UNIVERSIDADE ESTADUAL DO MARANHÃO - UEMA
CENTRO DE ENSINO SUPERIORES DE BACABAL – CESB
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

ANDRÉ DA SILVA ARAÚJO

ENTRE PRIMOS E COMPOSTOS: Um estudo sobre abordagem do Teorema Fundamental da Aritmética no 6º ano do Ensino Fundamental.

BACABAL – MA
2024

ANDRÉ DA SILVA ARAÚJO

ENTRE PRIMOS E COMPOSTOS: Um estudo sobre abordagem do Teorema Fundamental da Aritmética no 6º ano do Ensino Fundamental.

Trabalho de Conclusão de Curso apresentado ao Departamento de Ciências Exatas e Naturais, da Universidade Estadual do Maranhão – UEMA do Campus Bacabal, para obtenção do grau de Licenciatura em Matemática.

Orientador:
Professor Ms. Vilmar Martins da Silva.

BACABAL – MA

2024

A658e Araújo, André da Silva.

Entre primos e compostos: Um estudo sobre abordagem do teorema fundamental da aritmética no 6º ano do Ensino Fundamental/André da Silva Araújo –Bacabal-MA, 2024.

62 f:il.

Monografia (Graduação) – Curso de Matemática Licenciatura - Universidade Estadual do Maranhão-UEMA/ Campus Bacabal-MA, 2024.

Orientador: Profº Vilmar Martins da Silva
1. Números primos e compostos 2. Teorema Fundamental da Aritmética

CDU: 510.3

Elaborada por Poliana de Oliveira J. Ferreira CRB/13-702 MA

ANDRÉ DA SILVA ARAÚJO

Entre primos e compostos: Um estudo sobre abordagem do Teorema Fundamental da Aritmética no 6º ano do Ensino Fundamental.

Trabalho de Conclusão de Curso apresentado à Universidade Estadual do Maranhão – Campus Bacabal como requisito para obtenção de grau de Licenciatura em Matemática

Data: _____ /_____ / _____

Nota: _____

BANCA EXAMINADORA

Prof. Ma. Vilmar Martins da Silva

Universidade Estadual do Maranhão - UEMA

ORIENTADOR

Prof. Fabiano Brito Dualibe

Universidade Estadual do Maranhão - UEMA

1º EXAMINADOR

Prof. Ma. Caio Renan Damasceno Sampaio

Universidade Estadual do Maranhão - UEMA

2º EXAMINADOR

Dedico esta, a Bernarda Silva, cujos conselhos e advertências evidenciaram seu carinho e ocasionaram benefícios incontáveis.

Agradecimentos

Agradeço aos meus pais, pelas demonstrações de amor mais simples e sinceras, como os concelhos e carinho no momento oportuno, a minha esposa por esta sempre ao meu lado em todos os momentos da minha vida e aos meus filhos que Deus com imenso amor me deu.

Minha gratidão a Deus pelo amor imensurável.

Resumo

Neste trabalho, apresentamos discussões sobre as principais definições e propriedades relacionadas a alguns conceitos da aritmética básica, como os números primos e compostos, que nos levam ao Teorema Fundamental da Aritmética (TFA): múltiplo, divisor, números primos e compostos e decomposição em fatores primos. Nosso objetivo foi abordar o estudo do TFA e dos conceitos-chave associados a ele, com um grupo de alunos do 6º ano do Ensino Fundamental. A pesquisa utilizou como base teórica a Teoria dos Campos Conceituais de Vergnaud (1983, 2001) e as ideias de Barbosa (2015), Carvalho (2015), Costa (2015), Alencar Filho (1981), Hefez (2016), Krerley e Adán (2012), França (2019) e Santos (2009), além disso, a Base Nacional Comum Curricular (BNCC) será considerada para a aprendizagem dos conceitos relacionados à Teoria Elementar dos Números, sendo o TFA parte fundamental deste processo. Buscamos apresentar os números primos, analisar sua história e os resultados obtidos por matemáticos ao longo do tempo, além de explorar curiosidades e aplicações em diferentes contextos. O trabalho consistirá em uma pesquisa qualitativa sobre o ensino de números primos no Ensino Básico. Durante o desenvolvimento do trabalho de conclusão de curso, analisaremos as abordagens desse tema por meio de pesquisas e estudos disponíveis sobre o assunto. No fechamento do estudo, são apresentadas as considerações finais cujo foco mostra que os a importância do estudo sobre TFA e suas aplicações ao longo da Educação Básica.

Palavras–chave: Números primos e compostos; Teorema Fundamental da Aritmética.

Abstract

In this work, we present discussions on the main definitions and properties related to some basic arithmetic concepts, such as prime and composite numbers, which lead us to the Fundamental Theorem of Arithmetic (TFA): multiple, divisor, prime and composite numbers and decomposition into factors cousins. Our objective was to approach the study of TFA and the key concepts associated with it, with a group of students in the 6th year of Elementary School. The research used as a theoretical basis Vergnaud's Theory of Conceptual Fields (1983, 2001) and the ideas of Barbosa (2015), Carvalho (2015), Costa (2015), Alencar Filho (1981), Hefez (2016), Krerley and Adán (2012), França (2019) and Santos (2009), furthermore, the National Common Curricular Base (BNCC) will be considered for learning concepts related to Elementary Number Theory, with TFA being a fundamental part of this process. We seek to present prime numbers, analyze their history and the results obtained by mathematicians over time, in addition to exploring curiosities and applications in different contexts. The work will consist of qualitative research on the teaching of prime numbers in Basic Education. During the development of the course conclusion work, we will analyze the approaches to this topic through research and studies available on the subject. At the end of the study, final considerations are presented whose focus shows that the importance of studying TFA and its applications throughout Basic Education

Keywords: Prime and compound numbers; Fundamental Theorem of Arithmetic.

Lista de Figuras

Lista de Abreviaturas e Siglas

BNCC Base Nacional Comum Curricular.

MDC Máximo Divisor Comum.

MMC Mínimo Múltiplo Comum.

TFA Teorema Fundamental da Aritmética.

Lista de Símbolos

ζ	Letra grega minúscula zeta

Sumário

1 Introdução

Este trabalho de pesquisa tem como temática "Abordagem do Teorema Fundamental da Aritmética no 6º ano do Ensino Fundamental: entre primos e compostos", com objetivo geral de apresentar o Teorema Fundamental da Aritmética (TFA) e analisar suas possibilidades de ensino e estudo do TFA com foco nos principais conceitos associados a ele no 6° ano do Ensino Fundamental Anos Finais.

Objetivando especifico, será apresentada estratégias adequadas para que os alunos quanto professores compreendam e diferenciem o conceito de número primo e número composto, favorecendo a compreensão do conceito de múltiplos, divisores, decomposição em fatores primos e apresentar o Teorema Fundamental da Aritmética (TFA).

Quando os alunos Ensino Fundamental Anos Finais ou até mesmo no Ensino Médio se deparam com questões que envolvam os conceitos utilizados na decomposição de um número em fatores primos, é comum apresentarem manifestações que demonstram as dificuldades no procedimento dos cálculos associados a essa operação tais como os critérios de divisibilidade e a identificação de múltiplos e divisores. Sobretudo, quando se trata de números que possuem em sua composição três ou mais algarismos, onde em geral os alunos só conseguem resolver tais operações com auxílio de uma calculadora.

Autores que embasam a pesquisa são Barbosa (2015), Carvalho (2015), Costa (2015), Alencar Filho (1981), Hefez (2016), Krerley e Adán (2012), França (2019) e Santos (2009). Contaremos com a Base Nacional Comum Curricular (BNCC).

Este estudo justifica–se nesse sentido, que nossa pesquisa bibliográfica parte da necessidade de uma abordagem que priorize a apropriação de conceitos e não simplesmente a memorização de algoritmos que são abordados desde os anos iniciais do Ensino Fundamental dando oportunidade para o aluno se expressar e decentralizando do professor a fala e o desenvolvimento de modo de pensar sobre o conteúdo matemático que está sendo estudado. Para o Universidade Estadual do Maranhão, enquanto instituição formadora, este trabalho pretende enriquecer discussões já levantadas, bem como auxiliar as disciplinas de Didática e Metodologia do Ensino de Matemática.

Teve como metodologia a analise bibliográfico de livros, artigos, dissertações e tese com a temática em questão. Essa pesquisa bibliográfica parte da necessidade de uma abordagem que priorize a apropriação de conceitos e não simplesmente a memorização de algoritmos que são abordados desde os anos iniciais do Ensino Fundamental dando oportu-

nidade para o aluno se expressar e decentralizando do professor a fala e o desenvolvimento de modo de pensar sobre o conteúdo matemático que está sendo estudado.

A Problemática que será descrita visando na dificuldade do tema e abordar estrategias de ensino. Assim, como abordar o estudo do Teorema Fundamental da Aritmética e dos principais conceitos associados a ele com alunos do 6° ano do ensino fundamental?

Conforme Alencar Filho (1988), o TFA (Teorema Fundamental da Aritmética) 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. Esse teorema foi formulado há mais de 2.300 anos, pelo matemático grego Euclides, e é considerado por muitos como o mais importante da aritmética. Ele permite que números muito grandes sejam decompostos em primos, o que é essencial para a criptografia.

Dessa forma, os conceitos que se associam possibilitando 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. Uma delas é a propriedade da divisibilidade, que estabeleça relação entre o dividendo, o divisor e o quociente. Outra propriedade é a multiplicidade, que estabelece relações entre o multiplicando, o multiplicador e o produto.

A compreensão destes princípios e suas aplicações práticas são fundamentais para que se possa desenvolver habilidades e competências necessárias para a vida acadêmica e profissional. Por exemplo, o cálculo e a geometria são fundamentais para o desenvolvimento das habilidades de raciocínio lógico e matemático, que são essenciais para a solução de problemas e para a tomada de decisões racionais. Além disso, o conhecimento de algumas noções de estatística e probabilidade são de grande utilidade para a análise de dados, que é uma ferramenta importante para a tomada de decisões. Portanto, a compreensão dos conceitos básicos de matemática é essencial para a formação de um indivíduo apto a lidar com as demandas de sua vida acadêmica e profissional.

Se tratando do TFA como verificar se um número é divisível por 3, basta somar os seus algarismos e verificar se a soma resultante é divisível por 3.

Admirando 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.

Entretanto pesquisas em Educação Matemática sinalizam a existência de problemas no ensino e na aprendizagem da Aritmética. A principal causa, segundo alguns estudos,

é o fato de que muitos alunos não desenvolvem as habilidades necessárias para resolver problemas aritméticos, como a capacidade de interpretar dados, raciocinar logicamente e usar recursos para solucionar problemas. Além disso, o ensino tradicional da Aritmética tem focado mais na memorização de fórmulas e regras do que na compreensão das estruturas matemáticas subjacentes.

Direcionando o foco para o campo pedagógico, na busca pela compreensão dessa dificuldade acerca desses conceitos, vemos que o tratamento dado aos mesmos e a forma como são abordados em salas de aula, conduzem o aluno à memorização de algoritmos e de definições "vazios de sentido". Assim, quando os mesmos são indagados, por exemplo, a respeito do processo utilizado em tais algoritmos, ou ainda sobre conexões entre as definições mencionadas, notamos que, em geral, as respostas não apresentam indícios de que haja um domínio eficaz sobre esses conceitos matemáticos.

Em virtude, quando os objetivos de tais conceitos como a decomposição de um número em fatores primos que, por exemplo, auxilia na simplificação e na otimização de cálculos não são alcançados, o estudante se vê limitado a memorizar e reproduzir uma série de regras cujos significados e aplicações ele desconhece, tomando para si a ideia de que os conhecimentos matemáticos são inatingíveis e fortalecendo aquela imagem, socialmente construída, de que aprender matemática fica restrito a um grupo seleto de pessoas cujo intelecto seria mais evoluído.

Pesquisas realizadas por Machado et. al. (2005), Resende (2007) e Santos (2007) em Educação Matemática, sinalizam a existência destes problemas no ensino e na aprendizagem da Aritmética. No que diz respeito à proposta curricular, podemos perceber que o estudo dos conceitos aritméticos não tem sido enfatizado no Ensino Fundamental. Embora tal estudo ocorra, observamos este tratamento mecanizado, com base em problemas e exercícios repetitivos. Com isso, os alunos não têm tido oportunidade de se apropriarem das variações nos algoritmos que possam ser úteis para o desenvolvimento de habilidades de cálculo mental e estimativas.

Todo esse trabalho é estruturado sobre em seções: a primeira a Introdução, a segunda seção Fundamentação Teórica, terceira noções Preliminares, quarto procedimentos Metodológicos e por fim considerações finais e referências.

2 Procedimento Teórico

Diante desta problemática educacional relativa ao ensino da Matemática no que diz respeito à Aritmética, tomaremos, como tópico a ser abordado e apresentado no presente trabalho, o Teorema Fundamental da Aritmética (TFA) e os principais conceitos associados a ele, os quais contemplam noções básicas essenciais como, por exemplo, a de número primo na resolução de problemas e no desenvolvimento de conceitos mais complexos.

Segundo Hefez (2016, p.123), o TFA garante que "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". 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. Trata-se, portanto, de conceitos relevantes em relação ao corpo de conhecimentos matemáticos a serem estudados durante o ensino Fundamental e Médio. Neste sentido, o texto da BNCC apresenta algumas habilidades a serem desenvolvidas pelos alunos no 6º ano do ensino fundamental como:

> (EF06MA05) Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000. (EF06MA06) Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor (BRASIL, 2017, p. 297).

A base teórica que dará suporte a tal metodologia, bem como será aporte para a superação da defasagem de conteúdo, será a Teoria dos Campos Conceituais de Gèrard Vergnaud. Esta Teoria foi criada por Gérard Vergnaud, um matemático, psicólogo e filósofo francês. Aluno de Jean Piaget em Genebra, atualmente é diretor emérito de estudos do Centro Nacional de Pesquisas Científicas (CNRS) em Paris.

