Creilson de Jesus Conceição

FUNÇÕES ARITMÉTICAS E O TEOREMA DE CESÀRO

Itabaiana-SE

Janeiro de 2020

Creilson de Jesus Conceição

FUNÇÕES ARITMÉTICAS E O TEOREMA DE CESÀRO

Dissertação submetida ao Corpo Docente do Programa de Mestrado Profissional em Matemática da Universidade Federal de Sergipe como requisito para a obtenção do título de Mestre em Matemática.

Universidade Federal de Sergipe

Departamento de Matemática

Programa de Pós-Graduação

Orientador: Prof. Me. Samuel Brito Silva

Itabaiana-SE

Janeiro de 2020

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA PROFESSOR ALBERTO CARVALHO
UNIVERSIDADE FEDERAL DE SERGIPE

C744f Conceição, Creilson de Jesus.
Funções aritméticas e o teorema de Cesàro / Creilson de Jesus Conceição; orientação: Samuel Brito Silva. – Itabaiana, 2020.
68 f.; il.

Dissertação (Mestrado em Matemática) – Universidade Federal de Sergipe, 2020.

1. Matemática. 2. Funções Aritméticas. 3. Teorema de Cesàro. I. Silva, Samuel Brito. II. Título.

CDU 511.174

UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

Funções Aritméticas e o Teorema de Cesàro

por

Creilson de Jesus Conceição

Aprovada pela banca examinadora:

Samuel Brito Silva

Prof. Samuel Brito Silva - UFS
Orientador

Mateus Alegri

Prof. Mateus Alegri - UFS
Primeiro Examinador

Charles Braga Amorim

Prof. Charles Braga Amorim - UFS
Segundo Examinador

Itabaiana, 14 de Fevereiro de 2020

Cidade Universitária "Prof. José Aloísio de Campos" – Av. Marechal Rondon, s/no - Jardim Rosa Elze – Campus de São Cristóvão. Tel. (00 55 79) 3194-6887
CEP: 49100-000 - São Cristóvão – Sergipe - Brasil – E-mail: promat.ufs@gmail.com

Dedico este trabalho a Deus e aos meus pais.

Agradecimentos

Essa é uma das etapas mais importante de minha vida. Primeiramente, agradeço a Deus, pois, acredito que sem ele não somos nada.

Aos meus pais, Dilma e Raimundo, que através das inúmeras situações, me mostraram as conquistas não poderiam ser fáceis, deveriam ser vivenciadas, com dignidade e verdade e, que Deus, a família, os amigos são mais importantes que qualquer outra coisa.

Ao meu amor, Aline Oliveira, por sua sinceridade, por todo o carinho e por ter sempre me incentivado a nunca desistir.

Ao meu orientador, Professor Me. Samuel Brito Silva, pela dedicação, incentivo, atenção e auxílio no acompanhamento de cada etapa deste trabalho.

Aos professores do PROFMAT - FUFS, Me. Wagner Ferreira dos Santos, Me. Viviane de Jesus Lisboa Aquino, Me. Samuel Brito Silva, Dr. Alejandro Caicedo Roque, Dr. Éder Mateus de Souza e Dr. Ricardo Nicasso Benito, que estiveram comigo ao Longo deste percurso, orientando e compartilhando um pouco dos seus conhecimentos.

Aos colegas do PROFMAT - FUFS que estiveram comigo ao longo destes dois anos me apoiando e ajudando.

Aos professores Jorge Araújo e Tarciso Éder que me ensinaram a essência da matemática e que me fez perceber que a demonstração era uma maneira de tornar as coisas verdadeiras, sem espaço para questionamentos.

A Universidade Federal de Sergipe por ter me dado a oportunidade de vivenciar este sonho.

Por fim, a todos que contribuíram de forma direta e indireta para a realização deste sonho.

A matemática vista corretamente, possui não apenas verdade, mas também suprema beleza.

(Bertrand Russel)

Resumo

Esta dissertação tem como objetivo principal demonstrar o Teorema de Ernesto Cesàro, o qual afirma que, a probabilidade de escolher dois números primos entre si, aleatoriamente, no conjunto dos inteiros positivos é igual a $\frac{6}{\pi^2}$, utilizando as funções μ de Möbius e φ de Euler. Além disso, realizaremos um estudo detalhado sobre funções aritméticas, abordando o produto de Dirichlet para funções aritméticas e utilizaremos esse resultado para provar de forma fácil a fórmula da inversão de Möbius.

Palavras-chaves: Funções Aritméticas, Produto de Dirichlet, Teorema de Cesàro.

Abstract

In this dissertation has as main objective to demonstrate Ernesto Cesàro's Theorem, which states that the probability of choosing two prime numbers among themselves, randomly, in the set of positive integers is equal to $\dfrac{6}{\pi^2}$, using the Möbius μ and Euler φ functions. In addition, we will carry out a detailed study of arithmetic functions, covering Dirichlet's product for arithmetic functions and use this result to easily prove the Möbius inversion formula.

Key-words: Arithmetic Functions, Dirichlet's Product, Cesàro's Theorem.

Sumário

1 Introdução

A teoria dos números é o ramo da matemática pura que se preocupa com o estudo de propriedades relativas aos números inteiros. No campo da teoria dos números muitos problemas podem ser facilmente compreendidos, mesmo por pessoas que não trabalham diretamente com matemática, entretanto, alguns destes são extremamente complicados de resolver, tanto que muitos problemas em aberto na atualidade provém desse ramo da matemática, o mais famoso deles é a hipótese de Riemann.

As funções aritméticas são objetos de estudo da teoria dos números. Elas são definidas no conjunto dos números inteiros positivos e assumem valores reais ou complexos. As funções aritméticas têm aplicações em combinatória, contagem, teoria das probabilidades e análise, nas quais elas surgem como coeficientes das séries de potências. Além disso, há uma diferença entre esse tipo de funções com as funções típicas, pois, geralmente não podem ser descritas por uma simples expressão.

Esta dissertação está organizada em quatro partes. Na primeira parte, intitulada "Resultados Preliminares", definimos os principais termos utilizados ao longo deste trabalho e apresentamos resultados básicos sobre números binomiais e divisibilidade. Além disso, estudamos sequências e séries numéricas, em especial, a série de Taylor. Essa abordagem será importante para compreensão de alguns teoremas que iremos demonstrar ao longo deste trabalho.

Na segunda parte, intitulada "Funções Aritméticas", descreveremos as propriedades e teoremas referentes as funções μ de Möbius e φ de Euler que informa a quantidade de números primos entre si menores do que um número n dado. Além disso, enunciaremos e demonstraremos uma notável fórmula que relaciona estas duas funções.

Na terceira parte, intitulada "O Produto de Dirichlet de Funções Aritméticas", utilizaremos a multiplicação de Dirichlet para provar a fórmula da inversão de Möbius. Nesta parte ainda são apresentadas as funções aritméticas Λ de Magoldt, λ de Lioville e a função divisor σ. Além disso, mostraremos que muitas funções aritméticas possuem a propriedade multiplicativas e faremos uma generalização para o produto de Dirichlet.

E finalmente, na quarta parte, intitulada "O Teorema de Ernesto Cesàro", utilizando as funções μ de Móbius e φ de Euler, mostraremos que a probabilidade de escolhermos, aleatoriamente, dois inteiros primos entre si no conjunto dos inteiros positivos é igual a $\dfrac{6}{\pi^2}$. Este resultado é conhecido como o Teorema de Cesàro.

2 Resultados Preliminares

Nesta seção enunciaremos alguns resultados que serão de grande valia para melhor compreensão deste trabalho.

2.1 Números binomiais

Definição 2.1. *Chamamos de número binomial ou coeficiente binomial, o número de modos de escolher p dentre n objetos, com $p \leq n$. Podemos representar o número binomial da seguinte forma:*

$$\binom{n}{p} = \frac{n!}{p!(n-p)!} = \frac{n(n-1)(n-2)\cdots(n-p+1)}{p!}.$$

Exemplo 2.1.

$$\binom{6}{4} = \frac{6!}{4!(6-4)!} = \frac{6 \cdot 5}{2} = 30.$$

Proposição 2.1. *Se p e n são números inteiros não negativos, com $p \leq n$, então*

$$\binom{n}{p} = \binom{n}{n-p}.$$

Demonstração: Sejam p e n são números inteiros não negativos, com $p \leq n$. Pela definição 2.1, temos

$$\begin{aligned}\binom{n}{p} &= \frac{n!}{p!(n-p)!} \\ &= \frac{n!}{(n-p)!(n-(n-p))!} \\ &= \binom{n}{n-p}.\end{aligned}$$

□

Exemplo 2.2.

$$\binom{6}{4} = \binom{6}{6-4} = \binom{6}{2}.$$

2.2 Binômio de Newton

Antes de enunciarmos o Teorema do Binômio de Newton, iremos demonstrar a Relação de Stifel que será utilizada na demostração do mesmo.

Teorema 2.1. *(Relação de Stifel) Se n e p são números inteiros não negativos com $p < n$, então*

$$\binom{n}{p} + \binom{n}{p+1} = \binom{n+1}{p+1}.$$

Demonstração: Sejam n e p são números inteiros não negativos com $p < n$. Pela definição 2.1, temos

$$\begin{aligned}
\binom{n}{p} + \binom{n}{p+1} &= \frac{n!}{p!(n-p)!} + \frac{n!}{(p+1)!(n-p-1)!} \\
&= \frac{n!(p+1) + n!(n-p)}{(p+1)!(n-p)!} \\
&= \frac{n!(n+1)}{(p+1)!(n-p)!} \\
&= \frac{(n+1)!}{(p+1)!(n+1-(p+1))!} \\
&= \binom{n+1}{p+1}.
\end{aligned}$$

□

Problema 2.1. *Dada a sequência de números inteiros*

$$\begin{cases} a_1 = \binom{2}{2} \\ a_n = \binom{2}{2} + \binom{3}{2} + \cdots + \binom{n+1}{2}, \ n \geq 2. \end{cases}$$

Mostre que $a_n = \binom{n+2}{3}$.

Solução: Para $n = 1$ a propriedade é verdadeira, pois

$$a_1 = \binom{1+2}{3} = \binom{3}{3} = \binom{2}{2}.$$

Suponhamos que a propriedade seja válida para algum $n \in \mathbb{Z}_+$, ou seja,

$$a_n = \binom{2}{2} + \binom{3}{2} + \cdots + \binom{n+1}{2} = \binom{n+2}{3}.$$

Mostraremos que a validade de n implica na validade de $n+1$. Logo,

$$\begin{aligned}
a_{n+1} &= \binom{2}{2} + \binom{3}{2} + \cdots + \binom{n+1}{2} + \binom{n+2}{2} \\
&= \binom{n+2}{3} + \binom{n+2}{2} \ (usando\ a\ Relação\ de\ Stifel) \\
&= \binom{n+3}{3}
\end{aligned}$$

Portanto, mostramos, por indução, que a propriedade é válida para todos os inteiros positivos.

Depois de provar a validade da Relação de Stifel, vamos enunciar e demonstrar, a seguir, o Teorema do Binômio de Newton.

Teorema 2.2. *(Binômio de Newton) Se a e b são números reais e n é um número inteiro positivo, então*

$$(a+b)^n = \sum_{p=0}^{n} \binom{n}{p} a^{n-p} b^p.$$

Demonstração: Vamos demonstrar essa propriedade por indução matemática. Para $n = 1$ a propriedade é verdadeira, pois,

$$a+b = (a+b)^1 = \sum_{p=0}^{1} \binom{1}{p} a^{1-p} b^p = \binom{1}{0} a^{1-0} b^0 + \binom{1}{1} a^{1-1} b^1 = 1 \cdot a \cdot 1 + 1 \cdot 1 \cdot b = a + b.$$

Suponhamos então, a validade da propriedade para algum número inteiro positivo n. Mostraremos que a validade de n implica na validade de $n+1$. Assim,

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)(a+b)^n \\
&= (a+b) \sum_{p=0}^{n} \binom{n}{p} a^{n-p} b^p \\
&= (a+b) \left[\binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n-1} a b^{n-1} + \binom{n}{n} b^n \right] \\
&= \binom{n}{0} a^{n+1} + \binom{n}{1} a^n b + \cdots + \binom{n}{n} a b^n + \binom{n}{0} a^n b + \binom{n}{1} a^{n-1} b^2 + \cdots + \binom{n}{n} b^{n+1} \\
&= \binom{n}{0} a^{n+1} + \left[\binom{n}{0} + \binom{n}{1} \right] a^n b + \cdots + \left[\binom{n}{n-1} + \binom{n}{n} \right] a b^n + \binom{n}{n} b^{n+1} \\
&= \binom{n}{0} a^{n+1} + \binom{n+1}{1} a^n b + \binom{n+1}{2} a^{n-1} b^2 + \cdots + \binom{n+1}{n} a b^n + \binom{n}{n} b^{n+1} \\
&= \binom{n+1}{0} a^{n+1} + \binom{n+1}{1} a^n b + \cdots + \binom{n+1}{n} a b^n + \binom{n+1}{n+1} b^{n+1} \\
&= \sum_{p=0}^{n+1} \binom{n+1}{p} a^{n+1-p} b^p.
\end{aligned}$$

Portanto, por indução matemática, a propriedade é válida para todo número inteiro positivo.

□

Problema 2.2. *Determine o desenvolvimento de $(x+2)^4$.*

Solução: Utilizando o teorema do Binômio de Newton temos,

$$
\begin{aligned}
(x+2)^4 &= \sum_{p=0}^{4} \binom{4}{p} x^{4-p} 2^p \\
&= \binom{4}{0} x^4 2^0 + \binom{4}{1} x^3 2^1 + \binom{4}{2} x^2 2^2 + \binom{4}{3} x^1 2^3 + \binom{4}{4} x^0 2^4 \\
&= x^4 + 8x^3 + 24x^2 + 32x + 16.
\end{aligned}
$$

2.3 Divisibilidade

Definição 2.2. *Se a e b são números inteiros, dizemos que a divide b, e denotamos por $a \mid b$, se existe um número inteiro c tal que $b = ac$. Caso o inteiro c não exista, dizemos que a não divide b, em símbolos $a \nmid b$.*

Proposição 2.2. *Se a, b e c são números inteiros tais que $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração: Como $a \mid b$ e $b \mid c$ existem números inteiros q_1 e q_2 tais que $b = aq_1$ e $c = bq_2$. Fazendo a substituição de $b = aq_1$ em $c = bq_2$, temos que $c = aq_1q_2 = a(q_1q_2)$ e portanto $a \mid c$.

□

Exemplo 2.3. *Como* $5 \mid 20$ *e* $20 \mid 100$, *então* $5 \mid 100$.

Proposição 2.3. *Se a, b, c, x e y são números inteiros, tais que $c \mid a$ e $c \mid b$ então $c \mid (ax \pm by)$.*

Demonstração: Como $c \mid a$ e $c \mid b$ existem números inteiros q_1 e q_2 tais que $a = q_1c$ e $b = q_2c$. Fazendo a multiplicação das duas equações anteriores, respectivamente, por x e y obtemos $ax = q_1cx$ e $by = q_2cy$. Agora, somando ou subtraindo membro a membro as equações que foram multiplicadas teremos $ax \pm by = q_1cx \pm q_2cy = c(q_1x \pm q_2y)$. Logo, $c \mid (ax \pm by)$.

□

Exemplo 2.4. *Como* $5 \mid 15$ *e* $5 \mid 25$, *então* $5 \mid 15 \cdot 12 + 25 \cdot 17$.

Antes de introduzirmos o chamado algoritmo da divisão euclidiana vamos mostrar uma propriedade denominada Teorema de Eudoxius que será utilizada na demonstração do algoritmo da divisão de Euclides.

Teorema 2.3. *(Teorema de Eudoxius) Dados a, b números inteiros, com $b \neq 0$, existe um número inteiro q tal que:*
1) para $b > 0$,

$$qb \leq a < (q+1)b$$

2) para $b < 0$,

$$qb \leq a < (q-1)b.$$

Demonstração: Sem perda de generalidade, vamos considerar o caso em que $a > 0$ e $b > 0$. A demonstração dos demais casos se faz de maneira análoga.
Sejam a e b números inteiros tais que $a > 0$ e $b > 0$. Dessa forma, temos duas possibilidades, $a = q_1 b$ ou $a \neq q_1 b$, para algum número inteiro q_1. Se $a = q_1 b$, não há nada para mostrar. Suponhamos então que $a \neq q_1 b$. Desse modo, existe um menor número inteiro c tal que $a < cb$, logo $(c-1)b < a$, pois caso contrário, teríamos um absurdo, pois c é o menor inteiro que isso acontece. Logo, concluímos que $(c-1)b < a < cb$. Fazendo $q = c - 1$, temos que $qb \leq a < (q+1)b$.

