UNIVERSIDADE FEDERAL DO CEARÁ

CENTRO DE CIÊNCIAS

DEPARTAMENTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA EM REDE NACIONAL

LUCAS MOISÉS CARNEIRO DE CARVALHO

TÓPICOS DE FUNÇÕES ARITMÉTICAS E O TEOREMA DE EULER

FORTALEZA

2020

LUCAS MOISÉS CARNEIRO DE CARVALHO

TÓPICOS DE FUNÇÕES ARITMÉTICAS E O TEOREMA DE EULER

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matemática.
Área de concentração: Ensino da Matemática.

Orientador: Prof. Dr. Marcelo Ferreira de Melo.

FORTALEZA
2020

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

C325t Carvalho, Lucas Moisés Carneiro de.
Tópicos de funções aritméticas e o teorema de Euler / Lucas Moisés Carneiro de Carvalho. – 2020.
56 f. : il.

Dissertação (mestrado) – Universidade Federal do Ceará, Centro de Ciências, Departamento de Matemática, Programa de Pós-Graduação em Matemática em Rede Nacional, Fortaleza, 2020.
Orientação: Prof. Dr. Marcelo Ferreira de Melo.

1. Função aritmética. 2. Teorema de Euler. 3. Teorema de Fermat. 4. Raízes primitivas. 5. Ensino básico. I. Título.

CDD 510

LUCAS MOISÉS CARNEIRO DE CARVALHO

TÓPICOS DE FUNÇÕES ARITMÉTICAS E O TEOREMA DE EULER

Dissertação apresentada ao Programa de Pós-Graduação em Matemática em Rede Nacional do Departamento de Matemática da Universidade Federal do Ceará, como requisito parcial à obtenção do título de mestre em Matemática.
Área de concentração: Ensino da Matemática.

Aprovada em: 03/07/2020

BANCA EXAMINADORA

_____
Prof. Dr. Marcelo Ferreira de Melo (Orientador)
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Marcos Ferreira de Melo
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Ângelo Papa Neto
Instituto Federal de Educação, Ciência e Tecnologia do Ceará (IFCE)

À minha esposa Syntia e ao meu filho Davi.

Matemáticos têm tentado em vão, até o dia de hoje, descobrir alguma ordem na sequência de números primos, e nós temos razões para acreditar que é um mistério no qual a mente humana jamais penetrará. (LEONHARD EULER)

AGRADECIMENTOS

A Deus por tudo de bom e maravilhoso que ele reservou em minha, fazendo-me sempre acreditar em seu amor infinito.

À minha esposa, por todo companheirismo e parceria em todos os nossos projetos de vida e amor incondicional.

Ao meu filho Davi, minha força motora que se renova a cada olhar.

Aos meus pais, Paulo Tarcísio de Carvalho (In Memoriam) e Emília Carneiro de Carvalho por nunca medirem esforços em minha educação.

Aos meus tios, Edvandro Rodrigues Carneiro (In Memoriam) e Antônia Fernandes Carneiro por proporcionarem apoio financeiro e emocional com meus estudos quando meus pais não podiam.

Aos meus irmãos, João Candido Carneiro de Carvalho e Paulo Emílio Carneiro de Carvalho, que sempre foram minhas fontes de inspirações.

Ao meu primo Francisco Sérgio Fernandes Carneiro por acreditar.

Ao meu amigo Arquimedes Pompeu pela disposição em ajudar-me no texto.

Aos meus colegas de Mestrado por todas as discussões, almoços, piadas, companheirismo, desfrutando com eles todas as angústias e todas as conquistas.

Aos professores do PROFMAT-UFC por transmitir com entusiasmo e qualidade tudo que aprendi. Meu mais sincero obrigado.

Ao professor Dr. Marcelo Ferreira Melo, grande professor e orientador por suas valiosas observações para a melhoria desse trabalho.

Aos participantes da banca examinadora Marcos Ferreira Melo e Ângelo Papa Neto, pelas valiosas sugestões e colaborações.

A todos os meus mais sinceros agradecimentos.

RESUMO

O presente trabalho tem por objetivo, apresentar uma pequena introdução ao estudo de Funções Aritméticas, apresentando algumas propriedades dando um pouco mais de destaque as funções aritméticas específicas, como a Função de Euler e a Função de Möbius. Destacamos também o Teorema de Euler e um corolário dele, conhecido como Pequeno Teorema de Fermat que servirá de base para a resolução de alguns problemas que são cobrados frequentemente em Olimpíadas de Matemática ao redor do mundo. A ideia de Raízes Primitivas também será abordada no presente trabalho no intuito de fornecer ao professor de ensino Médio uma ferramenta poderosa que não é ensinado no Ensino Básico. Por fim, dedicamos um capítulo inteiro somente com problemas sobre os assuntos abordados, apresentado todas as soluções dos mesmos para servir de apoio aos professores.

Palavras-chave: Funções Aritméticas. Função de Euler. Função de Möbius. Teorema de Euler. Pequeno Teorema de Fermat. Raízes Primitivas. Matemática – Problemas e Exercícios.

ABSTRACT

The main goal of this paper is present a brief introduction to the studies of the arithmetic functions, bringing up some properties emphasizing some specific arithmetic functions as the Euler and Möbius functions. It was also highlighted the Euler's theorem and one of its corollaries, known as Fermat's little theorem, that will serve as a basis for the solution of some problems that are frequent on Mathematical Olympiads around the world. The idea of primitive roots will also be covered in this paper in order to provide high school teachers a powerful tool that is not taught on basic education. In closing, a whole chapter is dedicated to mathematical problems about the topics mentioned, presenting every solution in order to support teachers.

Keywords: Arithmetic Functions. Euler Function. Möbius Function. Euler's Theorem. Fermat's Little Theorem. Primitive Roots. Mathematics – Problems and Exercises.

SUMÁRIO

1 INTRODUÇÃO

Segundo Gauss, a Matemática é Rainha das Ciências, enquanto a Teoria dos Números é a rainha da Matemática. Muitos matemáticos proeminentes compartilhavam da mesma ideia de Gauss e fizeram suas contribuições nesse ramo. Podemos citar dentre eles: Fermat, Euler, Möbius, Kummer, Hardy, Ramanujan dentre outros.

A teoria dos Números estuda basicamente as propriedades dos números inteiros, sendo que para esse trabalho não precisamos de matemática de nível superior para o seu entendimento. No que permeia tal teoria, o estudo dos números primos que por definição são aqueles inteiros positivos que possuem somente dois divisores, ele próprio e o número um, é um dos mais pesquisados em toda matemática, desde Euclides que provou a sua infinidade até a prova do Último Teorema de Fermat, feita pelo matemático inglês Andrew Wiles em 1995.

Salientamos nesse trabalho a importância das Funções Aritméticas e dois de seus exemplos que são a Função de Euler e a Função de Möbius que servirá como base para o desenvolvimento desse trabalho no que tange a Fórmula da Inversão de Möbius e o Teorema de Euler e um dos resultados que permeiam esse trabalho que é o Pequeno Teorema de Fermat, que nada mais é do que um corolário do Teorema de Euler e é bastante cobrado em exames e Olímpiadas de Matemática ao redor mundo.

Deste modo, no final desse trabalho, apresentamos uma lista com problemas de competições de matemática olímpicas sobre os assuntos abordados nessa dissertação, todos eles resolvidos, onde para isso foram feitas pesquisas bibliográficas.

Ademais acreditamos poder contribuir com professores e alunos do ensino básico, que buscam aperfeiçoar seus conhecimentos em teorias que não são disponibilizadas nos currículos da educação Básica.

2 UM POUCO DE HISTÓRIA

2.1 Fermat

Pierre Simon de Fermat, nasceu na cidade francesa Beaumont-de-Lomagne no ano de 1607 e pertencia a uma família que podia proporcionar uma educação de qualidade ao jovem francês.

Estudou no colégio dos jesuítas em La Fleche, estudava direito participando também de campanhas militares.

A matemática ainda se recuperava da idade das trevas no início do século XVII, não constituindo um assunto muito respeitado, sendo que a maioria dos matemáticos bancavam seus próprios estudos. Um dos centros europeus mais importantes que via na matemática uma disciplina fundamental era Oxford na Inglaterra. Isso nos mostra que a maioria dos matemáticos da época era amadores sendo Fermat um deles.

Fermat tem contribuições fundamentais em teoria das probabilidades e também no estudo do Cálculo diferencial.

Com relação à Teoria dos Números, Fermat foi atraído sobre maneira ao livro de Diofante[1] chamado de "Arithmetica", onde vários assuntos atiçaram a sua imaginação, sendo que alguns de seus resultados ele demonstrou utilizando um método elaborado por ele denominado de "Descida Infinita".

Conta a história que em uma das margens do livro de Diofante, Fermat escreveu algo que atormentou por vários séculos a mente de muitos matemáticos. Ele escreveu que embora existissem infinitos ternos que satisfaziam a equação $x^n + y^n = z^n$ para n = 2 isso não seria verdadeiro para n inteiro maior ou igual a 3. Dizendo que a margem daquele livro era extremamente pequena para conter sua demonstração.

[1] Matemático grego

Essas frases escritas no livro de Diofante passou a ser conhecido como o **Último Teorema de Fermat,** demonstrado em 1995 por Andrew Willes[2], com contribuições de Richard Taylor[3], em 1995.

Acredita-se que Fermat não tinha realmente uma demonstração de seu teorema e que tenha usado de alguma forma a redução ao absurdo e seu método da descida infinita. Para termos uma ideia do uso dessas duas ferramentas Boyer (1996), nos mostra como provar que $\sqrt{3}$ é irracional usando o seu método.

Vejamos:

Para isso vamos supor que $\sqrt{3}$ é racional, ou seja, supor que exista dois inteiros *a* e *b* positivos com $a > b$ tal que $\sqrt{3} = \frac{a}{b}$.

A partir da relação acima podemos afirmar que:

$$\frac{1}{-1+\sqrt{3}} = \frac{1+\sqrt{3}}{2}$$

Substituindo a primeira $\sqrt{3}$ por $\frac{a}{b}$ teremos:

$$\sqrt{3} = \frac{3b-a}{a-b}$$

Como a e b são inteiros então $3b - a$ e $a - b$ também são. Sendo assim chamaremos de $a_1 = 3b - a$ e $b_1 = a - b$. Aqui podemos perceber que $\frac{3}{2} < \sqrt{3} < 2$, logo:

1. Desigualdade da esquerda:

$$\frac{3}{2} < \frac{a}{b}$$
$$3b < 2a$$
$$3b < a + a$$
$$3b - a < a$$

2. Desigualdade da direita:

$$\frac{a}{b} < 2$$
$$a < 2b$$
$$a < b + b$$
$$a - b < b$$

[2] Matemático inglês
[3] Matemático inglês

Sabendo que $a_1 = 3b - a$ e $b_1 = a - b$, concluímos que $a_1 < a$ e $b_1 < b$. Daí podemos escrever:

$$\sqrt{3} = \frac{a_1}{b_1}$$

Esse raciocínio pode ser repetido infinitas vezes, nos levando a crer que não existe o menor inteiro positivo. Portanto a premissa que $\sqrt{3}$ é racional é falsa logo $\sqrt{3}$ é irracional.

No nosso trabalho falaremos de um teorema específico denominado "Pequeno Teorema de Fermat" que afirma que, se o máximo divisor comum entre a e n é 1 então $a^n - 1$ é divisível por n. E generalizaremos esse resultado com uma ideia de Euler.

Fermat morreu em Castres na França em 1665 aos 61 anos de idade.

2.2 Euler

O suiço Leonhard Paul Euler, nasceu na cidade da Basiléia no ano de 1707 tendo sido alunos dos Bernoullis[4].

Euler talvez tenha sido o mais prolífico matemático da história, contribuindo em praticamente em todos os ramos dela, tais como: geometria, análise, topologia e teoria dos números.

