UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

Eldaline Rocha da Silva

Funções elementares e teoria dos números

RECIFE
2019

UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO
DEPARTAMENTO DE MATEMÁTICA
Mestrado Profissional em Matemática em Rede Nacional

Eldaline Rocha da Silva

Funções elementares e teoria dos números

Dissertação de mestrado apresentada ao Departamento de Matemática da Universidade Federal Rural de Pernambuco como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Rodrigo Genuino Clemente

RECIFE
2019

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema Integrado de Bibliotecas da UFRPE
Biblioteca Central, Recife-PE, Brasil

S586f Silva, Eldaline Rocha da
Funções elementares e teoria dos números / Eldaline Rocha da Silva. – 2019.
85 f.: il.

Orientador: Rodrigo Genuino Clemente.
Dissertação (Mestrado) – Universidade Federal Rural de Pernambuco, Programa de Pós-Graduação Mestrado Profissional em Matemática em Rede Nacional, Recife, BR-PE, 2019.
Inclui referências.

1. Matemática – Estudo e ensino 2. Teoria dos números 3. Análise combinatória 4. Aritmética 5. Funções numéricas I. Clemente, Rodrigo Genuino, orient. II. Título

CDD 510

Eldaline Rocha da Silva

Funções elementares e teoria dos números

Trabalho apresentado ao Programa de Mestrado Profissional em Matemática - PROFMAT do Departamento de Matemática da UNIVERSIDADE FEDERAL RURAL DE PERNAMBUCO, como requisito parcial para obtenção do grau de Mestre em Matemática.

Aprovado em 29 / 03 / 2019

BANCA EXAMINADORA

_____

Prof. Dr. Rodrigo Genuino Clemente [Orientador] - PROFMAT/UFRPE

_____

Prof. Dr. Eudes Mendes Barboza - PROFMAT/UFRPE

_____

Prof. Dr. Ricardo Burity Croccia Macedo - PROFMAT/UFPB

Dedico esse trabalho a Deus, que é a minha maior força nos momentos difíceis. A minha família, que sempre acreditaram no meu potencial e contribuíram com essa conquista. E aos leitores interessados e fascinados pela matemática.

Agradecimentos

Agradeço primeiramente a Deus, que sempre iluminou o meu caminho e colocou força em meu coração para vencer essa etapa de minha vida. Também sou grato ao senhor por ter me dado saúde, força e disposição para concluir o mestrado. Agradeço todas as bênçãos que recaíram sobre mim e sobre todos aqueles que amo.

Agradeço a minha família e a meus amigos por todo o apoio, força e amor. Sou grata, especialmente, a minha mãe Severina Félix da Silva, que tanto lutou pela minha educação e nunca me deixou perder a fé. A meu pai, José Rocha da Silva, que sempre foi o meu exemplo de luta e determinação. E sou grata também a meu irmão, Rodrigo Rocha da Silva, por ser tão companheiro. Jamais serei capaz de retribuir todo carinho, amor e incentivo que recebi de vocês.

A todos meus colegas de mestrado, especialmente Elizeu Odilon, Eduardo Macedo, Maurílio Muniz e Thiago Andrade, meu muito obrigado. Agradeço a ajuda dada em vários momentos de dificuldade, e agradeço as palavras de incentivo e otimismo que não me deixaram desistir. Vocês foram fundamentais para minha formação, sem essa ajuda não conseguiria chegar tão longe.

Por fim, sou grata a todos os professores que contribuíram com a minha trajetória acadêmica, em particular, ao Professor e orientador Dr. Rodrigo Genuíno Clemente. Muito obrigada por ser tão atencioso, paciente e acessível. Agradeço todo o tempo dedicado e o entusiasmo com a pesquisa.

“A matemática, vista corretamente, possui
não apenas verdade, mas também suprema beleza
- uma beleza fria e austera, como a da escultura.”
(Bertrand Russell)

Resumo

Nesta dissertação realizaremos um estudo sobre algumas funções aritméticas. Veremos teoremas, propriedades, demonstrações e alguns resultados importantes. Além disso, usaremos de técnicas de análise combinatória para estabelecer relações entre elas, o que é de extrema importância pois descaracteriza a ideia de que a matemática é desvinculada e segmentada. Buscamos oferecer uma abordagem combinatória para a teoria elementar de números. A justificativa para este ponto de vista é que podemos apresentar a analise combinatória e teoria dos números como disciplinas irmãs. Eles compartilham uma certa interseção do conhecimento comum e cada um genuinamente enriquece o outro. Desta forma, ao estudar a teoria dos números a partir de uma perspectiva combinatória, alunos e professores se beneficiam da consequente simplicidade das provas de muitos teoremas, sendo poupados de repetição e adquirindo novos *insights*.

Palavras-chave: funções aritméticas, teoria dos números, combinatória.

Abstract

In this dissertation we will perform a study on some arithmetic functions. We will see theorems, properties, demonstrations, and some important results. In addition, we will use usual techniques in combinatorial analysis to establish relationships between them, which is extremely important because it changes the idea that mathematics is unlinked and segmented. We seek to offer a combinatorial approach to the elementary theory of numbers. The justification for this view is that we can present combinatorial analysis and number theory as sister disciplines. They share a certain intersection of common knowledge and each one genuinely enriches the other. In this way, when studying number theory from a combinatorial perspective, students and teachers benefit from the consequent simplicity of proofs of many theorems, being spared repetition and acquiring new insights.

Keywords: arithmetic functions, number theory, combinatorics.

Lista de ilustrações

Sumário

Introdução

Neste trabalho serão estudados conceitos, propriedades e alguns resultados sobre funções aritméticas. Qualquer função cujo domínio seja algum subconjunto dos inteiros positivos e expressem alguma propriedade aritmética sobre eles é chamada de função aritmética. Nosso estudo aborda as propriedades dos inteiros positivos relacionados com a primalidade, a divisibilidade e a operações elementares.

As funções $\phi(n)$ de Euler, a quantidade de números coprimos com n menores que n, $\tau(n)$, a quantidade de divisores de n e $\sigma(n)$, a soma dos divisores de n, são funções aritméticas que desempenham um papel importante em teoria dos números. Realizaremos um estudo de cada uma destas funções aritméticas, usaremos algumas técnicas de análise combinatória para estabelecer relações entre elas e então generalizaremos nossos resultados das por meio da função de Möbius $\mu(n)$.

Para alguns importantes teoremas são apresentadas demonstrações combinatórias e fornecemos alguns exemplos que ajudam a compreender as ideias utilizadas nas demonstrações. Apresentamos ainda um significativo número de problemas resolvidos, dentre estes há questões de olimpíadas internacionais envolvendo as funções apresentadas neste trabalho.

Tentamos relacionar nosso trabalho com alguns temas pertinentes ao Ensino Básico. Por exemplo, números primos, divisores de um número natural e operações elementares (adição, subtração, multiplicação, divisão) são abordados no 6º ano do Ensino Fundamental, e também são conteúdos necessários e suficientes para entender as definições das funções aritméticas apresentadas. Além disso, apresentaremos a função de Euler interligando com o Princípio da Inclusão e Exclusão, que é visto por alunos do Ensino Médio quando estudam Teoria dos conjuntos.

1 Resultados preliminares

Neste capítulo faremos uma breve revisão de alguns conteúdos da aritmética como: propriedades dos inteiros, divisibilidade, números primos e compostos. Algumas resultados importantes serão apresentados sobre os números primos, como por exemplo, o Teorema Fundamental da Aritmética, onde todo inteiro maior do que 1 pode ser representado de modo único como um produto de fatores primos, a menos da permutação dos fatores. O leitor que desejar informações mais detalhadas pode consultar as referências citadas.

1.1 Números inteiros

O conjunto nos números inteiros é representado por $\mathbb{Z}$, e é formado pela união de três conjuntos, os números naturais, o conjunto contendo apenas o zero e o conjunto dos simétrico dos naturais. Denotamos por $\mathbb{Z} = \{\mathbb{N}\} \cup \{0\} \cup \{-\mathbb{N}\}$, ou ainda

$$\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$$

A seguir veremos algumas propriedades dos números inteiros com relação a adição e multiplicação. Essas operações estão bem definidas nos inteiros, ou seja, quando somamos ou multiplicamos dois números inteiros iremos obter como resultado outro inteiro. Vale ressaltar que operação divisão não está bem definida para os inteiros.

Para todos $a, b, c \in \mathbb{Z}$ valem as propriedades:

Propriedade 1.1. As operações de adição e multiplicação em inteiros satisfazem as seguintes propriedades:

(i) (Comutatividade) $a + b = b + a$ e $a \cdot b = b \cdot a$

(ii) (Associatividade) $(a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

(iii) (Elemento neutro) $a + 0 = a$ e $a \cdot 1 = a$

(iv) (Elemento simétrico da adição) $a + b = 0$, onde $b = -a$

(v) (Multiplicação distributiva em relação à adição.) $a \cdot (b + c) = a \cdot b + a \cdot c$

Propriedade 1.2. $a \cdot 0 = 0$, para todo $a \in \mathbb{Z}$.

Propriedade 1.3. $\mathbb{Z}$ é um domínio de integridade, isto é, se $a \cdot b = 0$ então $a = 0$ ou $b = 0$.

Propriedade 1.4. (Tricotomia) Dados $a, b \in \mathbb{Z}$, apenas uma das possibilidades a seguir é verdadeira

(1) $a = b$;

(2) $b - a \in \mathbb{N}$;

(3) $-(b - a) = (a - b) \in \mathbb{N}$

Iremos agora definir a relação "menor que" entre dois números inteiros, observe a próxima definição.

Definição 1.5. Para $a, b \in \mathbb{Z}$ dizemos que a é 'menor que' b se $b - a \in \mathbb{N}$, denotamos por $a < b$.

Propriedade 1.6. Para $a, b \in \mathbb{Z}$ valem as seguintes propriedades

(i) Seja $c \in \mathbb{Z}$, $a < b$ se, e somente se, $a + c < b + c$.

(ii) Seja $c \in \mathbb{N}$, $a < b$ se, e somente se, $a \cdot c < b \cdot c$.

(iii) Se $a < b$ e $c < 0$ então $b \cdot c < a \cdot c$.

(iv) Se $a < b$ e $b < c$ então $a < c$.

Agora iremos definir a relação "menor ou igual que" entre dois números inteiros, observe a seguinte definição.

Definição 1.7. Para $a, b \in \mathbb{Z}$ dizemos que a é *menor ou igual* que b se $a < b$ ou $a = b$, denotamos por $a \leq b$ ou $a \leq b$.

Propriedade 1.8. Para $a, b, c \in \mathbb{Z}$ valem as seguintes propriedades

(i) (Reflexiva) Para todo $a \in \mathbb{Z}$, $a \leq a$.

(ii) (Antissimétrica) Para todo $a, b \in \mathbb{Z}$, $a \leq b$ e $b \leq a$ teremos $a = b$.

(iii) (Transitiva) Para todo $a, b, c \in \mathbb{Z}$, $a \leq b$ e $b \leq c$ teremos $a \leq c$.

(iv) (Cancelativa em relação com a adição) Para todo $a, b, c \in \mathbb{Z}$, se $a \leq b$ então $a + c \leq b + c$.

Note que a relação "menor ou igual que" é uma relação de ordem pois $a \leq a$ é verdadeiro para $a \in \mathbb{N}$. Vamos agora definir o valor absoluto de um inteiro. Por outro lado, observe que a relação $<$ não é uma relação de ordem pois $a < a$ é falso para $a \in \mathbb{N}$.

Definição 1.9. Seja $a \in \mathbb{Z}$, o *valor absoluto* de a ou *módulo* de a, é definido como:

$$|a| = \begin{cases} a & \text{se } a \geq 0, \\ -a & \text{se } a < 0. \end{cases}$$

Observe que $|a| \geq 0$ para todo $a \in \mathbb{Z}$.

Propriedade 1.10. Para $a, b \in \mathbb{Z}$ teremos as seguintes propriedades do valor absoluto:

(i) $|a \cdot b| = |a| \cdot |b|$

(ii) $|a| \geq b \Leftrightarrow -a \leq b \leq a$

(iii) $|-a| \leq a \leq |a|$

(iv) $||a| - |b|| \leq |a \pm b| \leq |a| + |b|$

Caso o leitor tenha interesse, as demonstrações das propriedades citadas nesta seção podem ser encontradas em (1).

1.2 Divisibilidade

Teorema 1.11. *(Divisão Euclidiana (1, Teorema 3.10)) Dados $a, b \in \mathbb{Z}$ com $b \neq 0$, existem $q, r \in \mathbb{Z}$ tais que*

$$a = bq + r, \quad 0 \leq < |b|.$$

Tais q e r são unicamente determinados e os chamamos de quociente e de resto da divisão de a por b.

Definição 1.12. Dados $a, b \in \mathbb{Z}$ dizemos que a *divide* b quando existir $c \in \mathbb{Z}$ tal que $b = a \cdot c$, denotamos por $a|b$ e dizemos que a é um divisor de b, ou ainda, b é múltiplo de a. Caso a não divida b denotaremos por $a \nmid b$.

Exemplo 1.13. De acordo com a definição temos que $2|6$ pois $6 = 2 \cdot 3$. Também podemos afirmar que para todo $a \in \mathbb{Z}$ temos $a|a$ e $1|a$ pois $a = a \cdot 1$, além disso $a|0$ pois $0 = a \cdot 0$. E se $0|a$ teremos $a = 0$.

A seguir temos algumas propriedades da divisibilidade.

Propriedade 1.14. Se $a|b$ e $b|c$ então $a|c$.

Demonstração. Se $a|b$ e $b|c$ então existem $p, q \in \mathbb{Z}$ tais que $b = a \cdot p$ e $c = b \cdot q$. Assim teremos $c = b \cdot q = (a \cdot p) \cdot c = a \cdot (p \cdot c)$, logo $a|c$. □

Propriedade 1.15. Se $a|b$ e $a|c$ então $a|(b \pm c)$.

Demonstração. Como $a|b$ e $a|c$, existem $r, s \in \mathbb{Z}$ tais que $b = a \cdot r$ e $c = a \cdot s$. Assim $b \pm c = a \cdot r \pm a \cdot s = a \cdot (r \pm s)$, logo $a|(b \pm c)$. □

Propriedade 1.16. Se $a|b$ então $a|bp$ para qualquer $p \in \mathbb{Z}$.

Demonstração. Como $a|b$ existe $r \in \mathbb{Z}$ tais que $b = a \cdot r$. Assim $bp = a \cdot r \cdot p = a \cdot (r \cdot p)$, logo $a|(bp)$. □

Propriedade 1.17. Se $a|b$ e $a|c$ então $a|(bp + cq)$ para quaisquer $p, q \in \mathbb{Z}$.

Demonstração. Como $a|b$ e $a|c$, existem $r, s \in \mathbb{Z}$ tais que $b = a \cdot r$ e $c = a \cdot s$. Assim

$$bp + cq = (a \cdot r)p + (a \cdot s)q = a \cdot (r \cdot p) + a \cdot (s \cdot q), \text{ logo } a|(b \cdot p + c \cdot q).$$

□

A partir dessas propriedades outras seguem:

Propriedade 1.18. Para $a, b, c \in \mathbb{Z}$ temos:

(i) Sejam $a, b, p, q \in \mathbb{Z}$ com $a \neq 0$ e $b \neq 0$, se $a|p$ e $b|q$, então $a \cdot b|p \cdot q$.

(ii) Sejam $a, b, c \in \mathbb{Z}$ com $a \neq 0$, tal que $a|(b \pm c)$ então $a|b \iff a|c$.

(iii) Sejam $a, b \in \mathbb{Z}$ com $b \neq 0$, tais que $a|b$, então $|b| \geq |a|$.

Um divisor próprio de um inteiro positivo n é qualquer divisor de n diferente dele mesmo. Desta forma, um número primo possui exatamente um divisor próprio, a saber, o número 1, e qualquer outro número possui ao menos dois divisores próprios. Veremos agora os conceitos de mdc e mmc. Para as definições a seguir considere os seguintes conjuntos:

Conjuntos dos divisores de n: $D_n = \{r_i \in \mathbb{N} \,|\, r_i \text{ divide } n\}$

Conjuntos dos multiplos de n: $M_n = \{s_i \in \mathbb{N} \,|\, s_i \text{ é multiplo de } n\}$

Definição 1.19. (Máximo Divisor Comum) Dados dois números naturais a e b não nulos, o *máximo divisor comum* de a e b será o maior elemento da interseção de D_a e D_b, denotaremos por $mdc(a, b)$ ou (a, b).

Exemplo 1.20. Considere os números 24 e 36. Os conjuntos dos divisores são $D_{24} = \{1, 2, 3, 4, 6, 8, 12, 24\}$ e $D_{36} = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$. Temos a interseção desses conjuntos $D_{24} \cup D_{36} = \{1, 2, 3, 4, 6, 12\}$. O maior elemento de $D_{24} \cup D_{36}$ é 12, portanto $(24, 36) = 12$

Definição 1.21. (Mínimo Múltiplo Comum) Dados dois números naturais a e b não nulos, o *mínimo múltiplo comum* de a e b será o menor elemento não nulo da interseção de M_a e M_b, denotaremos por $mmc(a, b)$.

Exemplo 1.22. Considere os números 6 e 4. Temos $M_4 = \{0, 4, 8, 12, 16, 20, \cdots\}$ e $M_6 = \{0, 6, 12, 18, 24, 30, \cdots\}$. A interseção desses conjuntos é $M_4 \cap M_6 = \{0, 12, 24, 36, 48\}$. O menor elemento não nulo da interseção desses conjuntos é 12, portanto $mmc(4, 6) = 12$

Para um estudo mais aprofundado sobre divisibilidade ou propriedades do mmc e mdc, consultar(2).

1.3 Números Primos

Um número natural maior do que 1 pode ser um número primo ou um número composto, observe as seguintes definições:

Definição 1.23. Todo inteiro positivo maior que 1 e divisível por apenas 1 e ele mesmo é chamado de *primo*.

Definição 1.24. Todo inteiro positivo maior que 1 que possui como divisores números naturais diferentes de 1 e ele mesmo é chamado de *composto*.

Exemplo 1.25. O número 5 possui como divisores 1 e o próprio 5, portanto é primo. Já o número 6 possuí como divisores os números $\{1, 2, 3, 6\}$, logo não é primo.

Dados $a, p, q \in \mathbb{N}$, com p e q primos, teremos as seguintes proposições:

Proposição 1.26. *Se $p|q$, então $p = q$.*

Demonstração. Se $p|q$ e q é primo, então ou $p = 1$ ou $p = q$. Mas como definimos um número primo como sendo um número maior que 1, então $p = q$. □

Observação 1.27. Dizemos que dois inteiros a e b são relativamente primos ou coprimos se $mdc(a, b) = 1$. Por exemplo, como $mdc(6, 13) = 1$ temos que 6 e 13 são relativamente primos, já 6 e 16 não são coprimos pois $mdc(6, 16) = 2$.

Proposição 1.28. *Se $p \nmid a$, então p e a são primos entre si, ou seja $mdc(p, a) = 1$.*

Demonstração. Se $mdc(p, a) = r$ então $r|p$ e $r|a$. Como p é primo teremos $r = 1$ ou $r = p$, mas $p \neq r$, já que p não divide a, logo $r = 1$. □

Teorema 1.29. *(Bachet-Bézout (3, Teorema 2.3)) Sejam $a, b \in \mathbb{Z}$. Existem $x, y \in \mathbb{Z}$ com*

$$ax + by = mdc(a, b).$$

Demonstração. O leitor pode verificar a prova deste teorema em (3, Teorema 2.3). □

Teorema 1.30. *(Lema de Gauss (3, Teorema 2.3)) Sejam $a, b, c \in \mathbb{Z}$. Se $a|bc$ e $mdc(a, b) = 1$ então $a|c$.*

Demonstração. Como $a|bc$, existe $r \in \mathbb{Z}$ tal que $bc = ra$. Mas como $mdc(a, b) = 1$ existem $m, n \in \mathbb{Z}$ tais que $am + bn = 1$. Podemos então fazer o seguinte cálculo $c(am + bn) = 1.c$. Como $c(am + bn) = acm + cbn = acm + ran = a(cm + rn)$ teremos $c = a(cm + rn)$ logo $a|c$. □

Teorema 1.31. *(Lema de Euclides (3, Teorema 2.3)) Sejam $a, b, p \in \mathbb{Z}$. Se $p|ab$, então $p|a$ ou $p|b$.*

Demonstração. Suponha que $p \nmid a$ então $mdc(p,a) = 1$. Temos $p|ab$ e $mdc(p,a) = 1$, pelo teorema anterior $p|b$. □

Corolário 1.32. *Considere $p_1, p_2, p_3, \cdots, p_n$ números primos, se $p|p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n$, então $p = p_i$ para algum $i = 1, 2, 3, \cdots, n$.*

O próximo teorema é primordial para o nosso estudo sobre funções aritméticas, o leitor pode saber mais sobre ele em (1, Capítulo 7).

Teorema 1.33. *(Teorema Fundamental da Aritmética (1, Teorema 7.3)). Todo número natural maior do que 1 ou é primo ou se escreve de modo único, a menos da ordem dos fatores, como um produto de números primos.*

$$n = p_1 \cdot p_2 \cdot ... \cdot p_i,$$

onde p_i são todos primos.

Corolário 1.34. *Dado n número natural, existem primos $p_1 < p_2 < p_3 < \cdots < p_i \in \mathbb{N}$ tais que*

$$n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot ... \cdot {p_i}^{r_i},$$

com r_i números naturais.

No Livro IX dos Elementos, Euclides respondeu uma pergunta: Quantos serão os números primos? Para mostrarmos que existem infinitos números primos utilizaremos a mesma demonstração dada por ele. Este é o primeiro registro de uma demonstração por redução ao absurdo em matemática.

