UNIVERSIDADE ESTADUAL DO PIAUÍ,
CENTRO DE CIÊNCIAS DA NATUREZA – CCN
CAMPUS POETA TORQUATO NETO
CURSO DE LICENCIATURA EM MATEMÁTICA

Francisco das Chagas Pereira de Oliveira Araujo

UMA INTRODUÇÃO ÀS FUNÇÕES ARITMÉTICAS

TERESINA – PI
2022

Francisco das Chagas Pereira de Oliveira Araujo

UMA INTRODUÇÃO ÀS FUNÇÕES ARITMÉTICAS

Trabalho de Conclusão de Curso apresentado ao Curso de Matemática, do Departamento de Matemática – Centro de Ciências da Natureza da Universidade Estadual do Piauí, como parte dos requisitos para a obtenção do título de Licenciado em Matemática.

Orientador: Prof. Dr. Afonso Norberto da Silva

TERESINA – PI

2022

A658i Araujo, Francisco das Chagas Pereira de Oliveira.
Uma introdução às funções aritméticas / Francisco das Chagas Pereira de Oliveira Araujo. - 2022.
63 f.

TCC (graduação) - Universidade Estadual do Piauí - UESPI, Curso Licenciatura em Matemática, *Campus* Poeta Torquato Neto, Teresina-PI, 2022.
"Orientador(a): Prof. Dr. Afonso Norberto da Silva."

1. Função aritmética multiplicativa. 2. Função de Euler. 3. Função de Mobius. I. Título.

CDD: 510

Ficha elaborada pelo Serviço de Catalogação da Biblioteca Central da UESPI
Grasielly Muniz Oliveira (Bibliotecária) CRB 3/1067

Agradecimentos

Primeiramente agradeço a Deus por ter guiado meus passos para que eu concluísse esta monografia com sucesso. Também agradeço a minha mãe, Deusenir, por ter me apoiado e me incentivado a seguir firme no curso até o fim.

Agradecimento especial a minha avó, Francisca, que cuidou de mim durante toda minha infância e que me educou e me mostrou o caminho do bem. Agradeço aos meus colegas de turma, em particular à Vanessa, Marielle, Erika e Mamede por várias vezes me ajudarem a resolver alguns exercícios ou tirando dúvidas, também pelas conversas agradáveis e por acreditarem em mim nos momentos em que eu desanimei.

Agradeço imensamente ao meu amigo e professor, Edio Aquino, que foi o responsável por eu ter escolhido o curso de Licenciatura em Matemática e que me ajudou com materiais e ideias que despertou minha paixão pela matemática.

Por último agradeço a todos os professores com quem pude ter aula durante o curso, em especial ao professor Pitágoras por me mostrar maneiras de questionar a minha própria intuição e me fazer ser mais rigoroso com minhas análises. Ao meu professor e orientador, Afonso, meus mais sinceros agradecimentos por ter me ensinado tudo o que pode nas disciplinas de Teoria dos Números e Análise Real, que me deram uma base sólida e madura para que eu pudesse está redigindo este trabalho.

Resumo

Na primeira parte deste trabalho é apresentado as fórmulas para determinar o número, soma e multiplicação de divisores, que são noções básicas para o estudo das funções aritméticas. Também é desenvolvido a noção de função aritmética multiplicativa seguido de vários exemplos, com destaque para as funções de Mobius e de Euler. Ainda é feito uma caracterização para a função e o Teorema de Euler, além de propriedades relativas à função de Euler. Por fim, é demonstrado a fórmula de inversão de Mobius que é usada para se chegar a uma importante relação entre a função de Mobius e de Euler.

Palavras chaves: Função Aritmética Multiplicativa, Função de Euler e Função de Mobius.

Abstract

The first part of this work presents the formulas to determine the number, sum and multiplication of divisors, which are basic notions for the study of arithmetic functions. The notion of multiplicative arithmetic function is also developed, followed by several examples, highlighting the Mobius and Euler functions. It is still made a characterization for the function and Euler's Theorem, in addition to properties related to the Euler function. Finally, the Mobius inversion formula is demonstrated, which is used to arrive at an important relationship between the Mobius and Euler functions.

Keywords: Multiplicative Arithmetic Function, Euler Function and Mobius Function.

Sumário

1. Introdução

Primeiramente gostaríamos de esclarecer que a presente monografia não tem caráter pedagógico, ou seja, os assuntos abordados aqui não são destinados para estudantes do Ensino Básico, exceto aqueles que se destinam as atividades olímpicas. Por conta disso, este trabalho é recomendado para estudantes graduandos e entusiastas que se interessam pelos assuntos tratados no decorrer do desenvolvimento dos capítulos.

A motivação para o estudo das funções aritméticas multiplicativas se dá pelo fato de que a propriedade multiplicativa delas permite a criação de uma infinidade de novas funções que também têm a mesma propriedade. Uma ferramenta que contribui enormemente para gerar funções desse tipo, é a fórmula de inversão de Mobius.

Neste trabalho acadêmico tratamos de definir o que é uma função aritmética, em particular, as multiplicativas completas ou não. Nas funções multiplicativas, mostraremos que se tivermos um número decomposto em potências de primos (que chamaremos de decomposição canônica), e aplicarmos a uma $f: \mathbb{N}^* \to \mathbb{Z}$ multiplicativa, fica determinado que a f do produto é igual ao produto das f's.

Para um bom entendimento do conteúdo, é importante ter conhecimentos prévios sobre congruências (módulo m), congruências lineares, existência de inverso multiplicativo (módulo m), decomposição em fatores primos, propriedades de somatórios e produtórios, de divisibilidade e mdc.

A real importância do estudo destas funções se dá em Teoria Algébrica dos Números e Teoria Analítica dos Números, que são cursos em nível de pós-graduação, por esse motivo, os resultados alcançados nesta monografia são apenas os elementos introdutórios para um estudo muito mais aprofundado.

Após esta introdução, iniciamos o segundo capítulo provando o teorema **2.1** (EDGARD, 1981) que, dado um inteiro positivo n, podemos reescrevê-lo como $n = dd'$, onde d e d' dividem n. Os teoremas **2.2, 2.3** e **2.4** (EDGARD, 1981), (CASTRO, Jânio; 2010) nos fornecem fórmulas para contar o número de divisores positivos de um inteiro, a soma dos divisores e por último o produto dos divisores, respectivamente.

No terceiro capítulo, a definição **3.1** (EDGARD, 1981) explica o que são funções aritméticas, em particular, as funções multiplicativas, já no teorema **3.1** (EDGARD, 1981), provamos que as funções τ e σ são multiplicativas**.** No teorema **3.2** (PLINIO, 2020), dada uma função f multiplicativa, então a F definida por $F(n) = \sum_{d|n} f(d)$, também é multiplicativa. A definição **3.3** (PLINIO 2020) se refere a função de Mobius, cujo teorema **3.3** (PLINIO, 2020) garante que a função de Mobius é multiplicativa, ainda sobre a função de Mobius, o teorema **3.4** (PLINIO, 2020) nos garante que $F(n) = \sum_{d|n} \mu(d) = 0$ para todo inteiro $n > 1$ e $F(1) = 1$. A definição **3.4** (EDGARD, 1981) estende a noção de função aritmética multiplicativa, sendo agora denominadas como funções aritméticas multiplicativas completas, ou seja, $f(ab) = f(a)f(b)$ para quaisquer inteiros positivos a e b. Vale destacar o exemplo **3.4** (Neto, Antônio Caminha Muniz) onde provamos uma desigualdade envolvendo as funções τ e σ.

Na definição **3.5** (EDGARD, 1981), definimos a função maior inteiro, que não é aritmética multiplicativa, mas pode se relacionar com elas de várias maneiras. Em seguida, o teorema **3.5** (PLINIO, 2020) estabelece uma serie de propriedades a respeito da função maior inteiro, já o teorema **3.6** (PLINIO, 2020) permite calcular a maior potência de um primo que divide $n!$ e com base neste resultado provamos o teorema **3.7** (PLINIO, 2020) que afirma que dados $n_i's$ naturais é válido que $(n_1 + \cdots . + n_r)!/n_1! \ldots n_r!$ é sempre inteiro.

O teorema **3.8** (EDGARD, 1981) nos mostra a fórmula de inversão de Mobius, que permite transformar uma função aritmética $f(n) = \sum_{d|n} g(d)$ para $g(n) = \sum_{d|n} \mu(d) f(n/d)$. Antes de abordamos o teorema de Wilson é necessário definir o que é um sistema completo de resíduos módulo m, definição **3.6** (PLINIO, 2020), em posse deste conceito, demonstraremos o teorema de Wilson e sua recíproca **3.9** e **3.10** (CASTRO, Jânio; 2010) que afirma que se p é primo, então $(p-1)! \equiv -1(mod\, p)$, já no caso da recíproca, temos $(n-1)! \equiv -1(mod\, n)$, então n é primo. O próximo resultado é o pequeno teorema de Fermat **3.11** (EDGARD, 1981) e como consequência do teorema de Fermat vem o corolário **3.1** (PLINIO, 2020) dado pela relação $a^p \equiv a(mod\, p)$, sendo p primo e a um inteiro positivo.

O quarto capítulo é voltado ao estudo da função e teorema de Euler, sendo que a primeira definição **4.1** (EDGARD, 1981), é justamente sobre a

função φ de Euler, que dado um inteiro n positivo, $\varphi(n)$ conta a quantidade de primos relativos com n e que são menores ou iguais a n, onde ocorre a igualdade se $n = 1$.

O teorema **4.1** (EDGARD, 1981) garante que φ é uma função multiplicativa (não completamente). Para provar o teorema de Euler, vamos precisar conhecer a noção de sistema reduzido de resíduos módulo m dada na definição **4.2** (PLINIO, 2020) seguida do lema **4.1** (EDGARD, 1981), a partir disso podemos provar o teorema de Euler **4.2** (EDGARD, 1981), onde temos $a^{\varphi(n)} \equiv 1(mod\, n)$, com $mdc(a, n) = 1$. Os dois próximos resultados vão possibilitar caracterizar a função φ de Euler, ou seja, obteremos uma fórmula fechada que satisfaz as condições dadas na sua definição, sendo assim, o teorema **4.3** (EDGARD, 1981) nos diz que $\varphi(n) = n - 1$, se, e somente se n for primo. O teorema **4.4** (EDGARD, 1981) afirma que dados p primo e k positivo, tem-se $\varphi(p^k) = p^k - p^{k-1}$ e finalmente o teorema **4.5** (PLINIO, 2020) resulta na seguinte expressão:$\varphi(n) = n\prod_{i=1}^{r}(1 - 1/p_i)$.

Após caracterizarmos a função φ de Euler, vamos abordar algumas propriedades da função φ. Começando com o teorema **4.6** (EDGARD, 1981) que garante que $\varphi(n)$ é sempre par para todo $n > 2$. De acordo com o teorema **4.7** (EDGARD, 1981), é válido a expressão:$\sum_{i=1}^{k}\varphi(p^i) = p^k$.

Antes de provarmos o teorema de Gauss, vamos precisar da definição **4.3** que classifica os subconjuntos do conjunto $\{1, 2, \dots, n\}$ em classes de acordo com um certo critério. E o teorema de Gauss é o **4.8** (EDGARD, 1981) que é uma generalização do teorema **4.7**, ou seja, $\sum_{d|n}\varphi(d) = n$ para todo $n > 1$. Sabemos que a função $\varphi(n)$, conta os números que são menores que n e são primos com n, mas no teorema **4.9** (EDGARD, 1981) aprendemos a somar todos os números que satisfazem essa condição, na qual é calculada pela seguinte fórmula: $\frac{1}{2}.n.\varphi(n)$.

O último teorema do capítulo quatro estabelece uma relação entre a função φ de Euler e μ de Mobius, de modo que no teorema **4.10** (EDGARD, 1981) podemos chegar a uma relação que leva a uma nova caracterização da função φ fazendo uma aplicação direta da fórmula de inversão de Mobius de modo a obter $\varphi(n) = n\sum_{d|n}\mu(d)/d$.

O quinto capítulo conta com resolução de problemas e comentários a respeito dos resultados anteriores aplicados aos problemas e no total são 14 problemas variados sobre os assuntos que foram abordados nos capítulos $2, 3$ e 4. Todas as questões foram adaptadas e traduzidas do livro Elementary Number Theory de autoria de David M. Burton.

2. Noções preliminares

Antes de enunciarmos as definições e os teoremas relacionados às funções aritméticas, que são o principal objeto de estudo deste trabalho, vamos desenvolver formas de calcular o número de divisores positivos de um inteiro, a soma dos divisores positivos, e por último, o produto dos divisores. Tais fórmulas serão úteis para o estudo do próximo capítulo.

2.1 Divisores de um inteiro

Teorema 2.1: Seja $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ a decomposição canônica do inteiro $n > 1$, então os divisores positivos de n são precisamente os inteiros d da forma

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$$

onde $0 \leq \beta_i \leq \alpha_i$ com $i = 1, 2, 3, \dots, r$.

Demonstração:

É fácil ver que os divisores triviais $d = 1$ e $d = n$ se obtêm quando ocorre, respectivamente

$$\beta_i = 0, \qquad i = 1, 2, \dots, r$$

$$\alpha_i = \beta_i, \qquad i = 1, 2, \dots, r$$

Suponhamos que d seja um divisor não trivial de n, isto é,

$$n = dd_1, \text{ com } d, d_1 > 1$$

Denotando $d \; e \; d_1$ como produto de primos, não necessariamente distintos, vêm

$$d = q_1 q_2 \dots q_s \; e \; d_1 = t_1 t_2 \dots t_u$$

Daí, obtemos

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = q_1 q_2 \dots q_s t_1 t_2 \dots t_u$$

que são duas decomposições do inteiro positivo n num produto de primos, e como a fatoração em primos é única a menos da ordem dos fatores, então cada primo q_i coincide com um p_j de modo que, substituindo os produtos de primos iguais por potências de expoente inteiro, teremos

$$d = q_1 q_2 \dots q_s = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$$

onde é possível algum $\beta_i = 0$.