Devido a sua vasta produção, Euler possui vários teoremas que levam o seu nome. Destacamos aqui o Teorema dos poliedros convexos, que afirma que, se V, F e A representam nessa ordem o número de vértices, o número de faces e o número de arestas do poliedro convexo então podemos demonstrar que V + A = F + 2.

Euler possui contribuições em análise, onde podemos destacar a constante de Euler, representada pela letra **e** cujo valor é representado pelo limite abaixo:

$$e = \lim_{n \to \infty} \left(1 + \frac{1}{n}\right)^n$$

[4] Família de matemáticos suíços

Em teoria dos números, Euler possui contribuições de destaque, dentre elas, provou que o Último Teorema de Fermat, teorema esse que afirma que para x, y e z inteiros positivos a equação $x^n + y^n = z^n$ não possui solução para n inteiro com $n \geq 3$ não possui solução, para o caso $n = 3$.

Com relação ao Pequeno Teorema de Fermat, Euler foi o primeiro a publicar uma demonstração. Euler provou usando indução.

Abaixo enunciaremos e provaremos usando a ideia de Euler.

Pequeno Teorema de Fermat: Se p é um primo e p não divide a então $a^{p-1} - 1$ é divisível por p.

Demonstração: A indução será sobre a.

Para $a = 1$ temos que $1^{1-1} - 1$ é divisível por p.

Suponha que o teorema seja válido para $a = k$, isto é $k^{p-1} - 1$ é divisível por p.

Sendo assim existe um inteiro b tal que $p.b = k^{p-1} - 1$.

Vamos provar agora que o resultado também é válido para $a = k + 1$.

Vejamos:

$a^{p-1} - 1 = (k + 1)^{p-1} - 1 = k^{p-1} + m(p - 1) + 1 - 1 = k^{p-1} + mp - 1$.

Como por hipótese $p.b = k^{p-1} - 1$, então:

$a^{p-1} - 1 = k^{p-1} + mp - 1 = pb + mp = p(b + m)$.

Isto é:

p divide $a^{p-1} - 1$ provando assim o teorema.

Logo após demonstrar esse teorema, Euler demonstrou o caso mais Geral, utilizando para isso o que se veio a chamar Função de Euler.

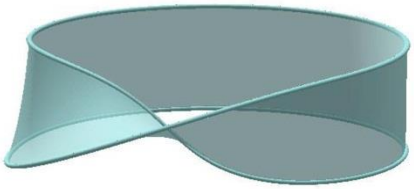
Durante esse trabalho mostraremos com mais profundidade esses resultados.

2.3 Möbius

Nascido em 1790, na cidade alemã de Schulpforta, tendo morrido no ano de 1868 aos 78 anos, o alemão August Ferdinando Möbius é mais reconhecido pela faixa que leva seu nome.

Essa faixa que pode ser construída fisicamente bastando para isso colar as duas extremidades mediante a uma meia rotação de uma delas é um dos primeiros modelos topológicos de superfície de um lado apenas.

Abaixo mostramos a fita de Möbius.



E relação ao estudo de funções aritméticas, assunto que será tratado de maneira um pouco mais profundo nesse trabalho, Möbius introduziu a função que leva seu nome, a Função de Möbius, denominada função μ.

Com essa função, Möbius separou os inteiros em 3 categorias:

1ª categoria – múltiplos de quadrados perfeitos, a qual associou o número 0. Podemos citar como exemplo $\mu(50) = 0$, pois 50 é múltiplo do quadrado 25. O número 1 embora seja um quadrado perfeito não pertencerá a essa categoria.

2ª categoria – números inteiros que são fatorados em uma quantidade ímpar de primos distintos, a qual associou o número –1. Podemos citar como exemplo $\mu(105) = -1$, pois 105 = 3 x 5 x 7.Vale ressaltar que $\mu(p) = -1$ para qualquer primo p.

3ª categoria – números inteiros que são fatorados em uma quantidade pares de primos distintos, a qual associou o número 1. Podemos citar como exemplo $\mu(210) = 1$, pois 210 = 2 x 3 x 5 x 7.o número 1 fará parte dessa categoria.

Segue abaixo os 10 primeiros termos da função μ de Möbius.

{1, -1,-1,0,-1,1,-1,0,0,1}

O que nos chama a atenção é que a ideia da Função de Möbius tem várias aplicações na física, principalmente na física de partículas.

3 FUNÇÕES ARITMÉTICAS

Definição: Uma função é denominada de função aritmética quando a mesma está definida para todo inteiro positivo.

No nosso estudo, essa função terá como contradomínio o conjunto dos números inteiros.

Isto é:

Se f : A $\rightarrow$ B é uma função aritmética, então:

$A = \mathbb{Z}$

$B = \mathbb{Z}$

ou seja:

$$\text{Im}(f) = \{ f(n) \in \mathbb{Z} ; n \in \mathbb{Z} \}$$

Seguem abaixo alguns exemplos de funções aritméticas.

Exemplo 1:

$$d : \mathbb{Z} \rightarrow \mathbb{Z}$$

definida por:

$d(n)$ = número de divisores positivos de n.

Logo, $d(8) = 4$, pois os divisores positivos de 8 são {1; 2; 4; 8}

Exemplo 2:

$$s : \mathbb{Z} \rightarrow \mathbb{Z}$$

definida por:

$s(n)$ = soma dos divisores positivos de n.

Logo:

$s(8) = 15$.

pois $1 + 2 + 4 + 8 = 15$.

Existem algumas funções aritméticas que possuem uma propriedade especial.

Essa propriedade será de fundamental importância no desenvolvimento do estudo de uma função aritmética denominada **Função de Euler**.

Definição: Uma função aritmética é denominada multiplicativa se:

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

sempre que m e n são inteiros relativamente primos, ou seja, o m.d.c. (m, n) = 1.

Exemplos:

1) A função $f: \mathbb{N} \to \mathbb{N}$ definida por $f(n) = 1$ é multiplicativa pois:

$f(m \cdot n) = 1$

$f(m) = 1$

$f(n) = 1$

logo: $f(m \cdot n) = f(m) \cdot f(n)$ para todo m e n natural.

2) A função $g: \mathbb{N} \to \mathbb{N}$ definida por $g(n) = n$ é multiplicativa pois:

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

É importante ressaltar que as funções f e g definidas acima satisfazem a expressão abaixo:

$$\begin{cases} f(m \cdot n) = f(m) \cdot f(n) \\ g(m \cdot n) = g(m) \cdot g(n) \end{cases}$$

sem a necessidade do m.d.c. (m, n) = 1.

Quando isso acontece, nós afirmamos que a função aritmética é denominada de completamente multiplicativa.

Teorema 1: Se *f* é uma função multiplicativa e $n = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot ... \cdot p_r^{\alpha r}$ é a fatoração do inteiro positivo *n* em potências de primos. Então:

$$f(n) = f\left(p_1^{\alpha 1}\right) \cdot f\left(p_2^{\alpha 2}\right) \cdot ... \cdot \left(p_r^{\alpha r}\right)$$

Demonstração: Como *f* é uma função multiplicativa e m.d.c. $\left(p_1^{\alpha 1}; p_2^{\alpha 2}; ...; p_r^{\alpha r}\right) = 1,$ pois todas são potencias de primos distintos.

Então:

$$f(n) = f\left(p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot ... \cdot p_r^{\alpha r}\right) =$$
$$= f\left(p_1^{\alpha 1}; \left(p_2^{\alpha 2}; ...; p_r^{\alpha r}\right)\right)$$
$$= f\left(p_1^{\alpha 1}\right) \cdot f\left(p_2^{\alpha 2}; ...; p_r^{\alpha r}\right)$$
$$= f\left(p_1^{\alpha 1}\right) \cdot f\left(p_2^{\alpha 2}\right) \cdot f\left(p_3^{\alpha 3}; p_4^{\alpha 4}; ...; p_r^{\alpha r}\right)$$

Continuando por esse caminho indutivo, nós encontraremos que $f(n) = f\left(p_1^{\alpha 1}\right) \cdot f\left(p_2^{\alpha 2}\right) \cdot ... \cdot \left(p_r^{\alpha r}\right).$ □

Abaixo seguem duas funções aritméticas bastante usuais. Mas, para isso, precisamos definir quantidade de divisores positivos de um número inteiro positivo e a soma dos divisores positivos de um número inteiro positivo.

Definição: Um número inteiro positivo *d* divide um inteiro positivo *n* se existe um inteiro positivo *k* tal que:

$$n = d \cdot k$$

Notação:

d | n (lê-se *d* divide *n*)

Existe uma função denominada função soma dos divisores positivos denotados pela letra grega σ (sigma), definida por:

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

onde *n* é um inteiro positivo.

Exemplo:

$\sigma(12) = 1 + 2 + 3 + 4 + 5 + 6 + 12$

$\sigma(12) = 28$

$\sigma(10) = 1 + 2 + 5 + 10 = 18$

$\sigma(10) = 18$

Outra função importante que vale a pena citar é a função números de divisores positivos que será denotada pela letra grega τ (tau), definida por:

$\tau(n)$ = número de divisores positivos de *n.*

onde *n* é um inteiro positivo.

Exemplo:

$\tau(12) = 6$

$\tau(10) = 4$

Cabe aqui representar essas duas novas funções com a notação de somatório.

Vejamos:

01. $\sigma(12) = 1+2+3+4+6+12 = \sum_{d|12} d$

$\sigma(10) = 1+2+5+10 = \sum_{d|10} d$

Generalizando.

01. $\sigma(n) = \sum_{d|n} d$ 02. $\tau(n) = \sum_{d|n} 1$

onde *d* é um inteiro positivo.

Vamos demonstrar que as duas funções citadas acima são funções multiplicativas.

Isto é:

$\sigma(12) = \sigma(3 \cdot 4) = \sigma(3) \cdot \sigma(4) = 4 \cdot 7 = 28$

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

Para isso, vamos, primeiramente, demonstrar o lema abaixo.

Lema: Seja *f* uma função multiplicativa, então a função definida por $F(n) = \sum_{d|n} f(d)$ também será multiplicativa.

Demonstração: Devemos mostrar que F($m \cdot n$) = F(m) · F(n), com m.d.c. (m, n) = 1, para *m* e *n* inteiros positivos.

Vamos assumir, então, que m.d.c. (m, n) = 1.

Logo:

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

Como m.d.c. (m, n) = 1, então os divisores de $m \cdot n$ são escritos de forma única como o produto dos divisores relativamente primos d_1 de m e d_2 de n, onde cada par de divisores de d_1 de m e d_2 de n corresponde a um divisor $d = d_1 \cdot d_2$ de $m \cdot n$.

Daí, podemos escrever:

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

Como f é multiplicativa e m.d.c. (d_1:d_2) = 1

Então:

$$\mathrm{F}(m\cdot n) = \sum_{\substack{d_1|m \\ d_2|n}} f\left(\mathrm{d}_1\cdot \mathrm{d}_2\right) = \sum_{\substack{d_1|m \\ d_2|n}} f\left(\mathrm{d}_1\right)\cdot f\left(\mathrm{d}_2\right) = \sum_{d_1|m} f\left(\mathrm{d}_1\right)\cdot \sum_{d_2|n} f\left(\mathrm{d}_2\right) = \mathrm{F}(m)\cdot \mathrm{F}(n)$$

Assim, as funções σ e τ são multiplicativas.

Vamos agora introduzir uma maneira de calcularmos $\sigma(n)$ e $\tau(n)$ a partir da decomposição de n em fatores primos.

Para isso, iremos utilizar como ferramenta o lema abaixo.