Ao desenvolver sua teoria, Vergnaud demonstra interesse pelo processo de ensino e aprendizagem da matemática no contexto escolar, investigando como o estudante aprende em ação. Desta forma, a Teoria dos Campos Conceituais foi inicialmente desenvolvida para explicar o processo de construção de conceitos das estruturas aditivas, das estruturas multiplicativas, das relações número-espaço e da álgebra.

Vergnaud a define da seguinte maneira:

> A teoria dos campos conceituais é uma teoria cognitivista que visa a fornecer um quadro coerente e alguns princípios de base para o estudo do desenvolvimento e da aprendizagem de competências complexas, notadamente das que se relevam das ciências e das técnicas. (VERGNAUD, 1990a, p. 135)

Neste sentido, o autor propõe o estudo de um campo conceitual em vez de um conceito isolado, pois resolver uma situação qualquer exige a união de vários outros conceitos ali envolvidos. Por exemplo, se considerarmos o processo de decomposição de números em números primos, podemos ver claramente que trataremos com vários tópicos ao mesmo tempo: multiplicação, divisão, potenciação, critérios de divisibilidade e números primos são alguns deles. Portanto, o campo conceitual é um conjunto de situações, e as representações simbólicas de vários conceitos, processos e conexões são necessárias para serem compreendidas gradualmente.

2.1 Campo Conceitual

Para Vergnaud (1993), um conceito é uma síntese do conjunto das situações que constituem a referência de suas diversas propriedades e do conjunto dos esquemas que são utilizados pelo estudante. Esta definição é chamada pelo autor de uma definição pragmática, em que ele apresenta de forma completa todos os elementos que permitem ao estudante construir de fato um conceito. Ao identificar a operacionalidade de um conceito, não se pode considerar apenas a ação operatória, mas é necessário analisar o uso de significantes; ou seja, o indivíduo deve ser capaz de expressar o conceito de forma simbólica, através de uma linguagem natural, símbolos, representações, diagramas, entre outros. Além disso, Vergnaud define conceito como uma trinca de conjuntos C = (S, I, R), sendo:

- S - Conjunto das situações. A análise de um campo conceitual se inicia a partir de situações, que são responsáveis pelo sentido que é atribuído ao conceito (referência);
- I - Conjunto das invariantes em que se baseia a operacionalidade dos esquemas. Representam aquilo que se preserva nos conceitos e em seus processos de manipulações. São suas propriedades e os teoremas relacionados. Os invariantes simbolizam o significado do conceito;
- R - Conjunto das representações simbólicas. São as diversas formas em que um conceito pode se apresentar, uma ideia pode ser descrita, por exemplo, através de

um gráfico, tabela, por uma linguagem algébrica ou ainda pela própria linguagem idiomática tanto oral, quanto escrita. Trata-se do significante do conceito.

Figura 1: Definição de conceito descrita por Vergnaud

Fonte: França (2019, p. 55)

Grande é a importância dada à noção de esquema nesta teoria. O conceito de esquema criado por Piaget é complementado por Vergnaud quando o define como:

> [...] a organização invariante do comportamento para uma classe de situações dada. É nos esquemas que se devem pesquisar os conhecimentos-em-ação do estudante, isto é, os elementos cognitivos que fazem com que a ação do estudante seja operatória. (VERGNAUD, 1993, p. 2).

Para o autor, o conceito de esquema designa a atividade organizada que o sujeito desenvolve em face de uma certa classe de situações. Ao verificar um esquema utilizado por um aluno frente a um problema, construindo sua solução, podemos selecionar os elementos cognitivos que fizeram, ou não, com que a ação desse sujeito fosse operatória. A análise de um esquema que alcançou seu objetivo, leva o educador a inferir, por exemplo, se o meio utilizado foi o mais eficiente. Além disso, a observação de um esquema equivocado, dá ao professor ferramentas para buscar a superação de dúvidas, já que poder revelar o ponto em que o aluno está tendo dificuldades para explorar e aplicar propriedades que estão sendo ensinadas. A partir desses dados o educador consegue elaborar um planejamento mais adequado a seu grupo, aprimorando sua técnica e ampliando as chances de sua turma obter um bom rendimento.

A construção dos conceitos ocorre a partir do domínio dos alunos. Portanto, podemos dizer que tem características locais, e o campo do aluno se limita aos seus esquemas que ele precisa expandir. Vergnaud (2011) acredita que esse tipo de construção não parte

imediatamente da explicação, mas um processo lento, novas situações devem ser introduzidas continuamente, situação está se tornando cada vez mais complicada e ampliando o repertório de esquemas. Se o aluno tiver um mal-entendido, ele só pode ser alterado quando se deparar com uma situação que não pode ser utilizada.

Decompor números em fatores primos é constante em atividades como: simplificar frações, calcular a enésima raiz aritmética de um determinado número, determinar a quantidade de divisores inteiros positivos de qualquer número e calcular o MMC (mínimo múltiplo comum) e MDC (máximo divisor comum) de dois ou mais números dados. Estes exemplos de cálculo utilizam o conceito de decomposição em fatores primos em diferentes aspectos, que mudam com a situação e permitem aos alunos explorar e testar seus esquemas para a construção e aprimoramento dos conceitos.

2.2 História da Teoria Elementar dos Números

O estudo da História da Matemática, até este momento, não se firma, seu local de evidência na formação de professores. Porém, vários trabalhos têm sido realizados nesse sentido, principalmente no âmbito universitário.

A História da Matemática pode ser entendida como um instrumento para se compreender a evolução da Matemática ao longo do tempo, assim como os principais pensadores que contribuíram para o desenvolvimento da ciência. Isso permite que o professor entenda o contexto da Matemática e o modo como ela foi sendo construída ao longo dos tempos.

Além disso, a História da Matemática também é importante para a compreensão dos princípios básicos da Matemática, pois permite que o professor entenda porquê e como as teorias foram criadas, assim como os princípios matemáticos que serviram de base para a sua construção.

Este fato tem argumento direto no processo de uma sala de aula, uma vez que não é habitual que docentes procurem manusear este recurso de ensino, que é a contextualização histórica dos conceitos matemáticos o qual se pretende ensinar, na maioria das classes. No entanto, a contextualização histórica dos conceitos matemáticos permite que os alunos aprofundem o seu conhecimento, pois lhes dá a oportunidade de ver como esses conceitos se relacionam com o mundo real e histórico. Esta abordagem torna o processo de ensino mais interessante, pois os alunos têm uma visão mais abrangente do assunto em questão e isso pode ajudá-los a compreender melhor o assunto, além de aumentar o seu interesse

e envolvimento.

Também, a História da Matemática nos ajuda a entender como a matemática se desenvolveu ao longo dos séculos, desde as primeiras contas feitas pelos sumérios até às modernas teorias matemáticas. Além do mais nos ajuda a compreender como algumas das grandes conjecturas foram provadas e quais são as que ainda estão abertas. De acordo com os Base Nacional Comum Curricular (BNCC), destaca nas competências gerais da Educação Básica:

> Valorizar e utilizar os conhecimentos historicamente construídos sobre o mundo físico, social, cultural e digital para entender e explicar a realidade, continuar aprendendo e colaborar para a construção de uma sociedade justa, democrática e inclusiva (BRASIL, 2017, p. 9).

Considerando a área de Matemática e, por esse motivo, o componente curricular de Matemática deve garantir aos alunos o desenvolvimento da seguinte competências específicas.

> Reconhecer que a Matemática é uma ciência humana, fruto das necessidades e preocupações de diferentes culturas, em diferentes momentos históricos, e é uma ciência viva, que contribui para solucionar problemas científicos e tecnológicos e para alicerçar descobertas e construções, inclusive com impactos no mundo do trabalho (BRASIL, 2017, p. 267).

Reconhecer também que a Matemática se relaciona com outras áreas do conhecimento, o que permite ao seu estudo contribuir para o desenvolvimento de habilidades e competências que são fundamentais para o exercício da cidadania.

Partindo para a história da Teoria dos Números remonta à Grécia antiga, onde os filósofos gregos começaram a se interessar pela natureza dos números.

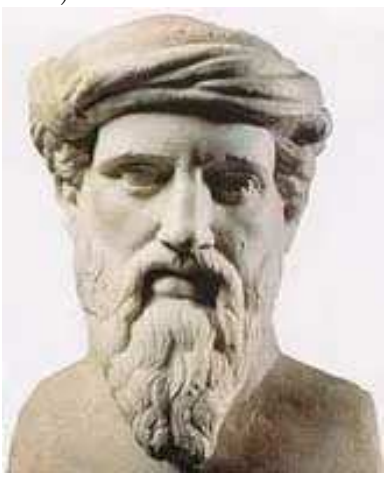
A Teoria dos Números surgiu há mais de dois mil anos, quando os gregos começaram a se questionar sobre as propriedades dos números inteiros e a buscar relações entre eles. A abordagem deles foi baseada na geometria e incluía tópicos como: divisibilidade, sistemas de números, algoritmos e teoremas.

Os primeiros a se interessar por esta teoria foram Pitágoras, Euclides e Arquimedes.

Esses filósofos estudaram a geometria com a intenção de descobrir mais sobre a natureza dos números e suas propriedades.

O trabalho de Pitágoras foi fundamental para a descoberta do teorema de Pitágoras, que estabelece a relação entre os catetos de um triângulo retângulo e a hipotenusa. Esta

Figura 2: Estátua de Pitágoras (580 a.C. a 500 a.C.).



Fonte: https://brasilescola.uol.com.br/mitologia/pitagoras.htm

Figura 3: Euclides de Alexandria

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

Figura 4: Arquimedes

Fonte: https://sites.google.com/site/greciaantigamatematicos/home/arquimedes

descoberta foi um marco na história da Teoria dos Números, pois abriu caminho para a descoberta de outros teoremas, bem como a compreensão das relações entre os números.

Pitágoras foi pioneiro em diversos conceitos, como a ideia de um mundo geométrico estruturado com base na matemática, a existência do número irracional e a existência de números inteiros na natureza. Desenvolveu a ideia de que os números possuem uma essência própria, sendo capazes de dar significado ao mundo. Esta ideia o levou a acreditar na existência de uma "Ordem Divina", onde todos os acontecimentos estariam relacionados e ligados entre si, de acordo com a lógica e a matemática.

No entanto, a compreensão de tais matemáticos acerca de conceitos mencionados era

concreta, havia uma íntima ligação entre a aritmética e a geometria, sendo os números figurados a sustentação para seus exemplos e generalizações. Os números figurados se baseavam na geometria descritiva, que era uma forma de expressar a aritmética de maneira intuitiva e gráfica. Esses números eram geométricos e possuíam características especiais que permitiam aos matemáticos aplicar teoremas e leis da geometria a eles, possibilitando assim a obtenção de resultados a partir de operações aritméticas. Por exemplo, a área de um quadrado é a soma de seus quatro lados, e a área de um triângulo é a metade da soma dos seus lados. Estas leis foram usadas para calcular áreas, volumes e outros resultados matemáticos a partir dos números figurados.

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:

Figura 5: Número 16

Fonte: (CARVALHO, 2015, p.11)

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

Figura 6: Número 7

Fonte: (CARVALHO, 2015, p.11)

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

Euclides foi considerado o pai da Geometria. Ele foi o primeiro a formular os axiomas, ou seja, as proposições fundamentais, com as quais todas as demais provas de geometria

são construídas. Ele também desenvolveu métodos matemáticos para a solução de problemas geométricos. Além disso, Euclides foi responsável por escrever importantes obras sobre geometria, incluindo The Elements, que são referidos como um dos trabalhos mais importantes já realizados na história da matemática.

Os livros de I a VI aborda os principais conceitos de Geometria Plana, incluindo ângulos, áreas, polígonos, triângulos, círculos, retas, paralelismo e perpendicularidade, entre outros. Os livros VII a IX tratam da Teoria dos Números, abordando números inteiros, fracionários, racionais, irracionais, reais, complexos, entre outros. O livro X lida com o assunto dos números incomensuráveis, que não podem ser expressos como uma proporção de números inteiros. Por fim, os livros XI a XIII discutem Geometria Espacial, abordando tópicos como sólidos geométricos, áreas de superfícies, volumes, ângulos esféricos, projeções e transformações, entre outros.

Euclides desenvolveu o que é conhecido como o primeiro tratado moderno sobre a Teoria dos Números, intitulado Elementos. O tratado contém resoluções e demonstrações de diversos teoremas sobre aritmética, álgebra e geometria, com o objetivo de estabelecer uma abordagem elementar para a discussão da teoria dos números.

Vários outros filósofos contribuíram para a evolução da Teoria dos Números ao longo dos séculos. No século XVII, o matemático francês Pierre de Fermat desenvolveu a Teoria dos Números em suas notas, que foram publicadas pós-mortem em 1679. Um dos tópicos abordados por ele foi a prova do Teorema de Fermat, que diz que seja $\mathfrak{a}^{\mathfrak{n}} + \mathfrak{b}^{\mathfrak{n}} = \mathfrak{c}^{\mathfrak{n}}$, então n deve ser igual a 2.

No século XIX, o alemão Carl Friedrich Gauss abriu novas possibilidades para a Teoria dos Números. Ele desenvolveu a teoria das funções elípticas e a teoria dos números quadráticos, que foram fundamentais para a moderna Teoria dos Números.

No século XX, matemáticos como Kurt Gödel e Alan Turing contribuíram para a Teoria dos Números e seus trabalhos levaram ao desenvolvimento de novos conceitos, como o Teorema de Gödel e o Teorema de Turing.

Atualmente, a Teoria dos Números é um campo de estudo em constante evolução, que continua a desenvolver novos resultados e descobertas. O trabalho de matemáticos modernos tem contribuído para o aprimoramento das abordagens elementares para a discussão da teoria, tornando-a mais acessível e compreensível para um público mais amplo.

