; caso contrário, podemos descartar intervalos em excesso para obter conjuntos menores E_k e F para os quais isso acontece. Defina uma distribuição de massa μ em F atribuindo uma massa $(m_1 \ldots m_k)^{-1}$ a cada um dos $m_1 \ldots m_k$ intervalos de k-ésimo nível. Seja U um intervalo com $0 < |U| < \varepsilon_1$; vamos estimar $\mu(U)$. Seja k o número inteiro tal que $\varepsilon_k \leqslant |U| < \varepsilon_{k-1}$. O número de intervalos de k-ésimo nível que intersectam U é

(i) no máximo m_k já que U intersecta no máximo um intervalo de $(k-1)$-ésimo nível

(ii) no máximo $(|U|/\varepsilon_k) + 1 \leqslant 2|U|/\varepsilon_k$, uma vez que os intervalos do k-ésimo nível têm lacunas de pelo menos ε_k entre eles.

Cada intervalo de nível k aguenta uma massa de $(m_1 \cdots m_k)^{-1}$ de modo que

$$\begin{aligned}\mu(U) &\leqslant (m_1 \cdots m_k)^{-1} \min\{2|U|/\varepsilon_k, m_k\} \\ &\leqslant (m_1 \cdots m_k)^{-1} (2|U|/\varepsilon_k)^s m_k^{1-s}\end{aligned}$$

para cada $0 \leqslant s \leqslant 1$.

Daí

$$\frac{\mu(U)}{|U|^s} \leqslant \frac{2^s}{(m_1 \cdots m_{k-1}) m_k^s \varepsilon_k^s}.$$

Se

$$s < \underline{\lim}_{k\to\infty} \log(m_1 \cdots m_{k-1})/-\log(m_k\varepsilon_k)$$

então $(m_1 \cdots m_{k-1})m_k^s\varepsilon_k^s > 1$ para k grande o suficiente, portanto $\mu(U) \leqslant 2^s|U|^s$, e $\dim_{\mathrm{H}} F \geqslant s$ pelo princípio de distribuição de massa, resultando em (12.7). □

Agora suponha que no Exemplo 12.4 os intervalos de k-ésimo nível sejam todos de comprimento δ_k, e que cada intervalo de nível $(k-1)$ contenha exatamente m_k intervalos de k-ésimo nível que são "grosseiramente igualmente espaçados" no sentido de que $m_k\varepsilon_k \geqslant c\delta_{k-1}$, onde $c > 0$ é uma constante. Então (12.7) torna-se

$$\dim_{\mathrm{H}} F \geqslant \underline{\lim}_{k\to\infty} \frac{\log(m_1 \cdots m_{k-1})}{-\log c - \log \delta_{k-1}} = \underline{\lim}_{k\to\infty} \frac{\log(m_1 \cdots m_{k-1})}{-\log \delta_{k-1}}.$$

Mas E_{k-1} compreende $m_1 \cdots m_{k-1}$ intervalos de comprimento δ_{k-1}, então esta expressão é igual ao limite superior para $\dim_{\mathrm{H}} F$ dado pela Proposição 12.1. Assim, na situação em que os intervalos são bem espaçados, obtemos igualdade em (12.7).

Exemplo 12.5. Fixe $0 < s < 1$ e seja $n_0, n_1, n_2, \ldots$ uma sequência crescente de números inteiros, digamos $n_{k+1} \geqslant \max\{n_k^k, 4n_k^{1/s}\}$ para cada k. Para cada k, suponha que $H_k \subset \mathbb{R}$ consiste de intervalos igualmente espaçados de comprimentos $n_k^{-1/s}$ com os pontos médios de intervalos consecutivos a n_k^{-1} de distância. Então escrevendo $F = \bigcap_{k=1}^{\infty} H_k$, temos $\dim_{\mathrm{H}} F = s$.

Demonstração. Como $F \subset H_k$ para cada k, o conjunto $F \in [0,1]$ está contido em no máximo $n_k + 1$ intervalos de comprimento $n_k^{-1/s}$, então a Proposição 12.1 nos dá

$$\dim_{\mathrm{H}}(F \cap [0,1]) \leqslant \underline{\lim}_{k\to\infty} \log(n_k+1)/-\log n_k^{-1/s} = s.$$

Da mesma forma, $\dim_{\mathrm{H}}(F \cap [n, n+1]) \leqslant s$ para todo $n \in \mathbb{Z}$, então $\dim_{\mathrm{H}} F \leqslant s$ já que é união enumerável de tais conjuntos.

Agora seja $E_0 = [0,1]$ e, para $k \geqslant 1$, seja E_k consistindo nos intervalos de H_k que estão completamente contidos em E_{k-1}. Então cada intervalo I de E_{k-1} contém pelo menos $n_k|I| - 2 \geqslant n_k n_{k-1}^{-1/s} - 2 \geqslant 2$ intervalos de E_k, que são separados por intervalos de pelo menos $n_k^{-1} - n_k^{-1/s} \geqslant \frac{1}{2}n_k^{-1}$ se k for suficientemente grande. Usando o Exemplo 12.4 e observando que definindo $m_k = n_k n_{k-1}^{-1/s}$ ao invés de $m_k = n_k n_{k-1}^{-1/s} - 2$ não afeta o limite,

$$\begin{aligned}\dim_{\mathsf{H}}(F \cap [0,1]) \geqslant \dim_{\mathsf{H}} \bigcap_{k=1}^{\infty} E_k &\geqslant \varliminf_{k\to\infty} \frac{\log((n_1 \cdots n_{k-2})^{1-1/s} n_{k-1})}{-\log(n_k n_{k-1}^{-1/s} \frac{1}{2} n_k^{-1})} \\ &= \varliminf_{k\to\infty} \frac{\log(n_1 \cdots n_{k-2})^{1-1/s} + \log n_{k-1}}{\log 2 + (\log n_{k-1})/s}.\end{aligned}$$

Desde que n_k esteja aumentando rápido o suficiente, os termos em $\log n_{k-1}$ no numerador e denominador desta expressão são dominantes, de forma que $\dim_{\mathrm{H}} F \geqslant \dim_{\mathrm{H}}(F \cap [0,1]) \geqslant s$, como queríamos demonstrar. □

13 Sistema Iterado de Funções

Muitos fractais são compostos de partes que, de alguma forma, são semelhantes ao todo. Por exemplo, o conjunto de Cantor é a união de duas cópias semelhantes de si mesmo, e a curva de von Koch é composta por quatro cópias semelhantes. Essas autossimilaridades não são apenas propriedades dos fractais: elas podem realmente ser usadas para defini-los. Sistemas iterados de funções fazem isso de forma unificada e, além disso, frequentemente levam a uma maneira simples de encontrar dimensões.

Seja D um subconjunto fechado de $\mathbb{R}^n$, frequentemente temos $D = \mathbb{R}^n$. Uma função $S : D \to D$ é chamada de contração em D se existir um número c com $0 < c < 1$ tal que $|S(x) - S(y)| \leqslant c|x - y|$ para todos $x, y \in D$. Claramente, toda contração é contínua. Se a igualdade for satisfeita, ou seja, se $|S(x) - S(y)| = c|x - y|$, então S transforma conjuntos em conjuntos geometricamente semelhantes, e chamamos S de similaridade.

Uma família finita de contrações $S_1, S_2, \ldots, S_m$, com $m \geq 2$, é chamada de sistema iterado de funções ou SIF. Chamamos um subconjunto F de D que é compacto e não vazio de atrator (ou conjunto invariante) para o SIF se

$$F = \bigcup_{i=1}^{m} S_i\,(F)\,.$$

A propriedade fundamental de um sistema iterado de funções é que ele determina um atrator único, que normalmente é um fractal. Para um exemplo simples, tome F como o conjunto de Cantor. Sejam S_1 e $S_2 : \mathbb{R} \to \mathbb{R}$ dados por

$$S_1(x) = \frac{1}{3}x; \quad S_2(x) = \frac{1}{3}x + \frac{2}{3}.$$

Então, $S_1(F)$ e $S_2(F)$ são apenas as "metades" esquerda e direita de F, de modo que $F = S_1(F) \cup S_2(F)$; assim, F é um atrator do SIF composto pelas contrações S_1, S_2, as duas funções que representam as autossimilaridades básicas do conjunto de Cantor.

Vamos provar a propriedade fundamental de que um SIF possui um atrator único (não vazio, compacto). Isso significa, por exemplo, que o conjunto de Cantor é unicamente determinado como o atrator das funções S_1, S_2 dadas acima.