Lema: Se "p" é um número primo e "a" um inteiro positivo. Então:

$$\sigma\left(p^{\mathrm{a}}\right) = 1 + p + p^2 + \ldots + p^{\mathrm{a}} = \frac{p^{\mathrm{a}+1}-1}{p-1}$$

e

$\tau(p^{\mathrm{a}}) = \mathrm{a} + 1$

Demonstração: Como p é primo, então p^a possui os seguintes divisores positivos:

$\{1; p; p^2; p^3; \ldots; p^a\}$

Logo:

$$\sigma\left(p^{\mathrm{a}}\right) = 1 + p + p^2 + \ldots + p^{\mathrm{a}}$$

$$\sigma\left(p^{\mathrm{a}}\right) = \frac{1\left(p^{\mathrm{a}+1}-1\right)}{p-1} = \frac{p^{\mathrm{a}+1}-1}{p-1}$$

para isso, aplicamos a fórmula da soma dos termos de uma Progressão Geométrica finita de razão p.

Podemos também concluir que o número de divisores positivos de p^a é $a + 1$, isto é:

$\tau(p^{\mathrm{a}}) = \mathrm{a} + 1$.

Exemplo:

$$\sigma\left(3^4\right)=1+3+3^2+3^3+3^4=\frac{3^{4+1}-1}{3-1}=\frac{3^5-1}{2}=121$$

$\tau(3^4) = 4 + 1 = 5$

Agora podemos enunciar e demonstrar dois teoremas que nos auxiliarão nos cálculos da soma dos divisores positivos de um número inteiro positivo e na quantidade de divisores positivos.

Vejamos.

Teorema 2: Seja um número inteiro positivo *n* com fatoração em números primos dada por:

$$n=p_1^{a1}\cdot p_2^{a2}\cdot p_3^{a3}\cdot\ldots\cdot p_s^{as}$$

Então:

$$\sigma\left(n\right)=\left(\frac{p_1^{a_1+1}-1}{p_1-1}\right)\cdot\left(\frac{p_2^{a_2+1}-1}{p_2-1}\right)\cdot\ldots\cdot\left(\frac{p_s^{a_s+1}-1}{p_s-1}\right)$$

$$\sigma\left(n\right)=\prod_{j=1}^{s}\frac{p_j^{aj+1}-1}{p_j-1}$$

e

$$\tau\left(n\right)=\left(a_1+1\right)\cdot\left(a_2+1\right)\cdot\ldots\cdot\left(a_s+1\right)$$

$$\tau\left(n\right)=\prod_{j=1}^{s}\left(aj+1\right)$$

Demonstração: Sabemos que σ e τ são funções multiplicativas.

Portanto:

$$\sigma\left(n\right)=\sigma\left(p_1^{a1}\cdot p_2^{a2}\cdot\ldots\cdot p_s^{as}\right)=\sigma\left(p_1^{a1}\right)\cdot\sigma\left(p_2^{a2}\right)\cdot\ldots\cdot\sigma\left(p_s^{as}\right)$$

$$\sigma\left(n\right)=\left(\frac{p_1^{a_1+1}-1}{p_1-1}\right)\cdot\left(\frac{p_2^{a_2+1}-1}{p_2-1}\right)\cdot\ldots\cdot\left(\frac{p_s^{a_s+1}-1}{p_s-1}\right)$$

$$\sigma\left(n\right)=\prod_{j=1}^{s}\left(\frac{p_j^{j+1}-1}{p_j-1}\right)$$

e

$$\tau(n) = \tau\left(p_1^{a1} \cdot p_2^{a2} \cdot \ldots \cdot p_s^{as}\right) = \tau\left(p_1^{a1}\right) \cdot \tau\left(p_2^{a2}\right) \cdot \ldots \cdot \tau\left(p_s^{as}\right)$$

$$\tau(n) = (a_1 + 1) \cdot (a_2 + 1) \cdot \ldots \cdot (a_s + 1)$$

$$\tau(n) = \prod_{j=1}^{s} (a_j + 1)$$

□

Exemplo:

$$\sigma(100) = \sigma\left(2^2 \cdot 5^2\right) = \sigma\left(2^2\right) \cdot \sigma\left(5^2\right) = \left(\frac{2^3 - 1}{2 - 1}\right) \cdot \left(\frac{5^3 - 1}{5 - 1}\right)$$

$$\sigma(100) = \frac{7}{1} \cdot \frac{124}{4} = 7 \cdot 31 = 217$$

e

$$\tau(100) = \tau\left(2^2 \cdot 5^2\right) = \tau\left(2^2\right) \cdot \tau\left(5^2\right) = (2 + 1) \cdot (2 + 1)$$

$$\tau(100) = 3 \cdot 3 = 9$$

4 FUNÇÃO DE EULER

Definição: Denotamos por $\varphi(n)$, lê-se (fi de n) o número de inteiros positivos menores ou iguais a n que sejam relativamente primos com n.

Em notação matemática:

$\varphi(n) = \#\{x \in \mathbb{N}; x \leq n \text{ e m.d.c. } (x,n) = 1\}$

Sendo assim, a função de Euler é uma função aritmética.

Exemplo 1:

$\varphi(20) = 8$

pois os números inteiros positivos que são relativamente primos com 20, sem exceder 20, são: {1; 3; 7; 9; 11; 13; 17; 19}.

Exemplo 2:

$\varphi(13) = 12$

pois os números inteiros positivos que são relativamente primos com 13, sem exceder 13, são: {1; 2; 3; 4; 5; 6; 7; 8; 9; 10; 11; 12}.

Observação: $\varphi(1) = 1$, pois o número 1 é o único inteiro positivo relativamente primo com 1, sem exceder 1.

Podemos então afirmar, pela definição, que se n é um inteiro positivo maior que 1, então podemos afirmar que $\varphi(n)$ representa o número de inteiros menores que n tal que m.d.c. de n e cada um desses inteiros é 1.

Abaixo demonstraremos um importante resultado a respeito de $\varphi(p)$, para p um número primo.

Teorema 3: Seja p um número primo então $\varphi(p) = p - 1$.

Demonstração: Se n > 1 for composto então existe um número b positivo tal que b divide n com $1 < b < n$.

Dito isto, vemos que dentre os números 1, 2, 3, 4, ..., b; ...; n existem, pelo menos, dois que não são relativamente primos com n, a saber: b e n.

Daí concluímos que:

$\varphi(n) \leq n - 2$, para $n > 1$ composto.

Então:

$\varphi(p) = p - 1$

De outra forma, para p primo, o único número inteiro positivo menor ou igual a p que não é relativamente primo é ele próprio. □

Teorema 3: Se p é um número primo e k inteiro positivo, então:

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

Demonstração: Sabe-se que se $p \nmid n$, então m.d.c. $(n, p^k) = 1$.

Percebe-se, também, que entre 1 e p^k existem exatamente p^{k-1} inteiros que são divisíveis por p.

Abaixo, temos a lista deles:

$p; 2p; 3p; ...; (p^{k-1})p$

Então, o conjunto $\{1, 2, 3, ...; p^k\}$ contém exatamente $p^k - p^{k-1}$ que são relativamente primos com p^k.

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

Vamos entender a demonstração, calculando $\varphi(81)$.

Solução:

$\varphi(81) = \varphi(3^4) = 54$

pois, de todos os elementos do conjunto $A = \{1; 2; 3; 4; 5; 6; 7; ...; 3^4\}$, os elementos do conjunto abaixo não são relativamente primos com 81:

$\{3; 6; 9; 12; 15; ...; 3^4\} = B$

Como:

$B = \{3; 6; 9; 12; 15; ...; 3^4\} = \{3 \cdot 1; 3 \cdot 2; 3 \cdot 3; ...; 3 \cdot 3^3\}$

então existem 3^3 elementos no conjunto B.

Logo:

$\varphi(3^4) = 3^4 - 3^3 = 81 - 27 = 54$

Exemplo 1:

$\varphi(5^4) = 5^4 - 5^3 = 625 - 125 = 500$

Demonstraremos agora um teorema que estenderá essa ideia para qualquer número positivo n > 1.

Para isso, usaremos o fato da função $\varphi(n)$ ser uma função multiplicativa.

Teorema 4: Sejam m e n inteiros positivos relativamente primos. Então $\varphi(mn) = \varphi(m) \cdot \varphi(n)$.

Demonstração: Sejam res dois inteiros positivos tais que o m.d.c.(m, n) = l.

Cumpre demonstrar que $\varphi(m \cdot n) = \varphi(m)\ \varphi(n)$.

A proposição é verdadeira se m ou n é igual a 1, pois, temos:

$$(1 \cdot \mathrm{n}) = \varphi(n) = 1 \cdot \varphi(n) = \varphi(1)\ \cdot \varphi(n)$$

$$(\mathrm{m} \cdot 1) = \varphi(m) = \varphi(n) \cdot\ 1 = \varphi(r)\ \cdot \varphi(1)$$

Suponhamos, pois, $m > 1$ e $n > 1$. Neste caso, os inteiros de 1 a mn podem ser dispostos em m colunas com n inteiros em cada uma delas, do seguinte modo:

1	2	. . .	h	. . . m
$m + 1$	$m + 2$		$m + \mathrm{h}$	$2m$
$2m + 1$	$2m + 2$		$2m + \mathrm{h}$	$3m$
.	.		.	.
.	.		.	.
.	.		.	.
$(n - 1)m + 1$	$(n - 1)m + 2$		$(n - 1)m + \mathrm{h}$	nm

Por ser o m.d.c.$(qm + h, m)$ = m.d.c.(h, m), os inteiros da h-ésima coluna são primos com m se e somente se h é primo com m. E como na primeira linha o número de inteiros que são primos com m é igual a $\varphi(m)$, segue-se que existem somente $\varphi(m)$ colunas formadas com inteiros que são todos primos com m. Por outro lado, em cada uma destas $\varphi(m)$ colunas existem precisamente $\varphi(n)$ inteiros que são primos com n, porque na progressão aritmética:

$$h,\ m + h,\ 2m + h,\ ...,\ (n - \mathrm{l})r + h$$

onde o m.d.c.$(h, r) = 1$, o número de termos que são primos com n é igual a $\varphi(n)$. Assim sendo, o número total de inteiros que são primos com m e com n, isto é, que são primos com mn, é igual a $\varphi(m)\ \varphi(n)$, e isto significa que $\varphi(mn) = \varphi(m)\ \varphi(n)$.

Teorema 5: Seja n um inteiro maior que 1 cuja fatoração em números primos é dada por:

$n = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot p_3^{\alpha 3} \cdot \ldots \cdot p_k^{\alpha k}$

então:

$$\varphi(n) = \left(p_1^{\alpha 1} - p_1^{\alpha 1-1}\right) \cdot \left(p_2^{\alpha 2} - p_2^{\alpha 2-1}\right) \cdot \ldots \cdot \left(p_k^{\alpha k} - p_k^{\alpha k-1}\right)$$

Demonstração: Faremos indução sobre *k*.

Para $k = 1$, temos $n = p_1^{\alpha 1}$

$\varphi(n) = p_1^{\alpha 1} - p_1^{\alpha 1-1}$, como já foi demonstrado.

Suponhamos, agora, o Teorema Válido para $k = r$.