Reciprocamente todo inteiro

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}, \qquad 0 \leq \beta_i \leq \alpha_i$$

é um divisor de n, logo,

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r} = \left(p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}\right)\left(p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} \dots p_r^{\alpha_r-\beta_r}\right) =$$

$$= d\left(p_1^{\alpha_1-\beta_1} p_2^{\alpha_2-\beta_2} \dots p_r^{\alpha_r-\beta_r}\right)$$

onde $\alpha_i - \beta_i \geq 0$ para todo $1 \leq i \leq r$. Logo, d é um divisor de n.

Exemplo 2.1: Escreva o número 360 como produto de dois divisores positivos.

Solução:

Os divisores positivos de $n = 2^3.3^2.5 = 360$ são precisamente os inteiros d da forma

$$d = 2^{\alpha_1}.3^{\alpha_2}.5^{\alpha_3}$$

onde,

$$0 \leq \alpha_1 \leq 3, \qquad 0 \leq \alpha_2 \leq 2, \qquad 0 \leq \alpha_3 \leq 1$$

isto é,

$$\alpha_1 = 0, 1, 2, 3,\ \alpha_2 = 0, 1, 2,\ \alpha_3 = 0, 1.$$

Tomando $\alpha_1 = 2,\ \alpha_2 = 0$ e $\alpha_3 = 1$, obtemos o divisor

$$d = 2^2.3^0.5 = 4.1.5 = 20$$

do inteiro 360, portanto, $360 = 18.20$

2.2 Número de divisores

Seja n um inteiro positivo. O número de divisores positivos de n será denotado por $\tau(n)$. Assim, por exemplo, os divisores de 18 são $1, 2, 3, 6, 9\ e\ 18$, portanto $\tau(18) = 6$. Em particular, se p é um primo, então $\tau(p) = 2$, pois para qualquer primo p positivo, os únicos números que dividem p são $1\ e\ p$. Para p^2 temos como divisores positivos, $1, p\ e\ p^2$, onde $\tau(p^2) = 3$. De modo geral, $\tau(p^n) = n + 1$, pois os divisores positivos de p^n são $1, p, p^2, \dots, p^n$.

A tabela abaixo dá o número de divisores positivos dos inteiros de $1\ até\ 10$:

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

Como vimos, é muito inconveniente contar o número de divisores positivos de um inteiro. No próximo teorema, vamos deduzir uma fórmula para calcular o número de divisores positivos de um inteiro usando o princípio multiplicativo.

Teorema 2.2: Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ é a decomposição canônica do inteiro positivo $n > 1$, então:

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1)$$

Demonstração:

Pelo teorema **2.1** os divisores positivos de n são precisamente os inteiros d da forma:

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r}$$

onde,

$$0 \leq \beta_i \leq \alpha_i,\ i = 1, 2, \dots, r.$$

Note que temos $\alpha_1 + 1$ maneiras de escolher o expoente de β_1. Analogamente temos $\alpha_2 + 1$ maneiras para β_2, e assim por diante, até o último expoente que são $\alpha_r + 1$ maneiras de escolher β_r, logo, pelo princípio multiplicativo, o número total de maneiras de escolher os expoentes $\beta_1, \beta_2, \dots, \beta_r$ é dado pelo produto:

$$(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1)$$

Portanto, o número $\tau(n)$ de divisores positivos do inteiro $n > 1$ é dado por:

$$\tau(n) = \prod_{i=1}^{r} (\alpha_i + 1)$$

Note que

$$\tau(n) = \tau\left(p_1^{\alpha_1}\right)\tau\left(p_2^{\alpha_2}\right) \dots \tau(p_r^{\alpha_r})$$

A propriedade acima será melhor explorada no capítulo de funções aritméticas.

Exemplo 2.2: Qual o número de divisores positivos de $n = 504 = 2^3.3^2.7$?

Solução:

Usando a fórmula que fornece o número de divisores, temos:

$$\tau(504) = (3+1)(2+1)(1+1) = 4.3.2 = 24$$

Para determinar todos os 24 divisores positivos de 504, podemos dividir a contagem dos divisores por etapas, por exemplo, calculando as potências individuais de $2, 3\ e\ 7$, depois os seus produtos dois a dois e por último o produto dos três números variando suas potências, assim:

$$1, 2, 4\ e\ 8$$

$$3\ e\ 9$$

$$7$$

$$6, 12, 14, 18, 21, 36, 28, 24, 63, 72, 56$$

$$42, 126, 168, 84, 252, 504$$

Exemplo 2.3: Achar o menor inteiro positivo n que tem 9 divisores positivos.

Solução:

Como $9 = 1.9 = 3.3$, temos

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) = 1.9$$

ou

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) = 3.3$$

De modo a obter o menor inteiro n positivo, temos que escolher as menores bases, assim, teremos $2^{\alpha}.3^{\beta}$, e os possíveis expoentes são $0\ e\ 8\ ou\ 2\ e\ 2$..

Como $2^8.3^0 > 2^2.3^2$, concluímos que o menor inteiro positivo n com 9 divisores é:

$$2^2.3^2 = 36$$

Exemplo 2.4: Achar o inteiro positivo da forma 28.15^{α} e que admite 54 divisores positivos.

Solução:

Decompondo $28.15^{\alpha} = 2^2.7.3^{\alpha}.5^{\alpha}$, temos:

$$(2+1)(1+1)(\alpha+1)(\alpha+1) = 54 \Rightarrow$$
$$(\alpha+1)^2 = 9 \Rightarrow$$
$$\alpha + 1 = 3$$

Ou seja, $\alpha = 2$, o que nos dá $28.15^2 = 6300$.

2.3 Soma de divisores

Seja n um inteiro positivo, a soma dos divisores positivos de n será denotado por $\sigma(n)$. Assim, por exemplo, os divisores positivos de 18 são $1, 2, 3, 6, 9\ e\ 18$, portanto a soma resulta em

$$\sigma(18) = 1 + 2 + 3 + 6 + 9 + 18 = 39$$

Em particular, se p é um primo, então $\sigma(p) = p + 1$, pois os únicos divisores positivos de $p\ são\ 1\ e\ p$. Pelo mesmo raciocínio, $\sigma(p^2) = p^2 + p + 1$. Note que $\sigma(p^2)$ é a soma de uma PG finita de razão p que é dada por:

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

De modo geral, os divisores positivos de p^n são

$$1, p, p^2, \ldots, p^n$$

Portanto,

$$\sigma(p^n) = 1 + p + p^2 + \cdots + p^n = \frac{p^{n+1} - 1}{p - 1}$$

Teorema 2.3: Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ é a decomposição canônica do inteiro positivo $n > 1$, então

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{\alpha_r} - 1}{p_r - 1}$$

Demonstração:

Consideremos o produto

$$\left(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}\right)\left(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}\right) \ldots \left(1 + p_r + p_r^2 + \cdots + p_r^{\alpha_r}\right)$$

Pelo teorema **2.1,** cada divisor positivo de n é um termo do desenvolvimento deste produto e vice-versa, de modo que

$$\sigma(n) = \left(1 + p_1 + p_1^2 + \cdots + p_1^{\alpha_1}\right)\left(1 + p_2 + p_2^2 + \cdots + p_2^{\alpha_2}\right) \ldots (1 + p_r + p_r^2 + \cdots + p_r^{\alpha_r})$$

Aplicando a cada parênteses do lado direito a fórmula da soma dos termos de uma PG finita, temos

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{\alpha_r+1} - 1}{p_r - 1}$$

Isto é,

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

Note ainda que

$$\sigma(n) = \sigma\left(p_1^{\alpha_1}\right)\sigma\left(p_2^{\alpha_2}\right) \ldots \sigma(p_r^{\alpha_r})$$

Exemplo 2.5: Qual soma dos divisores positivos do inteiro $n = 600 = 2^3.3.5^2$?

Solução:

$$\sigma(600) = \frac{2^4 - 1}{2 - 1} \cdot \frac{3^2 - 1}{3 - 1} \cdot \frac{5^3 - 1}{5 - 1} = 15.4.31 = 1860$$

.

2.4 Produto de divisores

Teorema 2.4: O produto dos divisores positivos de um inteiro positivo $n > 1$ é igual a $n^{\tau(n)/2}$

Demonstração:

Basta verificar que sempre que $d|n$ então existe a inteiro tal que $a = n/d$ e também $a|n$. Assim, considere

$$Q = \prod_{d|n} d$$

Do mesmo modo, vale que

$$Q = \prod_{d|n} \frac{n}{d}$$

Daí, multiplicando as duas igualdades membro a membro, temos

$$Q^2 = \prod_{d|n} d \prod_{d|n} \frac{n}{d} = \prod_{d|n} d \cdot \frac{n}{d} = \prod_{d|n} n$$

Isto é,

$$Q^2 = \prod_{d|n} n$$

No segundo membro, temos o produto onde todos os fatores são iguais a n, cujo número de fatores equivale a quantidade de divisores de n, o que significa que o produto tem $\tau(n)$ fatores iguais a n, ou seja,

$$Q^2 = n^{\tau(n)}$$

Extraindo a raiz quadrada em ambos os membros e levando em conta que $Q > 0$, temos finalmente

$$Q = n^{\tau(n)/2}$$

Pode haver dúvidas quanto a validade desta fórmula, pois se $\tau(n)$ for ímpar, o expoente $\tau(n)/2$ não seria inteiro, mas de fato o expoente será sempre inteiro, pois o número de divisores de um inteiro positivo só é ímpar se n for um quadrado perfeito. Vejamos com um exemplo.

Exemplo 2.6: Determine o produto dos divisores positivos do inteiro $n = 16$.
Solução:

$$\prod_{d|16} d = 16^{\tau(16)/2} = 16^{5/2} = (4^2)^{5/2} = 4^5 = 1024$$

Vamos justificar agora porque $\tau(n)$ é ímpar quando n é um quadrado perfeito. Seja $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ um inteiro positivo e pelo teorema **2.2,** temos

$$\tau(n) = (1 + \alpha_1)(1 + \alpha_2) \dots (1 + \alpha_k)$$

Do mesmo modo, tomando $m = n^2$, obtemos

$$\tau(m) = (1 + 2\alpha_1)(1 + 2\alpha_2) \dots (1 + 2\alpha_k)$$

Note que todos os termos $1 + 2\alpha_i$ são ímpares, e o produto de ímpares sempre resulta em um número ímpar, logo

$$\tau(m) = \prod_{i=1}^{k} (1 + 2\alpha_i)$$

é um número ímpar.

3. Funções Aritméticas

Neste terceiro capítulo vamos esclarecer o que são funções aritméticas, explorando especialmente a propriedade multiplicativa destas funções. As fórmulas do número e soma de divisores positivos vão passar a ser definidas como funções que cumprem a propriedade multiplicativa mediante a um certo critério.

Outra função aritmética multiplicativa que iremos estudar é a função de Mobius e algumas de suas propriedades, além da famosa fórmula de inversão de Mobius. A função parte inteira e suas propriedades também são objeto de estudo neste capítulo, mas ela não é propriamente uma função aritmética multiplicativa, mas podemos formar relações que envolvem os dois tipos de funções. Por último, veremos os teoremas de Wilson e Fermat.

3.1 Funções Aritméticas e Multiplicativas

Definição 3.1: Chama-se função aritmética toda função f definida de $\mathbb{N}^* \; em \; \mathbb{Z}$, isto é, toda $f: \mathbb{N}^* \to \mathbb{Z}$. Além disso, uma função aritmética f é chamada de função aritmética multiplicativa se

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

Para todo par de inteiros positivos $a \; e \; b$ tais que o $mdc(a, b) = 1$.

Duas funções aritméticas importantes são as funções $\tau \; e \; \sigma$ de $\mathbb{N}^* \; em \; \mathbb{N}$ assim definidas para todo inteiro positivo n:

$$\tau(n) = número \; de \; divisores \; positivos \; de \; n$$

$$\sigma(n) = soma \; dos \; divisores \; positivos \; de \; n$$

Note que qualquer função pode ser uma função aritmética se restringirmos o domínio da função a $\mathbb{N}^*$. O contradomínio de uma função aritmética poderia ser o conjunto $\mathbb{R}$, mas no contexto que estamos estudando, não é necessário fazer isso.

Podemos dar como exemplo de funções aritméticas multiplicativas, as funções $f\ e\ g$ definidas por $f(n) = 1$ e $g(n) = n$, que são respectivamente as funções constante (unitária) e identidade. É fácil comprovar isso fazendo $n = ab$, daí temos

$$f(ab) = 1 = 1.1 = f(a)f(b)$$

$$g(ab) = ab = g(a)g(b)$$

Note que as funções $f\ e\ g$ acima satisfazem a igualdade

$$f(mn) = f(m)f(n)$$

mesmo se o $mdc(m,n) \neq 1$.

Podemos ainda definir as funções $\tau\ e\ \sigma$ como um somatório das duas funções anteriores, de modo que obteremos

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

e

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

Esta notação indica que a soma irá percorrer todos os divisores positivos de n, logo, teremos $\tau(n)$ parcelas nas respectivas somas, por exemplo:

$$\sigma(30) = \sum_{d|30} d = 1 + 2 + 3 + 5 + 6 + 10 + 15 + 30 = 72$$

Seja f uma função aritmética multiplicativa com $n_1, n_2, \dots, n_k$ inteiros positivos primos entre si dois a dois, então, usando o *teorema da indução matemática*, obtemos

$$f(n_1.n_2 \dots n_k) = f(n_1)f(n_2) \dots f(n_k)$$

Portanto, se $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ é a decomposição canônica de um inteiro positivo com $n > 1$, e além disso, os fatores

$$p_i^{\alpha_i}, \quad 1 \leq i \leq r$$

são primos entre si dois a dois, então temos

$$f(n) = f\left(p_1^{\alpha_1}\right) f\left(p_2^{\alpha_2}\right) \dots f(p_r^{\alpha_r}).$$

Esta igualdade mostra que uma função aritmética multiplicativa fica completamente determinada quando seus valores para as potências de primos são conhecidos.

Importa ainda convencionar que para toda função aritmética multiplicativa não identicamente nula se tem $f(1) = 1$, pois existe um inteiro positivo n tal que $f(n) \neq 0$ e como o $mdc(n, 1) = 1$, temos:

$$f(n) = f(n.1) = f(n)f(1) \Rightarrow f(1) = 1.$$

A justificativa para que a função identicamente nula não seja multiplicativa fica evidente no último resultado, pois cancelamos $f(n)$ em ambos os membros, por isso é necessário que $f(n)$ não seja identicamente nula dentro do contexto das funções aritméticas multiplicativas. Importante também não confundir $f(n) = 0$, para algum inteiro $n \geq 1$ e $f(n) = 0$ para quaisquer valor de n, apenas no segundo caso, a função é identicamente nula.