Teorema 1.35. *(1, Teorema 7.13) Existem infinitos números primos.*

Demonstração. Por absurdo, suponha que existe uma quantidade finita de números primos, sejam eles $\{p_1, p_2, p_3, \cdots, p_i\}$. Considere o número natural $n = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_i$, e considere seu sucessor $m = n + 1 = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_i + 1$. Como m sempre deixa resto 1 na divisão por qualquer p_j, vemos que p_j não divide m. Por outro lado, teremos m composto, pois $m \neq p_j$, para todo $j = \{1, ..., i\}$. Logo existe um fator primo p_j que divide m, o que é uma contradição. □

Existem alguns tipos de números primos especiais, como por exemplo os primos de Mersene, que são do formato $2^p - 1$, e os primos gêmeos p e $p + 2$ (veja Observação 2.30 e Exemplo 3.6 respectivamente). Para mais detalhes sobre primos especiais, o leitor pode consultar em (1). Ainda em (1), o leitor pode ler a Seção 7.2 e estudar um pouco mais sobre a distribuição dos primos, o crivo de Eratóstenes, teorema dos números primos e problemas em aberto.

"Esses números desempenham papel fundamental e a eles estão associados muitos problemas famosos cujas soluções têm resistido aos esforços de várias gerações de matemáticos" (HEFEZ, 2016, p.122). Como por exemplo, a conjectura de Goldbach, a qual afirma que todo

número natural par maior que três pode ser escrito como a soma de dois números primos. Ela foi proposta em 1742 e segue sem demonstração.

Em (2), o leitor pode encontrar uma leitura mais aprofundada sobre problemas em aberto, o teorema dos números primos, como também sobre os primos de Sophie Germain, fórmulas para primos, critérios de primalidade e programas que encontraram os maiores primos conhecidos.

2 Funções $\tau(n)$ e $\sigma(n)$

Neste capítulo estudaremos duas importantes funções aritméticas: $\tau(n)$ e $\sigma(n)$. Apresentaremos teoremas significativos e suas demonstrações, mostraremos como calcular $\tau(n)$ e $\sigma(n)$ para um n relativamente grande e, além de disso, traremos questões relacionadas a este tema.

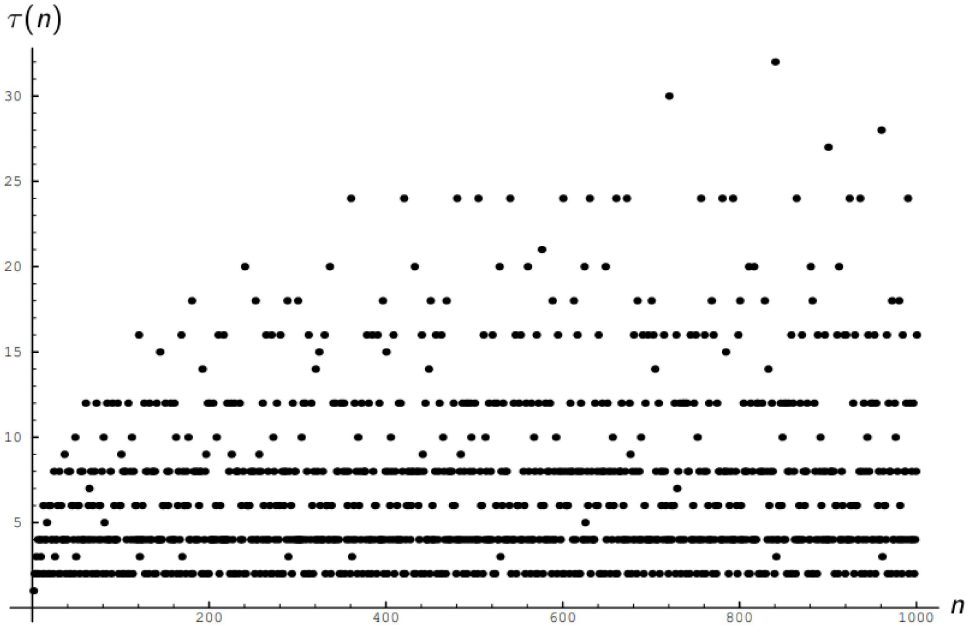
2.1 Função $\tau(n)$ a quantidade de divisores de n

Definição 2.1. Para $n \in \mathbb{N}$ defina $\tau(n)$, o número de divisores naturais de n, por

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

Observe que $\tau(n) = 1$ se, e somente se, $n = 1$. Para um primo p teremos $\tau(p) = 2$, pois teremos dois divisores, a saber, 1 e o próprio n. Abaixo temos o gráfico de $\tau(n)$ para $1 \leq n \leq 1000$:

Figura 1 – Gráfico de $\tau(n)$.



Fonte:<http://sites.millersville.edu/bikenaga/number-theory/divisor-functions/divisor-functions.html>

Perceba que a linha horizontal $y = 2$ limita os pontos por baixo. Para $n \geq 2$ temos $\tau(n) \geq 2$, pois se n for primo teremos $\tau(p) = 2$ e caso n seja composto contaremos mais de dois divisores.

Teorema 2.2. *Seja p um número primo, $\tau(p^m) = m + 1$*

Demonstração. Os divisores de p^m são $1, p^1, p^2, p^3, \cdots, p^m$, totalizando $(m + 1)$ números. Portanto $\tau(p^m) = m + 1$. □

Teorema 2.3. *(3, Teorema 6-3) Seja $n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$ a decomposição de n em fatores primos.*

$$\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot (\alpha_3 + 1) \cdots (\alpha_k + 1) = \prod_{i}^{k} (\alpha_i + 1)$$

Demonstração. Por indução sobre o número de fatores primos de n. Se n possuir apenas um fator primo, $n = p^\alpha$, iremos ter os seguintes divisores $1, p^1, p^2, p^3, \cdots, p^\alpha$. O que nos fornece um total de $(\alpha + 1)$ divisores, logo $\tau(n) = \tau(p^\alpha) = \alpha + 1$. Agora, assuma que o teorema é válido para k ou menos fatores primos. Então para $n' = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$ temos $\tau(n') = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot (\alpha_3 + 1) \cdots (\alpha_k + 1)$. Considere $d_1, d_2, d_3, \cdots, d_s$ os divisores de n'. Seja $n = n'.p^{\alpha_{k+1}}$, onde p é um primo que não é fator de n'. Então os divisores de n são d_1, d_2, d_3, $\cdots$, d_s, pd_1, pd_2, pd_3, $\cdots$, pd_s, p^2d_1, p^2d_2, p^2d_3, $\cdots$, $p^{\alpha_{k+1}}d_s$, $p^{\alpha_{k+1}}d_1$, $p^{\alpha_{k+1}}d_2$, $p^{\alpha_{k+1}}d_3$, $\cdots$, $p^{\alpha_{k+1}}d_s$, totalizando $d_1 \cdot d_2 \cdot d_3 \cdots d_s \cdot (\alpha_{k+1} + 1)$ divisores. Portanto $\tau(n) = \tau(n') \cdot (\alpha_{k+1} + 1)$=$(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_k + 1) \cdot (\alpha_{k+1} + 1)$. □

Tendo em vista que τ é calculável em potências de primos, iremos mostrar que esta função é multiplicativa.

Teorema 2.4. *Sejam m e n números naturais com $mdc(m, n) = 1$, então*

$$\tau(m \cdot n) = \tau(m) \cdot \tau(n)$$

Demonstração. Queremos mostrar que τ é uma função multiplicativa. Sejam m e n relativamente primos e considere as seguintes decomposições em fatores primos $m = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_s}^{\alpha_s}$ e $n = {q_1}^{\beta_1} \cdot {q_2}^{\beta_2} \cdots {q_r}^{\beta_r}$, com $p_i \neq q_j$ para todos i e j. Logo

$$\tau(m \cdot n) = \tau({p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_s}^{\alpha_s} \cdot {q_1}^{\beta_1} \cdot {q_2}^{\beta_2} \cdots {q_r}^{\beta_r})$$

Pelo Teorema 2.3

$$\begin{aligned}
\tau(m \cdot n) &= \tau({p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_s}^{\alpha_s} \cdot {q_1}^{\beta_1} \cdot {q_2}^{\beta_2} \cdots {q_r}^{\beta_r}) \\
&= (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_s + 1) \cdot (\beta_1 + 1) \cdot (\beta_2 + 1) \cdots (\beta_r + 1) \\
&= \tau(m) \cdot \tau(n)
\end{aligned}$$

□

Corolário 2.5. *Se $n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$, então $\tau(n) = \tau({p_1}^{\alpha_1}) \cdot \tau({p_2}^{\alpha_2}) \cdot \tau({p_3}^{\alpha_3}) \cdots \tau({p_k}^{\alpha_k})$.*

Exemplo 2.6. Vamos calcular $\tau(504)$.

$$\begin{aligned}\tau(504) &= \tau(2^3 \cdot 3^2 \cdot 7)\\ &= \tau(2^3) \cdot \tau(3^2) \cdot \tau(7)\\ &= 4 \cdot 3 \cdot 2\\ &= 24\end{aligned}$$

Corolário 2.7. *Sejam r, s números naturais e p um número primo. Então*

$$\tau(p^r) \cdot \tau(p^s) > \tau(p^{r+s}).$$

Demonstração. Pelo Teorema 2.2 temos $\tau(p^r) = r + 1$ e $\tau(p^s) = s + 1$. Então

$$\begin{aligned}\tau(p^r) \cdot \tau(p^s) &= (r+1) \cdot (s+1)\\ &= r + s + 1 + r \cdot s\end{aligned}$$

Note que $r \cdot s > 1$, logo $\tau(p^r) \cdot \tau(p^s) > r + s + 1 = \tau(p^{r+s})$. □

Exemplo 2.8. Observe os seguintes resultados

$$\begin{aligned}\tau(2^2) &= \tau(4) = 3\\ \tau(2^3) &= \tau(8) = 4\\ \tau(2^2 \cdot 2^3) &= \tau(32) = 6\end{aligned}$$

Note que $\tau(4) \cdot \tau(8) = 3 \cdot 4 > 6 = \tau(32)$. Concluímos que $\tau(2^2) \cdot \tau(2^3) > \tau(2^{2+3})$.

Teorema 2.9. *Se m e n são números naturais que não são primos entre si, então $\tau(m) \cdot \tau(n) > \tau(m \cdot n)$.*

Demonstração. Como não são coprimos, m e n possuem fatores primos em comum, sejam eles $p_1, p_2, p_3, \ldots, p_k$. Podemos escrever $m = a \cdot {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot {p_3}^{r_3} \cdots {p_k}^{r_k}$ e $n = b \cdot {p_1}^{s_1} \cdot {p_2}^{s_2} \cdot {p_3}^{s_3} \cdots {p_k}^{s_k}$, onde mdc(a,b)=1, com $mdc(a, p_i) = mdc(b, p_i) = 1$ para todo i. Daí,

$$\tau(m \cdot n) = \tau(a \cdot {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot {p_3}^{r_3} \cdots {p_k}^{r_k} \cdot b \cdot {p_1}^{s_1} \cdot {p_2}^{s_2} \cdot {p_3}^{s_3} \cdots {p_k}^{s_k})$$

$$= \tau(a \cdot b \cdot {p_1}^{r_1+s_1} \cdot {p_2}^{r_2+s_2} \cdot {p_3}^{r_3+s_3} \cdots {p_k}^{r_k+s_k})$$

Como a, b, p_r e p_s são coprimos para quaisquer r e s, pelo Teorema 2.4, podemos fazer o seguinte cálculo:

$$\tau(m \cdot n) = \tau(a) \cdot \tau(b) \cdot \tau({p_1}^{r_1+s_1}) \cdot \tau({p_2}^{r_2+s_2}) \cdot \tau({p_3}^{r_3+s_3}) \cdots \tau({p_k}^{r_k+s_k})$$

O Corolário 2.7 nos diz que para cada $i = 1, 2, 3, \cdots, k$ teremos $\tau({p_i}^{r_i+s_i}) < \tau(p_i^{r_i}) \cdot \tau({p_i}^{s_i})$, portanto

$$\tau(m \cdot n) < \tau({p_1}^{r_1}) \cdot \tau({p_1}^{s_1}) \cdot \tau({p_2}^{r_2}) \cdot \tau({p_2}^{s_2}) \cdot \tau({p_3}^{r_3}) \cdot \tau({p_3}^{s_3}) \cdots \tau({p_k}^{r_k}) \cdot \tau({p_k}^{s_k}) \cdot \tau(a) \cdot \tau(b) = \tau(m) \cdot \tau(n)$$

Portanto,

$$\tau(m \cdot n) < \tau(m) \cdot \tau(n)$$

□

Mostramos no Teorema 2.4 que a função τ é multiplicativa. Mas esta função não é completamente multiplicativa, isto é, existem m e n inteiros tais que $\tau(m \cdot n) \neq \tau(m) \cdot \tau(n)$. De fato, vimos acima que $\tau(m \cdot n) < \tau(m) \cdot \tau(n)$ para m e n não coprimos.

Exemplo 2.10. (4, Problema 6.2.3)(Olimpíada Austríaca de Matemática - 1995) Quantos números pares e ímpares dividem $3^{12} - 1$ e não dividem $3^k - 1$, para $k = 1, 2, 3, \cdots, 11$.

Demonstração. Note que $3^{12} - 1 = 531440 = 2^4 \cdot 5 \cdot 7 \cdot 13 \cdot 73$. O número de divisores, $\tau(3^{12} - 1)$ é dado por $(4+1) \cdot (1+1) \cdot (1+1) \cdot (1+1) \cdot (1+1) = (4+1) \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 80$. Da decomposição em fatores primos, vemos que destes divisores $1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 16$ são ímpares e $4 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 64$ são pares. Para $3^k - 1$ com $k = 1, 2, 3, \cdots, 11$ temos:

$$\begin{aligned}
3^1 - 1 &= 2 \\
3^2 - 1 &= 2^3 \\
3^3 - 1 &= 2 \cdot 13 \\
3^4 - 1 &= 2^4 \cdot 5 \\
3^5 - 1 &= 2 \cdot 11^2 \\
3^6 - 1 &= 2^3 \cdot 7 \cdot 13 \\
3^7 - 1 &= 2 \cdot 1093 \\
3^8 - 1 &= 2^5 \cdot 5 \cdot 41 \\
3^9 - 1 &= 2 \cdot 13 \cdot 757 \\
3^{10} - 1 &= 2^3 \cdot 11^2 \cdot 61 \\
3^{11} - 1 &= 2 \cdot 23 \cdot 3851
\end{aligned}$$

Olhando os divisores ímpares destes termos temos alguns que dividem $3^{12} - 1$, são eles: $1, 5, 7, 13, 91$. Já os divisores pares em comum com $3^{12} - 1$ são:

$$\begin{aligned}
&2^i \quad \text{para} \quad 1 \leq i \leq 4, \\
&2^i \cdot 5 \quad \text{para} \quad 1 \leq i \leq 4 \\
&2^j \cdot 7 \quad \text{para} \quad 1 \leq j \leq 3 \\
&2^j \cdot 13 \quad \text{para} \quad 1 \leq j \leq 3 \\
&2^j \cdot 91 \quad \text{para} \quad 1 \leq j \leq 3
\end{aligned}$$

Totalizando 17 divisores pares. Assim, restam 47 divisores pares e 11 ímpares que dividem $3^{12} - 1$ e que não dividem $3^k - 1$ para $k = 1, 2, 3, \cdots, 11$. □

Exemplo 2.11. (4, Problema 6.2.2)(Olimpíada Iraniana de Matemática - 1998) Encontre todos os inteiros positivos d que tenham exatamente 16 divisores inteiros positivos $d_1, d_2, \cdots, d_{16}$ tais que

$$1 = d_1 < d_2 < \cdots < d_{16} = d, \quad d_6 = 18 \quad \text{e} \quad d_9 - d_8 = 17.$$

Demonstração. Considere $d = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$ sendo $p_1, p_2, \cdots, p_k$ primos distintos. Sabemos que n possui $\tau(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_k + 1)$ divisores. Do enunciado temos $d_6 = 18 = 2 \cdot 3^2$, então os fatores 2 e 3 também são fatores de d. Note que $\tau(d_6) = (1+1) \cdot (2+1) = 6$. Como d_6 possui 6 divisores e d possui 16 divisores, as possibilidades para d são: $d = 2 \cdot 3^7$ ou $d = 2 \cdot 3^3 \cdot p$ (p primo diferente de 2 e 3). Se $d = 2 \cdot 3^7 = 4374$ os divisores são $\{1, 2, 3, 6, 9, 18, 27, 54, 81, 162, 243, 486, 729, 1458, 2187, 4374\}$, e $d_9 - d_8 = 81 - 54 \neq 17$, o que contradiz o enunciado, logo $d = 2 \cdot 3^3 \cdot p$. Como $d_6 = 18$ temos $p > 18$. Se $18 < p < 27$, então $d_7 = p$, $d_8 = 27$, e seguindo a ordem de divisores teremos $d_9 = 2p$ mas pelo enunciado $d_9 = 17 + d_8 = 24 + 17 = 44$ o que resulta em $p = 22$, contradição pois 22 não é primo. Se $27 < p < 54$, $d_7 = 27$, $d_8 = p$, $d_9 = 54$ e pelo enunciado $d_9 = d_8 + 17$, então $p = 37$. Se $p > 54$, então $d_7 = 27$, $d_8 = 54$, seguindo a ordem de divisores teremos $d_9 = p$ e temos $d_9 = d_8 + 17 = 71$. Assim, encontramos duas soluções para o problema: $d = 2 \cdot 3^3 \cdot 37$ ou $d = 2 \cdot 3^3 \cdot 71$. □

Para a proposição seguinte, considere a função "maior inteiro" $\lfloor x \rfloor$, uma função importante em teoria dos números, que associa o número real x o maior número inteiro menor ou igual a x. Por exemplo,

$$\lfloor 1,2 \rfloor = 1; \quad \lfloor 0,9 \rfloor = 0; \quad \lfloor 1 \rfloor = 1.$$

Proposição 2.12. *Para todo* $n \geq 2$

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

Demonstração. Note que se k divide n, então $n = kq$. Logo, a parte inteira de $\left(\frac{n}{k}\right)$ é q. Daí, $n - 1 = kq - 1 = k(q-1) + (k-1)$. Como $k - 1 < k$ então $(k-1)$ é o resto da divisão de $n - 1$ por k, portanto, a parte inteira de $n - 1$ sobre k é $q - 1$. Desta forma, a diferença é $q - (q-1) = 1$. O caso k não divide n é similar. Assim,

$$\left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \frac{n-1}{k} \right\rfloor = \begin{cases} 1 & se \quad k|n \\ 0 & k \nmid n \end{cases}$$

Então

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

□

Observação 2.13. Vimos que n é primo se e somente se $\tau(n) = 2$. Então

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

se e somente se n for primo.

Exemplo 2.14. Considere $n = 7$, teremos

$$\begin{aligned}
\sum_{k=1}^{7} \left(\left\lfloor \frac{7}{k} \right\rfloor - \left\lfloor \frac{7-1}{k} \right\rfloor \right) &= \left(\left\lfloor \frac{7}{1} \right\rfloor - \left\lfloor \frac{6}{1} \right\rfloor \right) + \left(\left\lfloor \frac{7}{2} \right\rfloor - \left\lfloor \frac{6}{2} \right\rfloor \right) \\
&+ \left(\left\lfloor \frac{7}{3} \right\rfloor - \left\lfloor \frac{6}{3} \right\rfloor \right) + \left(\left\lfloor \frac{7}{4} \right\rfloor - \left\lfloor \frac{6}{4} \right\rfloor \right) + \left(\left\lfloor \frac{7}{5} \right\rfloor - \left\lfloor \frac{6}{5} \right\rfloor \right) \\
&+ \left(\left\lfloor \frac{7}{6} \right\rfloor - \left\lfloor \frac{6}{6} \right\rfloor \right) + \left(\left\lfloor \frac{7}{7} \right\rfloor - \left\lfloor \frac{6}{7} \right\rfloor \right) \\
&= (7-6) + (3-3) + (2-2) + (1-1) + (1-1) \\
&+ (1-1) + (1-0) \\
&= 1 + 0 + 0 + 0 + 0 + 0 + 1 = 2.
\end{aligned}$$

Pela Observação 2.13 concluímos assim que 7 é um número primo.

Exemplo 2.15. (2, Problema 5.6) Demonstrar que

$$\tau(n) \leq 2\sqrt{n}$$

Demonstração. Sejam d_i os divisores de n. Considere os pares ordenados $\left(d_i, \frac{n}{d_i}\right)$ e tome o conjunto de todos os pares, $P(n) = \left\{ \left(d_1, \frac{n}{d_1}\right), \left(d_2, \frac{n}{d_2}\right), \cdots, \left(d_k, \frac{n}{d_k}\right) \right\}$. Podemos dividir os elementos deste conjunto em três grupos onde $d_i < \frac{n}{d_i}$, $d_i > \frac{n}{d_i}$ ou $d_i = \frac{n}{d_i}$. Esta última condição só ocorre para um único elemento de $p(n)$, quando $d = \sqrt{n}$, para isto teríamos n um quadrado perfeito. Seja $A(n)$ o conjunto dos os elementos que satisfazem a primeira condição. Perceba que os elementos que satisfazem a segunda condição estão em bijeção com os elementos de $A(n)$, invertendo os termos de cada par ordenado. Então teremos

$$|P(n)| = \begin{cases} 2 \cdot |A(n)| & \text{se } n \text{ não for quadrado perfeito} \\ 2 \cdot |A(n)| + 1 & \text{se } n \text{ for quadrado perfeito} \end{cases}$$

O menor elemento de um par ordenado $\left(d_i, \frac{n}{d_i}\right)$ é menor que $\sqrt{n}$. Então $A(n)$ possui no máximo $\sqrt{n}$ elementos. Assim:

$$|P(n)| < \begin{cases} 2 \cdot \sqrt{n} & \text{se } n \text{ não for quadrado perfeito} \\ 2 \cdot \sqrt{n} + 1 & \text{se } n \text{ for quadrado perfeito} \end{cases}$$

Para um quadrado perfeito temos $|P(n)| < 2 \cdot \sqrt{n} + 1$, como esse resultado é um número inteiro podemos dizer que $|P(n)| \leq 2 \cdot \sqrt{n}$. Como existem $\tau(n)$ pares ordenados, podemos afirmar que $|P(n)| = \tau(n) \leq 2\sqrt{n}$ é verdadeiro para todo $n \in \mathbb{N}$. □

Exemplo 2.16. (4, Problema 6.2.4)(Olimpíada de São Petersburgo - 1988) Seja $\tau(n)$ o número de divisores do número natural n. Prove que a sequência $\tau(n^2+1)$ não se torna monotônica a partir de qualquer ponto dado.

