**INSTITUTO DE MATEMÁTICA PURA E APLICADA – IMPA/RJ**
**MESTRADO PROFISSIONAL EM MATEMÁTICA - PROFMAT**

# NÚMEROS PRIMOS E O TEOREMA FUNDAMENTAL DA ARITMÉTICA NO SEXTO ANO DO ENSINO FUNDAMENTAL

**Fernando Ramires Carvalho**

## Resumo

O objetivo deste trabalho é apresentar o conteúdo que um professor da educação básica deve dominar para desenvolver e aplicar um trabalho em uma turma de 6º ano sobre divisibilidade e números primos.



**Palavras-chave:** Aritmética, divisibilidade, números primos.

## Abstract

The objective of this paper is to introduce what a basic education teacher must know to work on a project with a $6^{th}$ grade class about divisibility and primes numbers.



**Key words:** Arithmetic, divisibility, primes numbers.

**SUMÁRIO**


**1. Introdução 5**

**2. Introdução à História da Teoria Elementar dos Números 9**

**3. Teorema Fundamental da Aritmética 19**

**3.1 Divisibilidade: conceitos e propriedades 19**

**3.1.1 Definição de divisibilidade 19**

**3.1.2 Propriedades da divisibilidade 19**

**3.2 Algoritmo da Divisão 27**

**3.3 Máximo divisor comum e Algoritmo de Euclides 30**

**3.3.1 Máximo divisor comum 30**

**3.3.2 Algoritmo de Euclides 32**

**3.3.3 Propriedades do mdc 34**

**3.4 Mínimo múltiplo comum 39**

**3.5 Números Primos 41**

**3.5.1 Conceito e Propriedades 41**

**3.5.2 Números especiais 43**

**3.5.3 O conjunto dos números primos é infinito 45**

**3.5.4 A distribuição dos números primos 46**

**3.6 Teorema Fundamental da Aritmética 49**

**3.6.1 Enunciado e demonstrações 49**

**3.6.2 Aplicações do Teorema Fundamental da Aritmética 49**

**4. Considerações Finais 52**

**Referências 52**

# 1 Introdução

Esta dissertação tem como objetivo geral apresentar o Teorema Fundamental da Aritmética (TFA) e analisar suas possibilidades de ensino no 6º ano do Ensino Fundamental.

Segundo Alencar Filho (1988), o TFA garante que todo número natural maior do que um, ou é primo, ou pode ser decomposto de maneira única num produto de números primos, a menos de permutações dos fatores. Dessa forma, os conceitos que se associam favorecendo a sua compreensão são as relações de múltiplos e fatores que podem se estabelecer entre um par de números naturais e as propriedades que derivam destas relações, os critérios de divisibilidade, a diferenciação entre primos e compostos e decomposição de um número em fatores primos.

É importante destacar a relevância de tais conceitos dentro do corpo de conhecimentos matemáticos a serem estudados pelos alunos durante os ensinos Fundamental e Médio. Conhecendo alguns critérios de divisibilidade, o aluno pode efetuar cálculos mentais e estimativas. Observando a decomposição de números naturais em fatores primos, podemos obter rapidamente o mínimo múltiplo comum (m.m.c.) e o máximo divisor comum (m.d.c.) destes números, calcular o número de divisores de cada um ou mesmo listá-los.

Em 1998, o Governo Federal publicou os Parâmetros Curriculares Nacionais (PCN), documento que aponta diretrizes para a construção dos currículos escolares. Eles receberam críticas relacionadas à linguagem (apontada como elemento dificultador da compreensão da proposta) e à sua presença num contexto democrático (como estabelecer um currículo comum numa democracia?). Entretanto, no que diz respeito à Matemática, concordamos com Angeloe Silva (2008) que:"(...) os documentos são relevantes, uma vez que estes refletem as recomendações dos educadores matemáticos desde os anos 80 e sistematizam questões de primeira ordem sobre o ensino e a aprendizagem dessa área do conhecimento"(p.33). Tanto o PCN de Matemática para 1ª a 4ª série quanto aquele que se volta para 5ª a 8ª série distribui os conteúdos matemáticos a serem trabalhados no Ensino Fundamental em quatro blocos: *números e operações*, *espaço e forma*, *grandezas e medidas* e *tratamento da informação.* O TFA e

os demais conceitos associados a ele pertencem ao bloco *números e operações* e, sendo assim, na maioria das escolas brasileiras e nos livros didáticos, são apresentados desde o 4º ano (antiga 3ª Série) do Ensino Fundamental, sendo retomado nos anos subsequentes apenas com aumento gradual dos números, cuja decomposição é solicitada aos alunos.

Cabe mencionar ainda que, além de elencar os conteúdos a serem estudados, os PCN refletem sobre o ensino e, no caso do ensino da Aritmética, sugerem uma abordagem mais reflexiva dos números considerando que o aluno deve perceber

> a existência de diversos tipos de números (naturais, negativos, racionais e irracionais) bem como de seus diferentes significados à medida que deparar com situações-problema, envolvendo operações ou medidas de grandeza, como também ao estudar algumas das questões que compõem a história do desenvolvimento matemático (PCN, 1998, p. 50).

Em outras palavras, com relação às operações, o trabalho a ser realizado deve se concentrar na compreensão dos diferentes significados dos números e operações, nas relações existentes entre eles e suas propriedades. Entretanto, as pesquisas mais recentes em Educação Matemática sinalizam a existência de problemas no ensino e na aprendizagem da Aritmética. Embora ocorra, observamos um tratamento mecanizado, com base em exercícios repetitivos e problemas idealizados. Os alunos não têm tido oportunidade de descobrir variações nos algoritmos que possam ser úteis para o desenvolvimento de habilidades de cálculo mental e estimativas. Lins e Gimenez reforçam esta constatação ao afirmarem que:

> Os conceitos aritméticos usados na Educação Matemática têm correspondido a relações quantitativas sobre coleções de objetos. Tem-se esquecido frequentemente que a aritmética inclui também: a) representações e significações diversas (pontos de referência e núcleos, que ampliam a ideia simples do manipulativo); b) análise do porquê dos algoritmos e divisibilidade (elementos conceituais); c) uso adequado e racional de regras (técnicas, destrezas e habilidades); e d) descobertas ou "teoremas" (descobertas, elaboração de conjecturas e processos de raciocínios). (LINS e GIMENEZ, 1997, p. 33).

Especificamente sobre o TFA, Coelho et al. (2005) investigaram a compreensão do TFA por professores de Matemática em curso de formação continuada e por alunos de 8ª série do Ensino Fundamental de São Paulo. As autoras concluíram que, comparativamente, existem diferenças entre os dois grupos. Na maioria das vezes, o grupo de alunos reproduz algoritmos sem saber interpretar cada etapa de suas ações e seus resultados. Voltando-se para o grupo de professores, elas perceberam uma compreensão conceitual mais aprofundada, decorrente do estudo recente da Teoria dos Números no curso de formação continuada que estão frequentando. Este estudo permitiu ainda a conclusão de que é possível criar cursos voltados para estudantes

brasileiros de qualquer nível de ensino nos quais a compreensão conceitual seja enfatizada, mas, o professor deve estar atento para que essa abordagem não seja perturbada por um ensino prévio muito calcado em algoritmos.

Assim, reforçamos a necessidade de uma abordagem que priorize a formação de conceitos e não simplesmente a memorização de algoritmos, desde os anos iniciais do Ensino Fundamental, ou seja, justificamos nossa pesquisa. Se a construção de conceitos não for favorecida, o indivíduo enfrentará dificuldades durante sua vida escolar, sobretudo, quando confrontado com situações que lhe exijam tomar decisões e estabelecer estratégias de resolução de problemas. As dificuldades poderão se fazer presentes, inclusive, em níveis de ensino mais elevados. Ideias mal concebidas inicialmente se constituirão em obstáculos para a compreensão de futuros conceitos.

Sintetizando os objetivos gerais de um trabalho curricular aritmético diferente do mecanizado baseado em algoritmos que está presente no ensino tradicional, Lins e Gimenez (1997), propõem que o ensino deve:

> - Buscar a compreensão da quantidade e a observação e a manipulação de processos operativos.
> - Fomentar a criatividade e a sensibilidade na busca de propriedades e relações.
> - Conhecer, assumir e usar uma metodologia heurística, motivando a intuição para ajudar a formulação de hipóteses, generalizações e, em alguns casos, estratégias indutivas.
> - Reconhecer processos dedutivos e iterativos usados na história, tentando reconhecer e identificar seus fundamentos, e reviver suas reflexões (p. 40-44).

Influenciadas pelas ideias de Lins e Gimenez (1997) e Coelho et al. (2005), as pesquisas de Barbosa (2008),Groenwald, Franke eOlgin(2009) eGroenwald eOlgin (2010) descrevem intervenções de ensino voltadas para tópicos da Teoria dos Números que foram aplicadas e promoveram a aprendizagem significativa em alunos do Ensino Fundamental. Já Machado e Oliveira (2015), com base numa análise minuciosa de livros didáticos de Matemática do Ensino Médio, propõem a inclusão do tópico equações diofantinas neste nível de ensino.

Groenwald, Franke e Olgin (2009) desenvolveram atividades envolvendo as aplicações da Teoria dos Números à criptografia em turmas de 9º ano. Groenwald eOlgin(2010) retomaram esta proposta inserindo o uso da calculadora como recurso didático e Barbosa (2008) desenvolveu, aplicou e analisou à luz da Teoria dos Campos Conceituais uma longa intervenção de ensino visando a compreensão e aplicação na simplificação de cálculos do Teorema Fundamental da Aritmética por alunos do 6º ano do Ensino Fundamental. Em suas análises, Barbosa (2008) verificou que o TFA não pode ser ensinado isoladamente, pois existem outros conceitos, já mencionados neste texto, que se associam a ele permitindo a sua compreensão. Além disso, constatou que, com base nos padrões numéricos envolvidos nas situações problema

que vivenciaram, os alunos realizaram generalizações. A compreensão do TFA demandou dos alunos o percurso de um longo caminho que teve início na distinção entre divisões exatas e não exatas, passando pelos conceitos de múltiplo e fator e suas propriedades, conceitos de primos e compostos e decomposição em fatores primos. Esse percurso, no entanto, não é linear. Nele os alunos cometem e superam parcial ou totalmente determinados erros, levantam, testam, validam ou refutam hipóteses. Além disso, podem recorrer a materiais manipulativos e utilizar várias representações como desenhos, tabelas, além do registro numérico tradicional.

Este trabalho pretende ser parte de um trabalho maior; uma pesquisa qualitativa em educação com características de um estudo de caso. Apresentamos as principais definições, teoremas e propriedades relacionados ao Teorema Fundamental da Aritmética.

