UNIVERSIDADE ESTADUAL DO CEARÁ
CENTRO DE CIÊNCIAS E TECNOLOGIA
MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL

JOSIELSON BATISTA MELO

OS NÚMEROS PERFEITOS E O TEOREMA DE EUCLIDES-EULER

FORTALEZA – CEARÁ
2021

JOSIELSON BATISTA MELO

OS NÚMEROS PERFEITOS E O TEOREMA DE EUCLIDES-EULER

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional do Programa de Pós-Graduação em Matemática do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial à obtenção do título de Mestre em Matemática em Rede Nacional. Área de Concentração: Matemática.

Orientador: Prof. Dr. Claudemir Silvino Leandro

FORTALEZA – CEARÁ

2021

Dados Internacionais de Catalogação na Publicação
Universidade Estadual do Ceará
Sistema de Bibliotecas

Melo, Josielson Batista.
Os números perfeitos e o teorema de Euclides-Euler [recurso eletrônico] / Josielson Batista Melo. - 2021.
52 f. : il.

Dissertação (MESTRADO PROFISSIONAL) - Universidade Estadual do Ceará, Centro de Ciências e Tecnologia, Curso de Mestrado Profissional Em Matemática Rede Nacional - Profissional, Fortaleza, 2021.
Orientação: Prof. Dr. Claudemir Silvino Leandro.
1. Matemática. Números perfeitos. Teorema Euclides-Euler.. I. Título.

JOSIELSON BATISTA MELO

OS NÚMEROS PERFEITOS E O TEOREMA DE EUCLIDES-EULER

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática em Rede Nacional do Programa de Pós-Graduação em Matemática do Centro de Ciências e Tecnologia da Universidade Estadual do Ceará, como requisito parcial à obtenção do título de Mestre em Matemática em Rede Nacional. Área de Concentração: Matemática.

Aprovada em: 31 de agosto de 2021

BANCA EXAMINADORA

Prof. Dr. Claudemir Silvino Leandro (Orientador)

Universidade Estadual do Ceará – UECE

Prof. Dr. Tiago Caúla Ribeiro

Universidade Estadual do Ceará – UECE

Prof. Dr. Valberto Rômulo Feitosa Pereira

Instituto Federal de Educação, Ciência e Tecnologia do Ceará – IFCE

Dedico este trabalho a Deus, pelo dom da vida.

Aos meus pais e irmãos, por sempre acreditarem na realização dos projetos.

A minha esposa Renata Keylla e meus filhos Josielson Júnior e Ruan Alef, pelo companheirismo, paciência e incentivo.

A memória do meu grande amigo e colega de mestrado Diego Aguiar Lima, que faleceu em decorrência da COVID-19.

AGRADECIMENTOS

Agradeço primeiramente a Deus, pelo dom da vida.

Aos meus pais e irmãos, por sempre acreditarem na realização dos projetos.

A minha esposa Renata Keylla e meus filhos Josielson Júnior e Ruan Alef, pelo incentivo e paciência.

Aos meus professores e em especial ao meu orientador Prof. Dr. Claudemir Silvino Leandro pelos seus ensinamentos e parceria.

Aos colegas de mestrado pelo convívio e companheirismo nesses anos.

“Os números governam o mundo”.

(Galileu Galilei)

RESUMO

Este trabalho tem o objetivo de apresentar um estudo sobre a matemática, em especial, sobre a Teoria dos Números. Através de um levantamento bibliográfico de obras que abordam o tema, mostraremos conceitos de números naturais, números inteiros, divisibilidade de números inteiros, congruências, máximo divisor comum, números primos, teorema fundamental da aritmética, Pequeno Teorema de Fermat, infinidade dos números primos, primos de Mersenne, primos de Fermat, teste de primalidade, números perfeitos e por fim demonstraremos o Teorema de Euclides-Euler.

Palavras-chave: Matemática. Números perfeitos. Teorema Euclides-Euler.

ABSTRACT

This work aims to present a study on mathematics, in particular, on Number Theory. Through a bibliographical survey of works that address the topic, we will show concepts of natural numbers, integers, integer divisibility, congruences, greatest common divisor, prime numbers, fundamental theorem of arithmetic, Fermat's Little Theorem, infinity of prime numbers, Mersenne primes, Fermat primes, primality test, perfect numbers and finally we will demonstrate the Euclid-Euler Theorem.

Keywords: Mathematics. Perfect numbers. Euclid-Euler theorem.

SUMÁRIO

1 INTRODUÇÃO

Este trabalho busca demonstrar propriedades de alguns números, em especial os números naturais, inteiros, primos e os números perfeitos. A seguir descreveremos, brevemente, os assuntos abordados em cada capítulo.

No capítulo 2 apresentaremos conceitos de números naturais, números inteiros, divisibilidade de números inteiros, congruências e máximo divisor comum. No capítulo 3, abordaremos os números primos e algumas de suas propriedades, enfatizando os primos de Mersenne e de Fermat. No capítulo 4, definiremos os números perfeitos, amigáveis, defectivos e abundantes. E, finalmente, no capítulo 5 demonstraremos o Teorema de Euclides-Euler, mostrando sua relação com os números perfeitos.

A metodologia utilizada foi um levantamento bibliográfico dos assuntos relacionados à Aritmética e a Teoria dos Números.

2 ARITMÉTICA INICIAL

Neste capítulo, apresentaremos tópicos relacionados a Teoria Elementar dos Números, bem como conceitos de números naturais, números inteiros, divisibilidade de números inteiros e congruências. Tais conceitos serão úteis para o desenvolvimento do trabalho.

2.1 Números Naturais

Para estudar os números primos, números perfeitos, entre outros, e demonstrarmos alguns de seus resultados, é necessário um prévio conhecimento dos números inteiros e suas propriedades. Antes de abordar tais propriedades, uma menção ao conjunto dos números naturais se faz necessário. Não faremos aqui uma abordagem ampla desses números, admitiremos que o leitor já conheça o conjunto dos números naturais, denotado por $\mathbb{N} = \{1,2,3,4, \dots\}$, e as operações de adição e multiplicação desses números. Porém, não poderíamos deixar de mencionar a base da construção dos números naturais, ou seja, os Axiomas de Peano, escritos por Giussepe Peano.

Figura 1 – Giuseppe Peano (1858-1932)

Fonte: https://pt.wikipedia.org/wiki/Giuseppe_Peano.

Axiomas de Peano

(1) Todo número natural tem um único sucessor;

(2) Números naturais diferentes têm sucessores diferentes;

(3) Existe um único número natural, chamado de um (representado por 1), que não é sucessor de nenhum outro número;

(4) Seja $X \subset \mathbb{N}$ tal que:

- $1 \in X$;
- O sucessor de n pertence a X sempre que n pertencer a X. Então, $X = \mathbb{N}$.

O item 4 dos *Axiomas de Peano* é a base para o *Princípio de Indução Finita* e gera uma técnica para demonstrações de afirmações sobre o conjunto dos números naturais denominada *Demonstração por Indução* que enunciamos à seguir.

Princípio de Indução. Seja P uma afirmação sobre o conjunto dos números naturais. Se $P(1)$ é verdadeira e, além disso, sempre que $P(a)$ for verdadeira implicar que $P(a+1)$ é verdadeira, então $P(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Vejamos alguns problemas:

Exemplo 2.1. Prove por indução matemática que:

$$1.2^0 + 2.2^1 + 3.2^2 + \cdots + n.2^{n-1} = 1 + (n-1).2^n.$$

Demonstração:

i) Para $n = 1$.

$1.2^0 = 1 + (1-1).2^1 \Rightarrow 1 = 1 + 0.2 \Rightarrow 1 = 1$ é verdadeiro.

ii) Se é verdadeira para $n = k$, então deve ser verdadeira para $n = k + 1$.

Hipótese indutiva:

$$1.2^0 + 2.2^1 + 3.2^2 + \cdots + k.2^{k-1} = 1 + (k-1).2^k$$

Deve-se mostrar que:

$$1.2^0 + 2.2^1 + 3.2^2 + \cdots + (k+1).2^k = 1 + k.2^{k+1}$$

Sabe-se que:

$$1.2^0 + 2.2^1 + 3.2^2 + \cdots + k.2^{k-1} = 1 + (k-1).2^k$$

somando $(k+1).2^k$ aos dois membros, temos:

$$1.2^0 + 2.2^1 + 3.2^2 + \cdots + k.2^{k-1} + (k+1).2^k = 1 + (k-1).2^k + (k+1).2^k$$

$$= 1 + 2^k.(k - 1 + k + 1)$$

$$= 1 + 2^{k}.2k$$

$$= 1 + k.2^{k+1}$$

Assim por indução, a proposição está demonstrada.

■

Exemplo 2.2. Prove por indução matemática que:

$$1.1! + 2.2! + 3.3! + \cdots + n.n! = (n+1)! - 1.$$

Demonstração:

i) Para $n = 1$, temos

$$1.1! = (1+1)! - 1 \Rightarrow 1 = 2! - 1 \Rightarrow 1 = 1 \text{ é verdadeiro.}$$

ii) Se é verdadeira para $n = k$, então deve ser verdadeira para $n = k + 1$.

Hipótese indutiva:

$$1.1! + 2.2! + 3.3! + \cdots + k.k! = (k+1)! - 1.$$

Deve-se mostrar que:

$$1.1! + 2.2! + 3.3! + \cdots + k.k! + (k+1).(k+1)! = (k+2)! - 1.$$

Sabe-se que:

$$1.1! + 2.2! + 3.3! + \cdots + k.k! = (k+1)! - 1.$$

somando $(k+1).(k+1)!$ aos dois membros, temos:

$$1.1! + 2.2! + 3.3! + \cdots + k.k! + (k+1).(k+1)! = (k+1)! - 1 + (k+1).(k+1)!$$

$$= (k+1)!.(1+k+1) - 1$$

$$= (k+1)!.(k+2) - 1$$

$$= (k+2)! - 1$$

Assim por indução, a proposição está demonstrada.