Demonstração. Iniciaremos recordando o que significa monotônica. Uma sequência x_n é dita monotônica se $x_n \leq x_{n+1}$ ou $x_n \geq x_{n+1}$ para todo $n \in \mathbb{N}$. Com isto em mente, observe que n^2+1 não é um quadrado perfeito, assim nenhum divisor d_i de n^2+1 torna verdadeira a seguinte igualdade $d = \frac{n}{d}$, além disso, vimos na resolução do Exemplo 2.15 que $\tau(n^2+1)$ será par. Considere $n^2+1 = d_1 \cdot d_2$, afirmamos que um desses divisores é menor que n. Suponha por absurdo que não, $d_1 > n$ e $d_2 > n$ então

$$n^2+1 = d_1 \cdot d_2 \geq (n+1)\cdot(n+1) = n^2+2n+1$$

Absurdo, portanto, para cada par de divisores $(d_i, \frac{n}{d_i})$ um deles é menor que n. Concluímos assim que metade dos divisores de n^2+1 é menor que n. Iremos supor n par, pois estamos olhando valores de n suficientemente grandes e, desta forma, podemos sempre tomar seu sucessor. Daí, n^2+1 é ímpar e seus divisores são ímpares. Como metade dos divisores de n^2+1 são menores que n e todos são ímpares, há no máximo $2 \cdot \left(\frac{n}{2}\right)$ divisores, logo $\tau(n^2+1) \leq n$ para qualquer n par. Agora suponha que $\tau(n^2+1)$ se torna estritamente monótono para $n > N$, então

$$\tau(n^2+1) > \tau(N^2+1)$$
$$\tau(n^2+1) \geq \tau(N^2+1)+2$$

para $n > N$. Daí $\tau((k+1)^2+1) \geq \tau(k^2+1)+2$ para todo $N \leq k \leq n$. Assim, iterando $n-N$ vezes, obtemos

$$\tau(n^2+1) \geq \tau(N^2+1) + 2(n-N).$$

Portanto, se n é par e suficientemente grande temos

$$n \geq \tau(n^2+1) \geq \tau(N^2+1) + 2(n-N)$$

o que é uma contradição. □

Exemplo 2.17. (3, Problema 6.2.5) Existe um inteiro positivo tal que o produto de seus divisores próprios termina exatamente com 2001 zeros?

Demonstração. Considere p o produto dos divisores de n. Como os divisores de n podem ser

escrito de duas formas, a saber d e $\frac{n}{d}$, então

$$\begin{aligned} p = \sqrt{p \cdot p} &= \sqrt{\left(\prod_{d|n} d\right)\left(\prod_{d|n} \frac{n}{d}\right)} \\ &= \sqrt{\prod_{d|n} d\left(\frac{n}{d}\right)} \\ &= \sqrt{n^{\tau(n)}} \\ &= n^{\frac{\tau(n)}{2}} \end{aligned}$$

Como queremos o produto de seus divisores próprios, teremos que retirar o fator n, então queremos

$$\frac{p}{n} = n^{\frac{\tau(n)}{2}-1}$$

Para $n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$, vimos em Teorema 2.3 que $\tau(n) = \prod_i^k (\alpha_i + 1)$. Defina $n = 2 \cdot 5 \cdot p_1^6 \cdot p_2^{10} \cdot p_3^{12}$, para p_1, p_2, p_3 primos diferentes de 2 e 5. Temos

$$\frac{\tau(n)}{2} - 1 = \frac{(2 \cdot 2 \cdot 7 \cdot 11 \cdot 13)}{2} - 1 = 2001$$

Assim o produto dos divisores próprios de n é

$$p = n^{\frac{\tau(n)}{2}-1} = n^{2001} = 2^{2001} \cdot 5^{2001} \cdot p_1^{6 \cdot 2001} \cdot p_2^{10 \cdot 2001} \cdot p_3^{12 \cdot 2001}$$

Devido a $(2^{2001} \cdot 5^{2001} = 10^{2001})$, n terá exatamente 2001 zeros. □

2.2 Função $\sigma(n)$ a soma dos divisores de n

Definição 2.18. Para $n \in \mathbb{N}$ defina $\sigma(n)$, a soma dos divisores de n, por

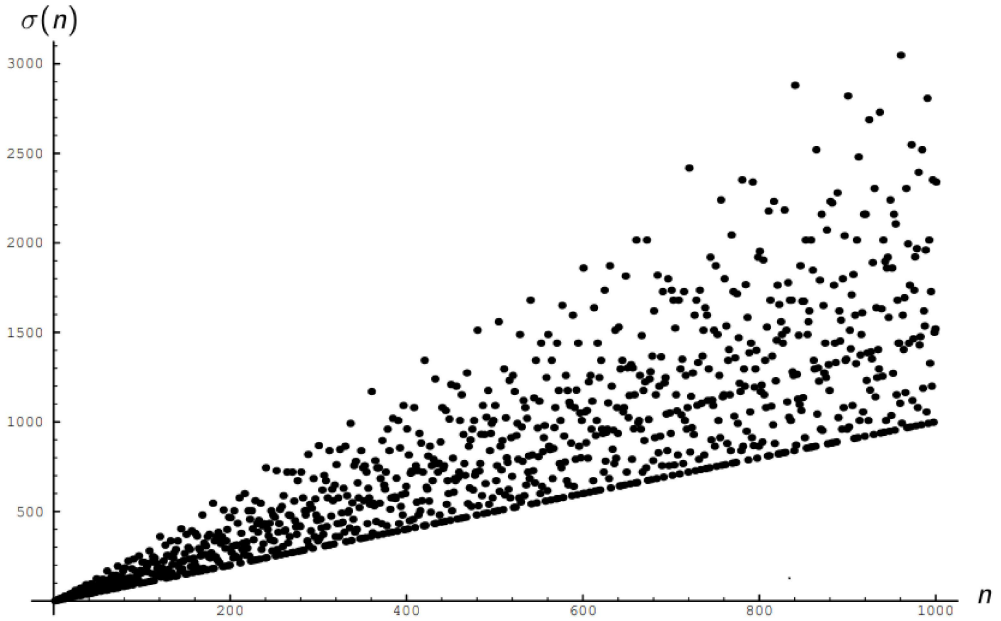
$$\sigma(n) = \sum_{d|n} d.$$

Observe que $\sigma(n) = 1$ se, e somente se $n = 1$. Para um primo p teremos $\sigma(p) = 1 + p$. Para $n \geq 2$ temos $\sigma(n) \geq 1 + n$, pois existem pelo menos dois divisores, o 1 e o próprio n. Este é o gráfico de $\sigma(n)$ para $1 \leq n \leq 1000$:

Observe que temos a reta $y = x + 1$ limitando os pontos por baixo. De fato, considere os pontos da forma $(n, n + 1)$ tais que pertencem a reta $y = x + 1$. Quando n for primo, temos $\sigma(n) = 1 + n$. Caso n seja composto, teremos $\sigma(n) \geq 1 + n$.

Observação 2.19. Um *número perfeito* é um número natural tal que a soma de todos os seus divisores naturais próprios, excluindo ele mesmo, é igual ao próprio número. Divisores próprios

Figura 2 – Gráfico de $\sigma(n)$



Fonte: <http://sites.millersville.edu/bikenaga/number-theory/divisor-functions/divisor-functions.html>

de um número positivo n são todos os divisores inteiros positivos de n exceto o próprio n. Então, n é um número perfeito se e somente se

$$\sigma(n) - n = n$$
$$\sigma(n) = 2n$$

Por exemplo, o número 6 é um número perfeito, pois $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6$. Para $n = 28$ temos $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \cdot 28$, então 28 é um número perfeito. Para saber mais sobre números perfeitos, o leitor pode consultar em (5).

Teorema 2.20. *(3, Teorema 6-3) Seja p um número primo então*

$$\sigma(p^m) = \frac{p^{m+1} - 1}{p - 1}.$$

Demonstração. Os divisores de p^m são $1, p^1, p^2, p^3, ..., p^m$. Fazendo a soma desses números teremos a soma dos termos de uma progressão geométrica finita, de razão p,

$$\sigma(p^m) = 1 + p^1 + p^2 + p^3 + ... + p^m = \frac{p^{m+1} - 1}{p - 1}.$$

□

Teorema 2.21. *Seja $n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot ... \cdot {p_k}^{\alpha_k}$ a decomposição de n em fatores primos.*

$$\sigma(n) = \left(\frac{{p_1}^{\alpha_1+1} - 1}{p_1 - 1}\right) \cdot ... \cdot \left(\frac{{p_k}^{\alpha_k+1} - 1}{p_k - 1}\right) = \prod_i^k \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Demonstração. Por indução sobre o número de fatores primos de n. Se n possuir apenas um fator primo, $n = p^\alpha$, teremos os seguintes divisores $1, p^1, p^2, p^3, ..., p^\alpha$. Logo a soma dos divisores é uma soma dos termos de uma progressão geométrica finita, de razão p, logo $\sigma(n) = 1 + p^1 + p^2 + p^3 + ... + p^\alpha = \frac{{p_1}^{\alpha_1+1}-1}{p_1-1}$. Agora, assuma que o teorema é válido para k ou menos fatores primos. Então para $n' = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_k}^{\alpha_k}$ temos

$$\sigma(n') = \left(\frac{{p_1}^{\alpha_1+1}-1}{p_1-1}\right) \cdot ... \cdot \left(\frac{{p_k}^{\alpha_k+1}-1}{p_k-1}\right).$$

Considere $d_1, d_2, d_3, ..., d_s$ os divisores de n'. Seja $n = n'.p^\alpha$, onde p é um primo que não é fator de n'. Então os divisores de n são $d_1, d_2, d_3, ..., d_s, p \cdot d_1, p \cdot d_2, p \cdot d_3, ..., p \cdot d_s, p^2 \cdot d_1, p^2 \cdot d_2, p^2 \cdot d_3, ..., p^2 \cdot d_s, p^\alpha \cdot d_1, p^\alpha \cdot d_2, p^\alpha \cdot d_3, ..., p^\alpha \cdot d_s$. Note a soma desses divisores

$$\begin{aligned}
\sigma(n) &= \sigma(n') + p \cdot \sigma(n') + ... + p^\alpha \cdot \sigma(n') \\
&= \sigma(n') \cdot (1 + p + ... + p^\alpha) \\
&= \sigma(n') \cdot \left(\frac{p^{\alpha+1}-1}{p-1}\right) \\
&= \left(\frac{{p_1}^{\alpha_1+1}-1}{p_1-1}\right) \cdot ... \cdot \left(\frac{{p_k}^{\alpha_k+1}-1}{p_k-1}\right) \cdot \left(\frac{p^{\alpha+1}-1}{p_1-1}\right).
\end{aligned}$$

□

Mostraremos que a função σ é multiplicativa sabendo apenas o seu valor em potência de primos.

Teorema 2.22. *Sejam m e n números naturais com $mdc(m, n) = 1$, então*

$$\sigma(m \cdot n) = \sigma(m) \cdot \sigma(n).$$

Demonstração. Queremos mostrar que σ é uma função multiplicativa. Considere as seguintes decomposições em fatores primos $m = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot ... \cdot {p_s}^{\alpha_s}$ e $n = {q_1}^{\beta_1} \cdot {q_2}^{\beta_2} \cdot ... \cdot {q_r}^{\beta_r}$. Temos

$$m \cdot n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot ... \cdot {p_s}^{\alpha_s} \cdot {q_1}^{\beta_1} \cdot {q_2}^{\beta_2} \cdot ... \cdot {q_r}^{\beta_r}$$

Pelo Teorema 2.21

$$\begin{aligned}
\sigma(m \cdot n) &= \sigma({p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot ... \cdot {p_s}^{\alpha_s} \cdot {q_1}^{\beta_1} \cdot {q_2}^{\beta_2} \cdot ... \cdot {q_r}^{\beta_r}) \\
&= \left(\frac{{p_1}^{\alpha_1+1}-1}{p_1-1} \cdot ... \cdot \frac{{p_s}^{\alpha_s+1}-1}{p_s-1} \cdot \frac{{q_1}^{\beta_1+1}-1}{q_1-1} \cdot ... \cdot \frac{{q_r}^{\beta_r+1}-1}{q_r-1}\right) \\
&= \left(\frac{{p_1}^{\alpha_1+1}-1}{p_1-1} \cdot ... \cdot \frac{{p_s}^{\alpha_s+1}-1}{p_s-1}\right) \cdot \left(\frac{{q_1}^{\beta_1+1}-1}{q_1-1} \cdot ... \cdot \frac{{q_r}^{\beta_r+1}-1}{q_r-1}\right) \\
&= \sigma(m) \cdot \sigma(n).
\end{aligned}$$

□

Corolário 2.23. *Se $n = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdot ... \cdot {p_k}^{\alpha_k}$, então $\sigma(n) = \sigma({p_1}^{\alpha_1}) \cdot \sigma({p_2}^{\alpha_2}) \cdot ... \cdot \sigma({p_k}^{\alpha_k})$.*

Exemplo 2.24. Vamos calcular $\sigma(504)$.

$$\sigma(504) = \sigma(2^3) \cdot \sigma(3^2) \cdot \sigma(7) = \frac{2^4-1}{2-1} \cdot \frac{3^3-1}{3-1} \cdot \frac{7^2-1}{7-1} = 1560.$$

Corolário 2.25. *Sejam r, s números naturais e p um número primo. Então*

$$\sigma(p^r) \cdot \sigma(p^s) > \sigma(p^{r+s}).$$

Demonstração. Vimos na demonstração do Teorema 2.20 que $\sigma(p^m) = 1 + p^1 + p^2 + ... + p^m$ para p primo. Então $\sigma(p^r) = 1 + p^1 + p^2 + ... + p^r$ e $\sigma(p^s) = 1 + p^1 + p^2 + ... + p^s$. Portanto:

$$\begin{aligned}
&\sigma(p^r) \cdot \sigma(p^s) = \\
&= \left(1 + p^1 + p^2 + ... + p^r\right)\left(1 + p^1 + p^2 + ... + p^s\right) \\
&= [1 + \left(p^1 + p^2 + ... + p^r\right)] \cdot \left(1 + p^1 + p^2 + ... + p^s\right) \\
&= 1 \cdot \left(1 + p^1 + p^2 + ... + p^s\right) + \left(p^1 + p^2 + ... + p^r\right) \cdot \left(1 + p^1 + p^2 + ... + p^s\right) \\
&= 1 \cdot \left(1 + p^1 + p^2 + ... + p^s\right) + [\left(p^1 + p^2 + ... + p^{r-1}\right) + p^r] \cdot \left(1 + p^1 + p^2 + ... + p^s\right) \\
&= 1 \cdot \left(1 + p^1 + p^2 + ... + p^s\right) + \left(p^1 + p^2 + ... + p^{r-1}\right) \cdot \left(1 + p^1 + p^2 + ... + p^s\right) + \\
&p^r \left(1 + p^1 + p^2 + ... + p^s\right).
\end{aligned}$$

Considere $s > r$, note que

$$\begin{aligned}
\sigma(p^{r+s}) &= 1 + p^1 + p^2 + ... + p^r + ... + p^{r+s} \\
&= [1 + p^1 + p^2 + ... + p^r] + [p^{r+1} + ... + p^{r+s}] \\
&= [1 + p^1 + p^2 + ... + p^r] + p^r[p^1 + ... + p^s] \\
&< 1 \cdot \left(1 + p^1 + p^2 + ... + p^s\right) + \left(p^1 + p^2 + ... + p^{r-1}\right) \cdot \left(1 + p^1 + p^2 + ... + p^s\right) + \\
&p^r \left(1 + p^1 + p^2 + ... + p^s\right).
\end{aligned}$$

Logo $\sigma(p^r) \cdot \sigma(p^s) > \sigma(p^{r+s})$. □

Exemplo 2.26. Observe os seguintes resultados

$$\begin{aligned}
\sigma(2^2) &= \sigma(4) = 1 + 2 + 4 = 7 \\
\sigma(2^3) &= \sigma(8) = 1 + 2 + 4 + 8 = 15 \\
\sigma(2^2.2^3) &= \sigma(32) = 1 + 2 + 4 + 8 + 16 + 32 = 63
\end{aligned}$$

Note que $\sigma(4) \cdot \sigma(8) = 7 \cdot 15 = 105 > 63 = \sigma(32)$. Concluímos que $\sigma(2^2) \cdot \sigma(2^3) > \sigma(2^{2+3})$.

Teorema 2.27. *Se m e n são números naturais que não são primos entre si, então $\sigma(m) \cdot \sigma(n) > \sigma(m \cdot n)$.*

Demonstração. Como não são coprimos, m e n possuem fatores primos em comum, sejam eles $p_1, p_2, p_3, \ldots, p_k$. Podemos escrever $m = a \cdot {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot {p_3}^{r_3} \cdots {p_k}^{r_k}$ e $n = b \cdot {p_1}^{s_1} \cdot {p_2}^{s_2} \cdot {p_3}^{s_3} \cdots {p_k}^{s_k}$, onde mdc(a,b)=1, com $mdc(a, p_i) = mdc(b, p_i) = 1$ para todo i. Daí

$$\sigma(m \cdot n) = \sigma(a \cdot {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot {p_3}^{r_3} \cdots {p_k}^{r_k} \cdot b \cdot {p_1}^{s_1} \cdot {p_2}^{s_2} \cdot {p_3}^{s_3} \cdots {p_k}^{s_k})$$

$$= \sigma(a \cdot b \cdot {p_1}^{r_1+s_1} \cdot {p_2}^{r_2+s_2} \cdot {p_3}^{r_3+s_3} \cdots {p_k}^{r_k+s_k}).$$

Como a, b, p_r e p_s são coprimos para quaisquer r e s, pelo Corolário 2.23, podemos fazer o seguinte cálculo:

$$\sigma(m \cdot n) = \sigma(a) \cdot \sigma(b) \cdot \sigma({p_1}^{r_1+s_1}) \cdot \sigma({p_2}^{r_2+s_2}) \cdot \sigma({p_3}^{r_3+s_3}) \cdots \sigma({p_k}^{r_k+s_k})$$

O Corolário 2.25 nos diz que para cada i=1,2,3,...,k teremos $\sigma({p_i}^{r_i+s_i}) < \sigma(p_i^{r_i}) \cdot \sigma({p_i}^{s_i})$, portanto

$$\sigma(m \cdot n) = \sigma(a) \cdot \sigma(b) \cdot \sigma({p_1}^{r_1+s_1}) \cdot \sigma({p_2}^{r_2+s_2}) \cdots \sigma({p_k}^{r_k+s_k})$$

$$< \sigma({p_1}^{r_1}) \cdot \sigma({p_1}^{s_1}) \cdot \sigma({p_2}^{r_2}) \cdot \sigma({p_2}^{s_2}) \cdots \sigma({p_k}^{r_k}) \cdot \sigma({p_k}^{s_k}) \cdot \sigma(a) \cdot \sigma(b) = \sigma(m) \cdot \sigma(n)$$

o que resulta em:

$$\sigma(m \cdot n) < \sigma(m) \cdot \sigma(n)$$

□

Mostramos no Teorema 2.22 que a função σ é multiplicativa. Mas esta função não é completamente multiplicativa, pois não temos $\sigma(m \cdot n) = \sigma(m) \cdot \sigma(n)$ para todos os números naturais m e n. Vimos que $\sigma(m \cdot n) < \sigma(m) \cdot \sigma(n)$ para m e n não coprimos.

Observação 2.28. Dois números diferentes que satisfazem $\sigma(m) - m = n$ e $\sigma(n) - n = m$ são chamados de *Números Amigáveis*, são números cuja a soma dos divisores próprios de cada um é igual ao outro número. Perceba que podemos reescrever esta propriedades em conjunto $\sigma(m) = \sigma(n) = m + n$, se tornando uma condição necessário e suficiente para obtermos Números Amigáveis. O primeiro par de números amigáveis foi descobertos por Pythagoras, 220 e 284, e são o menor par encontrado. Observe que os divisores próprios de 220 são 1, 2, 4, 5, 10, 11, 20, 22, 44, 55 e 110, cuja soma é 284; e os divisores próprios de 284 são 1, 2, 4, 71 e 142, e a soma deles é 220. Números com esta característica foram encontrados por Euler, Fermat, Descartes e outros matemáticos, ver mais em (5). Em 1946 haviam sido encontrados 390 pares, mas com o avanço das tecnologias e programas computacionais atualmente há mais de 1.222.744.828 pares amigáveis conhecidos. Uma lista de pares amigáveis conhecidos, organizada de acordo com o número de dígitos no menor membro, está disponível em (6). Neste referência o leitor pode encontrar os nomes dos descobridores e a quantidade de pares que cada um descobriu, artigos sobre o tema, um espaço para envio de um par que ele possa encontrar e ainda pode participar do projeto que visa encontrar todos os pares amigáveis com números menores que 10^{20}.