# 2 Introdução à História da Teoria Elementar dos Números

O estudo da História da Matemática, até então, não possui fixado, seu local de destaque na formação de professores. Este fato tem reflexão direta na dinâmica de uma sala de aula, visto que não é habitual que educadores procurem utilizar este recurso de ensino, que é a contextualização histórica dos conceitos matemáticos que se pretende ensinar, na maioria das classes. Grande parte dos educandos mistifica essa disciplina por não entender de que forma ela evoluiu, que grandes conjecturas permaneceram em aberto por séculos até serem provadas e quantas ainda permanecem. De acordo com os Parâmetros Curriculares Nacionais de matemática, de 1997, temos:

> *"Ao revelar a Matemática como uma criação humana, ao mostrar necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, ao estabelecer comparações entre os conceitos e processos matemáticos do passado e do presente, o professor tem a possibilidade de desenvolver atitudes e valores mais favoráveis do aluno diante do conhecimento matemático.*
>
> *Além disso, conceitos abordados em conexão com sua história constituem-se veículos de informação cultural, sociológica e antropológica de grande valor formativo. A História da Matemática é, nesse sentido, um instrumento de resgate da própria identidade cultural.*
>
> *Em muitas situações, o recurso à História da Matemática pode esclarecer ideias matemáticas que estão sendo construídas pelo aluno, especialmente para dar respostas*

*a alguns "porquês" e, desse modo, contribuir para a constituição de um olhar mais crítico sobre os objetos de conhecimento."*

Partindo dessa premissa, apresentaremos um breve estudo sobre a História da Teoria dos Números, desde a Grécia antiga, até a evolução de uma abordagem elementar para a discussão moderna desta teoria.

Relatar fatos históricos sobre o surgimento da Teoria dos Números é narrar sobre o instante em que os números deixaram de ser meras ferramentas para cálculos, contagens e medições e assumiram a posição de objetos de reflexão. A humanidade passa então a especular sobre as propriedades do número, sobre suas relações, pensando em estudá-los de maneira sistêmica. Uma data e um protagonista, para tal evento, determinados com exatidão numa linha do tempo da História da Matemática, são dados pouco palpáveis, visto que as fontes não possuem total credibilidade. Contudo, atribui-se à Pitágoras, filósofo e matemático grego, nascido entre 580a.C. e 500a.C., e aos estudiosos que constituíam a Escola Pitagórica, fundada pelo mesmo, a autoria dos primeiros estudos sobre a essência numérica.

Para os pitagóricos os números eram mais do que elementos matemáticos, eram traduções da realidade. Com uma visão mística, estes pensadores acreditavam que tudo poderia ser explicado através deles. Os membros dessa Escola são considerados como os pioneiros na discussão sobre as propriedades numéricas, dentre os vários assuntos abordados, há registros sobre a ideia de primalidade e sobre números perfeitos, que eram aqueles iguais a soma de seus divisores, excetuado, claro, ele próprio. Porém, a compreensão de tais matemáticos sobre os conceitos mencionados era concreta, existia uma íntima relação entre a aritmética e a geometria, sendo os números figurados a base para seus exemplos e generalizações. Os números figurados dos pitagóricos eram

conjuntos de elementos discretos, que representaremos aqui por pontos. Seguem as configurações que eram utilizadas, por exemplo, para diferenciar um número primo de um composto:

Disposições de elementos discretos em forma de retângulos, representado o número 16:

Disposição de elementos discretos em forma de retângulo, representando o número 15:

Disposição de elementos discretos em forma de linha, representando o número 7:



Note que o número 7, segundo essa concepção, não pode ser representado por um retângulo, somente por uma linha. Tais números eram ditos “primários” ou ainda “lineares”, ou seja, eram números que quando combinados, formavam os demais, que podiam ser representados por retângulos, conhecidos por nós como números compostos.

Foi com Euclides, matemático grego que viveu em torno de 300 a.C. , que a matemática ganhou formalidade. Sua principal obra, os Elementos, composta por treze livros que resumem a maior parte do conhecimento matemático da época, nos apresenta o método axiomático-dedutivo, onde a partir de fatos tido como verdades: definições ou postulados, chega-se através de uma sequência lógica, as demonstrações, aos resultados: propriedades, lemas ou teoremas. Em tais escritos encontramos fundamentos, nem todos de autoria do próprio Euclides, que são os pilares da matemática, sendo ensinados até hoje tanto nas escolas em cursos elementares, como em universidades em cursos avançados. Eles tratam sobre Geometria Plana, nos livros de I a VI, Teoria dos Números nos livros de VII a IX, os incomensuráveis no livro X e Geometria Espacial nos livros de XI a XIII.

Seguiremos com comentários a respeito da aritmética encontrada nos Elementos.

Euclides fez uma abordagem da Teoria dos Números tratando os mesmos como segmentos de reta, no livro VII encontramos definições, como a terceira, que nos diz "um número é parte de um número, o menor do maior, quando mede o maior", equivalente, para nós, à definição de divisor. Considere a ilustração abaixo, onde CD mede AB, já que sendo CD = m e AB= 4m, temos AB = 4CD, ou seja, CD é um divisor de AB.



Neste mesmo livro temos o famoso Algoritmo de Euclides, tal como é conhecido nos dias de hoje, estando descrito nas proposições 1 e 2.

*"Proposição 1:Sendo dados dois números desiguais, se o menor quando continuamente retirado do maior, nos deixa um resto que nunca mede o número precedente, até sobrar a unidade, então dizemos que os números originais são primos entre si.*

*Proposição 2: Encontrar a maior medida comum entre dois números que não são primos entre si."*

Na linguagem atual, escreveríamos: Dados dois números diferentes, subtrai-se o menor d do maior D, repetidamente, até obtermos um resto $r_1$, tal que $r_1 < d$; assim, subtrai-se repetidamente $r_1$ de d até resultar um resto $r_2 < r_1$; então subtrai-se repetidamente $r_2$ de $r_1$; e assim por diante. O processo nos conduz a um resto $r_n$ que mede $r_{n-1}$, da mesma forma que todos os restos precedentes, bem como d e D; este número $r_n$ é o máximo divisor comum de d e D.

Números em proporção continuada, ou seja, em progressão geométrica, são o assunto do livro VIII.

É no livro IX, na proposição 20, que está o resultado mais interessante da obra. Nesta proposição, Euclides prova que há infinitos números primos, usando a redução ao absurdo: Suponha seja finito o número de primos. Tome P como sendo o produto de todos esses números e ainda, consideremos, K = P + 1. Logo, K não pode ser primo, pois a hipótese seria contrariada, uma vez que P é produto de todos os primos. Assim, só nos resta afirmar que K é composto e deve então ser medido por algum p, primo.

Porém, p não poderia ser um fator de P, pois automaticamente seria também fator de 1. Assim, p é um primo diferente daqueles que são fatores de P, levando ao absurdo.

A evolução da Teoria dos Números foi lenta. Após os Elementos, temos destaque apenas para o livro do grego Nikomachos (100 d.C), Arithmetiké, que deu base para a primeira obra deste campo matemático escrita em latim, De InstitutioneArithmetica, do romano Boethius (500 d.C). No decorrer da idade média, esta última fonte foi a principal pra divulgar o conhecimento matemático sobre as propriedades numéricas.

O renascimento científico, por volta de 1200, contou com a grande contribuição de Leonardo de Pisa, conhecido como Fibonacci, cujo livro, LiberAbbaci, que tratou sobre métodos e problemas algébricos, além de divulgar os algarismos indo-arábicos. Encontramos nele o problema que dá origem a tão conhecida sequência de Fibonacci:

*Quantos pares de coelhos serão produzidos num ano, começando com um só par, se em cada mês cada par gera um novo par que se torna produtivo a partir do segundo mês?*

A questão nos conduz a sequência (1, 1, 2, 3, 5, 8, 13, 21 ,...), expressa algebricamente na atualidade por $a_n = a_{n-1} + a_{n-2}$, ou seja, cada termo após os dois primeiros é igual à soma dos dois anteriores.

Foi no século XVII, que viveu o fundador da moderna Teoria dos Números. Pierre de Fermat (1601-1665), jurista francês e matemático amador, foi tido como o mais célebre estudioso que contribuiu para o desenvolvimento da Teoria dos Números. Apesar de não ter feito publicações ou exposições sistemáticas de suas produções, seus registros inspiraram grandes matemáticos que vieram depois dele. Um fato que vale ser citado foi a busca por uma fórmula que fornecesse os números primos, que aliás perdura

até hoje, levou Fermat a conjecturar que os números da forma $F_n = 2^{2^n} + 1$ são primos para todo n, inteiro não negativo. Ele provou ser verdade para n= 0, 1, 2, 3 e 4:

$F_0 = 2^{2^0} + 1 = 3$

$F_1 = 2^{2^1} + 1 = 5$

$F_2 = 2^{2^2} + 1 = 17$

$F_3 = 2^{2^3} + 1 = 257$

$F_4 = 2^{2^4} + 1 = 65537$

Assim, assumiu que para $n \geq 5$, todos os $F_n$ também seriam primos. Porém, essa conjectura se revelou falsa quando Leonard Euler (1707-1783) mostrou que para n = 5, ela não tinha validade, $F_5 = 2^{2^5} + 1 = 4.294.967.297 = 641 \cdot 6.700.417$, ou seja, $F_5$ é divisível, por exemplo, por 641, logo não é primo.

Sua mais famosa contribuição foi o teorema que ficou conhecido como "O último Teorema de Fermat". Em seu exemplar do livro "Aritmética" de Diofanto (III a. C.), onde se encontravam descritas as infinitas soluções da equação pitagórica $x^2 + y^2 = z^2$, ele deixou a seguinte anotação:

> *"Por outro lado, é impossível separar um cubo em dois cubos, ou uma biquadrada em duas biquadradas, ou, em geral, uma potência qualquer, exceto um quadrado em duas potências semelhantes. Eu descobri uma demonstração verdadeiramente maravilhosa disto, que todavia esta margem não é sufcientemente grande para cabê-la."*

O enunciado deste teorema afirma que não existem inteiros não nulos, a , b e c , tais que $a^n + b^n = c^n$, para $n > 2$.

Por mais de três séculos grandes matemáticos se debruçaram sobre esta questão. As inúmeras tentativas, ainda que mal sucedidas, tiveram grandes implicações para o desenvolvimento da matemática e consequentemente de outras ciências. Podemos citar como produtos acadêmicos resultantes da busca pela demonstração de tal teorema a Teoria dos Anéis Comutativos e ainda dos Números Complexos Ideais. Foi somente em 1995, que o matemático britânico Andrews Wiles conseguiu vencer esse desafio.

Leonard Euler (1707-1783) já citado acima, foi um dos maiores matemáticos de todos os tempos. Com contribuições em diversos campos da matemática, como no cálculo diferencial e integral e na teoria dos números, na mecânica e na música, ele se revelou um ícone da produtividade científica. Em se tratando de aritmética, cabe a ele por exemplo,a primeira demonstração do Pequeno Teorema de Fermat: Dado um número primo p, tem-se que p divide o número $a^p$ – a, para todo a $\in \mathbb{N}$, que apresentaremos mais adiante.

Segundo [HEFEZ, p127], Carl Friederich Gauss (1777-1855) foi considerado pelos seus contemporâneos e pelas gerações que o sucederam, um príncipe da rainha das ciências, um príncipe da Matemática. Aos 19 anos, solucionou a questão sobre que polígonos regulares de n lados poderiam ser inscritos num círculo, usando régua e compasso, sendo n primo. Obteve como resposta que o número de lados deveria ser um primo da forma $2^{2^k} + 1$, para que um polígono pudesse ser construído de tal maneira. Como consequência, demonstrou que um polígono de 7 lados não poderia ser construído com régua e compasso.