Para isso, definimos uma métrica ou distância d entre subconjuntos de D. Seja $\mathcal{S}$ a classe de todos os subconjuntos compactos não vazios de D. Lembre-se de que a δ-vizinhança de um conjunto A é o conjunto de pontos a uma distância δ de A, ou seja,

$$A_\delta = \{x \in D : |x - a| \leq \delta \text{ para algum } a \in A\}.$$

Transformamos $\mathcal{S}$ em um espaço métrico definindo a distância entre dois conjuntos A e B como o menor valor de δ tal que a δ-vizinhança de A contenha B e vice-versa:

$$d_H(A, B) = \inf\{\delta : A \subset B_\delta \text{ e } B \subset A_\delta\}$$

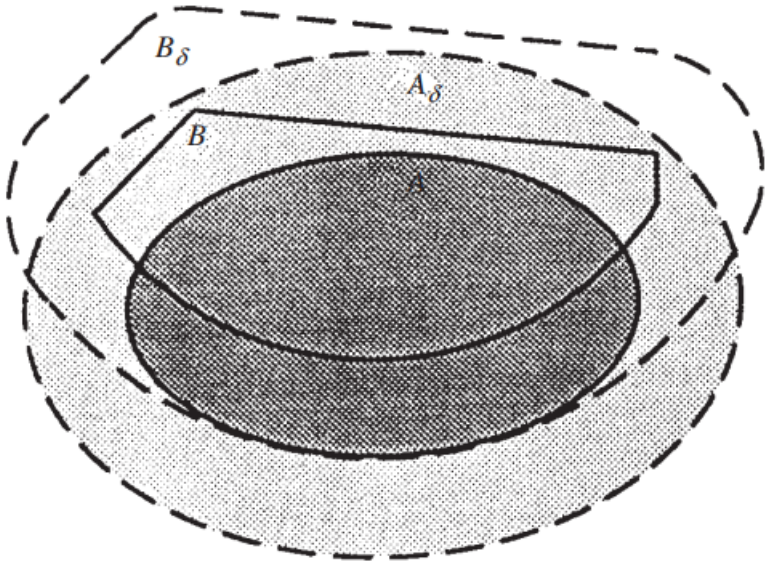


Figura 16 – Exemplo de coberturas para conjuntos A e B - Fonte: (FALCONER, 2014)

Afirmação. d_H, chamada de distância de Hausdorff, é uma métrica.

Demonstração. (i) $d_H(A,B) \geqslant 0$, pois δ é positivo. Se $d_H(A,B) = 0$, então $A \subset B$ e $B \subset A \iff A = B$, usando que A e B são compactos.

(ii) $d_H(A,B) = d_H(B,A)$ por definição.

(iii) Suponha $\delta > 0$ tal que $A \subset B_\delta$ e $B \subset A_\delta$ e $\varepsilon > 0$ tal que $B \subset C_\varepsilon$ e $C \subset B_\varepsilon$. Tome x qualquer em B_δ, por definição existe $b \in B$ tal que $d(x,b) < \delta$. Como $B \subset C_\varepsilon$, existe $c \in C$ tal que $d(b,c) < \varepsilon$.

Pela desigualdade triangular para a distância euclidiana temos

$$d(x,c) \leq d(x,b) + d(b,c) < \delta + \varepsilon.$$

Além disso, observe que tomamos x qualquer em B_δ, como $A \subset B_\delta$. Segue que a desigualdade vale para qualquer $a \in A$, isto é, $d(a,c) \leq d(a,b) + d(b,c) < \delta + \varepsilon$.

Isto implica que $A \subset C_{\delta+\varepsilon}$. Analogamente, podemos mostrar que $C \subset A_{\delta+\varepsilon}$, juntando ambos temos

$$\{\delta > 0; A \subset B_\delta \text{ e } B \subset A_\delta\} + \{\varepsilon > 0; C \subset B_\varepsilon \text{ e } B \subset C_\varepsilon\} \subset \{\delta > 0; A \subset C_\delta \textbf{ e } C \subset A_\delta\}.$$

Tomando ínfimos temos $d_H(A,B) + d_H(B,C) \geqslant d_H(A,C)$. □

Exemplo 13.1. $d_H([0,1/3],[2/3,1]) = 2/3$, pois a maior distância entre ambos os intervalos é $2/3 - 0 = 2/3 = 1 - 1/3$.

Teorema 13.1. Considere o sistema iterado de funções dado pelas contrações $\{S_1, \ldots, S_m\}$ em $D \subset \mathbb{R}^n$ em que

$$|S_i(x) - S_i(y)| \leqslant c_i|x - y| \quad (x,y) \in D \tag{13.1}$$

com $0 < c_i < 1$ para cada i. Então existe um atrator único F, isto é, um conjunto compacto não vazio tal que

$$F = \bigcup_{i=1}^{m} S_i(F). \tag{13.2}$$

Além disso, se definirmos uma transformação S na classe $\mathcal{S}$ de conjuntos compactos não vazios por

$$S(E) = \bigcup_{i=1}^{m} S_i(E) \tag{13.3}$$

para $E \in \mathcal{S}$, e escreva S^k para a k-ésima iteração de S ($S^0(E) = E$ e $S^k(E) = S(S^{k-1}(E))$ para $k \geqslant 1$), então

$$F = \bigcap_{k=0}^{\infty} S^k(E) \tag{13.4}$$

para cada conjunto $E \in \mathcal{S}$ tal que $S_i(E) \subset E$ para todo i.

Demonstração. Seja E qualquer conjunto em $\mathcal{S}$ tal que $S_i(E) \subset E$ para todo i; por exemplo $E = D \cap B(0, r)$ servirá desde que r seja suficientemente grande. Então $S^k(E) \subset S^{k-1}(E)$, de modo que $S^k(E)$ é uma sequência decrescente de conjuntos compactos não vazios, cuja interseção $F = \bigcap_{k=1}^{\infty} S^k(E)$ é não vazia pelo Teorema dos intervalos encaixados (disponível em (LIMA, 2013). Como $S^k(E)$ é uma sequência decrescente de conjuntos, segue que

$$S(F) = S\left(\bigcap_{k=0}^{\infty} S^k(E)\right) = \bigcap_{k=0}^{\infty} S(S^k(E)) = \bigcap_{k=1}^{\infty} S^k(E) = F$$

onde usamos a compacidade de E. Disso ganhamos que F satisfaz 13.2 e é um atrator do SIF. Observe que os conjuntos em $\mathcal{S}$ são transformados por S em outros conjuntos de $\mathcal{S}$ pois imagem de um conjunto compacto por uma função contínua é compacta. Se $A, B \in \mathcal{S}$ então

$$d_H(S(A), S(B)) = d_H\left(\bigcup_{i=1}^{m} S_i(A), \bigcup_{i=1}^{m} S_i(B)\right) \leqslant \max_{1 \leqslant i \leqslant m} d_H(S_i(A), S_i(B))$$

usando a definição da métrica d_H e observando que se a δ-vizinhança $(S_i(A))_\delta$ contém $S_i(B)$ para todo i então $(\bigcup_{i=1}^{m} S_i(A))_\delta$ contém $\bigcup_{i=1}^{m} S_i(B)$ e vice-versa. Por 13.1,

$$d_H(S(A), S(B)) \leqslant (\max_{1 \leqslant i \leqslant m} c_i) d_H(A, B). \tag{13.5}$$

Suponha que A e B sejam ambos atratores, de modo que $S(A) = A$ e $S(B) = B$. Como $0 < \max c_i < 1$ segue de 13.5 que $d(A, B) = 0$, implicando $A = B$. □

Segundo (FALCONER, 1985), a primeira apresentação sistemática do que conhecemos dos SIFs deriva de Hutchinson. De fato, o seguinte teorema, que apenas enunciaremos, hoje recebe o seu nome e é muito parecido com o que fizemos. A demonstração pode ser consultada em (HUTCHINSON, 1981).

Teorema 13.2 (Teorema de Hutchinson)**.** Seja $X = (X, d)$ um espaço métrico completo e $\mathcal{S} = \{S_1, \ldots, S_N\}$ um conjunto finito de contrações em X. Então existe um conjunto fechado e limitado único K tal que $K = \bigcup_{i=1}^{N} S_i K$. Além disso, K é compacto e é o fecho do conjunto de pontos fixos $s_{\{i_1 \ldots i_p\}}$ das composições finitas $S_{i_1} \circ \cdots \circ S_{i_p}$ dos membros de $\mathcal{S}$. Para um conjunto arbitrário $A \subset X$, defina $\mathcal{S}(A) = \bigcup_{i=1}^{N} S_i A$, $\mathcal{S}^p(A) = \mathcal{S}(\mathcal{S}^{p-1}(A)$. Então, para A fechado e limitado, $\mathcal{S}^p(A) \to K$ na métrica de Hausdorff.

13.1 DIMENSÃO DE CONJUNTOS AUTOSSIMILARES

Uma das vantagens da representação por um SIF é que a dimensão do atrator é muitas vezes relativamente fácil de calcular ou estimar em termos das contrações definidas. Nesta seção, discutimos o caso em que $S_1, \ldots, S_m : \mathbb{R}^n \to \mathbb{R}^n$ são *similaridades* ou seja, com

$$|S_i(x) - S_i(y)| = r_i|x - y| \quad (x, y \in \mathbb{R}^n), \tag{13.6}$$

onde $0 < r_i < 1$ (r_i é chamado de proporção de S_i). Assim, cada S_i transforma subconjuntos de $\mathbb{R}^n$ em conjuntos geometricamente semelhantes. O atrator de tal conjunto de similaridades é chamado de conjunto autossimilar, sendo uma união de um número de cópias semelhantes menores de si mesmo. Exemplos padrão incluem o conjunto de Cantor do terço médio, o triângulo de Sierpinski e a curva de von Koch.