Teorema 2.29 (Euler)**.** *Seja n um número inteiro par. Então n é perfeito, se e somente se, n é da forma $n = 2^{p-1} \cdot (2^p - 1)$, onde p e $2^p - 1$ são primos.*

Demonstração. Pela definição de número perfeito que foi dada no Observação 2.19, devemos mostrar que $\sigma(n) = 2n$. Vimos que $\sigma(n)$ é uma função multiplicativa quando restrita a números

coprimos (veja Teorema 2.22), então podemos calcular $\sigma(n)$ para $n = 2^{p-1}(2^p - 1)$ da seguinte forma:

$$\sigma(2^{p-1} \cdot (2^p - 1)) = \sigma(2^{p-1}) \cdot \sigma\,(2^p - 1) \tag{2.1}$$

Do enunciado $(2^p - 1)$ é um número primo, então $\sigma\,(2^p - 1) = (2^p - 1) + 1 = 2^p$. E do Teorema 2.20 teremos $\sigma(2^{p-1}) = \frac{2^{(p-1)+1}-1}{2-1} = 2^p - 1$. Retornando para equação (2.1)

$$\begin{aligned}\sigma(2^{p-1} \cdot (2^p - 1)) &= \sigma(2^{p-1}) \cdot \sigma(2^p - 1)\\ &= (2^{(p)} - 1) \cdot 2^p\\ &= 2 \cdot 2^{p-1} \cdot (2^{(p)} - 1) = 2n\end{aligned}$$

Mostramos que n é um número perfeito. Por outro lado, suponha que n seja um número perfeito, como n é par podemos escrever $n = 2^{k-1}m$, com m um natural ímpar e $k \geq 2$. Sabemos que σ é multiplicativa, então

$$\sigma(n) = \sigma(2^{k-1}m) = \sigma(2^{k-1})\sigma(m) = (2^k - 1)\sigma(m)$$

E como n é perfeito teremos $\sigma(n) = 2n = 2(2^{k-1}m) = 2^k m$. Assim

$$2^k m = (2^k - 1)\sigma(m)$$

Como $(2^k - 1)$ não divide 2^k, então $(2^k - 1)$ divide m, então podemos considerar $m = (2^k - 1)M$, para algum $M \in \mathbb{N}$, assim

$$2^k M = \sigma(m).$$

Como m e M são ambos divisores de m, teremos

$$2^k M = \sigma(m) > m + M = 2^k M$$

assim $\sigma(m) = m + H$, ou seja, m possui apenas dois divisores, portanto m é primo. Assim $m = 2^k - 1$ é primo e provamos que o número n tem a forma prescrita. □

Observação 2.30. Um grande mistério relacionado a esse teorema é saber quantos primos na forma $2^p - 1$ existem, até hoje não foi provado se existem infinitos. Primos nesta forma são chamados de *Primos de Mersene*. Os primeiros primos de Mersene entre $2^2 - 1$ e $2^{13.466.917} - 1$ foram identificados, sendo 39 ao todo. Atualmente, temos o registro de 51 primos de Mersene. A descoberta mais recente foi devida a Patrick Laroche em dezembro de 2018, sendo $p = 2^{82.589.933} - 1$ um primo com $24.862.048$ dígitos. A descoberta anterior ocorreu com uma diferença de aproximadamente um ano, por Jonathan Pace, onde o primo de Mersene $p = 2^{77.232.917} - 1$ possuía $23.249.426$ dígitos. Para mais informações sobre os primos de Mersene, Patrick Laroche e detalhes sobre a descoberta e a verificação deste primo conhecido como M82589933, o leitor pode acessar (7). Neste site ainda é possível baixar um software grátis para buscar primos de Mersenne, e caso encontre algum novo primo, ainda pode receber prêmios em dinheiro.

Proposição 2.31. *(4, Problema 6.3.1) Para todo* $n \geq 2$

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

Demonstração. Note que

$$\left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \frac{n-1}{k} \right\rfloor = \begin{cases} 1 & se \quad k|n, \\ 0 & k \quad no \quad divide \quad n. \end{cases}$$

Então

$$\sum_{k=1}^{n} k \left(\left\lfloor \frac{n}{k} \right\rfloor - \left\lfloor \frac{n-1}{k} \right\rfloor \right) = \sum_{k|n} k = \sigma(n)$$

□

Observação 2.32. Um número natural n é um número primo, se somente se $\sigma(n) = n+1$. Então

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

se e somente se n for primo.

Exemplo 2.33. Considere $n = 7$, teremos

$$\begin{aligned} \sum_{k=1}^{7} k \left(\left\lfloor \frac{7}{k} \right\rfloor - \left\lfloor \frac{7-1}{k} \right\rfloor \right) &= 1 \left(\left\lfloor \frac{7}{1} \right\rfloor - \left\lfloor \frac{6}{1} \right\rfloor \right) + 2 \left(\left\lfloor \frac{7}{2} \right\rfloor - \left\lfloor \frac{6}{2} \right\rfloor \right) + 3 \left(\left\lfloor \frac{7}{3} \right\rfloor - \left\lfloor \frac{6}{3} \right\rfloor \right) \\ &\quad + 4 \left(\left\lfloor \frac{7}{4} \right\rfloor - \left\lfloor \frac{6}{4} \right\rfloor \right) + 5 \left(\left\lfloor \frac{7}{5} \right\rfloor - \left\lfloor \frac{6}{5} \right\rfloor \right) + 6 \left(\left\lfloor \frac{7}{6} \right\rfloor - \left\lfloor \frac{6}{6} \right\rfloor \right) \\ &\quad + 7 \left(\left\lfloor \frac{7}{7} \right\rfloor - \left\lfloor \frac{6}{7} \right\rfloor \right) \\ &= 1(7-6) + 2(3-3) + 3(2-2) + 4(1-1) + 5(1-1) \\ &\quad + 6(1-1) + 7(1-0) \\ &= 1(1) + 2(0) + 3(0) + 4(0) + 5(0) + 6(0) + 7(1) \\ &= 1 + 7 \end{aligned}$$

Concluímos assim que 7 é um número primo.

A seguir temos dois exemplos que envolvem a função estudada, sendo um deles da Olimpíada Bielorrussa de Matemática, e encerraremos esta seção com a generalização da função.

Exemplo 2.34. (8, Problema 6.2.15) Se n é um inteiro positivo composto, então

$$\sigma(n) > n + \sqrt{n}$$

Demonstração. Como n é composto, existe um divisor d_1 de n, tal que $d_1 \neq 1$ e $d_1 \leq n$. Como $\frac{n}{d_1}$ é divisor de n, segue que $\frac{n}{d_1} \geq \sqrt{n}$. Desta forma, se $d_1 \leq n$ então $\frac{n}{d_1} \geq \sqrt{n}$. Portanto

$$\sigma(n) = \sum_{d|n} d \geq n + \frac{n}{d_1} + 1 \geq n + \sqrt{n} + 1 > n + \sqrt{n}$$

□

Exemplo 2.35. (2, Problema 5.7) Demonstrar que

$$\frac{\sigma(n)}{\tau(n)} \geq \sqrt{n}$$

Demonstração. Note que a desigualdade vale para $n = 1$, pois $\frac{\sigma(1)}{\tau(1)} = 1 = \sqrt{1}$. Agora vamos mostrar que vale para qualquer $n \geq 2$. Sejam $d_1, d_2, \cdots, d_k$ todos os divisores de n, onde $k = \tau(n)$. Eles podem ser reescritos como $\frac{n}{d_1}, \frac{n}{d_2}, \cdots, \frac{n}{d_k}$. Então

$$\begin{aligned}\sigma(n)^2 &= (d_1 + d_2 + \cdots + d_k) \cdot \left(\frac{n}{d_1} + \frac{n}{d_2} + \cdots + \frac{n}{d_k}\right) \\ &= n \cdot (d_1 + d_2 + ... + d_k) \cdot \left(\frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_k}\right) \geq n \cdot \tau(n)^2\end{aligned}$$

Como todos os termos são positivos, podemos fazer algumas operações:

$$\begin{aligned}\sigma(n)^2 &\geq n \cdot \tau(n)^2 \\ \frac{\sigma(n)^2}{\tau(n)^2} &\geq n \\ \frac{\sigma(n)}{\tau(n)} &\geq \sqrt{n}.\end{aligned}$$

□

Exemplo 2.36. (4, Problema 6.3.5)(Olimpíada Bielorrussa de Matemática - 1999) Para qualquer $n \geq 2$

$$\sigma(n) < n \cdot \sqrt{2\tau(n)}$$

Demonstração. Os divisores de n podem ser escritos como $\frac{n}{d_1}, \frac{n}{d_2}, ..., \frac{n}{d_{\tau(n)}}$. Da expansão do quadrado, temos a seguinte desigualdade:

$$\sigma(n)^2 \leq \tau(n) \sum_{i=1}^{\tau(n)} d_i^2$$

temos

$$\sigma(n) \leq \sqrt{\tau(n) \sum_{i=1}^{\tau(n)} d_i^2}.$$

Note que

$$\sum_{i=1}^{\tau(n)} d_i^2 = n^2 \cdot \frac{1}{n^2} \cdot \sum_{i=1}^{\tau(n)} d_i^2 = n^2 \left(\frac{1}{n^2} \cdot \sum_{i=1}^{\tau(n)} d_i^2 \right) = n^2 \cdot \sum_{i=1}^{\tau(n)} \frac{1}{d_i^2}$$

e como

$$\sum_{i=1}^{\tau(n)} \frac{1}{d_i^2} \leq \sum_{j=1}^{\tau(n)} \frac{1}{j^2} < \sum_{i=1}^{\infty} \frac{1}{j^2} = \frac{\pi^2}{6}$$

teremos

$$\sigma(n) \leq \sqrt{\tau(n) \sum_{i=1}^{\tau(n)} d_i^2} = \sqrt{\tau(n) \cdot n^2 \cdot \sum_{i=1}^{\tau(n)} \frac{1}{d_i^2}} < \sqrt{\tau(n) \cdot n^2 \cdot \frac{\pi^2}{6}}$$

Mas $\frac{\pi^2}{6} < 2$, logo

$$\sigma(n) < \sqrt{\tau(n) \cdot n^2 \cdot 2} < n\sqrt{2\tau(n)}.$$

□

Observação 2.37. A generalização da função $\sigma(n)$ é representada por $\sigma_k(n)$, que é o resultado da soma das $k - simas$ potências dos divisores positivos de n, incluindo 1 e n, sendo k é um número complexo.

$$\sigma_k(n) = \sum_{d|n} d^k$$

Esta função se envolve em várias relações, como a Função Zeta de Riemann e a Série de Eisenstein. Essas funções foram bastante estudadas pelo matemático indiano Srinivasa Ramanujan, responsável por um grande número de congruências e identidades a elas referentes. Perceba que neste capítulo realizamos o estudo de $\sigma_1(n)$, que é a soma das primeira potências dos divisores positivos de n, para este caso onde $k = 1$ usamos a simbologia $\sigma(n)$. Em particular, temos a soma dos divisores positivos elevados a $k = 0$ potência:

$$\sigma_0(n) = \sum_{d|n} d^0 = \sum_{d|n} 1 = \tau(n).$$

3 Função Totiente de Euler

A função Totiente é também chamada por Função Fi de Euler, é a função que calcula a quantidade de números inteiros positivos que são relativamente primos com n não excedendo n e denotaremos por $\phi(n)$.

Foi o matemático suíço Leonhard Euler (1707-1783) que a determinou. Ele foi um dos maiores matemáticos de todos os tempos. Nascido na Suíça, era filho de um pastor protestante que esperava que seguisse os passos do pai. Euler possuía facilidade para o aprendizado de línguas e uma enorme habilidade para efetuar contas mentalmente. Aos 14 anos já ingressava na Universidade da Basiléia, mas foi aos 20 anos que ganhou reconhecimento internacional, quando recebeu uma menção honrosa da Academia de Ciências de Paris. Assumiu a função de físico na nova Academia de São Petersbugo, na Rússia, em 1727, começando assim sua vida profissional. Em 1733, Euler já assumiu a cátedra de matemática nesta mesma academia.

Euler produziu resultados matemáticos ao longo de sua vida, mesmo quando a doença o assolou e ficou totalmente cego em 1771, isto não diminuiu a sua produtividade científica. Ele escreveu sobre vários temas como números complexos, teoria das funções, cálculo diferencial e integral, música, teoria dos números, teoria das partições e mecânica, tornando assim um dos maiores matemáticos de todos os tempos (1).

No entanto, na época Euler não escolheu nenhum símbolo específico para representar esta função. A notação ϕ foi introduzida por Gauss no livro *Disquisitiones Arithmeticae* publicado a primeira vez em 1801, mas uso do parênteses em torno do argumento não foi utilizado, sendo usado na seguinte forma ϕn. Foi o matemático James Joseph Sylvester que escolheu o nome Totiente, que tinha o costume de inventar palavras novas para as coisas com as quais tratava. Este matemático fez contribuições nas áreas da teoria matricial, teoria dos invariantes, análise combinatória e teoria dos números.

Uma das aplicações da função ϕ é na descoberta da ordem do grupo multiplicativo de inteiros módulo n, temos que ϕ é a cardinalidade do grupo de unidades do anel $\mathbb{Z}/n\mathbb{Z}$. Ela também foi usada por Leonhard Euler para provar o Pequeno Teorema de Fermat. Além disso desempenha um papel fundamental na definição do sistema de criptografia do método RSA criado em 1977 por R. Rivest, A. Shamire e L. Adleman.

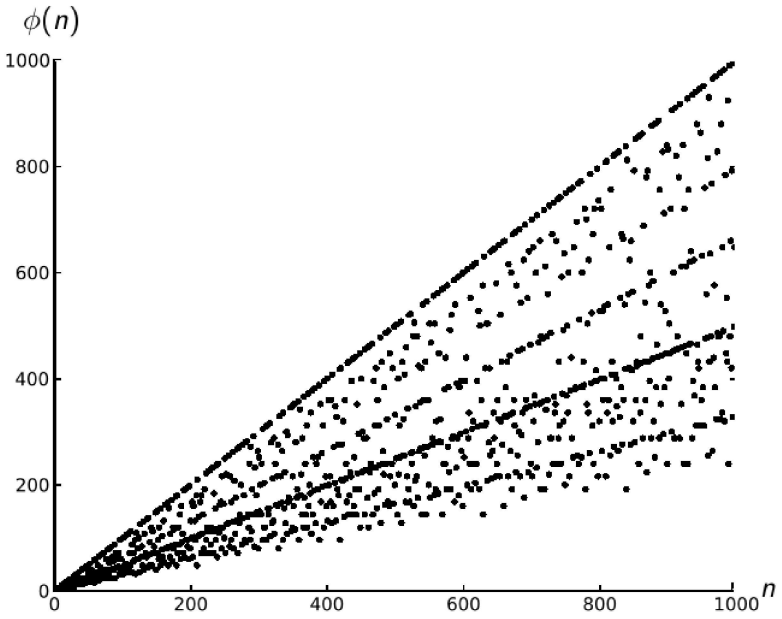
Nesta seção faremos um estudo sobre a função Totiente, iniciamos apresentando a definição, em seguida trazemos algumas propriedades e exemplos. Alem disso, nas próximas subseções faremos um estudo combinatorial desta função e a relacionaremos com o principio da inclusão e exclusão.

Definição 3.1. Seja n um número natural. Definimos a função $\phi : \mathbb{N} \to \mathbb{N}$ dada por $\phi(n) =$

$|\{k \in \mathbb{N} : 1 \leq k \leq n \text{ e } \text{mdc}(k,n) = 1\}|$, na qual $|A|$ indica o números de elementos do conjunto A.

A seguir temos o gráfico de $\phi(n)$ para $1 \leq n \leq 1000$:

Figura 3 – Gráfico de $\phi(n)$



Fonte:<www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/euler-s-totient-function-phi-function> (Editada pelo autor)

Observe que $\phi(1) = 1$, pois o único inteiro menor ou igual a 1 é ele mesmo e ainda temos $\text{mdc}(1,1) = 1$. Para $n \geq 2$ temos $n = \text{mdc}(n,n) \neq 1$, de onde podemos concluir que $\phi(n) < n$.

Exemplo 3.2. Vamos calcular $\phi(8)$. Observe que

$$\{x \in \mathbb{N} : 1 \leq x \leq 8 \text{ e } \text{mdc}(x,8) = 1\} = \{1,3,5,7\}.$$

Desde que o conjunto acima possui 4 elementos, concluímos que $\phi(8) = 4$.

Exemplo 3.3. Vamos calcular $\phi(15)$. Temos

$$\{x \in \mathbb{N} : 1 \leq x \leq 15 \text{ e } \text{mdc}(x,15) = 1\} = \{1,2,4,7,8,11,13,14\}.$$

Observe que o conjunto acima possui 8 elementos, portanto $\phi(15) = 8$.

Proposição 3.4. *Temos $\phi(2) = 1$ e $\phi(n) \geq 2$, para todo número natural $n \geq 3$.*

Demonstração. Temos que o único número relativamente primo com 2 e menor que 2 é o 1, logo $\phi(2) = 1$. Para $n \geq 3$ temos $n - 1 \geq 2$, como dois números consecutivos são primos entre si, segue que, para $n \geq 3$, n e $n-1$ são relativamente primos. E como $\text{mdc}(n,1) = 1$, temos 1 e $(n-1)$ coprimos com n. Logo $\phi(n) \geq 2$ para todo número natural $n \geq 3$. □

Proposição 3.5. *Seja n é um número natural, então $\phi(n) = n - 1$, se, e somente se, n é primo.*

Demonstração. Suponha que $\phi(n) = n - 1$, então para todo $m < n$ temos mdc$(n, m) = 1$. Logo, n não pode ser composto por um produto de fatores primos menores que n, ou seja, n é primo. Suponha que n seja primo, então todos os números naturais menores que n são relativamente primos com n, os números naturais menores que n são $1, 2, 3, ..., n - 1$, portanto $\phi(n) = n - 1$. □

Exemplo 3.6. Primos da forma p e $p + 2$ são chamados de *primos gêmeos*. Mostraremos que para primos gêmeos teremos $\phi(p + 2) = \phi(p) + 2$. Pela proposição anterior, para $n = p + 2$ primo temos

$$\phi(p + 2) = (p + 2) - 1 = p + 1 = (p - 1) + 2 = \phi(p) + 2$$

Como queríamos mostrar.

Para calcularmos o valor de $\phi(n)$ para um natural n qualquer, precisaremos provar que a função ϕ de Euler é multiplicativa, ou seja, $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$ para m e n inteiros positivos com mdc$(m, n) = 1$. Para conseguirmos demonstrar este fato, iremos nos apoiar na seguinte proposição e definição:

Proposição 3.7. *Dados k, m e n com mdc$(m, n) = 1$, então os restos das divisões de $k, k + n, k + 2n, ..., k + (m - 1)n$ por m, são todos diferentes.*

Definição 3.8. Um sistema completo de resíduo é um conjunto de números inteiros $\{a_1, a_2, \cdots, a_k\}$ coprimos com n, tais que para qualquer $x \in \mathbb{Z}$, se $mdc(x, n) = 1$ então existe um e só um i tal que x e a_i deixam o mesmo resto quando dividido por n.

Demonstração. Sejam t e s inteiros positivos não nulo tais que $t \neq s$ e $t < m$. Suponha, por absurdo, que $k + sn$ e $k + tn$ deixem o mesmo resto na divisão por m. Assim $k + sn = mq + r$ e $k + tn = mq' + r$. Observe que

$$(k + sn) - (k + tn) = (mq + r) - (mq' + r),$$

então

$$q - q' = \frac{(s - t)n}{m}.$$

Desta forma, m divide o produto $(s-t)n$. Como, por hipótese, temos mdc$(m, n) = 1$, concluímos que m divide $(s - t)$, o que é impossível pois $0 \leq s$ e $t < m$. Portanto, concluímos que os restos são todos diferentes. □

Teorema 3.9. *Dados m e n inteiros positivos com mdc$(m, n) = 1$, então*

$$\phi(m \cdot n) = \phi(m) \cdot \phi(n).$$

Demonstração. Vamos dispor dos números de 1 até $m \cdot n$ da seguinte maneira:

1	2	$\cdots$	k	$\cdots$	n
1n+1	1n+2	$\cdots$	1n+k	$\cdots$	2n
2n+1	2n+2	$\cdots$	2n+k	$\cdots$	3n
3n+1	3n+2	$\cdots$	3n+k	$\cdots$	4n
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$
(m-1)n+1	(m-1)n+2	$\cdots$	(m-1)n+k	$\cdots$	mn

Para encontrar os inteiros que são primos com n, devemos observar a coluna k somente se mdc$(n,k) = 1$, ou seja, observar as colunas dos $\phi(n)$ elementos que são primos com n. Na primeira linha temos $\phi(n)$ elementos que são primos com n, logo são $\phi(n)$ colunas para encontrarmos os elementos primos com m. Agora, vamos analisar os elementos de cada coluna. Para a coluna k os elementos $0n+k, 1n+k, 2n+k, ..., (m-1)n+k$, deixam restos diferentes quando divididos por m, onde mdc$(m,n) = 1$, formando um sistema completo de resíduos módulo m. Suponha que não forme um sistema completo de resíduos, então pegue dois elementos quaisquer desta coluna obedecendo a seguinte equação $(m-x)\cdot n+k \equiv (m-y)\cdot n+k \mod m \iff (m-x)\cdot n \equiv (m-y)\cdot n \mod m \iff (m-x) \equiv (m-y) \mod m \iff x \equiv y \mod m$, contradição. Além disso sabemos que $(m,x) = (m,r)$ onde r é o resto na divisão de x por m, assim em cada coluna teremos os elementos perpassando por todos os restos de m. Logo, cada uma dessas colunas tem $\phi(m)$ elementos primos com m, e como já são primos com n, serão primos com $m \cdot n$. Concluímos, portanto, que $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$. □

Exemplo 3.10. Para ilustrar o método do Teorema 3.9, sejam $m = 6$ e $n = 5$. Vamos mostrar que $\phi(5 \cdot 6) = \phi(5) \cdot \phi(6)$. Observe a tabela abaixo contendo os números de 1 a $5 \cdot 6 = 30$

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25
26	27	28	29	30

Para encontrar os inteiros que são primos com 5, devemos observar a coluna k somente se mdc$(5,k) = 1$, ou seja, observar as colunas dos $\phi(5) = 4$ elementos que são primos com 5, então consideraremos $k = \{1,2,3,4\}$. Na primeira linha temos 4 elementos que são primos com 5, logo são 4 colunas para encontrarmos os elementos primos com 6. Como mdc$(5,6) = 1$, os elementos de cada coluna deixam restos diferentes quando divididos por 6, pois formam um sistema completo de resíduos módulo 6. Suponha que não forme um sistema completo de resíduos, então pegue dois elementos quaisquer desta coluna obedecendo a seguinte equação $(6-x)\cdot 5+k \equiv (6-y)\cdot 5+k \mod 6 \iff (6-x)\cdot 5 \equiv (6-y)\cdot 5 \mod 6 \iff (6-x) \equiv (6-y) \mod 6 \iff x \equiv y \mod 6$, contradição. Além disso sabemos que $(6,x) = (6,r)$ onde r é o resto na divisão de x por 6, assim em cada coluna teremos os elementos

perpassando por todos os restos de 6. (Por exemplo na coluna $k = 1$ teremos {1,6,11,16,21,26} correspondem respectivamente aos restos {1,0,5,4,3,2} na divisão por 6). Logo, cada uma dessas colunas tem $\phi(6) = 2$ elementos primos com 6. Na coluna 1 temos $\{1, 11\}$. Na coluna 2 temos {7, 17}. Na coluna 3 temos {13, 23}. Na coluna 4 temos {19, 25}. Concluímos, portanto, que $8 = \phi(5 \cdot 6) = \phi(5) \cdot \phi(6) = 4 \cdot 2$.