A busca por um padrão na distribuição dos números primos, levou Gauss a refletir sobre a relação entre a quantidade de primos entre 1 e N e a função logarítmica. Segundo [DU SAUTOY,M., p56]:

*"O grande avanço de Gauss foi fazer uma pergunta diferente. Em vez de tentar prever a localização precisa do próximo primo, ele buscou ao menos descobrir quantos primos haveria entre os primeiros 100 números, os primeiros 1.000 e assim por diante. Se tomássemos o número N, haveria alguma maneira de estimar quantos primos encontraríamos entre os números 1 e N?"*

Podemos acrescentar ainda, aos exemplos de contribuição de Gauss para a Teoria dos números, que o mesmo com 21 anos de idade, introduziu o conceito de congruência, ou seja, da aritmética dos restos de uma divisão euclidiana, em sua obra mais célebre, o livro Disquisitiones Arithmeticae.

A abordagem feita acima, nos permite ter uma visão, ainda que geral, sobre a forma como evoluiu a Teoria dos Números. Seria válido ainda citar que são inúmeras as conjecturas que permanecem como alvos de investigação, necessitando ser provadas. Citaremos, para finalizar um desses casos, que é a conjectura de Goldbach (1690 – 1764): "Todo número inteiro par maior que dois é a soma de dois primos". Milhares de somas que verificam a veracidade dessa afirmação já foram encontradas, contudo, até hoje ninguém conseguiu prová-la.

Ao educador cabe não somente ter se apropriado dos conceitos que pretende ensinar, é necessário que sua esfera de conhecimento seja mais abrangente. Elaborar uma metodologia de ensino dotada de estratégias que estimulem a capacidade de dedução, a memorização e a habilidade de generalizar é possível quando o profissional de educação matemática se envolveu de forma mais avançada com os teoremas e propriedades que embasam suas aulas. Consideramos que os tópicos que serão abordados a seguir são essenciais para o educador conceber uma forma própria de trabalhar, num nível adequado às turmas do sexto ano do Ensino Fundamental, com as

ideias de divisibilidade, múltiplos, divisores, divisão euclidiana, números primos e o Teorema Fundamental da Aritmética. A maneira como tais conceitos são discutidos nesse primeiro momento de aprendizagem pode guiar o estudante a uma concepção sólida, em seu futuro contato com tópicos menos elementares. Logo, entendemos que o educando não deve limitar-se a reprodução. Para subir os degraus da abstração, ele precisa construir definições, refletir e argumentar sobre conceitos e processos matemáticos, orientado pelo professor que domina o assunto em patamares mais elevados.

# 3 Teorema fundamental da aritmética

## 3.1 Divisibilidade: Conceitos e Propriedades

Iniciaremos a discussão sobre divisibilidade, no conjunto dos números naturais, em um caminho distinto dos livros didáticos tradicionais. Usualmente o que vemos nas salas de aula é a definição de divisibilidade atrelada a noção de divisão euclidiana. Um número é considerado divisível por outro quando sua divisão por ele deixa resto zero. Ao partir dessa premissa, podemos levar os alunos a pensar que a divisão somente pode ser realizada quando um número é divisível por outro, criando um obstáculo para a aprendizagem de posteriores divisões que deixam restos não nulos.

Assim, partiremos da ideia de que um número é divisível por outro quando é múltiplo do mesmo.

### 3.1.1 Definição de Divisibilidade

Considere dois números naturais $d$ e $D$, teremos que $d$ divide $D$, escrevendo $d|D$, quando existir $q \in \mathbb{N}$ tal que $D = qd$. Podemos afirmar ainda que $d$ é um divisor ou um fator d e $D$, ou, ainda, que $D$ é um múltiplo de $d$, ou que $D$ é divisível por $d$.

Assim a sentença $d|D$ nos diz que existe um $q$ tal que $D = qd$. A mesma pode ser negada através da simbologia $d \nmid D$, significando que não existe nenhum número natural $q$ tal que $D = qd$.

### 3.1.2 Propriedades da Divisibilidade

#### Proposição 1

Sejam $n_1, n_2, n_3 \in \mathbb{N}$. Tem-se que

i) Todo número natural é divisível por 1, ou seja, $1|n_1$;

ii) Todo número natural é divisível por ele mesmo, ou seja, $n_1|n_1$;

iii) Todo número natural é divisor de zero, ou seja, $n_1|0$.

iv) O único número que tem o zero como divisor é o próprio zero, ou seja, $0|n_1 \Leftrightarrow n_1 = 0$.

v) Se $n_1|n_2$ e $n_2|n_3$, então $n_1|n_3$.

vi) Se $n_1|n_2$ e $n_1|n_3$, então $n_1|n_2 + n_3$.

## Demonstração

(i) Decorre diretamente da igualdade $n_1 = n_1 \cdot 1$;

(ii) Decorre diretamente da igualdade $n_1 = 1 \cdot n_1$;

(iii) Decorre diretamente da igualdade $0 = 0 \cdot n_1$;

(iv) Partiremos do princípio que $0| n_1$; temos com isso que existe $q \in \mathbb{N}$ tal que $n_1 = q \cdot 0$, o que implica $n_1 = 0$. Para a recíproca basta observar que $0|0$, o que foi provado (iii);

(v) $n_1|n_2$ e $n_2|n_3$ logo existem $q_1, q_2 \in \mathbb{N}$, tais que $n_2 = q_1 n_1$ e $n_3 = q_2 n_2$. Substituindo o valor de $n_2$ da primeira equação na outra, obtemos

$$n_3 = q_2 n_2 = q_2(q_1 n_1) = (q_2 q_1) n_1,$$

o que nos mostra que $n_1| n_3$.

(vi) $n_1|n_2$ e $n_1|n_3$ logo existem $q_2, q_3 \in \mathbb{N}$, tais que $n_2 = q_2n_1$ e $n_3 = q_3n_1$. Então, $n_2 + n_3 = q_2n_1 + q_3n_1 = (q_2 + q_3)\, n_1$, o que mostra que $n_1|n_2 + n_3$.

Consideraremos então o caso 0 | 0 (estamos assumindo que $0 \in \mathbb{N}$) e, portanto, todo número natural divide 0. Assim, 0 tem infinitos divisores.

## Definição

Tomando como verdade que $d|D$ e que $d \neq 0$. Seja $q \in \mathbb{N}$ tal que $D = qd$. O número natural $q$, univocamente determinado, é chamado de *quociente* de $D$ por $d$ e denotado por $q = \frac{D}{d}$.

## Proposição 2

Se $n_1, n_2, n_3, n_4 \in \mathbb{N}$, então

$$n_1|n_2 \text{ e } n_3|n_4 \implies n_1n_3|n_2n_4.$$

## Demonstração

Se $n_1|n_2$ e $n_3|n_4$, então $\exists q_1, q_2 \in \mathbb{N}$, $n_2 = q_1n_1$ e $n_4 = q_3n_3$. Portanto, $n_2n_4 = (q_1q_2)(n_1n_2)$, logo, $n_1n_3|n_2n_4$.

Em particular, se $n_1|n_2$, então $n_1q|n_2q$, para todo $q \in \mathbb{N}$.

## Proposição 3

Sejam $d, D_1, D_2 \in \mathbb{N}$, $D_1 > D_2$ tais que $d|(D_1 \pm D_2)$. Então

$$d|D_1 \Leftrightarrow d|D_2.$$

## Demonstração

Partiremos do princípio que $d|(D_1 + D_2)$. Logo, existe $q \in \mathbb{N}$ tal que $D_1 + D_2 = qd$.
Então, se $d|D_1$, temos que existe $q_1 \in \mathbb{N}$ tal que $D_1 = q_1 d$.
A partir das duas igualdades acima, temos

$$q_1 d + D_2 = qd,$$

Com isso temos que $D_2 = (q - q_1)d$, logo $d|D_2$.
Analogamente para o caso em que d| $D_2$.

Observando a outra premissa, partiremos do princípio que $d|(D_1 - D_2)$. Logo, existe $q \in \mathbb{N}$ tal que $D_1 - D_2 = qd$.

Então, se $d|D_1$, temos que existe $q_1 \in \mathbb{N}$ tal que $D_1 = q_1 d$. Juntando as duas igualdades acima, temos

$$q_1 d - D_2 = qd,$$

Com isso temos que $D_2 = (q_1 - q)d$, logo $d|D_2$.

## Proposição 4

Se $d, D_1, D_2 \in \mathbb{N}$ são tais que $d|D_1$ e $d|D_2$, então para todo $x, y \in \mathbb{N}$

$$d|(xD_1 + yD_2).$$

## Demonstração

$d|D_1$ e $d|D_2$ implicam que existem $q_1, q_2 \in \mathbb{N}$ tais que $D_1 = q_1 d$ e $D_2 = q_2 d$. Logo,

$$xD_1 + yD_2 = x(q_1 d) + y(q_2 d) = (xq_1 + yq_2)d.$$

Com isso, $d|(xD_1 + yD_2)$.

## Proposição 5

Dados $d, D \in \mathbb{N}$, onde $D \neq 0$, temos que

$$d|D \Longrightarrow d \leq \mathrm{D}.$$

## Demonstração

De fato, se $d|D$, existe $q \in \mathbb{N}$ tal que $D = qd$. Como $D \neq 0$, temos que $q \neq 0$, logo $1 \leq$ q e, consequentemente, $d \leq qd = D$.

Podemos deduzir da proposição 5 dois importantes resultados:

(i) O único divisor 1 é ele mesmo.

Claro, se $d \in \mathbb{N}$ e $d|1$, então $0 < d \leq 1$, logo $d = 1$.

(ii) Um número natural D, possui um número finito de divisores.

Como, para $D \neq 0$, temos que todo divisor $d$ de $D$ é tal que $d \leq D$, segue-se, nesse caso, que $D$ tem um número finito de divisores que estão no intervalo $1 \leq d \leq D$.

Note que a relação de divisibilidade em $\mathbb{N}$ é uma relação de ordem, pois:

i) é reflexiva: $\forall\, n \in \mathbb{N}$, $n|n$.

ii) é transitiva: se $n_1|n_2$ e $n_2|n_3$, então $n_1|n_3$.

ii) é antissimétrica: se $n_1|n_2$ e $n_2|n_1$, então $n_1 = n_2$.

Aprofundando nosso estudo sobre as propriedades da divisibilidade, apresentaremos alguns critérios envolvendo a divisão de binômios:

## Proposição 6

Sejam $x, y, n \in \mathbb{N}$, $x > y$, $n \neq 0$. Temos que $x - y$ divide $x^n - y^n$.

## Demonstração

Provaremos por indução sobre $n$.

É fácil ver que a afirmação é verdadeira para $n = 1$, pois $x - y$ divide $x^1 - y^1 = x - y$.

Partiremos do princípio que $(x - y)|(x^n - y^n)$. Assim,

$$x^{n+1} - y^{n+1} = xx^n - yx^n + yx^n - yy^n = (x - y)x^n + y(x^n - y^n).$$

Como $(x - y)|(x - y)$e, por hipótese, $(x - y)|(x^n - y^n)$, decorre da igualdade acima que $x - y|x^{n+1} - y^{n+1}$.

Como provamos ser verdadeira a sentença para n + 1, podemos afirmar que ela também é válida para todo $n \in \mathbb{N}$.