□

Exemplo 2.5. *Sendo $a = 13$ e $b = 6$, devemos tomar $q = 2$, assim*

$$2 \cdot 6 \leq 13 < 3 \cdot 6.$$

Sendo $a = 19$ e $b = -4$, devemos tomar $q = (-4)$, assim

$$(-4) \cdot (-4) \leq 19 < (-5) \cdot (-4).$$

2.4 Algoritmo da divisão euclidiana

Teorema 2.4. *Dados a e b números inteiros, com $b \neq 0$, existe um único par de números inteiros q e r tais que $a = qb + r$, com $0 \leq r < |b|$.*

Demostração: Suponhamos primeiro que $b > 0$. Pelo Teorema de Eudoxius existe um número inteiro q tal que $qb \leq a < (q+1)b$, o que implica em $0 \leq a - qb < b$. Fazendo $r = a - qb$, temos que $0 \leq r < b$. Suponhamos agora que $b < 0$, assim, $-b > 0$. Logo existem números inteiros q e r tais que $a = q(-b) + r$, com $0 \leq r < -b = |b|$. Dessa forma, mostramos que existem os inteiros q e r. Mostraremos agora que eles são únicos.
Suponhamos por absurdo que $a = qb + r = q_1 b + r_1$, sendo q_1 e r_1 números inteiros com

$0 \leq r < |b|$ e $0 \leq r_1 < |b|$. Como, $qb + r = q_1 b + r_1$ temos que $b(q - q_1) = r_1 - r$. Como $r, r_1 < |b|$, temos que $|r - r_1| < |b|$. Se $q \neq q_1$, então $|q - q_1| \geq 1$. Desse modo,

$$|b| \leq |b| \cdot |q - q_1| = |r_1 - r| < |b|.$$

Mas, isso é absurdo. Portanto temos que $q = q_1$ e $r = r_1$.

□

2.5 O máximo divisor comum

Definição 2.3. *O máximo divisor comum de dois inteiros a e b, não ambos nulos, denotado por (a, b), é o maior inteiro que divide a e b.*

Teorema 2.5. *Se $d = (a, b)$, então existem inteiros x e y tais que $d = ax + by$.*

Demonstração: Seja $A = \{ax + by; x, y \in \mathbb{Z}\}$. Este conjunto possui números negativos, positivos e o zero. Escolheremos x e y inteiros de modo que $f = ax + by$ seja o menor inteiro positivo pertencente ao Conjunto A. Iremos mostrar que $f \mid a$ e $f \mid b$. Suponhamos por absurdo que $f \nmid a$, assim pelo algoritmo da divisão de Euclides existem os inteiros q e r tais que $a = qf + r$ com $0 < r < f$. Mas, $r = a - qf = a - q(ax + by) = (1 - qx)a + (-qy)b$. Esse resultado mostra que $r \in A$, absurdo, uma vez que $0 < r < f$ e f é o menor elemento positivo do conjunto A. Dessa forma, concluímos que $f \mid a$. De maneira análoga, mostra-se que $f \mid b$.
Sendo d o máximo divisor comum de a e b, existem inteiros q_1 e q_2, tais que $a = q_1 d$ e $b = q_2 d$, logo, $f = ax + by = q_1 dx + q_2 dy = d(q_1 x + q_2 y)$, o que implica que $d \mid f$. Dessa forma, temos que $d \leq f$ (ambos positivos) e como $d < f$ é absurdo, uma vez que $d = (a, b)$, concluímos que $d = f = ax + by$.

□

Vale ressaltar que a recíproca do teorema anterior não é válida, vamos ilustrar isso com um contra-exemplo. De fato, $5(-2) + 3(4) = 2$, porém o $(5, 3) = 1 \neq 2$.

Teorema 2.6. *Se $(a, b) = d$, então* $\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$.

Demonstração: Suponhamos por absurdo que $\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = f > 1$. Pelo teorema 2.5, existem $x, y \in \mathbb{Z}$ tais que $\dfrac{a}{d}x + \dfrac{b}{d}y = f$. Multiplicando a última igualdade por d, obtemos $ax + by = df$, o que implica que $(a, b) = df > d$, absurdo. Portanto, $\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$.

□

Exemplo 2.6. *Como* $(12, 18) = 6$, *temos que* $\left(\frac{12}{6}, \frac{18}{6}\right) = 1$.

2.6 O Teorema Fundamental da Aritmética

Definição 2.4. *Um número* $n \in \mathbb{Z}, n \geq 2$ *é primo se possui apenas dois divisores inteiro positivo, 1 e ele mesmo. Caso contrário, definimos* n *como sendo composto.*

Teorema 2.7. *Todo número inteiro positivo* $n > 1$ *ou é primo ou se escreve de modo único (a menos da ordem dos fatores) como uma multiplicação de fatores primos.*

Demonstração: Se $n = 2$ não há nada para provar, pois 2 é um número primo. Seja $n > 2$, suponhamos o resultado válido para todo inteiro positivo menor do que n e vamos provar que vale para n. Se n for primo, a propriedade estará demonstrada. Suponhamos, então que n seja composto. Assim, existem números inteiros positivos n_1 e n_2 tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese, existem números primos $p_1 p_2 \cdots p_k$ e $q_1 q_2 \cdots q_l$ tais que $n_1 = p_1 p_2 \cdots p_k$ e $n_2 = q_1 q_2 \cdots q_l$. Portanto, $n = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_l$. Provaremos, agora, a unicidade. Suponha que tenhamos $n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$, onde os p_i e os q_j são números primos. Como $p_1 \mid q_1 q_2 \cdots q_l$ ele divide pelo menos um dos fatores q_j. Sem perda de generalidade podemos supor que $p_1 \mid q_1$. Como p_1 e q_1 são ambos primos, concluímos que $p_1 = q_1$. Assim, $\frac{n}{p_1} = p_2 \cdots p_k = q_2 \cdots q_l$. Dessa forma, $1 < \frac{n}{p_1} < n$, mas a hipótese nos afirma que essas fatorações são idênticas a menos da ordem e, portanto, $k = l$.

□

Teorema 2.8. *Dados dois inteiros positivos* a, b *que possuem fatorações*

$$a = \prod_{i=1}^{j} p_i^{\alpha_i}, \;\; b = \prod_{i=1}^{k} p_i^{\beta_i}$$

então

$$(a, b) = \prod_{i=1}^{l} p_i^{c_i}$$

onde $c_i = min\{\alpha_i, \beta_i\}, \;\; i \in \mathbb{Z}_+$.

Demonstração: Para que um produto de fatores primos seja um divisor comum é necessário que nenhum expoente c_i de p_i seja superior a α_i e nem a β_i. Entretanto, queremos o maior dos divisores positivos, logo, para isso, tomaremos c_i, o menor número entre α_i e β_i.

□

Problema 2.3. *Mostre que a sequência de números primos é infinita.*

Solução: Suponhamos, por absurdo, que a sequência dos números primos é finita, seja $p_1, p_2, \ldots, p_k$ todos os números primos. Consideremos o número $n = p_1 p_2 \cdots p_k + 1$. Note que o número n não é divisível por nenhum $p_j,\ j = 1, 2, \ldots, k$ da nossa lista, pois se isso acontecesse $p_j \mid 1$, o que seria absurdo. Além disso, $n > p_j$, logo pelo Teorema Fundamental da Aritmética, ou n é primo ou é composto por um produto de números primos, isso implica na existência de um primo que não está em nossa lista. Portanto, a sequência de números primos deve ser infinita.

Proposição 2.4. *Sejam m, n números inteiros positivos tais que $(m, n) = 1$. Então se d é um divisor positivo de mn, existe um único par de números inteiros a, b divisores de m e n, respectivamente, tais que $d = ab$. Reciprocamente, se a e b são divisores positivos de m e n, respectivamente, então $d = ab$ é um divisor positivo de mn.*

Demonstração: Utilizando o Teorema Fundamental da Aritmética, escreveremos m e n em suas formas fatoradas. Assim,

$$m = p_1^{m_1} p_2^{m_2} \cdots p_j^{m_j} \text{ e } n = q_1^{n_1} q_2^{n_2} \cdots q_k^{n_k}.$$

Note que $p_r \neq q_s$, $r = 1, 2, \ldots, j$ e $s = 1, 2, \ldots, k$, pois o $(m, n) = 1$. Logo, a fatoração do produto mn será,

$$mn = p_1^{m_1} p_2^{m_2} \cdots p_j^{m_j} q_1^{n_1} q_2^{n_2} \cdots q_k^{n_k}.$$

Desta forma, se $d > 0$, $d \mid mn$, então

$$d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_j} q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k},$$

com, $0 \leq \alpha_r \leq m_r,\ r = 1, 2, \ldots, j \text{ e } 0 \leq \beta_s \leq n_s,\ s = 1, 2, \ldots, k.$
Definimos

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_j} \text{ e } b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k}.$$

É fácil ver que $(a, b) = 1$ e $ab = d$.
Vamos mostrar a recíproca, para isso, consideremos $a, b > 0$ divisores de m e n, respectivamente. Assim,

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_j},\ 0 \leq \alpha_r \leq m_r,\ r = 1, 2, \ldots, j$$

e

$$b = q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k},\ 0 \leq \beta_s \leq n_s,\ s = 1, 2, \ldots, k.$$

Portanto, fica evidente que o número,

$$d = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_j^{\alpha_j} q_1^{\beta_1} q_2^{\beta_2} \cdots q_k^{\beta_k}.$$

é tal que $d \mid mn$.

$\square$

Exemplo 2.7. *Sendo $m = 45$ e $n = 56$, temos que $(45, 56) = 1$. Um divisor positivo d de $45 \cdot 56 = 2520$ pode ser expresso por $d = 2^a \cdot 3^b \cdot 5^c \cdot 7^d$, com $a = 0, 1, 2, 3$, $b = 0, 1, 2$, $c = 0, 1$ e $d = 0, 1$. Tomando $d_1 = 3^b \cdot 5^c$ e $d_2 = 2^a \cdot 7^d$, temos que $d_1 \mid m$ e $d_2 \mid n$. Em particular, se $d = 5 \cdot 2^3 = 40$, temos que $d \mid 2520$, onde $d_1 = 5 \mid 45$ e $d_2 = 2^3 \mid 56$.*

2.7 Parte inteira de um número real

Definição 2.5. *A parte inteira de um número real x é o maior inteiro que não é maior do que x. A parte inteira de x será denotado por $\lfloor x \rfloor$.*

Definição 2.6. *A parte fracionária de x será denotado por $\{x\}$ e definido por $\{x\} = x - \lfloor x \rfloor$.*

Teorema 2.9. *Sejam x e y números reais, então*
(a) $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$.
(b) $\lfloor x + m \rfloor = \lfloor x \rfloor + m$, $m \in \mathbb{Z}$.
(c) $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x + y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.
(d) $\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor$, se $m \in \mathbb{Z}_+$.
(e) se $n, a \in \mathbb{Z}_+$, $a \leq n$, então $\left\lfloor \frac{n}{a} \right\rfloor$ é o número de inteiros entre $1, 2, \ldots, n$ que são divisíveis por a.

Demonstração: Os itens (a) e (b) são consequências imediatas da definição de parte inteira de um número real.
Parte (c):

$$\begin{aligned}
\lfloor x \rfloor + \lfloor y \rfloor &\leq \lfloor x \rfloor + \lfloor y \rfloor + \lfloor \{x\} + \{y\} \rfloor \\
&= \lfloor \lfloor x \rfloor + \lfloor y \rfloor + \{x\} + \{y\} \rfloor \\
&= \lfloor x + y \rfloor.
\end{aligned}$$

Como $\{x\} + \{y\} < 2$ temos que $\lfloor \{x\} + \{y\} \rfloor \leq 1$. Assim,

$$\begin{aligned}
\lfloor x + y \rfloor &= \lfloor x \rfloor + \lfloor y \rfloor + \lfloor \{x\} + \{y\} \rfloor \\
&\leq \lfloor x \rfloor + \lfloor y \rfloor + 1.
\end{aligned}$$

Parte (d): Seja $\lfloor x \rfloor = qm + r$, com $0 \leq r < m$. Assim,

$$\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor q + \frac{r}{m} \right\rfloor = q.$$

Como, $0 \leq \{x\} < 1$, temos

$$q = q + \left\lfloor \frac{r + \{x\}}{m} \right\rfloor = \left\lfloor \frac{qm + r + \{x\}}{m} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor + \{x\}}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor.$$

Parte (e): Sejam $a, 2a, ..., ka$ todos os inteiros positivos menor do que ou igual a n que são divisíveis por a. Assim,

$$\begin{aligned} ka \leq n < (k+1)a &\implies k \leq \frac{n}{a} < k + 1 \\ &\implies k = \left\lfloor \frac{n}{a} \right\rfloor. \end{aligned}$$

□

2.8 Sequências numéricas

Uma sequência de números reais é uma função que associa a cada número inteiro positivo n, um número real x_n. O número x_n será denominado o n-ésimo termo da sequência. Para indicar uma sequência utilizamos $(x_n)_{n \in \mathbb{Z}_+}$, ou simplesmente (x_n).

A seguir, definiremos o que vem a ser o limite de uma sequência numérica.

Definição 2.7. *Dizemos que o* $\lim\limits_{n \to \infty} x_n = L$ *se* $\forall \epsilon > 0$, $\exists\ N_0 \in \mathbb{Z}_+$ *tal que* $n > N_0$ *implica* $|x_n - L| < \epsilon$.

É importante salientar que $|x_n - L| < \epsilon$ se, somente se, $L - \epsilon < x_n < L + \epsilon$. O $|x_n - L| < \epsilon$ significa que a distância de x_n ao número positivo L é sempre inferior a ϵ. Essa ideia é de extrema importância na demonstração de alguns teoremas nessa parte da matemática.

Definição 2.8. *Se o* $\lim\limits_{n \to \infty} x_n = L$*, dizemos que* (x_n) *é convergente. Caso contrário, a sequência será divergente.*

Exemplo 2.8. *A sequência* $x_n = \dfrac{1}{n}$ *é convergente, pois* $\lim\limits_{n \to \infty} x_n = 0$*. De fato, dado* $\epsilon > 0$ *queremos que* $|x_n - 0| < \epsilon$*. Tomemos* $n > \dfrac{1}{\epsilon}$*, assim, uma vez fixado* $N_0 \in \mathbb{Z}_+$ *tal que* $N_0 > \dfrac{1}{\epsilon}$*, temos* $|x_n - 0| < \epsilon$*, para* $n > N_0$.

Definição 2.9. *Dizemos que o* $\lim\limits_{n \to \infty} x_n = \infty$ *se* $\forall A \in \mathbb{R}$, $\exists\ N_0 \in \mathbb{Z}_+$ *tal que* $n > N_0$ *implica* $x_n > A$.

Definição 2.10. *Dizemos que o* $\lim_{n\to\infty} x_n = -\infty$ *se* $\forall A \in \mathbb{R}$, $\exists\ N_0 \in \mathbb{Z}_+$ *tal que* $n > N_0$ *implica* $x_n < A$.

As definições 2.9 e 2.10, nos dizem que a sequência x_n é divergente. Uma sequência também será divergente se, o $\lim_{n\to\infty} x_n$ não existir.

Definição 2.11. *Uma sequência* (x_n) *é limitada superiormente se existir um número* A *tal que* $x_n \leq A$, $\forall n \in \mathbb{Z}_+$ *e, será limitada inferiormente se existir um número* A' *tal que* $x_n \geq A'$, $\forall n \in \mathbb{Z}_+$. *Além disso, dizemos que* (x_n) *é limitada se for ao mesmo tempo, limitada inferiormente e superiormente.*

Teorema 2.10. *Se* (x_n) *é uma sequência convergente, então* (x_n) *é limitada.*

Demonstração: Seja o $\lim_{n\to\infty} x_n = L$. Tomando $\epsilon = 1$, temos que $\exists\ N \in \mathbb{Z}_+$ tal que $n > N$ *implica* $|x_n - L| < 1$. Sejam x, y o maior e o menor, respectivamente, elemento do conjunto $X = \{x_1, x_2, \ldots, x_N, L-1, L+1\}$. Todos os termos da sequência x_n estão contidos no intervalo $I = [x, y]$. Portanto, x_n é limitada.

$\square$

Exemplo 2.9. *A sequência* $x_n = n$ *não é convergente, pois não é limitada.*

Definição 2.12. *Dizemos que uma sequência* (x_n) *será monótona*
(1) crescente: se $x_n < x_{n+1}$.
(2) decrescente: se $x_n > x_{n+1}$.
(3) não-decrescente: se $x_n \leq x_{n+1}$.
(4) não-crescente: se $x_n \geq x_{n+1}$.

Definição 2.13. *Dado um conjunto* $X \subset \mathbb{R}$ *limitado superiormente e não-vazio. Dizemos que um número* $y \in \mathbb{R}$ *é o supremo de* X *quando* y *é a menor das cotas superiores. Mais precisamente,* y *será o supremo de* X *quando*
(1) $\forall x \in X$, *tem-se* $x \leq y$;
(2) se $b < y$ *então existe* $x \in X$ *tal que* $b < x$.
O supremo do conjunto X *será denotado por* $y = sup\ X$.

Teorema 2.11. *Se* (x_n) *é uma sequência monótona e limitada, então* (x_n) *é convergente.*

Demonstração: Sem perda de generalidade, suponhamos a sequência (x_n) monótona não-decrescente e limitada. Assim, o conjunto $X = \{x_1, x_2, \ldots, x_n, \ldots\}$ possui um supremo. Seja $x = sup\ X$, afirmamos que o $\lim_{n\to\infty} x_n = x$. De fato, dado $\epsilon > 0$, o número $x - \epsilon$ não é cota superior de X. Logo, deve existir um $k \in \mathbb{Z}_+$ tal que $x - \epsilon < x_k \leq x$. Portanto, $n > k$ implica em $x - \epsilon < x_k \leq x_n < x + \epsilon$, dessa forma, $\lim_{n\to\infty} x_n = x$.