■

2.2 Números Inteiros

Uma das principais propriedades dos números inteiros é o Princípio da Boa Ordenação enunciado a seguir:

Princípio da Boa Ordem: Se A é um subconjunto do conjunto dos números inteiros não negativos, com $A \neq \emptyset$, então existe um elemento n em A satisfazendo $n \leq a$ para cada inteiro a do conjunto A.

Demonstração:

Seja um conjunto A subconjunto dos números naturais, ou seja, $A \subset \mathbb{N}$. Por esse princípio, existe um determinado número n menor ou igual a todos os elementos do conjunto A, ou seja, $\exists\, n \leq a, \forall\, a \in A$. Existem duas possibilidades para o conjunto X:

1. O número 1 pertence ao conjunto A, ou seja, $1 \in A$, neste caso, 1 será o menor elemento de A.

   Do contrário, existiria um número a pertencente ao conjunto A tal que $a < 1$, ou seja, isso implicaria dizer que existe um número natural q tal que sua soma com a resultasse em 1: $a < 1 \Rightarrow \exists\, q \in \mathbb{N}, a + q = 1$. Entretanto, a soma de dois números naturais é sempre o sucessor de algum número natural, e como 1 não é sucessor de nenhum número, essa tese contrária é um absurdo.
2. O número 1 não pertence ao conjunto A, ou seja, $1 \notin A$..

   Seja um conjunto B, subconjunto dos números naturais, tal que todos os seus elementos são menores que os elementos de A, ou seja, $B = \{b \in \mathbb{N}: b < a, \forall\, a \in A\}$.

   Obviamente, $1 \in B$. Como se $a \in A \Rightarrow a \notin B$ então $B \neq \mathbb{N}$ e deve existir $b_i \in B$ tal que $b_i + 1 \notin B$ pois do contrário o princípio da indução finita implicaria que $B = \mathbb{N}$ um absurdo. Além disso como $b_i \in B \Rightarrow a > b_i, \forall\, a \in A$ e como $b_i + 1 \notin B \Rightarrow \exists a \in A, b_i + 1 \geq a$ então para algum $a \in A, b_i < a \leq b_i + 1 \Leftrightarrow a = b_i + 1$, por fim se existisse

$a \in A, a < b_i + 1$ como $b_i \in B \Rightarrow b_i < a < b_i + 1$ absurdo, logo existe o menor elemento de A, o número $b_i + 1$.

■

O conjunto dos números inteiros originou-se do conjunto dos números naturais. Admitiremos que o leitor já conheça o conjunto dos números inteiros, denotado por $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$, bem como as operações de adição e multiplicação.

Abordaremos a seguir as propriedades das operações de adição e multiplicação dos números inteiros que são denominadas propriedades básicas da aritmética.

(1) 0 é o elemento neutro da adição. Dado $a \in \mathbb{Z}$ temos que $a + 0 = a = 0 + a$, $\forall\, a \in \mathbb{Z}$;

(2) 1 é o elemento neutro da multiplicação. Dado $a \in \mathbb{Z}$ temos que $a.1 = a = 1.a$, $\forall\, a \in \mathbb{Z}$;

(3) elemento oposto da adição. Dado $a \in \mathbb{Z}$ temos que existe $-a \in \mathbb{Z}$ tal que $a + (-a) = 0 = (-a) + a$;

(4) Comutatividade: Dados $a, b \in \mathbb{Z}$ temos então que $a + b = b + a$ e $a.b = b.a$;

(5) Associatividade: Dados $a, b, c \in \mathbb{Z}$ temos então que $(a + b) + c = a + (b + c)$ e $(a.b).c = a.(b.c)$;

(6) Distributiva da multiplicação em relação a adição: Dados $a, b, c \in \mathbb{Z}$ temos então que $(a + b)c = ac + bc$.

Dentre os conceitos relacionados aos números inteiros, destaca-se o conceito de divisibilidade, definido a seguir.

2.3 Divisibilidade em $\mathbb{Z}$

Definição 2.1. Dados dois números inteiros a e b, dizemos que b divide a, e escreveremos, $b|a$, se existir um inteiro c tal que $a = bc$. Caso não exista o inteiro c dizemos que b não divide a e denotaremos por $b \nmid a$.

Definição 2.2. Um número natural n é dito par se existir um número natural k de modo que $n = 2k$.

Definição 2.3. Um número natural n é dito ímpar se existir um número natural k de modo que $n = 2k + 1$.

Exemplo 2.3.

$6|48$, pois $48 = 6 \,.\, 8$.

Exemplo 2.4.

$2 \nmid 5$. De fato, se 2 divide 5, então por definição, existe um inteiro c tal que $5 = 2c$. Daí, 5 seria um número par, mas isso é um absurdo. Portanto, $2 \nmid 5$.

Teorema 2.1. Dados a, b, c e d números inteiros, valem as seguintes propriedades:

(1) $a|a$, $1|a$ e $a|0$;
(2) Se $a|b$ e $b|c$, então $a|c$;
(3) Se $a|b$ e $c|d$, então $ac|bd$;
(4) Se $ab|ac$ e $a \neq 0$, então $b|c$;
(5) Se $a|b$ e $b \neq 0$, então $|a| \leq |b|$;
(6) $a|1 \Leftrightarrow a = \pm 1$;
(7) $a|b$ e $b|a \Rightarrow |a| = |b|$;
(8) Se $a|b$ e $a|c$, então $a|(bx + cy)\ \forall\, x, y \in \mathbb{Z}$;
(9) Se $a|(b \pm c)$, então $a|b \Leftrightarrow a|c$.

Demonstração:

(1) Basta notar que $a = 1.a$ e $0 = a.0$.
(2) Se $a|b$ e $b|c$, então por definição, existem inteiros k_1 e k_2 tais que $b = ak_1$ e $c = bk_2$. Desse modo, concluímos das duas igualdades que $c = a(k_1k_2)$ e, assim, $a|c$.
(3) Se $a|b$ e $c|d$, então existem inteiros k_1 e k_2 de modo que $b = ak_1$ e $d = ck_2$. Logo, $bd = ac(k_1k_2)$. Portanto, $ac|bd$.

(4) Como $ab|ac$, existe $r \in \mathbb{Z}$ tal que $ac = abr$, ou seja, $a.(c - br) = 0$. Mas $a \neq 0$, donde $c = br$, isto é, $b|c$.

(5) Da hipótese existe $r \in \mathbb{Z}$ tal que $b = ar$. Assim, $|b| = |ar| = |a|.|r|$. Como $b \neq 0$, segue que $r \neq 0$, e isto significa que $|r| \geq 1$. Por isso, $|b| = |a|.|r| \geq |a|.1 = |a|$. Logo, $|a| \leq |b|$.

(6) Do item anterior, tem-se $|a| \leq |1| = 1$. Como $a \neq 0$, decorre que $|a| = 1$, isto é, $a = \pm 1$. A recíproca é óbvia e $|a| \geq |b|$.

(7) Do item (5), temos $|a| \leq |b|$, ou seja, $|a| = |b|$.

(8) Por hipótese, $b = ak_1$ e $c = ak_2$, com $k_1, k_2 \in \mathbb{Z}$. Daí, para quaisquer inteiros x e y, tem-se que $bx + cy = ak_1x + ak_2y = a(k_1x + k_2y)$, isto é, $a|(bx + cy)$.

(9) Se $a|(b \pm c)$ e $a|b$ então, pelo item anterior, $a|[1(b \pm c) - b]$, isto é, $a| \pm c$, ou ainda, $a|c$: A recíproca é análoga.

■

O Algoritmo da Divisão, também conhecido como Algoritmo de Euclides, é um resultado clássico da Teoria dos Números, e é encontrado no famoso Livro VII dos Elementos de Euclides.

Teorema 2.2 (Algoritmo da Divisão). Dados $a \in \mathbb{Z}$ e $b \in \mathbb{N}$, existem únicos $q, r \in \mathbb{Z}$ tais que

$$a = q.b + r, \text{com } 0 \leq r < b.$$

Demonstração:

Seja $X = \{a - bx : x \in \mathbb{Z} \text{ e } a - bx \geq 0\}$.

Notemos que $X \subset \mathbb{N} \cup \{0\}$ e $X \neq \emptyset$, pois tomando $x = -|a| \in \mathbb{Z}$, tem-se:

$$a - bx = a - b(-|a|) = a + b|a| \geq a + |a| \geq 0, \text{ pois } b \geq 1 \text{ e } |a| \geq \pm a.$$

Como $X \subset \mathbb{N} \cup \{0\}$ e $X \neq \emptyset$, o Princípio da Boa Ordenação garante a existência de um menor elemento $r \in X$. Assim, existe $q \in \mathbb{Z}$ tal que

$$r = a - bq.$$

Ou seja,

$$a = qb + r, \text{ com } r \geq 0.$$

Afirmamos que $r < b$. De fato, suponhamos que fosse $r \geq b$. Então $r - b \geq 0$.

Mas $r = a - bq$, daí

$$r - b = a - bq - b = a - b(q + 1) \geq 0,$$

ou seja, $r - b \in X$. Contradição, pois $r - b \in X$ e $r - b < r$, o que contraria a minimalidade de r. Logo,

$$a = q.b + r, \text{com } 0 \leq r < b.$$

Mostraremos agora a unicidade. Para tanto, suponhamos que existam duas formas, isto é

$$a = q_1.b + r_1, \text{com } 0 \leq r_1 < b \text{ e } a = q_2.b + r_2, \text{com } 0 \leq r_2 < b.$$

Então

$$q_1.b + r_1 = q_2.b + r_2 \qquad (I)$$

ou melhor,

$$b(q_1 - q_2) = r_2 - r_1$$

o que significa que $b|(r_1 - r_2)$. Mas

$$\begin{cases} 0 \leq r_1 < b; \\ 0 \leq r_2 < b. \end{cases}$$

Multiplicando a segunda inequação por -1, obtém-se

$$\begin{cases} 0 \leq r_1 < b; \\ 0 \geq -r_2 > -b. \end{cases}$$

Ou ainda

$$\begin{cases} 0 \leq r_1 < b; \\ -b < -r_2 \leq 0. \end{cases}$$

Somando as duas inequações membro a membro, obtém-se $-b < r_1 - r_2 < b$ o que implica $|r_1 - r_2| < b$. Então, pelo Teorema 2.1. (5), decorre que $r_1 = r_2$.