Exemplificando o caso acima, temos a seguinte questão:

Prove que $8 | (3^{2n} - 1)$.

Ora, uma vez que já mostramos ser verdade que $x - y$ divide $x^n - y^n$, basta reescrevermos a expressão dada no enunciado:

$8 | (3^{2n} - 1) = (9 - 1) | ((3^2)^n - 1) = (9 - 1) | (9^n - 1)$, considerando x = 9 e y = 1, está provado.

## Proposição 7

Sejam $x, y, n \in \mathbb{N}$. Temos que $x + y$ divide a $x^{2n+1} + y^{2n+1}$.

## Demonstração

Provaremos por indução sobre $n$.

É fácil ver que a afirmação é verdadeira para $n = 0$, pois $x + y$ divide $x^1 + y^1 = x + y$.

Partiremos do princípio que $(x + y) | (x^{2n+1} + y^{2n+1})$. Assim,

$x^{2(n+1)+1} + y^{2(n+1)+1} = x^2x^{2n+1} - y^2x^{2n+1} + y^2x^{2n+1} + y^2y^{2n+1} = (x^2 - y^2)x^{2n+1} + y^2(x^{2n+1} + y^{2n+1})$.

Como temos que $x + y$ divide $x^2 - y^2$, pois, $x^2 - y^2 = (x + y)(x - y)$, e, além disso, admitimos por hipótese, que $(x + y) | (x^{2n+1} + y^{2n+1})$,decorre da igualdade acima, que $(x + y) | (x^{2(n+1)+1} + y^{2(n+1)+1})$.

Como provamos ser verdadeira a sentença para n + 1, podemos afirmar que ela também é válida para todo $n \in \mathbb{N}$.

## Proposição 8

Sejam $x, y, n \in \mathbb{N}$. Temos que $x + y$ divide $x^{2n} - y^{2n}$.

## Demonstração

Provaremos por indução sobre $n$.

É fácil ver que a afirmação é verdadeira para $n = 1$, pois claramente $x + y$ divide $x^2 - y^2 = (x + y)(x - y)$.

Partiremos do princípio que $(x + y) | (x^{2n} - y^{2n})$. Assim,

$$x^{2(n+1)} - y^{2(n+1)} = x^2 x^{2n} - y^2 x^{2n} + y^2 x^{2n} - y^2 y^{2n} =$$
$$(x^2 - y^2) x^{2n} + y^2 (x^{2n} - y^{2n}).$$

Como temos que $x + y | x^2 - y^2$e, além disso, admitimos por hipótese, que $(x + y) | (x^{2n} - y^{2n})$, decorre das igualdades acima que $(x + y) | (x^{2(n+1)} + y^{2(n+1)})$.

Como provamos ser verdadeira a sentença para n + 1, podemos afirmar que ela também é válida para todo $n \in \mathbb{N}$.

## 3.2 Algoritmo da Divisão

### Processo de Divisão Euclidiana

Veremos agora um importante resultado descrito por Euclides, em sua mais famosa obra, *Os Elementos*. Esse resultado trata do fato de que dados dois números naturais d e D, com $d \neq 0$, é sempre possível realizar a divisão de D por d, ainda que haja um pequeno resto. Tal algoritmo continua sendo a forma mais prática de se efetuar uma divisão com resto, e por isso, é marcante sua presença nas salas de aula e nos livros didáticos de matemática do Ensino Básico.

### Teorema

Sejam $D$ e $d$ dois números naturais com $d \neq 0$. Existem dois únicos números naturais $q$ e $r$ tais que

$$D = dq + r, \quad \text{como } 0 \leq r < d.$$

Onde $D$ é chamado de dividendo, $d$ de divisor, $q$ de quociente $r$ de resto.

### Demonstração

Se $D < d$ então $q = 0$ e $r = D$. Se $D = d$, então $q = 1$ e $r = 0$. Suponha, então, que $D > d$.

Provaremos primeiro a existência: Considere, enquanto fizer sentido dentro do conjunto dos naturais, os números:

$D$, $D - d$, $D - 2d$, $D - 3d$, ... ,$D - nd$, ..., como sendo elementos de um determinado conjunto $S$.

Pelo Princípio da Boa Ordem, o conjunto $S$ formado pelos números acima possui um menor elemento $r = D - qd$. Queremos mostrar que $r < d$.

Temos duas possibilidades:

Se $d|D$, o resultado é imediato, já que $r = 0 < d$.

Pensaremos agora no caso em que $d \nmid D$, ou seja, $r \neq d$. Fica claro que $r < d$, pois se não, admitiríamos a existência de um número natural $a < r$ tal que $r = a + d$. Consequentemente, sendo $r = a + d = D - qd$, teríamos

$$a = D - (q + 1)d \in S, \text{ com } a < r,$$

Essa sentença contradiz a hipótese, que afirma ser $r$ o menor elemento de $S$.

Logo, temos que $D = dq + r$ com $r < d$, o que prova a existência de $q$ e $r$.

Agora provaremos a unicidade: Tomando a diferença entre dois elementos distintos de $S$ temos um múltiplo de $d$. Sendo o valor mínimo desta diferença igual ao próprio $d$. Logo, se $r = D - dq$ e $r' = D - dq'$, com $r < r' < d$, teríamos $r' - r \geq d$, o que implica que $r' \geq r + d \geq d$, que é um absurdo. Com isso, $r' = r$, e, por consequência, $dq' = dq$ e $q' = q$.

Podemos então escrever uma nova definição para divisibilidade: Dizemos que $d$ divide $D$, se, e somente se, o resto da divisão euclidiana de $D$ por $d$ é zero.

Com o resultado que nos garante a unicidade de q e r na divisão euclidiana de $D$ por $d$, construiremos a função que segue:

Denotamos por $q_d(D)$ o quociente da divisão do número $D$ por $d$, definimos a *função quociente* por $d$ como segue:

$$q_d : \mathbb{N} \longrightarrow \mathbb{N}$$
$$D \longmapsto q_d(D)$$

## Corolário

Dados dois números naturais $D$ e $d$ com $d > 0$, existe um único número natural $n$ $(=q_d(D))$ tal que

$$nd \leq D < (n + 1)d.$$

## Demonstração

Pela divisão euclidiana, temos que existem $q, r \in \mathbb{N}$, únicos,com $0 \leq r < b$, tais que $D = dq + r$. Considere $n = q$, está provado.

O natural$q_d(D)$ pode ser também interpretado como o maior natural menor ou igual do que o número racional $\frac{D}{d}$.

De fato, temos que, se $r$ é o resto da divisão de $D$ por $d$, então

$$q_d(D)d \leq D = q_d(D)d + r < (q_d(D) + 1)d, \text{ logo,}$$

$$q_d(D) \leq \frac{D}{d} < q_d(D) + 1.$$

Denotaremos o natural $q_d(D)$ pelo símbolo $\left[\frac{D}{d}\right]$, enomearemos o mesmo como *parte inteira* do número racional $\frac{D}{d}$.

## Proposição 9

Dados os naturais $d$, $D^{'}$e $D^{''}$tais que $0 < d < D' < D^{''}$, então o número de múltiplos de $d$entre $D^{'}$e $D^{''}$ é dado por

i) $[\frac{D''}{d}] - [\frac{D'-1}{d}]$ , se incluirmos $D^{'}$ na contagem.

ii) $[\frac{D''}{d}] - [\frac{D'-1}{d}]$ , se não incluirmos $D^{'}$ na contagem.

Demonstração

(i) Dados $0 < d < D' < D''$, podemos contar quantos são os múltiplos de $d$ entre $D'$e $D''$, da seguinte forma:

Como $[\frac{D''}{d}]$ é o número de múltiplos de $d$ entre 1 e $D''$, devemos subtrair $[\frac{D'-1}{a}]$, que é o número de múltiplos de $d$ anteriores a $D'$.

Portanto, o número de múltiplos de $d$entre $D'$e$D''$, incluindo $D'$ se esse for múltiplo de $d$, é

$$[\frac{D''}{d}] - [\frac{D'-1}{d}]$$

A demonstração de (ii) é análoga.

## 3.3 M.D.C. e Algoritmo de Euclides

### 3.3.1. Máximo Divisor Comum

### Definição

Sejam dados dois números naturais $n_1$ e $n_2$, distintos ou não. Um número natural $d$ será dito um *divisor comum* de $n_1$ e $n_2$ se $d|n_1$ e $d|n_2$.

### Definição

Diremos que um número natural $d \geq 0$ é um *máximo divisor comum* (*mdc*) de $n_1$ e $n_2$, se possuir as seguintes propriedades:

i) $d$ é um divisor comum de $n_1$ e $n_2$, e

ii) $d$ é divisível por todo divisor comum de $n_1$e $n_2$, ou seja, se $c$ é um divisor comum de $n_1$e $n_2$, então $c|d$.

A unicidade do mdc fica garantida na condição (ii) acima. Note que, se $d$ e $d'$ são dois mdc de um mesmo par de números, então, $d|d'$ e $d'|d$, o que, juntamente implicam que $d = d'$.

Denotaremos por $mdc(n_1, n_2)$ o mdc de $n_1$ e $n_2$. Além disso, temos pela definição que $mdc(n_1, n_2) = mdc(n_2, n_1)$.

## Propriedades:

(i) $mdc\ (0, n) = n$
(ii) $mdc\ (1, n) = 1$
(iii) $mdc\ (n, n) = n$
(iv) Para todo $N \in \mathbb{N}$, temos que $n|N \Leftrightarrow mdc\ (n, N) = n$.
(v) $mdc\ (n, N) = 0 \Leftrightarrow n = N = 0$

## Demonstração

(i) Como zero é divisível por todo número natural, temos que $n$ é divisor de zero. E sendo $n$ divisível por todos os divisores de $n$, por definição, decorre que $mdc(0, n) = n$.

(ii) 1 é o único divisor de 1. E sendo 1 também divisor de $n$, decorre que $mdc(1, n) = 1$.

(iii) Como $n$ é divisível por todos os divisores de $n$, temos por definição que $mdc(n, n) = n$.

(iv) De fato, se $n|N$, temos que $n$ é um divisor comum de $n$ e $N$, e se $d$ é um divisor comum de $n$ e $N$, então $d$ divide $n$, o que mostra que $n = mdc(n, N)$.
A recíproca é clara, se $mdc\ (n, N) = n$, segue-se que $n$ divide $N$.

(v) Como todo número natural divide 0, o $mdc$ de $n$ e $N$, onde $n = N = 0$, é 0, pois esse é um divisor comum de $n$ e $N$ e é o único número divisível por todos os divisores de 0. Reciprocamente, se o $mdc$ de $n$ e $N$ é 0, então 0 divide $n$ e divide $N$, mas o único número divisível por 0 é o próprio 0, logo $n = N = 0$.

Provaremos agora a existência do $mdc$ de qualquer par de números naturais, ambos não nulos.

Iniciaremos mostrando que o máximo divisor comum de dois números, não ambos nulos, quando existe, é efetivamente o maior dentre todos os divisores comuns desses números:
Seja $d > 0$ um $mdc$ de $n$ e $N$, não nulos, partindo do princípio que exista, e seja $c$ um divisor comum qualquer desses números, então $c$ divide $d$ e, portanto, $c \leq d$.