Mostraremos que, sob condições bastante gerais, um conjunto autossimilar F tem dimensões de Hausdorff e box dadas por sua dimensão de similaridade, ou seja, o número s que satisfaz

$$\sum_{i=1}^{m} r_i^s = 1, \tag{13.7}$$

e ainda que F tem medida $\mathcal{H}^s$ positiva e finita. Um cálculo heurístico indica que o valor dado acima é pelo menos plausível. Se $F = \bigcup_{i=1}^{m} S_i(F)$ tem a união "quase disjunta", temos que

$$\mathcal{H}^s(F) = \sum_{i=1}^{m} \mathcal{H}^s(S_i(F)) = \sum_{i=1}^{m} r_i^s \mathcal{H}^s(F) \tag{13.8}$$

usando 13.6 e a propriedade de escala 10.5. Supondo que $0 < \mathcal{H}^s(F) < \infty$ no valor de "salto" $s = \dim_{\mathrm{H}} F$, podemos cancelar o $\mathcal{H}^s(F)$ para obter que s satisfaz 13.7.

Para que este argumento dê a resposta correta, precisamos de uma condição que garanta que os componentes $S_i(F)$ de F não se sobreponham "muito". Dizemos que os S_i satisfazem a *condição de conjunto aberto* se existe um aberto V não vazio limitado tal que

$$V \supset \bigcup_{i=1}^{m} S_i(V) \tag{13.9}$$

e esta união é disjunta.

Lema 13.1. Seja $\{V_i\}$ uma coleção de subconjuntos abertos disjuntos de $\mathbb{R}^n$ tais que cada V_i contém uma bola de raio $a_1 r$ e está contido em uma bola de raio $a_2 r$. Então qualquer bola B de raio r intersecta no máximo $(1 + 2a_2)^n a_1^{-n}$ dos fechados $\overline{V}_i$.

Demonstração. Se $\overline{V}_i$ encontra B, então V_i está contido na bola concêntrica com B de raio $(1+2a_2)r$. Suponha que q dos conjuntos $\overline{V}_i$ cortem B. Somando os volumes das bolas interiores correspondentes de raios $a_1 r$, segue que $q(a_1 r)^n \leqslant (1+2a_2)^n r^n$ como queríamos. □

A demonstração do próximo teorema é devido a (FALCONER, 2014). É útil pensar no Conjunto de Cantor para entendê-la.

Teorema 13.3. Suponha que a condição de conjunto aberto 13.9 seja válida para as contrações S_i em $\mathbb{R}^n$ com proporções $0 < r_i < 1$ para $1 \leqslant i \leqslant m$. Se F é o atrator do SIF $\{S_1, \ldots, S_m\}$, isto é,

$$F = \bigcup_{i=1}^{m} S_i(F), \tag{13.10}$$

então $\dim_{\mathrm{H}} F = \dim_B F = s$, onde s é dado por

$$\sum_{i=1}^{m} r_i^s = 1. \tag{13.11}$$

Além disso, para este valor de s, $0 < \mathcal{H}^s(F) < \infty$.

Demonstração. Suponha s satisfazendo (13.11). Seja $\mathcal{I}_k$ o conjunto de todas as sequências com k termos $(i_1, \ldots, i_k)$ com $1 \leqslant i_j \leqslant m$. Para qualquer conjunto A e $(i_1, \ldots, i_k) \in I_k$, escrevemos $A_{i_1,\ldots,i_k} = S_{i_1} \circ \cdots \circ S_{i_k}(A)$. Segue-se, usando (13.10) repetidamente, que

$$F = \bigcup_{\mathcal{I}_k} F_{i_1,\ldots,i_k}.$$

Vamos verificar que estas coberturas de F fornecem uma estimativa superior adequada para a medida de Hausdorff. Como o mapa $S_{i_1} \circ \cdots \circ S_{i_k}$ é uma similaridade de razão $r_{i_1} \cdots r_{i_k}$,

$$\sum_{I_k} |F_{i_1,\ldots,i_k}|^s = \sum_{I_k} (r_{i_1} \cdots r_{i_k})^s |F|^s = \left(\sum_{i_1} r_{i_1}^s \right) \cdots \left(\sum_{i_k} r_{i_k}^s \right) |F|^s = |F|^s \tag{13.12}$$

por (13.11). Para cada $\delta > 0$, podemos escolher k tal que $|F_{i_1,\ldots,i_k}| \leqslant (\max_i r_i)^k |F| \leqslant \delta$, então $\mathcal{H}^s_\delta(F) \leqslant |F|^s$ e, portanto, $\mathcal{H}^s(F) \leqslant |F|^s$ e $\dim_{\mathrm{H}} F \leqslant s$.

Agora vamos encontrar o limite inferior. Seja I o conjunto de todas as sequências infinitas $\mathcal{I} = \{(i_1, i_2, \ldots) : 1 \leqslant i_j \leqslant m\}$, e seja $I_{i_1,\ldots,i_k} = \{(i_1, \ldots, i_k, q_{k+1}, \ldots) : 1 \leqslant q_j \leqslant m\}$ o "cilindro"que consiste nessas sequências em $\mathcal{I}$ com termos iniciais $(i_1, \ldots, i_k)$. Podemos colocar uma distribuição de massa μ em $\mathcal{I}$ tal que $\mu(I_{i_1,\ldots,i_k}) = (r_{i_1} \cdots r_{i_k})^s$. Como $(r_{i_1} \cdots r_{i_k})^s = \sum_{i=1}^m (r_{i_1} \cdots r_{i_k} r_i)^s$, isto é, $\mu(I_{i_1,\ldots,i_k}) = \sum_{i=1}^m \mu(I_{i_1,\ldots,i_k,i})$, segue que μ é de fato uma distribuição de massa em subconjuntos de $\mathcal{I}$ com $\mu(\mathcal{I}) = 1$. Podemos estender μ para uma distribuição de massa $\tilde{\mu}$ em F de maneira natural definindo $\tilde{\mu}(A) = \mu\{(i_1, i_2, \ldots) : x_{i_1,i_2,\ldots} \in A\}$ para subconjuntos A de F. (Lembre-se de que $x_{i_1,i_2,\ldots} = \bigcap_{k=1}^{\infty} F_{i_1,\ldots,i_k}$.) Assim, a $\tilde{\mu}$-massa de um conjunto é a μ-massa das sequências correspondentes. É facilmente verificado que $\tilde{\mu}(F) = 1$.

Vamos mostrar que $\tilde{\mu}$ satisfaz as condições da Proposição 12.2. Seja V um conjunto aberto satisfazendo (13.9). Como $\overline{V} \supset S(\overline{V}) = \bigcup_{i=1}^m S_i(V)$, a sequência decrescente de iterações

$S^k(\overline{V})$ converge para F (veja (13.4)). Em particular, $\overline{V} \supset F$ e $\overline{V}_{i_1,\dots,i_k} \supset F_{i_1,\dots,i_k}$ para cada sequência finita $(i_1,\dots,i_k)$. Seja B qualquer bola de raio $r < 1$. Estimamos $\tilde{\mu}(B)$ considerando os conjuntos $V_{i_1,\dots,i_k}$ com diâmetros comparáveis ao de B e com fechos que intersectam $F \cap B$.

Restringimos cada sequência infinita $(i_1, i_2, \dots) \in \mathcal{I}$ após o primeiro termo i_k para o qual

$$\left(\min_{1\leqslant i\leqslant m} r_i\right) r \leqslant r_{i_1} r_{i_2} \cdots r_{i_k} \leqslant r \tag{13.13}$$

e denote por $\mathcal{Q}$ o conjunto finito de todas as sequências (finitas) obtidas desta forma. Então, para cada sequência infinita $(i_1, i_2, \dots) \in \mathcal{I}$, há exatamente um valor de k com $(i_1,\dots,i_k) \in \mathcal{Q}$. Como $V_1,\dots,V_m$ são disjuntos, então $V_{i_1,\dots,i_k,1},\dots,V_{i_1,\dots,i_k,m}$ também são disjuntos para cada $(i_1,\dots,i_k)$. Usando isso de maneira aninhada, segue-se que a coleção de conjuntos abertos $\{V_{i_1,\dots,i_k} : (i_1,\dots,i_k) \in \mathcal{Q}\}$ é disjunta. Além disso, $F \subset \bigcup_Q F_{i_1,\dots,i_k} \subset \bigcup_Q \overline{V}_{i_1,\dots,i_k}$.

Escolhemos a_1 e a_2 para que V contenha uma bola de raio a_1 e esteja contido em uma bola de raio a_2. Então, para todo $(i_1,\dots,i_k) \in \mathcal{Q}$, o conjunto $V_{i_1,\dots,i_k}$ contém uma bola de raio $r_{i_1}\cdots r_{i_k}a_1$ e, portanto, uma de raio $(\min_i r_i)a_1 r$ e está contida em uma bola de raio $r_{i_1}\cdots r_{i_k}a_2$ e, portanto, em uma bola de raio $a_2 r$. Sejam $\mathcal{Q}_1$ as sequências $(i_1,\dots,i_k)$ em $\mathcal{Q}$ tais que B intercepta $\overline{V}_{i_1,\dots,i_k}$. Pelo Lema 13.1, existem no máximo $q = (1+2a_2)^n a_1^{-n}(\min_i r_i)^{-n}$ sequências em $\mathcal{Q}_1$. Então

$$\tilde{\mu}(B) = \tilde{\mu}(F\cap B) = \mu\{(i_1,i_2,\dots) : x_{i_1,i_2,\dots} \in F\cap B\} \leqslant \mu\left\{\bigcup_{Q_1} I_{j_1,\dots,j_k}\right\}$$

já que $x_{i_1,i_2,\dots} \in F\cap B \subset \bigcup_{\mathcal{Q}_1} \overline{V}_{j_1,\dots,j_k}$, existe um inteiro k tal que $(i_1,\dots,i_k) \in \mathcal{Q}_1$. Assim,

$$\tilde{\mu}(B) \leqslant \sum_{\mathcal{Q}_1} \mu(I_{i_1,\dots,i_k}) = \sum_{alQ_1} (r_{i_1}\cdots r_{i_k})^s \leqslant \sum_{\mathcal{Q}_1} r^s \leqslant r^s q$$

usando (13.13). Como qualquer conjunto U está contido em uma bola de raio $|U|$, temos $\tilde{\mu}(U) \leqslant |U|^s q$, então o princípio de distribuição de massa nos dá que $\mathcal{H}^s(F) \geqslant q^{-1} > 0$ e $\dim_{\mathrm{H}} F \geqslant s$.