Substituindo em (I), concluímos que $q_1 = q_2$, provando, assim, a unicidade.

■

Corolário 2.1. Dados $a, b \in \mathbb{Z}$ e $b \neq 0$, existem únicos $q, r \in \mathbb{Z}$ tais que

$$a = q.b + r, \text{com } 0 \leq r < |b|.$$

Demonstração:

Se $b > 0$ o resultado segue imediatamente do Teorema 2.2.

Se $b < 0$ então $-b > 0$ e pelo Teorema 2.2 existem únicos $q_1, r \in \mathbb{Z}$, com $0 \leq r \leq -b$, tais que

$$a = (-b)q_1 + r = b(-q_1) + r, \text{com } 0 \leq r < -b$$

Tomando, $q = -q_1$ temos o resultado. Logo, existem únicos $q, r \in \mathbb{Z}$ tais que

$$a = q.b + r, \text{com } 0 \leq r < |b|.$$

■

Exemplo 2.5. Achar o quociente e o resto na divisão de -79 por 11 que satisfazem as condições do algoritmo da divisão.

$$79 = 11 \,.\, 7 + 2$$
$$-79 = 11 \,.\, (-7) - 2.$$

Como o termo $r = -2 < 0$ não satisfaz à condição $0 \leq r < 11$, somando e subtraindo o valor 11 de b ao segundo membro da igualdade anterior, temos:

$$-79 = 11 \,.\, (-7) - 11 + 11 - 2 = 11 \,.\, (-8) + 9 \text{ com } 0 \leq 9 < 11.$$

Logo, o quociente é -8 e o resto 9.

Exemplo 2.6. Vamos achar o quociente e o resto da divisão de 20 por 6.

Considere as diferenças sucessivas:

$$20 - 6 = 14, \qquad 20 - 2.6 = 8, \qquad 20 - 3.6 = 2 < 6.$$

Isto nos dá $q = 3$ e $r = 2$.

Exemplo 2.7. Vamos achar os múltiplos de 4 que se encontram entre 1 e 142.

Pelo algoritmo da divisão temos que

$$142 = 4 \,.\, 35 + 2$$

ou seja, o maior múltiplo de 4 que cabe em 142 é $4 \,.\, 35$, onde 35 é o quociente da divisão de 142 por 4. Portanto, os múltiplos de 4 entre 1 e 142 são

$$1 \,.\, 4 = 4$$
$$2 \,.\, 4 = 8$$
$$3 \,.\, 4 = 12$$
$$\vdots$$
$$35 \,.\, 4 = 140$$

e, consequentemente, são em número de 35.

2.4 Congruência

O conceito de congruência é importante na Teoria dos Números. Ele é a base da Aritmética Modular e, por meio dele, estabelecemos resultados substanciais sobre divisibilidade.

O conceito e a notação de congruência, utilizados até os dias atuais, devem-se a Gauss, que os introduziu em seu famoso livro *Disquisitiones Arithmeticae* (Investigações Aritméticas) publicado em 1801.

Definição 2.4. Sejam a, b e p inteiros dados, sendo $\mathrm{p} > 1$, dizemos que a é congruente a b, módulo p, denotamos $\mathrm{a} \equiv \mathrm{b} (\mathrm{mod}\, \mathrm{p})$, se $\mathrm{p} | (\mathrm{a} - \mathrm{b})$. Se $\mathrm{p} \nmid (\mathrm{a} - \mathrm{b})$ dizemos que a é incongruente a b módulo p e denotamos $\mathrm{a} \not\equiv \mathrm{b} (\mathrm{mod}\, \mathrm{p})$.

De acordo com a definição, temos:

$$\mathrm{a} \equiv \mathrm{b} (\mathrm{mod}\, \mathrm{p}) \Leftrightarrow \mathrm{p} | (\mathrm{a} - \mathrm{b})$$

Exemplo 2.8.

$21 \equiv 16 (\mathrm{mod}\, 6)$, pois $6 | (21 - 15)$;

$$4 \equiv 15(\text{mod } 11), \text{ pois } 11|(4-15);$$

$$32 \equiv 0(\text{mod } 4), \text{ pois } 4|(32-0)$$

Proposição 2.1. Se a e b são inteiros, temos que $a \equiv b(\text{mod } p)$ se, e somente se, existir um inteiro k tal que $a = b + kp$.

Demonstração:

($\Rightarrow$) Se $a \equiv b(\text{mod } p)$, então $p|(a-b)$ o que implica na existência de um inteiro k tal que $a - b = kp$, isto é, $a = b + kp$.

($\Leftarrow$) A recíproca é trivial pois a existência de um k satisfazendo $a = b + kp$, nos dá $kp = a - b$, ou seja, que $p|(a-b)$ isto é, $a \equiv b(\text{mod } p)$.

■

Proposição 2.2. Sejam $a, b, c, p \in \mathbb{Z}$, com $p > 1$. Então, as seguintes propriedades são verdadeiras:

(1) $a \equiv a(\text{mod } p)$ (reflexiva);

(2) $a \equiv b(\text{mod } p)$ então $b \equiv a(\text{mod } p)$ (simétrica);

(3) $a \equiv b(\text{mod } p)$ e $b \equiv c(\text{mod } p)$ então $a \equiv c(\text{mod } p)$ (transitiva);

Demonstração:

(1) Para qualquer inteiro a tem-se que $a - a = 0 = 0.p$ e, portanto, por definição de congruência $a \equiv a(\text{mod } p)$.

(2) Por definição, $a \equiv b(\text{mod } p)$ implica que $p|(a-b)$. Logo, existe um inteiro k tal que $a - b = pk$. Daí, $b - a = p(-k)$, ou seja, $b = a(\text{mod } p)$.

(3) Por hipótese, existem k_1 e k_2 inteiros tais que

$$a - b = pk_1 \text{ e } b - c = pk_2.$$

Somando membro a membro as duas igualdades acima, temos $a - c = p(k_1 + k_2)$. Portanto, $a \equiv c(\text{mod } p)$.

■

Teorema 2.3. Sejam $a, b, c, p \in \mathbb{Z}$ tais que $a \equiv b(\text{mod } p)$. Então:

(1) $a + c \equiv b + c(\text{mod } p)$

(2) $a - c \equiv b - c(\mathrm{mod}\ p)$

(3) $a.c \equiv b.c(\mathrm{mod}\ p)$

Demonstração:

(1) Como $a \equiv b(\mathrm{mod}\ p)$, temos que $a - b = kp$ e, portanto, como $a - b = (a + c) - (b + c)$ temos $a + c \equiv b + c(\mathrm{mod}\ p)$.

(2) Como $(a - c) - (b - c) = a - b$ e, por hipótese, $a - b = kp$ temos que $a - c \equiv b - c(\mathrm{mod}\ p)$.

(3) Como $a - b = kp$ então $a.c - b.c = c.kp$ o que implica $p|(ac - bc)$ e, portanto, $a.c \equiv b.c(\mathrm{mod}\ p)$.

■

Teorema 2.4. Se $a, b, c, d, p \in \mathbb{Z}$ tais que $a \equiv b(\mathrm{mod}\ p)$ e $c \equiv d(\mathrm{mod}\ p)$, então:

(1) $a + c \equiv b + d(\mathrm{mod}\ p)$

(2) $a - c \equiv b - d(\mathrm{mod}\ p)$

(3) $a.c \equiv b.d(\mathrm{mod}\ p)$

Demonstração:

(1) De $a \equiv b(\mathrm{mod}\ p)$ e $c \equiv d(\mathrm{mod}\ p)$ temos $a - b = km$ e $c - d = k_1 m$. Somando-se membro a membro obtemos $(a + c) - (b + d) = (k + k_1)m$ e isto implica $a + c \equiv b + d(\mathrm{mod}\ p)$.

(2) Basta subtrair membro a membro $a - b = km$ e $c - d = k_1 m$ obtendo $(a - b) - (c - d) = (a - c) - (b - d) = (k - k_1)m$ o que implica $a - c \equiv b - d(\mathrm{mod}\ p)$.

(3) Multiplicamos ambos os lados de $a - b = km$ por c e ambos os lados de $c - d = k_1 m$ por b, obtendo $ac - bc = ckm$ e $bc - bd = bk_1 m$. Basta agora, somarmos membro a membro estas últimas igualdades obtendo $ac - bc + bc - bd = ac - bd = (ck + bk_1)m$ o que implica $ac \equiv bd(\mathrm{mod}\ p)$.

■

Definição 2.5. Se a e b são dois inteiros com $a \equiv b(\mathrm{mod}\ p)$, dizemos que b é um resíduo de a módulo p.

Observação: $a = b.q + r,\ 0 \leq r < b \Leftrightarrow a \equiv r(\mathrm{mod}\ b),\ 0 \leq r < b$.

Definição 2.6. Um conjunto dos inteiros $\{r_1, r_2, \cdots, r_s\}$ é sistema completo de resíduos(SCR) módulo p se

(1) $r_i \not\equiv r_j (\mathrm{mod}\ p)$ para $i \neq j$;

(2) Para todo inteiro n existe um r_i tal que $n \equiv r_i (\mathrm{mod}\ p)$.

Observação: Todo SCR módulo p tem p elementos.

Exemplo 2.9. $\{0, 1, 2, \cdots, p-1\}$ é um SCR módulo p.

Exemplo 2.10. Para p ímpar o conjunto abaixo é um SCR módulo p.

$$\left\{-\frac{p-1}{2}, -\frac{p-3}{2}, \cdots, -1, 0, 1, \cdots, \frac{p-3}{2}, \frac{p-1}{2}\right\}$$

Proposição 2.3. Se $a, b, k, p \in \mathbb{Z}$ com $k > 0$ e $a \equiv b (\mathrm{mod}\ p)$, então $a^k \equiv b^k (\mathrm{mod}\ p)$.