□

Exemplo 2.10. *A sequência* $x_n = \dfrac{1}{n}$ *é convergente. De fato,* $x_n > x_{n+1}$*, logo a sequência* x_n *é monótona decrescente, portanto, monótona. Além disso,* $0 \leq x_n \leq 1,\ \forall n \in \mathbb{Z}_+$*. Portanto, pelo teorema 2.11,* x_n *é convergente.*

Teorema 2.12. *Se* (x_n) *e* (y_n) *são sequências convergentes, então*
(a) $\lim\limits_{n\to\infty}(x_n + y_n) = \lim\limits_{n\to\infty} x_n + \lim\limits_{n\to\infty} y_n$.
(b) $\lim\limits_{n\to\infty} x_n y_n = \lim\limits_{n\to\infty} x_n \cdot \lim\limits_{n\to\infty} y_n$.
(c) $\lim\limits_{n\to\infty} \dfrac{1}{y_n} = \dfrac{1}{\lim\limits_{n\to\infty} y_n},\ \lim\limits_{n\to\infty} y_n \neq 0$.
(d) $\lim\limits_{n\to\infty} \dfrac{x_n}{y_n} = \dfrac{\lim\limits_{n\to\infty} x_n}{\lim\limits_{n\to\infty} y_n},\ \lim\limits_{n\to\infty} y_n \neq 0$.

Demonstração: Sejam o $\lim\limits_{n\to\infty} x_n = L_1$ *e* $\lim\limits_{n\to\infty} y_n = L_2$.
Parte (a): Se o $\lim\limits_{n\to\infty} x_n = L_1$, então $\forall \epsilon > 0,\ \exists N_1 \in \mathbb{Z}_+$ tal que $n > N_1 \implies |x_n - L_1| < \epsilon/2$. De maneira análoga, $\exists N_2 \in \mathbb{Z}_+$ tal que $n > N_2 \implies |y_n - L_2| < \epsilon/2$. Seja $N = máx\{N_1, N_2\}$. Assim, $n > N \implies n > N_1\ e\ n > N_2$. Logo, $|(x_n + y_n) - (L_1 + L_2)| = |(x_n - L_1) + (y_n - L_2)| \leq |x_n - L_1| + |y_n - L_2| < \epsilon/2 + \epsilon/2 = \epsilon$. Portanto, $\lim\limits_{n\to\infty}(x_n + y_n) = \lim\limits_{n\to\infty} x_n + \lim\limits_{n\to\infty} y_n$.
Parte (b): Primeiramente, pelo teorema 2.10, $x_n \leq k,\ \forall n \in \mathbb{Z}_+,\ k \in \mathbb{R}$. Agora, se o $\lim\limits_{n\to\infty} x_n = L_1$, então $\forall \epsilon > 0,\ \exists N_1 \in \mathbb{Z}_+$ tal que $n > N_1 \implies |x_n - L_1| < \epsilon/2|L_2|$. De maneira análoga, $\exists N_2 \in \mathbb{Z}_+$ tal que $n > N_2 \implies |y_n - L_2| < \epsilon/2k$. Seja $N = máx\{N_1, N_2\}$. Assim, $n > N \implies n > N_1\ e\ n > N_2$. Logo, $|x_n y_n - L_1 L_2| = |x_n y_n - x_n L_2 + x_n L_2 - L_1 L_2| \leq |x_n y_n - x_n L_2| + |x_n L_2 - L_1 L_2| \leq |x_n| \cdot |y_n - L_2| + |L_2| \cdot |x_n - L_1| < \epsilon$. Portanto, $\lim\limits_{n\to\infty} x_n y_n = \lim\limits_{n\to\infty} x_n \cdot \lim\limits_{n\to\infty} y_n$.
Parte (c): Como $\lim\limits_{n\to\infty} y_n = L_2 \neq 0$, $\exists N_1 \in \mathbb{Z}_+$ tal que $|y_n| > \dfrac{|L_2|}{2},\ n > N_1$. Também, dado $\epsilon > 0, \exists N_2 \in \mathbb{Z}_+$ tal que $|y_n - L_2| < \dfrac{|L_2|^2\epsilon}{2},\ se\ n > N_2$. Tomando, $N = máx\{N_1, N_2\}$, obtemos

$$\left|\frac{1}{y_n} - \frac{1}{L_2}\right| = \frac{|y_n - L_2|}{|y_n| \cdot |L_2|} \leq \frac{2|y_n - L_2|}{|L_2|^2} < \epsilon,\ se\ n > N.$$

Portanto, $\lim\limits_{n\to\infty} \dfrac{1}{y_n} = \dfrac{1}{\lim\limits_{n\to\infty} y_n}$.
Parte (d): A demonstração dessa parte segue diretamente, aplicando as partes (b) e (c).

□

Teorema 2.13. *(Teorema do Confronto) Sejam* $(x_n), (y_n)$ *e* (z_n) *sequências tais que* $x_n \leq y_n \leq z_n$*, para todo* $n \in \mathbb{Z}_+$*. Se o* $\lim\limits_{n\to\infty} x_n = \lim\limits_{n\to\infty} z_n = L$*, então* $\lim\limits_{n\to\infty} y_n = L$*.*

Demonstração: Se o $\lim_{n\to\infty} x_n = L$, então $\forall\epsilon > 0$, $\exists N_1 \in \mathbb{Z}_+$ tal que $n > N_1 \implies L-\epsilon < x_n < L+\epsilon$. De maneira análoga, $\exists N_2 \in \mathbb{Z}_+$ tal que $n > N_2 \implies L-\epsilon < z_n < L+\epsilon$. Tomamos $N = máx\{N_1, N_2\}$. Assim, para $n > N$ temos que $L - \epsilon < x_n < L + \epsilon$ e $L - \epsilon < z_n < L + \epsilon$. Logo, $L - \epsilon < x_n \leq y_n \leq z_n < L + \epsilon$. Portanto, $\lim_{n\to\infty} y_n = L$.

□

Problema 2.4. *Mostre que a sequência* $x_n = \dfrac{n!}{n^n}$ *é convergente.*

Solução: Note que a sequência $x_n = \dfrac{n!}{n^n} \geq 0, \ \forall n \in \mathbb{Z}_+$. Por outro lado, temos que

$$\frac{n!}{n^n} = \prod_{k=1}^{n} \frac{k}{n}.$$

Como $\dfrac{k}{n} \leq 1, \ k \leq n, \ k \in \mathbb{Z}_+$, temos

$$\frac{n!}{n^n} = \prod_{k=1}^{n} \frac{k}{n} \leq \frac{1}{n}.$$

Sejam $y_n = 0$ e $z_n = \dfrac{1}{n}, \forall n \in \mathbb{Z}_+$. Assim, $\lim_{n\to\infty} y_n = 0$ e $\lim_{n\to\infty} z_n = 0$. Como $y_n \leq x_n \leq z_n$, concluímos pelo teorema do confronto que $\lim_{n\to\infty} x_n = 0$ e, portanto, a sequência x_n é convergente.

2.9 Séries numéricas

Dada uma sequência (x_k), chamamos de série a soma $\sum_{k=1}^{\infty} x_k = x_1 + x_2 + x_3 + \cdots + x_k + \cdots$.

Definição 2.14. *Seja a série* $\sum_{k=1}^{\infty} x_k$. *Definimos como soma parcial desta série o* $\sum_{k=1}^{n} x_k$.

Se o $\lim_{n\to\infty} \sum_{k=1}^{n} x_k$ existir, diremos que a série é convergente. Caso contrário, diremos que a série é divergente.

Teorema 2.14. *(Teste da comparação) Sejam* $\sum_{k=1}^{\infty} x_k$ *e* $\sum_{k=1}^{\infty} y_k$ *séries de temos não-negativos. Se existem* $x > 0$ *e* $N_1 \in \mathbb{Z}_+$ *tais que* $x_k \leq x y_k, \forall k > N_1$, *então a convergência de* $\sum_{k=1}^{\infty} y_k$ *implica a de* $\sum_{k=1}^{\infty} x_k$, *enquanto a divergência de* $\sum_{k=1}^{\infty} x_k$ *implica a de* $\sum_{k=1}^{\infty} y_k$.

Demonstração: Suponhamos, sem perda de generalidade, que $x_k \leq xy_k, \forall k \in \mathbb{Z}_+$. Dessa forma, as somas parciais s_k *e* t_k, de $\sum_{k=1}^{\infty} x_k$ e $\sum_{k=1}^{\infty} y_k$, respectivamente, formam sequências não-decrescentes tais que $s_k \leq xt_k$, $\forall k \in \mathbb{Z}_+$. Como $x > 0$, (t_k) sendo limitada implicará em (s_k) limitada e (s_k) ilimitada implicará em (t_k) ilimitada, pois $\dfrac{s_k}{x} \leq t_k$.

□

Problema 2.5. *Mostre que a série* $\sum_{n=1}^{\infty} \left(\dfrac{n}{3n+1}\right)^n$ *é convergente.*

Solução: Sejam $x_n = \left(\dfrac{n}{3n+1}\right)^n$ e $y_n = \left(\dfrac{n}{3n}\right)^n$, duas séries de termos positivos, assim, $x_n \leq y_n$ o que implica em $\sum_{n=1}^{\infty} x_n \leq \sum_{n=1}^{\infty} y_n$. Mas,

$$\sum_{n=1}^{\infty} y_n = \sum_{n=1}^{\infty} \left(\frac{1}{3}\right)^n = \frac{1}{2}.$$

Logo, o $\sum_{n=1}^{\infty} y_n$ é convergente. Portanto, pelo teste da comparação, o $\sum_{n=1}^{\infty} x_n$ também será convergente.

Definição 2.15. *Uma série* $\sum_{k=1}^{\infty} x_k$ *diz-se absolutamente convergente quando* $\sum_{k=1}^{\infty} |x_k|$ *converge.*

Teorema 2.15. *Toda série absolutamente convergente é convergente.*

Demonstração: Como $0 \leq x_k + |x_k| \leq 2|x_k|$ e como $2\sum_{k=1}^{\infty} |x_k|$ é convergente, pelo teorema 2.14, o $\sum_{k=1}^{\infty}(x_k + |x_k|)$ converge por ser séries de termos positivos. Assim, $\sum_{k=1}^{\infty} x_k = \sum_{k=1}^{\infty}(x_k + |x_k|) - \sum_{k=1}^{\infty} |x_k|$ que é uma diferença de séries convergentes, o que implica que o $\sum_{k=1}^{\infty} x_k$ é convergente.

□

Teorema 2.16. *(Teste da Integral) Suponha que f seja uma função contínua, positiva e decrescente no intervalo $[1, \infty)$ e seja $y_n = f(n)$. Então, a série $\sum_{n=1}^{\infty} y_n$ é convergente se, somente se, a integral imprópria $\int_1^{\infty} f(x)dx$ converge. Ou seja,*

1) se $\int_1^{\infty} f(x)dx$ converge, então $\sum_{n=1}^{\infty} y_n$ converge.

2) Se $\int_1^{\infty} f(x)dx$ diverge, então $\sum_{n=1}^{\infty} y_n$.

Demonstração: Sejam f uma função decrescente no intervalo $[1,\infty)$ e $y_i, i = 2, 3, \ldots, n$ as áreas dos retângulos de base igual a 1 e altura y_i. Isto é, $f(i) = y_i$. Assim, comparando as áreas desses retângulos com as área sob o gráfico de $y = f(x)$ de 1 até n,temos

$$y_2 + y_3 + \cdots + y_n \leq \int_1^n f(x)dx. \tag{2.1}$$

Note que, ao invés de começarmos na extremidade $i = 2$, começarmos na extremidade $i = 1$, teremos

$$\int_1^n f(x)dx \leq y_1 + y_2 + y_3 + \cdots + y_{n-1}. \tag{2.2}$$

1) Se $\displaystyle\int_1^\infty f(x)dx$ for convergente, então (2.1) fornece

$$\sum_{i=2}^n y_i \leq \int_1^n f(x)dx \leq \int_1^\infty f(x)dx$$

uma vez que $f(x) \geq 0$. Portanto,

$$s_n = y_1 + \sum_{i=2}^n y_i \leq y_1 + \int_1^\infty f(x)dx = A.$$

Como $s_n \leq A$ para todo $n \in \mathbb{Z}_+$, temos que, a sequência $(s_n)_{n\,\in\,\mathbb{Z}_+}$ é limitada superiormente. Além disso,

$$s_{n+1} = s_n + y_{n+1} \geq s_n,$$

uma vez que $f(n+1) = y_{n+1} \leq 0$. Logo, a sequência $(s_n)_{n\,\in\,\mathbb{Z}_+}$ é crescente e limitada, mas, pelo teorema 2.11 temos que $(s_n)_{n\,\in\,\mathbb{Z}_+}$ é convergente. Portanto, $\displaystyle\sum_{n=1}^\infty y_n$ é convergente.

2) Se $\displaystyle\int_1^\infty f(x)dx$ for divergente, então $\displaystyle\int_1^n f(x)dx$ tende para infinito quando n tende para infinito, pois $f(x) \leq 0$. Entretanto, (2.2) nos dá que

$$\int_1^n f(x)dx \leq \sum_{i=1}^{n-1} y_i = s_{n-1}$$

e, dessa forma, s_{n-1} tende para infinito. Isso implica que s_n tende para infinito. Portanto, $\displaystyle\sum_{n=1}^\infty y_n$ é divergente.

□

Problema 2.6. *Mostre que a série* $\displaystyle\sum_{n=1}^\infty \frac{1}{n^5}$ *é convergente.*

Solução: Vamos mostrar que $\displaystyle\int_1^\infty \frac{1}{x^5}dx$ é convergente e, isso implicará, pelo Teste da Integral, na convergência da série $\displaystyle\sum_{n=1}^\infty \frac{1}{n^5}$.

$$\int_1^\infty \frac{1}{x^5}dx = \lim_{m\to\infty}\int_1^m \frac{1}{x^5}dx = \lim_{m\to\infty} \frac{-1}{4x^4}\bigg|_1^m = \lim_{m\to\infty}\frac{-1}{4m^4} + \frac{1}{4} = \frac{1}{4}.$$

2.10 Série de Taylor

Vamos supor que uma dada função f pode ser representada por uma série da seguinte forma:

$$f(x) = \sum_{k=0}^{\infty} y_k(x-x_0)^k = y_0 + y_1(x-x_0) + y_2(x-x_0)^3 + \cdots + y_k(x-x_0)^k + \cdots . \quad (2.3)$$

Fazendo $x = x_0$ na expressão anterior, obtemos $f(x_0) = y_0$.

Agora, efetuando a primeira derivada na função (2.3), temos

$$f'(x) = y_1 + 2y_2(x-x_0) + 3y_3(x-x_0)^2 + \cdots + ky_k(x-x_0)^{k-1} + \cdots . \quad (2.4)$$

Substituindo, $x = x_0$ na expressão (2.4), encontraremos $f'(x_0) = y_1$.

Efetuando mais uma derivada na função (2.4), obtemos

$$f''(x) = 2y_2 + 3\cdot 2y_3(x-x_0) + 4\cdot 3y_4(x-x_0)^2 + \cdots + k(k-1)y_k(x-x_0)^{k-2} + \cdots . \quad (2.5)$$

Fazendo a substituição $x = x_0$, encontraremos $f''(x_0) = 2y_2$.

Vamos aplicar esse procedimento mais uma vez. Assim, a derivada da função (2.5) ficará

$$f'''(x) = 3\cdot 2y_3 + 4\cdot 3\cdot 2y_4(x-x_0) + \cdots + k(k-1)(k-2)y_k(x-x_0)^{k-3} + \cdots . \quad (2.6)$$

E, fazendo a substituição de $x = x_0$ em (2.6), obteremos $f'''(x_0) = 3\cdot 2y_3 = 3!y_3$.

Se continuarmos a efetuar as derivadas e substituir $x = x_0$ em todas elas, obteremos

$$f^{(k)}(x_0) = k!y_k \implies y_k = \frac{f^{(k)}(x_0)}{k!}.$$

Agora, fazendo uso do resultado anterior para y_k e substituindo em (2.3), ficaremos com

$$f(x) = \sum_{k=0}^{\infty} \frac{f^{(k)}(x_0)}{k!}(x-x_0)^k.$$

A expressão que acabamos de encontrar é denominada de série de Taylor da função f em torno de x_0. Fazendo $x_0 = 0$ na série Taylor, temos

$$f(x) = \sum_{k=0}^{\infty} \frac{f^{(k)}(0)}{k!}x^k.$$

Esse caso particular, onde tomamos $x_0 = 0$ é conhecido como a série de Maclaurin.

Exemplo 2.11. *Para ilustrar a utilização deste último resultado, vamos encontrar a série de Maclaurin para a função $f(x) = \sin x$.*

Fazendo uso da série de Maclaurin, temos

$$\begin{aligned}
\sin x &= \sin 0 + \frac{\cos 0}{1!}x + \frac{-\sin 0}{2!}x^2 + \frac{-\cos 0}{3!}x^3 + \frac{\sin 0}{4!}x^4 + \frac{\cos 0}{5!}x^5 + \frac{-\sin 0}{6!}x^6 + \cdots \\
&= x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots \\
&= \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k+1}}{(2k+1)!}.
\end{aligned}$$

3 Funções Aritméticas

A teoria dos números, assim como outros ramos da matemática, se preocupa com o estudo de sequências de números reais ou complexos. Na teoria dos números essas sequências são chamadas de funções aritméticas.

Definição 3.1. *Uma função de valores reais ou complexos definida no conjunto dos inteiros positivos é chamada de função aritmética ou função da teoria dos números.*

Neste trabalho apresentaremos várias funções aritméticas que desempenham um papel importante no estudo das propriedades de divisibilidade de números inteiros e na distribuição de números primos.