Exemplo 3.1: Mostrar que as funções $F(n) = f(n)g(n)$ e $G(n) = f(n)/g(n)$ são multiplicativas sendo $f(n)$ e $g(n)$ multiplicativas com $g(n) \neq 0$.

Solução:

Queremos mostrar que as funções F e G são multiplicativas, sabendo que f e g são multiplicativas, assim, considere inteiros positivos m e n tais que $mdc(m, n) = 1$, logo

$$F(mn) = f(mn)g(mn) = f(m)f(n)g(m)g(n) =$$
$$= f(m)g(m)f(n)g(n) = F(m)F(n)$$

Além disso,

$$G(mn) = \frac{f(mn)}{g(mn)} = \frac{f(m)f(n)}{g(m)g(n)} = \frac{f(m)}{g(m)} \cdot \frac{f(n)}{g(n)} = G(m)G(n)$$

Com isso, concluímos que o produto e o quociente de funções multiplicativas, também são multiplicativas.

Teorema 3.1: As funções $\tau(n)\ e\ \sigma(n)$ são ambas funções aritméticas multiplicativas.

Demonstração:

Sejam $u\ e\ v$ dois inteiros positivos tais que o $mdc(u, v) = 1$.

Se $u = 1\ ou\ v = 1$, o resultado segue de imediato.

Suponhamos então, $u > 1\ e\ v > 1$, e sejam

$$u = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i}\ e\ v = q_1^{\beta_1} q_2^{\beta_2} \dots q_j^{\beta_j}$$

as decomposições canônicas de $u\ e\ v$.

Como $p_x \neq q_y$, onde $x = 1, 2, \dots, i\ e\ y = 1, 2, \dots, j$, e também $mdc(u, v) = 1$ segue que a decomposição canônica do produto uv é dada pela igualdade:

$$uv = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_i^{\alpha_i} q_1^{\beta} q_2^{\beta_2} \dots q_j^{\beta_j}$$

Portanto,

$$\tau(uv) = [(\alpha_1 + 1) \dots (\alpha_i + 1)].\left[(\beta_1 + 1) \dots \left(\beta_j + 1\right)\right] = \tau(u)\tau(v)$$

e

$$\sigma(uv) = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \dots \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}\right) \cdot \left(\frac{q_1^{\beta_1+1} - 1}{q_1 - 1} \dots \frac{q_j^{\beta_j+1} - 1}{q_j - 1}\right) = \sigma(u)\sigma(v)$$

Segue que $\tau(n)\ e\ \sigma(n)$ são funções aritméticas multiplicativas.

Mas, e quanto a fórmula do produto dos divisores? Não podemos provar que ela também é multiplicativa?

Seja $f(n) = n^{\tau(n)/2}$, vamos verificar que $f(20) \neq f(4)f(5)$, com $mdc(4, 5) = 1$

$$f(20) = 20^{\tau(20)/2} = 20^{6/2} = 20^3$$

$$f(4)f(5) = 4^{\tau(4)/2}.5^{\tau(5)/2} = 4^{3/2}.5^{2/2} = 2^3.5$$

Claramente $20^3 \neq 2^3.5$, logo, esta função assim definida, não é aritmética multiplicativa.

Exemplo 3.2: Verificar que a função $\tau(n)$ é uma função aritmética multiplicativa para $n = 36$.

Solução:

Temos $36 = 2^2.3^2$ e o $mdc(4,9) = 1$. Logo:

$$\tau(36) = (2 + 1)(2 + 1) = 3.3 = 9$$

$$\tau(4) = \tau(2^2) = 2 + 1 = 3$$

$$\tau(9) = \tau(3^2) = 2 + 1 = 3$$

ou seja,

$$\tau(36) = \tau(4)\tau(9)$$

Exemplo 3.3: Verificar que a função $\sigma(n)$ é uma função aritmética multiplicativa para $n = 72$.

Solução:

Temos $72 = 2^3.3^2$ e o $mdc(8,9) = 1$. Logo:

$$\sigma(72) = \frac{2^4 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} = 15.13 = 195$$

$$\sigma(8) = \frac{2^4 - 1}{2 - 1}$$

$$\sigma(9) = \frac{3^3 - 1}{3 - 1}$$

ou seja,

$$\sigma(72) = \sigma(8)\sigma(9)$$

Exemplo 3.4: Prove que, para todo n natural, temos $\frac{\sigma(n)}{\tau(n)} \geq \sqrt{n}$.

Solução:

Sejam d e n inteiros positivos tais que $d|n$, então n/d é inteiro, sendo assim, vamos usar a desigualdade entre a média aritmética e geométrica com os números d e n/d, logo

$$\frac{d + n/d}{2} \geq \sqrt{d.\frac{n}{d}} \Rightarrow d + \frac{n}{d} \geq 2\sqrt{n}$$

Repetindo o uso da desigualdade para cada divisor positivo de n e somando ordenadamente os resultados, obteremos

$$\sum_{d|n} d + \sum_{d|n} \frac{n}{d} \geq \tau(n)2\sqrt{n}$$

Como as somas percorrem os mesmos divisores, segue que

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

Portanto,

$$2\sigma(n) \geq 2\tau(n)\sqrt{n} \Rightarrow \frac{\sigma(n)}{\tau(n)} \geq \sqrt{n}$$

Este exemplo pode ser encontrado na coleção “Tópicos da Matemática Elementar *Volume* 5” (Neto, Antônio) como um exercício, mas aqui ilustramos como um exemplo envolvendo as funções τ e σ.

Teorema 3.2: Se f é uma função aritmética multiplicativa e F é a função aritmética assim definida

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

então F também é multiplicativa.

Demonstração:

Devemos mostrar que $F(mn) = F(m)F(n)$ onde o $mdc(m,n) = 1$. Pela definição de $F(n)$ devemos ter

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

Como $mdc(m,n) = 1$, o teorema **2.1** nos garante que todo divisor de mn pode ser expresso de modo único, como o produto de $d_1 \, e \, d_2 \, onde \, d_1|m \, e \, d_2|n$ e $mdc(d_1, d_2) = 1$ e para cada par de divisores $d_1 \, de \, m \, e \, d_2 \, de \, n$ corresponde um único divisor $d = d_1 d_2 \, de \, mn$. Logo,

$$F(mn) = \sum_{d|mn} f(d) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1 d_2)$$

Mas, como f é, por hipótese, multiplicativa, temos:

$$F(mn) = \sum_{\substack{d_1|m \\ d_2|n}} f(d_1) f(d_2)$$

$$= \sum_{d_1|m} \sum_{d_2|n} f(d_1) f(d_2)$$

$$= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) = F(m)F(n).$$

Exemplo 3.5: Verificar que a função aritmética $F(n)$ é multiplicativa para $n = 24$.

Solução:

Temos $24 = 3.8 \, e \, o \, mdc(3,8) = 1$. Portanto:

$$F(3.8) = \sum_{d|24} f(d) =$$

$$= f(1) + f(2) + f(3) + f(4) + f(6) + f(8) + f(12) + f(24)$$

Ou seja,

$$F(3.8) = f(1.1) + f(1.2) + f(1.3) + f(1.4) +$$
$$+f(2.3) + f(1.8) + f(3.4) + f(3.8) =$$
$$= f(1)f(1) + f(1)f(2) + f(1)f(3) + f(1)f(4) +$$
$$+f(2)f(3) + f(1)f(8) + f(3)f(4) + f(3)f(8)$$

Agrupando os termos semelhantes, temos

$$F(3.8) = [f(1) + f(3)].[f(1) + f(2) + f(4) + f(8)] =$$
$$= \sum_{d|3} f(d) \sum_{d|8} f(d) = F(3)F(8)$$

3.2 Função de Mobius

Definição 3.2: Dado um inteiro positivo $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, a função aritmética μ de Mobius é definida por:

$$\mu(n) = \begin{cases} 1, & se\ n = 1 \\ (-1)^r\ se\ \alpha_1 = \alpha_2 = \cdots = \alpha_r = 1 \\ 0, & se\ p_i^k | n,\ \ para\ k > 1 \end{cases}$$

Com isso queremos dizer que a função $\mu(n)$ sempre irá se anular quando houver algum primo com expoente maior que 1 na decomposição de n, e se todos os expoentes forem iguais a 1, dizemos que o número n é livre de quadrados. Note ainda que r corresponde ao número de primos distintos do inteiro n. Vejamos alguns exemplos:

$$\mu(10) = \mu(2.5) = (-1)^2 = 1$$
$$\mu(18) = \mu(2.3^2) = 0$$
$$\mu(30) = \mu(2.3.5) = (-1)^3 = -1$$
$$\mu(100) = \mu(2^2.5^2) = 0$$

Em particular, se p é primo, então:

$$\mu(p) = -1\ e\ \mu(p^k) = 0\ para\ todo\ k \geq 2$$

A tabela abaixo nos dá os valores de $\mu(n)$ para os 10 primeiros inteiros positivos:

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

Teorema 3.3: A função μ de Mobius é uma função aritmética multiplicativa.

Demonstração:

Devemos mostrar que $\mu(mn) = \mu(m)\mu(n)$. Se $m = 1$, temos

$$\mu(mn) = \mu(n) = 1.\mu(n) = \mu(1)\mu(n) = \mu(m)\mu(n)$$

O resultado segue análogo para $n = 1$.

Suponhamos que $m > 1\ e\ n > 1$ tais que $mdc(m,n) = 1$. Se para algum primo p, tivermos $p^2|mn,$ então $p^2|m\ ou\ p^2|n$, visto que $mdc(m,n) = 1$. Logo, em ambos os casos, temos $\mu(mn) = \mu(m)\mu(n)$. Se $m\ ou\ n$ não é divisível pelo quadrado de nenhum primo, então $m = p_1p_2 \dots p_r\ e\ n = q_1q_2 \dots q_s$ e, portanto,

$$mn = p_1p_2 \dots p_rq_1q_2 \dots q_s.$$

Logo,

$$\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n)$$

Teorema 3.4: Seja n um inteiro positivo, então:

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

Demonstração:

Sabendo que $\mu(d)$ é multiplicativa, o teorema **3.2** nos garante que $F(n)$ é multiplicativa. É fácil verificar para o caso $n = 1$, pois

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

Suponhamos $n > 1$, podemos tomar $n = p^r$, onde p é um primo e $r > 1$. Logo

$$F(p^r) = \sum_{d|p^r} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^r) =$$

$$= 1 + \mu(p) = 1 - 1 = 0$$

Portanto $F(n) = 0$ para todo $n > 1$. O que conclui a demonstração.

Uma maneira alternativa de chegar a este resultado seria observar que na soma

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

os únicos termos que não são nulos vêm de $d = 1$ e dos divisores que são produto de primos distintos e livre de quadrados, isto é,

$$\sum_{d|n} \mu(d) = 1 + \mu(p_1) + \cdots + \mu(p_r) + \mu(p_1 p_2) + \mu(p_1 p_3) +$$

$$+ \cdots + \mu(p_1 p_r) + \cdots + \mu(p_1 p_2 \ldots p_r) =$$

$$= 1 + \binom{r}{1}(-1)^r + \binom{r}{2}(-1)^2 + \cdots + \binom{r}{r}(-1)^r =$$

$$= (1-1)^r = 0.$$

Onde na última linha foi usado o teorema do Binômio de Newton.

3.3 Funções Aritméticas Multiplicativas Completas

Definição 3.3: Uma função aritmética $f: \mathbb{N}^* \to \mathbb{Z}$ diz-se uma função aritmética multiplicativa completa se $f(ab) = f(a)f(b)$ para todo par de inteiros positivos $a\ e\ b$.

Assim, por exemplo, a função aritmética f definida por $f(n) = n^k$, para algum k inteiro não negativo fixado, é uma função aritmética multiplicativa completa, pois, quaisquer que sejam os inteiros positivos $a\ e\ b$, temos:

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

Usando o teorema **3.2,** podemos definir uma nova função aritmética $F(n)$ que também será multiplicativa, de modo a obter

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

Note que fazendo $k = 0\ e\ k = 1$, temos respectivamente

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

As funções $\tau(n), \sigma(n)\ e\ \mu(n)$ não são funções aritméticas multiplicativas completas, pois:

$$\tau(2.14) = \tau(28) = 6 \neq 2.4 = \tau(2)\tau(14)$$
$$\sigma(2.14) = \sigma(28) = 56 \neq 3.24 = \sigma(2)\sigma(14)$$
$$\mu(2.14) = \mu(28) = 0 \neq (-1).1 = \mu(2)\mu(14)$$

Um exemplo de função aritmética multiplicativa completa, seria $f(n) = n^5$ e para quaisquer inteiros a e b positivos, vale que

$$f(ab) = (ab)^5 = a^5b^5 = f(a)f(b)$$

Na próxima seção vamos definir a função maior inteiro, que é conhecida também como função parte inteira ou função "piso" que é muito importante em Teoria dos Números, embora normalmente não seja uma função aritmética multiplicativa, tal função será útil para chegarmos em alguns resultados interessantes.

3.4 Função Maior Inteiro

Definição 3.4: A função "*maior inteiro*", definida de $\mathbb{R}\ em\ \mathbb{Z}$ associa a cada real x o maior inteiro menor do que ou igual a x. Denotamos este valor por $\lfloor x \rfloor$. Em outras palavras, $\lfloor x \rfloor$ é o único inteiro que satisfaz à condição:

$$x - 1 < \lfloor x \rfloor \leq x$$

A seguir, damos alguns exemplos:

$$\lfloor \sqrt{3} \rfloor = 1, \qquad \lfloor -\pi \rfloor = -4,$$
$$\lfloor \pi \rfloor = 3, \qquad \lfloor 2{,}333\ldots \rfloor = 2$$

Importante notar que a igualdade $\lfloor x \rfloor = x$ ocorre se e somente se x é um inteiro, e que todo número real x pode escrever-se na forma:

$$x = n + \alpha, \quad \text{onde } n \text{ é inteiro e } 0 \leq \alpha < 1.$$

Agora veremos algumas propriedades relacionadas à função maior inteiro.