Demonstração:

Da fatoração

$$a^k - b^k = (a-b)\left(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + \cdots + ab^{k-2} + b^{k-1}\right).$$

E como $p|(a-b)$, segue da $Definição\ 2.2$ que $p|(a^k - b^k)$.

Logo $a^k \equiv b^k (\mathrm{mod}\ p)$.

■

Exemplo 2.11. Calcular o resto da divisão de 2^{45} por 7.

Solução:

Como $2^3 \equiv 1 (\mathrm{mod}\ 7)$, então $(2^3)^{15} \equiv 1^{15} (\mathrm{mod}\ 7)$.

Logo $2^{45} \equiv 1 (\mathrm{mod}\ 7)$, ou seja, a divisão de 2^{45} por 7 deixa resto 1.

Exemplo 2.12. Mostre que $246^{2015} \equiv 1 (\mathrm{mod}\ 7)$.

Solução:

Notemos que $246 = 6 \,.\, 41$. Como $6 \equiv -1 (\mathrm{mod}\ 7)$, podemos elevar esta congruência a 2015, donde

$$6^{2015} \equiv (-1)^{2015} \equiv -1 (\mathrm{mod}\ 7).$$

Analogamente, $41 \equiv -1(\mathrm{mod}\ 7)$. Então, elevando esta congruência a 2015, obtemos

$$41^{2015} \equiv (-1)^{2015} \equiv -1(\mathrm{mod}\ 7).$$

Multiplicando as duas congruências obtidas membro a membro, ficamos com

$$6^{2015}\ .\ 41^{2015} \equiv (-1).(-1)(\mathrm{mod}\ 7).$$

Como $6^{2015}\ .\ 41^{2015} = (6\ .45)^{2015} = 246^{2015}$, seque que

$$246^{2015} \equiv 1(\mathrm{mod}\ 7).$$

2.5 Máximo Divisor Comum

Definição 2.7. Divisores de um número natural n são todos os números naturais que ao dividirem n, resultarão em uma divisão exata, isto é, com resto igual a zero. Denotaremos por $\mathrm{D(n)}$, todos os divisores de n.

Definição 2.8. Sejam $\mathrm{a, b} \in \mathbb{Z}$ com pelo menos um deles diferente de zero. O máximo divisor comum de a e b, denotado por $\mathrm{mdc(a, b)}$, é o maior inteiro que divide a e b.

As propriedades mais básicas do mdc são as seguintes:

(1) $\mathrm{mdc(a, b)} = \mathrm{d} > 0$.

(2) Se $\mathrm{mdc(a, b)} = \mathrm{d}$ então tem-se que $\mathrm{d|a}$ e $\mathrm{d|b}$.

(3) Se $\mathrm{c|a}$ e $\mathrm{c|b}$ então $\mathrm{c|mdc(a, b)}$.

(4) $\mathrm{mdc(a, b)} = \mathrm{mdc(b, a)}$.

(5) $\mathrm{mdc(a, 1)} = 1$.

(6) Se a e b são primos tais que $\mathrm{a} \neq \mathrm{b}$, temos que $\mathrm{mdc(a, b)} = 1$.

Exemplo 2.13. Determinar o máximo divisor comum dos números 18 e 24.

Solução:

Inicialmente será determinado os divisores de 18 e 24. Assim, tem-se:

$$\mathrm{D}(18) = \{1, 2, 3, \mathbf{6}, 9, 18\}$$

$$\mathrm{D}(24) = \{1, 2, 3, 4, \mathbf{6}, 8, 12, 24\}$$

O maior divisor comum aos dois números é o 6. Logo, o $\mathrm{mdc}(18, 24) = 6$.

Um dos mais antigos métodos matemáticos utilizados para se determinar o máximo divisor comum é chamado de algoritmo de Euclides. Ele é encontrado no *Livro VII da obra Os Elementos* e ainda é uma das maneiras mais simples e eficientes de se calcular o mdc. Este é obtido a partir de divisões sucessivas e se desenvolve utilizando os seguintes passos:

Passo 1. Primeiramente, efetua-se a divisão de a por b, com $0 < \mathrm{b} < \mathrm{a}$ representado através da expressão $\mathrm{a} = \mathrm{b}.\mathrm{q}_1 + \mathrm{r}_1$, com $0 \leq \mathrm{r}_1 < \mathrm{b}$ e escreve-se os valores no diagrama:

	q_1	
a	b	
r_1		

Passo 2. A seguir, efetua-se a divisão de b por r_1, com $\mathrm{r}_1 < \mathrm{b}$. Representado através da expressão $\mathrm{b} = \mathrm{r}_1.\mathrm{q}_2 + \mathrm{r}_2$, com $0 \leq \mathrm{r}_2 < \mathrm{q}_2$, e escreve-se os valores no diagrama:

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Passo 3. Prosseguindo, o processo de divisão, enquanto for possível, até que se obtenha:

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	$\mathrm{r}_n = mdc(a, b)$
r_1	r_2	r_3	$\cdots$	r_n	0		

Sejam a e b inteiros positivos, com $\mathrm{a} \geq \mathrm{b}$. Naturalmente, repetindo o algoritmo da divisão euclidiana, temos:

$$\mathrm{a} = \mathrm{b}\mathrm{q}_1 + \mathrm{r}_1, \mathrm{com}\ 0 \leq \mathrm{r}_1 < \mathrm{b}$$

$$\mathrm{b} = \mathrm{r}_1\mathrm{q}_2 + \mathrm{r}_2, \mathrm{com}\ 0 \leq \mathrm{r}_2 < \mathrm{r}_1$$

$$\mathrm{r}_1 = \mathrm{r}_2\mathrm{q}_3 + \mathrm{r}_3, \mathrm{com}\ 0 \leq \mathrm{r}_3 < \mathrm{r}_3$$

$$\vdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, \text{com } 0 \leq r_n < r_{n-1}$$
$$r_{n-1} = r_n q_{n+1} + r_{n+1}, \text{com } r_{n+1} = 0.$$

Como o resto diminui a cada passo, o processo não pode continuar indefinidamente, e alguma das divisões deve ser exata.

Suponhamos então que r_{n+1} seja o primeiro resto nulo então temos que:

$$\text{mdc}(a, b) = \text{mdc}(b, r_1) = \text{mdc}(r_1, r_2) = \cdots = \text{mdc}(r_{n-1}, r_n)$$

Finalmente, como $r_n | r_{n-1}$ é fácil ver que $\text{mdc}(r_{n-1}, r_n) = r_n$, logo, $\text{mdc}(a, b) = r_n$.

Deste modo, fica demonstrado por este processo que o máximo divisor comum de a e b é o último resto diferente de zero das divisões sucessivas a partir da divisão euclidiana de a por b.

Exemplo 2.14. Calcular o $\text{mdc}(64, 28)$.

Solução:

	2	3	2
64	28	8	4
8	4	0	

Logo, o $\text{mdc}(64, 28) = 4$.

Exemplo 2.15. Verificar se os números 200 e 21 são primos entre si.
Observação: Dois números a e b são primos entre si, se $\text{mdc}(a, b) = 1$.

Solução:

Para resolver é necessário determinar o $\text{mdc}(220, 21)$. Assim, aplicando o algoritmo de Euclides tem-se:

	10	2
220	21	10
10	1	

Logo, o $\text{mdc}(220, 21) = 1$. Portanto, eles são primos entre si.

O teorema seguinte sobre o máximo divisor comum é bastante importante e, é conhecido por Teorema de Bézout.

Teorema 2.5. Se $d = mdc(a, b)$, então existem inteiros x e y tais que:

$$d = ax + by.$$

Demonstração:

Seja A o conjunto de todos os inteiros positivos da forma $ax + by$, com $x, y \in \mathbb{Z}$, isto é:

$$A = \{ax + by: x, y \in \mathbb{Z} \text{ e } ax + by > 0\}.$$

Este conjunto A é não vazio, porque, se $a \neq 0$, então um dos dois inteiros $a = a.1 + b.0$ e $-a = a.(-1) + b.0$ é positivo e pertence a A.

Logo, pelo PBO, existe e é único o elemento mínimo d de A, digamos $minA = d > 0$. E, de acordo com a definição de A, existem inteiros x e y tais que $d = ax + by$.

Posto isto, vamos mostrar que $d = mdc(a, b)$. Com efeito, pelo algoritmo da divisão, temos:

$$a = dq + r, \qquad \text{com } 0 \leq r < d.$$

O que dá

$$r = a - dq = a - (ax + by)q = a(1 - qx) + d(-qy).$$

Isto é, o resto r é uma combinação linear de a e b. Como $0 \leq r < d$ e $d > 0$ é o elemento mínimo de A, segue-se que $r = 0$ e $a = dq$, isto é, $d|a$.

Analogamente se conclui que também $d|b$. Logo, d é um divisor comum positivo de a e b.

Finalmente, se c é um divisor comum positivo qualquer de a e b $(c|b, c > 0)$, então:

$$c|(ax + by) \Rightarrow c|d \Rightarrow c \leq d.$$

Isto é, d é o maior divisor comum positivo de a e b, ou seja:

$$mdc(a, b) = d = ax + by \qquad x, y \in \mathbb{Z}$$

e o teorema fica demonstrado.

■

Teorema 2.6. Dados $d, m, n \in \mathbb{Z}$, tais que $d = m \,.\, n$ e $mdc(m, n) = 1$, então $d|a$, com $a \in \mathbb{Z}$, se e somente se, $m|a$ e $n|a$.

Demonstração:

($\Rightarrow$) Como $d|a$, pela Definição 2.1, existe um $r \in \mathbb{Z}$ tal que $a = d \,.\, r$, mas por hipótese $d = m \,.\, n$, donde $a = m \,.\, n \,.\, r$, o que implica que $m|a$ e $n|a$.