2.3 Números primos na história

Desde os tempos da Grécia antiga até hoje, os números primos têm uma história rica em descobertas importantes, especialmente no século XIX. Foram estudados com grande esforço para compreender a natureza de sua distribuição. Na antiguidade, os resultados mais significativos foram a prova de sua infinitude (primeiramente demonstrada por Euclides por volta de 300 a.C.) e o método de Eratóstenes, que permite determinar os números primos menores que um certo inteiro $\mathfrak{n}$.

De acordo com Sautoy (2007, p. 45–47) relata que Euclides em uma das obras mais influentes da História chamada de "Os Elementos" expõe na proposição 20 uma verdade primordial sobre os números primos. Ele exprime que há infinitos número primos, onde a ideia inicia pelo fato de que todo número pode ser concebido por fatores primos.

Ao longo de muitas gerações, houve diversas tentativas infrutíferas de aprimorar o entendimento de Euclides acerca dos números primos. No entanto, em relação ao Teorema de Euclides sobre a infinitude dos números primos, Eves (2004, p. 624) demonstra que Lejeune-Dirichlet (1805–1859) alcançou uma notável generalização. Ele demonstrou que toda progressão aritmética

$$\mathfrak{p},\ \mathfrak{p}+\mathfrak{q},\ \mathfrak{p}+2\mathfrak{q},\ \mathfrak{p}+3\mathfrak{q},\ \ldots,$$

onde $\mathfrak{p}$ e $\mathfrak{q}$ são primos entre si, contém infinitos números primos.

Uma definição amplamente utilizada acerca dos números primos é que eles são uma categoria de números inteiros que não possuem divisores além de si mesmos e de 1. Além disso conforme Rooney (2012, p. 52), sua ocorrência diminui à medida que os valores numéricos aumentam .

O que hoje é conhecido como Teorema Fundamental da Aritmética é uma descoberta de grande importância. Esse teorema afirma que qualquer número natural maior que 1 é ou um número primo pode ser expresso de maneira única como um produto de números primos. No entanto, foram os gregos os primeiros a conceber um argumento que demonstra a impossibilidade de existir um número inteiro maior que 1 que não possa ser gerado por fatores primos (Sautoy, 2007, p. 44).

Ainda segundo Sautoy (2007, p. 13–14), os números primos podem ser comparados aos átomos do reino físico. No entanto, neste caso, eles são os átomos da aritmética, pois

a importância desses números está em sua capacidade de gerar todos os outros números inteiros. Mesmo ao listar esses números, é impossível prever quando surgirá o próximo número primo. A sequência desses números parece ser caótica e aleatória, sem fornecer qualquer indício do próximo número.

A busca por um padrão que explique o comportamento dos números primos tem sido um desafio constante para os matemáticos de todas as épocas, que se recusam a aceitar a possibilidade de não existir uma explicação para a sua natureza.

Não há um método prático para determinar se um número grande é ou não um número primo. O maior número testado foi realizado pelo matemático francês Anatole Lucas (1842-1891) em 1876:

$$2^{127} - 1 = 170.141.183.460.469.231.731.687.303.715.884.105.727.$$

Em 1952, o computador EDSAC, localizado em Cambridge, Inglaterra, demonstrou que o número $180(2^{127} - 1)^2 + 1$, com setenta e nove dígitos, é um número primo. Outros computadores também mostraram que os números $2^{\mathfrak{n}} - 1$, nos quais escolhemos para n os números: 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 86243, 132049, e 216091 também são primos (Eves, 2004, p. 623).

No quarto século a.C, foram os gregos da Antiguidade quem entenderam que esses números seriam capazes gerar todos os demais através da multiplicação, até então a primeira pessoa que elaborou tabelas de números primos foi o diretor da biblioteca do instituto de pesquisa da Grécia Antiga em Alexandria, porém no terceiro século a.C Eratóstenes mostrou uma nova maneira de determinar quais números são primos e com esse método, chamado mais tarde de crivo de Eratóstenes, construiu tabelas de primos (Sautoy, 2007, p. 30-31).

No século XVII, os matemáticos pensaram ter descoberto um método em que podiam estabelecer se um número era primo ou não, o método consistia em calcular $2^{\mathfrak{n}}$ e dividi–lo por $\mathfrak{n}$, se o resto fosse 2, o número $\mathfrak{n}$ seria primo, esse teste foi eliminado em 1819, pois o teste funcionava corretamente para os números menores que 341, que falha ao indicar que 341 é primo, pois $11 \times 31 = 341$ (Sautoy, 2007, p. 38).

Os matemáticos sempre buscaram encontrar fórmulas que produziam uma lista de primos, um desses matemáticos foi Fermat (1601–1665), ele teria encontrado uma fórmula que produzir essa lista. Conhecemos apenas os primeiros cinco primos de Fermat, mas

ele diz que $2^{2^n}+1$ chamado de n–ésimo número de Fermat para cada número inteiro não negativo n é primo, entretanto o quinto número dessa lista que contém 10 algarismos é divisível por 641.

Em meados do século XIX, Bernhard Riemann abordou o problema de decifrar uma determinada ordem nos números primos de uma nova maneira e começou a compreender parte do modelo responsável pelo caos primo e fez uma previsão ousada que ficou conhecida como Riemann. partindo da hipótese de que o caos dos números primos parece estar ordenado e revelar um modelo coerente, ele conjecturou então que essa ordem seria sempre mantida (Sautoy, 2007, p. 18).

A hipótese de Riemann é uma famosa conjectura que está ainda em aberto, a princípio Euler chamou a atenção para a ligação entre a teoria dos números primos e a série

$$\frac{1}{1^s}+\frac{1}{2^s}+\frac{1}{2^s}+\ldots+\frac{1}{n^s}+\ldots,$$

onde s é um número inteiro, desse modo, Riemann estudou essa série para um número complexo do tipo $s=\sigma+i\tau$, onde a soma dessa série define uma função $\zeta(s)$ que veio a ser conhecida como função zeta de Riemann que está associada à hipótese de Riemann.

Ao longo do século, os matemáticos tentaram descobrir um padrão para o comportamento caótico dos números primos. No entanto, Riemann foi o primeiro a descobrir, percebendo que a distribuição dos números primos está ligada à localização dos zeros na linha crítica e conjecturou a hipótese que deu nome ao seu trabalho.

Até hoje, a hipótese de Riemann não foi comprovada como verdadeira e é o único problema não resolvido dentre a seleção de 23 propostas de David Hilbert (1862–1943) em 1900. Além disso, está entre os sete problemas que desafiam os matemáticos do novo milênio. Esses problemas foram propostos no ano 2000 por um grupo de matemática que eram considerados os melhores do mundo na época.

3 Noções Preliminares

Os tópicos a seguir estabelece as definições, os resultados básicos e os teoremas da aritmética elementar que são fundamentais ao desenvolvimento desta sessão, valido para o professor planejar e preparar sua própria forma de trabalhar em um nível apropriado às turmas do sexto ano do Ensino Fundamental com as definições de divisibilidade, múltiplos, divisores, divisão euclidiana, números primos e compostos, por fim o Teorema Fundamental da Aritmética.

Estas definições destacam pelos tipos de problemas e resultados que possuem e pela interdisciplinaridade e imaginação que eles exigem em sua resolução, nunca pela linguagem e/ou pela técnica que desenvolvem. Por esta razão, a área atrai simpatizantes de todos os ramos da matemática. Sua apresentação a alunos do Ensino Fundamental se torna uma boa alternativa para o ensino do rigor e do pensamento matemático.

O modo como as definições são vistas, nesse primeiro momento de aprendizagem, pode guiar o aluno a uma compreensão sólida em seu futuro convívio com tópicos menos elementares. Logo, entendemos que o educando não deve limitar–se à reprodução. Para subir os degraus que, para alguns, pode ser abstrato, ele precisa se apropriar das definições refletindo e argumentando sobre definições e processos matemáticos direcionado pelo professor que domina o assunto em níveis mais elevados.

3.1 Divisibilidade

Iremos começar com o conjunto dos números inteiros, a argumentação sobre divisibilidade em uma percurso diferente dos livros didáticos. Frequentemente o que observamos nas salas de aula é a definição de divisibilidade relacionada à noção de divisão euclidiana, ou seja, um número é considerado divisível por outro quando sua divisão por ele deixa resto zero.

Ao partir desse pressuposto, somos capazes de conduzir os alunos a pensar que a divisão somente pode ser realizada quando um número é divisível por outro, gerando uma bloqueio para a aprendizagem de decorrentes divisões que deixam restos não nulos. Assim afirmamos que um número é divisível por outro quando é múltiplo do mesmo.

Definição 1 (Divisibilidade)**.** *Dados dois números inteiros* $\mathtt{a}$ *e* $\mathtt{b}$*, com* $\mathtt{a} \neq 0$*, diremos que* $\mathtt{a}$ *divide* $\mathtt{b}$*, escrevendo* $\mathtt{a} \mid \mathtt{b}$*, quando existir um número inteiro* $\mathtt{c}$ *tal que*

$$b = a \cdot c.$$

Nessa situação, diremos também que a é um divisor ou fator de b ou, ainda, que b é um múltiplo de a ou que b é divisível por a.

Observe que a notação $a \mid b$ não representa nenhuma operação em $\mathbb{Z}$, nem representa uma fração. Trata–se de uma afirmação que diz ser verdade que existe um número c inteiro tal que $b = a \cdot c$. A negação dessa afirmação é representada por $a \nmid b$, significando que não existe nenhum número inteiro c tal que $b = a \cdot c$.

Exemplo 1. *Observe que* $5 \mid 35$ *pois* $35 = 7 \cdot 5$. *Por outro lado* $3 \nmid 10$ *pois considerando o conjunto* $A = \{3 \cdot k |\ k \in \mathbb{N}\} = \{3,\ 6,\ 9,\ 12, \ldots\}$ *dos múltiplos positivos de* 3 *vemos que* 11 *não pertence ao mesmo.*

A seguir, veremos um teorema crucial que Euclides explicou em sua obra mais famosa, "Os Elementos". Esse resultado demonstra que, mesmo com um pequeno resto, é sempre possível dividir a por b sempre que b seja diferente de 0. Observe que Euclides só tratou de números naturais. Este algoritmo continua sendo o método mais conveniente para fazer uma divisão com resto. Como resultado, é um dos resultados mais significativos da Teoria dos Números e é fácil de usar e entender. É estudado desde o Ensino Fundamental, passando pelo Ensino Médio e chegando ao Ensino Superior, onde é discutido mais extensamente.

Antes de apresentarmos a Divisão Euclidiana, também conhecida como Algoritmo da Divisão, enunciaremos e demonstraremos o Teorema de Eudoxius. Este resultado costuma ser erroneamente atribuído a Arquimedes e chamado de "Princípio de Arquimedes".

Teorema 1 (Eudoxius)**.** *Dados* a *e* b *inteiros com* $b \neq 0$*, então* a *é múltiplo de* b *ou se encontra entre dois múltiplos consecutivos de* b*, isto é, correspondendo a cada par de inteiros* a *e* $b \neq 0$ *existe um inteiro* n *tal que, para* $b > 0$*,*

$$nb \leqslant a < (n+1)b,$$

e para $b < 0$

$$nb \leqslant a < (n-1)b.$$

Demonstração. Segundo França (2019, p. 19–20). Para nossa demonstração vamos considerar $a > 0$ e $b > 0$ (os casos em que $a < 0$ ou $b < 0$ podem ser demonstrados de maneira análoga). Deste modo, temos duas possiblidades: ou $a|b$, ou $a \nmid b$.

1. Se $a \mid b$, então existe $n \in \mathbb{Z}$ tal que $a = n \cdot b$. Nesse caso não há o que provar e o resultado segue;

2. Se $a \nmid b$, então $a \neq n \cdot b \ \forall n \in \mathbb{Z}$. Nesse caso existe um menor inteiro k que satisfaz a condição: $a < k \cdot b$.

Afirmamos que

$$(k-1)b < a.$$

De fato, pois, caso $a < (k-1)b$ teríamos uma contradição uma vez que $a < k \cdot b$ e k é o menor inteiro em que isto ocorre. Deste modo, devemos ter que $(k-1)b < a$ e então $(k-1)b < a < kb$. Tomando $n = k-1$ obtemos

$$n \cdot b \leqslant a < (n+1)b,$$

□

Exemplo 2. *Para* $a = 15$ *e* $b = 7$*, devemos tomar* $n = 2$*.*

$$2 \cdot 7 \leqslant 15 < 3 \cdot 7 \Longrightarrow 14 \leqslant 15 < 21$$

O tema do teorema a seguir é o Algoritmo da Divisão de Euclides.

Teorema 2 (Algoritmo da Divisão de Euclides)**.** *Dados dois inteiros* a *e* b*, com* $b > 0$*, então existem e são único os inteiros* q *e* r *tais que*

$$a = qb + r, \ \textit{com } 0 \leqslant r < b.$$

Os inteiros q *e* r *são chamados respectivamente de quociente e resto,* $r = 0$ *se, somente se,* b *é divisor de* a*, ou seja,* $b \mid a$*.*

Demonstração. Em conformidade com França (2019, p. 21–22). Pelo Teorema de Eudoxius, como $b > 0$, existe um número inteiro q satisfazendo

$$qb \leqslant a < (q+1)b,$$

o que implica $0 \leqslant a - qb$ e $a - qb < b$. Desta forma, se definirmos $r = a - qb$, teremos, garantida, a existência de q e r. A fim de mostrarmos a unicidade, vamos supor a existência de outro par q_1 e r_1 verificando

$$a = q_1 b + r_1 \quad \text{com} \quad 0 \leqslant r_1 < b.$$

Temos $(qb + r) - (q_1 b + r_1) = 0$, isto é $b(q - q_1) = r_1 - r$, o que implica $b \mid (r_1 - r)$. Mas, como $r_1 < b$ e $r < b$, temos $|r_1 - r| < b$ e, portanto, como $b \mid (r_1 - r)$ devemos ter $r_1 - r = 0$ o que nos permite concluir que $r = r_1$. Logo $q_1 b = qb$ e daí $q_1 = q$, uma vez que $b \neq 0$. □

Corolário 1. *Se a e b são dois inteiros, com $b \neq 0$, existem e são únicos os inteiros q e r que satisfazem as condições:*

$$a = qb + r, \ \textit{com } 0 \leqslant r < |b|.$$

Demonstração. Em conformidade com França (2019, p. 22). Se $b > 0$, nada há para demostrar, e se $b < 0$, então $|b| > 0$, e por conseguinte existem e são únicos os inteiros q_1 e r tais que

$$a = q_1|b| + r, \ \text{com } 0 \leqslant r < |b|.$$

ou seja, por ser $|b| = -b$:

$$a = q_1(-b) + r \Rightarrow a = (-q_1)b + r, \ \text{com } 0 \leqslant r < |b|.$$

Portanto, existe e são únicos os inteiros $q = q_1$ e r tais que

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

□

Exemplo 3. *Determine o quociente q e o resto r na divisão de $a = 69$ por $b = -11$ que satisfazem às condições do Algoritmo da Divisão.*

Solução: Ao fazer a divisão usual dos valores absolutos a e b, podemos obter:

$$69 = 11 \cdot 6 + 3 \Rightarrow 69 = (-11) \cdot (-6) + 3$$

onde $0 \leqslant r < |-11|$.