Iniciaremos com duas importantes funções aritméticas, a função μ de Möbius e a função φ de Euler.

3.1 A função μ de Möbius

Definição 3.2. *A função μ de Möbius é definida da seguinte forma:*

$$\mu(n) = \begin{cases} 1, \ se \ n = 1, \\ (-1)^k, se \ n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}, \ com \ a_1 = a_2 = \ldots = a_k = 1, \\ 0, \ se \ algum \ dos \ a_i > 1, \ i = 1, 2, 3, \ldots, k. \end{cases}$$

A seguir apresentaremos uma pequena tabela de valores da função μ de Möbius.

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

Proposição 3.1. *Se $n \in \mathbb{Z}_+$, então $\mu(2n) = 0$ ou $\mu(2n+2) = 0$.*

Demonstração: Sendo $n \in \mathbb{Z}_+$, n pode ser par ou ímpar. Dessa forma, temos dois casos a considerar.

1) Caso: $n = 2k, k \in \mathbb{Z}_+$.

$$\mu(2n) = \mu(2 \cdot 2k) = \mu(2^2 k) = 0.$$

2) Caso: $n = 2k+1, k \in \mathbb{Z}_+$.

$$\mu(2n+2) = \mu(2 \cdot (2k+1) + 2) = \mu(4k+4) = \mu(2^2(k+1)) = 0.$$

□

Problema 3.1. *Seja $n \in \mathbb{Z}_+$, mostre que*

$$\prod_{k=0}^{3} \mu(n+k) = 0.$$

Solução: Se $n = 1$, temos que a propriedade é verdadeira, pois,

$$\prod_{k=0}^{3} \mu(n+k) = \mu(1)\mu(2)\mu(3)\mu(4) = 0$$

visto que $\mu(4) = 0$.

Suponhamos então, que a propriedade é válida para algum $n \in \mathbb{Z}_+$, ou seja, $\prod_{k=0}^{3} \mu(n+k) = 0$. Assim,

$$\prod_{k=0}^{3} \mu(n+1+k) = \mu(n+1)\mu(n+2)\mu(n+3)\mu(n+4).$$

Se na hipótese de indução $\mu(n) \neq 0$ a prova está concluída. Suponhamos então que $\mu(n) = 0$. Assim, n pode ser par ou ímpar. Mas, em qualquer caso dois dos fatores de $\mu(n+1)\mu(n+2)\mu(n+3)\mu(n+4)$ serão números pares consecutivos e, pela proposição 3.1, em um dos dois a função μ assume o valor nulo, fazendo com que o produto $\mu(n+1)\mu(n+2)\mu(n+3)\mu(n+4) = 0$.

A função de Möbius surge em diferentes contextos no campo da teoria dos números. Uma de suas propriedades fundamentais é a fórmula notavelmente simples para a soma dos divisores $\sum_{d|n} \mu(d)$ estendida sobre os divisores positivos de n.

Teorema 3.1. *Se $n \in \mathbb{Z}_+$, então*

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

Demonstração: Se $n = 1$ temos que $\sum_{d|1} \mu(d) = \left\lfloor \frac{1}{1} \right\rfloor = 1 = \mu(1)$. Suponhamos, então, que $n > 1$, assim, utilizando o Teorema Fundamental da Aritmética, podemos escrever n da seguinte forma, $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$. Na soma $\sum_{d|n} \mu(d)$ os únicos termos diferente de zero provém de $d = 1$ e dos divisores de n que são produtos de distintos números primos. Logo,

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

$\square$

Proposição 3.2. *Se $n \in \mathbb{Z}_+$, então*

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

Demostração: Utilizando o teorema 3.1 temos que

$$\sum_{d_1|1} \mu(d_1) + \sum_{d_2|2} \mu(d_2) + \cdots + \sum_{d_n|n} \mu(d_n) = 1.$$

Como 1 é divisor de cada inteiro pertencente ao conjunto $\{1, 2, 3, \cdots, n\}$, $\mu(1)$ aparecerá n vezes na soma acima. O número 2, sendo divisor de $\left\lfloor \frac{n}{2} \right\rfloor$ destes inteiros, $\mu(2)$ ocorrerá $\left\lfloor \frac{n}{2} \right\rfloor$. Seguindo este raciocínio, sendo d divisor de $\left\lfloor \frac{n}{d} \right\rfloor$ dos inteiros de 1 a n, $\mu(d)$ ocorrerá $\left\lfloor \frac{n}{d} \right\rfloor$ vezes nesta soma. Dessa forma,

$$\sum_{k=1}^{n} \left(\sum_{d_k|k} \mu(d_k) \right) = \mu(1) \left\lfloor \frac{n}{1} \right\rfloor + \mu(2) \left\lfloor \frac{n}{2} \right\rfloor + \cdots + \mu(n) \left\lfloor \frac{n}{n} \right\rfloor.$$

Portanto,

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

$\square$

Antes de enunciarmos o próximo teorema, exibiremos a solução de um caso particular do mesmo.

Problema 3.2. *Mostre que*

$$\sum_{d|30=2\cdot3\cdot5} \frac{\mu(d)}{d} = \prod_{i=1}^{3} \left(1 - \frac{1}{p_i}\right)$$

onde p_i é um divisor primo de 30.

Solução: Vamos desenvolver o lado esquerdo da equação acima. Assim, teremos

$$\begin{aligned}
\sum_{d|30=2\cdot3\cdot5} &= \frac{\mu(1)}{1}+\frac{\mu(2)}{2}+\frac{\mu(3)}{3}+\frac{\mu(5)}{5}+\frac{\mu(6)}{6}+\frac{\mu(10)}{10}+\frac{\mu(15)}{15}+\frac{\mu(30)}{30}\\
&= \frac{1}{1}-\frac{1}{2}-\frac{1}{3}-\frac{1}{5}+\frac{1}{6}+\frac{1}{10}+\frac{1}{15}-\frac{1}{30}\\
&= 1-\frac{1}{2}-\frac{1}{3}-\frac{1}{5}+\frac{1}{2\cdot3}+\frac{1}{2\cdot5}+\frac{1}{3\cdot5}-\frac{1}{2\cdot3\cdot5}.
\end{aligned}$$

Façamos agora o desenvolvimento do produtório do lado direito. Logo,

$$\begin{aligned}
\prod_{i=1}^{3}\left(1-\frac{1}{p_i}\right) &= \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\\
&= \left(1-\frac{1}{2}-\frac{1}{3}+\frac{1}{2\cdot3}\right)\left(1-\frac{1}{5}\right)\\
&= 1-\frac{1}{2}-\frac{1}{3}-\frac{1}{5}+\frac{1}{2\cdot3}+\frac{1}{2\cdot5}+\frac{1}{3\cdot5}-\frac{1}{2\cdot3\cdot5}.
\end{aligned}$$

Portanto, com o desenvolvimento de ambos os lados, concluímos que

$$\sum_{d|30=2\cdot3\cdot5}\frac{\mu(d)}{d}=\prod_{i=1}^{3}\left(1-\frac{1}{p_i}\right).$$

Agora, no nosso próximo teorema, mostraremos que esse resultado é válido para todo inteiro positivo.

Teorema 3.2. *Se $n \in \mathbb{Z}_+$, então*

$$\sum_{d|n}\frac{\mu(d)}{d}=\begin{cases}1, \textit{se } n = 1,\\ \displaystyle\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right), \textit{se } n > 1,\end{cases}$$

onde p_i é um divisor primo de n.

Demonstração: Se $n = 1$ temos que, $\displaystyle\sum_{d|1}\frac{\mu(d)}{d} = \mu(1) = 1$. Suponhamos então que $n > 1$, podemos escrever $n = p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$, para cada inteiro positivo $i = 1, 2, \cdots, k$, temos

$$\frac{\mu(p_i)}{p_i}=\frac{-1}{p_i}$$

para cada par de números i, j inteiros positivos distintos,

$$\frac{\mu(p_ip_j)}{p_ip_j}=\frac{1}{p_ip_j}$$

para cada terna de números i, j, k inteiros positivos distintos,

$$\frac{\mu(p_ip_jp_k)}{p_ip_jp_k}=\frac{-1}{p_ip_jp_k}$$

e assim por diante, o que resultará em

$$\begin{aligned}\sum_{d|n}\frac{\mu(d)}{d} &= 1-\sum\frac{1}{p_i}+\sum\frac{1}{p_ip_j}-\cdots+(-1)^k\sum\frac{1}{p_ip_j\cdots p_k}\\ &=\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right).\end{aligned}$$

□

3.2 A função φ de Euler

Definição 3.3. *Seja $n \in \mathbb{Z}_+$, a função φ de Euler é definida como o número de inteiros positivos coprimos com n e que não excedem n.*

Podemos sintetizar essa definição com o auxílio do símbolo de somatório, por meio da seguinte expressão:

$$\varphi(n)=\sum_{k=1}^{n}{}' \, 1, \tag{3.1}$$

onde o símbolo $'$ indica que essa soma é estendida sobre os números inteiros positivos k que são coprimos com n.

Aqui está uma pequena tabela de valores da função φ de Euler.

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

Assim, como no caso da função μ de Möbius, temos uma fórmula simples para a soma dos divisores $\sum_{d|n}\varphi(d)$.

Antes de realizamos a prova do próximo teorema vamos apresentar um exemplo que evidencia a ideia que será usada na demonstração.

Problema 3.3. *Mostre que*

$$\sum_{d|30}\varphi(d)=30.$$

Solução: De fato, Denotaremos por S o conjunto $S=\{1,2,3,\cdots,29,30\}$. Os divisores positivos de 30 são: 1, 2, 3, 5, 6, 10, 15 e 30. Note que, o máximo divisor comum de qualquer número k, $1\leqslant k\leqslant 30$ e 30, é um dos divisores de 30. Separando os elementos do conjunto S em conjuntos $A(d) = \{k : (k, 30) = d\}$, onde d é um dos divisores positivo de 30. Assim, teremos,

$$\begin{aligned}
&A(1) = \{1, 7, 11, 13, 17, 19, 23, 29\},\\
&A(2) = \{2, 4, 8, 14, 16, 22, 26, 28\},\\
&A(3) = \{3, 9, 21, 27\},\\
&A(5) = \{5, 25\},\\
&A(6) = \{6, 12, 18, 24\},\\
&A(10) = \{10, 20\},\\
&A(15) = \{15\},\\
&A(30) = \{30\},
\end{aligned}$$

Note que esses conjuntos são todos disjuntos e que a união deles forma o conjunto S. Na tabela a seguir temos a quantidade de elementos de cada conjunto $A(d)$.

Conjunto $A(d)$	**Quantidade de elementos em** $A(d)$
$A(1)$	$8 = \varphi(30) = \varphi(30/1)$
$A(2)$	$8 = \varphi(15) = \varphi(30/2)$
$A(3)$	$4 = \varphi(10) = \varphi(30/3)$
$A(5)$	$2 = \varphi(6) = \varphi(30/5)$
$A(6)$	$4 = \varphi(5) = \varphi(30/6)$
$A(10)$	$2 = \varphi(3) = \varphi(30/10)$
$A(15)$	$1 = \varphi(2) = \varphi(30/15)$
$A(30)$	$1 = \varphi(1) = \varphi(30/30)$

Note que se d é um divisor de 30, $\dfrac{30}{d}$ também é. Assim , mostramos que

$$\sum_{d|30} \varphi(d) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(5) + \varphi(6) + \varphi(10) + \varphi(15) + \varphi(30) = 30.$$

Teorema 3.3. *Se $n \in \mathbb{Z}_+$, então*

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

Demonstração: Vamos denotar por S o conjunto $\{1, 2, 3, \ldots, n\}$. Iremos distribuir os elementos de S em conjuntos disjuntos da seguinte maneira: para cada divisor $d > 0$ de S, seja o conjunto

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

Ou seja, $A(d)$ contém os elementos de S que posuem o máximo divisor comum d com n. O conjunto $A(d)$ forma uma coleção disjunta cuja união é S. Portanto, se $n'(d)$ denota o número de inteiros em $A(d)$, temos

$$\sum_{d|n} n'(d) = n. \tag{3.2}$$

Mas, pelo teorema 2.6, se $(k, n) = d$, então $\left(\frac{k}{d}, \frac{n}{d}\right) = 1$, e $0 < k \leq n$ se e somente se $0 < \frac{k}{d} \leq \frac{n}{d}$. Portanto, se deixarmos $q = \frac{k}{d}$, haverá uma correspondência biunívoca entre os elemento de $A(d)$ e os números inteiros q satisfazendo $0 < q \leq \frac{n}{d}$, com $\left(q, \frac{n}{d}\right) = 1$. A quantidade de elementos q é $\varphi\left(\frac{n}{d}\right)$. Logo $n'(d) = \varphi\left(\frac{n}{d}\right)$ e (3.2) torna-se

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

Mas, isso é equivalente ao $\sum_{d|n} \varphi(d) = n$, porque quando d percorre todos os divisores de n o mesmo ocorre com $\frac{n}{d}$. Isso completa a demonstração.

□

Na próxima seção apresentaremos um resultado que relaciona as funções φ de Euler e μ de Möbius.

3.3 Uma expressão que relaciona as funções φ e μ

A função φ de Euler está relacionada com a função μ de Möbius por meio da seguinte fórmula:

Teorema 3.4. *Se $n \in \mathbb{Z}_+$, então*

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

Demonstração: A soma (3.1) da definição da função φ pode ser expressa da seguinte forma:

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

Essa mudança é possível, pois, se $k \in \{1, 2, 3, \ldots, n\}$, então $\left\lfloor \frac{1}{(n, k)} \right\rfloor = 1$ se $(n, k) = 1$ e 0 se $(n, k) > 1$.

Agora, usando o teorema 3.1 com n substituído por (n, k), obtemos

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

Mas, se $d \mid (n,k)$ então $d \mid n$ e $d \mid k$, o que nos permite escrever a expressão anterior como,

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

Para um divisor fixo d de n, devemos somar 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 e somente se $1 \leq q \leq \frac{n}{d}$. Logo a igualdade acima para $\varphi(n)$ pode ser reescrita como,

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

Isso termina a prova do teorema.

Exemplo 3.1.

$$\begin{aligned}\varphi(30) &= \sum_{d|30} \mu(d) \frac{30}{d} \\ &= \mu(1)\frac{30}{1} + \mu(2)\frac{30}{2} + \mu(3)\frac{30}{3} + \mu(5)\frac{30}{5} = \mu(6)\frac{30}{6} + \mu(10)\frac{30}{10} + \mu(15)\frac{30}{15} + \mu(30)\frac{30}{30} \\ &= 30 - 15 - 10 - 6 + 5 + 3 + 2 - 1 \\ &= 8.\end{aligned}$$

□

Provamos nos teoremas 3.3 e 3.4 duas propriedades que representam uma situação particular da Fórmula de Inversão de Möbius, assunto que será abordado no próximo capítulo.

3.4 Uma fórmula de produto para a função φ

A soma para $\varphi(n)$ no Teorema 3.3 pode ser expressa como um produto, estendido sobre os distintos números primos divisores de n.

Teorema 3.5. *Se $n \in \mathbb{Z}_+$, então*

$$\varphi(n) = n \prod_{\substack{p \ primo \\ p|n}} \left(1 - \frac{1}{p}\right). \tag{3.3}$$

Demonstração: Para $n = 1$ o produto é vazio, pois não existe nenhum número primo que divide o número 1. Nesse caso, atribuímos ao produto o valor 1.

Suponhamos, então, que $n > 1$ e sejam $p_1, p_2, \cdots, p_r$ distintos divisores primos de n. Assim, produto pode ser escrito como

$$\begin{aligned} \prod_{\substack{p \text{ primo} \\ p|n}} \left(1 - \frac{1}{p}\right) &= \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) \\ &= 1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \sum \frac{1}{p_i p_j p_k} + \cdots + \sum \frac{(-1)^r}{p_1 p_2 \cdots p_r}. \end{aligned} \tag{3.4}$$

À direita, em um termo como o $\sum \frac{1}{p_i p_j p_k}$, entende-se que consideramos todos os possíveis $p_i p_j p_k$ de três fatores de primos distintos em cada vez. Observe que cada termo à direita de (3.4) tem a forma $\pm\frac{1}{d}$, em que d é um divisor de n que é 1 ou um produto de primos distintos. O numerador ± 1 é exatamente $\mu(d)$. Como $\mu(d) = 0$ se d possui um fator p_i com expoente maior do que 1, vemos que a soma em (3.4) é a mesma que

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

Isso prova o teorema.

□

Exemplo 3.2.

$$\varphi(30) = 30 \prod_{\substack{p \text{ primo} \\ p|30}} \left(1 - \frac{1}{p}\right) = 30\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = 8.$$

Muitas propriedades de $\varphi(n)$ podem ser facilmente deduzidas a partir desta fórmula do produto. Algumas destas propriedades estão listadas no próximo teorema.

Teorema 3.6. *A função φ de Euler goza das seguintes propriedades:*

(a) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$, *para p primo e $\alpha \geq 1$.*
(b) $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$, *onde $d = (m, n)$.*
(c) $\varphi(mn) = \varphi(m)\varphi(n)$, *se $(m, n) = 1$.*
(d) Se $a \mid b$ então $\varphi(a) \mid \varphi(b)$.
(e) $\varphi(n)$ é par para $n \in \mathbb{Z}$, $n \geq 3$. Além disso, se n tem r fatores primos distintos ímpares, então $2^r \mid \varphi(n)$.