($\Leftarrow$) Como $m|a$ e $n|a$, pela Definição 2.1, existem $r_1,\ r_2 \in \mathbb{Z}$, tal que

$$a = m \,.\, r_1 \text{ e } a = n \,.\, r_2 \qquad (I)$$

como por hipótese $mdc(m, n) = 1$ e $d = m \,.\, n$, segue-se do Teorema 2.3 que:

$m \,.\, b + n \,.\, c = 1$ (multiplicando ambos os membros por a)

$m \,.\, b \,.\, a + n \,.\, c \,.\, a = a$ (substituindo (I) no lado esquerdo da igualdade)

$m \,.\, b \,.\, n \,.\, r_2 + n \,.\, c \,.\, m \,.\, r_1 = a$

$m \,.\, n \,.\, (b \,.\, r_2 + c \,.\, r_1) = a \Rightarrow m \,.\, n|a \Rightarrow d|a.$

■

Teorema 2.7. Sejam $a, b, c \in \mathbb{Z}$. Se $a|b.\,c$ e $mdc(a, b) = 1$, então $a|c$.

Demonstração:

Como $mdc(a, b) = 1$ pelo Teorema 2.5 existem inteiros n e m tais que $n.\,a + m.\,b = 1$. Multiplicando-se os dois lados desta igualdade por c, se obtém:

$$n.\,(a.\,c) + m(b.\,c) = c.$$

Como $a|a.\,c$ e, por hipótese, $a|b.\,c$ então, pelo Teorema 2.1 (8), $a|c$.

■

Teorema 2.8. Dados $a, b \in \mathbb{Z}^*$, $a|b \Leftrightarrow mdc(a, b) = |a|$.

Demonstração:

($\Rightarrow$) Se $a|b$, então pela Definição 2.1, existe $k \in \mathbb{Z}$ tal

$b = a.k$ onde $mdc(a,b) = mdc(a,a.k) = a$, pois $mdc(1,k) = 1$.

($\Leftarrow$) Se $mdc(a,b) = a \Rightarrow a|a$ e $a|b$.

■

3 NÚMEROS PRIMOS

Os números primos começaram a ser estudados pela escola pitagórica e, até hoje, são objeto de estudo. Uma quantidade considerável dos resultados da Teoria dos Números deve-se a esses números.

3.1 Definição de número primo

Definição 3.1. Um inteiro p é primo se $p \geq 2$ e os únicos divisores positivos de p são 1 e p. Um inteiro n é composto se $n \geq 2$ e n não é primo.
Observação: O número 1 não é primo nem composto.

Teorema 3.1. Se um número primo p não divide um inteiro a, então a e p são relativamente primos (primos entre si).

Demonstração:

Seja d o mdc de a e p. Então $d|a$ e $d|p$. Da relação $d|p$, resulta que $d = 1$ ou $d = p$, porque p é primo, e como a segunda igualdade é impossível, porque p não divide a, segue-se que $d = 1$, isto é, o $mdc(a, p) = 1$.

Logo, a e p são relativamente primos.

■

Corolário 3.1. Se p é um primo e $p|ab$, então $p|a$ ou $p|b$.

Demonstração:

Se $p|a$ está provado.

Mas, se $p \nmid a$ então $mdc(a, p) = 1$. Logo, $p|ab \Rightarrow p|b$, pelo Teorema 2.7.

Assim, existem $r, s \in \mathbb{Z}$ tais que:

$$ar + ps = 1 \quad (I)$$

Multiplicando (I) por b, temos:

$$abr + pbs = b$$

Por hipótese, $p|ab$, então $p|abr$ e também $p|pbs$, assim $p|(abr + pbs)$.

Portanto, $p|b$.

■

3.2 Teorema fundamental da aritmética (TFA)

Teorema 3.2. (Teorema Fundamental da Aritmética) Todo número inteiro maior do que 1 pode ser representado de maneira única (a menos da ordem) como um produto de fatores primos.

Demonstração:

Existência de uma decomposição

Será usado para esta demonstração o PIF.

Para $n = 2$ existe uma decomposição trivial em números primos, já que 2 é, ele próprio, um número primo.

Suponhamos agora que existe uma decomposição para todo inteiro $b, 2 \leq b < n$. Mostraremos que também vale para n.

Se n é primo, admite a decomposição trivial. Caso contrário, n admite um divisor positivo b tal que $1 < b < n$, isto é, $n = bc$, e temos também $1 < c < n$. Pela hipótese de indução, b e c podem ser escritos como produtos de primos, na forma $b = p_1.\cdots.p_s$, $c = q_1.\cdots.q_k$.

Substituindo, temos $n = p_1.\cdots.p_s.q_1.\cdots.q_k$, e o resultado também vale para n.

Para mostrarmos a unicidade usaremos também a indução em n.

Para $n = 2$ a afirmação é verdadeira.

Assumimos, então, que ela se verifica para todos os inteiros maiores do que 1 e menores que n.

Vamos provar que ela também é verdadeira para n. Se n é primo, não há nada a provar. Vamos supor então, que n seja composto e que tenha duas fatorações, isto é,

$$n = p_1.p_2.\cdots.p_s = q_1.q_2.\cdots.q_r.$$

Vamos provar que $s = r$ e que cada p_i é igual a algum q_j.

Como p_1 divide o produto $q_1.q_2.\cdots.q_r$ ele divide pelo menos um dos fatores q_j.

Sem perda de generalidade podemos supor que $p_1|q_1$. Como são ambos primos, isto implica $p_1 = q_1$.

Logo $\frac{n}{p_1} = p_2.\cdots.p_s = q_2.\cdots.q_r$. Como $1 < \frac{n}{p_1} < n$, a hipótese de indução nos diz que as duas fatorações são idênticas, isto é, $s = r$ e, a menos da ordem, as fatorações $p_1.p_2.\cdots.p_s$ e $q_1.q_2.\cdots.q_r$ são iguais.

■

3.3 Pequeno Teorema de Fermat (PTF)

Lema 3.1. (Lei do Corte) Se $ax \equiv ay(\mathrm{mod}\ p)$ e $mdc(a,p) = 1$, então $x \equiv y(\mathrm{mod}\ p)$.

Demonstração:

Pela hipótese, temos que existe $q \in \mathbb{Z}$, tal que $ax = pq + ay$, daí

$$pq = ax - ay = a(x - y).$$

Assim, temos que $p|a(x-y)$, mas como o $mdc(a,p) = 1$, segue $p|(x-y)$, garantindo que

$$x \equiv y(\mathrm{mod}\ p).$$

■

Teorema 3.3. (PTF). Seja p primo. Se $p \nmid a$ então

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

Demonstração:

Sabemos que o conjunto formado pelos p números $0, 1, 2, \cdots, p-1$ constitui um sistema completo de resíduos módulo p. Isto significa que qualquer conjunto contendo no máximo p elementos incongruentes módulo p pode ser colocado em correspondência biunívoca com um subconjunto de $\{0, 1, 2, \cdots, p-1\}$.

Vamos agora, considerar os números $a, 2a, 3a, \cdots, (p-1)a$. Como $mdc(a,p) = 1$, nenhum destes números ia, $1 \leq i \leq p-1$ é divisível por p, ou seja, nenhum é

congruente a zero módulo p. Quaisquer dois deles são incongruentes módulo p, pois $aj \equiv ak(\mathrm{mod}\ p)$ implica $j \equiv k(\mathrm{mod}\ p)$ e isto só é possível se $j = k$, uma vez que ambos j e k são positivos e menores do que p. Temos, portanto, um conjunto de $p-1$ elementos incongruentes módulo p e não divisíveis por p.

Logo, cada um deles é congruente a exatamente um dentre os elementos $1, 2, 3, \cdots, p-1$. Se multiplicarmos estas congruências, membro a membro, teremos:

$$a(2a)(3a)\cdots(p-1)a \equiv 1.2.3.\cdots.p-1(\mathrm{mod}\ p)$$

ou seja, $a^{p-1}(p-1)! \equiv (p-1)!\,(\mathrm{mod}\ p)$. Mas p não divide $(p-1)!$, de onde concluímos que $\mathrm{mdc}\big((p-1)!,\ p\big) = 1$, então pelo $\mathrm{Lema\ 3.1\ (Lei\ do\ Corte)}$ temos

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

o que conclui a demonstração.

■

Corolário 3.2. Se p é um primo e a é um inteiro positivo, então $a^p \equiv a(\mathrm{mod}\ p)$.

Demonstração:

Temos que analisar dois casos, se $p|a$ e se $p \nmid a$.

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

Se $p \nmid a$, pelo PTF $p|(a^{p-1}-1)$ e, portanto, $p|(a^p - a)$.

Logo, em ambos os casos, $a^p \equiv a(\mathrm{mod}\ p)$.

■

3.4 Infinidade de números primos

Existem infinitos números primos? Diversas provas de que existe uma infinidade de números primos já foram formuladas. A mais ilustre é a demonstração de Euclides, que há mais de 2.300 anos demonstrou que os números primos são

infinitos. Esta demonstração consta dos Elementos de Euclides, escritos por volta de 300 a.C.

A prova de Euclides (de que o conjunto dos números primos é infinito) é considerada universalmente pelos matemáticos como um modelo de elegância matemática. Ela emprega o método indireto, ou redução ao absurdo (EVES, 1997).

Teorema 3.4. O conjunto formado pelos números primos é infinito.

3.4.1 Demonstração de Euclides

Suponhamos que exista somente uma quantidade finita de números primos, digamos:

$$p_1, p_2, p_3, \cdots, p_n.$$

Consideremos o número $k = p_1.p_2.p_3.\cdots.p_n + 1$.

Como k é inteiro e $k > 2$, existe um primo p tal que $p|k$. Segue então que $p = p_i$ para algum $1 \leq i \leq n$. Logo $p_i|k$. Mas $p_i|p_1.p_2.p_3.\cdots.p_n$. Assim $p_i|k - p_1.p_2.p_3.\cdots.p_n = 1$, o que é um absurdo.