## Lema

Sejam $n, N, a \in \mathbb{N}$. Se existe $mdc(n, N - an)$, então, $mdc(n, N)$ existe e

$$mdc(n, N) = mdc(n, N - an).$$

## Demonstração

Seja $d = mdc(n, N - an)$. Como $d|n$ e $d|(N - an)$, temos que $d$ divide $N = N - an + an$. Com isso, $d$ é divisor comum de $n$ e $N$. Partiremos agora do princípio que $c$ seja um divisor comum de $n$ e $N$. Logo, $c$ é um divisor comum de $n$ e $N - an$ e, portanto, $c|d$. Concluímos que $d = mdc(n, N)$.

Analisaremos o seguinte caso como aplicação do lema acima:

Dados $m, n \in \mathbb{N}$ com $n \neq 1$ temos que:
$mdc(\frac{n^m - 1}{n-1}, n - 1) = mdc(n - 1, m)$.

Faz-se necessária somente a prova para $m \geq 2$. Chamando de $N$ o primeiro membro da igualdade, temos que:

$$N = mdc(n^{m-1} + n^{m-2} + \cdots + n + 1, n - 1) =$$

$$mdc((n^{m-1} - 1) + (n^{m-2} - 1) + \cdots + (n - 1) + m, n - 1).$$

Já vimos pelo estudo dos critério de divisibilidade com binômios que>

$$n - 1 | (n^{m-1} - 1) + (n^{m-2} - 1) + \cdots + (n - 1),$$

Assim, $(n^{m-1} - 1) + (n^{m-2} - 1) + \cdots + (n - 1) = a(n - 1)$ para algum $a \in \mathbb{N}$, e, portanto, pelo Lema apresentado,tem-se que

$$N = mdc(a(n - 1) + m, n - 1) = mdc(n - 1, a(n - 1) + m) = mdc(n - 1, m).$$

## 3.3.2. Algoritmo de Euclides

O método para o cálculo do mdc, apresentado a seguir, é comumente conhecido por Algoritmo de Euclides, que foi descrito no Livro VII, em *Os Elementos*. E assim como o algoritmo da divisão já apresentado, essa é mais uma ferramenta utilizada na metodologia atual do Ensino Básico.

Dados $n$, $N \in \mathbb{N}$, podemos supor $n \leq N$. Se $n = 1$ ou $n = N$, ou ainda $n|N$, já vimos que $mdc(n, N) = n$. Então, partiremos do princípio que $1 < n < N$ e que $n \nmid N$. Logo, pela divisão euclidiana, podemos escrever

$$N = nq_1 + r_1, \quad \text{com } 0 < r_1 < n.$$

Teremos dois casos:

a) $r_1|n$. Logo, $r_1 = mdc(n, r_1)$ já sabemos pelo lema apresentado que

$$r_1 = mdc\,(n, r_1) = mdc(n, N - q_1 n) = mdc(n, N),$$

o que finaliza o algoritmo.

b) $r_1 \nmid n$. Em tal caso, podemos efetuar a divisão de $n$ por $r_1$, obtendo

$$n = r_1 q_2 + r_2, \text{ com } 0 < r_2 < r_1.$$

Novamente, teremos dois casos:

a') $r_2|r_1$. Nesse caso, $r_2 = mdc(r_1, r_2)$ e novamente, pelo Lema 5.2,

$r_2 = mdc(r_1, r_2) = mdc(r_1, \text{n} - q_2 r_1) = mdc(r_1, n) = (N - q_1 n, n) = mdc(N, n) = mdc(n, N)$,

o que finaliza o algoritmo.

b') $r_2 \nmid r_1$. Neste caso, podemos efetuar a divisão de $r_1$ por $r_2$, obtendo

$$r_1 = r_2 q_3 + r_3, \text{ com } 0 < r_3 < r_2.$$

E assim sucessivamente até que o processo pare. O fim do processo é garantido, pois, caso contrário, teríamos uma sequência de números naturais $n > r_1 > r_2 > \cdots$ que não possui menor elemento, o que não é possível pelo Princípio da Boa Ordenação. Logo, para algum $m$, temos que $r_m|r_{m-1}$, o que implica que $mdc(n, N) = r_m$.

Nas salas de aula do 5° e 6° anos do Ensino Fundamental, o algoritmo de Euclides assume uma outra representação, mais clara e acessível ao público, que traremos a seguir.

Começamos com o algoritmo da divisão N por $n$, $N = nq_1 + r_1$ e colocamos os números envolvidos no seguinte diagrama:

| | $q_1$ | |
|---|---|---|
| $N$ | $n$ | |
| $r_1$ | | |

A seguir, continuamos efetuando a divisão $n = r_1 q_2 + r_2$ e colocamos os números envolvidos no diagrama

| | $q_1$ | $q_2$ | |
|---|---|---|---|
| $N$ | $n$ | $r_1$ | |
| $r_1$ | $r_2$ | | |

Prosseguindo, enquanto for possível, teremos

| | $q_1$ | $q_2$ | $q_3$ | ⋯ | $q_{n-1}$ | $q_n$ | $q_{n+1}$ |
|---|---|---|---|---|---|---|---|
| $N$ | $n$ | $r_1$ | $r_2$ | ⋯ | $r_{n-2}$ | $r_{n-1}$ | $r_n = (n, \mathrm{N})$ |
| $r_1$ | $r_2$ | $r_3$ | $r_4$ | ⋯ | $r_n$ | | |

## 3.3.3. Propriedades do mdc

Sejam $n, N \in \mathbb{N}^*$. Definimos o conjunto

$$J(n, N) = \{a \in \mathbb{N}^* ; \exists\, x, y \in \mathbb{N},\ a = xn - yN\}.$$

Por definição temos que

$$J(N, n) = \{b \in \mathbb{N}^* ; \exists\, x, y \in \mathbb{N},\ b = yN - xn\}.$$

### Lema

Tem-se que: $J(n, N) = J(N, n) \neq \emptyset$.

## Demonstração

Inicialmente mostraremos que os dois conjuntos são iguais. Pelo caráter simétrico do resultado com relação a $n$ e $N$, basta mostrara que $J(n, N) \subset J(N, n)$.

Seja $a \in J(n, N)$, então $a = xn - yN$ com $x, y \in \mathbb{N}$. Pela Propriedade Arquimediana, existem números naturais $p$ e $q$ tais que $pn > y$ e $qN > x$. Tomando m = max $\{p, q\}$, tem-se que $mn > Y$ e $mN > X$. Portanto,

$$a = xn - yN = (mn - y)N - (mN - x)n \in J(N, n)$$

Agora, note que $n \in J(n, N)$ e, portanto, $J(n, N) \neq \emptyset$.

O resultado acima e a Propriedade da Boa Ordem garantem que existe min $J(n, N)$.

## Teorema

Sejam $n, N \in \mathbb{N}^*$ e seja $d = \min J(n, N)$, então
i) $d$ é o mdc de $n$ e $N$; e
ii) $J(n, N) = \{md; m \in \mathbb{N}\}$.

## Demonstração

(i) Tome que $c$ divida $n$ e $N$, logo $c$ divide todos os números naturais da forma $xn - yN$. Portanto, $c$ divide todos os elementos de $J(n, N)$, e, consequentemente, $c|d$.

Provaremos agora que $d$ divide todos os elementos de $J(n, N)$. Seja $a \in J(n, N)$ e suponha, por absurdo, que $d \nmid a$. Logo, pela divisão euclidiana,

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

Como $a = xn - yN$ e $d = uN - vn$, para alguns $x, y, u, v \in \mathbb{N}$, segue-se que

$$r = (x + qv)n - (y + qu)N \in J(n, N),$$

o que é um absurdo, pois $d = \min J(n, N)$ e $r < d$. Em particular, $d|n$ e $d|N$.

(ii) Dado que $ld = l(un - vN) = (lv)n - (lu)N \in J(n, N)$, é claro que

$$\{ld; l \in \mathbb{N}\} \subset J(n, N).$$

Mas, já foi provado que todo $a \in J(n, N)$ é tal que $d|a$, e, portanto,

$$J(a, b) \subset \{ld; l \in \mathbb{N}\}.$$

## Corolário

Quaisquer que sejam $n, N, x \in \mathbb{N}^*$ tem-se que

$$mdc(xn, xN) = x\, mdc(n, N).$$

## Demonstração

Note inicialmente que

$$J(xn, xN) = xJ(n, N) = \{xa;\ a \in J(n, N)\}$$

O resultado decorre do teorema e do fato de que

$$\min xJ(n, N) = x \min J(n, N).$$

## Corolário

Dados $n, N \in \mathbb{N}$, tem-se que

$$mdc\left(\frac{n}{mdc\ (n,N)}, \frac{N}{mdc\ (n,N)}\right) = 1.$$

## Demonstração

Temos que

$$mdc(n, N)\ mdc\left(\frac{n}{mdc\ (n,N)}, \frac{N}{mdc\ (n,N)}\right) =$$
$$= mdc\left(mdc\ (n, N)\ \frac{n}{mdc\ (n,N)}, mdc\ (n, N)\ \frac{N}{mdc\ (n,N)}\right) =$$
$$= mdc(n, N),$$

o que valida o resultado.

## Definição

Dois números naturais $n$ e $N$ serão ditos *primos entre si*, ou *coprimos*, se $mdc(n, N) = 1$; ou seja, se o único divisor comum de ambos é 1.

## Proposição 10

$mdc(n,N) = 1 \Leftrightarrow$ existem números naturais $x$ e $y$ tais que $xn - yN = 1$.

## Demonstração

($\Rightarrow$) Partindo do princípio que $n$ e $N$ são primos entre si. Logo, $mdc(n, N) = 1$. Temos que existem números naturais $x$ e $y$ tais que $xn - yN = mdc(n, N) = 1$.

($\Leftarrow$) Partindo do princípio que existam números naturais $x$ e $y$ tais que $xn - yN = 1$. Se $d = mdc(n, N)$, temos que $d|(xn - yN)$, o que mostra que $d|1$, e, portanto, $d = 1$.

## Lema de Gauss

Sejam $n_1$, $n_2$ e $n_3$ números naturais. Se $n_1|n_2n_3$ e $mdc(n_1, n_2) = 1$, então $n_1|n_3$.

## Demonstração

Se $n_1|n_2n_3$, então existe $a \in \mathbb{N}$ tal que $n_2n_3 = n_1a$.

Se $mdc(n_1, n_2) = 1$, então, pela Proposição 10, temos que existem $x, y \in \mathbb{N}$ tais que

$$xn_1 - yn_2 = 1.$$

Multiplicando por $n_3$ ambos os lados da igualdade acima, temos que

$$n_3 = xn_1n_3 - yn_2n_3.$$

Substituindo $n_2n_3$ por $n_1a$ nesta última igualdade, temos que

$$n_3 = xn_1n_3 - yn_1a = n_1(xn_3 - ya)$$

e, portanto, $n_1|n_3$.