Logo, o quociente $q = -6$ e o resto $r = 3$.

3.2 Máximo Divisor Comum e Mínimo Múltiplo Comum

Nesta seção estudaremos três conceitos fundamentais que aparecem naturalmente em vários problemas de divisibilidade, assim como a relação existente entre eles.

3.2.1 Máximo Divisor Comum

O primeiro destes conceitos está relacionado com os inteiros positivos que dividem simultaneamente dois inteiros prefixados e é denominado máximo divisor comum.

Daqui por diante só consideraremos os divisores positivos de um determinado número.

Definição 2 (Máximo Divisor Comum)**.** *Sejam* a *e* b *inteiros diferentes de zero. O máximo divisor comum, resumidamente mdc, entre* a *e* b *é o número* d *que satisfaz as seguintes condições:*

1. d *é um divisor comum de* a *e* b*, isto é,* $d \mid a$ *e* $d \mid b$*;*

2. d *é o maior inteiro positivo com a propriedade (1), isto é, se* $c \mid a$ *e se* $c \mid b$*, então* $c \leqslant d$.

Neste caso, denotamos o $\mathtt{mdc}$ entre a e b por $d = (a, b) = (b, a)$ ou por $d = \mathtt{mdc}(a, b) = \mathtt{mdc}(b, a)$. Se $\mathtt{mdc}(a, b) = 1$, então dizemos que a e b são primos entre si ou coprimos.

Exemplo 4. *Observando que* $16 = 2 \cdot 8$*,* $24 = 3 \cdot 8$ *temos que* $\mathtt{mdc}(16, 24) = 8$*. Por outro lado,* $\mathtt{mdc}(3, 19) = 1$*, logo os números* 3 *e* 19 *são primos entre si.*

Agora, vamos analisar algumas das propriedades dos divisores comuns de dois números inteiros a e b. Para esses números, as seguintes afirmações são imediatas e válidas, França (2019, p. 26):

1. $\mathtt{mdc}(0, 0)$ não existe;

2. $\mathtt{mdc}(a, 1) = 1$;

3. se $a \neq 0$, então o $\mathtt{mdc}(a, 0) = |a|$;

4. se $a \neq 0$, então o $mdc(a, a) = |a|$;

5. se $a \mid b$, então o $mdc(a, b) = |a|$.

Em especial, é imediato comprovar que:

$$mdc(a, b) = mdc(-a, b) = mdc(a, -b) = mdc(-a, -b).$$

Embora tenhamos conhecimento das propriedades teóricas do máximo divisor comum (mdc) entre dois números inteiros, encontrar o mdc na prática pode ser bastante desafiador sem o auxílio das ferramentas adequadas. Ao lembrar–se de seu significado, o leitor poderia supor que devemos calcular todos os divisores de a e todos os divisores de b, e então descobrir qual é o maior elemento comum entre esses conjuntos. No entanto, essa abordagem seria extremamente trabalhosa. Para encontrar o mdc, utilizamos um importante método conhecido como "Algoritmo de Euclides".

O seguinte resultado foi utilizado por Euclides para provar a existência do máximo divisor comum de dois inteiros não negativos.

Lema 1. *Sejam* a, b, $n \in \mathbb{Z}$. *Se existe* $mdc(a, b - an)$ *então* $mdc(a, b)$ *existe e*

$$mdc(a, b - an) = mdc(a, b)$$

Demonstração. Segundo França (2019, p. 28), seja $d = mdc(a, b - na)$. Como $d \mid a$ e $d \mid (b - n \cdot a)$, segue que d divide $b = b - na + na$. Logo, d é um divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b; logo, c é um divisor comum de a e $b - n \cdot a$ e, portanto, $c \mid d$. Isso prova que $d = mdc(a, b)$. □

Observe que, com a mesma técnica usada na prova do Lema acima, poder–se–ia provar que, para todos a, b, $n \in \mathbb{Z}$,

$$mdc(a, b - an) = mdc(a, b),$$

ou que, se $n \cdot a > b$, então $mdc(a, b - an) = mdc(a, b)$.

O teorema bem como sua demostração foram retirados de Hefez (2016, p. 56–57) e França (2019, p.28–30).

Teorema 3 (Algoritmo de Euclides)**.** *Dados* $a, b \in \mathbb{Z}$*, podemos supor* $b \leqslant a$*. Se* $b = 1$ *ou* $a = b$*, ou ainda* $b \mid a$*, já vimos que* $mdc(a, b) = b$*. Suponhamos, então, que* $1 < b < a$ *e que* $b \nmid a$*. Logo, pela divisão euclidiana, podemos escrever*

$$a = bq_1 + r_1, \quad com \quad r_1 < b.$$

Temos duas possibilidades:

a) $r_1 \mid b$. Em tal caso $r_1 = mdc(b,\ r_1)$ e, pelo Lema 2.1, temos que

$$r_1 = mdc(b,\ r_1) = mdc(b,\ a - q_1 b) = mdc(b,\ a) = mdc(a,\ b)$$

e o algoritmo termina.

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

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

Novamente, temos duas possibilidades:

i) $r_2 \mid r_1$. Nesse caso $r_2 = mdc(r_1, r_2)$ e novamente, pelo Lema 2.1,

$$r_2 = mdc(r_1,\ r_2) = mdc(r_1,\ b - q_2 r_1) = mdc(r_1,\ b) = mdc(a - q_1 b,\ b) = mdc(a,\ b)$$

e paramos, pois termina o algoritmo.

ii) $r_2 \nmid r_1$. Nesse caso, podemos efetuar a divisão de r_1 por r_2 obtendo

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

Este procedimento não pode continuar indefinidamente, pois teríamos uma sequência de números naturais $a > r_1 > r_2 > \ldots$ que não possui menor elemento, o que não é possível pela Propriedade da Boa Ordem. Logo, para algum n, temos que $r_n \mid r_{n-1}$, o que implica que $mdc(a, b) = r_n$.

O algoritmo acima pode ser sintetizado e realizado na prática, como mostramos a seguir.

Inicialmente, efetuamos a divisão $a = bq_1 + r_1$ e colocamos os números envolvidos no seguinte diagrama:

	q_1	
a	b	
r_1		

A seguir, continuamos efetuando a divisão $b = r_1q_2 + r_2$ e colocamos os números envolvidos no diagrama

	q_1	q_2	
a	b	r_1	
r_1	r_2		

Prosseguindo, enquanto for possível, teremos

	q_1	q_2	q_3	$\ldots$	q_n	q_{n+1}
a	b	r_1	r_2	$\ldots$	r_{n-1}	$r_n = mdc(a,\ b)$
r_1	r_2	r_3	r_4	$\ldots$		

Mostramos, a seguir, um exemplo de como aplicamos o algoritmo apresentado acima.

Exemplo 5. *Calculemos o mdc de 372 e 162 (HEZEZ, 2016, p. 57):*

	2	3	2	1	2
372	162	48	18	12	6
48	18	12	6		

Observe que, no exemplo acima, o Algoritmo de Euclides nos fornece:

$$\begin{aligned} 6 &= 18 - 1 \cdot 12 \\ 12 &= 48 - 2 \cdot 18 \\ 18 &= 162 - 3 \cdot 48 \\ 48 &= 372 - 2 \cdot 162 \end{aligned}$$

Donde se segue que

$$\begin{aligned} 6 &= 18 - 1 \cdot 12 = 18 - 1 \cdot (48 - 2 \cdot 18) = 3 \cdot 18 - 48 = 3 \cdot (162 - 3 \cdot 48) - 48 \\ &= 3 \cdot 162 - 10 \cdot 48 = 3 \cdot 162 - 10 \cdot (372 - 2 \cdot 162) = 23 \cdot 162 - 10 \cdot 372. \end{aligned}$$

Temos, então, que

$$\mathtt{mdc}(372, 162) = 6 = 23 \cdot 162 + (-10) \cdot 372.$$

Observe que, utilizando o Algoritmo de Euclides de maneira reversa, podemos expressar $6 = \mathtt{mdc}(372, 162)$ como a diferença entre um múltiplo de 162 e um múltiplo de 372."

De modo geral, ao seguir o procedimento detalhado exemplificado acima, observa–se que o Algoritmo de Euclides também nos oferece uma maneira de expressar o máximo divisor comum ($\mathtt{mdc}$) de dois números como a soma de múltiplos dos próprios números em questão. Assim, ao lidarmos com números pequenos, nos referimos aqui a números que possuem no máximo dois dígitos, encontrar o $\mathtt{mdc}$ se torna uma tarefa simples, pois podemos calculá–lo utilizando as fatorações dos números envolvidos. Porém, ao trabalhar com números grandes, números que têm três ou mais dígitos, o Algoritmo de Euclides, em geral, é mais acessível do que a fatoração, considerando que esta última pode ser bastante difícil.

Quando utilizamos o Algoritmo de Euclides para expressar $\mathtt{mdc}(\mathtt{a}, \mathtt{b})$ na forma $\mathtt{ma} + \mathtt{nb}$, com $\mathtt{m},\ \mathtt{n} \in \mathbb{Z}$, referir–nos–emos a ele como *Algoritmo de Euclides Estendido.*

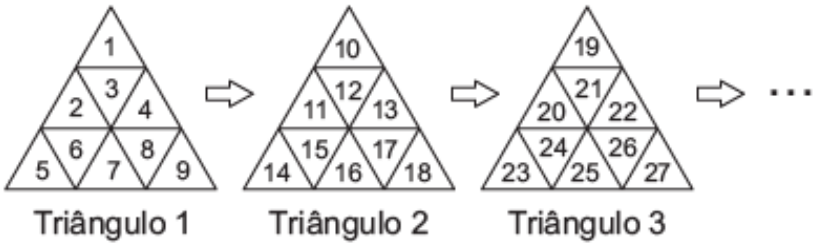
Exemplo 6. *Determine o máximo divisor comum dos números 471 e 1176.*

Solução: Aplicando o algoritmo de Euclides obtemos a seguinte sequência de divisões com resto:

$$\begin{aligned} 1176 &= 471 \cdot 2 + 234 \\ 471 &= 234 \cdot 2 + 3 \\ 234 &= 78 \cdot 3, \end{aligned}$$

então o $\mathtt{mdc}(471, 1176) = 3$.

Problema 1 (OBMEP 2014 – Nível 1)**.** *Guilherme começa a escrever os números naturais em figuras triangulares de acordo com o padrão abaixo:*



Nomeando as casas de cada um desses triângulos com as letras A, B, C, D, E, F, G, H e I, como na figura ao lado, ele pode codificar cada número natural por meio do número do triângulo e da letra da casa em que ele aparece.

Por exemplo, o número 5 é codificado por 1E, pois aparece na casa E do Triângulo 1. Já o número 26 é codificado por 3H, pois aparece na casa H do Triângulo 3. Como Guilherme codifica o número 2014?

A) 222E

B) 222G

C) 223H

D) 224E

E) 224G

Solução: Devemos ficar atentos ao quociente e ao resto da divisão de um número natural por 9, pois em cada triângulo são escritos 9 números. Observamos que no Triângulo 1 estão o 9 e os números que têm quociente 0 na divisão por 9; no Triângulo 2 estão o $18 = 2 \times 9$ e os números que têm quociente 1 na divisão por 9; no Triângulo 3 estão o $27 = 3 \times 9$ e os números que têm quociente 2 na divisão por 9, e assim por diante.

A posição do número em cada triângulo, descrita por uma letra de A até I, corresponde ao resto da divisão do número por 9, ou seja, resto 1 a posição é A, resto 2 é B, resto 3 é C, resto 4 é D, resto 5 é E, resto 6 é F, resto 7 é G, resto 8 a posição é H e, finalmente, se o resto for 0 a posição é I. Ora, pelo Algoritmo de Euclides temos

	223	
2014	9	
7		

Portanto, 2014 está no Triângulo $223 + 1 = 224$, na posição equivalente ao resto 7, ou seja, G. Logo, Guilherme codifica 2014 como 224G.

3.2.2 Mínimo Múltiplo Comum

A ideia final da seção está agora em andamento. O mesmo se aplica aos inteiros positivos que são múltiplos de dois inteiros prefixados simultaneamente. Esses inteiros são conhecidos como mínimos múltiplos comuns.