Logo:

$$\varphi\left(p_1^{\alpha 1} p_2^{\alpha 2} p_3^{\alpha 3} \ldots p_r^{\alpha r}\right) = \left(p_1^{\alpha 1} - p_1^{\alpha 1-1}\right) \cdot \left(p_2^{\alpha 2} - p_2^{\alpha 2-1}\right) \cdot \ldots \cdot \left(p_r^{\alpha r} - p_r^{\alpha r-1}\right)$$

Como m.d.c. $\left(p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots \cdot p_r^{\alpha r}; p_{r+1}^{\alpha r+1}\right) = 1$

temos que:

$$\begin{aligned}
&\varphi\left(\left(p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots p_r^{\alpha r}\right) \cdot p_{r+1}^{\alpha r+1}\right) \\
&= \varphi\left(p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots p_r^{\alpha r}\right) \cdot \varphi\left(p_{r+1}^{\alpha r+1}\right) \\
&= \varphi\left(p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots p_r^{\alpha r}\right) \cdot \varphi\left(p_{r+1}^{\alpha r+1}\right) \\
&= \varphi\left(p_1^{\alpha 1} - p_1^{\alpha 1-1}\right) \cdot \left(p_1^{\alpha 1} - p_1^{\alpha 1-1}\right) \cdot \ldots \cdot \left(p_r^{\alpha r} - p_r^{\alpha r-1}\right) \cdot \left(p_r^{\alpha r+1} - p_r^{\alpha r}\right)
\end{aligned}$$

Concluindo, assim, a demonstração. □

Exemplo:

$$\begin{aligned}
&\varphi(400) = \varphi\left(2^4 \cdot 5^2\right) = \varphi\left(2^4\right) \cdot \varphi\left(5^2\right) \\
&= \left(2^4 - 2^3\right) \cdot \left(5^2 - 5\right) = (16 - 8) \cdot (25 - 5) \\
&= 8 \cdot 20 = 160.
\end{aligned}$$

Corolário: Para todo inteiro $n > 2$ $\varphi(n)$ é um inteiro par.

Demonstração: Dividimos a demonstração em dois casos distintos:

<u>1º caso:</u>

$n = 2^{\alpha}$; com $\alpha \geq 2$

$$\text{temos} \quad \varphi(n) = 2^{\alpha} - 2^{\alpha-1} = 2^{\alpha}\left(1 - \frac{1}{2}\right)$$

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

que é um número par.

2º caso:

$n = 2\alpha \cdot p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot ... \cdot p_\pi^{\alpha\pi}$

com *pi* primo maior que 2, portanto, *pi* também é ímpar.

Logo:

$\varphi(n) = \varphi(2^\alpha) \cdot \varphi(p_1^{\alpha 1}) \cdot \varphi(p_2^{\alpha 2}) \cdot ... \cdot \varphi(p_\pi^{\alpha\pi})$

Sendo assim, chame $\varphi(n) = \varphi(2^\alpha) \cdot \varphi(p_1^{\alpha 1}) \cdot \varphi(p_2^{\alpha 2}) \cdot ... \cdot \varphi(p_{\pi-1}^{\alpha\pi-1})$ de q

Então:

$\varphi(n) = q \cdot \varphi(p_\pi^{\alpha\pi})$

Daí:

$\varphi(n) = q \cdot \varphi(p_\pi^{\alpha\pi} - p_\pi^{\alpha\pi-1})$

$\varphi(n) = q \cdot p^{\alpha\pi-1} \cdot (p-1)$

como $p - 1$ é par, pois p é primo ímpar, temos $\varphi(n)$ é par. □

Teorema 6 (Teorema de Euler): Se *n* é um inteiro positivo se m.d.c. (*a*, *n*) = 1, então:

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

Para demonstrarmos o teorema acima, precisamos demonstrar um lema anteriormente.

Lema: Seja *a* e *n* > 1 inteiros tais que o m.d.c. (*a*, *n*) = 1, e que a_1, a_2, a_3, ..., $a_{\varphi(n)}$, os inteiros positivos menores que *n* e que são relativamente primos com *n*.

Então, cada um dos elementos abaixo

aa_1, aa_2, aa_3, ..., $aa_{\varphi(n)}$

será congruente módulo *n* a um dos inteiros:

a_1, a_2, a_3, ..., $a_{\varphi(n)}$

que não precisa estar nessa mesma ordem.

Demonstração: Afirmamos que escolhidos dois quaisquer inteiros da lista abaixo

$aa_1, aa_2, aa_3, ..., aa_{\varphi(n)}$

eles serão congruentes módulo n, ou seja

$aa_i \equiv aa_j \pmod{n}$

com i e j satisfazendo

$1 \leq i \leq \varphi(n)$ e $i \leq j \leq \varphi(n)$

como m.d.c. $(a, n) = 1$, então

$a_i \equiv a_j \pmod{n}$

que é um absurdo.

A recíproca procederá da seguinte forma:

m.d.c. $(a_i, n) = 1$ e o m.d.c. $(a, n) = 1$ por definição.

Daí, concluímos que $(aa_i, n) = 1$. Sendo assim, existe um único b_i, com $0 \leq b_i < n$, que satisfaz:

$a \cdot a_i \equiv b_i \pmod{n}$

Então, b_i assumirá um dos valores

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

por ser m.d.c. (b_i, n) = m.d.c. $(aa_i, n) = 1$

Portanto:

$aa_1; aa_2; ...; aa_{\varphi(n)}$ e

$a_1; a_2; ...; a_{\varphi(n)}$

são congruentes, numa certa ordem, módulo n. □

Demonstrado o lema acima, podemos agora provar o Teorema de Euler.

Vamos enunciá-lo mais uma vez.

Teorema 6 (Teorema de Euler): Se n é um inteiro positivo e m.d.c. $(a, n) = 1$, então:

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

Demonstração: O caso $n = 1$ é fácil, pois

$a^{\varphi(1)} \equiv a \equiv 1 \pmod{1}$

Com $n > 1$ usaremos o lema demonstrado anteriormente.

Para isso, sejam $a_1, a_2, ..., a_{\varphi(n)}$ os números inteiros positivos menores que n e relativamente primos com ele.

Como o m.d.c. $(a, n) = 1$, então

aa_1; aa_2; ...; $aa_{\varphi(n)}$ são congruentes módulo n aos números

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

não necessariamente nessa mesma ordem.

Ou seja,

$$aa_1 \equiv a_1' \text{ (mod. } n)$$
$$aa_2 \equiv a_2' \text{ (mod. } n)$$
$$\vdots$$
$$aa_{\varphi(n)} \equiv a_{\varphi(n)}' \text{ (mod. } n) \quad \square$$

Observação: a_1', a_2', ... $a_{\varphi(n)}$ é uma ordem estabelecida de $a_1, a_2, ..., a_{\varphi(n)}$.

Fazendo o produto de todas essas congruências temos:

$aa_1 \cdot a \cdot a_2 \cdot ... \cdot aa\varphi(n) \equiv a_1 \cdot a_2 \cdot ... \cdot a_{\varphi(n)}$ (mod. n)

Que após alguns ajustes podemos escrever da seguinte forma:

$$\underbrace{(a \cdot a \cdot ... \cdot a)}_{\varphi(n) \text{ vezes}} \cdot (a_1 \cdot a_2 \cdot ... \cdot a_{\varphi(n)}) \cong a_1' \cdot a_2' \cdot ... \cdot a'_{\varphi(n)} \text{ (mod. } n)$$

Como todo a_i é igual a um único a_j e pelo fato de m.d.c. ($a_1 \cdot a_2 \cdot ... \cdot a_{\varphi(n)}$; n) = 1, podemos, então, cancelar esse fator comum nos dois lados obtendo

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

Isso encerra a demonstração do Teorema de Euler.

Existe um resultado específico do Teorema de Euler que é muito utilizado em problemas de olimpíadas.

Esse resultado é conhecido como “Pequeno Teorema de Fermat”.

Corolário (Fermat): Se p é um número primo e se $p \nmid a$, então:
$a^{p-1} \equiv 1$ (mod. p)

Demonstração: Sabe-se, pelo Teorema de Euler, que:

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

onde n é inteiro positivo e o m.d.c. (a, n) = 1.

Se $n = p$, onde p é um número primo, então:

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

como $\varphi(p) = p - 1$, $\forall p$ primo, então:

$a^{p-1} \equiv 1 \pmod{p}$ □

4.1 Alguns resultados importantes

01. $\varphi(n) \leq n - \sqrt{n}$ para todo *n* inteiro positivo composto.

Demonstração: Seja $n = p_1^{\alpha 1} \cdot p_2^{\alpha 2} \cdot \ldots \cdot p_k^{\alpha k}$ a decomposição em fatores primos de *n* como

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

Temos:

$$\varphi(n) \leq n\left(1 - \frac{1}{p_i}\right)$$

Podemos garantir que, do fato de "*n*" ser composto, existe um primo $p_i \leq \sqrt{n}$.

Daí:

$$\varphi(n) \leq n\left(1 - \frac{1}{p_i}\right) \leq n\left(1 - \frac{1}{\sqrt{n}}\right)$$

$$\varphi(n) \leq n - \frac{n}{\sqrt{n}}$$

$$\varphi(n) \leq n - \sqrt{n}$$

02. Seja *n* um inteiro positivo.

Então:

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

Demonstração: Dados os inteiros 1, 2, 3, ..., *n* vamos dividi-los em classes seguindo o critério abaixo.

O inteiro *m* está na classe C_d se o m.d.c. (*m*, *n*) = *d*.

Percebe-se, então, que se *m* pertence à classe C_d, isto é:

m.d.c. (m, n) = d se, e somente se

$$\text{m.d.c.}\left(\frac{m}{d}, \frac{n}{d}\right) = 1$$

Logo, podemos garantir que o número de inteiros em C_d é o número de inteiros que não excedem $\frac{n}{d}$ que são coprimos com $\frac{n}{d}$.

Daí a quantidade de $C_d = \varphi\left(\frac{n}{d}\right)$

Como dividimos 1, 2, 3, 4, ..., *n* em classes disjuntas e cada inteiro está exatamente em uma dessas classes.

Portanto:

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

5 FUNÇÃO DE MÖBIUS

Definição: Para n inteiro positivo, definimos:

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

Exemplo:

$$\mu(20) = \mu\left(2^2 \cdot 4\right) = 0$$

$$\mu(42) = \mu(2 \cdot 3 \cdot 7) = (-1)^3 = -1$$

$$\mu(1) = 1$$

Vale ressaltar que, se p é um número primo, então:

$\mu(p) = (-1)^r = -1$

e para $k \geq 2$

$\mu(p^k) = \mu(p^2 \cdot p^{k-2}) = 0$

Teorema 7: A função μ denominada função de Möbius é multiplicativa.

Demonstração: Suponha m, n inteiros positivos com m e n primos entre si, isto é, m.d.c. $(m, n) = 1$

Devemos mostrar que:

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

Se para um número primo p temos $p^2 | m$ ou $p^2 | n$, então $p^2 | m \cdot n$, daí pela definição da função de Möbius $\mu(m \cdot n) = 0$.

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

Assumiremos, agora, que m e n são livres de quadrados, isto é:

$m = p_1 \cdot p_2 \cdot \ldots \cdot p_\pi$ e $n = q_1 \cdot q_2 \cdot \ldots \cdot q_s$

onde p_i e q_j são números primos com $1 \leq i \leq r$ e $1 \leq j \leq s$ todos distintos.

Temos, então:

$$\begin{aligned} \mu(m \cdot n) &= \mu\left(p_1 \cdot p_2 \cdot \ldots p_\pi \cdot q_1 \cdot q_2 \cdot \ldots \cdot q_s\right) \\ &= (-1)^{r+s} \\ &= (-1)^r \cdot (-1)^s \\ &= \mu(m) \cdot \mu(n) \end{aligned}$$

□

Exemplo:

$$\mu(21)=\mu(3\cdot 7)=\mu(3)\cdot\mu(7)=(-1)\cdot(-1)=1$$

por outro lado

$$\mu(21)=\mu(3\cdot 7)=(-1)^2=1$$

Um resultado bastante importante em teoria dos números é denominado de Fórmula de Inversão de Möbius.

Ela nos permite explicitar uma função aritmética em termos de uma outra.

Antes de demonstrarmos este resultado, faremos uma abordagem sobre um resultado preliminar.

Vejamos:

Seja *n* um número inteiro positivo e seja *d* um divisor positivo de *n*.

Então:

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

O Somatório acima representa a soma dos valores de μ aplicado em todos os divisores positivos de *n*.

Exemplo:

Para $n = 1$, temos:

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

Para n > 1 faremos em dois casos:

1º caso

$n = p^k$; onde *p* é um número primo.