## Corolário

Dados $n_1, n_2, n_3 \in \mathbb{N}$, com $n_2$ e $n_3$ não ambos nulos, temos que

$$n_2|n_1 \quad \text{e } n_3|n_1 \Leftrightarrow \frac{n_2n_3}{mdc\,(n_2,n_3)}|n_1.$$

## Demonstração

Já sabemos que $n_1 = xn_2 = yn_3$ para alguns $x, y \in \mathbb{N}$. Então,

$$x\,\frac{n_2}{mdc\,(n_2,n_3)} = y\,\frac{n_3}{mdc\,(n_2,n_3)}.$$

Como $mdc(\frac{n_2}{mdc\,(n_2,n_3)}, \frac{n_3}{mdc\,(n_2,n_3)}) = 1$, decorre que $\frac{n_2}{mdc\,(n_2,n_3)} | y$ e $\frac{n_2}{mdc\,(n_2,n_3)} n_3 | y n_3$. Como $yn_3 = n_1$, a implicação direta fica provada. A recíproca é análoga.

## Definição

Vamos ampliar agora a definição de mdc de dois números naturais para o mdc de *m* números naturais:

Um número natural *d* será dito mdc de dados números naturais $n_1,..., n_m$, não todos nulos, se possuir as seguintes propriedades:
i) *d* é um divisor comum de $n_1,..., n_m$.
ii) Se *c* é um divisor comum de $n_1,..., n_m$, então $c|d$.

Denotaremos o mdc por:

$$mdc\ (n_1,...,n_m).$$

## Proposição 11

Dados números naturais $n_1,..., n_m$, não todos nulos, existe o seu mdc e

$$mdc(n_1,...,n_m) = \text{mdc}\ (n_1,..., (n_{m-1}, n_m)).$$

## Demonstração

Provaremos por indução sobre *m* ($\geq 2$). É fácil ver que para $m = 2$, o resultado é válido. Partiremos do princípio que o resultado vale para *m*. Para provar que o resultado é válido para $m + 1$, basta mostrar que se *d* é o mdc de $n_1,..., (n_m, n_{m+1})$, então *d* é o mdc de $n_1,..., n_m, n_{m+1}$, o que prova também a existência.

Seja *d* o *mdc* de $n_1,..., (n_m, n_{m+1})$. Logo, $d|n_1,..., d|n_{m-1}$ e $d|mdc(n_m, n_{m+1})$. Portanto, $d|n_1,..., d|n_{m-1}$, $d|n_m$ e $d|n_{m+1}$.

Por outro lado, seja *c* divisor comum de $n_1,...,n_m,n_{m+1}$; logo *c* é um divisor comum de $n_1,...,n_{m-1}$ e $mdc(n_m, n_{m+1})$; e, portanto, $c|d$.

## Definição

Os naturais $n_1,..., n_m$ serão ditos *primos entre si*, ou *coprimos*, quando $mdc(n_1,..., n_m) = 1$.

## 3.4 Mínimo Múltiplo Comum

### Definição

Um número natural é um *múltiplo comum* de dois números naturais dados se ele é simultaneamente múltiplo de ambos os números.

Um número natural $m$ é um *mínimo múltiplo comum (mmc*) dos números naturais $n_1$ e $n_2$, se possuir as seguintes propriedades:

(i) $m$ é um múltiplo comum de $n_1$ e $n_2$, e
(ii) se $c$ é um múltiplo comum de $n_1$ e $n_2$, então $m|c$.

Considerando que o mínimo múltiplo comum existe, sua unicidade é garantida em (ii), pois temos que se c é um múltiplo comum de $n_1$ e $n_2$ então $m|c$ e consequentemente $m \leq c$, ou seja, $m$ é o menor dos múltiplos comuns.

O mínimo múltiplo comum de $n_1$ e $n_2$, se existe, é denotado por $mmc(n_1, n_2)$.

### Corolário

O $mmc(n_1, n_2) = 0$ se, e somente se, $n_1 = 0$ ou $n_2 = 0$.

### Demonstração

Se $mmc(n_1, n_2) = 0$, então 0 divide $n_1n_2$, que é múltiplo de $n_1$ e de $n_2$, logo $n_1n_2 = 0$ e, portanto, $n_1 = 0$ ou $n_2 = 0$. Reciprocamente, se $n_1 = 0$ ou $n_2 = 0$, então 0 é o único múltiplo comum de $n_1$ *e* $n_2$, logo $mmc(n_1, n_2) = 0$.

### Proposição 12

Dados dois números $n_1$ e $n_2$ temos que $m = mmc(n_1, n_2)$ existe e $mmc(n_1, n_2).mdc(n_1, n_2) = n_1n_2$.

## Demonstração

Vamos escrever $m = \frac{n_1 n_2}{mdc\,(n_1 n_2)}$, como

$$m = n_1 \frac{n_2}{mdc\,(n_1 n_2)} = n_2 \frac{n_1}{mdc\,(n_1 n_2)},$$

temos que $n_1 | m$ e $n_2 | m$. Portanto, $m$ é um múltiplo comum de $n_1$ e $n_2$.

Seja $c$ um múltiplo comum de $n_1$ e $n_2$; logo, $c = an_1 = bn_2$, para $a, b \in \mathbb{N}$. Decorre que:

$$a \frac{n_1}{mdc\,(n_1 n_2)} = b \frac{n_2}{mdc\,(n_1 n_2)}.$$

Já sabemos que $\frac{n_1}{mdc\,(n_1 n_2)}$ e $\frac{n_2}{mdc\,(n_1 n_2)}$ são primos entre si, segue-se, que $\frac{n_1}{mdc\,(n_1 n_2)}$ divide $b$, e, portanto, $m = \frac{n_1}{mdc\,(n_1 n_2)} n_2$ divide $bn_2$ que, é igual a $c$.

# Corolário

Se $n_1$ e $n_2$ são números inteiros primos entre si, então $mmc(n_1, n_2) = n_1 n_2$.

Vamos ampliar agora a definição de mmc de dois números naturais para o *mmc* de $k$ números naturais:

Um número natural $m$ é um *mmc* dos naturais não nulos $n_1, \ldots, n_k$, se $m$ é um múltiplo comum de $n_1, \ldots, n_k$, e, se para todo múltiplo comum $c$ desses números, tem-se que $m | c$.

É fácil ver que o *mmc*, se existe, é o único, sendo denotado por $mmc(n_1, \ldots, n_k)$.

Proposição 13

Sejam $n_1$,..., $n_k$ números naturais não nulos. Então existe o número *mmc*($n_1$,..., $n_k$) e

$$mmc(n_1,..., n_{k-1,}n_k) = mmc(n_1,..., mmc(n_{k-1,}n_k)).$$

Demonstração

Seja $m = mmc(n_1,..., mmc(n_{k-1,}n_k))$. Logo, $n_1$,..., $n_{k-2}$ e $mmc(n_{k-1,}n_k)$ dividem *m*. Como $n_{k-1}|mmc(n_{k-1,}n_k)$ e$n_k|mmc(n_{k-1,}n_k)$, segue que *m* é um múltiplo comum de $n_1$,..., $n_k$.

Por outro lado, suponha que *c* seja múltiplo comum de $n_1$,..., $n_k$. Logo, $n_1|c$,..., $n_{k-2}|c$ e $mmc(n_{k-1,}n_k)|c$; daí segue que *c* é múltiplo de $m = mmc(n_1,..., mmc(n_{k-1,}n_k))$.

## 3.5 Números Primos

O conceito de número primo é um dos mais importantes na Matemática. Estes números desempenham papel fundamental na Teoria dos Números e estão associados a muitos problemas famosos que permanecem sem soluções apesar dos esforços de vários matemáticos ao longo dos anos.

### 3.5.1 Conceito e propriedades

Um número natural maior do que 1 que só possui como divisores 1 e ele próprio é chamado de *número primo*.

Dados dois números primos *p* e *q* e um número inteiro *n* qualquer, decorrem da definição acima os seguintes fatos:

I) Se $p|q$, então $p = q$.

De fato, como $p|q$ e sendo *q* primo, temos que $p = 1$ ou $p = q$. Sendo *p* primo, tem-se que $p > 1$, o que acarreta $p = q$.

II) Se $p \nmid n$, então $mdc(p, n) = 1$.

De fato, se $mdc(p, n) = d$, temos que $d|p$ e $d|n$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois $p \nmid n$ e, consequentemente, $d = 1$.

Um número maior do que 1 e que não é primo será dito *composto*.

Portanto, se um número natural $n > 1$ é composto, existirá um divisor natural $n_1$ de$n$ tal que $1 < n_1 < n$. Logo, existirá um número natural $n_2$ tal que

$$n = n_1 n_2, \qquad \text{com } 1 < n_1 < n \text{ e } 1 < n_2 < n$$

Do ponto de vista de estrutura multiplicativa dos naturais, os números primos são os mais simples e ao mesmo tempo são suficientes para gerar todos os números naturais, conforme veremos mais adiante no *Teorema Fundamental da Aritmética*.

A seguir, estabelecemos um resultado fundamental de Euclides (*Os Elementos*, Proposição 30, Livro VII), chamado de *Lema de Euclides*.

## Lema de Euclides

Sejam $n_1, n_2, p \in \mathbb{N}$, com $p$ primo. Se $p|n_1n_2$, então $p|n_1$ ou $p|n_2$.

## Demonstração

Se $p|n_1$ não há mais o que demonstrar. Suponha que $p \nmid n_1$. Então $mdc(p, n_1) = 1$, e o resultado segue-se do Lema de Gauss.

A propriedade descrita acima pode ser utilizada para caracterizar a noção de número primo.

## Corolário

Se $p$, $p_1$,..., $p_n$ são números primos e, se $p|p_1...p_n$, então $p = p_i$ para algum $i$ = 1,..., $n$.

### Demonstração

Use o Lema de Euclides, indução sobre $n$ e o fato de que, se $p|p_i$, então $p = p_i$.

## 3.5.2 Números especiais

Alguns números primos possuem propriedades específicas que valem a pena serem estudadas, como faremos a seguir. São os Primos de Fermat, que recebem este nome em homenagem a Pierre de Fermat, os Primos de Mersenne, que recebem este nome em homenagem a Marin Mersenne, e abordaremos um teorema sobre números primos em PA, devido ao matemático Johann P. G. LejeuneDirichlet, do século XIX.

### Proposição 14

Sejam $x$ e $n$ números naturais maiores do que 1. Se $x^n + 1$ é primo, então $x$ é par e $n = 2^m$, com $m \in \mathbb{N}$.

### Demonstração

Suponhamos que $x^n + 1$ seja primo, onde $x > 1$ e $n > 1$. Logo, $x$ tem que ser par, pois, caso contrário, $x^n + 1$ seria par e maior do que dois, o que contraria o fato de ser primo.

Se $n$ tivesse um divisor primo $p$ diferente de 2, teríamos $n = n'p$ com $n' \in \mathbb{N}$. Portanto, pela Proposição 7, $x^{n'} + 1$ dividiria $(x^{n'})^p + 1 = x^n + 1$, contradizendo o fato de esse último número ser primo. Isto implica que $n$ é da forma $2^m$.

Os *números de Fermat* são os números da forma

$$F_n = 2^{2^n} + 1,\ n = 0, 1, 2,....$$

Em 1640, Fermat escreveu em uma de suas cartas a Mersenne dizendo que achava que esses números eram todos primos. De fato, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, e $F_4 = 65537$ são todos primos, mas não se sabe se havia algum outro motivo para que Fermat achasse que todos os números dessa forma fossem primos.

Em 1732, Leonhard Euler provou que a afirmação de Fermat era falsa mostrando que

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641 \text{ x } 6700417.$$

Os números de Fermat primos são chamados de *primos de Fermat*.