Demonstração: Parte (a): Da definição da função φ temos que $\varphi(p^\alpha)$ conta a quantidade de inteiros coprimos com p^α menores do que p^α. Mas, os números que não são coprimos com p^α pertence ao conjunto $A = \{p, 2p, 3p, \dots, p^{\alpha-1}p\}$. Logo, os inteiros que são coprimos com p^α menores que p^α será dado por $p^\alpha - p^{\alpha-1}$. Portanto, $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

Parte (b): Sabemos do teorema 3.4 que

$$\varphi(n) = n \prod_{\substack{p \ primo \\ p|n}} \left(1 - \frac{1}{p}\right).$$

Assim,

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

Observe que cada divisor primo de mn será um divisor primo de m ou de n. Além disso, os primos que dividem m e n também dividem o (m, n). Portanto,

$$\begin{aligned}
\frac{\varphi(mn)}{mn} &= \prod_{p|mn} \left(1 - \frac{1}{p}\right) \\
&= \frac{\prod_{p|m} \left(1 - \frac{1}{p}\right) \prod_{p|n} \left(1 - \frac{1}{p}\right)}{\prod_{p|(m,n)} \left(1 - \frac{1}{p}\right)} \\
&= \frac{\frac{\varphi(m)}{m} \frac{\varphi(n)}{n}}{\frac{\varphi(d)}{d}} \\
&= \frac{\varphi(m)}{m} \frac{\varphi(n)}{n} \frac{d}{\varphi(d)}.
\end{aligned}$$

Logo,

$$\frac{\varphi(mn)}{mn} = \frac{\varphi(m)}{m} \frac{\varphi(n)}{n} \frac{d}{\varphi(d)}.$$

Portanto,

$$\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}.$$

Parte (c): Se o $(m, n) = d = 1$, pelo item (b) temos

$$\varphi(mn) = \varphi(m)\varphi(n)\frac{1}{\varphi(1)} = \varphi(m)\varphi(n)\frac{1}{1} = \varphi(m)\varphi(n).$$

Parte (d): Como $a \mid b$ $\exists c \in \mathbb{Z}$ tal que $b = ac$, com $1 \leq c \leq b$. Se $c = b$, então $a = 1$ a parte (d) está trivialmente satisfeita. Suponhamos que $c < b$. Por (b) temos

$$\varphi(b) = \varphi(ac) = \varphi(a)\varphi(c)\frac{d}{\varphi(d)} = d\varphi(a)\frac{\varphi(c)}{\varphi(d)}, \tag{3.5}$$

onde $d = (a, c)$. Agora o resultado segue por indução em b. Para $b = 1$ o resultado é trivial, pois, se $a = 1$, então $a = c = 1$. Logo,

$$\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)\frac{1}{\varphi(1)} \implies 1 = 1.$$

Suponhamos, então, que a propriedade vale para todos os inteiros menores do que b. Assim, ela vale para c, dessa forma $\varphi(d) \mid \varphi(c)$ desde que $d \mid c$, mas isso acontece, visto que $d = (a, c)$. Portanto, o lado direito de (3.5) é múltiplo de $\varphi(a)$ o que significa que $\varphi(a) \mid \varphi(b)$. Isso termina a prova da parte (d).
Parte (e): Se $n = 2^\alpha, \alpha \geq 2$, pela parte (a), temos

$$\varphi(2^\alpha) = 2^\alpha - 2^{\alpha-1} = 2(2^{\alpha-1} - 2^{\alpha-2}).$$

O que mostra que $\varphi(n)$ é par. Agora, se n possui ao menos um número primo ímpar em sua decomposição, escrevemos

$$\begin{aligned}
\varphi(n) &= n\prod_{p|n}\left(1 - \frac{1}{p}\right) \\
&= n\prod_{p|n}\frac{p-1}{p} \\
&= \frac{n}{\prod_{p|n} p}\prod_{p|n}(p-1) \\
&= n'\prod_{p|n}(p-1).
\end{aligned}$$

onde n' é um número inteiro. Do lado direito, o produtório multiplicado por n' é igual a $\varphi(n)$, assim, $\varphi(n)$ é par, pois, sendo p primo, $p = 2$ ou p é ímpar, logo, como n tem pelo menos um um primo ímpar, faz com que $(p-1)$ seja par. Além disso, cada primo ímpar p contribui com um fator 2 para esse produto. Portanto, se n tem r fatores primos ímpares distintos em sua decomposição, então $2^r \mid \varphi(n)$.

□

Problema 3.4. *Mostre que se n é um inteiro positivo, então*

$$\varphi(2n) = \begin{cases} \varphi(n), \text{ se } n \text{ é ímpar} \\ 2\varphi(n), \text{ se } n \text{ é par.} \end{cases}$$

Solução: Se n for um inteiro positivo ímpar então $(2, n) = 1$, pela parte (c) do Teorema 3.6 temos

$$\varphi(2n) = \varphi(2)\varphi(n) = 1 \cdot \varphi(n) = \varphi(n)$$

Por outro lado, se n for um inteiro positivo par então pode ser escrito como $n = 2^{\alpha} \cdot a$, onde a é um número natural ímpar e α é um natural qualquer.
Assim, $(2, n) = (2, 2^{\alpha} \cdot a) = (2, 0) = 2$. Logo, pela parte (d) do Teorema 3.6, temos

$$\varphi(2n) = \varphi(2)\varphi(n)\frac{2}{\varphi(2)} = 2\varphi(n).$$

Problema 3.5. *Mostre que existem infinitos inteiros m para os quais $10 \mid \varphi(m)$.*

Solução: Note que $11 \mid 11k$, $k \in \mathbb{Z}_+ - \{0\}$. Assim, utilizando a parte (d) do teorema 3.6 temos,

$$11 \mid 11k \Rightarrow \varphi(11) \mid \varphi(11k) \Rightarrow 10 \mid \varphi(11k)$$

Logo, tomando $m = 11k$ fica evidente que existem infinitos números inteiros m tais que $10 \mid \varphi(m)$.

Proposição 3.3. *Se $n \in \mathbb{Z}_+$ e p um número primo, então*

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

Demonstração: Utilizando a parte (a) do teorema 3.6, temos

$$\begin{aligned} \sum_{k=1}^{n} \varphi(p^k) &= \sum_{k=1}^{n} p^k - p^{k-1} \\ &= (p-1) + (p^2 - p) + (p^3 - p^2) + \cdots + (p^{n-1} - p^{n-2}) + (p^n - p^{n-1}) \\ &= p^n - 1. \end{aligned}$$

□

Exemplo 3.3.

$$\sum_{k=1}^{10} \varphi(2^k) = 2^{10} - 1 = 1023.$$

4 O Produto de Dirichlet de Funções Aritméticas

No teorema 3.4, provamos que

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

A soma à direita é de um tipo que ocorre frequentemente na teoria dos números. Essas somas possui o seguinte formato

$$\sum_{d|n} f(d)g\left(\frac{n}{d}\right),$$

onde f e g são funções aritméticas. Como essas somas aparecem com frequência no estudo da teoria dos números, vale a pena estudar algumas propriedades que elas têm em comum. Somas como esta surgem naturalmente na teoria das séries de Dirichlet. Dessa forma, é de extrema importância tratarmos essas somas como um tipo de multiplicação para funções aritméticas.

Definição 4.1. *Se f e g são funções aritméticas, definimos o produto de Dirichlet (ou convolução de Dirichlet) como sendo a função h definida pela expressão*

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

Notação: Usaremos $f * g$ para a função h e $(f * g)(n)$ para $h(n)$. Além disso, o símbolo N será usado para as funções aritméticas na qual $N(n) = n$ para todo $n \in \mathbb{Z}_+$. Nesta notação, o Teorema 3.4 pode ser reescrito da seguinte forma

$$\varphi = \mu * N.$$

O próximo teorema descreve propriedades algébricas do produto de Dirichlet. Essas propriedades serão muito importantes para a demonstração de alguns teoremas que serão abordados adiante neste capítulo.

Teorema 4.1. *O produto de Dirichlet é comutativo e associativo, ou seja, para quaisquer funções aritméticas f, g, h temos*

$$f * g = g * f$$

$$(f * g) * h = f * (g * h).$$

Demonstração: Para provar a comutatividade, observe que, a definição de $f * g$ também pode ser expressa da seguinte forma

$$\begin{aligned}(f * g)(n) &= \sum_{d|n} f(d) g\left(\frac{n}{d}\right) \\ &= \sum_{a \cdot b = n} f(a) g(b) \\ &= \sum_{b \cdot a = n} g(b) f(a)\end{aligned}$$

onde a e b variam sobre todos os números inteiros positivos cujo produto é igual a n. Dessa forma, a propriedade comutativa fica evidente.
Provaremos agora a associatividade do produto de Dirichlet.

$$\begin{aligned}((f * g) * h)(n) &= \sum_{i \cdot c = n} (f * g)(i) \cdot h(c) \\ &= \sum_{i \cdot c = n} \left(\sum_{a \cdot b = i} f(a) \cdot g(b) \right) \cdot h(c) \\ &= \sum_{i \cdot c = n} \sum_{a \cdot b = i} f(a) \cdot g(b) \cdot h(c) \\ &= \sum_{a \cdot b \cdot c = n} f(a) \cdot g(b) \cdot h(c).\end{aligned}$$

De maneira análoga mostra-se que $(f * (g * h))(n) = \sum_{a \cdot b \cdot c = n} f(a) \cdot g(b) \cdot h(c)$.

□

Definição 4.2. *A função aritmética definida por*

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

$\forall n \in \mathbb{Z}_+$, *é denominada de função identidade.*

Teorema 4.2. *Qualquer que seja a função aritmética f, temos que $I * f = f * I = f$.*

Demonstração: Temos que

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

uma vez que $\left\lfloor \dfrac{d}{n} \right\rfloor = 0$, se $d < n$ e $\left\lfloor \dfrac{d}{n} \right\rfloor = 1$, se $d = n$.

□

4.1 A inversa de Dirichlet

Teorema 4.3. *Se f é uma função aritmética com $f(1) \neq 0$ existe uma única função aritmética f^{-1}, denominada de inversa de Dirichlet da função f, tal que*

$$f * f^{-1} = f^{-1} * f = I.$$

Além disso, f^{-1} é definida recursivamente pelas seguintes fórmulas

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

e para $n > 1$

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

Demonstração: Dada a função f, mostraremos 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 solucionar a equação

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

Note que a equação anterior pode ser reescrita da seguinte forma

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

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

Mas, como $f(1) \neq 0$ existe uma e, somente uma solução, que será expressa por $f^{-1}(1) = \dfrac{1}{f(1)}$.

Suponhamos agora, que os valores da função $f^{-1}(k)$ foram determinados unicamente para todos os $k < n$. Assim, temos que resolver a equação $(f * f^{-1})(n) = I(n)$, ou seja,

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

Entretanto, a equação acima pode ser reescrita da seguinte forma

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

Se os valores de $f^{-1}(d)$ são conhecidos para todos os divisores $d < n$, existe um valor determinado exclusivamente para $f^{-1}(n)$, a saber, que será dado por

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

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

sendo $f(1) \neq 0$. Dessa forma, demostramos por indução a existência e a unicidade da função f^{-1}.

□

Se f e g são funções aritméticas tais que $f(1) \neq 0$ e $g(1) \neq 0$, então $(f*g)(1) \neq 0$. De fato, $(f * g)(1) = \sum_{d|1} f(d)g\left(\frac{1}{d}\right) = f(1)g(1) \neq 0$. Esse fato, juntamente com os teoremas 4.1, 4.2 e 4.3, nos diz, na linguagem da teoria dos grupos, que o conjunto das funções aritméticas f com $f(1) \neq 0$ forma um grupo abeliano em relação à operação $*$, sendo o elemento de neutro desta operação, a função I.

Definição 4.3. *Definimos a função unitária u, como sendo a função aritmética de modo que $u(n) = 1, \ \forall n \in \mathbb{Z}_+$.*

Com a definição 4.2, o teorema 3.1 poderá ser reescrito como $\sum_{d|n} \mu(d) = I(n)$. Agora, utilizando a notação do produto de Dirichlet e a definição 4.3, essa propriedade torna-se

$$\sum_{d|n} \mu(d)u\left(\frac{n}{d}\right) = I(n)$$

$$\mu * u = I.$$

Assim u e μ são inversas de Dirichlet uma da outra. Ou seja,

$$u = \mu^{-1}$$

e

$$\mu = u^{-1}.$$

Essa simples propriedade da função de Möbius, juntamente com a propriedade associativa da multiplicação de Dirichlet, será capaz de fornecer uma prova simples para o nosso próximo teorema, que é conhecido como a fórmula da inversão de Möbius.

4.2 Fórmula da inversão de Möbius

Teorema 4.4. *Seja g uma função aritmética qualquer. A equação*

$$f(n) = \sum_{d|n} g(d) \tag{4.1}$$

implica

$$g(n) = \sum_{d|n} f(d)\mu\left(\frac{n}{d}\right). \tag{4.2}$$

Reciprocamente, (4.2) implica em (4.1).

Demonstração: A equação 4.1 pode ser reescrita utilizando a multiplicação de Dirichlet da seguinte forma, $f = g * u$. Multiplicando ambos os membros desta igualdade por μ obtemos

$$\begin{aligned} f * \mu &= (g * u) * \mu \\ &= g * (u * \mu) \\ &= g * I \\ &= g. \end{aligned}$$

Isso mostra que a equação 4.1 implica em 4.2.
De maneira análoga, a equação 4.2 pode ser reescrita utilizando o produto de Dirichlet como $g = f * \mu$ e multiplicando ambos os lados desta ultima equação por u e aplicando as propriedades da multiplicação de Dirichlet, chegaremos a conclusão que 4.2 implica em 4.1.

□

4.3 A função Λ de Mangoldt

O matemático alemão Von Mangoldt, exibiu uma rigorosa demonstração de uma fórmula explícita para $\psi(x) = \sum_{n \leq x} \Lambda(n)$ envolvendo uma soma sobre os zeros não triviais da função Zeta de Riemann. Essa foi uma parte importante da primeira prova do teorema dos números primos. Dessa forma, esta função desempenha um importante papel na distribuição dos números primos. A seguir, definiremos a função Λ de Mangoldt.

Definição 4.4. *Para todo número $n \in \mathbb{Z}_+$, definimos a função Λ de Mangoldt como sendo*

$$\Lambda(n) = \begin{cases} \log p, & se\ n = p^m,\ para\ algum\ primo\ p\ e\ algum\ número\ m \in \mathbb{Z}_+. \\ 0, & caso\ contrário. \end{cases}$$

Abaixo está uma pequena tabela com alguns valores da função Λ de Mangoldt.

$n:$	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

A demonstração do teorema a seguir evidencia o surgimento natural dessa função a partir do Teorema Fundamental da Aritmética.

Teorema 4.5. *Se $n \in \mathbb{Z}_+$, então*

$$\log n = \sum_{d|n} \Lambda(d). \tag{4.3}$$

Demonstração: Se $n = 1$, temos que a propriedade é verdadeira, pois,

$$\log 1 = 0 = \Lambda(1) = \sum_{d|1} \Lambda(d).$$

Suponhamos então, que $n > 1$. Assim, n pode ser escrito, utilizando o Teorema Fundamental da Aritmética, como

$$n = \prod_{i=1}^{k} p_i^{a_i}.$$

Aplicando o logaritmo em ambos os lados da igualdade acima, temos

$$\log n = \sum_{i=1}^{k} a_i \log p_i.$$

No somatório à direita da equação (4.3), os únicos termos que não são zeros advém dos divisores $d = p_i^m$, com $m = 1, 2, \ldots, a_i$ e $i = 1, 2, \ldots, k$. Logo,

$$\begin{aligned} \sum_{d|n} \Lambda(d) &= \sum_{i=1}^{k} \sum_{m=1}^{a_i} \Lambda(p_i^m) \\ &= \sum_{i=1}^{k} \sum_{m=1}^{a_i} \log p_i \\ &= \sum_{i=1}^{k} a_i \log p_i \\ &= \log n. \end{aligned}$$

□

Exemplo 4.1.

$$\begin{aligned} \sum_{d|12} &= \Lambda(1) + \Lambda(2) + \Lambda(3) + \Lambda(4) + \Lambda(6) + \Lambda(12) \\ &= 0 + \log 2 + \log 3 + \log 2 + 0 + 0 \\ &= \log 2 \cdot 3 \cdot 2 \\ &= \log 12. \end{aligned}$$

No próximo teorema utilizaremos a fórmula da inversão de Möbius na expressão $\Lambda(n)$ em função dos logaritmos.

Teorema 4.6. *Se $n \in \mathbb{Z}_+$, então*

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

Demonstração: Vamos utilizar a fórmula da inversão de Möbius na expressão 4.3. Faremos a inversão trocando g pela função Λ e a função f pela função log. Assim, obtemos

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

Mas, os conjuntos $A = \{d \in \mathbb{Z}_+ : d \mid n\}$ e $B = \left\{\frac{n}{d} \in \mathbb{Z}_+ : d \mid n\right\}$ são iguais, logo, podemos escrever a última igualdade como

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

Note que $\log nI(n) = 0$ para qualquer inteiro positivo, pois, se $n = 1$ então $\log 1 = 0$ e, se $n > 1$ então $I(n) = 0$. Portanto,

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

$\square$

4.4 Funções multiplicativas

Definição 4.5. *Uma função aritmética f é denominada multiplicativa se f não é identicamente igual a zero e se, $f(mn) = f(m)f(n)$, sendo $(m, n) = 1$, com $m, n \in \mathbb{Z}_+$.*

Definição 4.6. *Uma função aritmética f é denominada completamente multiplicativa se $\forall m, n \in \mathbb{Z}_+$, temos $f(mn) = f(m)f(n)$.*

Exemplo 4.2. *A função $f_\alpha(n) = n^\alpha$, onde α é um número real ou complexo fixado é completamente multiplicativa. De fato, dados m, n números inteiros positivos quaisquer e α un número real fixo, temos que*

$$f_\alpha(mn) = (mn)^\alpha = m^\alpha n^\alpha = f_\alpha(m)f_\alpha(n).$$

Em particular, a função unitária $u = f_0$ também é completamente multiplicativa. Denotamos a função f_α por N^α e esta é conhecida como função potência.