Teorema 3.5: Para um número real x, vale que:

1. $\lfloor x+n \rfloor = \lfloor x \rfloor + n$, para todo inteiro n.
2. $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1,\ x-1 < \lfloor x \rfloor \leq x,\ 0 \leq x - \lfloor x \rfloor < 1$.
3. Se $x \notin \mathbb{Z}$, então $\lfloor -x \rfloor = -\lfloor x \rfloor - 1$.
4. $\lfloor x \rfloor + \lfloor y \rfloor \leq \lfloor x+y \rfloor \leq \lfloor x \rfloor + \lfloor y \rfloor + 1$.
5. $\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0\ se\ x\ for\ inteiro \\ -1\ caso\ contrário. \end{cases}$
6. $\left\lfloor \frac{\lfloor x \rfloor}{m} \right\rfloor = \left\lfloor \frac{x}{m} \right\rfloor$ para m um inteiro positivo.
7. $\lfloor 2x \rfloor - 2\lfloor x \rfloor = \begin{cases} 1\ se\ \lfloor 2x \rfloor \text{ é } ímpar \\ 0\ se\ \lfloor 2x \rfloor \text{ é } par. \end{cases}$
8. Se n é um inteiro positivo, $\left\lfloor \frac{n}{a} \right\rfloor$ é o número de inteiros do conjunto $\{1, 2, 3, \ldots, n\}$ que são divisíveis por a.

Demonstração:

(1) Seja $x = m + \alpha$, onde m é um inteiro e $0 \leq \alpha < 1$, então

$$\lfloor x+n \rfloor = \lfloor m+\alpha+n \rfloor = \lfloor (m+n)+\alpha \rfloor = m+n = \lfloor x \rfloor + n$$

(2) Se $x = m + \alpha$, então $\lfloor x \rfloor = m$, onde m é inteiro e $0 \leq \alpha < 1$, assim

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1 \Rightarrow$$

$$m \leq m + \alpha < m + 1$$

Obviamente, $\lfloor x \rfloor = x$, quando $\alpha = 0$. Assim, reescrevendo a desigualdade, temos

$$x < \lfloor x \rfloor + 1 \Rightarrow$$

$$x - 1 < \lfloor x \rfloor \leq x \Rightarrow$$

$$\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$$

Finalmente, subtraindo $\lfloor x \rfloor$ na última desigualdade, vamos obter

$$0 \leq x - \lfloor x \rfloor < 1$$

(3) Seja $x = n + \alpha$, onde n é inteiro e $0 < \alpha < 1$, daí segue que

$$-x = -n - \alpha = -n - 1 + 1 - \alpha \Rightarrow$$

$$\lfloor -x \rfloor = -n + \lfloor -1 + 1 - \alpha \rfloor$$

Por (1), temos

$$\lfloor -x \rfloor = -n - 1 + \lfloor 1 - \alpha \rfloor$$

Assim,

$$0 < 1 - \alpha < 1 \Rightarrow \lfloor 1 - \alpha \rfloor = 0,$$

Logo,

$$\lfloor -x \rfloor = -n - 1 = -\lfloor x \rfloor - 1, \qquad se\ x \notin \mathbb{Z}$$

(4) Sejam $x = n + \alpha\ e\ y = m + \beta$ onde $m\ e\ n$ são inteiros e $\alpha, \beta \in [0,1)$. Logo,

$$\begin{aligned} \lfloor x \rfloor + \lfloor y \rfloor &= n + m \\ &= \lfloor n + m \rfloor \\ &\leq \lfloor n + \alpha + m + \beta \rfloor \\ &= \lfloor x + y \rfloor \\ &= n + m + \lfloor \alpha + \beta \rfloor \\ &\leq n + m + 1 \\ &= \lfloor x \rfloor + \lfloor y \rfloor + 1 \end{aligned}$$

(5) Seja $x = n + \alpha$, então temos $-x = -n - 1 + 1 - \alpha$. Logo,

$$\lfloor x \rfloor + \lfloor -x \rfloor = n + \lfloor -n - 1 + 1 - \alpha \rfloor$$

Por (1), temos

$$\lfloor x \rfloor + \lfloor -x \rfloor = n - n - 1 + \lfloor 1 - \alpha \rfloor$$

De onde concluímos que,

$$\lfloor x \rfloor + \lfloor -x \rfloor = \begin{cases} 0\ se\ \alpha = 0 \\ -1\ se\ 0 < \alpha < 1 \end{cases}$$

(6) Seja $x = n + \alpha, com\ 0 < \alpha < 1$. Sabemos, pelo algoritmo da divisão, que existem q e r inteiros tais que $n = qm + r, onde\ 0 \leq r \leq m - 1$. Portanto,

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

Pois $0 \leq r + \alpha < m$, visto que $0 \leq \alpha < 1$ e $0 \leq r \leq m - 1$. Porém,

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

(7) Se $x = n + \alpha, com\ 0 \leq \alpha < 1$, então $\lfloor x \rfloor = n$.

Se $0 \leq \alpha < \frac{1}{2}$, então $2\alpha < 1$ e $\lfloor 2x \rfloor = \lfloor 2n + 2\alpha \rfloor = 2n$ que é par, logo

$$\lfloor 2x \rfloor - 2\lfloor x \rfloor = 2n - 2n = 0.$$

Se $\frac{1}{2} \leq \alpha < 1 \Rightarrow 1 \leq 2\alpha < 2$ e $\lfloor 2x \rfloor = \lfloor 2n + 2\alpha \rfloor = 2n + 1$ que é ímpar, logo

$$\lfloor 2x \rfloor - 2\lfloor x \rfloor = 2n + 1 - 2n = 1.$$

(8) Dados os inteiros $n\ e\ a$, pelo algoritmo da divisão, existem $q\ e\ r$ inteiros, tais que $n = aq + r$, onde $0 \leq r < a$, daí temos

$$\frac{n}{a} = q + \frac{r}{a} \Rightarrow$$

$$\left\lfloor \frac{n}{a} \right\rfloor = \left\lfloor q + \frac{r}{a} \right\rfloor = q, \text{ pois } 0 \leq \frac{r}{a} < 1$$

Portanto,

$$\left\lfloor \frac{n}{a} \right\rfloor a + r = aq + r = n, onde\ 0 \leq r < a$$

Agora que conhecemos a função $\lfloor x \rfloor$, temos uma nova maneira de escrever o teorema **3.4** como vem a seguir:

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

Teorema 3.6: Seja n um número natural e p um primo. Então o expoente da maior potência de p que divide $n!$ é dado por:

$$N = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Demonstração:

Importante notar que a série acima não é infinita, pois, $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$ para todo k natural, tal que $p^k > n$.

Seja h_1 o número de termos na sequência $1, 2, 3, \ldots, n$ que são divisíveis por p, isto é, o número de múltiplos de p entre 1 e n é dado por $h_1 = \left\lfloor \frac{n}{p} \right\rfloor$. Cada um destes múltiplos vai contribuir com um fator p a mais se forem divisíveis por p^2, logo, $h_2 = \left\lfloor \frac{n}{p^2} \right\rfloor$, e assim por diante. Se os múltiplos de p tiverem no máximo α fatores iguais a p, então, o número de múltiplos de p^α é dado por $h_\alpha = \left\lfloor \frac{n}{p^\alpha} \right\rfloor$

Portanto, o expoente da maior potência de p que divide $n!$ é dado pela soma

$$N = h_1 + h_2 + \cdots + h_\alpha$$

Podemos ainda definir uma fórmula de recorrência usando o teorema **3.5**, daí temos

$$h_{\alpha+1} = \left\lfloor \frac{h_\alpha}{p} \right\rfloor$$

Isto nos permite determinar os números h_α dividindo, sucessivamente por p e não por potências de p.

Exemplo 3.6: Determine a maior potência de 2 que divide $30!$.

Solução:

Se $n = 30\ e\ p = 2$, temos

$$\left\lfloor \frac{30}{2} \right\rfloor = 15; \left\lfloor \frac{15}{2} \right\rfloor = 7; \left\lfloor \frac{7}{2} \right\rfloor = 3; \left\lfloor \frac{3}{2} \right\rfloor = 1$$

Logo,

$$N = 15 + 7 + 3 + 1 = 26$$

Ou seja, a maior potência de 2 que divide $30!$ é igual a 2^{26}.

Exemplo 3.7: Determine com quantos zeros termina $2000!$.

Solução:

O problema equivale a contar os fatores $2\ e\ 5$ de $2000!$, ou seja, devemos determinar a maior potência de 10 que divide $2000!$, por outro lado, há mais fatores 2 do que 5 em $2000!$, logo, é suficiente determinarmos a maior potência de 5 que divide $2000!$.

Note que $5^4 < 2000$, porém, $5^5 > 2000$, portanto

$$N = \left\lfloor \frac{2000}{5} \right\rfloor + \left\lfloor \frac{2000}{5^2} \right\rfloor + \left\lfloor \frac{2000}{5^3} \right\rfloor + \left\lfloor \frac{2000}{5^4} \right\rfloor =$$

$$= 400 + 80 + 16 + 3 = 499$$

Portanto, $2000!$ termina em 499 zeros.

Teorema 3.7: Se $n_1, n_2, \dots, n_r$ são números naturais tais que

$$n = n_1 + n_2 + \cdots + n_r$$

então o quociente

$$\frac{n!}{n_1!\, n_2! \dots n_r!} = \binom{n}{n_1, n_2, \dots, n_r}$$

é um inteiro.

Demonstração:

Seja m um número natural. Da relação

$$\frac{n}{m} = \frac{n_1}{m} + \frac{n_2}{m} + \cdots + \frac{n_r}{m}$$

obtemos, pelo teorema **3.5 (4),** a seguinte desigualdade

$$\left\lfloor \frac{n}{m} \right\rfloor \geq \left\lfloor \frac{n_1}{m} \right\rfloor + \left\lfloor \frac{n_2}{m} \right\rfloor + \cdots + \left\lfloor \frac{n_r}{m} \right\rfloor$$

Seja p um fator primo de $n!$ e, substituindo $m,$ na desigualdade anterior, sucessivamente por $p, p^2, p^3, \ldots$

Adicionando as desigualdades obtidas dessa forma, temos

$$\sum_{i \geq 1} \left\lfloor \frac{n}{p^i} \right\rfloor \geq \sum_{i \geq 1} \left\lfloor \frac{n_1}{p^i} \right\rfloor + \sum_{i \geq 1} \left\lfloor \frac{n_2}{p^i} \right\rfloor + \cdots + \sum_{i \geq 1} \left\lfloor \frac{n_r}{p^i} \right\rfloor$$

Pelo teorema **3.6** a soma do lado esquerdo da desigualdade nos dá o maior expoente de p que divide $n!$, pelo mesmo motivo, a j-ésima soma do lado direito é o expoente da maior potência de p que divide $n_j!$.

Pela última desigualdade, concluímos que a maior potência de p que divide o produto $n_1! \, n_2! \ldots n_r!$ também divide $n!$. Portanto,

$$\frac{n!}{n_1! \, n_2! \ldots n_r!}$$

é inteiro.

3.5 Fórmula de inversão de Mobius

Teorema 3.8: Sejam $f \; e \; g$ duas funções aritméticas relacionadas pela igualdade:

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

Então

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

Demonstração:

Para cada d que divide n existe um único inteiro positivo d' tal que $n = dd'$. Como n tem uma quantidade finita de divisores, então $d' = n/d$ percorre os mesmos divisores de d a medida que varia os valores de d, logo, se $c|d'$ então $c|{}^{n}/_{d}$. Daí, segue que

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

$$\sum_{d|n} \mu(d) \sum_{c|{}^{n}/_{d}} g(c) =$$

$$\sum_{d|n} \sum_{c|{}^{n}/_{d}} \mu(d) g(c) =$$

A última soma dupla é sobre todos os pares de inteiros positivos (c, d) tais que $d|n$ e $c|{}^{n}/_{d}$ se e somente se $c|n$ e $d|{}^{n}/_{d}$, daí segue que

$$\sum_{d|n} \sum_{c|{}^{n}/_{d}} \mu(d) g(c) =$$

$$\sum_{c|n} \sum_{d|{}^{n}/_{c}} \mu(d) g(c) =$$

$$\sum_{c|n} g(c) \sum_{d|{}^{n}/_{c}} \mu(d)$$

Pelo teorema **3.4,** temos que a soma

$$\sum_{d|{}^{n}/_{c}} \mu(d)$$

resultará em 0, se ${}^{n}/_{c} > 1$, por outro lado, resultará em 1 se ${}^{n}/_{c} = 1\ ou\ n = c$. Com isso, vamos obter

$$\sum_{d|n} \mu(d) f\left(\frac{n}{d}\right) = \sum_{c=n} g(c).1 = g(n)$$

Assim, por exemplo, no caso das funções aritméticas $\tau(n)\ e\ \sigma(n)$ temos, por definição:

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

E, portanto, pela fórmula de inversão de Mobius

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

Vale também que

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

As relações são válidas para todo $n \geq 1$.

Exemplo 3.8: Verificar a fórmula da inversão de Mobius para o caso $n = 10$

Solução:

$$\sum_{d|10} \sum_{c|{}^{10}/_{d}} \mu(d)f(c) =$$

$$\mu(1)[f(1) + f(2) + f(5) + f(10)] +$$

$$\mu(2)[f(1) + f(2) + f(5)] +$$

$$\mu(5)[f(1) + f(2)] + \mu(10)\, f(1) =$$

$$f(1)[\mu(1) + \mu(2) + \mu(5) + \mu(10)] +$$

$$f(2)[\mu(1) + \mu(2) + \mu(5)] +$$

$$f(5)[\mu(1) + \mu(2)] + f(10)\mu(1) =$$

$$\sum_{c|10} \sum_{d|{}^{10}/_{c}} \mu(c)f(d)$$

3.6 Os Teoremas de Fermat e Wilson

Definição 3.5: O conjunto dos inteiros $\{r_1, r_2, \dots, r_m\}$ é um sistema completo de resíduos módulo m se

(1) $r_i \not\equiv r_j (mod\ m)\ para\ i \neq j$

(2) Para todo inteiro n existe um r_i tal que $n \equiv r_i (mod\ m)$.