Definição 3 (Mínimo Múltiplo Comum)**.** *Sejam* $\mathfrak{a}$ *e* $\mathfrak{b}$ *inteiros diferentes de zero. O mínimo múltiplo comum, resumidamente* $\mathfrak{mmc}$*, entre* $\mathfrak{a}$ *e* $\mathfrak{b}$ *é o inteiro positivo* $\mathfrak{m}$ *que satisfaz as seguintes condições:*

1. $\mathfrak{m}$ *é um múltiplo comum de* $\mathfrak{a}$ *e* $\mathfrak{b}$*, isto é,* $\mathfrak{a} \mid \mathfrak{m}$ *e* $\mathfrak{b} \mid \mathfrak{m}$*;*

2. *se* $\mathfrak{c}$ *é um múltiplo comum de* $\mathfrak{a}$ *e* $\mathfrak{b}$*, então* $\mathfrak{m} \mid \mathfrak{c}$*.*

Se $\mathfrak{c}$ é um múltiplo comum de $\mathfrak{a}$ e $\mathfrak{b}$, então temos que $\mathfrak{m} \mid \mathfrak{c}$, e, portanto, $\mathfrak{m}$ é menor do que ou igual a $\mathfrak{c}$. Isso indica que, se existe, o mínimo múltiplo comum é único e é o menor dos múltiplos comuns de $\mathfrak{a}$ e $\mathfrak{b}$ e $\mathfrak{mmc}(\mathfrak{a}, \mathfrak{b})$ ou $[\mathfrak{a}, \mathfrak{b}]$ são os símbolos para o mínimo múltiplo comum de $\mathfrak{a}$ e $\mathfrak{b}$, se existir.

É simples demonstrar que se existir $\mathfrak{mmc}(\mathfrak{a}, \mathfrak{b})$ então:

$$\mathfrak{mmc}(-\mathfrak{a}, \mathfrak{b}) = \mathfrak{mmc}(\mathfrak{a}, -\mathfrak{b}) = \mathfrak{mmc}(-\mathfrak{a}, -\mathfrak{b}) = \mathfrak{mmc}(\mathfrak{a}, \mathfrak{b}).$$

Assim, podemos sempre supor que os dois números do cálculo do $\mathfrak{mmc}$ não são negativos.

Além disso, é simples verificar que $\mathfrak{mmc}(\mathfrak{a}, \mathfrak{b}) = 0$ se e apenas se $\mathfrak{a} = 0$ ou $\mathfrak{b} = 0$. Na verdade, se $\mathfrak{mmc}(\mathfrak{a}, \mathfrak{b}) = 0$, então 0 divide $\mathfrak{ab}$, que é o múltiplo de $\mathfrak{a}$ e $\mathfrak{b}$, então $\mathfrak{ab} = 0$ e, portanto, $\mathfrak{a} = 0$ ou $\mathfrak{b} = 0$. Se $\mathfrak{a} = 0$ ou $\mathfrak{b} = 0$, então 0 é o único múltiplo comum de $\mathfrak{a}$ e $\mathfrak{b}$, então $\mathfrak{mmc}(\mathfrak{a}, \mathfrak{b}) = 0$.

Proposição 1. *Dados dois números inteiros* a *e* b*, temos que* $mmc(a,b)$ *existe e*

$$mmc(a,b) \cdot mdc(a,b) = ab.$$

Demonstração. Vide (HEZEZ, 2016, p. 63–64). Ponhamos $m = \dfrac{ab}{mdc(a,b)}$. Como

$$m = a \cdot \frac{b}{mdc(a,b)} = b \cdot \frac{a}{mdc(a,b)}$$

temos que $a \mid m$ e $b \mid m$.

Seja c um múltiplo comum de a e b; logo, $c = na = n'b$. Segue daí que

$$n \cdot \frac{a}{mdc(a,b)} = n' \cdot \frac{b}{mdc(a,b)}.$$

Como, $\dfrac{a}{mdc(a,b)}$ e $\dfrac{b}{mdc(a,b)}$ são primos entre si, segue–se, que $\dfrac{a}{mdc(a,b)}$ divide n', e, portanto, $m = b \cdot \dfrac{a}{mdc(a,b)}$ divide $n'b$ que, é igual a c □

Em virtude da proposição acima, o Algoritmo de Euclides para o cálculo do mdc pode ser usado para encontrar o mínimo múltiplo comum de dois números inteiros não nulos simplesmente dividindo o módulo do produto dos dois números pelo seu mdc.

Exemplo 7. *Dois amigos passeiam de bicicleta, na mesma direção, em torno a uma pista circular. Para dar uma volta completa um deles demora 15 minutos e o outro demora 18 minutos. Eles partem juntos e combinam interromper o passeio quando os dois se encontrarem pela primeira vez no ponto de partida. Quantas voltas deu cada um? (FRANÇA, 2019, p. 34).*

Solução: Denotemos por n_1 e n_2, respectivamente, o número de voltas do primeiro e do segundo amigo. Notemos que o tempo total da corrida é o menor valor positivo de T que satisfaz as igualdades

$$T = 15n_1 = 18n_2,$$

ou seja

$$T = mmc(15, 18).$$

É fácil ver que $\mathtt{mdc}(15, 18) = 3$. Aplicamos agora o Proposição 2.5

$$\mathtt{mmc}(15, 18) \cdot \mathtt{mdc}(15, 18) = 15 \cdot 18.$$

Disso resulta que

$$\mathtt{T} = \mathtt{mmc}(15, 18) = \frac{15 \cdot 18}{3} = 90.$$

Portanto, $\mathtt{n}_1 = 6$ e $\mathtt{n}_2 = 5$.

Corolário 2. *Se* $\mathtt{a}$ *e* $\mathtt{b}$ *são números inteiros primos entre si, então* $\mathtt{mmc}(\mathtt{a}, \mathtt{b}) = \mathtt{ab}$.

Demonstração. Como $\mathtt{a}$ e $\mathtt{b}$ são primos, segue–se que $\mathtt{mdc}(\mathtt{a}, \mathtt{b}) = 1$, usando a proposição anterior, temos $1 \cdot \mathtt{mmc}(\mathtt{a}, \mathtt{b}) = \mathtt{ab}$. Logo segue que $\mathtt{mmc}(\mathtt{a}, \mathtt{b}) = \mathtt{ab}$. □

3.3 Números Primos e Compostos

Ao longo da história da matemática, os números primos foram os protagonistas de problemas conhecidos que impulsionaram o desenvolvimento de teorias e técnicas. Pessoas como Fermat, Euler e Gauss foram exemplos de pensadores excepcionalmente talentosos. Até hoje, muitos desses problemas fáceis de dizer que envolvem números primos constituem desafios intelectuais para o ser humano.

O estudo das propriedades básicas dos números primos será abordado nesta seção, as definições, teoremas e demostrações foram retiradas de Hezez (2016) e França (2019). Isso leva à próxima definição.

Definição 4 (Número Primo)**.** *Um número maior do que* 1 *que só possui como divisores* 1 *e ele próprio é chamado de número primo.*

Dados dois números primos $\mathtt{p}$ *e* $\mathtt{q}$ *e um número inteiro* $\mathtt{a}$ *qualquer, decorrem da definição acima os seguintes fatos:*

(i) *Se* $\mathtt{p} \mid \mathtt{q}$*, então* $\mathtt{p} = \mathtt{q}$.

De fato, como $\mathtt{p} \mid \mathtt{q}$ *e sendo* $\mathtt{q}$ *primo, temos que* $\mathtt{p} = 1$ *ou* $\mathtt{p} = \mathtt{q}$*. Sendo* $\mathtt{p}$ *primo, tem–se que* $\mathtt{p} > 1$*, o que acarreta* $\mathtt{p} = \mathtt{q}$.

(ii) *Se* $\mathtt{p} \nmid \mathtt{a}$*, então* $\mathtt{mdc}(\mathtt{p}, \mathtt{a}) = 1$.

De fato, se $\mathtt{mdc}(\mathtt{p}, \mathtt{a}) = \mathtt{d}$*, temos que* $\mathtt{d} \mid \mathtt{p}$ *e* $\mathtt{d} \mid \mathtt{a}$*. Portanto,* $\mathtt{d} = \mathtt{p}$ *ou* $\mathtt{d} = 1$*. Mas* $\mathtt{d} \neq \mathtt{p}$*, pois* $\mathtt{p}$ *não divide* $\mathtt{a}$ *e, consequentemente,* $\mathtt{d} = 1$.

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

Portanto, se um número natural $m > 1$ é composto, existirá um divisor natural k_1 de m tal que $1 < k_1 < m$. Logo, existirá um número natural k_2 tal que

$$m = k_1 k_2, \quad \text{com} \quad 1 < k_1 < m \quad \text{e,} \quad 1 < k_2 < m.$$

Por exemplo, 2, 3, 5, 7, 11 e 13 são números primos, enquanto que 4, 6, 8, 9, 10, 12 e 15 são compostos

Como pode ser visto, todos os números primos são ímpares, exceto o número 2. Além disso, o número 1 não é considerado primo ou composto.

Do ponto de vista da estrutura multiplicativa dos números naturais, os números primos são os mais simples e ao mesmo tempo são suficientes para gerar todos os números naturais, portanto todos os inteiros diferentes de zero, como encaremos mais adiante na proposição Fundamental Aritmética.

Proposição 2 (Lema de Euclides)**.** *Sejam* $a,\ b,\ p \in \mathbb{Z}$*, com* p *primo. Se* $p \mid ab$*, então* $p \mid a$ *ou* $p \mid b$*.*

Demonstração. Se $p \mid a$, nada há que o demostrar, e se, ao invés, p não divide a, então são dito primo, ou seja, $mdc(a, p) = 1$. Logo se tem que $p \mid b$. □

Corolário 3. *Se* $p,\ p_1,\ \ldots,\ p_n$ *são números primos e, se* $p \mid p_1 \cdots p_n$*, então* $p = p_i$ *para algum* $i = 1,\ \ldots,\ n$*.*

Demonstração. Use a Proposição anterior (Lema de Euclides) indução sobre n, e o fato de que, se $p \mid p_i$, então $p = p_i$. □

Exemplo 8. *Mostre que o número* $n = 2^{20} - 25^4$ *é composto.*

Solução: Escrevemos n de outra forma, com o objetivo de facilitar nosso trabalho. Com efeito, observamos que

$$n = \left(2^{10}\right)^2 - \left(25^2\right)^2 = 1024^2 - 625^2,$$

logo é composto por ser diferença de quadrados. Além disso,

$$\begin{aligned} n &= 1024^2 - 625^2 \\ &= (1024 - 625)(1024 + 625) \\ &= 399 \cdot 1649 \\ &= 3 \cdot 133 \cdot 1649. \end{aligned}$$

Portanto, podemos concluir que $3 \mid n$.

Problema 2 (Revista do Professor de Matemática – RPM Nº 47)**.** *Eu e meu irmão caçula temos idades entre 10 e 20 anos e hoje nossas idades são expressas ambas por números primos, fato que se repetirá pela próxima vez daqui há 18 anos. Determine minha idade sabendo que a idade de nosso irmão mais velho, que, hoje, também é um número primo, é uma unidade maior do que a soma das nossas idades.*

Solução: As duplas de primos entre 10 e 20 são:

$$11 \text{ e } 13, \quad 11 \text{ e } 17, \quad 11 \text{ e } 19, \quad 13 \text{ e } 17, \quad 13 \text{ e } 19 \quad \text{e} \quad 17 \text{ e } 19.$$

Como a soma dos números adicionada de 1 deve resultar um primo, descarto as duplas 11 e 13 e 13 e 19. Como daqui a 18 anos as idades voltam a ser representadas por números primos, descarto as duplas que incluem o 17. Resta apenas uma possibilidade: minha idade é 19 anos e a do meu irmão é 11 anos.

Problema 3 (Revista do Professor de Matemática – RPM Nº 47)**.** *Uma equação do* 2ž *grau, cujos coeficientes são todos números primos, pode apresentar duas raízes iguais?*

Solução: Para que a equação $ax^2 + bx + c = 0$ (com a, b e c primos) admita duas raízes iguais, devemos ter $b^2 - 4ac = 0$ ou $b^2 = 4ac$, o que implica b^2 par. Logo, b também é par e, como é primo, $b = 2$. De $b^2 = 4ac$ temos $ac = 1$, o que é absurdo para a e c primos.

Problema 4 (Revista do Professor de Matemática – RPM Nº 47)**.** *Para quantos pontos da circunferência* $x^2 + y^2 = 361$ *as duas coordenadas são números primos?*

Solução: Se x e y satisfazem a equação $x^2 + y^2 = 361$, sendo 361 ímpar, devemos ter x par e y ímpar ou x ímpar e y par. Se x é par e primo, então, $x = 2$; logo, $y^2 = 357$ e y

não é, então, um número inteiro. Do mesmo modo verificamos ser impossível ter y par e x ímpar; logo, nenhum ponto da circunferência de equação $x^2 + y^2 = 361$ tem ambas as coordenadas dadas por números primos.

Agora vamos enunciar um dos resultados mais clássicos da Matemática que garante a existência de infinitos números primos. Até onde se conhece, a demonstração a seguir foi a primeira demonstração escrita utilizando o método de redução ao absurdo e é devida a Euclides cerca de 300 a.C.

Teorema 4 (Teorema de Euclides)**.** *A quantidade de números primos é infinita.*

Demonstração. Faremos a prova por redução ao absurdo. Suponha que existe uma quantidade finita de números primos e denotemos estes por

$$p_1,\ p_2,\ p_3, \ldots,\ p_k$$

Consideremos o número

$$n = p_1 p_2 p_3 \cdots p_k + 1$$

e chamamos de q o seu menor divisor primo. Obviamente q não coincide com nenhum dos números p_i, $1 \leqslant i \leqslant k$, pois caso contrário, como ele divide n, teria que dividir 1, o que é impossível. Logo, temos uma contradição à hipótese de termos uma quantidade finita de primos. □

3.4 Teorema Fundamental da Aritmética

Qualquer número natural é produto de números primos; portanto, os números primos são "células"dos números naturais. Como exemplo,

$$720 = 72 \cdot 10 = 9 \cdot 8 \cdot 5 \cdot 2 = 3 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 2,$$

onde cada um dos componentes do produto é representado por números primos. Nos perguntamos o que aconteceria se começássemos com uma outra fatoração inicial de 720, por exemplo, $720 = 36 \times 20$. Veja isso:

$$720 = 36 \cdot 20 = 6 \cdot 6 \cdot 2 \cdot 10 = 3 \cdot 2 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 5$$

Observamos surpreendentemente a mesma representação anterior, exceto pela ordem dos fatores. Assim, quatro "células"do tipo 2, uma "célula"do tipo 5 e duas "células"do tipo 3 compõem o número 720.