Problema 4.1. *Prove que a função identidade $I(n) = \left\lfloor \frac{1}{n} \right\rfloor$ é completamente multiplicativa.*

Solução: Para justificar esse exemplo temos que considerar três casos.
1) Caso: $m = 1$ e $n = 1$.

$$I(mn) = \left\lfloor \frac{1}{mn} \right\rfloor = 1 = 1 \cdot 1 = \left\lfloor \frac{1}{m} \right\rfloor \cdot \left\lfloor \frac{1}{n} \right\rfloor = I(m)I(n).$$

2) Caso: um dos dois igual a 1 e o outro maior que 1. Sem perda de generalidade, consideremos $m = 1$ e $n > 1$.

$$I(mn) = \left\lfloor \frac{1}{mn} \right\rfloor = 0 = 1 \cdot 0 = \left\lfloor \frac{1}{m} \right\rfloor \cdot \left\lfloor \frac{1}{n} \right\rfloor = I(m)I(n).$$

3) Caso: $m, n > 1$.

$$I(mn) = \left\lfloor \frac{1}{mn} \right\rfloor = 0 = 0 \cdot 0 = \left\lfloor \frac{1}{m} \right\rfloor \cdot \left\lfloor \frac{1}{n} \right\rfloor = I(m)I(n).$$

Portanto, em qualquer caso, teremos $I(mn) = I(m)I(n)$.

Problema 4.2. *Mostre que a função μ de Möbius é multiplicativa, mas não é completamente multiplicativa.*

Solução: Sejam m, n dois números inteiros positivos tais que $(m, n) = 1$. Se m ou n tem um fator primo com o expoente maior que 1, o produto mn, também terá esse mesmo fator primo. Logo, pela definição da função μ, $\mu(mn) = 0$ e $\mu(m)\mu(n) = 0$. Assim, $\mu(mn) = \mu(m)\mu(n)$. Suponhamos então, que nem m e nem n tenham nenhum fator primo com expoente maior que 1. Dessa forma, pelo teorema fundamental da aritmética, $m = p_1p_2 \cdots p_j$ e $n = q_1q_2 \cdots q_k$, onde esses primos são todos distintos. Logo,

$$\mu(mn) = \mu(p_1p_2 \cdots p_j q_1 q_2 \cdots q_k) = (-1)^{j+k} = (-1)^j(-1)^k = \mu(m)\mu(n).$$

Entretanto, a função μ não é multiplicativa, pois $\mu(4) = 0 \neq \mu(2)\mu(2) = 1$.

Problema 4.3. *Mostre que a função φ de Euler é multiplicativa, mas não é completamente multiplicativa.*

Solução: A prova de que φ é multiplicativa está na parte (c) do teorema 3.6. Mas, essa função não é completamente multiplicativa, pois $\varphi(9) = 6 \neq \varphi(3)\varphi(3) = 4$.

Exemplo 4.3. *Se f e g são funções multiplicativas, então o produto usual fg de duas funções aritméticas f e g definido por*

$$(fg)(m) = f(m)g(m)$$

E o quociente usual f/g, definido por,

$$\left(\frac{f}{g}\right)(m) = \frac{f(m)}{g(m)},\ g(m) \neq 0$$

são multiplicativos.
Se f e g são funções completamente multiplicativas, também serão completamente multiplicativos, fg e f/g.

A seguir, vamos enunciar e demonstrar dois teoremas que são comuns a todas as funções multiplicativas.

Teorema 4.7. *Se f é uma função multiplicativa, então $f(1) = 1$.*

Demonstração: Primeiro, note que $(m, 1) = 1, \forall m \in \mathbb{Z}_+$. Logo, $f(m) = f(1 \cdot m) = f(1)f(m)$. Como a função f não é identicamente igual a zero, segue que $f(m) \neq 0$ para algum $m \in \mathbb{Z}_+$. Logo,

$$f(1) = \frac{f(m)}{f(m)} = 1.$$

□

Note que esse teorema inviabiliza a possibilidade da função Λ de Mangoldt ser multiplicativa, visto que, $\Lambda(1) = 0$.

Teorema 4.8. *Seja f uma função com $f(1) = 1$, então*
a) f é multiplicativa se, e somente se,

$$f\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} f(p_i^{a_i})$$

Para todo número primo p_i e todo número inteiro positivo a_i.
b) Se f é multiplicativa, então f é completamente multiplicativa se, e somente se,

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

Para todo número primo p_i e todo número inteiro positivo a_i.

Demonstração: Parte (a): ($\Rightarrow$) Se $n = 1$, temos que $f(1) = f(1 \cdot 1) = f(1)f(1) = 1$. Suponhamos então, que a propriedade seja válida para algum inteiro positivo k, ou seja, $f\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} f(p_i^{a_i})$. Mostraremos que a validade de k implica na validade de $k+1$. Logo,

$$f\left(\prod_{i=1}^{k+1} p_i^{a_i}\right) = f\left(\prod_{i=1}^{k} p_i^{a_i} \cdot p_{k+1}^{a_{k+1}}\right) = f\left(\prod_{i=1}^{k} p_i^{a_i}\right) f(p_{k+1}^{a_{k+1}}) = \prod_{i=1}^{k} f(p_i^{a_i}) f(p_{k+1}^{a_{k+1}}) = \prod_{i=1}^{k+1} f(p_i^{a_i}).$$

($\Leftarrow$) Como $f\left(\prod_{i=1}^{k} p_i^{a_i}\right) = \prod_{i=1}^{k} f(p_i^{a_i})$, temos da definição 4.5 que f é uma função multiplicativa.
Parte (b):($\Rightarrow$) Se a função f é completamente multiplicativa então $f(mn) = f(m)f(n)$ para quaisquer inteiros positivos m, n. Assim,

$$f(p^a) = f(pp^{a-1}) = f(p)f(p^{a-1}) = f(p)f(pp^{a-2}) = \ldots = f(p)f(p)\cdots f(p) = f(p)^a.$$

($\Leftarrow$) Como $f(p^a) = f(p)^a$, pela definição 4.6, a função f é completamente multiplicativa.

$\square$

Teorema 4.9. *Se f é uma função multiplicativa, então*

$$F(m) = \sum_{d|m} f(d)$$

também é multiplicativa.

Demonstração: Sejam m, n inteiros positivos tais que $(m, n) = 1$. Utilizando a definição da função F, temos que

$$F(mn) = \sum_{d|mn} f(d).$$

Sendo $(m, n) = 1$, pela proposição 2.4, temos que todo divisor d de mn pode ser escrito de modo único como um produto de dois inteiros positivos a, b, isto é, $d = ab$, onde $a \mid m$, $b \mid n$ e $(a, b) = 1$. Dessa forma,

$$F(mn) = \sum_{d|mn} f(d) = \sum_{\substack{a|m \\ b|n}} f(ab).$$

Agora, utilizando a hipótese da função f ser multiplicativa, obtemos

$$\begin{aligned} F(mn) &= \sum_{\substack{a|m \\ b|n}} f(a)f(b) \\ &= \sum_{a|m} \sum_{b|n} f(a)f(b) \\ &= \sum_{a|m} f(a) \sum_{b|n} f(b) \\ &= F(m)F(n). \end{aligned}$$

□

4.5 Funções multiplicativas e produto de Dirichlet

Teorema 4.10. *Se f e g são funções multiplicativas, então o produto $f * g$ de Dirichlet também será multiplicativo.*

Demonstração: Sejam $h = f * g$ e m, n inteiros positivos tais que $(m, n) = 1$. Assim,

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

Agora, todo divisor d de mn, pela proposição 2.4, pode ser expresso da forma $d = ab$, onde $a \mid m$ e $b \mid n$. Além disso, $(a, b) = 1$, $\left(\frac{m}{a}, \frac{n}{b}\right) = 1$ e existe uma correspondência biunívoca entre o conjunto de produtos ab e o conjunto de divisores d de mn. Logo,

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

Isso completa a prova.

□

É importante salientar que o produto de Dirichlet para duas funções completamente multiplicativas não necessariamente será completamente multiplicativo. Mas, se modificarmos um pouquinho a demonstração anterior, conseguimos demonstrar o seguinte teorema.

Teorema 4.11. *Se g e $f * g$ são multiplicativas, então f também é multiplicativa.*

Demonstração: Suponhamos por absurdo que a função f não é multiplicativa. Seja a função $h = f * g$. Como f não é multiplicativa existem inteiros m e n, com $(m, n) = 1$, tais que $f(mn) \neq f(m)f(n)$.
Se $mn = 1$ então $f(1) \neq f(1)f(1)$ e $f(1) \neq 1$. Assim, $h(1) = f(1)g(1) = f(1) \neq 1$, mas isso é absurdo, pois contradiz a hipótese. Se $mn > 1$, suponhamos que $f(ab) = f(a)f(b)$ para todos os inteiros positivos a e b, com $(a, b) = 1$ e $ab < mn$. Argumentaremos agora, como na demonstração do teorema anterior, exceto nos termos correspondentes a $a = m$ e $b = n$ na definição de $h(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right)$. Dessa forma, temos

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

Como $f(mn) \neq f(m)f(n)$, temos que $h(mn) \neq h(m)h(n)$. Logo, h não é multiplicativa, mas isso é absurdo.
Portanto, f tem que ser multiplicativa.

□

Teorema 4.12. *Se g é uma função multiplicativa, então g^{-1} também é, e g^{-1} será a inversa de Dirichlet.*

Demonstração: A demonstração segue diretamente do teorema 4.11, uma vez que g e $g * g^{-1} = I$ são multiplicativas.

□

Os teoremas 4.10 e 4.12, juntos mostram que o conjunto das funções multiplicativas é um subgrupo de todas as funções aritméticas g, com $g(1) \neq 0$. Isso acontece porque o conjunto das funções aritméticas multiplicativas é não vazio e possui as propriedades da associativa e do fechamento, esta última decorre do teorema 4.10. Além disso, esse conjunto tem a função identidade I que será o elemento neutro da operação. Por fim, existe a inversa de Dirichlet, dada pelo teorema 4.12, essa inversa será o elemento simétrico da operação. Gozando dessas propriedades, garantimos que esse conjunto trata-se de um subgrupo de todas as funções aritméticas onde a imagem do elemento 1 pela função será não-nulo.

4.6 A inversa de funções completamente multiplicativas

Não é tão complicado determinar a inversa de Dirichlet de funções completamente multiplicativas. O próximo resultado nos diz como encontrar essa função inversa, além disso, o resultado estabelece um critério para que uma função multiplicativa seja totalmente multiplicativa.

Teorema 4.13. *Seja f uma função multiplicativa. Então f será completamente multiplicativa se, e somente se,*

$$f^{-1}(n) = \mu(n)f(n), \text{ para todo } n \in \mathbb{Z}_+.$$

Demonstração: Seja $g(n) = \mu(n)f(n)$. Se f é completamente multiplicativa, temos

$$\begin{aligned}(g * f)(n) &= \sum_{d|n} g(d)f\left(\frac{n}{d}\right)\\ &= \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right)\\ &= f(n)\sum_{d|n}\mu(d)\\ &= f(n)I(n)\\ &= I(n).\end{aligned}$$

Sendo $f(1) = 1$ e $I(n) = 0$ para $n > 1$. Portanto, $g = f^{-1}$.
Para demonstrarmos a implicação contrária assumimos que $f^{-1}(n) = \mu(n)f(n)$. Para que a função f seja completamente multiplicativa é suficiente provar que $f(p^a) = f(p)^a$, para potências de primos. A equação $f^{-1}(n) = \mu(n)f(n)$ implica que

$$\sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = 0, \text{ para todo } n > 1, \ n \in \mathbb{Z}_+.$$

Agora, consideremos $n = p^a$, mas, os divisores de $n = p^a$ são $1, p, p^2, \ldots, p^a$. Assim, temos que os únicos termos que são diferentes de zero no $\sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right)$ provém de $d = 1$ e

$d = p$. Logo,

$$\mu(1)f(1)f(p^a) + \mu(p)f(p)f(p^{a-1}) = 0,$$

a partir da qual encontramos $f(p^a) = f(p)f(p^{a-1})$. Isso implica em $f(p^a) = f(p)^a$, pois, $(p, p^{a-1}) = p \neq 1$. Portanto, f é completamente multiplicativa.

□

Problema 4.4. *Encontre a inversa da função φ de Euler.*

Solução: Sabemos que a função φ pode ser expressa pelo produto de Dirichlet, da seguinte forma: $\varphi = \mu * N$. Assim, temos que $\varphi^{-1} = \mu^{-1} * N^{-1}$. Entretanto, $N^{-1} = \mu N$ e como N é completamente multiplicativa, temos

$$\varphi^{-1} = \mu^{-1} * \mu N = u * \mu N.$$

Portanto,

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

Teorema 4.14. *Se f é uma função multiplicativa, então*

$$\sum_{d|n} \mu(d)f(d) = \prod_{\substack{p \text{ primo} \\ p|n}} (1 - f(p)).$$

Demonstração: Seja

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

Então h é uma função multiplicativa. Dessa forma, para determinar $h(n)$ basta calcular $h(p^a)$. Mas,

$$\begin{aligned} h(p^a) &= \sum_{d|p^a} \mu(d)f(d) \\ &= \mu(1)f(1) + \mu(p)f(p) \\ &= 1 - f(p) \end{aligned}$$

Portanto,

$$h(n) = \prod_{p|n} h(p^a) = \prod_{p|n} (1 - f(p)).$$

□

Problema 4.5. *Seja f uma função multiplicativa. Mostre que $\varphi^{-1}(n) = \prod_{\substack{p \text{ primo} \\ p|n}} (1 - p)$.*

Solução: Seja a função f multiplicativa, definida por $f(n) = n$. Assim, utilizando o teorema 4.14, temos

$$\varphi^{-1}(n) = \sum_{d|n} d\mu(d) = \sum_{d|n} \mu(d)f(d) = \prod_{\substack{p \text{ primo} \\ p|n}} (1 - f(p)) = \prod_{\substack{p \text{ primo} \\ p|n}} (1 - p).$$

Problema 4.6. *Seja f uma função multiplicativa. Prove que $\sum\limits_{d|n} \mu^2(d) = 2^r$, onde r é o número de fatores primos distintos de n.*

Solução: Seja a função f multiplicativa. Utilizando o teorema 4.14, temos

$$\begin{aligned}\sum_{d|n} \mu^2(d) &= \sum_{d|n} \mu(d)\mu(d) \\ &= \prod_{\substack{p \text{ primo} \\ p|n}} (1 - \mu(p)) \\ &= (1 - \mu(p_1))(1 - \mu(p_2))(1 - \mu(p_3)) \cdots (1 - \mu(p_r))\end{aligned}$$

Como pela definição da função μ, $\mu(p_i) = -1, \ i = 1, 2, 3, \ldots, r$, temos

$$\sum_{d|n} \mu^2(d) = 2 \cdot 2 \cdot 2 \cdot \ldots \cdot 2 = 2^r.$$

4.7 A função λ de Liouville

Um importante exemplo de funções completamente multiplicativas é a função de λ de Liouville, função esta, que definiremos a seguir.

Definição 4.7. *A função λ de Liouville será definida para todo $n \in \mathbb{Z}_+$ da seguinte forma*

$$\lambda(n) = \begin{cases} 1, se \ n = 1. \\ (-1)^{\sum_{i=1}^{k} a_i}, \ para \ n = \prod\limits_{i=1}^{k} p_i^{a_i}. \end{cases}$$

Da definição da função de Liouville fica evidente que ela é completamente multiplicativa. De fato, sejam $m, n \in \mathbb{Z}_+$, tais que $m = \prod\limits_{i=1}^{k} p_i^{a_i}$ e $n = \prod\limits_{j=1}^{l} q_j^{b_j}$. Assim,

$$\lambda(mn) = (-1)^{a_1 + a_2 + \cdots + a_k + b_1 + b_2 + \cdots + b_j} = (-1)^{a_1 + a_2 + \cdots + a_k} \cdot (-1)^{b_1 + b_2 + \cdots + b_j} = \lambda(m)\lambda(n).$$

Teorema 4.15. *Se $n \in \mathbb{Z}_+$, então*

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

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

Demonstração: Seja $g(n) = \sum_{d|n} \lambda(d)$. Então a função g é multiplicativa. Dessa forma, para determinar $g(n)$ precisamos calcular apenas $g(p^a)$ para potências de primos. Assim, temos

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

Portanto, se $n = \prod_{i=1}^{k} p_i^{a_i}$ teremos $g(n) = \prod_{i=1}^{k} g(p_i^{a_i})$. Se algum expoente a_i for ímpar, então $g(p_i^{a_i}) = 0$ e $g(n) = 0$. Porém, se todos os expoentes a_i forem pares, então $g(p_i^{a_i}) = 1$ para todo i e $g(n) = 1$. Portanto, $g(n) = 1$ se n for um quadrado e $g(n) = 0$ caso contrário. Para provar a segunda parte, temos

$$\lambda^{-1}(n) = \mu(n)\lambda(n) = \mu^2(n) = |\mu(n)|.$$

□

4.8 A função divisor σ_α

Definição 4.8. *Para todo número α real ou complexo e todo inteiro $n \in \mathbb{Z}_+$, a função divisor é definida por*

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

A função σ_α é multiplicativa, pois ela pode ser expressa utilizando o produto de Dirichlet de duas funções multiplicativas da seguinte forma: $\sigma_\alpha = u * N^\alpha$.
Quando $\alpha = 0$, $\sigma_0(n) = \sum_{d|n} 1$ é a função que conta o número de divisores positivos do número n. Essa função pode ser denotada por $d(n)$.
Quando $\alpha = 1$, $\sigma_1(n) = \sum_{d|n} d$ é a função que soma todos os divisores positivos do número n. Essa função pode ser denotada por $\sigma(n)$.