Nenhum primo de Fermat foi encontrado até hoje além dos 5 primeiros. Conjucturou-se (Hardy e Wrigth) que os primos de Fermat são em número finito.

## Proposição 15

Sejam $x$ e $n$ números naturais maiores do que 1. Se $x^n - 1$ é primo, então $x = 2$ e $n$ é primo.

## Demonstração

Admitamos que $x^n - 1$ seja primo, com $x > 1$ e $n > 1$.

Suponhamos, por absurdo, que $x > 2$. Logo, $x - 1 > 1$ e $x - 1 | x^n - 1$ (Proposição 6). Portanto, $x^n - 1$ não é primo, o que é uma contradição. Consequentemente, $x = 2$.

Por outro lado, suponhamos, por absurdo, que $n$ não é primo. Temos que $n = ab$ com $a > 1$ e $b > 1$. Como $2^a - 1$ divide $(2^a)^b - 1 = 2^n - 1$ (novamente, pela Proposição 6), segue que $2^n - 1$ não é primo, contradição. Logo, $n$ é primo.

Os *números de Mersenne* são os números da forma

$$M_p = 2^p - 1,$$

Onde *p* é um número primo.

Até o presente momento, o maior número primo conhecido é o número de Mersenne $M_{57885161}$, descoberto em janeiro de 2013, e que possui 17425170 algarismos.

## 3.5.3 O conjunto dos números primos é infinito

A prova mais comumente apresentada sobre a infinidade dos números primos é a de Euclides, mas como esta já foi apresentada no início deste capítulo apresentaremos outra aqui.

Consideremos os números de Fermat, $F_n = 2^{2^n} + 1$ para n = 0, 1, 2, ....

Vamos mostrar a seguinte recorrência:

$$\bigcup_{k=0}^{n-1} F_k = F_n - 2 \qquad (n \geq 1),$$

Usaremos indução sobre *n*. Para *n* = 1, temos $F_0 = 3$ e $F_1 - 2 = 3$. Por indução concluímos que:

$$\bigcup_{k=0}^{n} F_k = \left(\bigcup_{k=0}^{n-1} F_k\right) F_n = (F_n - 2)\cdot F_n = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) = 2^{2^{n+1}} - 1 = F_{n+1} - 2$$

A validade da fórmula anterior nos diz que dois números de Fermat distintos são primos entre si. Com efeito, se d é um divisor de $F_m$ e$F_n$ ($m<n$), então *d* divide 2 e, consequentemente *d* = 1 ou *d* = 2. Mas *d* = 2 é impossível, pois todo número de Fermat é impar e, portanto, não é divisível por 2. Segue que *d* = 1. Como existem infinitos números de Fermat, segue que existem infinitos números primos.

### 3.5.4 A distribuição dos números primos

Sabendo que existem infinitos números primos, podemos nos perguntar como obter uma lista contendo os números primos até uma dada ordem. Um dos mais antigos métodos para elaborar tabelas de números primos é devido ao matemático grego Eratóstenes, que viveu por volta de 230 anos antes de Cristo. O método, chamado de *Crivo de Eratóstenes*, permite determinar todos os números primos até a ordem que se desejar, mas não é muito eficiente para ordens muito elevadas.

Como exemplo, vamos utilizar o crivo de Eratóstenes para encontrar os números primos menores que 120.

Primeiramente, escrevemos todos os números naturais de 2 a 120. Em seguida riscaremos todos os números compostos seguindo a seguinte procedimento:

Primeiro riscamos todos os múltiplos de 2 maiores que 2, que é o primeiro número primo.

O segundo número primo é o menor número maior que 2 que não foi riscado, isto é, o 3. Agora riscamos todos os múltiplos de 3 maiores que 3 (note que alguns já foram riscados).

O menor número maior que 3 que ainda não foi riscado, o 5, é o terceiro número primo. Então riscamos todos os múltiplos de 5 maiores que 5 (os que ainda não foram riscados).

Por fim, riscaremos os múltiplos do 4º número primo (com exceção dele mesmo) que é o menor número maior que 5 ainda não riscado, isto é, o 7.

O lema a seguir, devido ao próprio Eratóstenes, nos mostra que para encontrar os primos menores que 120 não precisamos repetir além do número 7 o procedimento descrito acima.

Lema

Se um número natural $n > 1$ não é divisível por nenhum número primo $p$ tal que $p^2 \leq n$, então ele é primo.

## Demonstração

Se $n$ é composto então ele é divisível por algum primo $p$. Se $p^2 \leq n$ nada há para demonstrar. Se, por outro lado $p^2 > n$ então $n = pn_1$ com $n_1^2 \leq n$, pois se $n_1^2 > n$ então $n^2 = (pn_1)^2 = p^2n_1^2 > nn = n^2$, o que é uma contradição. Se $n_1$ é primo nada há mais para demonstrar. Se, porém, $n_1$ é composto então existe um primo $q < n_1$ que divide $n_1$ e portanto $n$ e, assim, $q|n$ e $q^2 < n$.

Portanto, na nossa tabela de números de 2 a 120, devemos ir até alcançarmos o primo 7, pois o próximo primo é 11, cujo quadrado supera 120.

| | 2 | 3 | ~~4~~ | 5 | ~~6~~ | 7 | ~~8~~ | ~~9~~ | ~~10~~ | 11 | ~~12~~ |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | ~~14~~ | ~~15~~ | ~~16~~ | 17 | ~~18~~ | 19 | ~~20~~ | ~~21~~ | ~~22~~ | 23 | ~~24~~ |
| ~~25~~ | ~~26~~ | ~~27~~ | ~~28~~ | 29 | ~~30~~ | 31 | ~~32~~ | ~~33~~ | ~~34~~ | ~~35~~ | ~~36~~ |
| 37 | ~~38~~ | ~~39~~ | ~~40~~ | 41 | ~~42~~ | 43 | ~~44~~ | ~~45~~ | ~~46~~ | 47 | ~~48~~ |
| ~~49~~ | ~~50~~ | ~~51~~ | ~~52~~ | 53 | ~~54~~ | ~~55~~ | ~~56~~ | ~~57~~ | ~~58~~ | 59 | ~~60~~ |
| 61 | ~~62~~ | ~~63~~ | ~~64~~ | ~~65~~ | ~~66~~ | 67 | ~~68~~ | ~~69~~ | ~~70~~ | 71 | ~~72~~ |
| 73 | ~~74~~ | ~~75~~ | ~~76~~ | ~~77~~ | ~~78~~ | 79 | ~~80~~ | ~~81~~ | ~~82~~ | 83 | ~~84~~ |
| ~~85~~ | ~~86~~ | ~~87~~ | ~~88~~ | 89 | ~~90~~ | ~~91~~ | ~~92~~ | ~~93~~ | ~~94~~ | ~~95~~ | ~~96~~ |
| 97 | ~~98~~ | ~~99~~ | ~~100~~ | 101 | ~~102~~ | 103 | ~~104~~ | ~~105~~ | ~~106~~ | 107 | ~~108~~ |
| 109 | ~~110~~ | ~~111~~ | ~~112~~ | 113 | ~~114~~ | ~~115~~ | ~~116~~ | ~~117~~ | ~~118~~ | ~~119~~ | ~~120~~ |

Note que o Lema acima também nos fornece um teste de primalidade, pois, para verificar se um dado número *n* é primo, basta verificar que não é divisível por nenhum primo *p* menor que $\sqrt{n}$.

Não existe um padrão em relação à proximidade de dois primos consecutivos.

Note, por exemplo, que na tabela acima vemos que há vários pares de números primos que diferem de duas unidades. Números primos com essa propriedade são chamados *primos gêmeos*. Não se sabe ainda se existem infinitos pares de primos gêmeos.

Em contrapartida existem também primos consecutivos arbitrariamente afastados.

Observe que, dado *n*, a sequência

$$(n + 1)! + 2, (n + 1)! + 3,..., (n + 1)! + n + 1.$$

de números naturais é formada por *n* números consecutivos compostos. Repare que o k-ésimo número desta sequência é divisível por k + 1.

Em relação a densidade de números primos em um determinado intervalo, denotemos por $\pi(n)$, a quantidade de números primos menores ou iguais a *n*.

Legendre e Gauss, analisando tabelas, chegaram à conclusão de que essa função tem um crescimento próximo ao de $\frac{n}{\ln n}$. Por volta de 1900, J. Hadamard e Ch. de la Vallée-Poussin, independentemente, provaram o profundo *Teorema dos Números Primos*, cujo enunciado é simplesmente

$$\lim_{n\to\infty} \frac{\pi(n)}{n} \left(\frac{1}{\ln n}\right)^{-1} = 1.$$

## 3.6 Teorema Fundamental da Aritmética

### 3.6.1. Enunciado e Demonstração

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

#### Demonstração

Provaremos por indução sobre um número natural $n \geq 2$. Para $n = 2$, o resultado se verifica.

Partiremos do princípio que o resultado é válido para todo número natural menor do que $n$ e vamos provar que vale para $n$. Se o número $n$ é primo, nada temos a demonstrar. Suponhamos, então, que $n$ seja composto. Então, existem números naturais $n_1$ e $n_2$ tais que $n = n_1 n_2$, com $1 < n_1 < n$ e $1 < n_2 < n$. Pela hipótese de indução, temos que existem números primos $p_1,...,p_r$ e $q_1,...,q_s$ tais que $n_1 = p_1,...,p_r$ e $n_2 = q_1,...,q_s$. Portanto, $n = p_1,...,p_r q_1,...,q_s$.

Vamos, agora, provar a unicidade da escrita. Suponha que tenhamos $n = p_1,...,p_r = q_1,...,q_s$, onde os $p_i$ e os $q_j$ são números primos. Como $p_1 | q_1,...,q_s$, pelo corolário acima, temos que $p_1 = q_j$ para algum $j$, que, após reordenamento de $q_1,...,q_s$, podemos supor que seja $q_1$. Portanto,

$$p_2...p_r = q_2...q_s.$$

Como $p_2...p_r < n$, a hipótese de indução acarreta que $r = s$ e os $p_i$ e $q_j$ são iguais aos pares.

### 3.6.2. Aplicações do Teorema Fundamental da Aritmética

Uma das aplicações mais recorrentes do TFA em turmas do Ensino Básico é o uso do mesmo para determinar a quantidade de divisores de um número natural $n$.

Seguem duas proposições que nos darão uma fórmula pra encontrar o quantitativo de divisores e ainda uma outra não tão usual, que nos fornece o valor da soma dos divisores de um número natural.

#### Proposição

Seja $n = p_1^{\alpha_1}...p_r^{\alpha_r}$ um número natural. Se $m$ é um divisor positivo de $n$, então:

$m = p_1^{\beta_1}...p_r^{\beta_r}$, onde $0 \leq \beta_i \leq \alpha_i$, para $i = 1,..., r$.

## Demonstração

Considere $m$ um divisor de $n$ e seja $p^{\beta}$ a potência de um primo $p$ presente na decomposição de $m$ em fatores primos. Como $p^{\beta} | n$, decorre que $p^{\beta}$ divide algum $p_i^{\alpha_i}$, por ser primo com os demais $p_j^{\alpha_j}$, e, consequentemente, $p = p_i$ e $0 \leq \beta \leq \alpha_i$.