Finalmente, para dimensão box, dado $r < 1$, escolha $\mathcal{Q}$ como em (13.13). Segue indutivamente de (13.11) que $\sum_{\mathcal{Q}} (r_{i_1} r_{i_2}\cdots r_{i_k})^s = 1$, então Q contém no máximo $(\min_i r_i)^{-s} r^{-s}$ sequências. Para cada $(i_1,\dots,i_k) \in \mathcal{Q}$, temos $|\overline{V}_{i_1,\dots,i_k}| = r_{i_1}\cdots r_{i_k}|\overline{V}| \leqslant r|\overline{V}|$, então $\bigcup_{\mathcal{Q}} \overline{V}_{i_1,\dots,i_k}$ é uma cobertura de F por no máximo $(\min_i r_i)^{-s} r^{-s}$ conjuntos de diâmetro $r|\overline{V}|$. Segue-se da primeira definição equivalente de dimensão box que $\overline{\dim_B} F \leqslant s$. Observando as relações padrão $\dim_{\mathrm{H}} F \leqslant \underline{\dim}_{\mathrm{B}} F \leqslant \overline{\dim}_{\mathrm{B}} F$, completamos a prova. □

Exemplo 13.2 (Triângulo de Sierpinski)**.** O triângulo de Sierpinski F é construído a partir de um triângulo equilátero removendo repetidamente triângulos equiláteros invertidos. Então $\dim_{\mathrm{H}} F = \dim_B F = \log 3/\log 2$.

Demonstração. O conjunto F é o atrator das três contrações óbvias de proporções $\frac{1}{2}$, que mapeiam o triângulo E_0 nos triângulos de E_1. A condição de conjunto aberto é válida quando tomamos V como o interior de E_0. Assim, pelo Teorema 13.3, $\dim_{\mathrm{H}} F = \dim_{\mathrm{B}} F = \log 3/\log 2$, que é a solução de $3(\frac{1}{2})^s = \sum_1^3 \left(\frac{1}{2}\right)^s = 1$. □

13.2 VARIAÇÕES

Os cálculos subjacentes ao Teorema anterior podem ser adaptados para estimar a dimensão do atrator F de um SIF consistindo de contrações que não são similaridades.

Exemplo 13.3.

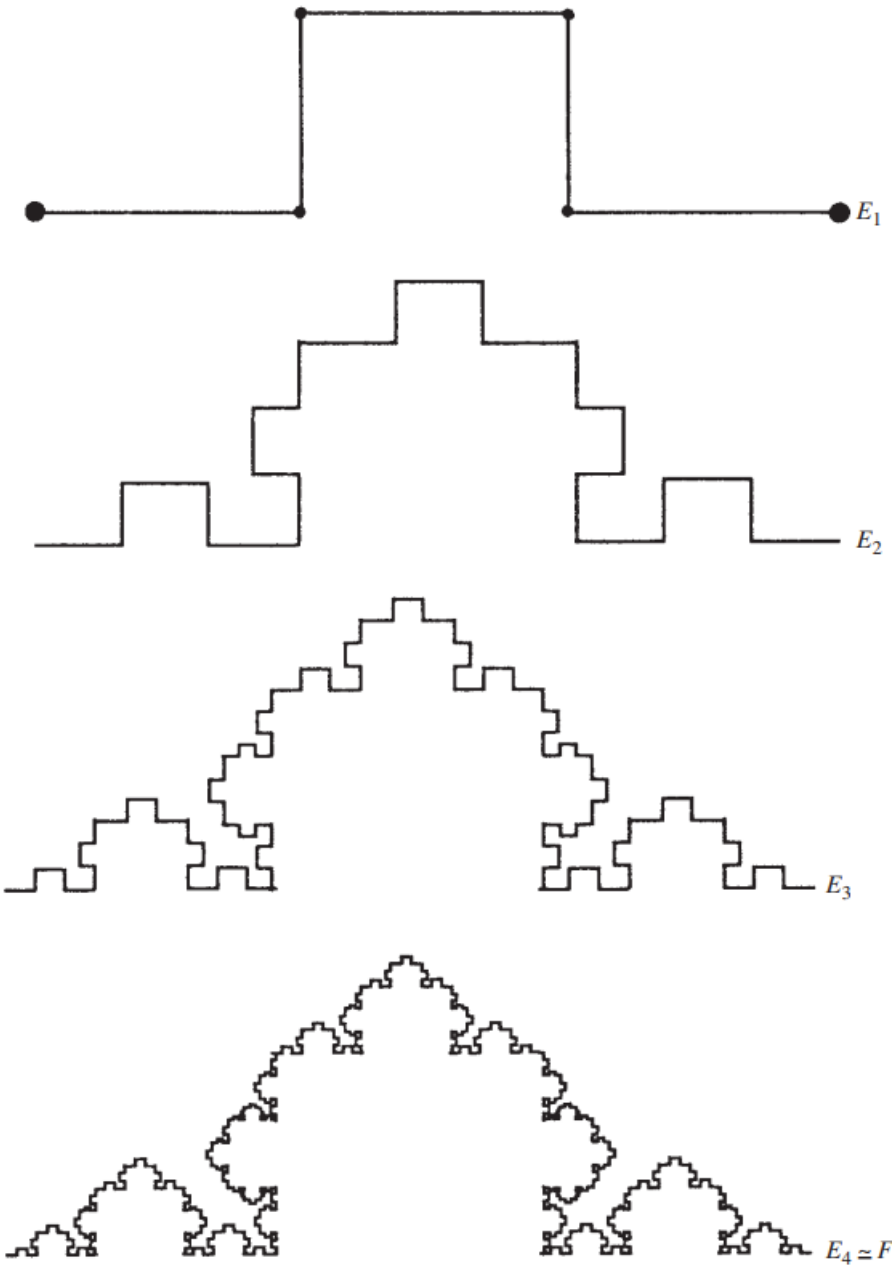


Figura 17 – Estágios na construção de uma curva fractal de um gerador (E_1). Os comprimentos dos segmentos do gerador são $1/3, 1/4, 1/3, 1/4, 1/3$, e as dimensões de Hausdorff e box de F são dadas por $3(1/3)^s + 2(1/4)^s = 1$ ou $s = 1,34...$ - Fonte: (FALCONER, 2014)

Proposição 13.1. Seja F o atrator de um SIF que consiste nas contrações $\{S_1, \ldots, S_m\}$ em um subconjunto fechado D de $\mathbb{R}^n$ tal que

$$|S_i(x) - S_i(y)| \leqslant r_i|x - y| \quad (x, y \in D)$$

com $0 < r_i < 1$ *para cada* i. Então $\dim_{\mathrm{H}} F \leqslant s$ e $\overline{\dim}_B F \leqslant s$, onde $\sum_{i=1}^{m} r_i^s = 1$.

Demonstração. Estas estimativas são essencialmente aquelas do primeiro e último parágrafos da prova do teorema anterior, observando que temos a desigualdade $|A_{i_1,\ldots,i_k}| \leqslant r_{i_1} \cdots r_{i_k}|A|$ para cada conjunto A, em vez de igualdade. □

Exemplo 13.4. Observe

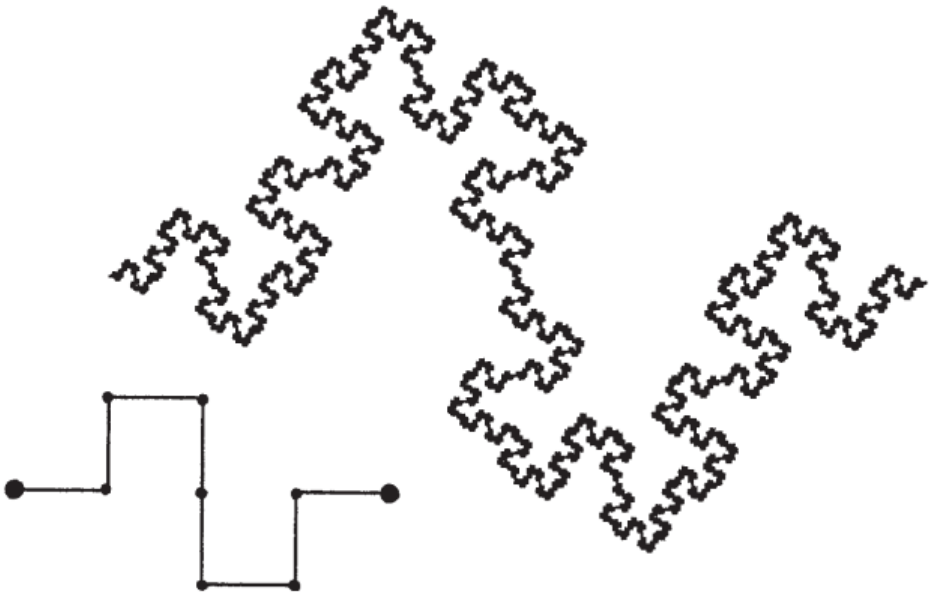


Figura 18 – Uma curva fractal e seu gerador. As dimensões de Hausdorff e box são iguais a $\log 8/\log 4 = \log 2^3/\log 2^2 = 3/2$ - Fonte: (FALCONER, 2014)