Por exemplo, $\{0, 1, 2, \dots, m-1\}$ é um sistema completo de resíduos módulo m. Ou seja, um conjunto que forma um sistema completo de resíduos módulo m tem exatamente m elementos, pois, para todo inteiro $a \neq 0$, existem m restos possíveis quando a é dividido por m. Por exemplo

$$S = \{0, 1, 2, 3, 4, 5\}$$

é um sistema completo de resíduos módulo 6, mas também podemos formar um sistema completo de resíduos módulo 6 com outros elementos. Por exemplo

$$S' = \{-42, -37, 13, 22, 38, 57\}$$

também é um sistema completo de resíduos módulo 6, pois

$$-42 \equiv 0(mod\ 6), \quad -37 \equiv 5(mod\ 6), \quad 13 \equiv 1(mod\ 6)$$
$$22 \equiv 4(mod\ 6), \quad 38 \equiv 2(mod\ 6), \quad 57 \equiv 3(mod\ 6)$$

De modo geral, se $S = \{r_1, r_2, \dots, r_m\}$ é um sistema completo de resíduos módulo m, então os elementos de S são congruentes módulo m aos inteiros $0, 1, 2, \dots, m-1$, numa certa ordem.

Teorema 3.9: (Teorema de Wilson): Se p é primo, então $(p-1)! \equiv -1(mod\ p)$

Demonstração:

O teorema é válido para $p = 2\ e\ p = 3$, pois,

$$(2-1)! = 1 \equiv -1(mod\ 2)$$
$$(3-1)! = 2 \equiv -1(mod\ 3)$$

Suponhamos, pois, que $p \geq 5$.

Considere o conjunto $S = \{1, 2, \dots, p-1\}$ um sistema completo de resíduos módulo p. Dentre todos os elementos de S, apenas $1\ e\ p-1$ são seus próprios inversos módulo p. O restante dos elementos em $S' = \{2, 3, \dots, p-2\}$, podem ser agrupados em pares cujo produto é congruente a 1 módulo p. Isso se deve ao fato de que eles possuem inverso módulo p, diferente de si mesmo e que pertencem a S', isto é, para todo $a \in S'$, existe um único $b \in S'$ com $a \neq b$, tal que $ab \equiv 1(mod\ p)$. Se multiplicarmos ordenadamente todos estes pares de inteiros sem repetição, vamos obter

$$2.3. \dots (p-2) \equiv 1(mod\ p).$$

Finalmente, multiplicando a última congruência por $p-1$, obteremos

$$2.3 \dots . (p-2)(p-1) \equiv -1(mod\ p)$$

Isto é,

$$(p-1)! \equiv -1(mod\ p).$$

Teorema 3.10 (Recíproca do Teorema de Wilson): Se $(n-1)! \equiv -1(mod\ n)$, então n é primo.

Demonstração:

Suponhamos que $(n-1)! \equiv -1(mod\ n)$, isto é, $n|[(n-1)!+1]$ e que n não seja primo, ou seja, $n = rs$ onde $1 < r < n\ e\ 1 < s < n$. Nestas condições, $r|(n-1)!$ e como $r|n$, isto implica que $r|[(n-1)!+1]$, e portanto, r divide a diferença, isto é, $r|[(n-1)!+1-(n-1)!] = 1$, mas isso é um absurdo, pois $r > 1$. Logo, se n satisfaz a congruência $(n-1)! \equiv -1(mod\ n)$, então n deve ser primo.

Exemplo 3.9: Verifique o teorema de Wilson para o caso onde $p = 11$.

Solução:

Para $p = 11$, temos os inteiros $2, 3, \ldots, 9$ que formam 4 pares cujo produto de cada par é congruente a 1 módulo 11, ou seja

$$2.6 \equiv 1(mod 11)$$

$$3.4 \equiv 1(mod\ 11)$$

$$5.9 \equiv 1(mod\ 11)$$

$$7.8 \equiv 1(mod\ 11)$$

Multiplicando ordenadamente as 4 congruências, temos

$$(2.6)(3.4)(5.9)(7.8) \equiv 9! \equiv 1(mod\ 11)$$

Por outro lado,

$$10 \equiv -1(mod\ 11)$$

Multiplicando esta última congruência com a anterior, obtemos

$$9!.10 = 10! \equiv -1(mod\ 11).$$

O teorema pode ser usado diretamente, mas com isso ilustramos que a ideia da demonstração também resolve qualquer problema particular no qual o teorema de Wilson pode ser aplicado.

Teorema 3.11 (Pequeno Teorema de Fermat): Seja p um primo. Se $p \nmid a$ então

$$a^{p-1} \equiv 1(mod\ p).$$

Demonstração:

Consideremos os $p-1$ primeiros múltiplos positivos de a, isto é,

$$a, 2a, 3a, \dots, (p-1)a$$

Nenhum desses $p-1$ inteiros é divisível por p e, além disso, dois quaisquer deles são incongruentes módulo p, caso contrário, teríamos

$$ra \equiv sa(mod\ p), \quad 1 \leq r < s \leq p-1$$

Então, o fator comum a poderia ser cancelado, visto que $mdc(a,p) = 1$, logo

$$r \equiv s\ (mod\ p) \Rightarrow p|(r-s)$$

o que é impossível, pois $0 < r - s < p$.

Dessa maneira, os $p-1$ inteiros $a, 2a, 3a, \dots, (p-1)a$ divididos por p deixam restos distintos dois a dois, além disso, cada um desses $p-1$ inteiros é congruente módulo p a um único dos inteiros $1, 2, 3, \dots., p-1$, numa certa ordem. Portanto, multiplicando ordenadamente todas as $p-1$ congruências, obtemos

$$a.2a.3a \dots (p-1)a \equiv 1.2.3 \dots (p-1)\ (mod\ p)$$

Isto é,

$$a^{p-1}(p-1)! \equiv (p-1)!\ (mod\ p)$$

Como o $mdc(p,(p-1)!) = 1$, pois p é primo e $p \nmid (p-1)!$, podemos cancelar o fator comum $(p-1)!$, o que resulta em

$$a^{p-1} \equiv 1(mod\ p)$$

Corolário 3.1: Se p é um primo e a é um inteiro positivo, então $a^p \equiv a(mod\ p)$.

Demonstração:

Temos que analisar dois casos: $p|a\ ou\ p \nmid a$.

Se $p|a$, então $p|a(a^{p-1}-1)$ e, portanto $a^p \equiv a(mod\ p)$.

Se $p \nmid a$, pelo teorema **3.11**, $p|(a^{p-1}-1)$ e, portanto, $p|(a^p - a)$. Logo, em qualquer caso, temos $a^p \equiv a(mod\ p)$.

Exemplo 3.10: Mostrar que, se o $mdc(p,q) = 1$ tais que

$$a^p \equiv a(mod\ q)\ e\ a^q \equiv a(mod\ p)$$

então

$$a^{pq} \equiv a(mod\ pq).$$

Solução:

Pelo corolário **3.1** e fazendo uso da hipótese, temos

$$(a^q)^p \equiv a^q \equiv a(mod\ p)$$

$$(a^p)^q \equiv a^p \equiv a(mod\ q)$$

portanto,

$$p|(a^{pq} - a)\ e\ q|(a^{pq} - a)$$

o que implica

$$pq|(a^{pq} - a)$$

isto é,

$$a^{pq} \equiv a(mod\ pq)$$

4. Função e Teorema de Euler

O quarto capítulo é voltado para o estudo da função e teorema de Euler, sendo que a função de Euler será provada como uma função aritmética multiplicativa e também veremos que o teorema de Euler é uma generalização do pequeno teorema de Fermat. Ainda sobre a função de Euler, vamos caracterizar a função de modo a obter uma fórmula fechada que represente algebricamente a função.

Também será provado várias propriedades relacionadas à função $\boldsymbol{\varphi}$ de Euler, sendo que o principal resultado a respeito disso, é o teorema de Gauss que é ferramenta necessária para o último resultado que relaciona a função $\boldsymbol{\varphi}$ (de Euler) e $\boldsymbol{\mu}$ (de Mobius).

4.1 Função de Euler

Definição 4.1: Chama-se função de Euler a função aritmética φ assim definida para todo inteiro positivo n:

$\varphi(n)$ é o número de inteiros positivos que são primos com n e que não são superiores a n, isto é, que são primos com n e menores ou iguais a n. Em símbolos, podemos denotar:

$$\varphi(n) = \#\{x \in \mathbb{N} | 1 \leq x \leq n \; e \; mdc(x,n) = 1\}$$

Em particular, definimos $\varphi(1) = 1$, pois o $mdc(1,1) = 1$, e para $n > 1$, temos que o $mdc(n,n) = n \neq 1$, de modo que $\varphi(n) \leq n$, onde a igualdade ocorre, se e somente se $n = 1$.

Exemplo 4.1: Encontre os números inteiros positivos que são menores que 18 e são primos com 18.

Solução:

Se $n = 18$, então os inteiros positivos menores que 18 e primos com 18 são $1, 5, 7, 11, 13, 17$, de modo que $\varphi(18) = 6$.

Exemplo 4.2: Calcular: $\tau(\varphi(12))\ e\ \varphi(\tau(12))$

Solução:

Assim,

$$\tau(\varphi(12)) = \tau(4) = 3$$
$$\varphi(\tau(12)) = \varphi(6) = 2$$

A tabela abaixo fornece os valores de $\varphi(n)$ para os dez primeiros inteiros positivos:

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

Até agora vimos que é trabalhoso calcular os valores da função φ, por isso precisamos de uma caracterização para esta função, de modo a calcular o valor de $\varphi(n)$ para qualquer n inteiro positivo. O primeiro passo para isso, é provar que $\varphi(n)$ é uma função aritmética multiplicativa.

Teorema 4.1: A função φ de Euler é uma função aritmética multiplicativa.

Demonstração:

Sejam $r\ e\ s$ dois inteiros positivos tais que o $mdc(r,s) = 1$. Devemos demonstrar que $\varphi(rs) = \varphi(r)\varphi(s)$.

O teorema é válido para $r = 1\ ou\ s = 1$. De fato,

$$\varphi(1.s) = \varphi(s) = 1.\varphi(s) = \varphi(1)\varphi(s)$$
$$\varphi(1.r) = \varphi(r) = 1.\varphi(r) = \varphi(1)\varphi(r)$$

Suponhamos então que $r > 1\ e\ s > 1$. Neste caso os inteiros de $1\ a\ rs$ podem ser dispostos em r colunas e s inteiros em cada uma delas, de modo que:

$$\begin{array}{cccccc} 1 & 2 & & k & & r \\ r+1 & r+2 & & r+k & & 2r \\ 2r+1 & 2r+2 & \ldots & 2r+k & \ldots & 3r \\ \vdots & \vdots & & \vdots & & \vdots \\ (s-1)r+1 & (s-1)r+2 & & (s-1)r+k & & sr \end{array}$$

Como o $mdc(qr+k,r) = mdc(k,r)$, os inteiros da $k-ésima$ coluna são primos com r se, e somente se, k é primo com r. E como na primeira linha o número de inteiros que são primos com r é igual a $\varphi(r)$, segue-se que existem somente $\varphi(r)$ colunas formadas com inteiros que são todos primos com r. Por outro lado, em cada uma destas $\varphi(r)$ colunas existem precisamente $\varphi(s)$ inteiros que são primos com s, pois na progressão aritmética

$$k, r+k, 2r+k, \dots, (s-1)r+k$$

onde o $mdc(k,r) = 1$, o número de termos que são primos com s é igual a $\varphi(s)$. Assim sendo, o número total de inteiros que são primos com $r\ e\ s$, isto é, que são primos com rs, é igual a $\varphi(s)\varphi(r)$, isto quer dizer que

$$\varphi(rs) = \varphi(r)\varphi(s).$$

4.2 Teorema de Euler

Definição 4.2: Um sistema reduzido de resíduos módulo m é todo conjunto $S = \{r_1, r_2, \dots, r_{\varphi(m)}\}$ de $\varphi(m)$ inteiros que verificam as duas seguintes condições:

$$(1)\ mdc(r_i, m) = 1,\ \forall r_i \in S$$

$$(2)\ r_i \not\equiv r_j (mod\ m),\ i \neq j$$

Assim, por exemplo, o conjunto $\{0,1,2,3,4,5,6,7\}$ é um sistema completo de resíduos módulo 8, portanto $\{1,3,5,7\}$ é um sistema reduzido de resíduos módulo 8. Sendo assim, dado um sistema completo de resíduos módulo m, para obtermos o sistema reduzido de resíduos módulo m, basta retirarmos os elementos que não são primos com m.

Lema 4.1: Sejam a e $n > 1$ inteiros tais que o $mdc(a,n) = 1$. Se

$$a_1, a_2, \dots, a_{\varphi(n)}$$

são os inteiros positivos menores do que n e que são primos com n, então cada um dos inteiros

$$aa_1, aa_2, \dots, aa_{\varphi(n)}$$

é congruente módulo n a um dos inteiros

$$a_1, a_2, \dots, a_{\varphi(n)}$$

não necessariamente nessa ordem.

Demonstração:

Dois quaisquer dos inteiros $aa_1, aa_2, \dots, aa_{\varphi(n)}$ são incongruentes módulo n, caso contrário, teríamos

$$aa_i \equiv aa_j (mod\ n), \text{ com } 1 \leq i < j \leq \varphi(n)$$

se cancelarmos o fator comum da congruência, vamos obter

$$a_i \equiv a_j (mod\ n)$$

o que é uma contradição. Por outro lado, como o

$$mdc(a_i, n) = 1 \left(i = 1, 2, \dots, \varphi(n)\right) e\ o\ mdc(a, n) = 1$$

Segue que o $mdc(aa_i, n) = 1$. Desse modo, para cada aa_i existe um único inteiro b_i, com $0 \leq b_i < n$, tal que $aa_i \equiv b_i (mod\ n)$. Além disso, por termos

$$mdc(b_i, n) = mdc(aa_i, n) = 1$$

então b_i é um dos inteiros $a_1, a_2, \dots, a_{\varphi(n)}$, isto é, os inteiros

$$aa_1, aa_2, \dots, aa_{\varphi(n)}\ e\ a_1, a_2, \dots, a_{\varphi(n)}$$

são idênticos módulo n numa certa ordem.