## Proposição

Seja $n = p_1^{\alpha_1}...p_r^{\alpha_r}$, a decomposição de um número $n > 1$ nas condições do Teorema Fundamental da Aritmética. Então, o número de divisores positivos de $n$ e a soma de todos esses divisores estão dados, respectivamente, por

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1).$$

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

## Demonstração

Constatamos na proposição anterior que existem tantos divisores positivos de $n$ quanto números da forma

$m = p_1^{\beta_1}...p_r^{\beta_r}$, onde $0 \leq \beta_i \leq \alpha_i$, para $i = 1,..., r$.

Note que, de acordo com tal critério, os divisores positivos de $n$ são todos os termos do desenvolvimento do produto

$$S = (p_1^0 + p_1^1 + ... + p_1^{\alpha_1}) \cdot (p_2^0 + p_2^1 + ... + p_2^{\alpha_2}) ... (p_r^0 + p_r^1 + ... + p_r^{\alpha_r})$$

Como cada parênteses contém $\alpha_i + 1$ parcelas, $1 \leq i \leq r$, logo, pelo princípio fundamental da contagem, temos que o total de divisores de $n$ e consequentemente o total de termos de S é:

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1).$$

Por construção temos que $S = s(n)$. Tomando a fórmula que dá a soma dos termos de uma progressão geométrica, temos:

$$p_i^0 + p_i^1 + p_i^{\alpha_i} = \frac{p_i^{\alpha_i + 1} - 1}{p_i - 1}, \ 1 \leq i \leq r.$$

Logo,

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

A decomposição de números naturais em fatores primos revela toda a estrutura multiplicativa desses números. Podemos então, a partir dela encontrar o mdc e o mmc de dois números naturais $n_1$ e $n_2$. Seguem os teoremas que fundamentam essa outra aplicação do TFA também explorada em classes do Ensino Básico.

## Teorema

Sejam $n_1 = p_1^{\alpha_1} \ldots p_n^{\alpha_n}$ e $n_2 = p_1^{\beta_1} \ldots p_n^{\beta_n}$. Pondo

$\gamma_i = \min\{\alpha_i, \beta_i\}$, $\quad \delta_i = \max\{\alpha_i, \beta_i\}$, $\quad i = 1,\ldots,n$,

tem-se que

(i) $mdc(n_1, n_2) = p_1^{\gamma_1} \ldots p_n^{\gamma_n}$ .

(ii) $mmc(n_1, n_2) = p_1^{\delta_1} \ldots p_n^{\delta_n}$ .

## Demonstração

(i) Sabemos que $p_1^{\gamma_1} \ldots p_r^{\gamma_r}$ é um divisor comum de $n_1$e $n_2$. Seja $c$ um divisor comum de $n_1$e $n_2$; logo, $c = p_1^{\varepsilon_1} \ldots p_r^{\varepsilon_r}$ , onde $\varepsilon_i \leq \min\{\alpha_i, \beta_i\}$ e, portanto, $c | p_1^{\gamma_1} \ldots p_n^{\gamma_n}$ . Como todo divisor comum de $n_1$e $n_2$ é divisor de $p_1^{\gamma_1} \ldots p_n^{\gamma_n}$, temos que: $mdc(n_1, n_2) = p_1^{\gamma_1} \ldots p_n^{\gamma_n}$.

(ii) Sabemos que $p_1^{\delta_1} \ldots p_n^{\delta_n}$ é um múltiplo comum de $n_1$e $n_2$.Seja $m$ um múltiplo como de $n_1$ e $n_2$, logo, $m = p_1^{\varepsilon_1} \ldots p_r^{\varepsilon_r}$ , onde $\varepsilon_i \geq \max\{\alpha_i, \beta_i\}$ e, portanto, $p_1^{\delta_1} \ldots p_n^{\delta_n} | m$. Como $p_1^{\delta_1} \ldots p_n^{\delta_n}$ é divisor de todo múltiplo como de $n_1$ e $n_2$, temos que: $mmc(n_1, n_2) = p_1^{\delta_1} \ldots p_n^{\delta_n}$.

## 4 CONSIDERAÇÕES FINAIS

Este trabalho se constitui uma primeira etapa de uma pesquisa que tem por objetivo geral apresentar o Teorema Fundamental da Aritmética (TFA) e analisar suas possibilidades de ensino no 6º ano do Ensino Fundamental.

Para alcançarmos o objetivo da pesquisa, traçamos um planejamento científico que envolveu algumas etapas. Esta primeira foi o estudo aprofundado do TFA e de pesquisas que se voltam para a sua compreensão e para a compreensão dos conceitos a ele associados por alunos de todos os níveis de ensino. As etapas posteriores incluem a aplicação de um teste diagnóstico e a análise do desempenho dos alunos (suas estratégias e os erros que cometeram à luz da Teoria dos Campos Conceituais. Por fim, com base nos dados do teste, uma intervenção de ensino composta por cinco atividades visando a compreensão do TFA por alunos do 6º ano do Ensino Fundamental.

Referências


HEFEZ, A. *Elementos de aritmética*. Rio de Janeiro, 2005.

ALENCAR FILHO, E. *Teoria elementar dos números*. São Paulo: Nobel, 1988.

BOYER, C. B. *História da Matemática*. Tradução: Elza F. Gomide. São Paulo: Edgar Blücher, 1996.

BRASIL, Ministério da Educação e do Desporto. Secretaria de Educação Fundamental. *Parâmetros Curriculares Nacionais: Matemática.* Brasília, DF, 1998.

BROWN, A.; THOMAS, k. e TOLIAS, G. *Conceptions of Divisibility: Sucess and Understanding. In* MAHER, Carolyn e SPEISER, Robert (orgs.). *Learning and Teaching number theory: Research in Cognition and Instruction*. (p. 1-14). Monograph Series of the Journal of Mathematical Behavior, V. 02. Connecticut, (EUA), 2002.

CAMPBELL, S. *Coming to terms with division: Preservice teachers' understanding*, in Learning and Teaching Number Theory, Ed. Campbell & Zazkis, Ablex Publishing, Westport, 2002.

_____, Zazkis, R. *Divisibility and multiplicative structure of natural numbers: preservice teachers' understanding*, Journal for Research in Mathematics Education, 27 (5), pp. 540-563, 1995.

_____, Zazkis, R. *Prime decomposition: understanding uniqueness*, Journal of Mathematical Behavior, 15 (2), 217-218, 1996.

253

_____, ZAZKIS, R. *Toward Number Theory as a Conceptual Field.* In MAHER, Carolyn e SPEISER, Robert (orgs.). *Learning and Teaching number theory: Research in Cognition and Instruction*. (p. 1-14). Monograph Series of the Journal of Mathematical Behavior, V. 02. Connecticut, (EUA), 2002.

COELHO, S.; MACHADO, S. e MARANHÃO, C. *Como é utilizado o Teorema Fundamental da Aritmética por atores do Ensino Fundamental?* Atas do CIBEM V, Cd-rom, Cidade do Porto, 2005.

EZPELETA, J. e ROCKWELL, E. *Pesquisa participante.* São Paulo, Cortez, 1986.

FIORENTINO, D; LORENZATO, S. *Investigação em Educação Matemática: percursos teóricos e metodológicos;* Campinas; SP. 2006. (Formação de Professores, 1)

LINS, R. C.Gimenez, J. *Perspectivas em aritmética e álgebra para o século XXI.*
Campinas: Papirus, 1997.

LÜDKE, Menga e ANDRÉ, Marli Elisa D. A. *Pesquisa em Educação*. São Paulo: EPU, 1986.

_____, *Abordagens Qualitativas Pesquisa em Educação.* São Paulo.
Editora Pedagógica e Universitária Ltda, 2001.

_____, *Novos enfoques em pesquisa em didática. In.:* CANDAU, Vera (org.).
*A Didática em questão.* Petropolis: Vozes, 1984.

PINTO, N.B. *O erro como estratégia didática: estudo do erro no ensino da matemática elementar*. São Paulo: Papirus, 2000.

RIBENBOIM, P. *Números Primos: mistérios e recordes.* Associação Instituto Nacional de Matemática Pura e Aplicada (IMPA), Rio de Janeiro, 2001.

SANTOS, J. P.O. *Introdução à Teoria dos Números*. Rio de Janeiro: Associação Instituto Nacional de Matemática Pura e Aplicada; IMPA, 2003.

TEPPO, A. R. *Integrating content and process in classroom mathematics* in Learning and Teaching Number Theory, Ed. Campbell & Zazkis, Ablex Publishing, Westport, 2002.

VERGNAUD, G. *A classification of cognitive tasks and operations of thought involved in addition and subtraction problems*. In Carpenter, T., Moser, J. & Romberg, T. Addition and subtraction. A cognitive perspective. Hillsdale, N.J.: Lawrence Erlbaum. pp. 39-59, 1982.

_____,. *Quelques problèmes theóriques de la didactique a propos d'un example: les structures additives*. Atelier International d'Eté: Récherche en Didactique de la Physique. La Londe les Maures, França, 26 de junho a 13 de julho, 1983a.

_____, *Multiplicative structures*. In Lesh, R. and Landau, M. (Eds.) Acquisition of Mathemtics Concepts and Processes. New York: Academic Press Inc. pp. 127-174, 1983b.

_____,. *Problem solving and concept development in the learning of mathematics*. E.A.R.L.I. Second Meeting. Tübingen, 1987.

_____, *Multiplicative structures*. In Hiebert, H. and Behr, M. (Eds.).
Research Agenda in Mathematics Education. Number Concepts and Operations in the Middle Grades. Hillsdale, N.J.: Lawrence Erlbaum. pp. 141-161, 1988.

_____, *La théorie des champs conceptuels. Recherches en Didactique des Mathématiques*, 10 (23): 133-170, 1990a.

_____, et al. *Epistemology and psychology of mathematics education*. In Nesher, P. & Kilpatrick, J. (Eds.) Mathematics and cognition: A research synthesis by International Group for the Psychology of Mathematics Education. Cambridge: Cambridge University Press, 1990b.

_____, *Teoria dos campos conceituais*. In Nasser, L. (Ed.) Anais do 1º
Seminário Internacional de Educação Matemática do Rio de Janeiro. p. 1-26, 1993.

_____, *Multiplicative conceptual field: what and why?* In Guershon, H. and Confrey, J. (Eds.) The development of multiplicative reasoning in the learning of mathematics. Albany, N.Y.: State University of New York Press. pp. 41-59, 1994.

_____, *The nature of mathematical concepts.* In Nunes, T. & Bryant, P.
(Eds.) Learning and teaching mathematics, an international perspective. Hove (East Sussex), Psychology Press Ltd., 1997.

_____, *A comprehensive theory of representation for mathematics education*. Journal of Mathematical Behavior, 17(2): 167-181, 1998.

_____, *L' enfant, la mathématique et la réalité.* Berne, Editions Peter Lang., 1981.

ZAZKIS, R. Language of Number Theory at the Undergraduate Level: A Semiotic Approach. *In* MAHER, Carolyn e SPEISER, Robert (orgs.). *Learning and*

*Teaching number theory: Research in Cognition and Instruction*. (p. 1-14). Monograph Series of the Journal of Mathematical Behavior, V. 02. Connecticut, (EUA), 2002.