Proposição 4.1. *Se p é um número primo e $\alpha \in \mathbb{Z}_+$, então*

$$\sigma_\alpha(p^k) = \frac{p^{\alpha(k+1)} - 1}{p^\alpha - 1}.$$

Demonstração: Note que os divisores positivos de p^k são $1, p, p^2, \cdots, p^k$. Portanto,

$$\sigma_\alpha(p^k) = 1^\alpha + p^\alpha + p^{2\alpha} + \cdots + p^{k\alpha} = 1^\alpha \frac{(p^\alpha)^{k+1} - 1}{p^\alpha - 1} = \frac{p^{\alpha(k+1)} - 1}{p^\alpha - 1}.$$

□

Proposição 4.2. *Se p é primo e $a \in \mathbb{Z}_+ \cup \{0\}$, então $\sigma_0(p^a) = (a+1)$.*

Demonstração: Todos os divisores do número p^a são da forma p^{a_i} com $0 \leq a_i \leq a$ e $a_i \in \mathbb{Z}$. Logo, de 0 até a, temos $(a+1)$ números e, portanto, $\sigma_0(p^a) = (a+1)$.

□

Proposição 4.3. *Se $n = \prod_{i=1}^{k} p_i^{a_i}$, $n \in \mathbb{Z}_+$, então*

$$\sigma_0(n) = \prod_{i=1}^{k} (a_i + 1).$$

Demonstração: Utilizando o fato de σ_α ser multiplicativa e a proposição 4.2, temos

$$\begin{aligned}
\sigma_0(n) &= \sigma_0\left(\prod_{i=1}^{k} p_i^{a_i}\right) \\
&= \sigma_0(p_1^{a_1})\sigma_0(p_2^{a_2}) \cdots \sigma_0(p_k^{a_k}) \\
&= (a_1+1)(a_2+1)\cdots(a_k+1) \\
&= \prod_{i=1}^{k}(a_i+1).
\end{aligned}$$

□

Proposição 4.4. *Se $n = \prod_{i=1}^{k} p_i^{a_i}$, $n \in \mathbb{Z}_+$, então*

$$\sigma_1(n) = \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}.$$

Demonstração: Utilizando o fato de σ_α ser multiplicativa e a proposição 4.1, temos

$$\begin{aligned}
\sigma_1(n) &= \sigma_1\left(\prod_{i=1}^{k} p_i^{a_i}\right) \\
&= \sigma_1(p_1^{a_1})\sigma_1(p_2^{a_2}) \cdots \sigma_1(p_k^{a_k}) \\
&= \frac{p_1^{a_1+1} - 1}{p_1 - 1} \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdots \frac{p_k^{a_k+1} - 1}{p_k - 1} \\
&= \prod_{i=1}^{k} \frac{p_i^{a_i+1} - 1}{p_i - 1}.
\end{aligned}$$

□

Teorema 4.16. *Se $n \in \mathbb{Z}_+$, então*

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

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

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

□

4.9 Generalização da Multiplicação de Dirichlet

Nesta seção, F será usada para denotar uma função que assume valores reais ou complexos, definida no intervalo $(0, +\infty)$, de modo que, $F(x) = 0$ para $0 < x < 1$.

Somas da forma

$$\sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right)$$

aparecem com frequência na teoria dos números. Aqui α representa uma função aritmética qualquer. Esta soma define uma nova função G no intervalo $(0, +\infty)$ e também para $0 < x < 1$. Denotamos a função G por, $\alpha \circ F$. Portanto,

$$(\alpha \circ F)(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right).$$

Se $F(x) = 0$ para todos os x não inteiros, a restrição de F para os números inteiros é uma função aritmética e, descobrimos que

$$(\alpha \circ F)(m) = (\alpha * F)(m)$$

para todo $m \in \mathbb{Z}_+$. Dessa forma, a operação $\circ$ pode ser considerada como uma generalização da multiplicação de Dirichlet.

A operação $\circ$, em geral, não possui as propriedades comutativa e a associativa. Mas, o próximo teorema é usado para substituir a propriedade associativa.

Teorema 4.17. *(Propriedade associativa que relaciona as operações $\circ$ e $*$) Sejam α e β duas funções aritméticas quaisquer, então*

$$\alpha \circ (\beta \circ F) = (\alpha * \beta) \circ F.$$

Demonstração: Para $x > 0$, temos

$$
\begin{aligned}
[\alpha \circ (\beta \circ F)](x) &= \sum_{n \leq x} \alpha(n) \sum_{m \leq x/n} \beta(m) F\left(\frac{x}{mn}\right) \\
&= \sum_{mn \leq x} \alpha(n)\beta(m) F\left(\frac{x}{mn}\right) \\
&= \sum_{k \leq x} \left(\sum_{n|k} \alpha(n) \beta\left(\frac{k}{n}\right) \right) F\left(\frac{x}{k}\right) \\
&= \sum_{k \leq x} (\alpha * \beta)(k) F\left(\frac{x}{k}\right) \\
&= [(\alpha * \beta) \circ F](x).
\end{aligned}
$$

□

A seguir, evidenciamos que a função identidade $I(n) = \left\lfloor \frac{1}{n} \right\rfloor$ para a multiplicação de Dirichlet, também será o elemento neutro para a operação $\circ$. Dessa forma, temos

$$
\begin{aligned}
(I \circ F)(x) &= \sum_{n \leq x} I(n) F\left(\frac{x}{n}\right) \\
&= \sum_{n \leq x} \left\lfloor \frac{1}{n} \right\rfloor F\left(\frac{x}{n}\right) \\
&= F(x).
\end{aligned}
$$

Utilizaremos o resultado anterior, juntamente, com a propriedade associativa para demonstrarmos a seguinte fórmula de inversão apresentada no próximo teorema.

Teorema 4.18. *(Generalização da fórmula de inversão). Se a função α tem uma inversa de Dirichlet α^{-1}, então a equação*

$$G(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right) \tag{4.4}$$

implica

$$F(x) = \sum_{n \leq x} \alpha^{-1}(n) G\left(\frac{x}{n}\right). \tag{4.5}$$

Reciprocamente, (4.5) implica em (4.4).

Demonstração: Se $G = \alpha \circ F$, então

$$
\begin{aligned}
\alpha^{-1} \circ G &= \alpha^{-1} \circ (\alpha \circ F) \\
&= (\alpha^{-1} * \alpha) \circ F \\
&= I \circ F \\
&= F.
\end{aligned}
$$

Portanto, (4.4) implica em (4.5). A implicação contrária mostra-se de maneira análoga.

□

Agora, mostraremos um caso particular do teorema anterior.

Teorema 4.19. *(Generalização da fórmula de inversão de Möbius). Se α é uma função completamente multiplicativa, então*

$$G(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right) \; se, \; somente \; se, \; F(x) = \sum_{n \leq x} \mu(n)\alpha(n) G\left(\frac{x}{n}\right).$$

Demonstração: Pelo Teorema 4.13 temos que $\alpha^{-1}(n) = \mu(n)\alpha(n)$. Portanto, com este fato e utilizando o teorema anterior, a demonstração fica completa.

□

5 O Teorema de Ernesto Cesàro

Ernesto Cesàro foi um matemático italiano que Nasceu no dia 12 de março de 1859 na cidade de Nápolis - Itália e faleceu em 12 de setembro de 1906 em Torre Annunziata - Itália. Sua maior contribuição foi no campo da Geometria Diferencial que está descrita no livro "Lezioni di geometria intrinseca". Nesta obra, são encontradas as descrições de curvas que são conhecidas como curvas de Cesàro. No ano de 1881, Cesàro mostrou que se escolhermos, aleatoriamente, dois números inteiros positivos de modo que esses números fossem coprimos, a probabilidade disso acontecer seria igual a $\frac{6}{\pi^2}$. Nesse capítulo exibiremos uma demonstração para este resultado, que é conhecido como o teorema de Cesàro, utilizando as funções μ de Móbius e φ de Euler.

Antes de enunciarmos o Teorema de Cesàro vamos relembrar algumas ideias sobre o conceito de probabilidade.

Sejam $U = \{u_1, u_2, u_3, \cdots, u_n\}$, $U \neq \varnothing$, o espaço amostral e P uma distribuição de probabilidades em U. Dessa forma, definimos a função $p : U \to [0,1]$, tal que

$$\sum_{u \in U} P(u) = 1.$$

O valor de $P(u)$, representará a probabilidade do número u, $u \in U$. Os elementos do conjunto U serão equiprováveis se

$$P(u) = \frac{1}{\sum_{i=1}^{n} 1}, \forall u \in U,\ i \in \mathbb{Z}_+.$$

Seja $U' \subseteq U,\ U' \neq \varnothing$. Esse conjunto U' será denominado de evento do conjunto U e sua probabilidade será dada por

$$P(U') = \sum_{u \in U'} P(u).$$

A seguir enunciaremos o Teorema de Cesáro, entretanto, a sua demonstração só será realizada no final do capítulo, pois, precisamos provar alguns resultados que serão utilizados em sua demonstração.

Teorema 5.1. *(Cesàro) Escolhendo aleatoriamente $a, b \in \mathbb{Z}_+$, a probabilidade de eles serem primos entre si é igual a $\frac{6}{\pi^2}$.*

Seja o conjunto $A = I_n \times I_n$, onde $I_n = \{1, 2, 3, \cdots, n\}$. Suponhamos que os elementos de A sejam equiprováveis, ou seja, cada um tem a mesma probabilidade de ser escolhido ao acaso, logo a probabilidade de cada um deles é $\frac{1}{n^2}$. Dado $n \in \mathbb{Z}_+$, definiremos

P_n como sendo a probabilidade de escolhermos um par de números $(a,b) \in A$ tais que $(a,b)=1$. Assim, queremos mostrar que

$$\lim_{n\to\infty} P_n = \frac{6}{\pi^2}.$$

Esta definição para P_n não é "boa" para ser trabalhada, dessa forma, faz-se necessário encontrar uma expressão melhor para podermos prosseguir na busca de solucionar o Teorema de Cesàro.

A probabilidade $P_n = \dfrac{\#A'}{n^2}$, onde

$$A' = \{(a,b) \in A : (a,b) = 1\}.$$

O número de elementos do conjunto A' é dado por

$$\begin{aligned}
\#A' &= 2\cdot\#\{(a,b)\in A : (a,b)=1, a\le b\} - \#\{(a,a)\in A : (a,b)=1\}\\
&= 2\sum_{b=1}^{n}\#\{a\in I_n : (a,b)=1, a\le b\} - 1\\
&= 2\sum_{b=1}^{n}\varphi(b) - 1.
\end{aligned}$$

Portanto,

$$P_n = \frac{2\sum_{b=1}^{n}\varphi(b)-1}{n^2}. \tag{5.1}$$

Esta expressão será usada mais adiante. Agora vamos demonstrar dois lemas que serão os primeiros resultados preliminares que utilizaremos na demonstração do Teorema de Cesàro.

Lema 5.1. *Se f é uma função qualquer e $n \in \mathbb{Z}_+$, então*

$$\sum_{k=1}^{n}\sum_{d|k} f(d) = \sum_{k=1}^{n} f(k)\left\lfloor\frac{n}{k}\right\rfloor.$$

Demonstração: Seja f uma função qualquer e $n \in \mathbb{Z}_+$. Assim,

$$\sum_{k=1}^{n}\sum_{d_k|k} f(d_k) = \sum_{d_1|1} f(d_1) + \sum_{d_2|2} f(d_2) + \cdots + \sum_{d_n|n} f(d_n)$$

Como 1 é divisor de cada inteiro pertencente ao conjunto $\{1,2,3,\cdots,n\}$, $f(1)$ aparecerá n vezes na soma acima. O número 2, sendo divisor de $\left\lfloor\frac{n}{2}\right\rfloor$ destes inteiros, $f(2)$ ocorrerá $\left\lfloor\frac{n}{2}\right\rfloor$. Seguindo este raciocínio, sendo d divisor de $\left\lfloor\frac{n}{d}\right\rfloor$ dos inteiros de 1 até n, $f(d)$ ocorrerá $\left\lfloor\frac{n}{d}\right\rfloor$ vezes nesta soma. Dessa forma,

$$\sum_{k=1}^{n}\sum_{d|k} f(d) = f(1)\left\lfloor\frac{n}{1}\right\rfloor + f(2)\left\lfloor\frac{n}{2}\right\rfloor + \cdots + f(n)\left\lfloor\frac{n}{n}\right\rfloor.$$

Portanto,

$$\sum_{k=1}^{n}\sum_{d|k} f(d) = \sum_{k=1}^{n} f(k)\left\lfloor\frac{n}{k}\right\rfloor.$$

□

Lema 5.2. *Se f é uma função qualquer e $n \in \mathbb{Z}_+$, então*

$$\sum_{k=1}^{n} k\sum_{d|k} f(d) = \frac{1}{2}\sum_{k=1}^{n} kf(k)\left\lfloor\frac{n}{k}\right\rfloor\left(\left\lfloor\frac{n}{k}\right\rfloor + 1\right).$$

Demonstração: Note que são coincidentes, o conjunto dos pares ordenados (d, k), $1 \leq k \leq n$ com $d \mid k$ e o conjunto de pares ordenados (d, k) tais que $1 \leq d \leq n$ e $k = qd$, para algum $q \in \mathbb{Z}_+$, dessa forma, $1 \leq q \leq \left\lfloor\frac{n}{d}\right\rfloor$. Assim, obtemos

$$\begin{aligned}
\sum_{k=1}^{n} k\sum_{d|k} f(d) &= \sum_{d=1}^{n}\sum_{\substack{k=qd\\ 1\leq q\leq\lfloor n/d\rfloor}} kf(d)\\
&= \sum_{d=1}^{n} df(d) + 2df(d) + 3df(d) + \cdots + \left\lfloor\frac{n}{d}\right\rfloor df(d)\\
&= \sum_{d=1}^{n} df(d)\left(1 + 2 + 3 + \cdots + \left\lfloor\frac{n}{d}\right\rfloor\right)\\
&= \frac{1}{2}\sum_{d=1}^{n} df(d)\left\lfloor\frac{n}{d}\right\rfloor\left(\left\lfloor\frac{n}{d}\right\rfloor + 1\right).
\end{aligned}$$

□

No teorema 3.5, demonstramos que

$$\varphi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right) = n\sum_{d|n}\frac{\mu(d)}{d}.$$

Logo, combinando este resultado com o lema 5.2, temos

$$\begin{aligned}
2\sum_{k=1}^{n}\varphi(k) &= 2\sum_{k=1}^{n} k\sum_{d|k}\frac{\mu(d)}{d}\\
&= \sum_{k=1}^{n}\mu(k)\left\lfloor\frac{n}{k}\right\rfloor\left(\left\lfloor\frac{n}{k}\right\rfloor + 1\right)\\
&= \sum_{k=1}^{n}\mu(k)\left\lfloor\frac{n}{k}\right\rfloor^2 + \sum_{k=1}^{n}\mu(k)\left\lfloor\frac{n}{k}\right\rfloor. \qquad (5.2)
\end{aligned}$$

Agora, utilizando o teorema 3.1 e o lema 5.1, temos

$$\sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor = \sum_{k=1}^{n} \sum_{d|k} \mu(d) = 1.$$

Dessa forma, de (5.1) e (5.2), obtemos

$$\begin{aligned} P_n &= \frac{\sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^2 + 1 - 1}{n^2} \\ &= \frac{1}{n^2} \sum_{k=1}^{n} \mu(k) \left\lfloor \frac{n}{k} \right\rfloor^2 . \end{aligned} \tag{5.3}$$

Antes de prosseguirmos para o próximo resultado, precisamos evidenciar dois fatos importantes. O primeiro é que, da definição da função μ de Möbius temos que $\mu(k) \in B = \{-1, 0, 1\}$, dessa forma, $0 \leq |\mu(k)| \leq 1$, $\forall k \in \mathbb{Z}_+$. O outro, é que a série $\displaystyle\sum_{k=1}^{\infty} \frac{1}{k^2}$ é convergente. De fato, seja $f : \{x \in \mathbb{R} : x \geq 1\} \to \mathbb{R}$, definida por $f(x) = \dfrac{1}{x^2}$. A função f é contínua em todo o seu domínio, decrescente e positiva. Utilizando o teste da integral, temos que

$$\int_1^{\infty} \frac{dx}{x^2} = \lim_{b \to \infty} \int_1^{b} \frac{dx}{x^2} = \lim_{b \to \infty} \left. \frac{-1}{x} \right|_1^b = \lim_{b \to \infty} \frac{-1}{b} + 1 = 1.$$

Como a integral acima converge, a série $\displaystyle\sum_{k=1}^{\infty} \frac{1}{k^2}$ também converge.