Corolário 3.11. *Se m_1, m_2,...,m_r são primos entre si, dois a dois, então*

$$\phi(m_1 \cdot m_2 \cdot ... \cdot m_r) = \phi(m_1) \cdot \phi(m_2) \cdots \phi(m_r).$$

Demonstração. Por indução sobre o número r de fatores. Para $r = 1$ temos $\phi(m_1) = \phi(m_1)$. Suponha que seja válido para $r = k$,

$$\phi(m_1 \cdot m_2 \cdot ... \cdot m_k) = \phi(m_1) \cdot \phi(m_2) \cdots \phi(m_k).$$

Mostraremos que é válida para $r = k + 1$. Considere m_1, m_2,...,m_k, m_{k+1} primos entre si, dois a dois. Considere $a = m_1 \cdot m_2 \cdot ... \cdot m_k$. Observe que a e m_{k+1} são primos entre si, pois mdc$(a, m_{k+1}) = mdc(m_1 \cdot m_2 \cdot ... \cdot m_k, m_{k+1}) = 1$. Como a e m_{k+1} são primos entre si, pelo Teorema 3.9 temos

$$\begin{aligned}\phi(m_1 \cdot m_2 \cdot ... \cdot m_k \cdot m_{k+1}) &= \phi(a \cdot m_{k+1}) \\ &= \phi(a) \cdot \phi(m_{k+1}) \\ &= \phi(m_1 \cdot m_2 \cdot ... \cdot m_k) \cdot \phi(m_{k+1}) \\ &= \phi(m_1) \cdot \phi(m_2) \cdot ... \cdot \phi(m_k) \cdot \phi(m_{k+1})\end{aligned}$$

Assim mostramos que a fórmula é válida para $r = k + 1$, logo, por indução finita, é válida para todo número natural r. □

Sejam m e n números naturais primos entre si, pelo Teorema 3.9 temos $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$. Este resultado não implica que os números relativamente primos com $m \cdot n$ sejam obtidos como produto dos números relativamente primos com m e os relativamente primos com n.

Exemplo 3.12. Sejam $m = 8$ e $n = 5$, são primos entre si. Logo

$$\phi(40) = \phi(8 \cdot 5) = \phi(8) \cdot \phi(5) = 4 \cdot 4 = 16$$

Note que os números relativamente primos com 8 são $\{1, 3, 5, 7\}$ os números relativamente primos com 5 são $\{1, 2, 3, 4\}$, enquanto que os números relativamente primos com 40 são $\{1, 3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39\}$. Note que há números no último conjunto que não são produtos de dois números dos outros dois conjuntos.

Exemplo 3.13. Se $p_1^{\alpha_1}$, $p_2^{\alpha_2}$,...,$p_r^{\alpha_r}$ são primos entre si, dois a dois, então

$$\phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdot ... \cdot \phi(p_r^{\alpha_r}).$$

Vamos agora demonstrar a fórmula para calcular $\phi(p^\alpha)$ para cada inteiro positivo α e cada primo p.

Teorema 3.14. *Seja p um primo e α um inteiro positivo. Então*

$$\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1} \cdot (p-1) = p^\alpha \cdot \left(1 - \frac{1}{p}\right).$$

Demonstração. Sabemos que $\phi(p^\alpha)$ é a quantidade de inteiros positivos não superior a p^α e relativamente primos com p^α. Os únicos números positivos menores e que são relativamente primos com p^α são aqueles que não possuem o fator p. Observe que os números que possuem o fator p são os seguintes múltiplos:

$$p, 2p, 3p, \cdots, kp,$$

onde $kp = p^\alpha$. Logo $k = p^{\alpha-1}$. Portanto, existem $p^{\alpha-1}$ inteiros não primos com p^α. Portanto, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. □

Exemplo 3.15. Vamos calcular $\phi(8)$. Temos $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$.

Teorema 3.16. *Seja $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot \ldots \cdot {p_k}^{r_k}$ a decomposição de n em fatores primos. Então*

$$\phi(n) = {p_1}^{r_1-1} \cdot {p_2}^{r_2-1} \cdot \ldots \cdot {p_k}^{r_k-1} \cdot (p_1 - 1) \cdot (p_2 - 1) \cdot \ldots \cdot (p_k - 1).$$

Demonstração. Como ${p_1}^{r_1}, {p_2}^{r_2}, \cdots, {p_k}^{r_k}$ são potências de números primos distintos, então são dois a dois primos entre si. Pelo Corolário 3.11 temos:

$$\phi({p_1}^{r_1} \cdot {p_2}^{r_2} \cdot \ldots \cdot {p_k}^{r_k}) = \phi({p_1}^{r_1}) \cdot \phi({p_2}^{r_2}) \cdot \ldots \cdot \phi({p_k}^{r_k})$$

Mas, pelo Teorema 3.14 temos $\phi({p_i}^{r_i}) = {p_i}^{r_i-1}(p_i - 1)$, para $i = 1, 2, \cdots, k$. Logo

$$\phi({p_1}^{r_1} \cdot {p_2}^{r_2} \cdot \ldots \cdot {p_k}^{r_k}) = {p_1}^{r_1-1}(p_1 - 1) \cdot {p_2}^{r_2-1}(p_2 - 1) \cdot \ldots \cdot {p_k}^{r_k-1}(p_k - 1).$$

□

Baseados neste teorema, podemos calcular o valor de $\phi(n)$ para algum n relativamente grande, veja um exemplo a seguir.

Exemplo 3.17. Decompondo o número 12600 em fatores primos obtemos $12600 = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7$. Utilizando o Teorema 3.16 temos

$$\begin{aligned}
\phi(12600) &= \phi(2^3 \cdot 3^2 \cdot 5^2 \cdot 7) \\
&= \phi(2^3) \cdot \phi(3^2) \cdot \phi(5^2) \cdot \phi(7) \\
&= 2^2(2-1) \cdot 3^1(3-1) \cdot 5^1(5-1) \cdot 7^0(7^1 - 1) \\
&= 4 \cdot 3 \cdot 2 \cdot 5 \cdot 4 \cdot 1 \cdot 6 \\
&= 2880
\end{aligned}$$

Portanto, o número 12600 possui 2880 inteiros positivos menores que ele mesmo e que relativamente primos com ele.

Exemplo 3.18. Para qualquer número p primo, considere a seguinte soma:

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

Corolário 3.19. *Para todo número natural $n > 2$, $\phi(n)$ é par.*

Demonstração. Se na decomposição de n contém um fator primo $p \geq 3$, considere p^k a maior potência de p nesta decomposição. Podemos escrever n como o seguinte produto de fatores primos entre si $n = p^k \cdot a$. Pelos Teoremas 3.9 e 3.14, segue que $\phi(n) = \phi(p^k) \cdot \phi(a) = p^{k-1}(p-1) \cdot \phi(a)$. Como p é um primo maior que 3, $(p-1)$ é par, logo, $\phi(n)$ é par. Agora, se na decomposição não existir um fator primo $p \geq 3$ podemos escrever n da seguinte forma $n = 2^r$, e como $n > 2$, temos $r > 1$. Temos $\phi(n) = \phi(2^r) = 2^{r-1}.(2-1)$. Como $r > 1$, assim $\phi(n)$ é par. □

Exemplo 3.20. (8, Problema 6.1.4) Mostre que se n é um inteiro positivo então:

$$\phi(2n) = \begin{cases} \phi(n) & \text{se } n \text{ for ímpar.} \\ 2 \cdot \phi(n) & \text{se } n \text{ for par.} \end{cases}$$

Demonstração. Iremos resolver este exemplo usando apenas as propriedades multiplicativas de $\phi(n)$. Se n for ímpar, teremos

$$\begin{aligned} \phi(2n) &= \phi(2) \cdot \phi(n) \\ &= 1 \cdot \phi(n) \\ &= \phi(n). \end{aligned}$$

Para n par, considere $n = 2^k \cdot m$, para algum m ímpar. Teremos

$$\begin{aligned} \phi(2n) &= \phi(2(2^k \cdot m)) \\ &= \phi(2^{k+1} \cdot m)) \\ &= \phi(2^{k+1}) \cdot \phi(m) \\ &= 2^k \cdot (2-1) \cdot \phi(m) \\ &= 2 \cdot 2^{k-1} \cdot (2-1) \cdot \phi(m) \\ &= 2 \cdot \left(2^{k-1} \cdot (2-1) \cdot \phi(m)\right) \\ &= 2 \cdot \left(\phi(2^k) \cdot \phi(m)\right) \\ &= 2 \cdot \left(\phi(2^k \cdot m\right) \\ &= 2 \cdot \phi(n). \end{aligned}$$

□

Corolário 3.21. *Sejam r, s números naturais e p um número primo. Então*

$$\phi(p^r) \cdot \phi(p^s) < \phi(p^{r+s})$$

Demonstração. Pelo Teorema 3.14 temos $\phi(p^r) = p^r\left(1-\frac{1}{p}\right)$ e $\phi(p^s) = p^s\left(1-\frac{1}{p}\right)$. Então

$$\begin{aligned}\phi(p^r)\cdot\phi(p^s) &= p^r\left(1-\frac{1}{p}\right)\cdot p^s\left(1-\frac{1}{p}\right)\\ &= p^{r-1}(p-1)\cdot p^{s-1}(p-1)\\ &= (p^{r+s-2})(p-1)^2\\ &= (p^{r+s-1})\left(\frac{p-1}{p}\right).(p-1)\end{aligned}$$

Note que $\frac{p-1}{p} < 1$, logo $\phi(p^r)\cdot\phi(p^s) < p^{r+s-1}(p-1) = \phi(p^{r+s})$. □

Exemplo 3.22. Observe os seguintes resultados

$$\begin{aligned}\phi(2^2) &= \phi(4) = 2\\ \phi(2^3) &= \phi(8) = 4\\ \phi(2^2\cdot 2^3) &= \phi(32) = 16\end{aligned}$$

Note que $\phi(4)\cdot\phi(8) = 2\cdot 4 < 16 = \phi(32)$. Concluímos que $\phi(2^2)\cdot\phi(2^3) < \phi(2^{2+3})$.

Exemplo 3.23. (9, Exemplo 5.20) Mostre que $\phi(m\cdot n) \geq \phi(m)\phi(n)$ para todo m e n, com igualdade se m e n forem coprimos.

Demonstração. O Teorema 3.9 nos mostra a igualdade ocorre para m e n coprimos. No caso em que não são primos entre si, m e n possuem fatores primos em comum, sejam eles $p_1, p_2, p_3, ..., p_k$. Podemos escrever $m = a\cdot {p_1}^{r_1}\cdot {p_2}^{r_2}\cdot {p_3}^{r_3}\cdots {p_k}^{r_k}$ e $n = b\cdot {p_1}^{s_1}\cdot {p_2}^{s_2}\cdot {p_3}^{s_3}\cdots {p_k}^{s_k}$, onde $mdc(a,b) = 1$. Temos

$$\phi(m\cdot n) = \phi({p_1}^{r_1+s_1}\cdot {p_2}^{r_2+s_2}\cdot {p_3}^{r_3+s_3}\cdots {p_k}^{r_k+s_k})\phi(a)\phi(b)$$

Como p_r e p_s são coprimos para quaisquer r e s, pelo Corolário 3.11, podemos fazer o seguinte cálculo:

$$\phi(m\cdot n) = \phi({p_1}^{r_1+s_1})\cdot\phi({p_2}^{r_2+s_2})\cdot\phi({p_3}^{r_3+s_3})\cdots\phi({p_k}^{r_k+s_k})\phi(a)\phi(b)$$

O Corolário 3.21 nos diz que para cada $i = 1, 2, 3, \cdots, k$ teremos $\phi(p_i^{r_i})\cdot\phi({p_i}^{s_i}) < \phi({p_i}^{r_i+s_i})$. Logo

$$\begin{aligned}\phi(m\cdot n) &> \phi({p_1}^{r_1})\phi({p_1}^{s_1})\phi({p_2}^{r_2})\phi({p_2}^{s_2})\phi({p_3}^{r_3})\phi({p_3}^{s_3})\cdots\phi({p_k}^{r_k})\phi({p_k}^{s_k})\phi(a)\phi(b)\\ &= \phi(m)\phi(n).\end{aligned}$$

Portanto, $\phi(m\cdot n) > \phi(m)\phi(n)$. □

Assim temos o seguinte teorema:

Teorema 3.24. *Se m e n são números naturais que não são primos entre si, então $\phi(m\cdot n) \neq \phi(m)\cdot\phi(n)$.*

Os resultados anteriores são obtidos a partir das propriedades multiplicativas da função ϕ de Euler. Sabemos que um número natural pode ser decomposto em um produto de fatores primos de modo único, mas pode ser escrito como a soma de dois outros números naturais de várias maneiras diferentes, por isso não se espera que ϕ tenha propriedades aditivas. Observe o seguinte exemplo para nos certificarmos:

Exemplo 3.25. Sabemos que $\phi(7) = 6$. Podemos decompor o número 7 das seguintes maneiras:

$$7 = 1 + 6, \text{ temos } \phi(7) \neq \phi(1) + \phi(6) = 1 + 2 = 3$$
$$7 = 2 + 5, \text{ temos } \phi(7) \neq \phi(2) + \phi(5) = 1 + 4 = 5$$
$$7 = 3 + 4, \text{ temos } \phi(7) \neq \phi(3) + \phi(4) = 2 + 2 = 4$$

Perceba que nenhumas das respostas é igual ao valor de $\phi(7)$. Além disso, note que os resultados são menores que $\phi(7)$, o que motiva a proposição seguinte.

Proposição 3.26. *Seja p um primo, para qualquer decomposição aditiva $p = m + n$, m e n naturais, tem-se $\phi(m) + \phi(n) < \phi(p)$.*

Demonstração. Como m e n podem ser primos ou não temos $\phi(m) \leq m - 1$ e $\phi(n) \leq n - 1$, então

$$\phi(m) + \phi(n) \leq (m - 1) + (n - 1) < m + n - 1 = p - 1 = \phi(p)$$

Portanto, $\phi(m) + \phi(n) < \phi(p)$. □

Teorema 3.27. *Seja $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot \ldots \cdot {p_k}^{r_k}$ a decomposição de n em fatores primos.*

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Demonstração. Como a função ϕ é multiplicativa,

$$\phi(n) = \phi({p_1}^{r_1} \cdot {p_2}^{r_2} \cdot \ldots \cdot {p_k}^{r_k}) = \phi({p_1}^{r_1}) \cdot \phi({p_2}^{r_2}) \cdot \ldots \cdot \phi({p_k}^{r_k}).$$

Pelo Teorema 3.14 temos $\phi(p^r) = p^r\left(1 - \frac{1}{p}\right)$, logo

$$\begin{aligned}
\phi(n) &= p_1^{r_1}\left(1 - \frac{1}{p_1}\right) \cdot p_2^{r_2}\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot p_k^{r_k}\left(1 - \frac{1}{p_k}\right) \\
&= p_1^{r_1} \cdot p_2^{r_2} \cdot \ldots \cdot p_k^{r_k}\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) \\
&= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).
\end{aligned}$$

□

Exemplo 3.28. Vamos calcular $\phi(15)$ de outra forma. Inicialmente encontramos os primos presentes na fatoração de $n = 15$. Temos que $15 = 3 \cdot 5$, então

$$\begin{aligned}\phi(15) &= 15\prod_{i=1}^{2}\left(1-\frac{1}{p_i}\right)\\ &= 15\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)\\ &= 15\left(\frac{2}{3}\right)\cdot\left(\frac{4}{5}\right)\\ &= 8\end{aligned}$$

Então $\phi(15) = 8$, assim como foi encontrado na resolução do Exemplo 3.3 quando encontramos os elementos do conjunto $\{x \in \mathbb{N}{:}1 \leq x \leq 15 \text{ e } \text{mdc}(x, 15) = 1\}$.

Exemplo 3.29. Vamos refazer o Exemplo 3.17 e calcular $\phi(n)$ para $n = 12600$ de outra forma. Vimos que a fatoração é $12600 = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7$, então consideraremos os primos 2,3,5 e 7.

$$\begin{aligned}\phi(12600) &= 12600\prod_{i=1}^{4}\left(1-\frac{1}{p_i}\right)\\ &= 12600\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)\cdot\left(1-\frac{1}{7}\right)\\ &= 12600\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)\left(\frac{6}{7}\right)\\ &= 2880\end{aligned}$$

Logo, confirmamos que existem 2880 números inteiros menores que 12600 primos com ele. Fica evidente a dificuldade que teríamos para determinar todos os elementos do conjunto $\{x \in \mathbb{N}{:}1 \leq x \leq n \text{ e } \text{mdc}(x, n) = 1\}$ quando n for relativamente grande. Mas, através da fórmula encontrada no Teorema 3.27 se torna rápido o cálculo de $\phi(n)$.

Proposição 3.30. *Se todo primo que divide n divide m então $\phi(m \cdot n) = n \cdot \phi(m)$.*

Demonstração. Podemos escrever m e n como um produto de fatores primos

$$\begin{aligned}n &= {p_1}^{r_1}\cdot {p_2}^{r_2}\cdot \ldots \cdot {p_i}^{r_i}\\ m &= {p_1}^{s_1}\cdot {p_2}^{s_2}\cdot \ldots \cdot {p_i}^{s_i}\cdot {q_1}^{t_1}\cdot {q_2}^{t_2}\cdot \ldots \cdot {q_i}^{t_i}\end{aligned}$$

Considere $t = m \cdot n$, logo $t = {p_1}^{r_1+s_1}\cdot {p_2}^{r_2+s_2}\cdot \ldots \cdot {p_i}^{r_i+s_i}\cdot {q_1}^{s_1}\cdot {q_2}^{s_2}\cdot \ldots \cdot {q_i}^{s_i}$

pelo Teorema 3.27

$$\begin{aligned}\phi(t) &= t\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot \ldots \cdot \left(1-\frac{1}{p_i}\right)\cdot\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdot \ldots \cdot \left(1-\frac{1}{q_i}\right)\\ &= m\cdot n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot \ldots \cdot \left(1-\frac{1}{p_i}\right)\cdot\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdot \ldots \cdot \left(1-\frac{1}{q_i}\right)\\ &= n\left[m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot \ldots \cdot \left(1-\frac{1}{p_i}\right)\cdot\left(1-\frac{1}{q_1}\right)\left(1-\frac{1}{q_2}\right)\cdot \ldots \cdot \left(1-\frac{1}{q_i}\right)\right]\\ &= n\cdot\phi(m)\end{aligned}$$

□

Exemplo 3.31. (2, Exemplo 5.15) Se n é composto, mostre que $\phi(n) \leq n - \sqrt{n}$.

Demonstração. Como n é composto, existe um fator primo $p_i \leq \sqrt{n}$. Então

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_k}\right) \leq n\left(1 - \frac{1}{p_i}\right) \leq n\left(1 - \frac{1}{\sqrt{n}}\right) = n - \sqrt{n}$$

. □

Exemplo 3.32. (9, Exemplo 5.21) Sejam d e n números naturais, se d divide n então $\phi(d)$ divide $\phi(n)$.

Demonstração. Vimos que $\phi(d) = d\prod\left(1 - \frac{1}{p_d}\right)$, onde p_d são os primos distintos que dividem d. Como d divide n então podemos escrever $n = kd$ para algum k natural, dependendo dos números primos presentes na fatoração de k, teremos 3 possibilidades.
Primeiro caso, se todos os fatores primos em k sejam diferentes dos fatores em d teremos

$$\phi(n) = \phi(kd) = k\prod\left(1 - \frac{1}{p_k}\right) \cdot d\prod\left(1 - \frac{1}{p_d}\right)$$

e portanto

$$\frac{\phi(n)}{\phi(d)} = k\prod\left(1 - \frac{1}{p_k}\right) = \phi(k)$$

Segunda possibilidade, se dentre os p_k fatores primos de k encontramos fatores presentes e não presentes na fatoração de d teremos outra forma de raciocínio. Sejam ${p'}_k$ os fatores existentes na fatoração de k que não existam na fatoração de d . Neste caso teremos

$$\phi(n) = \phi(kd) = kd\prod\left(1 - \frac{1}{{p'}_k}\right) \cdot \prod\left(1 - \frac{1}{p_d}\right)$$

E, por fim, se todos os fatores primos de k sejam fatores existentes em d teremos, pela Proposição 3.30

$$\phi(n) = \phi(kd) = k\phi(d) = k \cdot d\prod\left(1 - \frac{1}{p_d}\right).$$

E assim

$$\frac{\phi(n)}{\phi(d)} = k.$$

□

Exemplo 3.33. Considere $d = 15$ e $n = 135$, sabemos que 15 divide 135, então veremos que $\phi(15)$ divide $\phi(135)$.
Temos

$$\phi(15) = \phi(3 \cdot 5) = 15\prod\left(1 - \frac{1}{p_{15}}\right) = 15\left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 15\left(\frac{2}{3}\right) \cdot \left(\frac{4}{5}\right) = 8$$

e

$$\phi(135) = \phi(3^3 \cdot 5) = 135 \prod \left(1 - \frac{1}{p_{135}}\right) = 135\left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) = 135\left(\frac{2}{3}\right) \cdot \left(\frac{4}{5}\right) = 72.$$

Logo $\frac{\phi(135)}{\phi(15)} = \frac{72}{8} = 9$. Observe que $135 = k \cdot 15$ com $k = 9$. Como não existem primos na fatoração de $k = 9$ que sejam diferentes dos existentes na fatoração de $d = 15$ teremos $\frac{\phi(n)}{\phi(d)} = k$, como vimos na demonstração da proposição anterior.

