Elisangela Bastos de Mélo Espindola
Fabiano Barbosa Mendes da Silva
Marcelo Pedro dos Santos
organizadores

COLETÂNEA DE ESTUDOS DE EGRESSOS DO PROFMAT-UFRPE

Blucher Open Access

COLETÂNEA DE ESTUDOS DE EGRESSOS DO PROFMAT - UFRPE

Blucher Open Access

ELISANGELA BASTOS DE MÉLO ESPINDOLA
FABIANO BARBOSA MENDES DA SILVA
MARCELO PEDRO DOS SANTOS
(organizadores)

Editora Edgard Blücher Ltda.

Publisher Edgard Blücher
Editor Eduardo Blücher
Coordenação editorial Jonatas Eliakim
Produção editorial Kedma Marques
Diagramação Caroline Costa e Silva
Revisão de texto Danilo Villa
Capa Laércio Flenic
Imagem da capa iStockphoto

Editora Blucher
Rua Pedroso Alvarenga, 1245, 4º andar
CEP 04531-934 – São Paulo – SP – Brasil
Tel.: 55 11 3078-5366
contato@blucher.com.br
www.blucher.com.br

Dados Internacionais de Catalogação na Publicação (CIP)
Angélica Ilacqua CRB-8/7057

Coletânea de estudos de egressos do ProfMat-UFRPE / organizado por Elisangela Bastos de Mélo Espindola, Fabiano Barbosa Mendes da Silva, Marcelo Pedro dos Santos. – São Paulo : Blucher, 2021.283p.

ISBN (impresso): 978-65-5550-097-4

ISBN (digital): 978-65-5550-094-3

1. Matemática - Estudo e ensino 2. Geometria - Estudo e ensino I. Espindola, Elisangela Bastos de Melo II. Silva, Fabiano Barbosa Mendes da III. Santos, Marcelo Pedro dos

21-3242 CDD 620.001185

Índices para catálogo sistemático:

1. Matemática - Estudo e ensino

Apresentação

Anete Soares Cavalcanti
Fabiano Barbosa Mendes da Silva

A Universidade Federal Rural de Pernambuco – UFRPE, ao longo dos seus 108 anos de existência, consolidou-se em uma instituição com tradição em ensino, pesquisa e extensão, cuja missão tem como foco "distribuir e disseminar conhecimento e inovação" baseada nos anseios da sociedade. Nesse sentido, o Departamento de Matemática oferece o Mestrado Profissional em Matemática em Rede Nacional – PROFMAT, que é um curso semipresencial com oferta nacional coordenado pela Sociedade Brasileira de Matemática – SBM.

Em março de 2011 um grupo de 49 Instituições de Ensino Superior, distribuídas em todo o Brasil, lançou-se no desafio de compor o primeiro Programa de Mestrado Profissional para Qualificação de Professores da Rede Pública da Educação Básica (ProEB), PROFMAT. A UFRPE, como parte desse grupo, abraçou o sonho coletivo de mudar o Ensino de Matemática no Brasil em vários âmbitos através de ações como formação continuada de professores, projetos de ensino e extensão, e ainda promoção do envolvimento, direta ou indiretamente, de estudantes do PROFMAT com Cursos de Graduação e com Escolas do Ensino Básico. Atualmente o PROFMAT é composto por mais de 76 Instituições Associadas (101 cidades de atendimento) abrangendo todos os Estados do Brasil. A partir dessa experiência, outros Mestrados Profissionais do ProEB foram surgindo e hoje abrangem todas as grandes áreas da Educação Básica.

Ainda no âmbito da UFRPE, é importante destacar que o PROFMAT co-

memora 10 anos de existência em 2021 e vem crescendo ao longo dos anos, tendo sua qualidade reconhecida através do Conceito 5 na CAPES (nota máxima que um programa de pós-graduação apenas com o curso de mestrado pode obter) em duas avaliações quadrienais consecutivas, e já conta com mais de 100 defesas de Trabalho de Conclusão de Curso (TCC)/Dissertação.