Exemplo 13.5. Observe

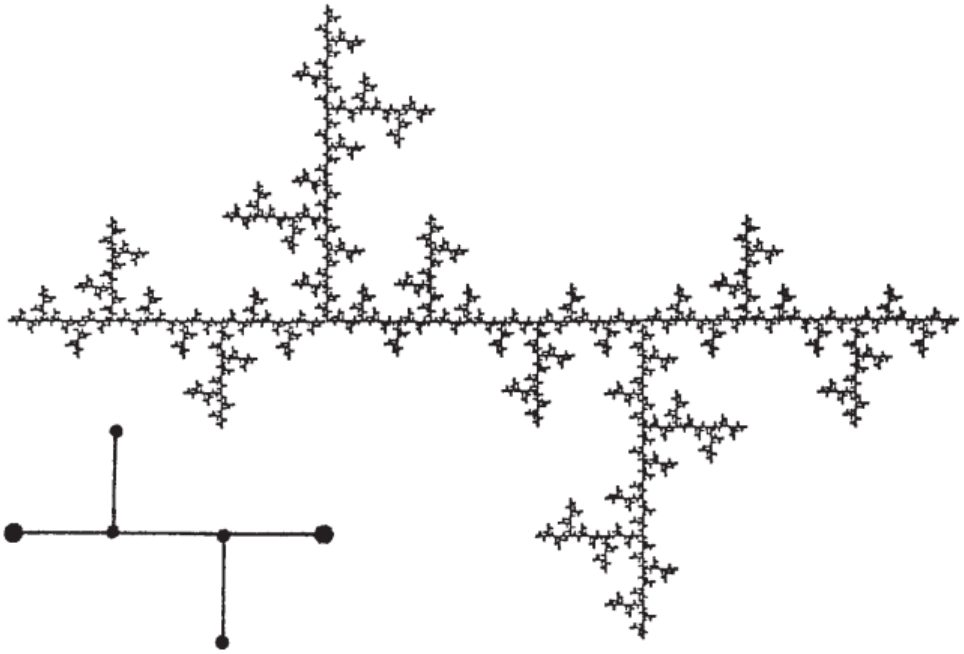


Figura 19 – Uma curva fractal e seu gerador. As dimensões de Hausdorff e box são iguais a $\log 5/\log 3 = 1,465...$ - Fonte: (FALCONER, 2014)

A seguir, obtemos um limite inferior para a dimensão no caso em que os componentes $S_i(F)$ de F são disjuntos. Observe que este certamente será o caso se houver $algum$ conjunto compacto não vazio E com $S_i(E) \subset E$ para todo i e com o $S_i(E)$ disjunto.

Proposição 13.2. Considere o SIF que consiste nas contrações $\{S_1, \ldots, S_m\}$ em um subconjunto fechado D do $\mathbb{R}^n$ tal que

$$b_i|x-y| \leqslant |S_i(x) - S_i(y)| \ (x, y \in D) \tag{13.14}$$

com $0 < b_i < 1$ para cada i. Suponha que o atrator F (compacto não vazio) satisfaz

$$F = \bigcup_{i=1}^{m} S_i(F), \tag{13.15}$$

com esta união disjunta. Então F é totalmente desconexo e $\dim_{\mathrm{H}} F \geqslant s$ onde

$$\sum_{i=1}^{m} b_i^s = 1. \tag{13.16}$$

Demonstração. Seja $d > 0$ a distância mínima entre qualquer par dos conjuntos compactos e disjuntos $S_1(F), \ldots, S_m(F)$, ou seja, $d = \min_{i \neq j} \inf\{|x-y| : x \in S_i(F), y \in S_j(F)\}$. Seja $F_{i_1,\ldots,i_k} = S_{i_1} \circ \cdots \circ S_{i_k}(F)$ e defina μ por $\mu(F_{i_1,\ldots i_k}) = (b_{i_1} \cdots b_{i_k})^s$. Como

$$\begin{aligned}\sum_{i=1}^{m} \mu(F_{i_1,\ldots,i_k,i}) &= \sum_{i=1}^{m} (b_{i_1} \cdots b_{i_k} b_i)^s = (b_{i_1} \cdots b_{i_k})^s \\ &= \mu(F_{i_1,\ldots,i_k})\end{aligned}$$

segue que μ define uma distribuição de massa em F com $\mu(F) = 1$.

Se $x \in F$, existe uma sequência infinita única $i_1, i_2, \ldots$ tal que $x \in F_{i_1,\ldots,i_k}$ para cada k. Para $0 < r < d$, seja k o menor número inteiro tal que

$$b_{i_1} \cdots b_{i_k} d \leqslant r < b_{i_1} \cdots b_{i_{k-1}} d.$$

Se $i'_1, \ldots, i'_k$ são diferentes de $i_1, \ldots, i_k$, os conjuntos $F_{i_1,\ldots,i_k}$ e $F_{i'_1,\ldots,i'_k}$ são disjuntos e separados por um gap de pelo menos $b_{i_1} \cdots b_{i_{k-1}} d > r$. (Para ver isso, observe que se j for o menor inteiro de forma que $i_j \neq i'_j$, então $F_{i_j,\ldots,i_k} \subset F_{i_j}$ e $F_{i'_j,\ldots,i'_k} \subset F_{i'_j}$ estão separados por d, então $F_{i_1,\ldots,i_k}$ e $F_{i'_1,\ldots,i'_k}$ estão separados por pelo menos $b_{i_1} \ldots b_{i_{j-1}} d$.) Segue-se que $F \cap B(x, r) \subset F_{i_1,\ldots,i_k}$ então

$$\mu(F \cap B(x, r)) \leqslant \mu(F_{i_1,\ldots,i_k}) = (b_{i_1} \ldots b_{i_k})^s \leqslant d^{-s} r^s.$$

Se U intersecta F, então $U \subset B(x, r)$ para algum $x \in F$ com $r = |U|$. Assim, $\mu(U) \leqslant d^{-s}|U|^s$, então pela Proposição 12.2, $\mathcal{H}^s(F) > 0$ e $\dim_H F \geqslant s$.

A separação dos componentes $F_{i_1,\ldots,i_k}$ indicada acima implica que F é totalmente desconexo. □

Exemplo 13.6. (Conjunto de Cantor "não linear"). Seja $D = \left[\frac{1}{2}\left(1 + \sqrt{3}\right), \left(1 + \sqrt{3}\right)\right]$ e seja S_1, $S_2 : D \to D$ dado por $S_1(x) = 1 + 1/x, S_2(x) = 2 + 1/x$. Então $0,44 < \dim_{\mathrm{H}} F \leqslant \underline{\dim}_{\mathrm{B}} F \leqslant \overline{\dim}_{\mathrm{B}} F < 0,66$ onde F é o atrator de $\{S_1, S_2\}$.

Demonstração. Primeiro note que

$$\begin{aligned} S_1(\tfrac{1}{2}(1+\sqrt{3})) &= 1 + \frac{2}{1+\sqrt{3}} \\ &= 1 + \frac{2}{1+\sqrt{3}} \frac{\sqrt{3}-1}{\sqrt{3}-1} \\ &= 1 + \sqrt{3} - 1 = \sqrt{3} \end{aligned} \qquad \begin{aligned} S_1(1+\sqrt{3}) &= 1 + \frac{1}{1+\sqrt{3}} \\ &= 1 + \frac{\sqrt{3}-1}{2} \\ &= \frac{1}{2}(1+\sqrt{3}). \end{aligned}$$

e

$$\begin{aligned} S_2(\tfrac{1}{2}(1+\sqrt{3})) &= 2 + \frac{2}{1+\sqrt{3}} \\ &= 2 + \frac{2}{1+\sqrt{3}} \frac{\sqrt{3}-1}{\sqrt{3}-1} \\ &= 2 + \sqrt{3} - 1 = \sqrt{3} + 1 \end{aligned} \qquad \begin{aligned} S_2(1+\sqrt{3}) &= 2 + \frac{1}{1+\sqrt{3}} \\ &= 2 + \frac{\sqrt{3}-1}{2} \\ &= \frac{1}{2}(3+\sqrt{3}). \end{aligned}$$