Observação 3.34. O matemático Robert Carmichael propôs um enigma em 1907 que ainda permanece sem solução. Basicamente, Carmichael conjeturou que para todo inteiro positivo n, há pelo menos um outro inteiro $m \neq n$ tal que $\phi(m) = \phi(n)$. Essa conjectura foi declarada em 1907, mas como um teorema, no entanto sua prova foi falha e em 1922 Carmichael retirou sua reivindicação e declarou a conjectura como um problema em aberto. Por exemplo, para $\phi(m) = 4$ quando m assume um dos seguintes valores 5,8,10 e 12. Assim se tomarmos qualquer um desses valores como m, então qualquer um dos outros três valores pode ser usado como m para o qual $\phi(m) = \phi(n)$ A conjectura nos diz que em cada caso há mais de um valor de n com o mesmo valor de $\phi(n)$. Observe alguns valores na tabela a seguir:

k	Números n tais que $\phi(n) = k$	Número de soluções
1	1,2	2
2	3,4,5	3
3	5,8,10,12	4
4	7, 9, 14, 18	4
6	7, 9, 14, 18	4
8	15,16,20,24,30	5
10	11, 22	2
12	13, 21, 26, 28, 36, 42	6
16	17, 32, 34, 40, 48, 60	6

A conjectura ainda não foi mostrada como verdadeira para os inteiros pares positivos, mas podemos verificar facilmente que é verdadeira para números ímpares. Considere r um inteiro ímpar positivo e relembre o no fato de que $\phi(2) = 1$.

$$\phi(2r) = \phi(2)\phi(r) = \phi(n).$$

Existem alguns limites inferiores muito altos para esta conjectura. Carmichael mostrou que qualquer contra-exemplo para a conjectura deve ser pelo menos 10^{37}. Victor Klee estendeu esse resultado para 10^{400}, e um limite inferior de $10^{10^{10}}$ foi determinado por Kevin Ford em 1998.

Mais um problema não resolvido é o problema de Lehmer: existe algum número n composto tal que $\phi(n)$ divida $n - 1$. Observe que para qualquer primo o problema é fácil de se resolver. Considere p um número primo, teremos $\phi(p) = p - 1$ e assim $\phi(p)$ divide $p - 1$. D. H. Lehmer conjecturou em 1932 que não há número composto com tal propriedade. Para esse e outros problemas não resolvidos em teoria dos números o leitor pode consultar (10).

3.1 Estudo combinatorial de $\phi(n)$

Estudaremos nessa seção um teorema devido a Gauss envolvendo a função ϕ de Euler. Segundo (1), Carl Friederich Gauss (1777-1855) é um dos maiores matemáticos de todos os tempos. Nasceu na Alemanha, filho de uma modesta família, aprendeu a ler sozinho e possuía enorme habilidade para realizar cálculos mentais. Em 1799 ele demonstra o Teorema Fundamental da Álgebra , que havia sido enunciado por vários matemáticos mas nenhuma prova correta tinha sido apresentada. Gauss foi um dos primeiros a tratar os números complexos dando-lhes a representação geométrica como pontos do plano cartesiano. Gauss foi um dos criadores das geometrias não-euclidianas, da geometria diferencial, das funções de variável complexas, da topologia e da teoria algébrica dos números. Deu contribuições à matemática aplicada, física e astronomia e teoria das probabilidades. "Gauss teve o poder de mudar os rumos da matemática a partir dos seus trabalhos revolucionários, apresentados como extremo rigor e grande concisão e elegância. Por isso, foi considerado, pelos seus contemporâneos e pelas gerações que se sucederam, um príncipe da rainha das ciências"(1).

Teorema 3.35. *(3, Teorema 6-1)(Gauss) Considere a soma dos valores da função $\phi(n)$ para todos os d divisores de n. Então*

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

Demonstração. Seja S_n o conjunto $\{1, 2, 3, .., n\}$. Temos claramente que a cardinalidade de S_n é $|S_n| = n$. Para cada d que divide n, denotamos por $T_d(n)$ o conjunto de inteiros positivos não excedendo n, cujo maior divisor comum com n é d. Daí, para cada n os conjuntos $T_d(n)$ não têm elementos comuns. Além disso, para qualquer $m \in S_n$, vemos que $m \in T_d(n)$ onde $d = \text{mdc}(m, n)$. Consequentemente, $n = |(S_n)| = \sum_{d|n} |T_d(n)|$. Agora, mostraremos que $T_d(n)$ tem $\phi\left(\frac{n}{d}\right)$ elementos. Primeiro note que todos os elementos de $T_d(n)$ são múltiplos de d e são menores ou iguais a n. Observe que os únicos números da forma ad em $T_d(n)$ são aqueles para os quais $\text{mdc}(a, \frac{n}{d}) = 1$, havendo $\phi\left(\frac{n}{d}\right)$ elementos. De fato, os elementos de $T_d(n)$ são encontrados entre os números $d, 2d, \cdots, \left(\frac{n}{d}\right) d$. Agora, se mdc $\left(a, \frac{n}{d}\right) = e$, então $\text{mdc}(ad, n) = ed$ e $ed = d$ se e somente se $e = 1$. Assim,

$$n = |(S_n)| = \sum_{d|n} |T_d(n)| = \sum_{d|n} \phi\left(\frac{n}{d}\right).$$

Por fim, note que

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

Temos que d assume os valores dos vários divisores de n, e o mesmo acontece com o divisor complementar $\frac{n}{d}$. Assim, provamos nosso teorema. □

Observe dois exemplos para ilustrar a ideia da demonstração do Teorema 3.35. Considere $n = 6$. Então d pode assumir os valores $1, 2, 3$ e 6. Teremos $T_1(6) = \{1, 5\}$, $T_2(6) = \{2, 4\}$,

$T_3(6) = \{3\}$ e $T_6(6) = \{6\}$. Considere agora $n = 45$, os divisores de n são: $d = 1, 3, 5, 9, 15, 45$. Vamos separar os números de 1 a 45 em conjuntos $T_d(n)$ cujo maior divisor comum deste número com n é d. Assim teremos

$$
\begin{aligned}
T_{45}(45) &= \{45\} \\
T_{15}(45) &= \{15, 30\} \\
T_9(45) &= \{9, 18, 27, 36\} \\
T_5(45) &= \{5, 10, 20, 25, 35, 40\} \\
T_3(45) &= \{3, 6, 12, 21, 24, 33, 39, 42\} \\
T_1(45) &= \{1, 2, 4, 7, 8, 11, 13, 14, 16, 17, 19, 22, 23, 26, 28, 29, 31, 32, 34, 37, 38, 41, 43, 44\}
\end{aligned}
$$

Observe que esses conjuntos são disjuntos e a união deles é o conjunto $\{1, 2, 3, \cdots, 45\}$. Observe abaixo que a quantidade de elementos em cada $T_d(45)$ é igual a $\phi(\frac{45}{d})$

Conjuntos $T_d(n)$	Números de elementos em $T_d(n)$
$T_1(45)$	$24 = \phi(45) = \phi(\frac{45}{1})$
$T_3(45)$	$8 = \phi(15) = \phi(\frac{45}{3})$
$T_5(45)$	$6 = \phi(9) = \phi(\frac{45}{5})$
$T_9(45)$	$4 = \phi(5) = \phi(\frac{45}{9})$
$T_{15}(45)$	$2 = \phi(3) = \phi(\frac{45}{15})$
$T_{45}(45)$	$1 = \phi(1) = \phi(\frac{45}{45})$

Observe que, se d é divisor de 45 então $\frac{45}{d}$ também é. Confirmamos que $\sum_{d|n} \phi\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d)$ e além disso temos $\sum_{d|45} \phi(d) = 45$.

3.2 Função ϕ de Euler e o Princípio de Inclusão e Exclusão

Uma ferramenta muito importante que nos permite encontrar a resolução de vários modelos de problemas matemáticos envolvendo a contagem de elementos é o Princípio da Inclusão e Exclusão. Este princípio nos permite calcular a quantidade de elementos que pertencem a união de conjuntos quaisquer, não necessariamente disjuntos. Motivados pelo (8, Problema 6.1.11), iremos utilizar este princípio para sistematizar a fórmula da função ϕ de Euler, provado no Teorema 3.27.

3.2.1 Cardinalidade da união de dois conjuntos

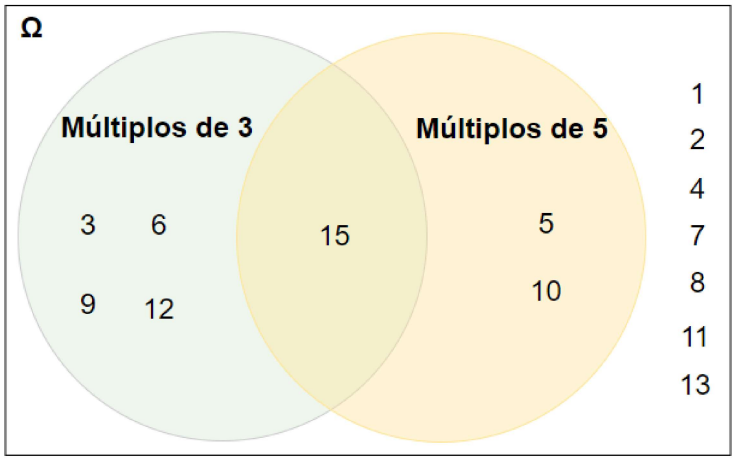
Simbolizemos por Ω o conjunto universo. Sejam A e B dois subconjuntos disjuntos de Ω, onde $(A \cap B) \neq \{0\}$. Para esta seção utilizamos o (11, Capítulo 4) como base do nosso estudo.

Teorema 3.36. *Sejam A e B conjuntos finitos, então* $|A \cup B| = |A| + |B| - |A \cap B|$.

Esta é a fórmula do Princípio da Inclusão e Exclusão para dois conjuntos não disjuntos. Esta regra também tem êxito para conjuntos disjuntos, uma vez que a interseção entre conjuntos disjuntos é o conjunto vazio, então $A \cap B = \{0\}$ e teríamos $|A \cup B| = |A| + |B|$. Iremos ver no próximo exemplo que é possível obter $\phi(n)$, n um número natural, com facilidade e de maneira precisa pela utilização do Princípio de Inclusão e Exclusão.

Exemplo 3.37. Vamos calcular $\phi(n)$ para $n = 15$. Inicialmente devemos encontrar os p_i primos presentes na decomposição em fatores primos de n, onde $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdots {p_i}^{r_i}$. Defina o conjunto $A_{p_i} = \{$números naturais menores que n e divisíveis por $p_i\}$, em seguida devemos determinar a quantidade de elementos pertencentes a cada conjunto A_{p_i}. Para encontrarmos a quantidade de números menores ou igual a 15 e coprimos com respeito a ele, devemos encontrar a cardinalidade do complementar da união dos A_{p_i}. Observe a figura abaixo:

Figura 4 – Quantidade de elementos para $\phi(15)$



Fonte: Autoria própria.

Temos $n = 15 = 3 \cdot 5$, então $A_3 = \{$Múltiplos de 3$\} = \{3, 6, 9, 12, 15\}$ $A_5 = \{$Múltiplos de 5$\} = \{5, 10, 15\}$. Além disso necessitaremos determinar a cardinalidade da interseção destes conjuntos $A_3 \cap A_5 = \{$Múltiplos de 15$\} = \{15\}$. Observe que a cardinalidade de cada conjunto pode ser dada por:

$$|A_3| = \frac{15}{3} = 5$$
$$|A_5| = \frac{15}{5} = 3$$
$$|A_3 \cap A_5| = \frac{15}{5 \cdot 3} = 1$$

Encontrado esses valores, podemos calcular $\phi(15)$.

$$\phi(15) = |\Omega| - |A_3 \cup A_5|$$

Pelo Teorema 3.36 temos

$$\begin{aligned}\phi(15) &= |\Omega| - (|A_3| + |A_5| - |A_3 \cap A_5|) \\ &= 15 - (5 + 3 - 1) = 8\end{aligned}$$

3.2.2 Cardinalidade da união de três conjuntos

Para aplicarmos o Princípio da Inclusão e Exclusão a três conjuntos devemos identificar as interseções dois a dois e a interseção entre os três conjuntos. Observe a seguir a fórmula que nos fornece a quantidade de elementos da união de três conjuntos:

Teorema 3.38. *Sejam A, B e C conjuntos finitos, então* $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

Exemplo 3.39. Vamos calcular calcularmos a quantidade de números menores ou igual a 30 coprimos com respeito a ele. Temos $n = 30 = 2 \cdot 3 \cdot 5$ a decomposição de n em fatores primos, então os p_i fatores primos de n são $3, 2, 5$. Para calcularmos a $\phi(n)$ para $n = 30$ por meio do Princípio da Inclusão e Exclusão, além de determinar a quantidade de elementos que pertencem a cada conjunto A_{p_i}, devemos encontrar a cardinalidade das interseções. Observe os conjuntos a seguir

$$\begin{aligned}A_2 &= \{2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30\} \\ A_3 &= \{3, 6, 9, 12, 15, 18, 21, 24, 27, 30\} \\ A_5 &= \{5, 10, 15, 20, 25, 30\} \\ A_2 \cap A_3 &= \{6, 12, 18, 24, 30\} \\ A_2 \cap A_5 &= \{10, 20, 30\} \\ A_3 \cap A_5 &= \{15, 30\} \\ A_2 \cap A_3 \cap A_5 &= \{30\}\end{aligned}$$

Podemos contar os elementos de cada conjunto citado, ou encontrar a cardinalidade de cada conjunto da seguinte maneira

$$\begin{aligned}|A_2| &= \frac{30}{2} = 15 \\ |A_3| &= \frac{30}{3} = 10 \\ |A_5| &= \frac{30}{5} = 6 \\ |A_2 \cap A_3| &= \frac{30}{2 \cdot 3} = \frac{30}{6} = 5 \\ |A_2 \cap A_5| &= \frac{30}{2 \cdot 5} = \frac{30}{10} = 3 \\ |A_3 \cap A_5| &= \frac{30}{5 \cdot 3} = \frac{30}{15} = 2 \\ |A_2 \cap A_3 \cap A_5| &= \frac{30}{2 \cdot 3 \cdot 5} = \frac{30}{30} = 1\end{aligned}$$

Os números menores ou igual a 30 coprimos com respeito a ele, são aqueles que não estão contidos nos conjuntos A_{p_i}. Então devemos encontrar a cardinalidade do complementar da união dos A_{p_i}, logo

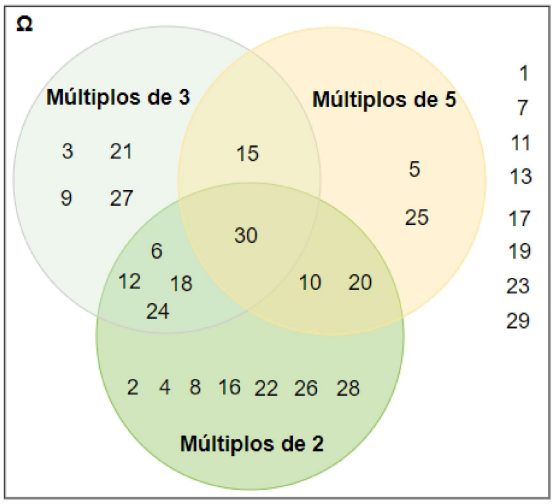
$$\phi(30) = |\Omega| - |A_2 \cup A_3 \cup A_5|$$

Onde $\Omega = \{1, 2, 3, \cdots, 30\}$. Pelo Princípio da Inclusão e Exclusão temos

$$\begin{aligned}\phi(30) &= |\Omega| - (|A_2| + |A_3| + |A_5| - |A_2 \cap A_3| - |A_2 \cap A_5| - |A_3 \cap A_5| + |A_2 \cap A_3 \cap A_5|) \\ &= 30 - (15 + 10 + 6 - 5 - 3 - 2 + 1) = 8\end{aligned}$$

Podemos conferir nosso resultado observando a figura abaixo

Figura 5 – Quantidade de elementos para $\phi(30)$



Fonte: Autoria própria.

3.2.3 Princípio da Inclusão e Exclusão

Vimos que para definirmos a cardinalidade da união de apenas dois conjuntos se resume ao Teorema 3.36, e para três conjunto se resume ao Teorema 3.38, a generalização para n conjuntos finitos se dá através do seguinte teorema:

Teorema 3.40. *(11, Teorema 4.1)(Princípio da Inclusão e Exclusão) Se $A_1, A_2, A_3, \cdots, A_k$ são conjuntos finitos, então*

$$\begin{aligned}\left|\bigcup_{i=1}^{k} A_i\right| &= \sum_{1\leq i<k} |A_i| - \sum_{1\leq i<j\leq k} |A_i \cap A_j| \\ &+ \sum_{1\leq i<j<p\leq k} |A_i \cap A_j \cap A_p| - \sum_{1\leq i<j<p<q\leq k} |A_i \cap A_j \cap A_p \cap A_q| \\ &+ \cdots + (-1)^{(k-1)} |A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_k|.\end{aligned}$$

Para a demonstração deste teorema consultar (11, Seção 4.2).

Vamos usar o Princípio da Inclusão e Exclusão para demostrar o Teorema 3.27, isto é, para cada $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdots {p_k}^{r_k}$, temos

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

De fato, considere $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdots {p_k}^{r_k}$ e defina os seguintes conjuntos

$$\begin{aligned}
A &= \{1, 2, 3, .., n\} \\
A_1 &= \{x \in A | \quad x \quad \text{é múltiplo de} \quad p_1\} \subset A \\
A_2 &= \{x \in A | \quad x \quad \text{é múltiplo de} \quad p_2\} \subset A \\
A_3 &= \{x \in A | \quad x \quad \text{é múltiplo de} \quad p_3\} \subset A \\
&\vdots \\
A_k &= \{x \in A | \quad x \quad \text{é múltiplo de} \quad p_k\} \subset A
\end{aligned}$$

Como os números contidos nesses conjuntos possuem fatores primos de n em sua fatoração, então nenhum desses é relativamente primos com n. Portanto, temos que retirar estes números do conjunto A para encontramos o valor de $\phi(n)$. Logo

$$\phi(n) = |A| - |A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_k|$$

Pelo Princípio da Inclusão e Exclusão temos

$$\begin{aligned}
\phi(n) &= |A| - \Bigg| \sum_{1 \le i < k} |A_i| - \sum_{1 \le i < j \le k} |A_i \cap A_j| + \sum_{1 \le i < j < p \le k} |A_i \cap A_j \cap A_p| \\
&\quad - \sum_{1 \le i < j < p < q \le k} |A_i \cap A_j \cap A_p \cap A_q| + \cdots + (-1)^{(k-1)} |A_1 \cap A_2 \cap \cdots \cap A_k| \Bigg| \\
&= |A| - \sum_{1 \le i < k} |A_i| - \sum_{1 \le i < j \le k} |A_i \cap A_j| + \sum_{1 \le i < j < p \le k} |A_i \cap A_j \cap A_p| \\
&\quad - \sum_{1 \le i < j < p < q \le k} |A_i \cap A_j \cap A_p \cap A_q| + \cdots + (-1)^{(k-1)} |A_1 \cap A_2 \cap \cdots \cap A_k|
\end{aligned} \tag{3.1}$$

Sabemos que $|A| = n$ e $|A_i| = \left(\frac{n}{p_i}\right)$ para qualquer $1 \le i \le k$. Assim, para r interseções destes conjuntos teremos

$$\begin{aligned}
|A_1 \cap A_2 \cap \cdots \cap A_r| &= |\{m \in N : m \le n; \quad p_{i_1} \text{ divide } m, p_{i_2} \text{ divide } m, \ldots, p_{i_r} \text{ divide } m\} \\
&= \frac{n}{p_{i_1} \cdot p_{i_2} \cdots p_{i_r}}.
\end{aligned}$$

Desta forma

$$\begin{aligned}
\sum_{1\leq i<k} |A_i| &= \sum_{1\leq i<k} \left(\frac{n}{p_i}\right) \\
\sum_{1\leq i<j\leq k} |A_i \cap A_j| &= \sum_{1\leq i<j\leq k} \left(\frac{n}{p_i p_j}\right) \\
\sum_{1\leq i<j<p\leq k} |A_i \cap A_j \cap A_p| &= \sum_{1\leq i<j<p\leq k} \left(\frac{n}{p_i p_j p_p}\right) \\
\sum_{1\leq i<j<p<q\leq k} |A_i \cap A_j \cap A_p \cap A_q| &= \sum_{1\leq i<j<p<q\leq k} \left(\frac{n}{p_i p_j p_p p_q}\right) \\
&\vdots \\
|A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_k| &= \left(\frac{n}{p_1 p_2 \ldots p_k}\right).
\end{aligned}$$

Voltando para (3.1),

$$\begin{aligned}
\phi(n) &= |A| - \sum_{1\leq i<k} |A_i| - \sum_{1\leq i<j\leq k} |A_i \cap A_j| + \sum_{1\leq i<j<p\leq k} |A_i \cap A_j \cap A_p| \\
&\quad - \sum_{1\leq i<j<p<q\leq k} |A_i \cap A_j \cap A_p \cap A_q| + \cdots + (-1)^{(k-1)} |A_1 \cap A_2 \cap \cdots \cap A_k| \\
&= n - \left|\sum_{1\leq i<k} \left(\frac{n}{p_i}\right)\right| + \left|\sum_{1\leq i<j\leq k} \left(\frac{n}{p_i p_j}\right)\right| + \left|\sum_{1\leq i<j<p\leq k} \left(\frac{n}{p_i p_j p_p}\right)\right| \\
&\quad + \cdots + (-1)^{(k)} \left|\left(\frac{n}{p_1 p_2 \ldots p_k}\right)\right| \\
&= n\left[1 - \left|\sum_{1\leq i<k} \left(\frac{1}{p_i}\right)\right| + \left|\sum_{1\leq i<j\leq k} \left(\frac{1}{p_i p_j}\right)\right| + \left|\sum_{1\leq i<j<p\leq k} \left(\frac{1}{p_i p_j p_p}\right)\right|\right. \\
&\quad \left. + \cdots + (-1)^{(k)} \left|\left(\frac{1}{p_1 p_2 \ldots p_k}\right)\right|\right] \\
&= n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right),
\end{aligned}$$

o que conclui a demonstração.