Teorema 4.2 (Teorema de Euler)**:** Se n é um inteiro positivo e a um inteiro tal que o $mdc(a, n) = 1$, então

$$a^{\varphi(n)} \equiv 1 (mod\ n).$$

Demonstração:

O Teorema é válido para $n = 1$, pois

$$a^{\varphi(1)} = a \equiv 1 (mod\ 1)$$

Suponhamos então que $n > 1$. Sejam $a_1, a_2, \dots, a_{\varphi(n)}$ os inteiros positivos menores do que n e que são primos com n. Como o $mdc(a, n) = 1$, pelo lema anterior **(4.1)**, os inteiros

$$aa_1, aa_2, \dots, aa_{\varphi(n)}$$

são congruentes módulo n, não necessariamente nesta ordem, aos inteiros

$$a_1, a_2, \dots, a_{\varphi(n)}$$

isto é,

$$aa_1 \equiv a_1' (mod\ n)$$
$$aa_2 \equiv a_2' (mod\ n)$$
$$\vdots$$
$$aa_{\varphi(n)} \equiv a'_{\varphi(n)} (mod\ n)$$

onde $a_1', a_2', \dots, a'_{\varphi(n)}$ são precisamente os inteiros

$$a_1, a_2, \dots, a_{\varphi(n)}$$

numa certa ordem.

Multiplicando ordenadamente essas $\varphi(n)$ congruências, obtemos

$$(aa_1)(aa_2) \dots \left(aa_{\varphi(n)}\right) \equiv a'_1 a'_2 \dots a'_{\varphi(n)} \ (mod\ n)$$

$$\equiv a_1 a_2 \dots a_{\varphi(n)} \ (mod\ n)$$

ou seja,

$$a^{\varphi(n)}\left(a_1 a_2 \dots a_{\varphi(n)}\right) \equiv (a_1 a_2 \dots a_{\varphi(n)})(mod\ n)$$

Como o $mdc(a_i, n) = 1, com\ 1 \leq i \leq \varphi(n)$, então

$$mdc\left(a_1 a_2 \dots a_{\varphi(n)}, n\right) = 1$$

Assim, podemos cancelar o fator comum

$$a_1 a_2 \dots a_{\varphi(n),}$$

o que resulta em

$$a^{\varphi(n)} \equiv 1(mod\ n)$$

Fazendo $n = p$, sendo p primo, então $\varphi(p) = p - 1$, visto que o $mdc(a, p) = 1$, logo

$$a^{p-1} \equiv 1(mod\ p)$$

Ou seja, recaímos no Teorema de Fermat. Com isso, concluímos que o Teorema de Euler é uma generalização do Teorema de Fermat.

Exemplo 4.3: Usando o teorema de Euler, resolver a congruência linear

$$ax \equiv b(mod\ m), onde\ o\ mdc(a, m) = 1$$

Solução:

Pelo teorema de Euler, temos

$$a^{\varphi(m)} \equiv 1(mod\ m) \Rightarrow a^{\varphi(m)} b \equiv b(mod\ m)$$

Portanto,

$$ax \equiv a^{\varphi(m)} b(mod\ m)$$

Como o $mdc(a, m) = 1$, podemos cancelar o fator comum a, o que nos dá

$$x \equiv a^{\varphi(m)-1} b(mod\ m)$$

Assim, por exemplo, usando o teorema de Euler para resolver a congruência linear $5x \equiv 7(mod\ 12)$, onde o $mdc(5, 12) = 1$, daí obtemos:

$$x \equiv 5^{\varphi(12)-1}.7 \equiv 5^{4-1}.7 \equiv 875(mod\ 12)$$

O que implica que,

$$x \equiv 875 \equiv -1 \equiv 11(mod\ 12)$$

4.3 Cálculo de $\varphi(n)$

Teorema 4.3: Seja n um inteiro, tal que $n > 1$, então $\varphi(n) = n - 1$ se e somente se n é primo.

Demonstração:

($\Longrightarrow$) Se $n > 1$ é primo, então é imediato que cada inteiro positivo menor que n é primo com n, logo

$$\varphi(n) = n - 1$$

($\Longleftarrow$) Reciprocamente, se $\varphi(n) = n - 1, com\ n > 1$, então n é primo, pois, se n fosse composto, então $n = rs\ onde\ 1 < r \leq s < n$, sendo que $r|n\ e\ s|n$. Desse modo, teríamos pelo menos dois dos inteiros $1, 2, \dots, n$ que não seriam primos com n, isto é,

$$\varphi(n) < n - 2$$

Portanto, n é primo.

Teorema 4.4: Se p é primo e se k é um inteiro positivo, então:

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

Demonstração:

O $mdc(n, p^k) = 1$ se e somente se p não divide n, e como existem p^{k-1} inteiros entre $1\ e\ p^k$ que são divisíveis por p, tais múltiplos de p são precisamente

$$p, 2p, 3p, \dots, (p^{k-1})p$$

Segue que o conjunto $\{1, 2, 3, \dots., p^k\}$ contém exatamente $p^k - p^{k-1}$ inteiros que são primos com p^k, de modo que pela definição da função φ de Euler, temos

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

Tome, por exemplo:

$$\varphi(27) = \varphi(3^3) = 3^3 - 3^2 = 27 - 9 = 18$$

Teorema 4.5: Se $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$ é a decomposição canônica do inteiro positivo $n > 1$, então:

$$\varphi(n) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

Pelo teorema **4.4,** temos

$$\varphi\left(p_i^{\alpha_i}\right) = p_i^{\alpha} - p_i^{\alpha-1} = p_i^{\alpha_i}\left(1 - \frac{1}{p_i}\right)$$

Usando sucessivamente o teorema **4.4** juntamente com o fato da função φ ser multiplicativa, iremos obter

$$\varphi(n) = \varphi\left(p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}\right) = \varphi\left(p_1^{\alpha_1}\right)\varphi\left(p_2^{\alpha_2}\right) \dots \varphi\left(p_r^{\alpha_r}\right) =$$

$$= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) p_2^{\alpha_2}\left(1 - \frac{1}{p_2}\right) \dots p_r^{\alpha_r}\left(1 - \frac{1}{p_r}\right) =$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_r}\right) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

.

Exemplo 4.4: Achar os dois últimos algarismos da direita do inteiro 3^{3333}.

Solução:

O problema equivale a encontrar o menor inteiro positivo n tal que

$$3^{3333} \equiv n (mod\ 100)$$

onde n é o número que corresponde aos dois últimos algarismos de 3^{3333}.

Como o $mdc(3{,}100) = 1$, então vale o teorema de Euler:

$$3^{\varphi(100)} \equiv 1 (mod\ 100) \Rightarrow 3^{40} \equiv 1 (mod\ 100)$$

Pelo algoritmo da divisão, temos:

$$3333 = 40.83 + 13$$

Logo,

$$3^{3333} = (3^{40})^{83}.3^{13} \equiv 3^{13} (mod\ 100)$$

Basta agora calcular o resto da potência 3^{13} quando dividido por 100, então

$$3^{13} = (3^6)^2.3 = (729)^2.3 \equiv 29^2.3 \equiv 41.3 \equiv 123 \equiv 23 (mod\ 100)$$

Ou seja,

$$3^{3333} \equiv 23 (mod\ 100)$$

Portanto, os dois últimos algarismos da direita do número 3^{3333} é 23.

4.4 Propriedades da Função de Euler

Teorema 4.6: Para todo inteiro positivo $n > 2$, $\varphi(n)$ é um inteiro par.

Demonstração:

Se n é uma potência de 2, isto é, $n = 2^k, com\ k \geq 2$, então, pelo teorema **4.4:**

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

que é um inteiro par.

Suponha então que n é divisível por um primo ímpar, ou seja,

$$n = p^k m, onde\ k \geq 1\ e\ o\ mdc(p^k, m) = 1$$

E, como $\varphi(n)$ é uma função aritmética multiplicativa, temos

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

que de fato, é um inteiro par, pois $2|(p-1)$

Portanto, $\varphi(n)$ é um inteiro ímpar somente para $n = 1\ ou\ n = 2$, isto é,

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

Teorema 4.7: Se p é primo, então

$$\sum_{i=0}^{k} \varphi(p^i) = p^k$$

Demonstração:

Pelo teorema **4.5,** temos

$$\varphi(p) = p - 1$$
$$\varphi(p^2) = p^2 - p = p(p-1)$$
$$\varphi(p^3) = p^3 - p^2 = p^2(p-1)$$
$$\vdots$$
$$\varphi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$$

Somando ordenadamente todas as igualdades, temos

$$\sum_{i=1}^{k} \varphi(p^i) = (p-1)\sum_{i=0}^{k-1} p^i$$

Ou seja,

$$\sum_{i=1}^{k} \varphi(p^i) = (p-1) \cdot \frac{p^k - 1}{p-1} = p^k - 1$$

Portanto,

$$\sum_{i=0}^{k} \varphi(p^i) = \varphi(1) + p^k - 1 = 1 + p^k - 1 = p^k$$

A seguir vamos definir o que são os subconjuntos S_d do conjunto $\{1, 2, \dots, n\}$, que serão usados no próximo teorema.

Definição 4.3: Seja o conjunto $A = \{1, 2, \dots, n\}$ e seja d algum divisor positivo de n, dizemos que um subconjunto de A é uma classe S_d quando

$$S_d = \{m; 1 \leq m \leq n \; e \; mdc(m, n) = d\}$$

De modo que cada classe S_d onde $d|n$, são disjuntas duas a duas e a união destas classes é o próprio conjunto A, isto é,

$$\bigcup_{d|n} S_d = A$$

Teorema 4.8 (de Gauss)**:** Para todo inteiro positivo $n \geq 1$, vale que

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

Demonstração:

Os inteiros $1, 2, 3, \dots, n$ podem ser separados em classes mediante o seguinte critério: se d é um divisor positivo de n, então o inteiro m $(1 \leq m \leq n)$ é incluído na classe S_d uma vez que o $mdc(m, n) = d$, isto é,

$$S_d = \{m; 1 \leq m \leq n \; e \; mdc(m, n) = d\}$$

Como o $mdc(m, n) = d$ se, e somente se, o $mdc\left({}^{m}/_{d}, {}^{n}/_{d}\right) = 1$, segue que o número de inteiros da classe S_d é igual ao número de inteiros positivos que não superam ${}^{n}/_{d}$ e que são primos com ${}^{n}/_{d}$, isto é, o número de inteiros da classe S_d é igual a $\varphi\left({}^{n}/_{d}\right)$. E como cada um dos n inteiros $1, 2, 3, \dots, n$ pertence precisamente a uma única classe S_d, temos

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

Mas, quando d percorre todos os divisores positivos de n, o mesmo ocorre com n/d e, portanto

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

Obs: O teorema de Gauss é uma generalização do teorema **4.7**.

Exemplo 4.5: Verificar o teorema **4.8** (de Gauss) para $n = 20$.

Solução:

Os divisores de 20 são $1, 2, 4, 5, 10\ e\ 20$, portanto, as classes S_d são:

$$S_1 = \{m; 1 \leq m \leq 20\ e\ mdc(m, 20) = 1\} = \{1, 3, 7, 9, 11, 13, 17, 19\}$$
$$S_2 = \{m; 1 \leq m \leq 20\ e\ mdc(m, 20) = 2\} = \{2, 6, 14, 18\}$$
$$S_4 = \{m; 1 \leq m \leq 20\ e\ mdc(m, 20) = 4\} = \{4, 8, 12, 16\}$$
$$S_5 = \{m; 1 \leq m \leq 20\ e\ mdc(m, 20) = 5\} = \{5, 15\}$$
$$S_{10} = \{m; 1 \leq m \leq 20\ e\ mdc(m, 20) = 10\} = \{10\}$$
$$S_{20} = \{m; 1 \leq m \leq 20\ e\ mdc(m, 20) = 20\} = \{20\}$$

Estas classes contêm

$$\varphi(20) = 8, \qquad \varphi(10) = 4, \qquad \varphi(5) = 4,$$
$$\varphi(4) = 2, \qquad \varphi(2) = 1, \qquad \varphi(1) = 1$$

inteiros, respectivamente, portanto

$$\sum_{d|20} \varphi(d) = \varphi(20) + \varphi(10) + \varphi(5) + \varphi(4) + \varphi(2) + \varphi(1) =$$

$$= 8 + 4 + 4 + 2 + 1 + 1 = 20$$

Teorema 4.9: Para todo inteiro positivo $n > 1$, a soma dos inteiros positivos menores que n e que são primos com n é igual a

$$\frac{1}{2} n.\varphi(n)$$

Demonstração:

Sejam

$$a_1, a_2, \ldots, a_{\varphi(n)}$$

os inteiros positivos menores que n e que são primos com n. Como o $mdc(a_i, n) = 1$ se e somente se o $mdc(n - a_i, n) = 1\ \big(i = 1, 2, \ldots, \varphi(n)\big)$, os inteiros positivos menores do que n e que são primos com n podem ser expressos pelas diferenças:

$$n - a_1, n - a_2, \dots, n - a_{\varphi(n)}$$

Portanto,

$$a_1 + a_2 + \cdots + a_{\varphi(n)} = (n - a_1) + (n - a_2) + \cdots + n - a_{\varphi(n)}) =$$
$$= n.\varphi(n) - (a_1 + a_2 + \cdots + a_{\varphi(n)})$$

Daí, resulta que

$$\sum_{i=1}^{\varphi(n)} a_i = \frac{1}{2} n.\varphi(n)$$

Exemplo 4.6: Verificar o teorema **4.9** com $n = 12$.

Solução:

$$\varphi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 4$$

Temos então, 4 primos menores do que 12 e que são primos com 12, que são

$$1, 5, 7 \; e \; 11$$

Logo,

$$1 + 5 + 7 + 11 = 24 =$$
$$= \frac{1}{2} \cdot 12 \cdot \varphi(12) = \frac{12}{2} \cdot 4 = 6.4$$

4.5 Relação entre as funções φ e μ

Teorema 4.10: Para todo inteiro $n \geq 1$

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

Demonstração:

Pelo teorema **4.8** (de Gauss), temos

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

Logo, pela fórmula de inversão de Mobius, segue que

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

Exemplo 4.7: Verificar o teorema **4.10** para o caso $n = 10$.