A diversidade de temas abordados nesses trabalhos motivou-nos a propor esta Coletânea de Estudos de Egressos do PROFMAT-UFRPE, que se constitui como um registro histórico e, sobretudo, científico, evidenciando o impacto que esse conhecimento pode ter na formação de professores e irrefutavelmente na sua prática em sala de aula. Nesse sentido, apresentamos a seguir uma breve descrição dos estudos trazidos nesta coletânea.

O primeiro estudo trata-se de Uma Proposta Didática para o Estudo de Área e Perímetro no Ensino Fundamental II, em que as autoras, motivadas pelas dificuldades e barreiras de aprendizagem dos estudantes do ensino fundamental no que concerne ao estudo da geometria, propõem uma sequência didática para o ensino de área e perímetro de figuras planas baseada em oficina de construções, medições de contornos e uso de geoplanos, buscando tornar a aprendizagem mais significativa.

Na sequência, o segundo capítulo aborda a Função de Euler e o Princípio da Inclusão e Exclusão, apresentando os principais conceitos, teoremas e exemplos que envolvem essa função, ressaltando ainda a sua interligação ao Princípio da Inclusão e Exclusão, conteúdo amplamente abordado no Ensino Médio.

O terceiro estudo, Considerações sobre Matemática Financeira e Educação Financeira no Ensino Médio: Uma breve análise de documentos oficiais e livro didáticos, apresenta as diferenças entre Educação Financeira e Matemática Financeira e ainda aborda as principais orientações dos documentos oficiais norteadores de propostas curriculares, com ênfase na Base Nacional Curricular Comum (BNCC), e discutem acerca das propostas de ensino de Educação Financeira nos livros didáticos aprovados no PNLE 2018.

O quarto capítulo consagra-se aos Códigos Corretores de Erros no Ensino Médio: Um estudo sobre o Código de Hamming, em que o objetivo é

contribuir para a inserção desse tema na Educação Básica através de uma apresentação mais elementar, propondo, adicionalmente, uma sequência didática para o ensino desse código.

Para o quinto capítulo reserva-se o tema O Estudo de Polinômios com Relatos de História da Matemática, que tem como objetivo apresentar uma abordagem mais atrativa do estudo dos polinômios na Educação Básica a partir da utilização da História da Matemática como ferramenta auxiliar no processo de ensino-aprendizagem, contando ainda com um diferente design na elaboração do texto. O sexto estudo versa Sobre Algoritmos de Ordenação e sua Abordagem no Ensino Médio, cujo objetivo é a realização de uma abordagem didática acerca dos algoritmos Bubble Sort, Selection Sort e Quick Sort, baseando-se nas competências e habilidades propostas na BNCC, nos Parâmetros Curriculares Nacionais de Matemática e nos Parâmetros Curriculares do Estado de Pernambuco.

No sétimo capítulo o tema desenvolvido é Teoria dos Números no Ensino Básico: Uma proposta de texto didático. O objetivo deste estudo é abordar teoricamente os conteúdos mais clássicos da Teoria dos Números que pertencem ao currículo do Ensino Fundamental, tais como divisibilidade e números primos, dentre outros, apresentando os principais resultados, demonstrações e exemplos.

O oitavo capítulo aborda o tema Cônicas: Refletindo e aprendendo. Com o objetivo de apresentar aos estudantes do Ensino Básico um viés menos abstrato e mais concreto e significativo das cônicas, este estudo propõe atividades como experimentos e sequências didáticas como auxiliares na formação dos principais conceitos.

Por fim, o último capítulo versa sobre A Utilização de Problemas Matemáticos em Aberto no Ensino Médio. A principal ideia deste estudo é abordar alguns desses problemas no Ensino Médio com o objetivo de incentivar o uso de atividades investigativas pelos estudantes. Para tal, foram apresentados problemas em aberto envolvendo números primos, progressões e geometria, dentre outros, e ainda sugestões de atividades para que professores do Ensino Médio possam utilizar em suas aulas.