O fato mencionado anteriormente se aplica a qualquer número natural maior que 1. O Teorema Fundamental da Aritmética foi proposto de forma precisa por Gauss (1777–1855), que é o foco de nosso estudo. Este teorema foi utilizado por Fermat, Euler, Lagrange e Legendre, entre outros pensadores anteriores, sem se preocupar em explicá-lo com precisão.

Teorema 5 (Teorema Fundamental da Aritmética)**.** *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. Usaremos a segunda forma do Princípio de Indução. Se $n = 2$, o resultado é obviamente verificado.

Suponhamos o resultado 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. Logo, existem números naturais n_1 e n_2 tais que

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

Pela hipótese de indução, temos que existem números primos $p_1, \ldots, p_r$ e $q_1, \ldots, q_s$ tais que

$$n_1 = p_1 \cdots p_r \quad \text{e} \quad n_2 = q_1 \cdots q_s.$$

Portanto, $n = p_1 \cdots p_r \cdot q_1 \cdots q_s$.

Vamos, agora, provar a unicidade da escrita. Suponha, agora, que $n = p_1 \cdots p_r = q_1 \cdots q_s$, onde os p_i e os q_j são números primos. Como $p \mid (q_1 \cdots q_s)$, pelo Corolário 2.3, temos que $p = q_j$ para algum j, que, após reordenamento de $q_1, \ldots, q_s$, podemos supor que seja q_1. Portanto,

$$p_2 \cdots p_r = q_2 \cdots q_s$$

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

Enunciado dessa forma, o Teorema Fundamental da Aritmética é um resultado que,

além de garantir a existência da representação de um número natural maior do que 1 como um produto de seus divisores primos, garante que essa representação é única. Entre outros benefícios, esse resultado garante que podemos iniciar o processo de procura dos divisores primos pelo primo que nos for conveniente.

Além disso, podemos observar que a maneira como representamos o número n na demonstração do Teorema como o produto de primos $n = p_1 \cdots p_r \cdot q_1 \cdots q_s$, estávamos admitindo que os primos que aparecem nesta decomposição *não são necessariamente distintos*, o que atende, inclusive, ao exemplo inicial dessa nossa seção onde vimos que o número 560 é composto de quatro células do tipo 2, uma célula do tipo 5 e uma célula do tipo 7, isto é

$$560 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 5 \cdot 7 \text{ ou ainda, } 560 = 2^4 \cdot 5 \cdot 7$$

Assim, em particular, também podemos enunciar o Teorema Fundamental da Aritmética da seguinte maneira.

Seja n *um número natural,* $n > 1$. *Então existem números primos* $p_1 < p_2 < p_3 < \ldots < p_r$, *e, também, números naturais não nulos* $n_1,\ n_2,\ n_3,\ \ldots,\ n_r$, *univocamente determinados, com* $r \geqslant 1$, *tais que*

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \cdots p_r^{n_r}.$$

Observamos que escrito nessa forma, n está decomposto como produto de potências cujas bases são números primos distintos dois a dois.

Esta forma de representar um número natural $n > 1$,

$$n = p_1^{n_1} \cdot p_2^{n_2} \cdot p_3^{n_3} \cdots p_r^{n_r}$$

é denominada "*decomposição canônica de n em fatores primos*".

Observação 1. *Dizemos que um inteiro positivo é livre de quadrados se ele não é divisível pelo quadrado de nenhum número inteiro maior do que* 1. *Por exemplo, os números* 15 *e* 42 *são livres de quadrados visto que* $15 = 3 \cdot 5$ *e* $42 = 2 \cdot 3 \cdot 7$ *(não estão decompostos como produto de potências cujas bases são números primos distintos dois a dois), enquanto que* 40 *e* 1372 *não são livres de quadrados, uma vez que* $40 = 2^3 \cdot 5$ *e* $1372 = 2^2 \cdot 7^3$ *(estão decompostos como produto de potências cujas bases são números primos distintos dois a*

dois).

A decomposição única em primos se aplica em contextos mais gerais, como veremos mais adiante (subseção 2.6.1). Aqui, como aplicação imediata do Teorema Fundamental da Aritmética, listaremos, a seguir, através de exemplos e problemas, o uso desta ferramenta em variados contextos e níveis de ensino.

Exemplo 9. *Nas turmas de sextos anos de uma escola há* 120 *alunos, e nos sétimos anos há* 105 *alunos. Para realizar um trabalho comunitário, os alunos serão organizados em grupos do maior tamanho possível, todos com o mesmo número de alunos e sem que se misturem alunos de anos diferentes. Pergunta–se:*
a) Qual é o número máximo de alunos que pode haver em cada grupo?
b) Que fração irredutível representa a razão entre o número de alunos do sétimo e sexto anos?
c) Seja $\mathtt{N}$ *o número total de alunos de ambas as turmas. Então* $\sqrt{\mathtt{N}}$ *vale?*
Aqui temos uma aplicação imediata do Teorema Fundamental da Aritmética na determinação do $\mathtt{mdc}$ *(máximo divisor comum) entre dois inteiros positivos, na simplificação de frações e, ainda, na obtenção de uma raiz exata.*

Solução item a): Conhecidas as decomposições canônicas de dois inteiros positivos $\mathtt{a} > 1$ e $\mathtt{b} > 1$, o $\mathtt{mdc}(\mathtt{a}, \mathtt{b})$ é o produto dos fatores comuns às duas decomposições tomados cada um com o menor expoente, e o $\mathtt{mmc}(\mathtt{a}, \mathtt{b})$, a saber, é o produto dos fatores primos comuns e não comuns às duas decomposições tomados cada um com o maior expoente. Assim, pelo Teorema Fundamental da Aritmética, temos:

$$120 = 2^3 \cdot 3 \cdot 5 \quad \text{e} \quad 105 = 3 \cdot 5 \cdot 7$$

Os fatores primos comuns são 3 e 5. Portanto, o número de alunos em cada grupo será o maior divisor comum aos dois números, nesse caso, $3 \cdot 5 = 15$. Logo, o número máximo de alunos em cada grupo será 15.
Solução item b): A razão entre o número de alunos do sétimo e sexto ano é $\dfrac{105}{120}$. Como o item solicita a fração irredutível representada por essa razão, basta utilizarmos a resposta do item a), isto é, dividir o numerador e o denominador dessa fração por 15

$$\frac{105}{120}\overset{\div 15}{}_{\div 15} = \frac{7}{8}.$$

Note que poderíamos, também, ter decomposto em fatores primos cada um dos termos dessa fração e, de uma maneira prática, cancelar aqueles fatores em comum chegando ao mesmo resultado.

$$\frac{105}{120} = \frac{\cancel{3} \cdot \cancel{5} \cdot 7}{2 \cdot 2 \cdot 2 \cdot \cancel{3} \cdot \cancel{5}} = \frac{7}{8}.$$

Solução item c): Como N é a soma do número de alunos das turmas do sexto e sétimo anos, temos:

$$\mathsf{N} = 120 + 105 = 225$$

Agora o nosso problema se resume em determinar $\sqrt{\mathsf{N}}$, isto é, $\sqrt{225}$.

Uma alternativa para a obtenção dessa raiz é o método da decomposição em fatores primos. Através da decomposição do número 225 em fatores primos e da simplificação dos expoentes dos fatores pelo índice do radicando, extraímos a sua raiz quadrada eliminando dessa forma o radical. Assim, pelo Teorema Fundamental da Aritmética, segue que:

$$225 = 3^2 \cdot 5^2.$$

Portanto, $\sqrt{225} = \sqrt{3^2 \cdot 5^2} = 3 \cdot 5 = 15$.

Problema 5 (OBM 2013 – 2º FASE – NÍVEL 1)**.** *Um número natural é chamado quadrado perfeito quando ele é o quadrado de outro número natural. Por exemplo,* 1 *e* 25 *são quadrados perfeitos pois* $1 = 1^2$ *e* $25 = 5^2$*. Qual é o menor valor de* $\mathfrak{a} + \mathfrak{b}$*, com* $\mathfrak{a}$ *e* $\mathfrak{b}$ *números naturais não nulos, para que os números* $28 \cdot \mathfrak{a}^3 \cdot \mathfrak{b}$ *e* $7 \cdot \mathfrak{a} \cdot \mathfrak{b}^5$ *sejam ambos quadrados perfeitos?*

Solução: Um número é quadrado perfeito quando os primos em sua fatoração tem expoente par. Assim, pelo Teorema Fundamental da Aritmética, observamos que $28 = 2^2 \cdot 7$ e $7 = 7^1$. Nota–se que devemos intervir no expoente do 7. Fora isso, não devemos nos preocupar com o 2, pois o seu expoente em 28 é 2, que é par. Então, pelo menos um dos números $\mathfrak{a}$ ou $\mathfrak{b}$ é divisível por 7, ou seja, um deles é pelo menos 7 e o outro é pelo menos 1 . Logo a soma é no mínimo 8. Note que os valores $\mathfrak{a} = 7$ e $\mathfrak{b} = 1$ satisfazem a condição, já que e que $28 \cdot \mathfrak{a}^3 \cdot \mathfrak{b} = 98^2$ e $7 \cdot \mathfrak{a} \cdot \mathfrak{b}^5 = 7^2$.

Exemplo 10. *Determine o menor inteiro positivo pelo qual se deve dividir o número* 10800 *para se obter um cubo perfeito.*

Solução: Um número é dito cubo perfeito quando os primos em sua decomposição tem expoente igual a um múltiplo de 3. Assim, pelo Teorema Fundamental da Aritmética, temos que

$$10800 = 2^4 \cdot 3^3 \cdot 5^2.$$

Desta forma, para determinar o número que devemos dividir 10800, devemos retirar de sua decomposição em primos um fator igual a dois (2) e os dois fatores iguais a cinco (5^2) resultando em um cubo perfeito

$$2^3 \cdot 3^3.$$

Portanto, o menor número que divide 10800 resultando em um cubo perfeito é $2 \cdot 5^2 = 50$.

Problema 6 (ENC 2002 – EXAME NACIONAL DE CURSOS)**.** *Qual é o menor número natural n que torna n! divisível por 1000?*

Solução: Pelo Teorema Fundamental da Aritmética segue que $1000 = 10^3 = 2^3 \cdot 5^3$. Assim, temos:

$$\mathtt{n}! = 1000 \cdot \mathtt{k} = 2^3 \cdot 5^3 \cdot \mathtt{k}, \;\; \mathtt{k} \in \mathbb{N}$$

Para que seja possível que $\mathtt{n}!$ tenha números cujo o produto seja 1000, deve acontecer $1000 = 2^3 \cdot 5^3$, isto é

$$\begin{aligned} \mathtt{n}! &= 2^3 \cdot 5^3 \cdot \mathtt{k} \\ \mathtt{n}! &= 1 \cdot 2 \cdot 3 \cdot (2^2) \cdot 5 \cdot (2 \cdot 3) \cdot 7 \cdot (2^3) \cdot 3^2 \cdot (2 \cdot 5) \cdot 11 \cdot (2^2 \cdot 3) \cdot 13 \cdot (2 \cdot 7) \cdot (3 \cdot 5) \end{aligned}$$

Note que com o produto de três números pares consecutivos obtemos o caso 2^3, por outro lado, o caso 5^3 acontece quando multiplicamos os números 5, 10 e 15. Portanto $\mathtt{n} = 15$.

Problema 7 (PROFMAT 2013 – ENA – EXAME NACIONAL DE ACESSO)**.** *Seja* $\mathtt{N} = 12^{2012} + 2012^{12}$*. O maior valor de* $\mathtt{n}$ *tal que* $2^{\mathtt{n}}$ *é divisor de* $\mathtt{N}$ *é*

(A) 10 *(B)* 12 *(C)* 16 *(D)* 24 *(E)* 36

Solução: Pelo Teorema Fundamental da Aritmética podemos escrever os números 12 e 2012 como um produto de fatores primos, isto é

$$12 = 2^2 \cdot 3 \quad \text{e} \quad 2012 = 2^2 \cdot 503$$

Logo,

$$\begin{aligned} N &= (2^2 \cdot 3)^{2012} + (2^2 \cdot 503)^{12} \\ N &= 2^{4024} \cdot 3^{2012} + 2^{24} \cdot 503^{12} \\ N &= 2^{24} \cdot \left(2^{4000} \cdot 3^{2012} + 503^{12} \right) \end{aligned}$$

Então 2^{24} divide N. Para saber se existe uma potência de 2 maior que 2^{24} que divide N, precisamos saber se o número entre parênteses é par ou ímpar. Se for ímpar, então não é divisível por 2 e 24 é a potência máxima que divide N.

Ora, o termo da esquerda, entre parênteses, é claramente um múltiplo de 2, portanto é par. Já o termo da direita é uma potência de um número ímpar, que sempre é ímpar. A soma dos dois termos é, portanto, ímpar. Logo, 24 é a maior potência de 2 que divide N.

Problema 8 (PROFMAT 2013–ENA – EXAME NACIONAL DE ACESSO)**.** *A média geométrica de três números positivos é a raiz cúbica do produto dos três. Se a média geométrica de três números naturais distintos é igual a 5, qual é a soma desses três números?*

(A) 15 *(B)* 16 *(C)* 21 *(D)* 30 *(E)* 31

Solução: Temos $\sqrt[3]{abc} = 5$, onde a, b e c são números naturais distintos, logo $abc = 5^3 = 125$. Pelo Teorema Fundamental da Aritmética, a, b e c são potências de 5. Supondo, sem perda de generalidade, que $a < b < c$, devemos ter $a = 5^0$, $b = 5$ e $c = 5^2$, pois se $c = 5^3$, os outros dois teriam que ser iguais a 1, e não seriam então distintos. Se nenhum deles for 5^2, então os três têm que ser 1 ou 5, ou seja, necessariamente dois deles seriam iguais, o que não é permitido. Logo $a + b + c = 1 + 5 + 25 = 31$.