Solução:

Para $n = 10$, temos

$$\varphi(10) = 10 \sum_{d|10} \frac{\mu(d)}{d} = 10\left(\frac{\mu(1)}{1} + \frac{\mu(2)}{2} + \frac{\mu(5)}{5} + \frac{\mu(10)}{10}\right) =$$

$$= 10\left(1 - \frac{1}{2} - \frac{1}{5} + \frac{1}{10}\right) = 10 - 5 - 2 + 1 = 4$$

De fato, $\varphi(10) = 4$

5. Discussão dos resultados e aplicações em exercícios

Este último capítulo tem como objetivo utilizar os resultados obtidos nos capítulos anteriores para resolver uma série de problemas onde entenderemos melhor a dinâmica das funções aritméticas multiplicativas.

A razão para isso é que os exemplos anteriores foram muito simples e serviram apenas para verificar que os resultados obtidos eram verdadeiros. Os problemas que vem a seguir trazem novas funções aritméticas multiplicativas e propriedades que não são óbvias de deduzir, portanto, a partir daqui, tudo o que foi abordado anteriormente passa a ser usado como ferramenta para chegar a novos resultados.

5.1 Soma dos inversos dos divisores

● Mostre que:

$$\sum_{d|n} \frac{1}{d} = \frac{\sigma(n)}{n}$$

para todo inteiro positivo n.

Solução:

Note que d é um divisor de n se, e somente se, $^{n}/_{d}$ também for divisor de n. Assim, o conjunto dos divisores de n é dado por $\{d_1, d_2, \dots, d_k\}$. Que também pode ser escrito como $\left\{\frac{n}{d_1}, \frac{n}{d_2}, \dots, \frac{n}{d_k}\right\}$. Daí, segue que

$$\sigma(n) = d_1 + d_2 + \cdots + d_k = \frac{n}{d_1} + \frac{n}{d_2} + \cdots + \frac{n}{d_k} =$$

$$= n\left(\frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_k}\right) \Rightarrow$$

$$\Rightarrow \frac{\sigma(n)}{n} = \frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_k} = \sum_{d|n} \frac{1}{d}$$

5.2 O caso onde $\tau(n) = 2^r$

● Se n é um inteiro livre de quadrados, prove que $\tau(n) = 2^r$, onde r é o número de primos distintos na decomposição de n.

Solução:

Seja $n = p_1 p_2 \dots p_r$, a decomposição do inteiro n em fatores primos e livre de quadrados. Sabemos que para qualquer primo p_i, vale que

$$\tau(p_i) = 2 \; com \; i = 1, 2, \dots, r \; e \; mdc(p_i, p_j) = 1, onde \; i \neq j$$

Logo,

$$\tau(n) = \tau(p_1)\tau(p_2) \dots \tau(p_r) = \overbrace{2.2.2.2 \dots 2}^{r} = 2^r$$

5.3 Quando é válido que $\sigma(n + 2) = \sigma(n) + 2$?

● Se n e $n + 2$ são um par de primos gêmeos, então mostre que a seguinte identidade é satisfeita

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

Verifique que vale também para $n = 434$.

Solução:

Se n e $n + 2$ são primos gêmeos, então os divisores positivos de n são apenas $1 \; e \; n$, da mesma forma, os divisores de $n + 2$ são $1 \; e \; n + 2$, logo

$$\sigma(n) = n + 1$$

$$\sigma(n + 2) = (n + 2) + 1 = (n + 1) + 2 = \sigma(n) + 2$$

Portanto, $\sigma(n + 2) = \sigma(n) + 2$, sempre que $n \; e \; n + 2$ forem primos gêmeos.

Para $n = 434 = 2.7.31$ e $n + 2 = 436 = 4.109$, temos

$$\sigma(434) = \sigma(2.7.31) = \sigma(2)\sigma(7)\sigma(31) = 3.8.32 = 768$$

$$\sigma(436) = \sigma(2^2)\sigma(109) = \frac{2^3 - 1}{2 - 1} \cdot 110 = 770 = 768 + 2 = \sigma(434) + 2$$

Ou seja,

$$\sigma(434 + 2) = \sigma(434) + 2$$

Concluímos com isto que a identidade $\sigma(n + 2) = \sigma(n) + 2$ também é válida quando n e $n + 2$ não forem primos gêmeos em alguns casos.

5.4 O número de primos distintos do inteiro n

● Seja $\omega(n)$ o número de primos distintos na fatoração do inteiro positivo n, sendo $\omega(1) = 0$. Por exemplo, temos $\omega(540) = \omega(2^2.3^3.5) = 3$.

a) Mostre que $2^{\omega(n)}$ é uma função multiplicativa

Solução

Sejam $m\ e\ n$ inteiros positivos tais que $mdc(m,n) = 1$ e considere a função $f(n) = 2^{\omega(n)}$.

Sejam $n = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_r^{\alpha_r}$ e $m = q_1^{\beta_1}q_2^{\beta_2}\dots q_s^{\beta_s}$. Além disso, n tem r primos distintos e m tem s primos distintos. Logo, $mn = p_1^{\alpha_1}\dots p_r^{\alpha_r}q_1^{\beta_1}\dots q_1^{\beta_s}$ tem $r+s$ primos distintos e pelo Teorema fundamental da aritmética podemos afirmar que a fatoração é única, sem levar em conta a ordem dos fatores. Daí, segue que

$$\omega(n) = r\ e\ \omega(m) = s\ e\ \omega(mn) = r+s \Rightarrow$$

$$\Rightarrow \omega(mn) = \omega(m) + \omega(n)$$

Logo,

$$f(mn) = 2^{\omega(mn)} = 2^{\omega(m)+\omega(n)} = 2^{\omega(m)}.2^{\omega(n)} = f(m)f(n)$$

Portanto, $2^{\omega(n)}$ é uma função multiplicativa.

b) Para todo inteiro positivo n, obtenha a seguinte fórmula

$$\tau(n^2) = \sum_{d|n} 2^{\omega(d)}$$

Solução:

Pelo item a) e pelo teorema **4.2**, é válido que a função

$$F(n) = \sum_{d|n} 2^{\omega(d)}$$

É multiplicativa

Então seja $n = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$, devemos obter

$$F(n) = F\left(p_1^{k_1}\dots p_r^{k_r}\right) = F\left(p_1^{k_1}\right)\dots F\left(p_r^{k_r}\right) =$$

$$= \sum_{d|p_1^{k_1}} 2^{\omega(d)} \dots \sum_{d|p_r^{k_r}} 2^{\omega(d)}$$

Lembrando que todos os divisores de $p_i^{k_i}$ são precisamente $1, p_i, p_i^2, \dots, p_i^{k_i}$

Por definição, temos $\omega\left(p_i^{a_i}\right) = 1, se\ \alpha_i > 0\ e\ \omega(p_i^0) = \omega(1) = 0$, assim

$$\sum_{d|p_i^{k_i}} 2^{\omega(d)} = 2^0 + \underbrace{2^1 + \cdots + 2^1}_{k_i\ termos} =$$

$$= 1 + k_i . 2^1 = 1 + 2k_i$$

O que implica que

$$F(n) = \sum_{d|p_1^{k_1}} 2^{\omega(d)} \ldots \sum_{d|p_r^{kr}} 2^{\omega(d)} =$$

$$= (1 + 2k_1) \ldots (1 + 2k_r)$$

E como $n^2 = p_1^{2k_1} \ldots p_r^{2k_r}$, então pelo teorema **2.2**, segue que

$$\tau(n^2) = (2k_1 + 1) \ldots (2k_r + 1)$$

Portanto,

$$\tau(n^2) = F(n) = \sum_{d|n} 2^{\omega(d)}$$

5.5 Teorema de Liouville

● Para todo n natural, prove que

$$\left(\sum_{d|n} \tau(d) \right)^2 = \sum_{d|n} \tau(d)^3$$

Solução:

Por resultados anteriores, já sabemos que $\tau(n)$ é uma função multiplicativa. Considere $m\ e\ n$ inteiros positivos, tais que $mdc(m,n) = 1$, logo

$$\tau(mn)^3 = \tau(m^3 n^3) = \tau(m)^3 \tau(n)^3$$

Portanto, $\tau(n)^3$ é uma função multiplicativa. E pelo teorema **3.2**, segue que

$$F(n) = \sum_{d|n} \tau(d)^3$$

é multiplicativa também. E, da mesma forma

$$G(n) = \sum_{d|n} \tau(d) \Rightarrow H(n) = [G(n)]^2 = \left(\sum_{d|n} \tau(d) \right)^2$$

Significa que tanto a função G como H, são multiplicativas. O que pode ser verificado a seguir

$$H(mn) = [G(mn)]^2 = [G(m)G(n)]^2 = [G(m)]^2[G(n)]^2$$

Sem perda de generalidade, podemos considerar um inteiro positivo da forma $n = p_i^{k_i}$, pois, pelo fato das funções $G\ e\ H$ serem multiplicativas, também é válido para $n = p_1^{k_1} \dots p_r^{k_r}$.

Seja $n = p^k$, os divisores de n são precisamente $1, p, p^2, \dots, p^k$. Ressaltando também que $\tau(p^a) = a + 1$, para algum p primo. Assim,

$$F(n) = \sum_{d|p^k} \tau(d)^3 = \tau(1)^3 + \tau(p)^3 + \tau(p^2)^3 + \cdots + \tau(p^k)^3 =$$

$$= 1 + (1+1)^3 + (2+1)^3 + \cdots + (k+1)^3 =$$

$$= 1 + 2^3 + 3^3 + \cdots + (k+1)^3 = \left[\frac{(k+1)(k+2)}{2}\right]^2$$

Por outro lado,

$$H(n) = \left(\sum_{d|p^k} \tau(d)\right)^2 = [\tau(1) + \tau(p) + \tau(p^2) + \cdots + \tau(p^k)]^2 =$$

$$= [1 + 2 + \cdots + (k+1)]^2 = \left[\frac{(k+1)(k+2)}{2}\right]^2$$

Portanto, vimos que $F(n) = H(n)$ o que resulta em

$$\sum_{d|n} \tau(d)^3 = \left(\sum_{d|n} \tau(d)\right)^2$$

5.6 Função geradora de funções multiplicativas

● Seja $n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$ a fatoração canônica do inteiro $n > 1$ em fatores primos. Se f é uma função multiplicativa não identicamente nula, prove que

$$\sum_{d|n} \mu(d) f(d) = \prod_{k=1}^{r} [1 - f(p_k)]$$

Solução:

Como μ e f são multiplicativas, então pelo exemplo **3.1** podemos garantir que μf também é multiplicativa. E pelo teorema **3.2** definimos F multiplicativa por

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

Se F é multiplicativa, então $F\left(p_1^{k_1} \dots p_r^{k_r}\right) = F\left(p_1^{k_1}\right) \dots F(p_r^{k_r})$, com isso, basta provarmos para o caso onde $n = p^k$, para p primo e $k \geq 0$. Logo,

$$F(p^k) = \sum_{d|p^k} \mu(d) f(d) = \mu(1) f(1) + \mu(p) f(p) + \cdots + \mu(p^k) f(p^k) =$$

$$= \mu(1) f(1) + \mu(p) f(p)$$

A soma se reduz a última igualdade, pois $\mu\left(p^i\right) = 0,\ para\ i \geq 2$ e como f é uma função multiplicativa não identicamente nula, segue que $f(1) = 1$, logo

$$F(p^k) = 1.f(1) + (-1) f(p) = 1 - f(p)$$

Como F é multiplicativa e tem-se $F\left(p_i^{k_i}\right) = 1 - f(p_i)$, segue que

$$\sum_{d|n} \mu(d) f(d) = (1 - f(p_1))(1 - f(p_2)) \dots (1 - f(p_r))$$

Este resultado nos permite criar muitas relações a partir de funções conhecidas, como a função $\tau\ e\ \sigma$. Veremos a aplicação disso no próximo problema.

5.7 Aplicações do resultado obtido na seção 5.6

● Dado um inteiro $n > 1$ cuja fatoração é dada por $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, Use o problema da sessão **5.6** para chegar aos seguintes resultados:

a) $\sum_{d|n} \mu(d) \tau(d) = (-1)^r$

Solução:

Pelo problema em **5.6**, temos

$$\sum_{d|n} \mu(d) \tau(d) = \left(1 - \tau(p_1)\right)\left(1 - \tau(p_2)\right) \dots (1 - \tau(p_r))$$

Note que $\tau(p_i) = 2$, o que implica que $1 - \tau(p_i) = -1$, logo

$$\sum_{d|n} \mu(d) \tau(d) = (-1)(-1) \dots (-1) = (-1)^r$$

b) $\sum_{d|n}\mu(d)\sigma(d) = (-1)^r p_1 p_2 \dots p_r$

Solução:

Pelo problema em **5.6**, temos

$$\sum_{d|n}\mu(d)\sigma(d) = \big(1-\sigma(p_1)\big)\big(1-\sigma(p_2)\big)\dots\big(1-\sigma(p_r)\big)$$

Note que $\sigma(p_i) = p_i + 1$, o que implica que $1-\sigma(p_i) = -p_i$, logo

$$\sum_{d|n}\mu(d)\sigma(d) = (-p_1)(-p_2)\dots(-p_r) = (-1)^r p_1 p_2 \dots p_r$$

c) $\sum_{d|n}\mu(d)/d = \big(1-{}^1\!/_{p_1}\big)\big(1-{}^1\!/_{p_2}\big)\dots\big(1-{}^1\!/_{p_r}\big)$

Solução:

Inicialmente vamos verificar que a função definida por $f(n) = {}^1\!/_n$ é multiplicativa. Sendo assim, tome $n = ab$, onde $mdc(a,b) = 1$, logo

$$f(ab) = \frac{1}{ab} = \frac{1}{a}\cdot\frac{1}{b} = f(a)f(b)$$

Pelo problema em **5.6**, temos

$$\sum_{d|n}\mu(d)\cdot\frac{1}{d} = \big(1-f(p_1)\big)\big(1-f(p_2)\big)\dots(1-f(p_r)) =$$

$$= \left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_r}\right)$$

Importante notar também que pelo teorema **4.11**, temos

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

d) $\sum_{d|n}\mu(d)d = (1-p_1)(1-p_2)\dots(1-p_r)$

Solução:

Já sabemos de resultados anteriores que a função identidade $f(n) = n$ é multiplicativa. Portanto, pelo problema em **5.6**, temos

$$\sum_{d|n}\mu(d)d = \big(1-f(p_1)\big)\big(1-f(p_2)\big)\dots\big(1-f(p_r)\big) =$$

$$= (1-p_1)(1-p_2)\dots(1-p_r).$$

5.8 O número de divisores de n livre de quadrados

● Seja $S(n)$ o número de divisores de n livre de quadrados. Mostre que

$$S(n) = \sum_{d|n} |\mu(d)| = 2^{\omega(n)}$$

onde $\omega(n)$ é o número de primos distintos do inteiro n.