Sumário

1 Uma proposta didática **15**

1.1 Introdução 16

1.2 Fundamentos teóricos e metodológicos 18

1.2.1 A geometria - breve histórico 18

1.2.2 A geometria euclidiana 19

1.2.3 Sequência didática 24

1.2.4 Metodologia - material e métodos 26

1.2.4.1 Montagem da sequência didática 27

1.2.4.2 Aplicação da sequência didática 30

1.3 Considerações finais 36

1.3.1 Análise pré-teste 37

1.3.2 Análise pós-teste 39

1.3.3 Conclusão 40

1.4 Referências bibliográficas 42

1.4.1 Anexo 1 pré-teste 44

1.4.2 Anexo 2 pós-teste 46

2 Função ϕ de Euler **49**

2.1 Introdução 50

2.2 Função totiente de Euler 51

2.3 Estudo combinatorial de $\phi(n)$ 61

2.4 Função ϕ de Euler e o princípio de inclusão e exclusão . . 63

2.4.1 Cardinalidade da união de dois conjuntos 63

2.4.2 Cardinalidade da união de três conjuntos 65

2.4.3 Princípio da inclusão e exclusão 68
2.5 Considerações finais 71
2.6 Referências bibliográficas 72

3 Considerações sobre matemática 73
3.1 Introdução 74
3.2 Educação financeira e matemática financeira 75
3.3 Considerações sobre a matemática financeira e a educação financeira em orientações curriculares 77
3.3.1 PCN + ensino médio 78
3.3.2 Orientações curriculares para o ensino médio . . . 78
3.3.3 Parâmetros curriculares para a educação básica no estado de Pernambuco 79
3.3.4 Base nacional comum curricular 80
3.4 Matemática financeira e educação financeira nos livros didáticos (PNLD 2018) 84
3.4.1 Organização dos capítulos sobre matemática financeira nos LD 85
3.4.2 Introdução do tema 87
3.5 Considerações finais 90
3.6 Referências bibliográficas 91

4 Códigos corretores 95
4.1 Introdução 96
4.2 Teoria da informação e códigos corretores de erros 98
4.2.1 O código de Hamming 100
4.2.2 Códigos detectores de um único erro 104
4.2.3 Códigos corretores de um único erro 106
4.2.4 Justificativa dos algoritmos e construção da tabela 2 113
4.2.5 O código $C(7,4)$ e a família de códigos $C(2^k-1, 2^k-k-1)$ 116

4.3 Considerações finais 127
4.4 Referências bibliográficas 128

5 O estudo de polinômios 131
5.1 Origem da álgebra 132
5.2 O cálculo algébrico 134
5.2.1 Expressão algébrica 135
5.2.2 Classificação das expressões algébricas 136
5.2.3 Valor numérico de uma expressão algébrica 136
5.3 Monômios 138
5.3.1 Grau de um monômio 141
5.3.2 Monômios semelhantes 141
5.3.3 Operações com monômios 141
5.4 Polinômios 142
5.4.1 Grau de um polinômio 143
5.4.2 Polinômio com uma variável 143
5.5 Operações com polinômios 144
5.5.1 Adição e subtração 144
5.5.2 Multiplicação e divisão 145
5.6 Produtos notáveis 149
5.6.1 Quadrado da soma de dois termos 149
5.6.2 Quadrado da diferença de dois termos 150
5.6.3 Produto da soma pela diferença de dois termos . . 151
5.6.4 Cubo da soma e da diferença de dois termos 153
5.6.5 Fatorial 153
5.6.6 Combinação 155
5.6.7 Binômio de Newton 156
5.6.8 Triângulo aritmético 160
5.6.9 Fatoração 163
5.7 Referências bibliográficas 166

6 Sobre algoritmos 167
6.1 Introdução 168

6.2 Fundamentos teóricos e metodológicos 169
6.2.1 Análise dos parâmetros curriculares 169
6.2.2 Algoritmos de ordenação e complexidade 174
6.2.2.1 *Bubble Sort* 176
6.2.2.2 *Selection Sort* 178
6.2.2.3 *Quick Sort* 180
6.2.2.4 Comparação gráfica das complexidades dos algoritmos de ordenação 186
6.2.3 Sequência didática 187
6.3 Considerações finais 190
6.4 Referências bibliográficas 191

7 Teoria dos números 193
7.1 Fundamentos teóricos e metodológicos 194
7.1.1 Divisibilidade 194
7.1.2 Divisão Euclidiana 197
7.1.3 Números primos 199
7.1.4 Máximo divisor comum - MDC 204
7.1.5 Menor múltiplo comum - MMC 209
7.1.6 Equações diofantinas 213
7.1.7 Congruências 216
7.1.8 Teorema de Euler e Fermat 220
7.2 Considerações finais 223
7.3 Referências bibliográficas 223