Exemplo 11. *Prove que um número n é par se, e somente se, o número 2 aparece na fatoração de n em fatores primos.*

Demonstração. Obviamente, se 2 aparece na fatoração em primos de N, então N é par. Ora, se n é par temos que $n = 2q$. Por outro lado q e n se fatoram, respectivamente, como

$$q = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_m^{\alpha_m} \quad \text{e} \quad p = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}.$$

Logo,

$$2 \cdot q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_m^{\alpha_m} = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}.$$

Pela unicidade de fatoração, para algum i, com $1 \leqslant i \leqslant s$, o correspondente p_i, deve ser igual a 2. Portanto, 2 aparece na fatoração de n. □

Para encerrar este capítulo, vejamos ainda outras aplicações do Teorema Fundamental da Aritmética no Ensino Básico.

3.5 Aplicações do Teorema Fundamental da Aritmética

Além do uso na simplificação de frações e radicais, na determinação da raiz enésima aritmética e do cálculo do mmc e do mdc de dois ou mais números inteiros positivos, uma das aplicações mais recorrentes do TFA em turmas do Ensino Básico é o uso do mesmo, por exemplo, para determinar a quantidade de divisores de um número inteiro qualquer positivo.

A seguir, listamos quatro teoremas que nos darão, por meio do TFA, fórmulas e procedimentos que nos fornecerão, respectivamente, os divisores, o número de divisores de um inteiro positivo e, as não tão usuais, soma e produto dos divisores de um número inteiro positivo.

3.5.1 Divisores de um inteiro positivo

Teorema 6. *Se* $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$ *é decomposição canônica do inteiro positivo* $n > 1$*, então os divisores positivos de* n *são precisamente os inteiros* d *da forma:*

$$d = p_1^{h_1} \cdot p_2^{h_2} \cdots p_r^{h_r},$$

onde $0 \leqslant h_i \leqslant k_i$ *(*$i = 1,\ 2,\ \ldots,\ r$*).*

Demonstração. Obviamente, os divisores triviais $d = 1$ e $d = n$ de n se obtém quando, respectivamente:

$$h_1 = h_2 = \ldots = h_r = 0$$

e

$$h_1 = k_1,\ h_2 = k_2,\ \ldots,\ h_r = k_r$$

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

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

Exprimindo d e d_1 como produtos de primos, não necessariamentes distintos, temos:

$$d = q_1 \cdot q_2 \cdots q_s, \quad d_1 = t_1 \cdot t_2 \cdots t_u$$

obtemos:

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r} = q_1 \cdot q_2 \cdots q_s \cdot t_1 \cdot t_2 \cdots t_u$$

que são duas decomposições do inteiros positivo n num produto de primos, e como é única uma decomposição de n de tal natureza, então cada primo q_i coincide com o p_j, de modo que, substituindo os produtos de primos iguais por potências de expoente inteiro, teremos:

$$d = q_1 \cdot q_2 \cdots q_s = p_1^{h_1} \cdot p_2^{h_2} \cdots p_r^{h_r}$$

onde é possivel alguma $h_i = 0$.

Reciprocamente, todo inteiro

$$d = p_1^{h_1} \cdot p_2^{h_2} \cdots p_r^{h_r}$$

onde $0 \leqslant h_i \leqslant k_i$ é um divisor de n, pois, podemos escrever:

$$\begin{aligned} n &= p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r} \\ n &= \left(p_1^{h_1} \cdot p_2^{h_2} \cdots p_r^{h_r}\right) \cdot \left(p_1^{k_1-h_1} \cdot p_2^{k_2-h_2} \cdots p_r^{k_r-h_r}\right) \\ n &= d \cdot \left(p_1^{k_1-h_1} \cdot p_2^{k_2-h_2} \cdots p_r^{k_r-h_r}\right) \end{aligned}$$

onde $k_i - h_i \geqslant 0$ para cada i. Logo, d é um divisor de n, ou seja, $d \mid n$. □

Exemplo 12. *Determine os divisores positivos do inteiro* $n = 1350$.

Solução: Pelo Teorema Fundamental da Aritmética, o número 1350 pode ser escrito da seguinte forma: $n = 1350 = 2 \cdot 3^3 \cdot 5^2$.

São precisamente os inteiros d da forma:

$$d = 2^{h_1} \cdot 3^{h_2} \cdot 5^{h_3}$$

onde $0 \leqslant h_1 \leqslant 1$, $0 \leqslant h_2 \leqslant 3$, $0 \leqslant h_3 \leqslant 2$, isto é,

$$h_1 = 0,\ 1; \quad h_2 = 0,\ 1,\ 2,\ 3; \quad h_3 = 0,\ 1,\ 2.$$

Assim, como $h_1 = 1$, $h_2 = 2$ e $h_3 = 0$, obtemos o divisor:

$$\begin{aligned} d &= 2^1 \cdot 3^2 \cdot 5^0 \\ d &= 2 \cdot 9 \cdot 1 \\ d &= 18 \end{aligned}$$

do inteiro 1350. Realmente: $1350 = 18 \cdot 75$.

Como $h_1 = h_2 = h_3 = 0$ e $h_1 = 1$, $h_2 = 3$, $h_3 = 2$ acham–se os divisores triviais $d = 1$ e $d = 1350$ do inteiro em questão.

3.5.2 Número de divisores

Teorema 7. *Se* $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$ *é a decomposição canônica do inteiro positivo* $n > 1$*, então:*

$$d(n) = (k_1 + 1)(k_2 + 1) \ldots (k_r + 1)$$

Demonstração. Pelo teorema anterior, os divisores positivos de n são precisamente os inteiros d da forma:

$$d = p_1^{h_1} \cdot p_2^{h_2} \cdots p_r^{h_r}$$

onde,

$$0 \leqslant h_1 \leqslant k_1, \quad 0 \leqslant h_2 \leqslant k_2, \quad \ldots, \quad 0 \leqslant h_r \leqslant k_r$$

Temos $k+1$ maneiras de escolher o expoente h_1, k_2+1 maneiras de escolher o expoente h_2, $\ldots$, k_r+1 maneiras de escolher o expoente h_r e, portanto, o número total de maneiras de escolher os expoentes $h_1,\ h_2,\ \ldots,\ h_r$ é dado pelo produto:

$$(k_1 + 1)(k_2 + 1) \ldots (k_r + 1)$$

Assim sendo, o número $d(n)$ de divisores positivos do inteiro $n > 1$ é dado pela fórmula:

$$d(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1),$$

ou seja,

$$d(n) = \prod_{i=1}^{r} (k_i + 1).$$

□

Exemplo 13. *Determinar a quantidade de divisores positivos do inteiro* $n = 756$.

Solução: Decompondo o número 756 em um poduto de números primos, temos:

$$n = 756 = 2^2 \cdot 3^3 \cdot 7$$

Assim,

$$\begin{aligned} d(756) &= (2+1) \cdot (3+1) \cdot (1+1) \\ d(756) &= 3 \cdot 4 \cdot 2 \\ d(756) &= 24 \end{aligned}$$

Logo existem 24 divisores positivos de 756.

Problema 9 (PROFMAT 2012 – ENA – EXAME NACIONAL DE ACESSO)**.** *O número total de divisores positivos de* $10! = 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ *é igual a:*
A) 15 *B)* 270 *C)* 320 *D)* 1024 *E)* 10!

Solução: Pelo Teorema Fundamental da Aritmética, observe que 10! pode ser escrito como

$$\begin{aligned} 10! &= 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \\ &= (2 \cdot 5) \cdot (3 \cdot 3) \cdot (2 \cdot 2 \cdot 2) \cdot 7 \cdot (2 \cdot 3) \cdot 5 \cdot (2 \cdot 2) \cdot 3 \cdot 2 \cdot 1 \\ &= 2^8 \cdot 3^4 \cdot 5^2 \cdot 7. \end{aligned}$$

Logo, cada divisor de 10! será da forma $2^m \cdot 3^n \cdot 5^p \cdot 7^q$ onde são números naturais tais que $0 \leqslant m \leqslant 8$; $0 \leqslant n \leqslant 4$; $0 \leqslant p \leqslant 2$; $0 \leqslant q \leqslant 1$.

Portanto, pelo princípio multiplicativo temos que a quantidade de divisores de 10! é

$$(8+1)\cdot(4+1)\cdot(2+1)\cdot(1+1) = 9\cdot 5\cdot 3\cdot 2 = 270$$

Problema 10 (ENEM 2014)**.** *Durante a Segunda Guerra Mundial, para decifrarem as mensagens secretas, foi utilizada a técnica de decomposição em fatores primos. Um número* N *é dado pela expressão* $2^{\mathtt{x}}\cdot 5^{\mathtt{y}}\cdot 7^{\mathtt{z}}$*, na qual* $\mathtt{x}$*,* $\mathtt{y}$ *e* $\mathtt{z}$ *são números inteiros não negativos. Sabe–se que* N *é múltiplo de* 10 *e não é múltiplo de* 7*. O número de divisores de* N*, diferentes de* N*, é*

A) $\mathtt{x}\cdot\mathtt{y}\cdot\mathtt{z}$

B) $(\mathtt{x}+1)\cdot(\mathtt{y}+1)$

C) $\mathtt{x}\cdot\mathtt{y}\cdot\mathtt{z}-1$

D) $(\mathtt{x}+1)\cdot(\mathtt{y}-1)\cdot\mathtt{z}$

E) $(\mathtt{x}+1)\cdot(\mathtt{y}+1)\cdot(\mathtt{z}+1)-1$

Solução: Temos que o número $\mathsf{N} = 2^{\mathtt{x}}\cdot 5^{\mathtt{y}}\cdot 7^{\mathtt{z}}$. O fato de N ser múltiplo de 10, significa que na decomposição de N irá aparecer pelo menos um fator 2 e pelo menos um fator 5, ou seja, tanto o expoente $\mathtt{x}$ como o expoente $\mathtt{y}$ são diferentes de 0. Do mesmo modo que o fato de N não ser múltiplo de 7 significa que na fatoração de N não haverá nenhum fator 7, ou seja, o expoente $\mathtt{z}$ será igual a 0. Para obtermos o número de divisores de um número N a partir de sua decomposição em fatores primos, devemos obter todas as combinações possíveis para seus expoentes incluindo o zero. Assim, em nosso caso, as possibilidades para o expoente do fator 2 são iguais a $\mathtt{x}$ mais o zero[1], isto é, $\mathtt{x}+1$. De modo análogo, as possibilidades para os expoentes $\mathtt{y}$ e $\mathtt{z}$, respectivamente são $\mathtt{y}+1$ e $\mathtt{z}+1$. Assim, temos que o número de divisores de N é $(\mathtt{x}+1)\cdot(\mathtt{y}+1)\cdot(\mathtt{z}+1)$, incluindo o próprio N. Como queremos os divisores diferentes de N, teremos: $(\mathtt{x}+1)\cdot(\mathtt{y}+1)\cdot(\mathtt{z}+1)-1$.

Problema 11 (OBM 2012 – 1º FASE – NÍVEL 2)**.** *Qual é o menor número ímpar que possui exatamente 10 divisores positivos incluindo o 1 e o próprio número?*

A) 1875 *B) 405* *C) 390* *D) 330* *E) 105*

Solução: Pelo Teorema Fundamental da Aritmética, os números que possuem exatamente 10 divisores positivos podem assumir apenas uma das possíveis formas: $\mathtt{p}^4\mathtt{q}$ ou $\mathtt{p}^9$ onde $\mathtt{p}$

[1]Note que o expoente $\mathtt{x}\in\{0,\ 1,\ 2,\ldots,\ \mathtt{x}\}$, isto é, este expoente $\mathtt{x}$ do fator 2 pode assumir $\mathtt{x}$ valores naturais variando de 1 até ele mesmo além do zero obtendo, assim, $\mathtt{x}+1$ possibilidades. De forma análoga segue para os expoentes $\mathtt{y}\in\{0,\ 1,\ 2,\ldots,\ \mathtt{y}\}$ e $\mathtt{z}\in\{0,\ 1,\ 2,\ldots,\ \mathtt{z}\}$ dos fatores 5 e 7 respectivamente.

e q representam primos distintos. O menor número ímpar da primeira forma é $3^4 \cdot 5 = 405$, enquanto o segundo número é 3^9, que é bem maior do que 405. Logo, a resposta correta é 405.

Problema 12 (OBMEP 2015 – 2º FASE – NÍVEL 3)**.** *Seja n um número inteiro positivo. Se, para cada divisor primo p de n, o número p^2 não divide n, dizemos então que n é livre de quadrados. Mostre que todo número livre de quadrados tem uma quantidade de divisores que é igual a uma potência de* 2*.*

Solução: Seja n um número inteiro positivo livre de quadrados. Pelo Teorema Fundamental da Aritmética, podemos escrever n como um produto de fatores primos

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

onde $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_k$ é igual a 0 ou 1, pois $p \nmid n$.

A quantidade de divisores de um número é a combinação entre todos os expoentes diferentes de cada fator primo variando de 0 a α_i, com $i = 0,\ 1,\ 2,\ 3,\ \ldots,\ k$.

Assim temos dois possíveis expoentes para α_1, dois para α_2, até k, dois para α_k. Logo a quantidade de divisores é

$$\underbrace{2 \cdot 2 \cdot 2 \cdots 2}_{k \text{ vezes}} = 2^k,$$

ou seja, uma potência de 2.