4 Função $\mu(n)$

Neste capítulo estudaremos a *função de Möbius* $\mu(n)$, cujos valores pertencem ao subconjunto $\{-1, 0, 1\}$. Denominada em homenagem a August Ferdinand Möbius, sua importância está relacionada com fórmula de inversão de Möbius, a qual detalharemos no decorrer deste capítulo.

Definição 4.1. (3, Definição 6-1). Seja n um número natural. Definimos a função $\mu : \mathbb{N} \to \mathbb{Z}$ dada por

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } p^2 | n \text{ para algum primo p}, \\ (-1)^r & \text{se } n = p_1 \cdot p_2 \cdots p_r, \text{ onde } p_i \text{ são primos distintos.} \end{cases}$$

Exemplo 4.2. Observe a tabela:

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

Exemplo 4.3. Mostre que, para qualquer inteiro positivo n,

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

Demonstração. Temos que

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

Observe que no desenvolvimento do produtório aparecem números consecutivos: $n, n+1, n+2, n+3$. Em uma sequência de quatro números consecutivos teremos um múltiplo de 4. Como 4 é um quadrado perfeito, pela Definição 4.1, um desses termos irá ser igual a 0, o que irá zerar todo produtório. □

Mostraremos que μ é multiplicativa sabendo apenas o seu valor em potência de primos.

Teorema 4.4. *Sejam m e n números naturais com $mdc(m, n) = 1$, então*

$$\mu(m \cdot n) = \mu(m) \cdot \mu(n)$$

Demonstração. Queremos mostrar que μ é uma função multiplicativa. Considere as seguintes decomposições em fatores primos $m = {p_1}^{\alpha_1} \cdot {p_2}^{\alpha_2} \cdots {p_s}^{\alpha_s}$ e $n = {q_1}^{\beta_1} \cdot {q_2}^{\beta_2} \cdots {q_r}^{\beta_r}$. Se um dos expoentes α_i ou β_i exceder 1 teremos $\mu(m) = 0$ ou $\mu(n) = 0$. Além disso, algum p^2 ou q^2 dividirá mn, assim teremos $\mu(m.n) = 0 = \mu(m) \cdot \mu(n)$. Caso todos α_i e β_i sejam iguais a 1 teremos $\mu(m) \cdot \mu(n) = (-1)^s \cdot (-1)^r = (-1)^{r+s} = \mu(m.n)$. □

Corolário 4.5. *Sejam r, s números naturais e p um número primo. Então*

$$\mu(p^r) \cdot \mu(p^s) \geq \mu(p^{r+s}).$$

Demonstração. Vimos na Definição 4.1 que $\mu(n)$ assume valores diferentes de acordo com algumas condições, então observe os casos a seguir:
No primeiro caso considere onde $r = 0$ e $s = 0$, como $\mu(1) = 1$ teremos a igualdade:

$$\mu(p^r) \cdot \mu(p^s) = \mu(p^0) \cdot \mu(p^0) = \mu(1) \cdot \mu(1) = 1 = \mu(1) = \mu(p^{0+0}) = \mu(p^{r+s}).$$

Já no caso onde $r = 1$ e $s = 1$, pela definição de $\mu(n)$ temos $\mu(p^1) = (-1)^1 = -1$, então

$$\mu(p^1) \cdot \mu(p^1) = (-1) \cdot (-1) = 1 > 0 = \mu(p^{1+1}).$$

E por fim vamos analisar o caso onde $r \geq 2$ ou/e $s \geq 2$, teremos que p^2 dividirá p^r ou/e p^s e consequentemente $p^2 | p^{r+s}$. Ora, sabemos que $\mu(n) = 0$ se $p^2 | n$ então

$$\mu(p^r) \cdot \mu(p^s) = 0 = \mu(p^{r+s}).$$

Assim, concluímos que

$$\mu(p^r) \cdot \mu(p^s) \geq \mu(p^{r+s}).$$

□

Exemplo 4.6. Observe os seguintes exemplos

$$\mu(5^0) \cdot \mu(5^0) = \mu(1) \cdot \mu(1) = 1 = \mu(1) = \mu(5^{0+0}) = \mu(5^0)$$
$$\mu(5^1) \cdot \mu(5^1) = (-1) \cdot (-1) = 1 > 0 = \mu(5^{1+1}) = \mu(5^2)$$
$$\mu(5^1) \cdot \mu(5^2) = (-1) \cdot (0) = 0 = \mu(5^{1+2}) = \mu(5^3)$$

Assim nos certificamos que

$$\mu(5^r) \cdot \mu(5^s) \geq \mu(5^{r+s}).$$

Teorema 4.7. *Se m e n são números naturais que não são primos entre si, então $\mu(m) \cdot \mu(n) \geq \mu(m \cdot n)$.*

Demonstração. Como não são coprimos, m e n possuem fatores primos em comum, sejam eles $p_1, p_2, p_3, \ldots, p_k$. Podemos escrever $m = a \cdot {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot {p_3}^{r_3} \cdots {p_k}^{r_k}$ e $n = b \cdot {p_1}^{s_1} \cdot {p_2}^{s_2} \cdot {p_3}^{s_3} \cdots {p_k}^{s_k}$, onde mdc(a,b)=1, com $mdc(a, p_i) = mdc(b, p_i) = 1$ para todo i. Daí

$$\mu(m \cdot n) = \mu(a \cdot {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot {p_3}^{r_3} \cdot \ldots \cdot {p_k}^{r_k} \cdot b \cdot {p_1}^{s_1} \cdot {p_2}^{s_2} \cdot {p_3}^{s_3} \cdot \ldots \cdot {p_k}^{s_k})$$

$$= \mu(a \cdot b \cdot {p_1}^{r_1+s_1} \cdot {p_2}^{r_2+s_2} \cdot {p_3}^{r_3+s_3} \cdot \ldots \cdot {p_k}^{r_k+s_k})$$

Como a, b, p_r e p_s são coprimos para quaisquer r e s, pelo Teorema 4.4, podemos fazer o seguinte cálculo:

$$\mu(m \cdot n) = \mu(a) \cdot \mu(b) \cdot \mu({p_1}^{r_1+s_1}) \cdot \mu({p_2}^{r_2+s_2}) \cdot \mu({p_3}^{r_3+s_3}) \cdot \ldots \cdot \mu({p_k}^{r_k+s_k})$$

O Corolário 4.5 nos diz que para cada $i = 1, 2, 3, ..., k$ teremos $\mu({p_i}^{r_i+s_i}) \leq \mu(p_i^{r_i}) \cdot \mu({p_i}^{s_i})$, portanto

$$\mu(m \cdot n) = \mu(a) \cdot \mu(b) \cdot \mu({p_1}^{r_1+s_1}) \cdot \mu({p_2}^{r_2+s_2}) \cdot ... \cdot \mu({p_k}^{r_k+s_k})$$

$$\leq \mu({p_1}^{r_1}) \cdot \mu({p_1}^{s_1}) \cdot \mu({p_2}^{r_2}) \cdot \mu({p_2}^{s_2}) \cdot ... \cdot \mu({p_k}^{r_k}) \cdot \mu({p_k}^{s_k}) \cdot \mu(a) \cdot \mu(b) = \mu(m) \cdot \mu(n)$$

o que resulta em:

$$\mu(m \cdot n) \leq \mu(m) \cdot \mu(n)$$

□

Mostramos no Teorema 4.4 que a função μ é multiplicativa. Mas esta função não é completamente multiplicativa, pois não temos $\mu(m \cdot n) \leq \mu(m) \cdot \mu(n)$ para alguns números naturais m e n.

Teorema 4.8.

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

Demonstração. Para $n = 1$ temos:

$$F(1) = \sum_{d|1} \mu(d) = \mu(1) = 1.$$

Vimos que $\mu(n)$ é uma função multiplicativa, então $F(n)$ também será multiplicativa. De fato, seja $n = a \cdot b$, com a e b inteiros e $mdc(a, b) = 1$. Logo

$$\begin{aligned} F(n) &= \sum_{d|n} \mu(d) \\ &= \sum_{d|a \cdot b} \mu(d) \\ &= \sum_{d_1|a \cdot d_2|b} \mu(d_1 \cdot d_2) \\ &= \sum_{d_1|a \cdot d_2|b} \mu(d_1) \cdot \mu(d_2) \\ &= \sum_{d_1|a} \mu(d_1) \cdot \sum_{d_2|b} \mu(d_2) \\ &= F(a) \cdot F(b) \end{aligned}$$

Sendo assim, para $n = p_1 \cdot p_2 \cdots p_r$, onde p_i são primos distintos, teremos

$$\begin{aligned} F(n) &= F(p_1 \cdot p_2 \cdot ... \cdot p_r) \\ &= F(p_1) \cdot F(p_2) \cdot ... \cdot F(p_r) \\ &= \sum_{d|p_1} \mu(d) \cdot \sum_{d|p_2} \mu(d) \cdot ... \cdot \sum_{d|p_r} \mu(d) \\ &= (\mu(1) + \mu(p_1)) \cdot (\mu(1) + \mu(p_2)) \cdot ... \cdot (\mu(1) + \mu(p_r)) \\ &= (1-1) \cdot (1-1) \cdot ... \cdot (1-1) \\ &= 0 \end{aligned}$$

Agora, basta analisar $F(n)$ se algum $p^2|n$,com p primo. Considere $n = m \cdot p^\alpha$, com $\alpha \geq 2$ e $(m, p) = 1$.

$$\begin{aligned} F(n) &= F(m \cdot p^2) \\ &= F(m)F(p^2) \\ &= \sum_{d|p^m} \mu(d) \cdot \sum_{d|p^\alpha} \mu(d) \\ &= \sum_{d|p^m} \mu(d) \cdot \big(\mu(1) + \mu(p) + \mu(p^2) + ... + \mu(p^\alpha)\big) \\ &= 1 + \mu(p) + 0 + \cdots + 0 \\ &= 1 - 1 \\ &= 0. \end{aligned}$$

Logo $F(n) = 0$ para todo $n > 1$. □

Exemplo 4.9. Considere $n = 45$, teremos os seguintes divisores $\{1, 3, 5, 9, 15, 45\}$. Logo:

$$\begin{aligned} F(45) =& \sum_{d|45} \mu(d) = \mu(1) + \mu(3) + \mu(5) + \mu(9) + \mu(15) + \mu(45) \\ =& 1 + (-1) + (-1) + 0 + 1 + 0 = 0 \end{aligned}$$

Exemplo 4.10. Mostre que dado um número natural m teremos $\sum_{n=1}^{m} \mu(n) \left\lfloor \frac{m}{n} \right\rfloor = 1$

Demonstração. Observe o seguinte somatório:

$$\sum_{n=1}^{m} \left(\sum_{d|n} \mu(d) \right) = \sum_{d_1|1}^{m} \mu(d_1) + \sum_{d_2|2}^{m} \mu(d_2) + \cdots + \sum_{d_m|m}^{m} \mu(d_m)$$

Como 1 é divisor de todos os inteiros, então ele irá aparecer em todos os somatórios acima. Já o número 2 é divisor de $\left\lfloor \frac{m}{2} \right\rfloor$ destes inteiros, logo $\mu(2)$ ocorrerá $\left\lfloor \frac{m}{2} \right\rfloor$ vezes. Generalizando, para d

divisor de $\left\lfloor \frac{m}{d} \right\rfloor$, dos inteiros de 1 a m, $\mu(d)$ aparecerá $\left\lfloor \frac{m}{d} \right\rfloor$ vezes. Portanto

$$\begin{aligned}\sum_{n=1}^{m}\left(\sum_{d|n}\mu(d)\right) &= \mu(1)\left\lfloor\frac{m}{1}\right\rfloor + \mu(2)\left\lfloor\frac{m}{2}\right\rfloor + \mu(3)\left\lfloor\frac{m}{3}\right\rfloor + \cdots + \mu(m)\left\lfloor\frac{m}{m}\right\rfloor \\ &= \sum_{n=1}^{m}\mu(n)\left\lfloor\frac{m}{n}\right\rfloor\end{aligned}$$

Sabemos, pelo Teorema 4.8, que

$$\sum_{d_1|1}^{m}\mu(d_1) + \sum_{d_2|2}^{m}\mu(d_2) + \cdots + \sum_{d_m|m}^{m}\mu(d_m) = 1 + 0 + ... + 0 = 1$$

Portanto

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

□

4.1 Fórmula de Inversão de Möbius

Para entendermos a Fórmula de Inversão de Möbius precisamos conhecer o *Produto de Dirichlet*, uma importante ferramenta entre as funções aritméticas. O leitor pode saber mais em (12, Capítulo 1.7).

Definição 4.11. (Produto de Dirichlet.) Sejam f e g duas funções aritméticas. O *Produto de Dirichlet* ou *produto de convolução*, é a função aritmética $f * g$ definida por:

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

Sabemos que d é um divisor de n, então pares da forma $\left(d, \frac{n}{d}\right)$ podem ser escritos como (a, b) onde $a, b \in \mathbb{N}$ tal que $n = ab$. Assim a definição anterior pode ser reescrita da seguinte maneira:

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

Exemplo 4.12. Sejam f e g duas funções aritméticas, para $n = 6$ teremos os divisores $d = \{1, 2, 3, 6\}$, vamos entender como se calcula o Produto de Dirichlet.

$$\begin{aligned}(f * g)(6) &= \sum_{d|6} f(d) \cdot g\left(\frac{6}{d}\right) \\ &= f(1) \cdot g\left(\frac{6}{1}\right) + f(2) \cdot g\left(\frac{6}{2}\right) + f(3) \cdot g\left(\frac{6}{3}\right) + f(6) \cdot g\left(\frac{6}{6}\right) \\ &= f(1) \cdot g(6) + f(2) \cdot g(3) + f(3) \cdot g(2) + f(6) \cdot g(1)\end{aligned}$$

Para o caso em que $f = \tau(n)$ e $g = \sigma(n)$ teremos

$$\begin{aligned}(f * g)(6) &= f(1) \cdot g(6) + f(2) \cdot g(3) + f(3) \cdot g(2) + f(6) \cdot g(1) \\ &= \tau(1) \cdot \sigma(6) + \tau(2) \cdot \sigma(3) + \tau(3) \cdot \sigma(2) + \tau(6) \cdot \sigma(1) \\ &= 1 \cdot 12 + 2 \cdot 4 + 2 \cdot 3 + 4 \cdot 1 \\ &= 30\end{aligned}$$

Para entendermos as propriedades do Produto de Dirichlet necessitamos de três funções auxiliares. Defina:

$$id(n) = n \text{ Para todo } n \in \mathbb{N}$$

$$I(n) = 1 \text{ Para todo } n \in \mathbb{N}$$

$$e(n) = \begin{cases} 1 \text{ se } n = 1 \\ 0 \text{ Para todo } n > 1;\ n \in \mathbb{N} \end{cases}$$

Propriedade 4.13. (12, Teorema 1.8) Considere f, g e k funções aritméticas. Valem as seguintes propriedades:

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

(ii) $(f * g) * k = f * (g * k)$.

(iii) $f * e = e * f = f$

(iv) Se $f(1) \neq 0$, f então existe uma função g, função inversa de Dirichlet, única, tal que $f * g = e$.

Demonstração. Vamos aceitar como verdadeira a propriedade (i), isto é, o Produto de Dirichlet é comutativo. Agora perceba que

$$\begin{aligned}((f * g) * k)(n) &= \sum_{dc=n} (f * g)(d)k(c) \\ &= \sum_{abc=n} f(a)g(b)k(c) \\ &= \sum_{ae=n} f(a)(g * k)(e) \\ &= (f * (g * k))(n),\end{aligned}$$

O que confirma a propriedade (ii), logo o Produto de Dirichlet é associativo. Para analisarmos a propriedade (iii) basta notar que

$$\begin{aligned}(f * e)(n) = (e * f)(n) &= \sum_{d|n} f(d)e\left(\frac{n}{d}\right) \\ &= f(n)e(1) \\ &= f(n).\end{aligned}$$

Temos assim e o elemento neutro.

Na propriedade (iv) queremos mostrar que há uma função g tal que $f * g = e$, então,

$$\sum_{d|n} g(d) f\left(\frac{n}{d}\right) = \begin{cases} 1 \text{ se } n = 1 \\ 0 \text{ Para todo } n > 1;\ n \in \mathbb{N} \end{cases}$$

Para $n = 1$ teremos um único divisor $d = 1$ então defina $g(1)f(1) = 1$. E se $n > 1$ teremos

$$\begin{aligned} \sum_{d|n} g(d) f\left(\frac{n}{d}\right) &= g(n)f(1) + \sum_{d|nn>d} g(d) f\left(\frac{n}{d}\right) \\ &= -\frac{f(1)}{f(1)} \sum_{d|nn>d} g(d) f\left(\frac{n}{d}\right) + \sum_{d|nn>d} g(d) f\left(\frac{n}{d}\right) = 0 \end{aligned}$$

Assim teremos a função inversa de Dirichlet como

$$g(1)f(1) = 1 \quad \text{e} \quad g = -\frac{1}{f(1)} \sum_{d|nn>d} g(d) f\left(\frac{n}{d}\right)$$

□

Exemplo 4.14. $f * I = I * f = \sum_{d|n} f(d)$

Demonstração. Temos

$$\begin{aligned} (f * I)(n) &= \sum_{d|n} f(d) I\left(\frac{n}{d}\right) \\ &= \sum_{d|n} f(d) \cdot 1 \\ &= \sum_{d|n} f(d) \\ &= 1 \cdot \sum_{d|n} f(d) \\ &= \sum_{d|n} I\left(\frac{n}{d}\right) f(d) \\ &= (I * f)(n). \end{aligned}$$

□

Exemplo 4.15. Mostre que $\mu * I = e$.

Demonstração. Vamos provar em duas etapas, na primeira considere $n = 1$:

$$(\mu * I)(n) = (\mu)(n) * I(n) = (\mu)(1) * I(1) = 1 = e(1).$$

Para segunda etapa seja $n > 0$ e $n \neq 1$

$$(\mu * I)(n) = (\mu)(n) * I(n) = \mu(n) * 1 = \sum_{d|n} \mu(d).$$

Pelo Teorema 4.8 podemos concluir que $\sum_{d|n} \mu(d) = 0 = e(n)$. Assim mostramos que $(\mu * I)(n) = e(n)$ para todo $n \in \mathbb{N}$. □

Exemplo 4.16. Mostre que $\tau(n) = (I * I)(n)$.

Demonstração. Temos

$$(I * I)(n) = \sum_{d|n} I(n) \cdot I\left(\frac{n}{d}\right) = \sum_{d|n} 1 \cdot 1 = \sum_{d|n} 1 = \tau(n)$$

□

Exemplo 4.17. Mostre que $(\phi * I)(n) = id(n)$.

Demonstração. Pelo Exemplo 4.14 e pelo Teorema 3.35 temos:

$$(\phi * I)(n) = \sum_{d|n} \phi(d) \cdot I\left(\frac{n}{d}\right) = \sum_{d|n} \phi(d) \cdot 1 = \sum_{d|n} \phi(d) = n = id(n)$$

□

As propriedades a seguir relacionam o produto de Dirichlet e funções multiplicativas.

Propriedade 4.18. (i) Se f e g são funções multiplicativas, então $f * g$ é multiplicativa

(ii) Se f é uma função multiplicativa, então a inversa de Dirichlet é multiplicativa.

(iii) Considere $f * g = h$, se f e h são funções multiplicativas, então g será multiplicativa

(iv) Se h for completamente multiplicativa, então $h(f * g) = (hf) * (hg)$ para qualquer funções f e g .

As demonstrações podem ser encontradas em (12).

Exemplo 4.19. Mostre que $\sigma(n)$ é multiplicativo usando o produto de convolução.

Demonstração. Temos

$$id(n) * I = \sum_{d|n} id(d) \cdot I\left(\frac{n}{d}\right) = \sum_{d|n} id(d) \cdot 1 = \sum_{d|n} id(d) = \sigma(n)$$

Como $\sigma(n) = id * I$, basta mostrar que I e id são multiplicativos para concluirmos a demonstração. Considere $n = a \cdot b$,

$$I(a \cdot b) = I(n) = 1 = 1 \cdot 1 = I(a) \cdot I(b)$$
$$id(a \cdot b) = id(n) = n = a \cdot b = id(a) \cdot id(b)$$

Pelo item i da Propriedade 4.18 teremos $id * I$ multiplicativo, logo a função $\sigma(n)$ é multiplicativa. □

Teorema 4.20. *(Fórmula de Inversão de Möbius (3, Teorema 6-6)) Sejam f e g funções aritméticas. Se, para cada n, satisfazem uma das condições*

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

então satisfazem ambas condições.