■

3.4.2 Demonstração de Goldbach

A demonstração de Goldbach se tornou conhecida após sua publicação em Berlim em 1924, entretanto ela se encontra em uma carta de C. Goldbach a Euler datada de 21/31 julho 1730.

Em 1891, A. Hurwitz descobriu independentemente a mesma demonstração em um exercício (RIBENBOIM, 2012). Ela utiliza a seguinte ideia: basta achar uma sucessão infinita $a_1 < a_2 < a_3 < \cdots$ de números naturais, primos entre si, dois a dois, isto é sem fator primo comum. Se p_1 é um fator primo de a_1, p_2 um fator primo de a_2, $\cdots$, p_n um fator primo de a_n, então $p_1, p_2, \cdots, p_n, \cdots$ são todos distintos.

■

3.5 Números primos de Mersenne

Esse conjunto de números recebe esse nome em homenagem a seu descobridor, Marin Mersenne.

Figura 2 – Marin Mersenne (1588 – 1648)

Fonte: https://pt.wikipedia.org/wiki/Marin_Mersenne.

Marin Mersenne foi um padre, matemático e teólogo. Ficou conhecido sobretudo pelo seu estudo dos chamados primos de Mersenne.

Definição 3.2. Um número da forma $M_n = 2^n - 1, n \geq 2$, é chamado número de Mersenne. Se M_n for primo, é chamado de primo de Mersenne.

Enunciaremos então a seguinte preposição:

Proposição 3.1. (Primos de Mersenne) Se $M_n = 2^n - 1$ é primo, então n é primo.

Demonstração:

Se n é composto, digamos $n = ab$, em que $1 < a, b < n$, então

$$M_n = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)\left(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1\right).$$

Como M_n é primo, $2^a - 1 = 2^{ab} - 1$ ou $2^a - 1 = 1$. Destas igualdades, obtemos $b = 1$ ou $a = 1$, uma contradição. Assim n é primo.

■

Observação: É importante ressaltar que a recíproca da proposição anterior não é válida.

Sabe-se, desde os tempos de Mersenne, que números desta forma podem ser primos ou compostos.

Por exemplo: $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$, são primos. Já, $M_{11} = 2047 = 23 \text{ x } 89$, não é primo.

Atualmente, os maiores números primos conhecidos são números de Mersenne, são eles:

n	M_n
43.112.609	$2^{43112609} - 1$
57.885.161	$2^{57885161} - 1$
74.207.281	$2^{74207281} - 1$
77.232.917	$2^{77232917} - 1$
82.589.933	$2^{82589933} - 1$

3.6 Números primos de Fermat

Figura 3 – Pierre de Fermat (1601 – 1665)

Fonte: https://pt.wikipedia.org/wiki/Pierre_de_Fermat.

Foi um dos maiores matemáticos do século XVII, ele se interessava profundamente pela Teoria dos Números, sendo considerado o primeiro matemático a contribuir para este ramo do ponto de vista teórico.

Definição 3.3. Um número da forma $F_n = 2^{2^n} + 1, n \geq 0$, é chamado de número de Fermat. Se F_n é primo, é chamado de primo de Fermat.

Pode-se verificar que $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ são primos.

À medida que n aumenta, os números de Fermat também aumentam rapidamente e não são fáceis de verificar quanto à primalidade. Sabe-se que F_n é composto para $5 \leq n \leq 30$.

Proposição 3.2. Todo número de Fermat é igual ao produto de seus anteriores somado a 2.

$$F_n = F_o F_1 \cdots F_{n-1} + 2$$

A prova é por indução. Como o caso $n = 1$ se verifica, isto é, $F_0 = F_1 - 2$, vamos supor a validade para n e mostrar que a mesma relação também vale para $n + 1$.

$$\begin{aligned} F_o F_1 \cdots F_n &= (F_0 F_1 \cdots F_{n-1}) F_n \\ &= (F_n - 2) F_n \\ &= \left(2^{2^n} + 1 - 2\right)\left(2^{2^n} + 1\right) \\ &= \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) \\ &= 2^{2^{n+1}} - 1 \\ &= 2^{2^{n+1}} + 1 - 2 \\ &= F_{n+1} - 2 \end{aligned}$$

Supondo $n < m$ temos, pela relação acima, que

$$F_o F_1 F_2 \cdots F_n \cdots F_{m-1} = F_m - 2$$

o que implica que $F_m - F_0 \cdots F_n \cdots F_{m-1} = 2$.

Logo, se um número d divide F_n e F_m então d divide 2. Como F_n é ímpar d não pode ser 2 e portanto $\text{mdc}(F_n, F_m) = 1$. (Confira 3.4.2).

■

3.7 Teste de primalidade

Apresentaremos os principais testes de primalidade, ou seja, mostraremos se um número é primo ou composto.

3.7.1 Divisões Sucessivas

Um dos mais simples testes de primalidade, consiste em dividir um número n por todos os números inteiros que estiverem na faixa que vai de 2 até $n-1$. Se n for divisível por qualquer um deles, então n é um número composto. Caso contrário, é um número primo.

Proposição 3.3. Seja n um número natural composto, então n tem um divisor primo p tal que $p \leq \sqrt{n}$.

Demonstração:

Seja p o menor divisor primo de n, então $n = pk$ para algum $k \in \mathbb{N}$.

Como $p \leq k$ temos que $p^2 \leq pk \Rightarrow p^2 \leq n \Rightarrow p \leq \sqrt{n}$.

■

Proposição 3.4. Se p é um número primo diferente de 2 e 3, então p é da forma $6k-1$ ou $6k+1$, onde k é um inteiro positivo.

Demonstração:

Todo número ao ser dividido por 6 é de uma das formas: $6k$, $6k+1$, $6k+2$, $6k+3$, $6k+4$ ou $6k+5$.

(1) $p = 6k$, p é múltiplo de 6, não é primo.

(2) $p = 6k+1$, pode ser primo.

(3) $p = 6k+2$, $p = 2(3k+1) \Rightarrow p$ é múltiplo de 2, $6k+2$ não é primo.

(4) $p = 6k+3$, $p = 3(2k+1) \Rightarrow p$ é múltiplo de 3, $6k+3$ não é primo.

(5) $p = 6k+4$, $p = 2(3k+2) \Rightarrow p$ é múltiplo de 2, $6k+4$ não é primo.

(6) $p = 6k+5 \Rightarrow p = 6k+6-1 = 6(k+1)-1 = 6k'-1$, pode ser primo.

Portanto, se $p \neq 2, 3$ for primo ele não pode ser das formas $6k$, $6k + 2$, $6k + 3$ e $6k + 4$. Assim, $p = 6k - 1$ ou $p = 6k + 1$.

■

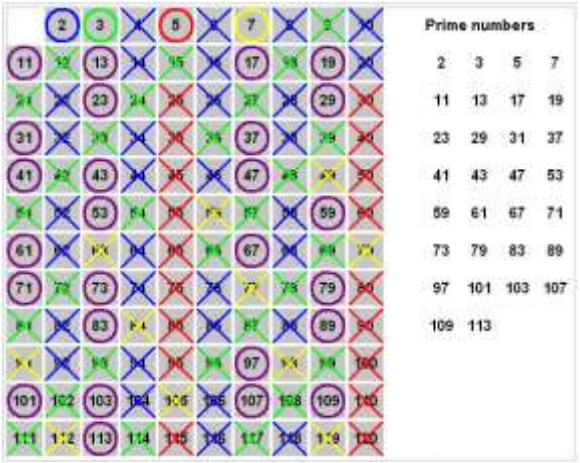
Utilizando a Proposição 3.3, Eratóstenes criou um método, chamado Crivo de Eratóstenes, para listar os primos menores que um certo inteiro positivo $n > 1$, que consiste do seguinte:

(1) Escreva uma lista com todos os inteiros entre 2 e $n - 1$;

(2) Para cada primo $p \leq \sqrt{n}$, elimina-se da lista todos os múltiplos pk de p, para $k \geq 2$;

(3) Os números que sobrarem são os primos menores que n.

Figura 4 – Crivo de Eratóstenes



Fonte: https://pt.wikipedia.org/wiki/Crivo_de_Eratóstenes.

De acordo com as Proposições 3.3 e 3.4, para verificarmos se um número é primo, usando o método das divisões sucessivas, devemos dividir o número por 2 e por 3 e, depois, faz-se as divisões por todos os inteiros na forma $6k \pm 1$ que sejam menores ou iguais à raiz quadrada do número testado.

Exemplo 3.1. Verifique se o número 113 é primo ou composto.

A $\sqrt{113}$ é aproximadamente $10{,}63$, devemos dividir 113 por 2, 3, 5 e 7. Se 113 não for divisível por nenhum destes números, então ele será primo:

- Dividindo por 2 e por 3:

$$113 = 2 \text{ x } 56 + 1$$
$$113 = 3 \text{ x } 37 + 2$$

- Para $k = 1$, dividimos por $6k - 1 = 5$ e $6k + 1 = 7$;

$$113 = 5 \text{ x } 22 + 3$$
$$113 = 7 \text{ x } 16 + 1$$

Assim, podemos afirmar que o número 113 é primo.

Exemplo 3.2. Verifique se o número 145 é primo ou composto.

$\sqrt{145} \approx 12{,}04$, devemos dividir 145 por 2, 3, 5, 7 e 11. Se 145 não for divisível por nenhum destes números, então ele será primo:

- Dividindo por 2 e por 3:

$$145 = 2 \text{ x } 72 + 1$$
$$145 = 3 \text{ x } 48 + 1$$

- Para $k = 1$, dividimos por $6k - 1 = 5$ e $6k + 1 = 7$;

$$145 = 5 \text{ x } 29 + 0$$

Portanto, o número 145 não é primo porque é divisível por 5.