Solução:

Note que

$$|\mu(n)| = \begin{cases} 1 \; se \; n = 1 \\ 0 \; se \; p^2|n, \quad para \; p \; primo \\ 1 \; se \; n = p_1 p_2 \ldots p_r, \quad com \; r \; primos \; distintos \end{cases}$$

Seja $f(n) = |\mu(n)|$ e considere $n = ab$, onde $mdc(a,b) = 1$. Suponha que $a \; e \; b$ são inteiros livre de quadrados, isto é,

$$a = p_1 p_2 \ldots p_k, \qquad b = q_1 q_2 \ldots q_s$$

Claramente tem-se $f(a) = f(b) = 1$, o que acarreta em $f(ab) = 1$ e consequentemente $f(ab) = f(a)f(b)$. Portanto, $|\mu(n)|$ é multiplicativa.

E pelo teorema **3.2**, segue que $S(n)$ é multiplicativa.

Seja $n = p^r$. Então, os divisores de n são $1, p, p^2, \ldots, p^r$, logo

$$\sum_{d|n} |\mu(d)| = |\mu(1)| + |\mu(p)| + |\mu(p^2)| + \cdots + |p^r| = 1 + 1 + 0 + \cdots + 0 = 2$$

Seja $n = p_1 p_2 \ldots p_r$, como $f(p_i) = 2$, podemos restringir os divisores de n para $p_1^{m_1} p_2^{m_2} \ldots p_r^{m_r}$, onde cada m_i vale 0 ou 1, portanto o número de divisores de n livre de quadrados é dado por 2^r ou $2^{\omega(n)}$. Daí, segue que

$$S(n) = S(p_1 p_2 \ldots p_k) = S(p_1)S(p_2) \ldots S(p_r) =$$

$$= \sum_{d|p_1} |\mu(d)| \sum_{d|p_2} |\mu(d)| \ldots \sum_{d|p_r} |\mu(d)| = 2.2 \ldots 2 = 2^r = 2^{\omega(n)}$$

5.9 A função λ de Liouville

● A função λ de Liouville é definida por $\lambda(1) = 1$ e $\lambda(n) = (-1)^{k_1 + k_2 + \cdots + k_r}$, se a fatoração de n em fatores primos é dada por $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$. Por exemplo

$$\lambda(360) = \lambda(2^3.3^2.5) = (-1)^{3+2+1} = (-1)^6 = 1.$$

a) Prove que λ é uma função multiplicativa

Solução:

Seja $m\ e\ n$ inteiros primos entre si, isto é,

$$n = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}, \qquad m = q_1^{j_1} q_2^{j_2} \dots q_s^{j_s}\ onde\ cada\ p_x \neq q_y$$

$$nm = p_1^{k_1} \dots p_r^{k_r} q_1^{j_1} \dots q_s^{j_s}$$

como $mdc(m,n) = 1$, segue que

$$\lambda(nm) = (-1)^{k_1+k_2+\cdots+k_r+j_1+j_2+\cdots+j_s} =$$

$$= (-1)^{k_1+k_2+\cdots+k_r}(-1)^{j_1+j_2+\cdots+j_s} =$$

$$= \lambda(n)\lambda(m)$$

b) Dado um inteiro positivo n, verifique que

$$\sum_{d|n} \lambda(d) = \begin{cases} 1, se\ n\ for\ um\ quadrado\ perfeito \\ 0, caso\ contrário \end{cases}$$

Solução:

Seja $F(n) = \sum_{d|n} \lambda(d)$, pelo teorema **3.2**, F é multiplicativa. Suponha então que $n = p^k$, onde p é primo, então temos que

$$F(n) = \lambda(1) + \lambda(p) + \cdots + \lambda(p^k) =$$

$$1 + (-1) + (-1)^2 + \cdots + (-1)^{k-1} + (-1)^k$$

Note que se k for ímpar, então a soma acima resulta em 0, pois p^k terá um número par de divisores, por outro lado, se k é par, então p^k terá um número ímpar de divisores e resultará sempre em 1. Ou seja,

$$F(p^k) = 0, se\ k\ é\ ímpar$$

$$F(p^k) = 1, se\ k\ é\ par$$

Seja $n = p_1^{k_1} \dots p_r^{k_r}$, então temos

$$F(n) = F\left(p_1^{k_1}\right) \dots F(p_r^{k_r})$$

Se n for um quadrado perfeito, então todos os k_i são necessariamente pares, o que significa que $F\left(p_i^{k_i}\right) = 1$, portanto $F(n) = 1$.

Se algum k_i for ímpar, então n não é um quadrado perfeito, logo $F\left(p_i^{k_i}\right) = 0$, o que nos dá $F(n) = 0$.

5.10 Cálculo de $\varphi(2n)$ quanto à paridade de n

● Mostrar que se n é inteiro, então

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

Solução:

Se n é ímpar, então $mdc(n,2) = 1$. Daí

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

Se n é par, então $n = 2^k m$, onde m é um inteiro ímpar e $k \geq 1$. Devemos lembrar também que $\varphi(2^k) = 2^{k-1}$. Daí, segue que

$$\varphi(2n) = \varphi(2.2^k m) = \varphi(2^{k+1}m) = \varphi(2^{k+1})\varphi(m) = 2^k\varphi(m) =$$

$$2\left(2^{k-1}\varphi(m)\right) = 2\varphi(2^k)\varphi(m) = 2\varphi(2^k m) = 2\varphi(n)$$

5.11 A condição para que $\varphi(mn) = n\varphi(m)$

● Mostre que $\varphi(mn) = n\varphi(m)$ se todo primo que divide n também divide m.

Solução:

Seja $p_1, p_2, \ldots, p_r$ todos os primos de n que dividem m. Então, seja $n = p_1^{k_1} \ldots p_r^{k_r}$ e $m = p_1^{s_1} \ldots p_r^{s_r} q_1^{t_1} \ldots q_u^{t_u}$, onde cada q_i é primo, além disso, $q_i \neq p_j$. Assim,

$$mn = p_1^{s_1+k_1} \ldots p_r^{s_r+k_r} q_1^{t_1} \ldots q_u^{t_u} \Rightarrow$$

$$\Rightarrow \varphi(mn) = p_1^{s_1+k_1} \ldots p_r^{s_r+k_r} q_1^{t_1} \ldots q_u^{t_u} \left(1-\frac{1}{p_1}\right) \ldots \left(1-\frac{1}{p_r}\right)\left(1-\frac{1}{q_1}\right) \ldots \left(1-\frac{1}{q_u}\right) =$$

$$= p_1^{s_1} \ldots p_r^{s_r} q_1^{t_1} \ldots q_u^{t_u} \left(1-\frac{1}{p_1}\right) \ldots \left(1-\frac{1}{p_r}\right)\left(1-\frac{1}{q_1}\right) \ldots \left(1-\frac{1}{q_u}\right) p_1^{k_1} \ldots p_r^{k_r} =$$

$$= \varphi(m) p_1^{k_1} \ldots p_r^{k_r} = \varphi(m)n$$

Em particular, se $m = n$, temos

$$\varphi(n.n) = \varphi(n^2) = n\varphi(n)$$

5.12 Cálculo da composta $\varphi(\varphi(n))$, se n é potência de um primo

● Se p é primo e $k \geq 2$. Mostre que $\varphi\left(\varphi(p^k)\right) = p^{k-2}\varphi((p-1)^2)$.

Solução:

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

Como $mdc(p-1, p^{k-1}) = 1$, segue que

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

$$= p^{k-2}(p-1)\varphi(p-1)$$

Pelo caso particular em **5.11,** temos

$$(p-1)\varphi(p-1) = \varphi((p-1)^2)$$

Logo,

$$\varphi(\varphi(p^k) = p^{k-2}\varphi((p-1)^2)$$

5.13 Desigualdade envolvendo a função φ e potência que divide φ

● Se $n > 1$ tem r primos ímpares distintos em sua fatoração, então prove que

a) $2^r | \varphi(n)$

Solução:

Seja $n = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}, p_i > 2$. Daí

$$\varphi(n) = p_1^{k-1}(p_1 - 1)p_2^{k_2-1}(p_2 - 1) \ldots p_r^{k_{r-1}}(p_r - 1)$$

Como cada p_i é ímpar, considere $p_i = 2m_i + 1$, para algum m_i.

Assim,

$$\varphi(n) = p_1^{k_1-1} p_2^{k_2-1} \ldots p_r^{k_{r-1}}(2m_1)(2m_2) \ldots (2m_r) =$$

$$= 2^r p_1^{k_1-1} p_2^{k_2-1} \ldots p_r^{k_{r-1}} m_1 m_2 \ldots m_r \Rightarrow$$

$$\Rightarrow 2^r | \varphi(n)$$

● Se $n > 1$ têm r primos distintos em sua fatoração, então prove que

b) $\varphi(n) \geq {}^{n}/_{2^r}$

Solução:

Seja $p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, então

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right)$$

Mas como $p_i \geq 2$, então

$$\frac{1}{2} \geq \frac{1}{p_i} \Longrightarrow -\frac{1}{p_i} \geq -\frac{1}{2} \Longrightarrow 1 - \frac{1}{p_i} \geq 1 - \frac{1}{2} = \frac{1}{2}$$

Logo,

$$\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_r}\right) \geq \left(\frac{1}{2}\right)\left(\frac{1}{2}\right)\ldots\left(\frac{1}{2}\right) = \frac{1}{2^r}$$

Portanto,

$$\varphi(n) \geq n \cdot \frac{1}{2^r} = \frac{n}{2^r}$$

5.14 Um exemplo da utilização do teorema de Euler

● Mostre que se $mdc(a, n) = mdc(a - 1, n) = 1$, então

$$a^{\varphi(n)-1} + a^{\varphi(n)-2} + \cdots + a^2 + a + 1 \equiv 0(mod\ n)$$

Solução:

Por hipótese, temos $mdc(a, n) = 1$, então podemos aplicar o teorema de Euler **4.2**, daí segue que

$$a^{\varphi(n)} - 1 \equiv 0(mod\ n)$$

Fatorando a expressão do lado esquerdo, temos

$$a^{\varphi(n)} - 1 = (a - 1)(a^{\varphi(n)-1} + \cdots + a^2 + a + 1) \equiv 0(mod\ n)$$

Como $mdc(a - 1, n) = 1$, segue que

$$a^{\varphi(n)-1} + \cdots + a^2 + a + 1 \equiv 0(mod\ n)$$

6. Conclusão

Comentando os principais resultados, deduzimos fórmulas para calcular a quantidade, soma e produto de divisores positivos, mas o fato intrigante é que a fórmula do produto não pôde ser definida como uma função aritmética multiplicativa, por isso recebeu pouca atenção durante o desenvolvimento da nossa teoria.

Outro resultado surpreendente é o teorema **3.2** no qual definimos uma função aritmética como uma soma, mas na verdade ela ainda preserva a propriedade multiplicativa, portanto, o teorema permite que criemos variações de funções multiplicativas já conhecidas, por exemplo, $f(n) = \sum_{d|n} \tau(d)$, onde já sabemos que a função τ é multiplicativa.

Exploramos outros resultados mais conhecidos como o teorema de Wilson, Fermat e de Euler, com vários exemplos de aplicações básicas. Também fizemos uso da função parte inteira e suas propriedades, além de provarmos dois teoremas importantes relacionados a função parte inteira.

Com tudo o que foi abordado, percebemos que dentre as funções aritméticas multiplicativas, as que mais chamam atenção são as funções de Mobius e de Euler, pois pela definição delas não se desconfia que se pode chegar a tantos resultados interessantes envolvendo as duas funções, como por exemplo, o teorema de Gauss e a fórmula de inversão de Mobius. Estudamos também várias propriedades a respeito da função de Euler, como por exemplo o fato de $\varphi(n)$ ser par para qualquer inteiro $n > 2$, além de outros resultados como achar uma fórmula que nos dê a soma de todos os números que são primos com n e menores que n.

Tendo em vista os resultados obtidos ao longo de todo o desenvolvimento do trabalho, é importante esclarecer que não foi possível encontrar aplicações concretas aplicadas a vida real, provavelmente porque tais aplicações são estudadas num nível mais alto de pesquisa, portanto retratamos aspectos básicos da Teoria dos Números. Por isso o último capítulo foi apresentado problemas mais difíceis e com mais abstração onde iríamos simplesmente provar propriedades ou identidades dadas nos enunciados.

7. Referência bibliográfica

[1] SANTOS, José Plínio de Oliveira., **Introdução à Teoria dos Números**. 3ª Edição, Rio de Janeiro: IMPA, 2020. 128 p. (Coleção Matemática Universitária).

[2] NETO, Antônio Caminha Muniz., **Tópicos de Matemática Elementar**: **Teoria dos Números, v.5**. 2ª Edição, Rio de Janeiro: SBM, 2013. v.5; 263p. (Coleção Professor de Matemática; 28).

[3] ALENCAR FILHO, Edgard., **Teoria Elementar dos Números**. São Paulo: Nobel, 1981.

[4] ALENCAR FILHO, Edgard., **Teoria das Congruências**. São Paulo: Nobel, 1981.

[5] CASTRO, Jânio Kléo Sousa., **Teoria dos Números**. Coordenação Cassandra Ribeiro Joye. Fortaleza: UAB/IFCE, 2010.

[6] MARTINEZ, Fabio Brochero; MOREIRA, Carlos Gustavo; SALDANHA, Nicolau; TENGAN, Eduardo., **Teoria dos Números: Um Passeio com Primos e Outros Números Familiares Pelo Mundo Inteiro**. 4º Edição, Rio de Janeiro: IMPA, 2018. 500p. (Coleção Projeto Euclides).

[7] BURTON, David M., **Elementary Number Theory**. 6th Edition, New York: McGraw-Hill Book Company, Inc. 2007.