8 Cônicas: Refletindo e aprendendo 225
8.1 Introdução 226
8.2 Fundamentos teóricos e metodológicos 228
8.2.1 Sequência didática - aplicação das atividades lúdicas 231
8.2.1.1 Atividade 1: Experimento com lanterna (Duração: 1 aula). 233
8.2.1.2 Atividade 2: Contruções das cônicas com barbante (Duração: 3 aulas). 235

8.2.1.3 Atividade 3: Construção das cônicas usando dobradura (Duração: 2 aulas). 240
8.2.1.4 Atividade 4: Experimento de reflexão (Duração: 2 aulas). 245
8.2.1.5 Atividade 5: Visita ao museu interativo de ciência de Pernambuco − Espaço Ciência (Duração: 4 aulas). 249
8.3 Considerações finais 251
8.4 Referências bibliográficas 253

9 A utilização de problemas matemáticos 257
9.1 Introdução 258
9.2 Fundamentos teóricos e metodológicos 261
9.2.1 Problemas em aberto de teoria dos números 261
9.2.1.1 Os Números primos 261
9.2.2 Problemas em aberto de combinatória 265
9.2.2.1 Quadrados mágicos 265
9.2.3 Quadrados mágicos de quadrados perfeitos 269
9.2.4 Quadrados mágicos de números primos 270
9.2.4.1 Problemas em aberto de geometria . . . 272
9.2.4.2 O Tijolo de Euler 273
9.2.5 Aplicação em sala de aula 274
9.2.5.1 Quadrados mágicos e progressões aritméticas 274
9.3 Considerações finais 287

Capítulo 1

Uma proposta didática para o ensino de perímetro e área no ensino fundamental II

Ma. Debora Simone Ferreira de Queiroz Araujo[1]
Dra. Anete Soares Cavalcanti [2]

Resumo: A Geometria é, sem dúvida, uma das partes mais fascinantes da Matemática. Sua integração com a Álgebra e a Aritmética torna essa unidade temática ainda mais envolvente, mas esse fascínio não é vivido pelos alunos do Ensino Fundamental II, pois, para a sua maioria, a Geometria tem se tornado uma inimiga, que traz consigo dificuldades e barreiras na aprendizagem. Diante dessa situação, viemos propor, com este trabalho, uma Sequência Didática para o ensino de Perímetro e Área das Figuras Planas no Ensino Fundamental II, baseada em oficina de construções, medições de contornos e uso de geoplanos, buscando tornar a aprendizagem mais significativa. A opção pelos conteúdos de Perímetro e Área das Figuras Planas se deu devido à unidade temática de Geometria ser revisada no

[1]Professora da Rede Estadual de Educação de Pernambuco e da Rede Municipal de Camocim de São Félix - PE, debora_simone@hotmail.com

[2]Professora da Universidade Federal Rural de Pernambuco - UFRPE, anete.soares@ufrpe.br

segundo semestre nas turmas do 9^o ano da Escola pesquisada e ao fato de que esses conteúdos têm tido baixo índice de acertos na Prova Brasil e em outras avaliações externas.

Palavras-chave: Perímetro; Área; Figuras Planas; Oficina; Sequência Didática.

1.1 Introdução

As dificuldades que norteiam o ensino da Matemática têm sido observadas em muitas situações, como na retenção de alunos nas suas séries, em avaliações nacionais (Prova Brasil e SAEPE - Sistema de Avaliação da Educação de Pernambuco) e também nas avaliações internacionais, como o PISA (Programa Internacional de Avaliação de Estudantes), no qual o Brasil se encontra entre os 10 piores desempenhos do mundo em Matemática (MORENO; OLIVEIRA, 2019).

A necessidade de inovação nas aulas de Matemática, buscando motivar o aluno de forma que este se torne protagonista e interaja no processo de aprendizagem, bem como o desenvolvimento de conhecimentos básicos que são requisitos em sua série/ano para uma aprendizagem eficaz, têm sido o anseio de muitos professores.