3.7.2 Teste de Fermat

O teste consiste em tomarmos um número a qualquer e calcularmos $a^{p-1} \equiv 1 (\text{mod } p)$, onde p é o número cuja primalidade desejamos atestar. Feito o cálculo, temos dois possíveis resultados:

(1) Caso $a^{p-1} \equiv 1 (\text{mod } p)$, dizemos que p provavelmente é primo, podendo o teste ser repetido para valores diferentes de a, afim de obter uma probabilidade melhor de que p seja primo.

(2) Caso $a^{p-1} \not\equiv 1 (\text{mod } p)$, confirmamos que p é composto, e encerramos o teste.

Lema 3.2. Sejam p primo e a e b inteiros. Então:

$$(a+b)^p \equiv (a^p + b^p)(\mathrm{mod}\ p)$$

Demonstração:

Temos que, para todo $a \in \mathbb{Z}$, $a^p \equiv a(\mathrm{mod}\ p)$, pois p divide $a^p - a$. Daí,

$$(a+b)^p \equiv a + b \equiv (a^p + b^p)(\mathrm{mod}\ p).$$

■

Exemplo 3.3. Seja $p = 11$ e $a = 2$, queremos testar a primalidade de 11.

$$a^{p-1} \equiv 1(\mathrm{mod}\ p)$$
$$2^{11-1} \equiv 1(\mathrm{mod}\ 11)$$
$$2^{10} \equiv 1(\mathrm{mod}\ 11)$$

Logo, pela Definição 2.4, $11|(2^{10} - 1)$ e, portanto, 11 é primo.

Exemplo 3.4. Seja $p = 8$ e $a = 3$, queremos testar a primalidade de 8.

$$a^{p-1} \equiv 1(\mathrm{mod}\ p)$$
$$3^{8-1} \equiv 1(\mathrm{mod}\ 8)$$
$$3^7 \equiv 1(\mathrm{mod}\ 8)$$

Logo, pela Definição 2.4, $8 \nmid (3^7 - 1)$ e, portanto, 8 não é primo.

3.7.3 Lucas-Lehmer

O teste de Lucas-Lehmer é um teste de primalidade, para números de Mersenne, originalmente desenvolvido por Edouard Lucas em 1879 e posteriormente melhorado por Derrick Henry Lehmer em 1936.

O algoritmo é de simples compreensão, usando aritmética modular e, para um inteiro n qualquer, uma equação recursiva da forma:

$$\begin{cases} S_0 = 4 \\ S_n \equiv S_{n-1}^2 - 2(\mathrm{mod}\ M_p) \end{cases}$$

Teorema 3.5 (Teste de Lucas-Lehmer). Para todo primo ímpar p, o número de Mersenne $M_p = 2^p - 1$ é primo se, e somente se, M_p divide S_{p-2}.

A demonstração deste teorema foge ao escopo deste trabalho e pode ser encontrada, em (COUTINHO, 2013).

Proposição 3.5. Seja a sequência $S_k = \left(2+\sqrt{3}\right)^{2^k} + \left(2-\sqrt{3}\right)^{2^k}$. S_k de forma recursiva é dada por: $S_0 = 4$ e $S_{k+1} = S_k^2 - 2$.

Demonstração:

Para $k = 0$, teremos

$$S_0 = \left(2+\sqrt{3}\right)^{2^0} + \left(2-\sqrt{3}\right)^{2^0} \Rightarrow S_0 = 2+\sqrt{3}+2-\sqrt{3} \Rightarrow S_0 = 4.$$

De modo análogo, vamos escrever S_{k+1} em função de S_k.

$$S_{k+1} = \left(2+\sqrt{3}\right)^{2^{k+1}} + \left(2-\sqrt{3}\right)^{2^{k+1}} = \left(2+\sqrt{3}\right)^{2^k.2} + \left(2-\sqrt{3}\right)^{2^k.2}$$

$$= \left[\left(2+\sqrt{3}\right)^{2^k}\right]^2 + \left[\left(2-\sqrt{3}\right)^{2^k}\right]^2 + 2\left(2+\sqrt{3}\right)^{2^k}\left(2-\sqrt{3}\right)^{2^k} - 2\left(2+\sqrt{3}\right)^{2^k}\left(2-\sqrt{3}\right)^{2^k}$$

$$= \left[\left(2+\sqrt{3}\right)^{2^k} + \left(2-\sqrt{3}\right)^{2^k}\right]^2 - 2\left[(2+\sqrt{3})(2-\sqrt{3})\right]^{2^k}$$

$$= \left[\left(2+\sqrt{3}\right)^{2^k} + \left(2-\sqrt{3}\right)^{2^k}\right]^2 - 2.1^{2^k}$$

$$= \left[\left(2+\sqrt{3}\right)^{2^k} + \left(2-\sqrt{3}\right)^{2^k}\right]^2 - 2$$

$$= S_k^2 - 2$$

■

Faremos alguns exemplos para entendermos como funciona esse teste.

Exemplo 3.5. Suponha que desejamos testar a primalidade de $M_7 = 2^7 - 1$.

Calculamos primeiro a sequência de Lucas-Lehmer S_k para $2^7 - 1$ $(k = 0, 1, 2, \ldots, p-2 = 5)$.

$$S_0 = 4$$

$$S_1 = 4^2 - 2 = 14$$

$$S_2 = 14^2 - 2 \equiv 67 (\text{mod } 127)$$

$$S_3 = 67^2 - 2 \equiv 42 (\text{mod } 127)$$

$$S_4 = 42^2 - 2 \equiv 111 (\mathrm{mod}\ 127)$$
$$S_5 = 111^2 - 2 \equiv 0 (\mathrm{mod}\ 127)$$

Logo, concluímos então que $M_7 | S_5$, portanto, 127 é primo.

Exemplo 3.6. Suponha que desejamos testar a primalidade de $M_{11} = 2^{11} - 1$.

Calculamos primeiro a sequência de Lucas-Lehmer S_k para $2^{11} - 1$ $(k = 0, 1, 2, \dots, p - 2 = 9)$.

$$S_0 = 4$$
$$S_1 = 4^2 - 2 = 14$$
$$S_2 = 14^2 - 2 = 194$$
$$S_3 = 194^2 - 2 \equiv 788 (\mathrm{mod}\ 2047)$$
$$S_4 = 788^2 - 2 \equiv 701 (\mathrm{mod}\ 2047)$$
$$S_5 = 701^2 - 2 \equiv 119 (\mathrm{mod}\ 2047)$$
$$S_6 = 119^2 - 2 \equiv 1877 (\mathrm{mod}\ 2047)$$
$$S_7 = 1877^2 - 2 \equiv 240 (\mathrm{mod}\ 2047)$$
$$S_8 = 240^2 - 2 \equiv 282 (\mathrm{mod}\ 2047)$$
$$S_9 = 282^2 - 2 \equiv 1736 (\mathrm{mod}\ 2047)$$

Logo, concluímos então que $M_{11} \nmid S_9$, portanto, 2047 não é primo.

4 NÚMEROS PERFEITOS

Os números perfeitos começaram a ser estudados pela escola pitagórica e até os dias atuais despertam a curiosidade de muitos teóricos dos números. Independentemente de serem tópicos relativamente simples, no sentido de considerar conceitos elementares, como divisores, soma de divisores, ainda assim, existem alguns problemas em aberto sobre eles.

4.1 Soma dos divisores de um número natural

Definição 4.1. Seja $n > 1, n \in \mathbb{N}$, denotamos por $S(n)$ a soma de todos os divisores de n.

Observe que $S(0)$ não está definido e $S(1) = 1$. Consideremos, então $n \geq 2$ e encontremos $S(n)$. Convém antes apresentar algumas afirmações sobre $S(n)$.

(1) Se p é primo, então $S(p) = p + 1$;

(2) Se p é primo, então

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

pois $1 + p + p^2 + \cdots p^r$ é a soma dos termos de uma PG finita de primeiro termo $a_1 = 1$, razão $q = p$ e $r + 1$ termos. Em particular, para $n = 2^r$, obtemos

$$S(n) = S(2^r) = \frac{2^{r+1} - 1}{2 - 1} = 2^{r+1} - 1 = 2.2^r - 1 = 2n - 1.$$

Concluímos daí que uma potência de base 2 nunca é um número perfeito.

(3) Se p e q são números primos distintos, então $S(p.q) = S(p).S(q)$.

Para provar esta relação, basta ver que os divisores de $p.q$ são $1, p, q$ e $p.q$.

Logo,

$$S(p.q) = 1 + p + q + p.q = 1 + p + q.(1 + p) = (1 + p)(1 + q) = S(p).S(q)$$

(4) Se a e b são relativamente primos entre si, isto é, $mdc(a, b) = 1$, então

$$S(a.b) = S(a).S(b)$$

Os divisores do produto $a.b$ são da forma $a_i.b_j$, onde $1 \leq i \leq s$ e $1 \leq j \leq t$, onde s e t são os números de divisores de a e b, respectivamente. Nestas condições, a soma $S(a.b)$ dos divisores de a e b será:

$$S(a.b) = a_1(b_1 + b_2 + \cdots + b_t) + a_2(b_1 + b_2 + \cdots + b_t) + \cdots + a_s(b_1 + b_2 + \cdots + b_t)$$

Colocando $(b_1 + b_2 + \cdots + b_t)$ em evidência,

$$S(a.b) = (a_1 + a_2 + \cdots + a_s).(b_1 + b_2 + \cdots + b_t) = S(a).S(b)$$

Exemplo 4.1.

$$S(3) = \frac{3^2 - 1}{3 - 1} = \frac{9 - 1}{2} = 4$$
$$D(3) = \{1, 3\}$$

$$S(28) = S(2^2 . 7) = \frac{2^3 - 1}{2 - 1}.\frac{7^2 - 1}{7 - 1} = \frac{8 - 1}{1}.\frac{49 - 1}{6} = 7 . 8 = 56$$
$$D(28) = \{1, 2, 4, 7, 14, 28\}$$

$$S(84) = S(2^2 . 3 . 7) = \frac{2^3 - 1}{2 - 1}.\frac{3^2 - 1}{3 - 1}.\frac{7^2 - 1}{7 - 1} = \frac{8 - 1}{1}.\frac{9 - 1}{2}.\frac{49 - 1}{6} = 7 . 4 . 8 = 224$$
$$D(84) = \{1, 2, 3, 4, 6, 7, 12, 14, 21, 28, 42, 84\}$$

Note que $S(84) = 224$ e que $S(84) = S(3 . 28) = S(3).S(28) = 4 . 56 = 224$. Observe que 6 é igual a metade da soma de seus divisores.