Logo $S_1(D) = \left[\frac{1}{2}\left(1 + \sqrt{3}\right),\ \sqrt{3}\right]$ e $S_2(D) = [\frac{1}{2}\left(3 + \sqrt{3}\right), 1 + \sqrt{3}]$. Observe que todo $x, y \in D$ é maior que 1, logo $|S_i(x) - S_i(y)| = |\frac{1}{x} - \frac{1}{y}| = |y - x|\frac{1}{|xy|} < k|y - x|$, com $1/xy < k < 1$. Segue que S_1 e S_2 são contrações e podemos usar as Proposições 13.1 e 13.2 para estimar $\dim_{\mathrm{H}} F$. Pelo Teorema do Valor Médio, se $x, y \in D$ são pontos distintos, então $(S_i(x) - S_i(y))/(x - y) = S'_i(z_i)$ para algum $z_i \in (x, y)$. Assim, para $i = 1, 2$

$$\inf_{x \in D} |S'_i(x)| \leqslant \frac{|S_i(x) - S_i(y)|}{|x - y|} \leqslant \sup_{x \in D} |S'_i(x)|.$$

Como $S_1'(x) = S_2'(x) = -1/x^2$ é fácil ver que S_i' é contínua, e toda função contínua definida num compacto assume um valor máximo e mínimo. Observe que $|S_i'|$ é decrescente neste domínio, e temos

$$\frac{1}{2}\left(2-\sqrt{3}\right) = \left(1+\sqrt{3}\right)^{-2} \leqslant \frac{|S_i(x)-S_i(y)|}{|x-y|} \leqslant \left(\frac{1}{2}\left(1+\sqrt{3}\right)\right)^{-2} = 2\left(2-\sqrt{3}\right)$$

para $i = 1$ e $i = 2$. De acordo com as proposições anteriores, os limites inferior e superior para as dimensões são dados pelas soluções de $2\big(\frac{1}{2}\big(2-\sqrt{3}\big)\big)^s = 1$ e $2(2(2-\sqrt{3}))^s = 1$ que resolvendo computacionalmente encontramos $s = \log 2/\log\big(2\big(2+\sqrt{3}\big)\big) = 0,34$ e $\log 2/\log\big(\frac{1}{2}\big(2+\sqrt{3}\big)\big) = 1,11$, respectivamente.

Para um subconjunto da reta real, um limite superior maior que l ainda não é bom. Uma maneira de obter melhores estimativas é observar que F também é o atrator dos quatro mapas em $[0,1]$

$$S_i \circ S_j = i + \frac{1}{j+1/x} = i + \frac{x}{jx+1} \quad (i,j=1,2).$$

Expandindo para visualizar melhor, temos

$$\begin{aligned} S_1 \circ S_2 &= 1 + \frac{x}{2x+1} & S_1 \circ S_1 &= 1 + \frac{x}{x+1} \\ S_2 \circ S_1 &= 2 + \frac{x}{x+1} & S_2 \circ S_2 &= 2 + \frac{x}{2x+1} \end{aligned}$$

Calculando derivadas e usando o Teorema do Valor Médio como antes, obtemos que

$$(S_i \circ S_j)'(x) = \frac{x'(jx+1) - xj}{(jx+1)^2} = \frac{1}{(jx+1)^2} = (jx+1)^{-2}$$

então

$$\left(j\left(1+\sqrt{3}\right)+1\right)^{-2}|x-y| \leqslant |S_i \circ S_j(x) - S_i \circ S_j(y)| \leqslant \left(\frac{1}{2}j\left(1+\sqrt{3}\right)+1\right)^{-2}|x-y|.$$

Os limites inferior e superior das dimensões são dados pelas soluções de

$$\begin{aligned} &2\left(\frac{1}{2}\left(3+\sqrt{3}\right)\right)^{-2s} && +2\left(2+\sqrt{3}\right)^{-2s} = 1 && (j=1) \\ &2\left(2+\sqrt{3}\right)^{-2s} && +2\left(3+2\sqrt{3}\right)^{-2s} = 1 && (j=2) \end{aligned}$$

usando uma calculadora achamos $0,44 < dim_H F < 0,66$, uma melhoria considerável em relação às estimativas anteriores. Na verdade, segundo (FALCONER, 2014), $\dim_{\mathrm{H}} F = 0.531$, um valor que pode ser obtido computacionalmente observando iterações de ordem ainda mais alta do S_i. □

14 Aplicações em Teoria dos Números

14.1 FRAÇÕES CONTÍNUAS

Qualquer número x que não é um inteiro pode ser escrito como

$$x = a_0 + \frac{1}{x_1}$$

onde a_0 é um inteiro e $x_1 > 1$. Analogamente, se x_1 não é inteiro, então

$$x_1 = a_1 + \frac{1}{x_2}$$

com $x_2 > 1$, daí

$$x = a_0 + \frac{1}{a_1 + \dfrac{1}{x_2}}.$$

Procedendo da mesma forma, suponha que x_j, $1 \leqslant j \leqslant n-1$ não são inteiros, e x_n é inteiro, teremos, então

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

Esta expressão é chamada **fração contínua** e os números $a_0, a_1, \ldots$ são chamados de **quocientes parciais** de x.

Exemplo 14.1.

$$\begin{aligned}
\sqrt{2} = 1 + (\sqrt{2} - 1) &= 1 + \cfrac{1}{\cfrac{1}{\sqrt{2}-1}} \\
&= 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{2 + \sqrt{2} - 1} \\
&= 1 + \cfrac{1}{2 + \cfrac{1}{\cfrac{1}{\sqrt{2}-1}}} = 1 + \cfrac{1}{2 + \cfrac{1}{\sqrt{2}+1}} \\
&= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \ldots}}} = [1; 2, 2, 2, \ldots]
\end{aligned}$$

Teorema 14.1. x é racional se, e somente se, sua representação por frações contínuas é finita.

Demonstração. ($\Leftarrow$) Suponha $x = [a_0; a_1, \ldots, a_n]$, podemos somar $a_{n-1} + 1/a_n = c_n$, e em seguida somar $a_{n-2} + 1/c_n$ e assim por diante. Como há uma quantidade finita este processo acaba em dado momento, e chegaremos a um número racional.

($\Rightarrow$) Reciprocamente, se $x \in \mathbb{Q}$, seus coeficientes vêm do algoritmo de Euclides: se $x = p/q$ temos

$$\begin{aligned} p &= a_0 q + r_1 & 0 &\leqslant r_1 < q \\ q &= a_1 r_1 + r_2 & 0 &\leqslant r_2 < r_1 \\ r_1 &= a_2 r_2 + r_3 & 0 &\leqslant r_3 < r_2 \\ &\vdots & &\vdots \\ r_{n-1} &= a_n r_n \end{aligned}$$

Temos então

$$\begin{aligned} x = p/q &= a_0 + \frac{1}{a_1 + r_2/r_1} = a_0 + \frac{1}{a_1 + \dfrac{1}{a_2 + r_3/r_2}} \\ &= \cdots = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_n}}} = [a_0; a_1, a_2, \ldots, a_n] \end{aligned}$$

□

Proposição 14.1. Seja F o conjunto dos reais positivos x com representação em frações contínuas infinitas onde todos os quocientes parciais são iguais a 1 ou 2. Prove que o menor número possível de F é o número $a = [1; 2, 1, 2, 1, 2, \ldots]$ e o maior número é $b = [2; 1, 2, 1, 2, \ldots]$.

Demonstração. De fato, se quisermos minimizar o número, o a_0 deve ser igual a 1, e a_1 deve ser igual a 2 para que a fração seja a menor possível, isto é, $x = 1 + \frac{1}{2}$, seguindo, a_2 deve ser o menor possível para que o termo $1/a_2$ seja o maior possível, resultando que $\frac{1}{a_1 + \frac{1}{a_2}}$ é o menor possível, seguindo a mesma lógica, a_3 deve ser o maior possível, e assim por diante, chegando a $a = [1; 2, 1, 2, 1, 2, \ldots]$. Para chegar em $b = [2; 1, 2, 1, 2, \ldots]$ é análogo. □

Proposição 14.2. $b = [2; 1, 2, 1, 2, 1, \ldots]$ é igual a $1 + \sqrt{3}$.

Demonstração. Seja $b = 2 + \cfrac{1}{1 + \cfrac{1}{2 + \cfrac{1}{1 + \ldots}}}$, observe que $b = 2 + \dfrac{1}{1 + \dfrac{1}{b}} \iff b = 2 + \dfrac{1}{\dfrac{b+1}{b}}$

Daí,

$$\begin{aligned} b(b+1) &= 2(b+1) + b \\ b^2 + b &= 2b + 2 + b \\ b^2 - 2b - 2 &= 0 \end{aligned}$$

Resolvendo a equação, encontramos $b = 1 + \sqrt{3}$. □

Para mais detalhes relacionados a frações contínuas, o leitor pode consultar (MARTINEZ et al., 2010).

Conjuntos de números definidos por condições em seus quocientes parciais podem ser pensados como atratores fractais de certos sistemas iterados de funções, como ilustra o exemplo a seguir.

Exemplo 14.2. Seja F o conjunto dos reais positivos x com representação em frações contínuas infinitas onde todos os quocientes parciais são iguais a 1 ou 2. Então F é o atrator do sistema iterado de funções $\{S_1, S_2\}$ em $[1, 3]$ onde $S_1(x) = 1 + 1/x$ e $S_2(x) = 2 + 1/x$, com $0,44 < \dim_H F < 0,66$.

Demonstração. Claramente F é limitado, pois o menor número possível de F é o número $a = [1; 2, 1, 2, 1, 2, \dots]$ e o maior número é $b = [2; 1, 2, 1, 2, \dots]$ pelas Proposições 14.1 e 14.2.