Segundo a BNCC, o Ensino Fundamental deve ter compromisso com o "letramento matemático",

> O Ensino Fundamental deve ter compromisso com o desenvolvimento do letramento matemático, definido como as competências e habilidades de raciocinar, representar, comunicar e argumentar matematicamente, de modo a favorecer o estabelecimento de conjecturas, a formulação e a resolução de problemas em uma variedade de contextos, utilizando conceitos, procedimentos, fatos e ferramentas matemáticas (BRASIL, 2018, p. 266).

Esse letramento matemático busca desenvolver no aluno a junção das competências e habilidades necessárias à Matemática, sendo aferido em

diversas avaliações como a avaliação do PISA, conforme sua matriz de 2012.

A Geometria, uma das cinco unidades temáticas que compõem o ensino da Matemática no Ensino Fundamental, conforme a BNCC, "envolve o estudo de um amplo conjunto de conceitos e procedimentos necessários para resolver problemas do mundo físico e de diferentes áreas do conhecimento" (BRASIL, 2018). Logo, contemplar todo esse "amplo conjunto de conceitos" não tem sido uma tarefa fácil, seja pelas dificuldades apresentadas pelos alunos ou mesmo de professores nessa área de ensino, seja pelo extenso currículo de cada ano/série, seja pelas lacunas existentes na vida escolar de alunos e professores.

Outra indicação da BNCC para o ensino da Geometria é que ele não fique inserido apenas ao uso de fórmulas e seus respectivos cálculos,

> Assim, a Geometria não pode ficar reduzida a mera aplicação de fórmulas de cálculo de área e de volume nem a aplicações numéricas imediatas de teoremas sobre relações de proporcionalidade em situações relativas a feixes de retas paralelas cortadas por retas secantes ou do teorema de Pitágoras. A equivalência de áreas, por exemplo, já praticada há milhares de anos pelos mesopotâmios e gregos antigos sem utilizar fórmulas, permite transformar qualquer região poligonal plana em um quadrado com mesma área (é o que os gregos chamavam "fazer a quadratura de uma figura"). Isso permite, inclusive, resolver geometricamente problemas que podem ser traduzidos por uma equação do 2º grau (BRASIL, 2018, p. 272).

Portanto, a experimentação e a construção de atividades que possibilitem ampliar o conhecimento do aluno tornam-se ainda mais atual. Diante disso, os conteúdos escolhidos para a pesquisa foram Perímetro e Área de Figuras Planas e o público-alvo para vivência da Oficina foram os alunos do Reforço Escolar. Na Escola onde foi feita a pesquisa, os alunos que apresentam baixo rendimento escolar são encaminhados para o Reforço, aulas que acontecem duas vezes na semana, com duração de 1 (uma) hora cada

aula no contra-turno. Nelas, são averiguadas as dificuldades dos alunos e são organizadas atividades para facilitar a aprendizagem e melhorar o desempenho dos mesmos junto às suas turmas.

Para avaliar a Oficina, aplicamos um Pré-Teste com 10 (dez) questões de Perímetro e Área das Figuras Planas, retiradas das avaliações anteriores do SAEPE, com as duas turmas das quais os alunos do Reforço Escolar participam, para que pudéssemos mensurar o nível dos alunos. E, após a aplicação da Oficina, um Pós-Teste, com o mesmo público envolvido.

Esse artigo é um recorte da dissertação de Araujo (2020), cujo objetivo é apresentar uma Sequência Didática a ser utilizada para o ensino de Perímetro e Área de Figuras Planas por professores do Ensino Fundamental II. Sendo ressaltado, como objetivo específico, o envolvimento de atividades práticas para consolidação dos conceitos de Perímetro e Área das Figuras Planas.

O artigo possui quatro seções, as duas primeiras trazem um breve histórico sobre a Geometria e a Geometria Euclidiana. A terceira traz uma Sequência Didática para o Ensino de Perímetro e Área de Figuras Planas aplicada com os alunos do Reforço Escolar de duas turmas do 9^o ano, sendo baseada em atividades de construção e medição de figuras planas. Na quarta, sintetizamos os resultados observados na aplicação da Oficina e fizemos uma comparação entre o Pré-Teste e o Pós-Teste.