4.2 Números perfeitos

Definição 4.2. Um número n é considerado perfeito se $S(n) = 2n$.

Exemplo 4.2. Os divisores do número 6 são $1, 2. 3$ e 6, e somando-os temos:

$$1 + 2 + 3 + 6 = 12 = 2 . 6$$

Logo, 6 é perfeito.

Exemplo 4.3. Os divisores do número 28 são $1, 2, 4, 7, 14$ e 28, e somando-os temos:

$$1 + 2 + 4 + 7 + 14 + 28 = 56 = 2 \,.\, 28$$

Logo, 28 é perfeito.

Os próximos números perfeitos seriam: 496 e 8128. Atualmente, conhece-se outros números perfeitos e todos são pares. Não se sabe ainda se existem ou não números perfeitos ímpares.

Proposição 4.1. Seja $n \in \mathbb{N}$. Tem-se que $S_n = n + 1$ se, e somente se, n é um número primo.

Demonstração:

Se $S(n) = n + 1$, segue-se que $n > 1$ e que os únicos divisores de n são 1 e n.

Logo n é primo.

Reciprocamente, se n é primo, os únicos divisores são 1 e n. Logo

$$S(n) = n + 1$$

■

4.3 Números amigáveis

Definição 4.3. Dois números naturais m e n são ditos amigáveis quando cada um deles é igual à soma de todos os divisores positivos do outro, exceto o próprio número.

Seja $m = S(n) - n$ e $n = S(m) - m$.

Logo, $m = S(n) - S(m) + m$, isto é $S(m) = S(n)$.

Daí, $m + n = 2S(n) - (n + m)$, ou melhor, $S(n) = m + n$.

Por isso, m e n são amigáveis se, e somente se,

$$S(m) = S(n) = m + n.$$

Exemplo 4.4. 220 e 284.

Soma dos divisores próprios de 220:

$$1 + 2 + 4 + 5 + 10 + 11 + 20 + 22 + 44 + 55 + 110 + 220 = 504.$$

Soma dos divisores próprios de 284:

$$1 + 2 + 4 + 71 + 142 + 284 = 504.$$

Logo, $S(220) = S(284) = 504 = 220 + 284$.

Portanto, os números 220 e 284 são amigáveis.

Outros números amigáveis são:

- 1184 e 1210;
- 17296 e 18416.

4.4 Números pares perfeitos

Historicamente, o primeiro matemático que categorizou os números pares perfeitos foi Euclides. Ele observou que os quatro primeiros números perfeitos apresentam uma forma específica.

$$6 = 2^1.(1 + 2) = 2 \,.\, 3$$

$$28 = 2^2.(1 + 2 + 2^2) = 4 \,.\, 7$$

$$496 = 2^4.(1 + 2 + 2^2 + 2^3 + 2^4) = 16 \,.\, 31$$

$$8128 = 2^6.(1 + 2 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6) = 64 \,.\, 127$$

Observe porém, que os números

$$90 = 2^3.(1 + 2 + 2^2 + 2^3) = 8 \,.\, 15$$

$$2016 = 2^5.(1 + 2 + 2^2 + 2^3 + 2^4 + 2^5) = 32 \,.\, 63$$

estão faltando nessa sequência porque $15 = 3\,.\,5$ e $63 = 3^2\,.\,7$ são números compostos, ao passo que $3, 7, 31$ e 127 são todos primos.

4.5 Números Defectivos

Definição 4.4. Um número natural n é defectivo se a soma de seus divisores, exceto o próprio número, é inferior a ele.

$$\mathrm{S(n) - n < n}$$

Exemplo 4.5. O número 26, tem como divisores $\{1, 2, 13, 26\}$ e é um número defectivo, pois:

$$\mathrm{S}(26) - 26 = (1 + 2 + 13 + 26) - 26 = 16 < 26.$$

Observação: Há ainda os quase perfeitos, que são os defectivos cuja soma dos divisores, exceto o próprio número, é igual ao seu antecessor. É o caso do 32, cuja soma dos divisores $(1 + 2 + 4 + 8 + 16 = 31)$ é o antecessor de 32.

4.6 Números Abundantes

Definição 4.5. Um número natural n é abundante se a soma de seus divisores, exceto o próprio número, é superior a ele.

$$\mathrm{S(n) - n > n}$$

Exemplo 4.6. O número 30, tem como divisores $\{1, 2, 3, 5, 6, 10, 15, 30\}$ e é um número abundante, pois:

$$\mathrm{S}(30) - 30 = (1 + 2 + 3 + 5 + 6 + 10 + 15 + 30) - 30 = 42 > 30.$$

Observação: Existem apenas 21 números abundantes menores que 100, os quais são todos pares. O primeiro número abundante ímpar é 945.

5 TEOREMA DE EUCLIDES-EULER

Teorema 5.1. Um número natural n é um número perfeito par se, e somente se, $n = 2^{p-1}(2^p - 1)$, em que $2^p - 1$ é um primo de Mersenne.

Demonstração:

Primeiramente, mostraremos que, se $n = 2^{p-1}(2^p - 1)$, em que $2^p - 1$ é um primo de Mersenne, então n é um número perfeito par.

Por hipótese, temos que $n = 2^{p-1}(2^p - 1)$, onde $2^p - 1$ é um primo de Mersenne.

Logo, $p > 1$, e, consequentemente, n é par.

Como $2^p - 1$ é ímpar, temos que $\mathrm{mdc}(2^{p-1}, 2^p - 1) = 1$.

Logo, temos que:

$$S(n) = S\left(2^{p-1} \,.\, (2^p - 1)\right)$$

$$= S(2^{p-1})S(2^p - 1)$$

$$= \frac{2^p - 1}{2 - 1} 2^p$$

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

$$= 2 \,.\, 2^{p-1} \,.\, (2^p - 1)$$

$$= 2n.$$

Portanto, n é perfeito.

Vamos verificar agora que se n é um número perfeito par, então $n = 2^{p-1}(2^p - 1)$, onde $2^p - 1$ é um primo de Mersenne.

Agora, suponhamos que n é perfeito e par.

Queremos provar que $n = 2^{p-1}(2^p - 1)$, com $2^p - 1$ primo (de Mersenne).

Seja 2^{p-1} a maior potência de 2 que divide n.

Logo, $p > 1$ e $n = 2^{p-1}.b$, com b ímpar.

Então $S(n) = (2^p - 1)S(b)$.

Como $S(n) = 2n$ segue que $(2^p - 1)S(b) = 2^p b$.

Daí temos que $(2^p - 1)|b$ pois $mdc(2^p, 2^p - 1) = 1$.

Logo existe $c \in \mathbb{N}$ com $c < b$ tal que $b = c(2^p - 1) \in \mathbb{N}$, portanto

$$(2^p - 1)S(b) = 2^p b = 2^p(2^p - 1)c, \text{ logo } S(b) = 2^p c.$$

Temos que b e c são dois divisores distintos de b tais que $c + b = 2^p c$.

Nessa situação, $c = 1$. De fato, suponha, $c \neq 1$.

Temos então, que $S(b) \geq 1 + c + b > c + b = 2^p c$; disto segue que $2^p c = c + b < S(b) = 2^p c$, uma contradição.

Portanto, temos que $S(b) = b + 1$, ou seja, b é primo.

Temos assim que $n = 2^{p-1}(2^p - 1)$, sendo $2^p - 1$ é primo.

■

6 **CONSIDERAÇÕES FINAIS**

O objetivo deste trabalho foi realizar um estudo bibliográfico sobre a Teoria dos Números, visando contribuir para o ensino da matemática tornando-o mais significativo e prazeroso. Buscou-se mostrar também a importância na compreensão das propriedades dos números para a construção dos conceitos matemáticos.

Espero que este trabalho possa ajudar os leitores e em especial professores e alunos e além disso, despertar o interesse para um estudo mais aprofundado sobre o referido assunto.

REFERÊNCIAS

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

BEZERRA, M. de N. C. **Teoria dos Números:** um curso introdutório. Belém: AEDI, UFPA, 2018.

BENATTI, K. A.; BENATTI, N. C. da C. M. **Teoria dos Números**. [S.l.]: Intersaberes, 2019.

CARAÇA, B. S. **Um estudo sobre os números especiais.** 2013. 56f. Trabalho de Conclusão de Curso (Graduação em Matemática) – Universidade Federal de São Carlos, São Paulo, 2013.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA**. [S.l.]: CIMPA, 2013. (Coleção Matemática e Aplicações).

DOMINGUES, H. H. **Fundamentos da aritmética**. São Paulo: Atual, 1991.

EVES, H. **Introdução à história da matemática**. Campinas, SP: Unicamp, 1997.

HEFEZ, A. **Aritmética.** Rio de Janeiro: Sociedade Brasileira de Matemática, 2014. (Coleção PROFMAT).

MARTINEZ, F.; MOREIRA, C. G.; SALDANHA, N.; TENGAN, E. **Teoria dos Números:** um passeio com primos e outros números familiares pelo mundo inteiro. 5. ed. [S.l.]: IMPA, 2018.

RIBENBOIM, P. **Números Primos:** Velhos mistérios e novos recordes. Rio de Janeiro: IMPA, 2012.

SANTOS, J. P. de O. **Introdução à Teoria dos Números**. 3. ed. Rio de Janeiro: IMPA, 2010.

SANTOS JÚNIOR, R. J. **Números perfeitos e amigáveis.** 2020. 98f. Dissertação (Mestrado Profissional em Matemática) – Universidade Estadual da Paraíba, João Pessoa, 2020.