Demonstração. Primeiro suponha que $f(n) = \sum_{d|n} g(d)$. Considere $d' = \frac{n}{d}$ então

$$\begin{aligned}\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) &= \sum_{dd'=n} \mu(d) f(d') \\ &= \sum_{dd'=n} \mu(d) \sum_{m|d'} g(m) \\ &= \sum_{dmh=n} \mu(d) g(m) \\ &= \sum_{d|h'} \mu(d) \sum_{mh'=n} g(m).\end{aligned}$$

Vimos no Teorema 4.8 que $\sum_{d|h'} \mu(d)$ pode assumir o valor 0 se $h' > 1$, e valor 1 se $h' = 1$. Então

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

Agora, suponha que $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$. Faremos a seguinte troca de variáveis, n para d e d para d', logo $g(n) = \sum_{d'|d} \mu(d') f\left(\frac{d}{d'}\right)$. A partir daí podemos fazer os seguintes cálculos:

$$\begin{aligned}\sum_{d|n} g(d) &= \sum_{d|n} \sum_{d'|d} \mu(d') f\left(\frac{d}{d'}\right) \\ &= \sum_{d'mh=n} \mu(d') f(m) \\ &= \sum_{d'|h'} \mu(d') \sum_{mh'=n} f(m)\end{aligned}$$

Vimos no Teorema 4.8 que $\sum_{d'|h'} \mu(d')$ pode assumir o valor 0 se $h' > 1$, e valor 1 se $h' = 1$. Então

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

□

Exemplo 4.21. (9, Exemplo 8.12) Prove que

$$\sum_{d|n} \tau(d) \cdot \mu\left(\frac{n}{d}\right) = \sum_{d|n} \mu(d) \cdot \tau\left(\frac{n}{d}\right) = 1$$

para todo $n \geq 1$. Verifique esta equação para $n = 12$

Demonstração. Perceba que nesta questão devemos provar que $(\mu * \tau)(n) = I$.

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

Sabemos que $\tau\left(\frac{n}{d}\right)$ é a soma de todos os divisores d_r de $\frac{n}{d}$, logo $\tau\left(\frac{n}{d}\right) = \sum_{d_r} 1$ então

$$(\mu * \tau)(n) = \sum_{d|n} \mu(d) \cdot \sum_{d_r} 1 = \sum_{d_r} \sum_{d_s} \mu(d_s)$$

Onde d_s são os divisores de $\frac{n}{d_r}$. Separamos esta demonstração em duas etapas, se $d_r = n$:

$$\sum_{d_r} \sum_{d_s} \mu(d_s)$$

$$\sum_{n} \sum_{d} \mu(d)$$

Pelo Teorema 4.8 temos $\sum_{d|n} \mu(d) = 1$ se $n = 1$, para os outros casos temos o somatório nulo. logo

$$\sum_{1} 1 = 1$$

Para segunda etapa seja e $d_r \neq n$, pelo Teorema 4.8 temos $\sum_{d|n} \mu(d) = 0$ para $n > 1$, logo

$$\sum_{n} \sum_{d} \mu(d) = 0$$

Assim,

$$\sum_{d|n} \mu(d) \cdot \tau\left(\frac{n}{d}\right) = 1$$

Para $n = 12$ teremos

$$\begin{aligned}
&\sum_{d|12} \mu(\frac{12}{d}) \cdot \tau(d) = \\
&= \mu(\frac{12}{1}) \cdot \tau(1) + \mu(\frac{12}{2}) \cdot \tau(2) + \mu(\frac{12}{3}) \cdot \tau(3) + \mu(\frac{12}{4}) \cdot \tau(4) + \mu(\frac{12}{6}) \cdot \tau(6) + \mu(\frac{12}{12}) \cdot \tau(12) \\
&= \mu(12) \cdot \tau(1) + \mu(6) \cdot \tau(2) + \mu(4) \cdot \tau(3) + \mu(3) \cdot \tau(4) + \mu(2) \cdot \tau(6) + \mu(1) \cdot \tau(12) \\
&= 0 \cdot 1 + (-1)^2 \cdot 2 + 0 \cdot 2 + (-1) \cdot 3 + (-1) \cdot 4 + 1 \cdot 6 \\
&= 0 + 2 + 0 - 3 - 4 + 6 \\
&= 1
\end{aligned}$$

□

4.2 Pares de Möbius

Definição 4.22. (3, Definição 6-3) Se f e g funções aritméticas satisfazem $f(n) = \sum_{d|n} g(d)$, então $\{f(n), g(n)\}$ é um *Par de Möbius*.

Teorema 4.23. *(3, Teorema 6-7) Seja $\{f(n), g(n)\}$ um Par de Möbius. Se uma da funções f e g for multiplicativa, a outra também é.*

Demonstração. Suponha que $g(n)$ seja multiplicativa e sejam m e n tais que $mdc(m, n) = 1$. Como m e n são relativamente primos, iremos separar os divisores d de $m \cdot n$ em r ou s, onde $r|m$ e $s|n$. Então:

$$\begin{aligned} f(m \cdot n) &= \sum_{d|m\cdot n} g(d) \\ &= \sum_{r|m} \sum_{s|n} g(r \cdot s) \\ &= \sum_{r||m} g(r) \cdot \sum_{s|n} g(s) \\ &= f(m) \cdot f(n). \end{aligned}$$

Portanto, $f(n)$ é multiplicativa.

Agora, suponha que $f(n)$ seja multiplicativa, pelo Teorema 4.20 sabemos que $g(n) = \sum_{d|n} \mu(d) f\left(\frac{n}{d}\right)$, considere a troca de variáveis de n para mn onde $mdc(m, n) = 1$. Então

$$\begin{aligned} g(m \cdot n) &= \sum_{d|mn} \mu(d) \cdot f\left(\frac{m \cdot n}{d}\right) \\ &= \sum_{r|m} \sum_{s|n} \mu(r \cdot s) \cdot f\left(\frac{m \cdot n}{r \cdot s}\right) \\ &= \sum_{r|m} \sum_{s|n} \mu(r) \cdot \mu(s) \cdot f\left(\frac{m}{r}\right) \cdot f\left(\frac{n}{s}\right) \\ &= \sum_{r||m} \mu(r) \cdot f\left(\frac{m}{r}\right) \cdot \sum_{s/n} \mu(s) \cdot f\left(\frac{n}{s}\right) \\ &= g(m) \cdot g(n). \end{aligned}$$

Logo $g(n)$ é multiplicativa. □

Exemplo 4.24. $\{n, \phi(n)\}$, $\{\tau(n), 1\}$ e $\{\sigma(n), n\}$ são Pares de Möbius.

Demonstração. Para mostrarmos que $f(n)$ e $g(n)$ são Pares Möbius basta verificar que $f(n) = \sum_{d|n} g(d)$. Observe que pela definição de $\tau(n)$ e $\sigma(n)$ temos

$$\tau(n) = \sum_{d|n} 1 \quad \text{e} \quad \sigma(n) = \sum_{d|n} d$$

E vimos em Teorema 3.35 que

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

□

4.3 Estabelecendo relações entre $\mu(n)$ e $\phi(n)$

O teorema a seguir estabelecer o valor de $\phi(n)$ a partir da função de Möbius, para esta seção tivemos como base o livro Number theory, de George E Andrews (3).

Teorema 4.25. *(3, Teorema 6-2) Seja n um número natural. Então*

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

Demonstração. Seguiremos utilizando o Princípio de indução sobre o número de fatores primos de n. Se n tem um fator primo, $n = q^\alpha$, então, pelo Teorema 3.14, temos $\phi(n) = \phi(q^\alpha) = q^\alpha - q^{\alpha-1}$. Agora iremos desenvolver o somatório

$$\begin{aligned}\sum_{d|n} \mu(d)\frac{n}{d} &= \mu(1)q^\alpha + \mu(q)q^{\alpha-1} + \mu(q^2)q^{\alpha-2} + \cdots + \mu(q^\alpha) \\ &= q^\alpha - q^{\alpha-1} + 0 + \cdots + 0 \\ &= q^\alpha - q^{\alpha-1}\end{aligned}$$

Consequentemente, a sentença é verdadeira quando n tem um fator primo. Agora vamos supor que o teorema seja verdadeiro para cada inteiro com k ou menos fatores primos. Suponha $n = n'p^\alpha$, onde n' tem k distintos fatores primos e p é primo que não divide n'. Então, pela hipótese de indução e Teorema 3.27 temos

$$\phi(n') = \sum_{d|n'} \mu(d)\frac{n'}{d} = n' \prod_{d|n'} \left(1 - \frac{1}{p}\right),$$

Vamos agora dividir o conjunto $\{1, 2, 3, \cdots, n\}$ em p^α subconjuntos, cada um consistindo de n' inteiros consecutivos. Cada subconjunto contém $\phi(n')$ inteiros relativamente primos a n'. Agora, dos $p^\alpha\phi(n)$ inteiros positivos em $\{1, 2, 3, \cdots, n\}$ que são relativamente primos para n', os únicos que possuem um fator comum com n são os $p^{\alpha-1}\phi(n')$ inteiros que são múltiplos de p. Consequentemente,

$$\phi(n) = p^\alpha\phi(n') - p^{\alpha-1}\phi(n'). \tag{4.1}$$

Para ilustrar esta construção, seja $n = 30 = (3 \cdot 2 \cdot 5)$ e $n' = 6 = (2 \cdot 3)$. Abaixo iremos destacar $5 \cdot \phi(6)$ números em $\{1, 2, 3, \cdots, 30\}$ que são relativamente primos com 6:

$$\underline{\mathbf{1}} - 2 - 3 - 4 - \underline{\mathbf{5}} - 6 - \underline{\mathbf{7}} - 8 - 9 - 10 - \underline{\mathbf{11}} - 12 - \underline{\mathbf{13}} - 14 - 15 - 16$$
$$\underline{\mathbf{17}} - 18 - \underline{\mathbf{19}} - 20 - 21 - 22 - \underline{\mathbf{23}} - 24 - \underline{\mathbf{25}} - 26 - 27 - 28 - \underline{\mathbf{29}} - 30$$

Para obter os $5 \cdot \phi(6)$ números em $\{1, 2, 3, \cdots, 30\}$ que são relativamente primos para 6 mas não para o 5. Tomamos todos os números menores ou iguais a $30|5 = 6$ que são relativamente primos com 6, e multiplicamos cada um por 5. Assim obtemos $5 \cdot 1 = 5$ e $5 \cdot 5 = 25$. A exclusão desses números nos sublinhados acima deixa $1, 7, 11, 13, 17, 19, 23$ e 29, ou seja, todos os números em $\{1, 2, 3, \cdots, 30\}$ que são relativamente primos com 30. Assim, usando (4.1) temos

$$\begin{aligned}
\phi(n) &= p^{\alpha}\phi(n') - p^{\alpha-1}\phi(n') \\
&= p^{\alpha}\sum_{d|n'}\mu(d)\frac{n'}{d} - p^{\alpha-1}\sum_{d|n'}\mu(d)\frac{n'}{d} \\
&= \sum_{d|n'}\mu(d)\frac{n}{d} - \frac{1}{p}\sum_{d|n'}\mu(d)\frac{n}{d} \\
&= \sum_{\substack{d|n \\ p\nmid d}}\frac{\mu(d)n}{d} + \sum_{d|n'}\mu(pd)\frac{n}{pd} \\
&= \sum_{\substack{d|n \\ p\nmid d}}\frac{\mu(d)n}{d} + \sum_{\substack{pd|n \\ p\nmid d}}\mu(pd)\frac{n}{pd},
\end{aligned}$$

onde usamos o fato de que se $p \nmid d$, então $\mu(pd) = -\mu(d)$. Além disso

$$\begin{aligned}
\sum_{\substack{d|n \\ p\nmid d}}\frac{\mu(d)n}{d} + \sum_{\substack{pd|n \\ p\nmid d}}\mu(pd)\frac{n}{pd} &= \sum_{\substack{d|n \\ p\nmid d}}\frac{\mu(d)n}{d} + \sum_{\substack{pd|n \\ p\nmid d}}\mu(pd)\frac{n}{pd} \\
&\quad + \sum_{\substack{p^2d|n \\ p\nmid d}}\mu(p^2d)\frac{n}{p^2d} + \cdots + \sum_{\substack{p^{\alpha}d|n \\ p\nmid d}}\mu(p^{\alpha}d)\frac{n}{p^{\alpha}d} \\
&= \sum_{d|n}\frac{\mu(d)n}{d},
\end{aligned}$$

onde usamos que os termos são iguais a zero, desde que $\mu(N) = 0$ se $q^2|N$ para algum q primo, e que, os termos p^2 ou com potência de p maiores que 2 aparecem no argumento de μ. Novamente, pela hipótese de indução, vemos que

$$\begin{aligned}
\phi(n) &= p^{\alpha}\phi(n') - p^{\alpha-1}\phi(n') \\
&= p^{\alpha}\phi(n')\left(1 - \frac{1}{p}\right) \\
&= p^{\alpha}n'\left(1 - \frac{1}{p}\right)\prod_{p|n'}\left(1 - \frac{1}{p}\right),
\end{aligned}$$

e assim provamos o teorema. □

Proposição 4.26. *Para n inteiro positivo teremos*

$$\frac{n}{\phi(n)} = \sum_{d|n}\frac{\mu^2(d)}{\phi(d)},$$

com d sendo os divisores positivos de n.

Demonstração. Vimos no Teorema 3.27 que $\phi(n) = n\prod\left(1-\frac{1}{p_n}\right)$, onde p_n são os primos distintos que dividem n. Seja $n = {p_1}^{r_1}\cdot {p_2}^{r_2}\cdot \ldots \cdot {p_k}^{r_k}$ a decomposição de n em fatores primos, temos

$$\begin{aligned}\phi(n) &= n\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)\\ &= n\left(\frac{p_1-1}{p_1}\right)\cdot\left(\frac{p_2-1}{p_2}\right)\cdot\ldots\cdot\left(\frac{p_k-1}{p_k}\right)\\ &= \frac{n\cdot(p_1-1)\cdot(p_2-1)\cdot\ldots\cdot(p_k-1)}{p_1\cdot p_2\cdot\ldots\cdot p_k}\end{aligned}$$

Temos que

$$\frac{n}{\phi(n)} = \frac{n}{\frac{n\cdot(p_1-1)\cdot(p_2-1)\cdot\ldots\cdot(p_k-1)}{p_1\cdot p_2\cdot\ldots\cdot p_k}} = \frac{p_1\cdot p_2\cdot\ldots\cdot p_k}{(p_1-1)\cdot(p_2-1)\cdot\ldots\cdot(p_k-1)} \tag{4.2}$$

Agora vamos analisar o somatório $\sum_{d|n}\frac{\mu^2(d)}{\phi(d)}$. Temos $n = {p_1}^{r_1}\cdot {p_2}^{r_2}\cdot\ldots\cdot {p_k}^{r_k}$, pela definição de μ sabemos que $\mu(d)^2 = 1$ ou $\mu(d)^2 = 0$. Como $\mu(d)^2 = 0$ se existir algum p primo tal que $p^2|d$, iremos apenas analisar o somatório sobre os divisores d_i que não sejam divisíveis por p^2. Assim

$$\sum_{d_i|n}\frac{\mu^2(d_i)}{\phi(d_i)} = \sum_{d_i|n}\frac{1}{\phi(d_i)}.$$

Como os divisores d_i não são divisíveis por p^2, cada primo p pode ser usado na fatoração primaria, desta forma d_i pode assumir os valores:

$$1, p_1, p_2, \cdots, p_k, p_1\cdot p_2, \cdots, p_1\cdot p_k, p_2\cdot p_3, \cdots, p_{k-1}\cdot p_k, p_1\cdot p_2\cdot p_3, \cdots, p_1\cdot p_2\cdot\ldots\cdot p_k.$$

Então

$$\begin{aligned}\sum_{d_i|n}\frac{1}{\phi(d_i)} &= \frac{1}{\phi(1)}+\frac{1}{\phi(p_1)}+\frac{1}{\phi(p_2)}+\cdots+\frac{1}{\phi(p_k)}+\frac{1}{\phi(p_1\cdot p_2)}+\cdots+\frac{1}{\phi(p_1\cdot p_k)}+\\ &+\frac{1}{\phi(p_2\cdot p_3)}+\cdots+\frac{1}{\phi(p_{k-1}\cdot p_k)}+\frac{1}{\phi(p_1\cdot p_2\cdot p_3)}+\cdots+\frac{1}{\phi(p_1\cdot p_2\cdot\ldots\cdot p_k)}\\ &= 1+\frac{1}{(p_1-1)}+\frac{1}{(p_2-1)}+\cdots+\frac{1}{(p_k-1)}+\frac{1}{(p_1-1)\cdot(p_2-1)}+\\ &+\cdots+\frac{1}{(p_1-1)\cdot(p_k-1)}+\frac{1}{(p_2-1)\cdot(p_3-1)}+\cdots+\frac{1}{(p_{k-1}-1)\cdot(p_k-1)}+\\ &+\frac{1}{(p_1-1)\cdot(p_2-1)\cdot(p_3-1)}+\cdots+\frac{1}{(p_1-1)\cdot(p_2-1)\cdot\ldots\cdot(p_k-1)}\\ &= \frac{(p_1-1)\cdot\ldots\cdot(p_k-1)+(p_2-1)\cdot\ldots\cdot(p_k-1)+\cdots+1}{(p_1-1)\cdot(p_2-1)\cdot\ldots\cdot(p_k-1)}.\end{aligned}$$

Observe que numerador da última fração é

$$\begin{aligned}&(p_1-1)\cdot\ldots\cdot(p_k-1)+(p_2-1)\cdot\ldots\cdot(p_k-1)+\cdots+1 =\\ &= \phi(p_1)+\phi(p_2)+\cdots+\phi(p_k)+\phi(p_1\cdot p_2)+\cdots+\phi(p_1\cdot p_k)\\ &+\phi(p_2\cdot p_3)+\cdots+\phi(p_{k-1}\cdot p_k)+\phi(p_1\cdot p_2\cdot p_3)+\\ &+\cdots+\phi(p_1\cdot p_2\cdot\ldots\cdot p_k)\\ &= \sum_{q|p_1\cdot p_2\cdots p_k}\phi(q)\end{aligned}$$

como $n = p_1 \cdot p_2 \cdot ... \cdot p_k$, pelo Teorema 3.35 teremos

$$\sum_{q|n} \phi(q) = n = p_1 \cdot p_2 \cdot ... \cdot p_k$$

Então

$$\begin{aligned} \sum_{d_i|n} \frac{1}{\phi(d_i)} &= \frac{(p_1 - 1) \cdot ... \cdot (p_k - 1) + (p_2 - 1) \cdot ... \cdot (p_k - 1) + \cdots + 1}{(p_1 - 1) \cdot (p_2 - 1) \cdot ... \cdot (p_k - 1)} \\ &= \frac{p_1 \cdot p_2 \cdot ... \cdot p_k}{(p_1 - 1) \cdot (p_2 - 1) \cdot ... \cdot (p_k - 1)} \end{aligned}$$

o que é igual a equação (4.2), terminando assim a nossa demonstração. □

Conclusão

O objetivo deste trabalho é criar um material rico sobre funções elementares, que ofereça uma abordagem combinatória para a teoria elementar dos números. Além disso, temos como motivação criar um material que aborde estas funções aplicadas em questões, visto que o aprendizado se torna mais intenso quando se analisa resolução de exercícios.

Para alguns leitores bem estudados neste tema de funções aritméticas, este trabalho pode ser visto como uma ampla revisão de conceitos conhecidos. Para outros leitores, este trabalho é uma nova forma de estudar o conteúdo, por meio de exemplos e resoluções questões, o que facilitam a compreensão de propriedades e demonstrações. Este trabalho será de proveitoso para aqueles leitores que buscam, em um só lugar, conceitos e aplicações em exercícios.

Sobre as funções estudadas, começamos com $\tau(n)$ a quantidade de divisores de n e $\sigma(n)$ a soma dos divisores de n. Depois foi estudada a função $\phi(n)$ de Euler, a quantidade de números coprimos com n menores que n, e por fim, a função de Möbius $\mu(n)$. Durante todo o processo trouxemos exemplos, exercícios resolvidos, questões de olimpíadas internacionais, problemas em aberto e ligações externas. Além disso buscamos relacionar as funções apresentadas, o que é de extrema importância pois modifica a ideia de que a matemática é desvinculada e segmentada.

Sobre as funções citadas, o presente trabalho trouxe algumas definições e exemplos que são de fácil entendimento, possibilitando assim a compreensão dos alunos do ensino básico. Desta forma espera-se que o trabalho contribua para despertar o interesse do professor a trabalhar conteúdos de nível superior com alunos da educação básica. Por exemplo, o estudo da função de Euler pelo princípio da inclusão e exclusão, que é proposta neste trabalho, é uma possibilidade de apresentação do conteúdo para alunos a partir do primeiro ano do ensino médio.

Referências

1 HEFEZ, A. *Aritmética - Coleção PROFMAT*. [S.l.]: Editora da SBM, Rio de Janeiro-RJ. v. 2.

2 MARTINEZ, F. B. et al. Teoria dos números: Um passeio com primos e outros números familiares pelo mundo inteiro. *Coleção Projeto Euclides, IMPA*, 2013.

3 ANDREWS, G. E. *Number Theory*. [S.l.]: Courier Corporation, 1994.

4 ANDREESCU TITU E ANDRICA, D. *Teoria dos Números: estruturas, exemplos e problemas*. [S.l.]: Springer Science & Business Media, 2009.

5 SIERPINSKI, W. *Elementary Theory of Numbers: Second English Edition (edited by A. Schinzel)*. [S.l.]: Elsevier, 1988. v. 31.

6 SERGEI CHERNYKH - POWERED BY BOINC. *Amicable pairs list*. Disponível em: <https://sech.me/ap/>. Acesso em: 30 jan 2018.

7 GREAT INTERNET MERSENNE PRIME SEARCH-GIMPS. *GIMPS Discovers Largest Known Prime Number:* $2^8 2,589,933 - 1$. Disponível em: <https://www.mersenne.org/primes/press/M82589933.html>. Acesso em: 20 jan 2018.

8 ROSEN KENNETH H E GODDARD, B. e. O. K. *Teoria Elementar dos Números e suas Aplicações*. [S.l.]: Pearson / Addison Wesley, 2005.

9 JONES GARETH A E JONES, J. M. *Elementary Number Theory*. [S.l.]: Springer Science & Business Media, 1998.

10 GUY, R. *Unsolved problems in number theory*. [S.l.]: Springer Science & Business Media, 2013. v. 1.

11 SANTOS, J. P. de O.; MELLO, M. P.; MURARI, I. T. C. *Introdução análise combinatória*. [S.l.]: Ed. Ciencia Moderna.

12 HILDEBRAND, A. Introdução à matemática da teoria analítica de números 531 notas de aula, outono de 2005. *URL: http: // www. matemática. uiuc. edu / hildebr / formiga. Versão*, v. 1, 2006.