Chamaremos, então:

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

Logo:

$$\begin{aligned}F(n)=F(p^k)&=\sum_{d|n}\mu(d)\\&=\mu(1)+\mu(p)+\mu(p^2)+\ldots+\mu(p^k)\\&=1+(-1)^1+0+\ldots+0\\&=1-1=0\end{aligned}$$

2º caso

$n = p_1^{k1} \cdot p_2^{k2} \cdot ... \cdot p_r^{kr}$; onde para $1 \leq i \leq \pi$, *pi* é um número primo.

Logo:

$$\begin{aligned} \mathrm{F}(n) &= \left(p_1^{k1} \cdot p_2^{k2} \cdot ... \cdot p_r^{kr} \right) = \\ &= \mathrm{F}\left(p_1^{k1} \right) \cdot \mathrm{F}\left(p_2^{k2} \right) \cdot ... \cdot \mathrm{F}\left(p_r^{kr} \right) \\ &= 0 \cdot 0 \cdot ... \cdot 0 = 0 \end{aligned}$$

Daí,

Para todo inteiro positivo $n \geq 1$, tem-se:

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

Exemplo:

$$\begin{aligned} \sum_{d|20} \mu(d) &= \mu(1) + \mu(2) + \mu(4) + \mu(5) + \mu(10) + \mu(20) \\ &= 1 + (-1) + 0 + (-1) + (-1)^2 + 0 \\ &= 0 + 0 + 0 + 0 = 0 \end{aligned}$$

Teorema 8 (Fórmula de Inversão de Möbius): Sejam *f* e *g* duas funções aritméticas relacionadas da seguinte forma:

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

Então:

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

Demonstração: Obviamente, temos:

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

A última soma dupla é sobre todos os pares de inteiros positivos (c,d) tais que *d*|*n* e $c \mid \left(\frac{n}{d} \right)$. E como *d*|*n* e $c \mid \left(\frac{n}{d} \right)$ se e somente se *c*|*n* e $d \mid \left(\frac{n}{c} \right)$, temos:

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

De acordo com o resultado preliminar apresentado neste mesmo capítulo, temos que a soma:

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

tem o valor 0 se $\frac{n}{c} > 1$ e tem o valor 1 se $\frac{n}{c} = 1$ ou n = c. Assim sendo, temos, finalmente:

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

Observe que

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

Podemos citar como caso particular da Fómula da Inversão de Möbius, o caso das funções aritméticas *d*(*n*) e *s*(*n*) temos, por definição:

$$d(n) = \sum_{e|n} 1 \text{ e } s(n) = \sum_{d|n} d$$

e, portanto, pela Fórmula de Inversão de Möbius:

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

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

fórmulas válidas para todo n $\geq$ 1.

6 RAÍZES PRIMITIVAS

O Teorema de Euler nos diz que $a^{\varphi(n)} \equiv 1$ quando m.d.c. (a, n) = 1.

Porém, existem potências de a menores que $a^{\varphi(n)}$ que são congruentes a 1 módulo n.

Para vermos essa possibilidade, precisamos definir o conceito de ordem módulo n.

Definição: Seja n > 1 e m.d.c. (a, n) = 1. A ordem de um inteiro a módulo n é o menor inteiro positivo k, tal que $a^k \equiv 1$ (mod. n).

Exemplo: Vamos calcular as potências de 3 módulo 8.

$3^1 \equiv 3$ (mod. 8)

$3^2 \equiv 1$ (mod. 8)

$3^3 \equiv 3$ (mod. 8)

$3^4 \equiv 1$ (mod. 8)

.
.
.

Logo, a ordem de 3 módulo 8 é 2.

Cabe aqui uma observação.

Observação: Se dois inteiros são congruentes módulo n, então eles possuem a mesma ordem módulo n.

Exemplo:

$$11 \equiv 3 \text{ (mod. 8)}$$

$3^1 \equiv 3$ (mod. 8)		$11^1 \equiv 3$ (mod. 8)
$3^2 \equiv 1$ (mod. 8)	e	$11^2 \equiv 1$ (mod. 8)
$3^3 \equiv 3$ (mod. 8)		$11^3 \equiv 3$ (mod. 8)

Veja que:

A ordem de 3 módulo 8 e a ordem de 11 módulo 8 é 2.

Vamos provar a observação acima.

Teorema 9: Sejam a e b dois inteiros tal que $a \equiv b$ (mod. n). E k é a ordem de a módulo n. Logo, a ordem de b módulo n também será k.

Demonstração: Sabendo que o inteiro positivo k é a ordem de a módulo n.

Logo podemos afirmar que:

$a^k \equiv 1$

Como, $a \equiv b$ (mod. n), então

$a^k \equiv b^k$ (mod. n)

Sabendo que $a^k \equiv 1$, temos que

$b^k \equiv 1$ (mod. n)

Logo, k é a ordem de b módulo n. □

Teorema 10: Seja k a ordem do inteiro a módulo n.

Então, $a^h \equiv 1$ (mod. n) se, e somente se, $k|h$.

Demonstração:

($\Leftarrow$) Suponha $k|h$.

Logo, existe um inteiro t tal que

$k \cdot t = h$

Como $a^k \equiv 1$ (mod. n), temos que

$(a^k)^t \equiv 1^t$ (mod. n)

$a^{k \cdot t} \equiv 1$ (mod. n)

$a^h \equiv 1$ (mod. n)

($\Rightarrow$) $a^h \equiv 1$ (mod. n).

Temos, pelo algoritmo de Euclides, que existem inteiros q e r, tais que:

$h = qk + r$

Com $0 \leq r < k$

Daí,

$a^h = a^{qk+r} = a^{qk} \cdot a^r = (a^q)^k \cdot a^r$

Como $a^h \equiv 1$ (mod. n) e $a^k \equiv 1$ (mod. n), tem-se:

$1 \equiv a^r$ (mod. n)

Como k é a ordem de a módulo n e $0 \leq r < k$, então $r = 0$.

Logo:

$h = qk$ e $k|h$. □

Ressaltamos que o teorema demostrado há pouco nos diz de maneira elegante que a ordem de um inteiro módulo *n* só pode ser um divisor de $\varphi(n)$.

Vejamos:

Corolário: Se o inteiro *a* tem ordem *k* módulo *n*, então $k \mid \varphi(n)$.

Demonstração: Pelo Teorema de Euler, temos $a^{\varphi(n)} \equiv 1$ (mod. *n*).

Logo, pelo teorema anterior, sabe-se que:

$k \mid \varphi(n)$ □

Exemplo:

A ordem de um inteiro *a* módulo 18 só pode ser um divisor $\varphi(18)$,ou seja:

$\varphi(18) = \varphi(2 \cdot 9) = \varphi(2) \cdot \varphi(9) = \varphi(2) \cdot \varphi(3^2)$

$\varphi(18) = 1 \cdot (3^2 - 3) = 6.$

Logo, a ordem será 1, 2, 3 ou 6.

Teorema 11: Se *a* tem ordem *k* módulo *n*, então $a^i \equiv a^j$ (mod. *n*) se, e somente se, $i \equiv j$ (mod. *k*).

Demonstração:

($\Longrightarrow$) Suponha que $a^i \equiv a^j$ (mod. *n*), com $i \geq j$.

Como *a* é relativamente primo com *n*, então:

$a^i \equiv a^j$ (mod. *n*)

$a^{i-j} \equiv 1$ (mod. *n*)

Logo, $k|(i - j)$ e, portanto, , $i \equiv j$ (mod. *k*).

($\Longleftarrow$) Assumimos, agora, que , $i \equiv j$ (mod. *k*), logo, $k|(i - j)$. Portanto, existe um inteiro *q* tal que $i = k \cdot q + j$.

Daí,

$a^i \equiv a^{kq+j} \equiv (a^k)^q \cdot a^j$ (mod. *n*)

Como $a^k \equiv 1$ (mod. *n*)

Então

$a^i \equiv a^j$ (mod. *n*)

Podemos concluir mediante o teorema acima que, se o inteiro *a* possui ordem *k*, então

$a, a^2, ..., a^k$ são incongruentes módulo *n*.

Se não, vejamos:

Sejam $1 \leq i \leq j \leq k$.

Se $a^i \equiv a^j$ (mod. n) então

$i \equiv j$ (mod. k)

$i = qk + j$ para algum q inteiro

logo $q = 0$ e $i = j$. □

Definição: Se o m.d.c. (a, n) = 1 e a tem ordem $\varphi(n)$ módulo n, então a é denominado raiz primitiva de n.

Exemplo:

3 é raiz primitiva módulo 7, pois:

* m.d.c. (3, 7) = 1 e

$3^1 \equiv 3$ (mod. 7)

$3^2 \equiv 2$ (mod. 7)

$3^3 \equiv 6$ (mod. 7)

$3^4 \equiv 4$ (mod. 7)

$3^5 \equiv 5$ (mod. 7)

$3^6 \equiv 1$ (mod. 7)

Como $\varphi(7) = 7 - 1 = 6$ e não existe $1 \leq k < 6$, tal que $3^k \equiv 1$ (mod. 7), então 3 é raiz primitiva módulo 7.

Um resultado importante afirma que, se n tem uma raiz primitiva, então n possui $\varphi(\varphi(n))$ raízes primitivas.

Para demonstrarmos esse resultado, precisamos do seguinte lema.

Lema: Seja m.d.c. (a, n) = 1 e dados $a_1, a_2, ..., a_{\varphi(n)}$ inteiros positivos menores que n e primos com n.

Se a é uma raiz primitiva de n, então:

$a, a^2, ..., a^{\varphi(n)}$

são congruentes módulo n a $a_1, a_2, ..., a_{\varphi(n)}$ em alguma ordem.

Demonstração:

Como o m.d.c. (a; n) = 1, então toda potência de a também será relativamente primo com n.

Podemos afirmar que cada a^k é congruente módulo n a algum a_i.

E sabendo que:

$a, a^2, ..., a^{\varphi(n)}$ são incongruentes módulo *n*, então essas potências de *a* são congruentes módulo *n* a algum dos valores abaixo:

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

Demonstração:

Suponhamos que *a* é uma raiz primitiva de *n*. Pelo teorema anterior, qualquer outra raiz primitiva de *n* se encontra entre os elementos do conjunto:

$$\left\{a, a^2, ..., a^{\varphi(n)}\right\}$$

Mas, o número de potências a^k, onde $1 \leq k \leq \varphi(n)$, que têm ordem $\varphi(n)$, é igual ao número de inteiros *k* tais que o m.d.c.(k, $\varphi(n)$) = 1, e como o número de tais inteiros é $\varphi(\varphi(n))$, segue-se que *n* tem exatamente $\varphi(\varphi(n))$ raízes primitivas.

7 LISTA DE EXERCÍCIOS COM SOLUÇÕES

1. Para $n \geq 3$ vale

$$\varphi(n) \equiv 0 \bmod 2.$$

Resposta:

Se n = 2^a com a ≥ 2, temos

$$\varphi(n) = 2^{a-1} \equiv 0 \bmod 2.$$

Se n = $p^a \cdot k$ com $a, k \in \mathbb{N}$, $2 < p \in \mathbb{P}$ e $p \nmid k$, temos também

$\varphi(n) = \varphi(p^a)\ \varphi(k) = p^{a-1}(p-1)\ \varphi(k) \equiv 0 \bmod 2$, pois $p-1$ é par.

$n-1$ é claramente uma cota superior para $\varphi(n)$.

Uma cota inferior é dada na seguinte.