Observe que $a = 1 + \dfrac{1}{2 + \dfrac{1}{a}} = 1 + \dfrac{a}{2a + 1}$. Resolvendo a equação do segundo grau encontramos $a = \dfrac{1 + \sqrt{3}}{2}$. E já encontramos $b = 1 + \sqrt{3}$. Afirmo que F é fechado. De fato, suponha uma sequência $(x_n)_n \in F$ tal que $(x_n) \to L$, se L não pertencesse a F, então F seria uma fração contínua infinita tal que algum quociente parcial é diferente de 1 e 2, ou seria um número racional. Em ambos os casos, tomando N suficientemente grande, deveríamos $|x_n - L| < \varepsilon$ para $n > N$ para qualquer $\varepsilon > 0$. Mas, pelo fato de L ter algum quociente parcial diferente de qualquer número de F, seria possível tomar uma bola de forma que nenhum x_n estaria próximo o suficiente.

É intuitivo perceber que se $y \in F$, então $x \in F$ fazendo $x = 1 + \frac{1}{y}$ ou $x = 2 + \frac{1}{y}$, assim descobrimos uma forma de "gerar" elementos de F. Esta é a descrição de S_1 e S_2, logo segue que $F = S_1(F) \cup S_2(F)$, ou seja, F é o atrator de $\{S_1, S_2\}$. No Exemplo 13.6 provamos que este conjunto tem $0,44 < \dim_{\mathrm{H}} F < 0,66$. □

14.2 APROXIMAÇÕES DIOFANTINAS

Quão perto um dado número irracional x pode ser aproximado por um racional p/q com denominador q menor ou igual a um número $q_0 \in \mathbb{N}$ fixo? Aproximação diofantina é o estudo de problemas desse tipo. Uma boa aproximação significa chegar muito próximo de x usando uma fração com denominador relativamente pequeno.

Uma ideia inicial simples é notar que se marcarmos todas as frações com denominador q na reta, x vai estar em algum desses intervalos de tamanho $1/q$. Se denotarmos o ponto que x está mais próximo por p/q, então x está no máximo a uma distância de $1/2q$ deste ponto. Logo, mostramos que para qualquer q, existe p tal que

$$\left| x - \frac{p}{q} \right| \leqslant \frac{1}{2q}.$$

Esta aproximação ainda não está tão boa. Por exemplo, se quisermos um racional distante no máximo 0.0001 de x, precisamos olhar frações com denominador no mínimo 5000.

Para melhorar essas aproximações, temos um famoso teorema de Dirichlet:

Teorema 14.2 (Teorema de Dirichlet para aproximações diofantinas)**.** Para qualquer irracional x, existem infinitos inteiros p, q satisfazendo

$$\left| x - \frac{p}{q} \right| \leqslant \frac{1}{q^2}.$$

Demonstração. Fixe N natural e considere as partes fracionárias dos números $0, x, 2x, \ldots, Nx$ e a partição de $[0, 1]$ em N intervalos:

$$\left[0; \frac{1}{N}\right), \left[\frac{1}{N}, \frac{2}{N}\right), \ldots, \left[\frac{N-1}{N}, 1\right)$$

Temos $N + 1$ números e N intervalos, pelo Princípio da Casa dos Pombos existem duas partes fracionárias que caem no mesmo intervalo, digamos $\{ax\}$ e $\{bx\}$. Daí

$$|\{ax\} - \{bx\}| < \frac{1}{N} \Leftrightarrow |(ax - \lfloor ax \rfloor) - (bx - \lfloor bx \rfloor| < \frac{1}{N}$$

$$|(a-b)x - (\lfloor ax \rfloor - \lfloor bx \rfloor)| < \frac{1}{N}.$$

Definimos $q = a - b$ e $p = \lfloor ax \rfloor - \lfloor bx \rfloor$, e temos

$$|qx - p| < \frac{1}{N} \Rightarrow \left| x - \frac{p}{q} \right| < \frac{1}{Nq} < \frac{1}{q^2},$$

onde estamos tomando $N \geq q$. Isto conclui a existência, mas por que haveria infinitos? Isto segue do fato de podermos tomar N tão qrande quanto desejarmos. De fato, se considerarmos N_1, obtemos um racional $r_1 = p_1/q_1$ tal que

$$\left| x - \frac{p_1}{q_1} \right| < \frac{1}{N_1 q_1} < \frac{1}{q_1^2}.$$

Agora, tomamos $N_2 > N_1$ tal que

$$\frac{1}{N_2} < \left| x - \frac{p_1}{q_1} \right|.$$

Obtemos assim $r_2 = p_2/q_2$ um racional associado N_2 tal que

$$\left| x - \frac{p_2}{q_2} \right| < \frac{1}{N_2 q_2} \leq \frac{1}{{q_2}^2}.$$

Segue da escolha de N_2 que $r_2 \neq r_1$, pois r_2 é uma melhor aproximação de x do que r_1, já que

$$\left| x - \frac{p_2}{q_2} \right| < \frac{1}{N_2 q_2} \leq \frac{1}{N_2} < \left| x - \frac{p_1}{q_1} \right|.$$

Repetindo esse processo, obtemos uma sequência de inteiros $N_1 < N_2 < N_3 < \cdots$ e uma sequência de números racionais $r_i = q_i/p_i$ tais que

$$\left| x - \frac{p_i}{q_i} \right| < \frac{1}{N_i q_i} \leq \frac{1}{{q_i}^2}$$

com $|\alpha - r_i| \leq 1/N_i$, e que aproximam x cada vez melhor, i.e.,

$$|x - r_1| > |x - r_2| > |x - r_3| > \cdots$$

□

Sabendo deste teorema, se quisermos uma fração distante 0.0001 de x, podemos fazer isso com um denominador menor ou igual a 100.

Outra forma de escrever o Teorema de Dirichlet é: Para todo número real x,

$$||qx|| \leqslant q^{-1}$$

para infinitos q, onde $||y|| = min_{m\in\mathbb{Z}}|y-m|$ denota a distância de y para o inteiro mais próximo.

Definição 14.1. Dizemos que um número x tal que

$$||qx|| \leqslant q^{1-\alpha} \tag{14.1}$$

para infinitos inteiros q é α**-bem-aproximável.**

14.3 O TEOREMA DE JARNÍK

Teorema 14.3. Suponha $\alpha > 2$. Seja F o conjunto dos números reais $x \in [0,1]$ para os quais a desigualdade

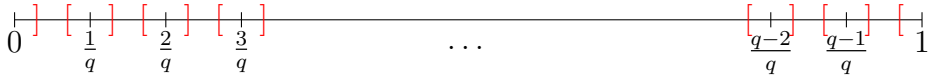
$$\|qx\| \leqslant q^{1-\alpha} \tag{14.2}$$

é satisfeita para infinitos inteiros positivos q. Então $\dim_{\mathrm{H}} F = 2/\alpha$.

Demonstração. Para cada $q \in \mathbb{N}$, seja G_q o conjunto dos $x \in [0,1]$ para os quais $||qx|| \leqslant q^{1-\alpha}$. Temos

$$||qx|| \leqslant q^{1-\alpha} \iff \exists\ p \in \mathbb{Z} \text{ tal que } |qx-p| \leqslant q^{1-\alpha}, \text{ i.e., } \left|x - \frac{p}{q}\right| \leqslant \frac{1}{q^{\alpha}}$$

Ou seja, dividimos $[0,1]$ em intervalos de comprimento $1/q$ e tomamos a bola fechada de raio $1/q^{\alpha}$ em cada ponto:



Isso nos dá $q-1$ intervalos de tamanho $i/q + 1/q^{\alpha} - (i/q - 1/q^{\alpha}) = 2q^{-\alpha}$ e 2 intervalos nos extremos de comprimento $q^{-\alpha}$.

Claramente $F \subset \bigcup_{q=k}^{\infty} G_q$ para cada k, então tomando esses intervalos de G_q para $q \geqslant k$ como uma cobertura de F nos dá

$$\mathcal{H}^s_{\delta}(F) \leqslant \sum_{q=k}^{\infty}(q+1)(2q^{-\alpha})^s \text{ se } 2k^{-\alpha} \leqslant \delta.$$

Para analisar a convergência da série $\sum_{q=k}^{\infty}(q+1)(2q^{-\alpha})^s$, podemos simplificar para

$$\sum_{q\geqslant k}(q+1)q^{-\alpha s} = \sum_{q\geqslant k}(q^{1-\alpha s} + q^{-\alpha s}).$$

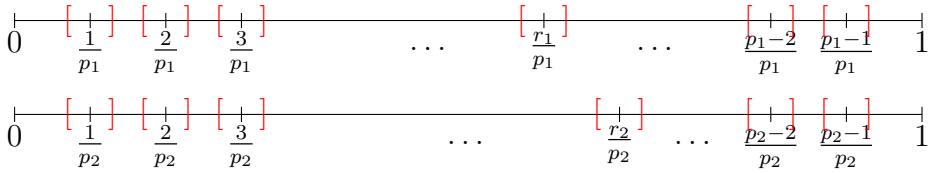
Sabemos que $\sum_{n=1}^{\infty}\frac{1}{n^{\beta}} < +\infty \iff \beta > 1$. Logo, se $-(1-\alpha s) > 1$ e $\alpha s > 1$, a série converge. Ou seja, para $\alpha s > 2$, a série converge.