Problema 13 (PROFMAT 2017 – ENQ – EXAME NACIONAL DE QUALIFICAÇÃO)**.** *Prove que um número inteiro positivo n possui uma quantidade ímpar de divisores positivos se, e somente se, é um quadrado perfeito.*

Demostração: Pelo Teorema Fundamental da Aritmética,

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$$

sendo $p_1 < p_2 < \ldots < p_k$ números primos e $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_k$ números inteiros positivos. A quantidade de divisores de n é dado por

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

($\Longrightarrow$) Se n tem um número ímpar de divisores, então todos os fatores de $d(n)$ são números ímpares, ou seja, $\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_k$ são números pares. Portanto

$$n = \left(p_1^{\frac{\alpha_1}{2}} \cdot p_2^{\frac{\alpha_2}{2}} \cdots p_k^{\frac{\alpha_k}{2}}\right)^2$$

($\Longleftarrow$) Por outro lado, se n é um quadrado perfeito, então $n = c^2$ para algum $c \in \mathbb{Z}$. Isto implica que todos os α_i são números pares e então $d(n)$ é ímpar, por ser o produto de ímpares.

3.5.3 Soma dos divisores

Teorema 8. *Se $n = p_1^{k_1} \cdot p_2^{k_2} \cdots p_r^{k_r}$ é a decomposição canônica do inteiro positivo $n > 1$, então a soma dos divisores de n, denotado por $S(n)$, é dada pela expressão:*

$$s(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

Demonstração. Consideremos o produto

$$\left(1 + p_1 + p_1^2 + \ldots + p_1^{k_1}\right)\left(1 + p_2 + p_2^2 + \ldots + p_2^{k_2}\right)\ldots\left(1 + p_r + p_r^2 + \ldots + p_r^{k_r}\right)$$

Pelo Teorema (2.8), cada divisor positivo de n é um termo do desenvolvimento deste produto e vice–versa, de modo que

$$s(n) = \left(1 + p_1 + p_1^2 + \ldots + p_1^{k_1}\right)\left(1 + p_2 + p_2^2 + \ldots + p_2^{k_2}\right)\ldots\left(1 + p_r + p_r^2 + \ldots + p_r^{k_r}\right)$$

Aplicando a cada parêntese do segundo membro desta igualdade a fórmula que dá a soma dos termos de uma progressão geométrica finita, temos:

$$s(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdots \frac{p_r^{k_r+1} - 1}{p_r - 1},$$

ou seja,

$$s(n) = \prod_{i=1}^{r} \frac{p_i^{k_i+1} - 1}{p_i - 1},$$

□

Exemplo 14. *Determine a soma dos divisores positivos do inteiro $n = 180$.*

Solução: Pelo Teorema Fundamental da Aritmática, temos: $n = 180 = 2^2 \cdot 3^2 \cdot 5$.

Logo,

$$\begin{aligned} s(180) &= \frac{2^{2+1}-1}{2-1} \cdot \frac{3^{2+1}-1}{3-1} \cdot \frac{5^{1+1}-1}{5-1} \\ s(180) &= 7 \cdot 13 \cdot 6 \\ s(180) &= 546 \end{aligned}$$

a soma de todos os divisores positivos é 546.

3.5.4 Produto dos divisores

Teorema 9. *O produto dos divisores positivos de um inteiro positivo* $n > 1$ *é igual a*

$$n^{\frac{d(n)}{2}}.$$

Demonstração. Sejam $d_1,\ d_2,\ \ldots,\ d_{n(d)}$ todos os divisores positivos de n, de modo que existem os inteiros $q_1,\ q_2,\ \ldots,\ q_{n(d)}$ tais que

$$n = d_1 q_1, \quad n = d_2 q_2, \quad \ldots, \quad n = d_{n(d)} q_{n(d)}.$$

Como $d_1 d_2 \cdots d_{n(d)} = q_1 q_2 \cdots q_{n(d)}$, porque cada um dos inteiros $q_1,\ q_2,\ \ldots,\ q_{n(d)}$ também é divisor de n, temos:

$$n^{d(n)} = \left(d_1 \cdot d_2 \cdots d_{n(d)} \right)^2 \Longrightarrow d_1 \cdot d_2 \cdots d_{n(d)} = n^{\frac{d(n)}{2}}.$$

□

Exemplo 15. *Determine o produto dos divisores positivos do inteiro* $n = 16$.

Solução: Temos que $d_1 \cdot d_2 \cdots d_{n(d)} = 16^{\frac{d(16)}{2}}$. Como $d(16) = 5$, segue que

$$\begin{aligned} d_1 \cdot d_2 \cdots d_5 &= 16^{\frac{5}{2}} \\ &= (4^2)^{\frac{5}{2}} \\ &= 4^5 \\ &= 1024 \end{aligned}$$

De fato, os divisores positivos do número 16 são $1,\ 2,\ 4,\ 8$ e 16, e o produto destes 5 divisores é igual a 1024.

Chegamos aos parágrafos finais deste capítulo no qual abordamos o Teorema Fundamental da Aritmética e suas aplicações e os principais conceitos fundamentais da aritmética elementar que estão associados a ele.

A seguir, descrevemos o quadro teórico fundamentado na Teoria dos Campos Conceituais que serviu de base para a nossa pesquisa e para a elaboração da nossa proposta de ensino.

4 Procedimentos Metodológicos

A natureza da abordagem que direciona este estudo é qualitativa, em que, de fato interessa é o levado em consideração dos métodos e os significados desenvolvidos e encontrados.

> "Pesquisa qualitativa trabalha com o universo de significados, motivos, aspirações, crenças, valores e atitude, o que corresponde a um espaço mais profundo das relações, dos processos e dos fenômenos que não podem ser reduzidos à operacionalização de variáveis [...]" (MINAYO, 2001, p.22).

Quanto ao método, será utilizada a pesquisa do tipo bibliográfico. "A pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos". (GIL, 2019, p. 44). Serão acessados a base de dados da Biblioteca Brasileira de Teses e Dissertações em busca de trabalhos já produzidos sobre a temática a fim de que seja elaborado um plano de estudos sobre o assunto.

Neste estudo, "desenvolvida com base em material já elaborado [...]" (GIL, 2002, p.44), buscar–se–á o reconhecimento da utilização do Teorema Fundamental da Aritmética visando indicá–lo para o ensino da Educação Básica.

Para a consecução da pesquisa observar–se–á os seguintes passos: identificação das fontes bibliográficas (que será em base de dados eletrônicos); leitura do material; seleção de trechos relevantes; fichamento; organização lógica do trabalho; redação do texto (GIL, 2019). Estes procedimentos visam todo o percurso do trabalho desde a seleção do material até a estruturação das categorias para análise. Segundo Gil (2002, p.45) "A principal vantagem da pesquisa bibliográfica reside no fato de permitir ao investigador a cobertura e uma gama de fenômenos muito mais ampla do que aquela que poderia pesquisar diretamente". .

Neste trabalho, observar-se-á como os sujeitos que produziram estudos a partir do Teorema Fundamental da Aritmética visando o Ensino Fundamental se posicionam quanto ao mérito da questão.

A técnica para a interpretação dos dados será a Análise Temática. Segundo Richardson (2012, p. 243), esta técnica "consiste em isolar temas de um texto e extrair as partes utilizáveis, de acordo com o problema pesquisado, para permitir sua comparação com outros textos escolhidos da mesma maneira".

Por fim, segundo Marconi e Lakatos (1992) "a pesquisa bibliografia já publicada, em forma de livros, revistas, publicação avulsas e imprensa escrita [...]". O tema da pesquisa já

foi material de estudos posteriores, por conta disso o estudo exposto fará uso de materiais como: livros, revistas, artigos científicos, sites, blogs e diversas outras fontes.

5 Conclusão

O intuito desse estudo foi explorar o Teorema Fundamental da Aritmética e os principais conceitos relacionados a ele com alunos do 6º ano do Ensino Fundamental Anos Finais.

Apresentamos um breve panorama da história dos números primos, alguns aspectos teóricos e uma das suas aplicações práticas. O objetivo dessa narrativa sobre os números primos é incentivar o leitor a despertar sua curiosidade investigativa. Por fim, sugerimos algumas abordagens para trabalhar com números primos no 6º ano do Ensino Fundamental.

Por fim, esperamos que esse trabalho possa servir como material de apoio para o docente de matemática da educação básica, com vistas a sanar algumas dificuldades e omissões dos nossos livros didáticos. E, também, que possa servir de motivação e inspiração para que o mesmo busque aperfeiçoar sua prática pedagógica, apresentando novas aplicações em sala de aula.

Referências

BARBOSA, Gabriela dos Santos. **Números Primos e o Teorema Fundamental da Aritmética no Sexto Ano do Ensino Fundamental**. Dissertação de mestrado PROFMAT: Instituto Nacional de Matemática Pura e Aplicada IMPA. Rio de Janeiro - RJ, 2015.

BARBOSA, Gabriela Dos Santos. **O Teorema Fundamental da Aritmética: jogos e problemas com alunos do sexto ano do Ensino Fundamental**. Tese de Doutorado - Programa de Pós-Graduação em Educação Matemática) –Pontifícia Universidade Católica de São Paulo – PUC/SP, 2008.

BRASIL. **Base Nacional Comum Curricular**: Educação Infantil e Ensino Fundamental. Brasília: MEC/Secretaria de Educação Básica, 2017.

CARVALHO, Fernando Ramires. **Números Primos e o Teorema Fundamental da Aritmética no Sexto Ano do Ensino Fundamental**. Dissertação de mestrado PROFMAT: Instituto Nacional de Matemática Pura e Aplicada IMPA. Rio de Janeiro - RJ, 2015.

COSTA, Roberta Marcele Vaz da. **Números Primos e o Teorema Fundamental da Aritmética no Sexto Ano do Ensino Fundamental**. Dissertação de mestrado PROFMAT: Instituto Nacional de Matemática Pura e Aplicada IMPA. Rio de Janeiro - RJ, 2015.

D'AMBROSIO, Ubiratan. **Educação Matemática**: Da Teoria à Prática, 4ª edição. São Paulo: Papirus Editora, 1998.

DANTE, L. R. **Didática da Resolução de Problemas de Matemática**, 12ª edição. São Paulo: Editora Ática, 2007.

DANTE, L. R. **Matemática**: Contexto e Aplicações, 3ª edição. São Paulo: Editora Ática, 2017. v. 1, 2 e 3.

DANTE, L. R. **Projeto Teláris**: Matemática, 6º, 7°, 8° e 9° ano, 2ª edição. São Paulo: Editora Ática, 2016.

EVES, Howard. **Introdução à História da Matemática**. São Paulo: Editora Unicamp, 2004.

FRANÇA, Francisco José da Silva. **Entre primos e compostos**: uma abordagem do Teorema Fundamental da Aritmética no 6º ano do Ensino Fundamental. Dissertação de mestrado PROFMAT: Universidade Estadual do Piauí - UESPI. Teresina - PI, 2019.

GIL, Antonio Carlos. **Com elaborar projetos de pesquisa**, 4º edição. São Paulo: Altas, 2002.

HEFEZ, Abramo. **Aritmética**. Coleção PROFMAT. Rio de Janeiro: SBM, 2016.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. **Fundamentos de Metodologia Científica**. 3ª edição. São Paulo: Editora Atlas, 1991.

LINS, Romulo Campos; GIMENEZ, Joaquim. **Perspectivas em aritmética e álgebra para o século XXI**. 4º Edição. Campinas: Papirus, 1997.

MACEDO, Carlos Eduardo de Carvalho. **Números primos, nossos amigos únicos**. Dissertação (Mestrado - Programa de Pós–Graduação em Matemática) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2019.

MACHADO, S. D. A.; MARANHÃO, M.C.; COELHO, S. P. **Como é utilizado o Teorema Fundamental da Aritmética por atores do Ensino Fundamental**. In: Actas do V CIBEM. Porto, julho de 2005, v.1, p. 1-12.

MARCONI, Mariana de Andrade, LAKATOS, Eva Maria. **Fundamentos de Metodologia Cientifica**, 8ª edição. São Paulo: Altas, 2017.

POLYA, G. **Sobre a Resolução de Problemas de Matemática na High School**. IN: KRULIK, Stephen; REYS, Robert E.A Resolução de Problemas na Matemática Escolar. São Paulo: Atual Editora, 1997. Cap 1, p. 1–3.

QUINTANS, Jeozadaque. **O ensino dos números primos inter-relacionados a conteúdos diversos através da resolução de problemas**. Dissertação (Mestrado - Programa de Pós-Graduação em Mestrado Profissional em Matemática em Rede Nacional) – Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, 2020.

RICHARDSON, Roberto Jarry; PERES, José Augusto de Sousa; WANDERLEY, José Carlos Vieira; PERES, Maria de Holanda de Melo. **Pesquisa Social**: métodos e técnicas. 3. ed. São Paulo: Atlas, 2012.

RIBENBOIM, P. **Números Primos, amigos que causam problemas**. Rio de Janeiro: SBM, 2015.

RIBENBOIM, P. **Números Primos**: Velhos Mistérios e Novos Recordes. Rio de Janeiro: IMPA, 2012.

RESENDE, M.R. **Re–Significando a disciplina Teoria dos Números na formação do Professor de Matemática na Licenciatura**. Tese de Doutorado. Pontifícia Universidade Católica De São Paulo. São Paulo. 2007

ROONEY, Anne. **A História da Matemática**: Desde a criação das pirâmides até a exploração do infinito. São Paulo: M. Books do Brasil Editora, 2012.

SANTOS, Josiel Almeida; FRANÇA, Kleber Vieira; SANTOS, Lúcia Silveira Brum dos. **Dificuldades na Aprendizagem de Matemática**. 2007, 41 f. Trabalho de Conclusão de Curso (Matemática) – Universidade Adventista de São Paulo, São Paulo, 2007.

SAUTOY, Marcus du. **A Música dos Números Primos**: a história de um problema não resolvido na matemática. Tradução: Diego Alfaro. Rio de Janeiro: Jorge Zahar Ed., 2007.

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.

VERGNAUD, G. **A criança, a Matemática e a Realidade**: problemas do ensino da matemática na escolar elementar. Trad. Moro, M. L. F. Curitiba: UFPR Press, 2009.

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