2. Seja $2 \leq n \in \mathbb{N}$. Então

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

Resposta:

Seja $n = 2^{a_0} \cdot p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_r^{a_r}$ com $2 < p_1 < p_2 < \ldots < p_r$ e inteiros a0 ≥ 0, $a_1, a_2, \ldots, a_r \geq 1$.

$$\varphi(n) = \varphi(2^{a_0}) \cdot p_1^{a_1-1} \cdot p_2^{a_2-1} \cdot \ldots \cdot p_r^{a_r-1} \cdot (p_1-1) \cdot (p_2-1) \cdot \ldots \cdot (p_r-1)$$

Onde $\varphi(2^{a_0}) = 1$ se $a_0 = 0$ ou 2^{a_0-1} se $a_0 \geq 1$. Segue

$$\varphi(n) \geq \varphi(2^{a_0}) \cdot p_1^{\frac{a_1-1}{2}} \cdot p_2^{\frac{a_2-1}{2}} \cdot \ldots \cdot p_r^{\frac{a_r-1}{2}} \cdot \sqrt{p_1}\sqrt{p_2} \cdot \ldots \cdot \sqrt{p_r} =$$

$$= \frac{\varphi(2^{a_0})}{2^{\frac{a_0}{2}}} \cdot 2^{\frac{a_0}{2}} \cdot p_1^{\frac{a_1}{2}} \cdot p_2^{\frac{a_2}{2}} \cdot \ldots \cdot p_r^{\frac{a_r}{2}} = \frac{\varphi(2^{a_0})}{2^{\frac{a_0}{2}}}\sqrt{n} \geq \frac{1}{2}\sqrt{n}.$$

Usa-se aqui a desigualdade $x - 1 \geq \sqrt{x}$ válida para $x \geq 3$. Provar isto! Fazer o gráfico das funções reais $y = x-1$ e $y = \sqrt{x}$. Onde as funções se interceptam?

3. Seja $n \in \mathbb{N}$, $n \equiv 1 \bmod 2$ e $n \neq 0 \bmod 5$. Então n divide algum número da forma 1111...1111.

Resposta:

Temos m.d.c.(n, 10) = 1 e m.d.c.(9n, 10) = 1. Logo, pelo teorema de Euler

$10^{\varphi(9n)} \equiv 1 \bmod 9n$, ou seja, $10^{\varphi(9n)} - 1 = 9nk$.

Segue

$$n \text{ divide } \frac{10^{\varphi(9n)}-1}{9} = \frac{9999...9999}{9} = 1111...1111.$$

4. Para todo $k \geq 3$ e todo $a \in \mathbb{Z}$ ímpar vale

$$a^{2k-2} \equiv 1 \bmod 2^k.$$

Resposta:

Esta afirmação é verdadeira para $k = 3$, pois sempre $a^2 \equiv 1 \bmod 8$. Provaremos a afirmação por indução sobre k:

Suponhamos $a^{2^{k-2}} \equiv 1 \bmod 2^k$ já provado para algum $k \geq 3$. Então

$a^{2^{k-2}} = 1 + \ell \cdot 2^k$ para algum $\ell \in \mathbb{Z}$ e segue

$$a^{2^{k-1}} = \left(a^{2^{k-1}}\right)^2 = \left(1 + \ell \cdot 2^k\right)^2 = 1 + 2\ell \cdot 2^k + \ell^2 \cdot 2^{2k} =$$

$$= 1 + \ell\left(1 + \ell^{2^{k-1}}\right)2^{k+1} \equiv 1 \bmod^{2k+1}.$$

Portanto vale $a^{2^{k-2}} \equiv 1 \bmod 2^k$ para todo k ≥ 3 e todo a ímpar.

5. a) Se $a \in \mathbb{Z}$ é decomponível como $n = rs$ com $r, s \geq 3$ e m.d.c.$(r, s) = 1$, então não existe raíz primitiva mod n.

b) Se $n = 2^k$ com $k \geq 3$, então não existe raiz primitiva mod n.

Resposta:

a) Se $a \in \mathbb{Z}$ com m.d.c.$(a, n) = 1$, segue m.d.c.(a, r) = m.d.c.$(a, s) = 1$. Sabemos que $\varphi(n) \equiv \varphi(r) \equiv \varphi(s) \equiv 0 \bmod 2$, pois $r, s \geq 3$. Usando-se o teorema de Euler, vemos

$$a^{\frac{\varphi(n)}{2}} = a^{\frac{\varphi(rs)}{2}} = a^{\frac{\varphi(r)\varphi(s)}{2}} = \begin{cases} \left(a^{\varphi(r)}\right)^{\frac{\varphi(s)}{2}} \equiv 1^{\frac{\varphi(s)}{2}} \equiv 1 \bmod r \\ \left(a^{\varphi(s)}\right)^{\frac{\varphi(r)}{2}} \equiv 1^{\frac{\varphi(r)}{2}} \equiv 1 \bmod s \end{cases}$$

Logo, $a^{\frac{\varphi(n)}{2}} \equiv 1 \bmod r$ e $a^{\frac{\varphi(n)}{2}} \equiv 1 \bmod s$. Segue

$$a^{\frac{\varphi(n)}{2}} \equiv 1 \bmod n,$$

Pois m.d.c.$(r, s) = 1$. Isto significa $\mathbf{o}n(a) \leq \dfrac{\varphi(n)}{2}$ para qualquer a: Não pode existir raiz primitiva mod n.

b) Temos $\varphi(2^k) = 2^{k-1}$. Observando

$$a^{\frac{\varphi(2^k)}{2}} = a^{2^{k-2}} \equiv 1 \bmod 2^k.$$

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

Resposta:

$2^{\varphi(5^{2000})} \equiv 1 (\text{módulo} 5^{2000})$, pelo teorema de Euler. Portanto, existe $b \in \mathbb{N}$ com $2^{\varphi(5^{2000})} = 5^{2000} b + 1$, e teremos $2^{2000+\varphi(5^{2000})} = 10^{2000} b + 2^{2000}$, e portanto os 20000 últimos dígitos de $2^{2000+\varphi(5^{2000})}$ coincidem com a representação decimal de 2^{2000}, que tem no máximo 667 dígitos, pois $23 < 10 \Longrightarrow 2^{2000} < 2^{3.667} < 10^{667}$. Desta forma, $2^{2000+\varphi(5^{2000})}$ tem pelo menos2000 – 667 = 1333 zeros consecutivos dentre as 2000 últimas casas decimais, de modo que $n = 4 \cdot 5^{1999} + 2000$ satisfaz as condições do enunciado (pois $\varphi(5^{2000}) = \varphi(5^{1999})$).

7. Se $k \geq 3$, então não existe nenhuma raiz primitiva módulo 2^k.

Resposta:

Basta provar que não existe raiz primitiva módulo 8, e isso segue do fato que se a é impar, $a = 2r + 1$, $r \in \mathbb{Z} \Longrightarrow a^2 = 4r(r + 1) + 1 \equiv 1$ (módulo 8)

8. Sejam p um número primo, e $a \in \mathbb{Z}$ raiz primitiva módulo p. então $a + p$ é raiz primitiva módulo p^2.

Resposta:

Por hipótese, $ord_p a = ord_p(a + p) = p - 1$. Portanto $p-1 \mid ord_{p^2} a$ (pois $a^t \equiv 1$ (módulo p^2) $\Longrightarrow a^t \equiv 1$ (módulo p)), e, como $ord_{p^2} a \mid \varphi(p^2) = p(p-1)$, devemos ter $ord_{p^2} a = p-1$ ou $ord_{p^2} a = p(p-1) = \varphi(p^2)$. Do mesmo modo, $ord_{p^2}(a+p) = p-1$ ou $ord_{p^2}(a+p) = p(p-1) = \varphi(p^2)$.

Basta provar, portanto, que $ord_{p^2} a \neq p-1$ ou $ord_{p^2}(a+p) \neq p-1$.

Suponha que $ord_{p^2} a = p-1$. Portanto, $a^{p-1} \equiv 1$ (módulo p^2), e então $(a+p)^{p-1} = a^{p-1} + (p-1)pa^{p-2} + C_{p-1}^2 a^{p-3} \cdot p^2 + \ldots \equiv 1 + (p-1)pa^{p-2}$ (módulo p^2), pois p^2 não divide $(p-1)pa^{p-2}$, donde $ord_{p^2}(a+p) \neq p-1$.

9. Mostre que existe n natural tal que os mil últimos dígitos de 2^n pertencem a {1, 2}.

Resposta:

Observamos inicialmente que para todo $k \in \mathbb{N}$ existe um número m_k de k algarismos, todos 1 ou 2, divisível por 2^k.

De fato, $m_1 = 2$ e $m_2 = 12$ satisfazem o enunciado.

Seja $m_k = 2^k \cdot r_k$, $r_k \in \mathbb{N}$. Se r_k é par, tome $m_{k+1} = 2 \cdot 10k + m_k = 2^{k+1}(5^k + r_k/2)$, e se r_k é ímpar, tome $m_{k11} = 10^k + m_k = 2^{k-1}(5^k + r_k)/2$.

10. Existe alguma raiz primitiva módulo n, se, e só se, $n = 2$, $n = 4$, $n = p^k$ ou $n = 2p^k$, onde p é primo ímpar.

Resposta:

Pelos resultados anteriores, basta provar que se p é primo ímpar, então existe raiz primitiva módulo p, ou seja, existe $a \in (\mathbb{Z}/p\mathbb{Z})^*$ com $ord_p a = p - 1$.

Temos, portanto, $p - 1 = \sum_{d|p-1} N(d)$. O resultado seguirá dos dois lemas seguintes:

Lema 1: $N(d) \leq \varphi(d)$ para todo d divisor de $p - 1$.

Prova: Se $N(d) > 0$ então existe existe $a \in (\mathbb{Z}/p\mathbb{Z})^*$ com $ord_p a$. Se $ord_p a = d$, então $a^d = 1$ e, para $0 \leq k < d$ as classes de a^k são todas distintas módulo p, e $(a^k)^d = 1$. Como a equação $x^d - 1 = 0$ tem no máximo d raízes distintas em $\mathbb{Z}/p\mathbb{Z}$ (pois $\mathbb{Z}/p\mathbb{Z}$ é um corpo), suas raízes são exatamente a^k, $0 \leq k < d$. Por outro lado, $ord_p a^k = d \Longrightarrow$ m.d.c.$(k, d) = 1$, pois se $r > 1$ é tal que $r \mid k$ e $r \mid d$ então $(a^k)^{d/r} = (a^d)^{k/r} \equiv 1$ (módulo p), logo $ord_p(a^k) \leq d/r < d$. Desta forma, $\{b \in (\mathbb{Z}/p\mathbb{Z})^* | ord_p b = d\} \subset \{a^k, 0 \leq k < d \text{ e m.d.c. } (k, d) = 1\}$, portanto $N(d) \leq \varphi(d)$.

Lema 2: $\sum_{d|n} \varphi(d) = n$, para todo $n \in \mathbb{N}$.

Prova: Considere os n números racionais $1/n$, $2/n$, ... n/n. Ao simplifica-los, aparecem exatamente $\varphi(d)$ deles com denominador d, para cada divisor d de n. Portanto, $\sum_{d|n} \varphi(d) = n$.

Fim da prova: Do Lema 2 segue que $\sum_{d|p-1} \varphi(d) = p - 1$ e, como $p - 1 = \sum_{d|p-1} N(d)$ e $N(d) \leq \varphi(d)$ para todo d, devemos ter $N(d) = \varphi(d)$ para todo d. Em particular, $N(p - 1) = \varphi(p - 1) > 0 \Rightarrow$ existem raízes primitivas módulo p.

11. Mostre que existem infinitos números da forma

$$20000 \ldots 009$$

que são múltiplos de 2009.

Resposta:

O problema é equivalente a encontrar infinitos naturais *k* tais que

pois 2000 é invertível módulo 2009. Como m.d.c. (10, 2009) = 1, pelo teorema de Euler-Fermat temos que $10^{\varphi(2009)} \equiv 1 \pmod{2009} \Longrightarrow 10^{\varphi(2009)t} \equiv 1 \pmod{2009}$ para todo $t \in \mathbb{N}$, logo basta tomar $k = \varphi(2009)t + 3$.