Com isso temos que $\lim_{k\to\infty}\sum_{q=k}^{\infty}(q+1)(2q^{-\alpha})^s = 0$ e $\mathcal{H}^s(F) = 0$. Por isso, $\dim_{\mathrm{H}} F \leqslant 2/\alpha$. Agora vamos trabalhar para encontrar o limite inferior

Seja G'_q o conjunto dos $x \in [q^{-\alpha}, 1-q^{-\alpha}]$ para os quais $||qx|| \leqslant q^{1-\alpha}$, ou seja, G'_q é G_q com os intervalos extremos removidos. Seja n um inteiro positivo e suponha p_1 e p_2 números primos tais que $n < p_1 < p_2 \leqslant 2n$. Vamos mostrar que G'_{p_1} e G'_{p_2} são disjuntos e razoavelmente bem separados. Observe que se $1 \leqslant r_1 < p_1$ e $1 \leqslant r_2 < p_2$, então $p_1 r_2 \neq p_2 r_1$ pois p_1 e p_2 são primos. Daí,

$$\left|\frac{r_1}{p_1} - \frac{r_2}{p_2}\right| = \frac{1}{p_1 p_2}|p_2 r_1 - p_1 r_2| \geqslant \frac{1}{p_1 p_2} \geqslant \frac{1}{4n^2}.$$

Para melhor entendimento, retomamos aos desenhos (sem apego a proporções corretas):



Nossos cálculos mostraram que a distância entre dois centros de qualquer intervalo de G'_{p_1} e de G'_{p_2} é pelo menos $1/4n^2$. Como os intervalos têm diâmetro no máximo $2n^{-\alpha}$ (pois $n < p_1$ e $n < p_2$, o que implica $1/n > 1/p_1$ e $1/n > p_2$), a distância entre qualquer ponto de G'_{p_1} e G'_{p_2} é pelo menos $\dfrac{1}{4n^2} - \dfrac{2}{n^\alpha} \geqslant \dfrac{1}{8n^2}$ para n grande o suficiente.

De fato, a desigualdade acima é válida se, e somente se

$$\frac{1}{4} - \frac{2}{n^{\alpha-2}} \geqslant \frac{1}{8} \to \frac{2}{n^{\alpha-2}} \leqslant \frac{1}{8}.$$

Desde que $\alpha > 2$, $\lim_{n\to+\infty}\dfrac{2}{n^{\alpha-2}} = 0$. Logo, dado $\varepsilon > 0$, existe $n_0 \in \mathbb{N}$ tal que para $n > n_0$,

$$\frac{2}{n^{\alpha-2}} < \frac{1}{8} + \varepsilon.$$

Para tais n, o conjunto

$$H_n = \bigcup_{\substack{p \text{ primo} \\ n<p\leqslant 2n}} G'_p$$

é uma união disjunta dos intervalos em G'_p, então H_n é composto de intervalos de comprimento no mínimo $(2n)^{-\alpha}$ que estão separados por gaps de comprimento no mínimo $1/8n^2$. Se $I \subset [0,1]$ é qualquer intervalo com $3/|I| < n < p \leqslant 2n$ então pelo menos $p|I|/3 \geqslant n|I|/3$ dos intervalos de G'_p estão completamente contidos em I. Uma versão do Teorema do Número Primo afirma

que $\pi(n) \sim n/\log n$, temos

$$\begin{aligned}\pi(2n) - \pi(n) = \frac{2n}{\log 2n} - \frac{n}{\log n} &= n\left(\frac{2}{\log 2 + \log n} - \frac{1}{\log n}\right) \\ &= n\left(\frac{2\log n - \log 2 - \log n}{\log n(\log 2 + \log n)}\right) \\ &= n\left(\frac{\log n - \log 2}{\log n(\log 2 + \log n)}\right) \\ &= \frac{n}{\log n}\left(\frac{1 - \log 2/\log n}{\log 2/\log n + 1}\right) \\ &= n/\log n\end{aligned}$$

pois $\log 2/\log n \xrightarrow{n\to\infty} 0$. Então, existem pelo menos $n/\log n$ primos no intervalo $(n, 2n)$ se $n > n_1$, para um $n_1 > n_0$ grande. Logo, pelo menos

$$\frac{n^2|I|}{6\log n} \tag{14.3}$$

intervalos de H_n estão contidos em I dado que $n > n_1$ e $|I| \geqslant 3/n$. Para terminar a prova, vamos usar o Exemplo 12.4. Dado n_1 como acima, seja $n_k =$max$\{n_{k-1}^k, 3 \times 2^a n_{k-1}^2\}$, para $k = 2, 3, \ldots$, onde $a > \alpha$ é um inteiro. Seja $E_0 = [0, 1]$, e para $k = 1, 2, \ldots$, denote por E_k os intervalos de H_{n_k} que estão completamente contidos em E_{k-1}. Os intervalos de E_k têm comprimento pelo menos $(2n_k)^{-\alpha}$ e estão separados por gaps de pelo menos $\varepsilon_k = \frac{1}{8}n_k^{-2}$. Usando (14.3), cada intervalo de E_{k-1} contém pelo menos m_k intervalos de E_k, onde

$$m_k = \frac{n_k^2(2n_{k-1})^{-\alpha}}{6\log n_k} = \frac{cn_k^2 n_{k-1}^{-\alpha}}{\log n_k}$$

se $k \geq 2$, onde $c = 2^{-\alpha}/6$. (Tomamos $m_1 = 1$.) Pelo Exemplo 12.5,

$$\begin{aligned}\dim_{\mathrm{H}}\left(\bigcap_{k=1}^{\infty} E_k\right) &\geqslant \varliminf_{k\to\infty} \frac{\log[c^{k-2}n_1^{-\alpha}(n_2\cdots n_{k-2})^{2-\alpha}n_{k-1}^2(\log n_2)^{-1}\cdots(\log n_{k-1})^{-1}]}{-\log[cn_{k-1}^{-\alpha}(8\log n_k)^{-1}]} \\ &= \varliminf_{k\to\infty} \frac{\log[c^{k-2}n_1^{-\alpha}(n_2\cdots n_{k-2})^{2-\alpha}(\log n_2)^{-1}\cdots(\log n_{k-1})^{-1}] + 2\log n_{k-1}}{-\log(c/8) + \log(k(\log n_{k-1})) + \alpha\log n_{k-1}} \\ &= 2/\alpha\end{aligned}$$

uma vez que os termos dominantes no numerador e denominador são aqueles em $\log n_{k-1}$. (Note que para k suficientemente grande, $\log n_k = k\log n_{k-1}$ então $\log n_k = ck!$). Se $x \in E_k \subset H_{n_k}$ para todo k, então x está em infinitos G'_p e segue que $x \in F$. Concluímos que $\dim_{\mathrm{H}} F \geqslant 2/\alpha$.

□

REFERÊNCIAS

ABBOTT, S. **Understanding Analysis**. New York: Springer, 2001.

APOSTOL, T. **Introduction to Analytic Number Theory**. [S.l.]: Springer, 1976.

BARTLE, R. G. **The elements of integration and Lebesgue measure**. [S.l.]: John Wiley & Sons, 2014.

FALCONER, K. **Fractal Geometry Mathematical Foundations and Applications**. 3. ed. [S.l.]: John Wiley & Sons Ltd, 2014.

FALCONER, K.; JÄRVENPÄÄ, M.; MATTILA, P. Examples illustrating the instability of packing dimensions of sections. **Real Analysis Exchange**, JSTOR, p. 629–640, 1999.

FALCONER, K. J. **The geometry of fractal sets**. [S.l.]: Cambridge university press, 1985.

FALCONER, K. J.; HOWROYD, J. D. Packing dimensions of projections and dimension profiles. In: CAMBRIDGE UNIVERSITY PRESS. **Mathematical Proceedings of the Cambridge Philosophical Society**. [S.l.], 1997. v. 121, n. 2, p. 269–286.

FEDERER, H. **Geometric measure theory**. [S.l.]: Springer, 2014.

FOLLAND, G. B. **Real analysis: modern techniques and their applications**. [S.l.]: John Wiley & Sons, 1999. v. 40.

HUTCHINSON, J. E. Fractals and self similarity. **Indiana University Mathematics Journal**, JSTOR, v. 30, n. 5, p. 713–747, 1981.

JACOBSON, N. **Basic algebra I**. [S.l.]: Courier Corporation, 2012.

LI, A. Dirichlet's theorem about primes in arithmetic progressions. The University of Chicago, 2012.

LIMA, E. L. **Curso de análise, vol. 1**. 14. ed. Rio de Janeiro: IMPA, 2013.

MANDELBROT, B. B.; NESS, J. W. V. Fractional brownian motions, fractional noises and applications. **SIAM review**, SIAM, v. 10, n. 4, p. 422–437, 1968.

MARTINEZ, F. B.; MOREIRA, C. G.; SALDANHA, N.; TENGAN, E. Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro. IMPA, 2010.

RANA, I. K. **An introduction to measure and integration**. [S.l.]: American Mathematical Soc., 2002. v. 45.

ROGERS, C. A. **Hausdorff measures**. [S.l.]: Cambridge University Press, 1998.

SANTOS, J. P. O. **Introdução à teoria dos números**. Rio de Janeiro: SBM, 1998.