Teorema 5.2. *Se $k \in \mathbb{Z}_+$, então*

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} \text{ é } \textit{convergente.}$$

Demonstração: Seja $x_k = \left(\dfrac{\mu(k)}{k^2} \right)_{k \in \mathbb{Z}_+}$. Logo, $\displaystyle\sum_{k=1}^{\infty} |x_k| = \sum_{p_i \ primo} \frac{1}{(p_1 p_2 \cdots p_i \cdots)^2}$, com $p_i \neq p_j$ para $i \neq j$. Como $\displaystyle\sum_{p_i \ primo} \frac{1}{(p_1 p_2 \cdots p_i \cdots)^2} < \sum_{k=1}^{\infty} \frac{1}{k^2}$ e como $\displaystyle\sum_{k=1}^{\infty} \frac{1}{k^2}$ é convergente, concluímos que $\displaystyle\sum_{k=1}^{\infty} |x_k|$ é convergente. Logo, a série $\displaystyle\sum_{k=1}^{\infty} x_k$ é absolutamente convergente, mas pelo teorema 2.14, $\displaystyle\sum_{k=1}^{\infty} x_k$ é convergente.

□

De posse da fórmula (5.3), mostraremos no próximo resultado, que o $\displaystyle\lim_{n \to \infty} P_n$ existe e é igual a $\displaystyle\sum_{k=1}^{\infty} \frac{\mu(k)}{k^2}$.

Proposição 5.1. *Se* $P_n = \dfrac{1}{n^2}\sum_{k=1}^{n}\mu(k)\left\lfloor\dfrac{n}{k}\right\rfloor^2$, *então o*

$$\lim_{n\to\infty} P_n = \sum_{k=1}^{\infty}\frac{\mu(k)}{k^2}.$$

Demonstração:

$$\begin{aligned}\left|P_n - \sum_{k=1}^{n}\frac{\mu(k)}{k^2}\right| &= \left|\sum_{k=1}^{n}\mu(k)\left(\frac{1}{n^2}\left\lfloor\frac{n}{k}\right\rfloor^2 - \frac{1}{k^2}\right)\right| \\ &\leq \sum_{k=1}^{n}\left|\frac{1}{k^2} - \frac{1}{n^2}\left\lfloor\frac{n}{k}\right\rfloor^2\right|. \end{aligned} \tag{5.4}$$

Para realizar uma estimativa do valor do último somatório acima, dados $n, k \in \mathbb{Z}_+$, com $1 \leq k \leq n$, temos que

$$\left|\frac{1}{k^2} - \frac{1}{n^2}\left\lfloor\frac{n}{k}\right\rfloor^2\right| < \frac{2}{nk} - \frac{1}{n^2}.$$

De fato,

$$\begin{aligned}\frac{n}{k} - 1 < \left\lfloor\frac{n}{k}\right\rfloor \leq \frac{n}{k} &\implies \frac{n^2}{k^2} - \frac{2n}{k} + 1 < \left\lfloor\frac{n}{k}\right\rfloor^2 \leq \frac{n^2}{k^2} \\ &\implies \frac{1}{k^2} - \frac{2}{kn} + \frac{1}{n^2} < \frac{1}{n^2}\left\lfloor\frac{n}{k}\right\rfloor^2 \leq \frac{1}{k^2} \\ &\implies 0 \leq \frac{1}{k^2} - \frac{1}{n^2}\left\lfloor\frac{n}{k}\right\rfloor^2 < \frac{2}{nk} - \frac{1}{n^2}.\end{aligned}$$

Demonstrada a propriedade acima, podemos retornar a (5.4). Assim,

$$\left|p_n - \sum_{k=1}^{n}\frac{\mu(k)}{k^2}\right| < \sum_{k=1}^{n}\left(\frac{2}{nk} - \frac{1}{n^2}\right) = \frac{2}{n}\sum_{k=1}^{n}\frac{1}{k} - \frac{1}{2n}.$$

Note que

$$\frac{2}{n}\sum_{k=1}^{n}\frac{1}{k} < \frac{2}{n}\left(1 + \int_1^n \frac{1}{x}dx\right) = \frac{2}{n}(\ln n + 1).$$

Mas, $\dfrac{2}{n}(\ln n + 1) \to 0$, quando $n \to \infty$. Dessa forma,

$$\lim_{n\to\infty}\left(\frac{2}{n}\sum_{k=1}^{n}\frac{1}{k} - \frac{1}{2n}\right) = 0.$$

Logo,

$$\lim_{n\to\infty}\left(P_n - \sum_{k=1}^{n}\frac{\mu(k)}{k^2}\right) = 0.$$

Portanto,

$$\lim_{n\to\infty} P_n = \lim_{n\to\infty}\left(P_n - \sum_{k=1}^{n}\frac{\mu(k)}{k^2}\right) + \sum_{k=1}^{\infty}\frac{\mu(k)}{k^2} = \sum_{k=1}^{\infty}\frac{\mu(k)}{k^2}.$$

□

Essa proposição é de extrema importância para o desenvolvimento da demonstração do Teorema de Cesàro. Com ela, a demonstração do teorema se reduz a mostrar que

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

Já sabemos que a série $\sum_{k=1}^{\infty} \frac{1}{k^2}$ é convergente. Agora, iremos mostrar para qual valor essa séria converge em nosso próximo teorema.

Teorema 5.3. *se $k \in \mathbb{Z}_+$, então*

$$\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}.$$

Demonstração: Utilizando a série de Maclaurin para $\sin x$, temos

$$\sin x = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots .$$

Note que, $\sin x = 0$ se, somente se, $x = \pm l\pi$, $l \in \mathbb{Z}$. Dessa forma, $x = \pm l\pi$ são raízes do polinômio $p(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots$. Logo, $p(x)$ pode ser fatorado da seguinte forma

$$x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots = ax(x-\pi)(x+\pi)(x-2\pi)(x+2\pi)(x-3\pi)(x+3\pi)\cdots, a \in \mathbb{R}.$$

Note que do lado direito da equação acima há produtos da soma pela diferença de dois termos, assim

$$x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots = ax(x^2-\pi^2)(x^2-4\pi^2)(x^2-9\pi^2)\cdots .$$

Dividindo a última igualdade por x, obtemos

$$1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \cdots = a(x^2-\pi^2)(x^2-4\pi^2)(x^2-9\pi^2)\cdots . \tag{5.5}$$

Tomando $x = 0$ na igualdade anterior, temos

$$1 = a(-\pi^2)(-4\pi^2)(-9\pi^2)\cdots . \tag{5.6}$$

Agora, dividindo membro a membro (5.5) por (5.6) temos

$$1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \cdots = \left(1 - \frac{x^2}{\pi^2}\right)\left(1 - \frac{x^2}{4\pi^2}\right)\left(1 - \frac{x^2}{9\pi^2}\right)\cdots .$$

Como, temos uma identidade de dois polinômios, podemos comparar os expoentes de cada um, façamos para o termo x^2. Assim

$$-\frac{x^2}{3!} = -\frac{x^2}{\pi^2} - \frac{x^2}{4\pi^2} - \frac{x^2}{9\pi^2} - \cdots .$$

Multiplicando a última identidade por $-\dfrac{\pi^2}{x^2}$,

$$\frac{\pi^2}{3!} = \frac{1}{1} + \frac{1}{4} + \frac{1}{9} + \cdots .$$

Portanto,

$$\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}.$$

□

Teorema 5.4. *Se p_n é o n-ésimo número primo, então*

$$\lim_{n\to\infty} \prod_{k=1}^{n} \left(1 - \frac{1}{p_k^2}\right)^{-1} = \sum_{k=1}^{\infty} \frac{1}{k^2}.$$

Demonstração: Sendo p_n o n-ésimo número primo, $p_n > n$, $\forall n \in \mathbb{Z}_+$. Dessa forma,

$$\sum_{k=1}^{n} \frac{1}{k^2} \leq \left(1 + \frac{1}{p_1^2} + \cdots + \frac{1}{p_1^{2j}}\right) \cdots \left(1 + \frac{1}{p_n^2} + \cdots + \frac{1}{p_n^{2j}}\right)$$

para cada $j \geq 1$. Além disso,

$$\left(1 + \frac{1}{p_1^2} + \cdots + \frac{1}{p_1^{2j}}\right) \cdots \left(1 + \frac{1}{p_n^2} + \cdots + \frac{1}{p_n^{2j}}\right) \leq \sum_{k=1}^{p_1^j \cdots p_n^j} \frac{1}{k^2}$$

para cada $j \geq 1$, visto que cada parcela obtida do desenvolvimento do lado direito da última desigualdade aparece no lado esquerdo. Entretanto, dado que

$$\sum_{k=1}^{p_1^j \cdots p_n^j} \frac{1}{k^2} \leq \sum_{k=1}^{\infty} \frac{1}{k^2},$$

temos,

$$\sum_{k=1}^{n} \frac{1}{k^2} \leq \left(1 + \frac{1}{p_1^2} + \cdots + \frac{1}{p_1^{2j}}\right) \cdots \left(1 + \frac{1}{p_n^2} + \cdots + \frac{1}{p_n^{2j}}\right) \leq \sum_{k=1}^{\infty} \frac{1}{k^2}.$$

Fazendo $j \to \infty$ e observando que

$$\lim_{j\to\infty} \left(1 + \frac{1}{p_i^2} + \cdots + \frac{1}{p_i^{2j}}\right) = \left(1 - \frac{1}{p_i^2}\right)^{-1},$$

obtemos

$$\sum_{k=1}^{n} \frac{1}{k^2} \leq \left(1 - \frac{1}{p_1^2}\right)^{-1} \cdots \left(1 - \frac{1}{p_n^2}\right)^{-1} \leq \sum_{k=1}^{\infty} \frac{1}{k^2}$$

$$\sum_{k=1}^{n} \frac{1}{k^2} \leq \prod_{k=1}^{n} \left(1 - \frac{1}{p_k^2}\right)^{-1} \leq \sum_{k=1}^{\infty} \frac{1}{k^2}.$$

Utilizando o teorema do confronto na última desigualdade, concluímos que

$$\lim_{n\to\infty} \prod_{k=1}^{n} \left(1 - \frac{1}{p_k^2}\right)^{-1} = \sum_{k=1}^{\infty} \frac{1}{k^2}.$$

□

Teorema 5.5. *Se p_n é o n-ésimo número primo, então*

$$\lim_{n\to\infty}\prod_{k=1}^{n}\left(1-\frac{1}{p_k^2}\right)=\sum_{k=1}^{\infty}\frac{\mu(k)}{k^2}.$$

demonstração: Em toda a demonstração, convencionaremos que se $e<f$, então $i_e<i_f$. Sejam $n\in\mathbb{Z}_+$,
$A_n=\{p_{i_1}p_{i_2}\cdots p_{i_{2s}} : s\in\mathbb{Z}_+, p_{i_1},\ p_{i_2},\dots,p_{i_{2s}}\ \textit{são primos},\ \textit{com}\ p_{i_1}p_{i_2}\cdots p_{i_{2s}}\leq n\}$;
$B_n=\{p_{i_1}p_{i_2}\cdots p_{i_{2s}} : s\in\mathbb{Z}_+, p_{i_1},\ p_{i_2},\dots,p_{i_{2s}}\ \textit{são primos e}\ i_1,i_2,\dots,i_{2s}\leq n\}$;
$C_n=\{p_{i_1}p_{i_2}\cdots p_{i_{2s+1}} : s\in\mathbb{Z}_+, p_{i_1},\ p_{i_2},\dots,p_{i_{2s+1}}\ \textit{são primos},\ \textit{com}\ p_{i_1}p_{i_2}\cdots p_{i_{2s+1}}\leq n\}$;
$D_n=\{p_{i_1}p_{i_2}\cdots p_{i_{2s+1}} : s\in\mathbb{Z}_+, p_{i_1},\ p_{i_2},\dots,p_{i_{2s+1}}\ \textit{são primos e}\ i_1,i_2,\dots,i_{2s+1}\leq n\}$.
Sejam, ainda,

$$a_n=1+\sum_{x\in A_n}\frac{1}{x^2},\ b_n=1+\sum_{x\in B_n}\frac{1}{x^2},\ c_n=\sum_{x\in C_n}\frac{1}{x^2},\ d_n=\sum_{x\in D_n}\frac{1}{x^2}.$$

Assim,

$$a_n-c_n=1+\sum_{x\in A_n}\frac{1}{x^2}-\sum_{x\in C_n}\frac{1}{x^2}=\sum_{k=1}^{n}\frac{\mu(k)}{k^2}$$

e

$$b_n-d_n=1+\sum_{x\in B_n}\frac{1}{x^2}-\sum_{x\in D_n}\frac{1}{x^2}=\prod_{k=1}^{n}\left(1-\frac{1}{p_k^2}\right).$$

Além disso, os limites das sequências a_n, b_n, c_n *e* d_n existem, pois, as sequências correspondentes são não-decrescentes e limitadas superiormente por $\sum_{k=1}^{\infty}\frac{1}{k^2}$. Pelo teorema 2.11, garantimos a existência do limite

$$\lim_{n\to\infty}\prod_{k=1}^{n}\left(1-\frac{1}{p_k^2}\right).$$

Mas, $p_n>n,\ \forall n\in\mathbb{Z}_+$, assim temos que $A_n\subseteq B_n\subseteq A_{p_1p_2\cdots p_n}$ e $C_n\subseteq D_n\subseteq C_{p_1p_2\cdots p_n}$. Logo, são verdadeiras as seguintes desigualdades

$$a_n\leq b_n\leq a_{p_1p_2\cdots p_n}\ e\ c_n\leq d_n\leq c_{p_1p_2\cdots p_n}.$$

Agora, utilizando o Teorema do Confronto, temos

$$\lim_{n\to\infty}a_n=\lim_{n\to\infty}b_n\ e\ \lim_{n\to\infty}c_n=\lim_{n\to\infty}d_n.$$

Portanto,

$$\begin{aligned}
\lim_{n\to\infty}\prod_{k=1}^{n}\left(1-\frac{1}{p_k^2}\right) &= \lim_{n\to\infty}(b_n - d_n)\\
&= \lim_{n\to\infty} b_n - \lim_{n\to\infty} d_n\\
&= \lim_{n\to\infty} a_n - \lim_{n\to\infty} c_n\\
&= \lim_{n\to\infty}(a_n - c_n)\\
&= \lim_{n\to\infty}\sum_{k=1}^{n}\frac{\mu(k)}{k^2}\\
&= \sum_{k=1}^{\infty}\frac{\mu(k)}{k^2}.
\end{aligned}$$

□

De posse dos resultados obtidos nos teoremas 5.4 e 5.5, podemos, finalmente, concluir a demonstração do Teorema de Cesàro. Então, vamos a ela.

$$\begin{aligned}
\lim_{n\to\infty} P_n &= \sum_{k=1}^{\infty}\frac{\mu(k)}{k^2}\\
&= \lim_{n\to\infty}\prod_{k=1}^{n}\left(1-\frac{1}{p_k^2}\right)\\
&= \left[\lim_{n\to\infty}\prod_{k=1}^{n}\left(1-\frac{1}{p_k^2}\right)^{-1}\right]^{-1}\\
&= \left[\sum_{k=1}^{\infty}\frac{1}{k^2}\right]^{-1}\\
&= \left[\frac{\pi^2}{6}\right]^{-1}\\
&= \frac{6}{\pi^2}
\end{aligned}$$

Dessa forma, a demonstração do Teorema de Ernesto Cesàro está completa.

□

Referências Bibliográficas

[1] APOSTOL, Tom M. Introducion to analytic number theory. New York: Springer-Verlag New York Heidelberg Berlin, 1976.

[2] LANDAU, Edmund. Elementary number theory. New York: Chelsea Publishing Company, 1958.

[3] LIMA, Elon Lages. Análise Real volume 1: funções de uma variável real. 12ª ed. Rio de Janeiro: IMPA, 2016.

[4] FILHO, Edgar de Alencar. Teoria elementar dos números. São Paulo: Nobel, 1981.

[5] HEFEZ, Abramo. Aritmética. Rio de Janeiro: SBM, 2016.

[6] MARTINEZ, Fábio Brochero; MOREIRA, Carlos Gustavo; SALDANHA, Nicolau; TEGAN, Eduardo. Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro. 4ª ed. Rio de Janeiro: IMPA, 2018.

[7] MCCARTHY, Paul Joseph. Introducion to arithmetical functions. New York: Springer-Verlag New York Inc, 1986.

[8] MONTREZOR, Camila Lopes. Funções aritméticas. Dissertação (Dissertação em matemática) – USP. São Carlos-SP, 2017. Disponível em: $< https : //sca.profmat - sbm.org.br/sca_v2/get_tcc3.php?id = 74036 >$. 5/arquivototal.pdf>. Acesso em: 29 de dez. de 2019.

[9] NETO, Antônio Caminha Muniz. Tópicos de matemática elementar: introdução a análise. 2ª ed. Rio de Janeiro: SBM, 2012.

[10] NETO, Antônio Caminha Muniz. Tópicos de matemática elementar: teoria dos números. 2ª ed. Rio de Janeiro: SBM, 2013.

[11] SANTOS, José Plínio de Oliveira. Introdução à Teoria dos Números.3ª ed. Rio de Janeiro: IMPA, 2018.

[12] STEWART, James. Cálculo - volume 2. 6ª ed. São Paulo: Cengage Learning, 2012.