12. Encontre um número n tal que $2^n > 10^{2000}$ e 2^n tenha entre suas 2000 últimas casas decimais pelo menos 1000 zeros consecutivos.

Resposta:

Sabemos que $2^{\varphi(5^{2000})} \equiv 1 \pmod{5^{2000}}$ pelo teorema de Euler-Fermat. Portanto existem $b \in \mathbb{N}$ com

$$2^{\varphi(5^{2000})} = 5^{2000}b + 1 \Rightarrow 2^{2000+\varphi(5^{2000})} = 10^{2000}b + 2^{2000}.$$

Logo os 2000 últimos dígitos de $2^{2000+\varphi(5^{2000})}$ coincidem com a representação decimal de 2^{2000}, que tem no máximo 667 dígitos pois $2^{2000} < (2^3)^{667} < 10^{667}$. Desta forma, há pelo menos 2000 – 667 = 1333 zeros consecutivos dentre as 2000 últimas casas decimais de $2^{2000+\varphi(5^{2000})}$ e assim n = $\varphi(5^{2000})$ + 2000 = $4 \cdot 5^{1999}$ + 2000 satisfaz as condições do enunciado.

13. Mostre que não existe inteiro *x* tal que $103 \mid x^3 - 2$.

Resposta:

Note primeiramente que 103 é primo. Agora suponha que $x^3 \equiv 2 \pmod{103}$, de modo que $103 \nmid x$. Elevando ambos os lados desta congruência a (103 – 1)/3 = 34, obtemos $x^{102} \equiv 2^{34} \pmod{103}$ e sabemos pelo teorema de Euler-Fermat que $x^{102} \equiv 1 \pmod{103}$. Porém, fazendo as contas, obtemos que $2^{34} \equiv 46 \pmod{103}$, que é uma contradição. Logo não há inteiro *x* tal que $103 \mid x^3 - 2$.

Utilizando o mesmo raciocínio da questão anterior, temos que se *p* é um primo tal que $p \equiv 1 \pmod 3$ e $p \nmid a$, então uma condição necessária para $x \equiv a \pmod p$ tenha solução em *x* é que $a^{(p-1)/3} \equiv 1 \pmod p$. Esta condição também é suficiente, pela existência de raízes primitivas módulo *p*.

14. Encontre um número positivo $k < 50$ tal que $a^k \equiv 1 \pmod{99}$ para todo inteiro a primo relativo com 99.

    Resposta:

    Temos $99 = 3^2 \cdot 11$, $\varphi(3^2) = 6$ e $\varphi(11) = 10$, e, se m.d.c.(a, 99) = 1 então m.d.c.(a, 3^2) = 1 e m.d.c.(a, 11) = 1. Como 30 é múltiplo de 6 e de 10, temos que, se m.d.c.(a, 99) = 1, então $a^{30} \equiv 1 \pmod{3^2}$ e $a^{30} \equiv 1 \pmod{11}$, donde $a^{30} \equiv 1 \pmod{99}$.

15. Mostre que para todo inteiro a temos que $a^{561} \equiv a \pmod{561}$ e $a^{1105} \equiv a(1105)$, mas 561 e 1105 não são primos, o que mostra que o recíproco do pequeno teorema de Fermat é falso.

    Resposta:

    Note que $561 = 3 \cdot 11 \cdot 17$, e 560 é múltiplo de 3 – 1, de 11 – 1 e de 17 – 1. Analogamente, $1105 = 5 \cdot 13 \cdot 17$, e 560 é múltiplo de 5 – 1, de 13 – 1 e de 17 – 1.

16. Mostre que $a^{12} \equiv b^{12} \pmod{91} \Leftrightarrow$ m.d.c. (a, 91) = m.d.c. (b, 91).

17. (OBM 1991) Demonstre que existem infinitos múltiplos de 1991 que são da forma 19999...99991.

    Resposta:

    Note que 19999...99991, com n 9's é igual a $2 \cdot 10^{n+1} - 9$, e $1991 = 2 \cdot 10^3 - 9$, donde $2 \cdot 10^3 \equiv 9 \pmod{1991}$. Como $2^{k \cdot \varphi(1991)} \equiv 1 \pmod{1991}$, $\forall k \in \mathbb{N}$, temos $2 \cdot 10^{k \cdot \varphi(1991)+3} \equiv 9 \pmod{1991}$, $\forall k \in \mathbb{N}$, e logo $2 \cdot 10^{k \cdot \varphi(1991)+3} - 9$ é múltiplo de 1991, para todo $k \in \mathbb{N}$.

18. Demonstre que se m.d.c.(a, b) = 1, então todos os divisores primos ímpares de $a^2 + b^2$ são da forma $4k + 1$.

    Resposta:

    Seja p um primo ímpar que divide $a^2 + b^2$. Como m.d.c.(a, b) = 1, então $p \nmid a$ ou $p \nmid b$. Suponhamos sem perda de generalidade que $p \nmid b$. Então b é invertível módulo p, e $(ab^{-1})^2 \equiv -1 \pmod{p}$. Se p fosse da forma $4k + 3$, teríamos $(ab^{-1})^{p-1} = ((ab^{-1})^2)^{2k+1} \equiv (-1)^{2k+1} = -1 \pmod{p}$, contradizendo o teorema de Euler-Fermat. Assim, p deve ser da forma $4k + 1$.

19. Demonstre que existem infinitos primos da $4k + 1$.

Resposta:

Suponha por absurdo que $p_1, p_2, ..., p_k$ sejam todos os primos da forma $4k + 1$. Seja $n = 2p_1p_2...p_k$. Temos que $n^2 + 1$ é ímpar, e portanto, pelo exercício anterior, qualquer fator primo de $n^2 + 1$ deve ser da forma $4k + 1$, ou seja, deve ser algum dos p_j, absurdo, pois $n^2 + 1 \equiv 1 \pmod{p_j}$ para todo j.

20. (IMO 2003) Seja p um número primo ímpar. Demonstre que existe um primo q tal que para todo n, o número $n^p - p$ não é divisível por q.

Resultado:

Seja $N = (p^p - 1)/(p - 1) = 1 + p + p^2 + ... + p^{p-1} \equiv p + 1 \not\equiv 1 \pmod{p^2}$. Então N tem um fator primo q com $q \not\equiv 1 \pmod{p^2}$. Temos que $p^p \not\equiv 1 \pmod{q}$, mas $p \not\equiv 1 \pmod{q}$, senão $N = 1 + p + p^2 + ... + p^{p-1} \equiv 1 + 1 + 1 + ... + 1 = p \pmod{q}$, donde $q \mid p$, e logo $p = q \mid N$, contradição, pois $N \equiv 1 \pmod{p}$. Suponha agora que $q \mid n^{p-p}$ para algum inteiro n. Então $n^p \equiv p \not\equiv 1 \pmod{q}$, e $n^{p^2} \equiv p \not\equiv 1 \pmod{q}$. Pelo teorema de Euler-Fermat, também temos $n^{q-1} \equiv 1 \pmod{q}$. Como $q \not\equiv 1 \pmod{p^2}$, m.d.c.$(p^2, q - 1) \mid p$, e logo existem x, y inteiros com $p^2x + (q - 1)y = p$, e $n^p = (n^{p^2})^x(n^{q-1})^y \equiv 1^x1^y = 1 \pmod{q}$, absurdo.

21. (Putman 1972) Prove que não existe inteiro positivo $n > 1$ tal que $n|2^n - 1$.

Resposta:

Suponha, por absurdo, que existe um inteiro positivo $n > 1$ com essa propriedade e que k é o menor dentre eles. Se $d = ord_k2$, então $d \mid k$. Como $2^d \equiv 1 \pmod{k}$, temos $2^d \equiv 1 \pmod{d}$. Em virtude da minimalidade de k, temos $d = 1$ ou $d = k$. No primeiro caso, teríamos $k = 1$ produzindo uma contradição. No segundo caso, em decorrência do teorema anterior, $k \mid \varphi(k)$. Entretanto, se $k > 1$, $\varphi(k) \leq k - 1$ e obtemos assim um absurdo.

22. (Leningrado 1990) Prove que para todos os inteiros $a > 1$ e n, $n|\varphi(a^n - 1)$.

Resposta:

Se $k = ord_an - 1a$, como $a^n \equiv 1 \pmod{a^n - 1}$, temos $k \mid n$ e consequentemente $k \leq n$. Não podemos ter $k < n$ porque $a^n - 1 \mid a^k - 1 \Longrightarrow a^n - 1 \leq a^k - 1$. Assim, $k = n$ e usando o teorema anterior podemos concluir que $k \mid \varphi(a^n - 1)$.

23. Mostre que:

a) $ord_{3^n}2 = 2 \cdot 3^{n-1}$

b) Se $2^m \equiv -1 \pmod{3^n}$, então $3^{n-1} \mid m$.

Resposta:

Provaremos por indução que $2^{3^k}+1 = 3^{k+1}m_k$ com $3 \nmid m_k$. Suponha que a afirmação vale para *k*. Provemos para *k* + 1:

$$\begin{aligned} 2^{3k+1} &= (3^{k+1}m_k - 1)^3 \\ &= 3^{3k+3}m_k^3 - 3^{2k+3}m_k^2 + 3^{k+2}m_k - 1 \\ &= 3^{k+2}(3^{2k+1}m_k^3 - 3^{k+1} + m_k) - 1 \\ &= 3^{k+2}m_{k+1} - 1 \end{aligned}$$

Claramente $3 \nmid m_{k+1}$. Voltemos ao problema. Seja $b = ord_{3^n} 2$, então $b \mid \varphi(3^n) = 2 \cdot 3^{n-1}$. Temos duas possibilidades: ou $b = 2 \cdot 3^j$ ou $b = 3^j$. Como $2^{3^{n-1}} \equiv -1 \pmod{3^n}$ e $3^j \mid 3^{n-1}$ se $j \leq n - 1$, devemos ter $b = 2 \cdot 3^j$. Assim, $(2^{3^j}-1)(2^{3^j}+1) \equiv 1 \pmod{3}^n$. Usando que $2^{3^j} - 1 \equiv 1 \pmod 3$, temos $2^{3^j} \equiv -1 \pmod{3^n}$. Novamente pelo lema provado no início, $3j \geq 3n - 1$ e assim $b = 2 \cdot 3^{n-1}$. Para o item b), de $2^m \equiv -1 \pmod{3^n}$, podemos concluir que $2^{2m} \equiv 1 \pmod{3}^n$. Daí, $2 \cdot 3^{n-1} \mid 2m$ e o resultado segue.

24. (Bulgária 1997) Encontre todos os números inteiros m, n ≥ 2 tais que

$$\frac{1 + m^{3n} + m^{2 \cdot 3^n}}{n}$$

é um inteiro.

Resposta:

Claramente *n* é ímpar, m.d.c.(*m*, *n*) = 1 e *n* > 2. Se *n* = 3, como m.d.c.(*m*, *n*) = 1 devemos ter que *m* ; 1 (mod 3) pois caso contrário $1 + m^{3n} + m^{2 \cdot 3n} \equiv 1 - 1 + 1 \equiv 1 \pmod 3$. É fácil ver que todo par (*m*, *n*) = (3*k* + 1, 3) é solução. Suponha agora *n* > 3 e seja $k = ord_n m$. Se $n > 3 \Longrightarrow m^{3n} \not\equiv 1 \pmod n$. Como $1 + m^{3n} + m^{2 \cdot 3^n} = \dfrac{m^{3^{n+1}} - 1}{m^{3n} - 1}$ segue que $n \mid m^{3^{n+1}} - 1 \Rightarrow k \mid 3^{n+1}$.

Logo, $k = 3^{n+1}$. Pelo teorema de Euler, $m^{\varphi(n)} \equiv 1 \pmod n$ então $k \leq \varphi(n)$ e $3^{n+1} \leq \varphi(n) \leq n - 1$, uma contradição.

25. Prove que se *p* é primo, então $p^p - 1$ tem um fator primo congruente a 1 módulo *p*.

Resposta:

Seja q um primo que divide $\frac{p^p-1}{p-1}$. Como $q \mid p^p - 1$ segue que $ord_q p \mid p$. Se $ord_q p = 1$ então $q \mid p^p - 1$ e $0 \equiv p^{p-1} + p^{p-2} + ... p + 1 \equiv 1 + 1 + ... + 1 + 1 \equiv p \pmod q$. Mas isso é um absurdo pois $p \neq q$. Logo $ord_q p = p$ e obtemos p | $\varphi(q) = q - 1$. Daí, todos os divisores primos de $\frac{p^p-1}{p-1}$ são congruentes a 1 módulo p.

26. Prove que existem infinitos inteiros positivos n tais que

$$\varphi(n) = \frac{n}{3}.$$

Resposta:

Basta tomar $n = 2 \cdot 3^m$, onde m é um inteiro positivo. Então:

$$\varphi(n) = \varphi(2 \cdot 3^m) = \varphi(2)\varphi(3^m) = 2 \cdot 3^{m-1} = \frac{n}{3}.$$

27. Se n é um inteiro positivo composto, então

$$\varphi(n) \leq n - \sqrt{n}$$

Resposta:

Se $n = p_1^{a_1} \cdot p_2^{a_2} \cdot ... \cdot p_k^{a_k}$, usando que n é composto, podemos garantir que existe um fator primo p_i tal que $p_i \leq \sqrt{n}$. Assim,

$$\begin{aligned}
\varphi(n) &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)...\left(1-\frac{1}{p_k}\right) \\
&\leq n\left(1-\frac{1}{p_i}\right) \\
&\leq n\left(1-\frac{1}{\sqrt{n}}\right) \\
&= n - \sqrt{n}
\end{aligned}$$

28. Encontre os últimos três dígitos de 7^{9999}

Resposta:

Como $\varphi(1000) = 400$, usando o Teorema de Euler, obtemos:

$7^{10000} = (7^{400})^{25}$

$\equiv 1 \pmod{1000}$

Note que $7 \cdot 143 = 1001 \equiv 1 \pmod{1000}$. Assim,

$7^{9999} \equiv 7^{9999} \cdot 7 \cdot 143$

$\equiv 7^{10000} \cdot 143$

$\equiv 143 \pmod{1000}$

Logo, 7^{9999} termina em 143.

29. (Putnam 1972) Prove que não existe um inteiro $n > 1$ tal que $n|2^n - 1$.

Resposta:

Se existem tais inteiros positivos, denotemos por m o menor deles. Claramente m é ímpar, pelo teorema de Euler, podemos garantir que:

$$m \mid 2^{\varphi(m)} - 1.$$

Seja d = m.d.c.(m, φ(m)). Temos $2^d - 1$ = m.d.c.($2^m - 1$, $2^{\varphi(m)} - 1$). Como m|m.d.c.($2^m - 1$, $2^{\varphi(m)} - 1$), d > 1. Além disso, d ≤ φ(m) < m e $d \mid 2^d - 1$. Isso é um absurdo pois m é o menor inteiro maior que 1 com tal propriedade.

30. (Olimpíada de Matemática Argentina) Demostre que para cada número natural n, existe uma potência de 2 cuja expansão decimal tem entre seus últimos n dígitos (da direita) mais de $\frac{2n}{3}$ dígitos que são iguais a 0.

Resposta:

Se 2^k tiver um resto muito pequeno módulo 10^n, poderemos garantir que existirão muitos zeros consecutivos entre seus últimos dígitos. Para obtermos a equação $2^k \equiv r \pmod{10^n}$ com r pequeno, é interessante começarmos analisando $2^k \pmod{5^n}$ uma vez que m.d.c.($2, 5^n$) = 1.

Façamos isso. Pelo teorema de Euler, temos:

$2^{\varphi(n)} \equiv 1 \pmod{5^n} \Rightarrow$

$2^{\varphi(n)+n} \equiv 2^n \pmod{10^n}$.

Como $2^n = 8^n/3 < 10^{n/3}$, podemos concluir que 2^n possui menos que $\frac{n}{3}$ dígitos e, consequentemente, entre os últimos n dígitos de $2^{\varphi(n)+n}$ existem pelo menos $n - \frac{n}{3} = \frac{2n}{3}$ dígitos consecutivos iguais a zero.

8 FUNÇÕES ARITMÉTICAS NO ENSINO BÁSICO

Após o que foi apresentado nos capítulos anteriores, resta-nos perguntar como poderíamos abordar tal conteúdo para alunos da escola básica?

Um primeiro argumento seria o fato que toda a teoria apresentada pode ser formulada com conteúdos que basicamente envolvem a ideia de divisibilidade no conjunto dos números inteiros que é bem conhecida nos anos iniciais do ensino fundamental.

Pode-se também, como propósito para seu ensino, colocar a importância desse assunto em competições matemáticas, inclusive na OBMEP (Olimpíada Brasileira de Matemática das Escolas Públicas), com grau de dificuldades variáveis.

Outro argumento que poderíamos fornecer seria dotar o professor e o aluno do ritmo adequado para tratar dos métodos matemáticos, dando a todos, as condições de trabalhar o que foi ensinado no ensino básico, ultrapassando de forma natural os novos conceitos.

Vale aqui ressaltar que o estudo de uma nova teoria pode ser mais atrativo quando podemos a esse estudo trabalhar a motivação do aluno em querer aprendê-lo. Uma dessas formas seria como aplicar todo o esforço despendido para o seu domínio em situações do cotidiano.

LIMA (2007) corrobora com o que foi dito acima salientando que o ensino da matemática deve ter como pilares a Conceituação, a Manipulação e a Aplicação.

> Cada tópico apresentado na sala de aula, cada novo assunto tratado no curso, cada tema estudado deve ser visto sob esses três aspectos: o conceitual, o manipulativo e o aplicativo. O professor deve se submeter-se ao desafio de compor esse trio a cada nova etapa do seu trabalho.

Afirma LIMA (2007) ainda, que a dosagem entre esses três pilares é exatamente o equilíbrio do processo de aprendizagem, não sendo fácil no início contemplar as três de maneira eficiente. Porém não devemos desistir, mas sim de anotar as dificuldades e com determinação superá-las mais tarde.

Aqui devemos salientar que muito do que foi visto nesse trabalho, faz parte de um ramo da matemática chamado de Teoria dos Números, que para muitos matemáticos de meados do século XX, achavam que era uma parte imaculada, sem aplicações. Isso foi defendido, na época, pelo famoso matemático inglês G.H.Hardy.

BOYER (1996) nos traz o que Hardy achava. Em suas próprias palavras:

> Ninguém descobriu ainda nenhum propósito bélico a ser servido pela teoria dos números ou da relatividade, e parece improvável que alguém o faça por muitos anos.

O teórico dos números Hardy em outro momento afirmava que sua matemática era inútil. Segundo BOYER (1996):

> Eu só posso dizer que se um jogo de xadrez é, num certo sentido rude, inútil, então isto ´e igualmente verdade para a maior parte da mais refinada matemática(...). Eu nunca fiz nada útil. Nenhuma descoberta que fiz já produziu, direta ou indiretamente, para o bem ou para o mal a menor diferença na melhoria do mundo. Nem é possível que venha a fazê-lo.

Ainda bem que Hardy não estava certo em sua previsão, o estudo da teoria dos números se mostrou bastante aplicável em especial o que foi tratado no contexto desse trabalho, as funções aritméticas e em especial o teorema de Euler no que diz respeito a criptografia, assim os três pilares defendido por LIMA(2007) estaria completo. Restando a nós professores saber dosar de forma adequada essas ideias.

8.1 Uma Proposta para o ensino de Funções Aritméticas e o teorema de Euler.

Apresentaremos a seguir uma sugestão de um plano de aula para o ensino do Teorema de Euler para alunos na fase final do ensino médio.

PLANO DE AULA

Conteúdo Programático: Teorema de Euler e Pequeno Teorema de Fermat.

Tempo previsto: Três aulas de 120 minutos em três momentos diferentes.

Objetivos: Apresentar a aritmética modular, explicando os assuntos prévios que o aluno deverá possuir, estimulando a participação dos mesmos mostrando que a teoria poderá ser mais bem compreendida em grupos.

Metodologia: Aula expositiva, resolução de textos e indicação de filmes que tratam sobre o assunto.

Recursos pedagógicos: Quadro, giz (pincel para quadro branco), lista de exercícios e discussões sobre os filmes.

AÇÃO DIDÁTICA

Momento 1: Apresentação da aritmética modular e de suas principais propriedades, ressaltando sempre que o desenvolvimento da teoria depende exclusivamente da definição de divisibilidade entre números inteiros. (Tempo de duração 120 minutos)

Momento 2: Apresentar o Teorema de Euler e como Consequência o Pequeno Teorema de Fermat, demonstrando alguns resultados, sendo que no final da aula, apresentaremos alguns problemas e indicaremos um filme sobre Criptografia para serem discutidos no próximo momento. (Tempo de duração 120 minutos)

Momento 3: Resolver os exercícios propostos no momento anterior e discutir o enredo do filme sugerido.

9 CONCLUSÃO

A presente dissertação teve como objetivo, apresentar aos professores de matemática da educação básica um tópico pouco visto da Teoria dos Números que são as Funções aritméticas, dando ênfase ao Teorema de Euler e, por conseguinte o Pequeno Teorema de Fermat.

Para a compreensão desse trabalho não há necessidade de matemática de nível superior, entretanto alguns resultados precisem de algum amadurecimento matemático.

Embora o foco tenha sido o Teorema de Euler, introduzimos de maneira simples a Função de Möbius apresentando no final a famosa Fórmula de Inversão.

O teorema de Euler e o Pequeno Teorema de Fermat são tópicos bastante cobrados em competições matemáticas em todo mundo, tendo o Brasil obtido resultados importantes, sendo que, para termos cada vez mais um fortalecimento nessas competições o IMPA (Instituto de Matemática Pura e Aplicada), desde 1979, realiza as Olímpiadas Brasileiras de Matemática.

O Trabalho apresenta também alguns problemas, todos eles com soluções, sobre os assuntos abordados, para servir de material de apoio aos professores que ministram aulas para seus alunos, sobre tópicos de matemática olímpica.

Acreditamos também que o assunto tratado na presente dissertação terá um alcance maior no segmento docente assim como no segmento discente de escolas públicas e privadas, por não apresentar temas de matemática de nível superior.

Ademais, acreditamos que a presente dissertação poderá elevar o interesse de alunos e professores a esse mundo fascinante da Teoria dos Números inteiros.

REFERÊNCIAS

ALENCAR FILHO, E. **Teoria elementar dos números**. São Paulo: Nobel, 1992. 386 p.

BOYER, C. B. **História da matemática**. 2 ed. São Paulo: Blücher, 1996. 508 p.

COUTINHO, S. C. **Números inteiros e criptografia RSA**. 2 ed. Rio de Janeiro: IMPA, 2009. 226 p.

ENGEL, A. **Problem-solving strategies**. 1 ed. New York: Springer, 1998. 416 p.

LIMA, E. L. **Matemática e ensino**. 3 ed. Rio de Janeiro: SBM, 2007. 250 p.

MORAIS FILHO, D. C. **Um convite à matemática**: com técnicas de demonstração e notas históricas. 3 ed. Rio de Janeiro: SBM, 2016. 310 p.

RIBENBOIM, P. **Números primos:** velhos mistérios e novos recordes. 1 ed. Rio de Janeiro: IMPA, 2014. 328 P.

TAO, T. **Como resolver problemas matemáticos**. 1 ed. Rio de Janeiro: SBM, 2013. 145 p.