1.2 Fundamentos teóricos e metodológicos

1.2.1 A geometria - breve histórico

Segundo Boyer, afirmar sobre a origem da Geometria é muito arriscado, pois os primórdios desse assunto são mais antigos do que a arte de escrever, uma vez que a origem da Geometria foi dada por Heródoto e Aristóteles à civilização egípcia. Ainda conforme Boyer, "Heródoto mantinha que a geometria se originava no Egito, pois acreditava que tinha surgido da necessidade prática de fazer novas medidas de terras após cada inundação anual no vale do rio", diferente do pensamento de Aristóteles que "achava que a existência no Egito de uma classe sacerdotal com lazeres é que tinha

conduzido ao estudo da geometria"(1974, p. 5).

As ideias de Heródoto e Aristóteles concordam que os egípcios foram os primeiros a utilizar a Geometria, mas divergem quanto à origem. Não podemos contradizê-los nem reafirmá-los, mas podemos pensar que a origem da Geometria se deu bem antes dos egípcios. O homem neolítico talvez não tivesse a necessidade de remarcar suas propriedades, talvez também não tivesse lazeres sacerdotais, mas seus desenhos e figuras sugerem uma preocupação com as relações espaciais, conforme Boyer (1974).

Vinda do Egito, a Geometria teria chegado até a Grécia no século 5 a.C. por Tales de Mileto, segundo Bicudo (2009). No Egito e na Babilônia, o critério de verdade era a experiência, ou seja, acreditava-se naquilo que a pessoa via. Mol (2013) ressalta que foram as necessidades práticas que serviram de estímulo para o desenvolvimento da matemática egípcia. Essas experiências eram repassadas por meio de registros, como o célebre *Papiro de Rhind*, datado de cerca de 1650 a.C., que contém 84 problemas de geometria e de aritmética acompanhados de soluções, entre eles, o cálculo de área.

Segundo Mol, na Grécia, a Matemática "deixou de ser uma coleção de resultados empíricos e passou a ter o formato de uma ciência organizada de maneira sistemática e por elementos racionais" (2013, p. 29). Dessa forma, com os conhecimentos práticos do Egito e da Babilônia, os gregos começaram a aperfeiçoar a Geometria. Por volta de 300 a.C., Euclides fez o primeiro grande resumo dos conhecimentos matemáticos existentes na época, que estão organizados em seu livro *Os Elementos*, no qual suas "noções comuns" e seus "postulados" do Livro I são as primeiras noções geométricas que são aceitas sem contestações, e, a partir delas, são organizados e demonstrados diversos conceitos (BICUDO, 2009).

1.2.2 A geometria euclidiana

A Geometria Euclidiana está fundamentada no livro *Os Elementos* de Euclides, no qual ele demonstra 465 proposições contidas em 13 livros (capítulos) utilizando "definições", "postulados" e "noções comuns" (também

chamadas de axiomas) e adotando o *método axiomático-dedutivo*.

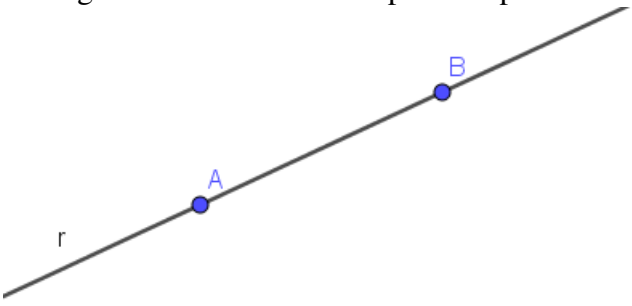
Segundo Mol (2013), Euclides utiliza a ideia de Aristóteles sobre os axiomas e os postulados, diferenciando-os em seu livro. Entretanto, hoje não fazemos distinção entre postulados e axiomas.

> Segundo Aristóteles, os axiomas eram "indispensáveis de conhecer para aprender qualquer coisa", eram verdades comuns a todos os estudos e tinham validade geral. Os postulados seriam menos óbvios, não pressupondo conhecimento prévio, uma vez que se aplicavam apenas ao objeto em estudo - a geometria, no caso. Essa ideia aristotélica é usada por Euclides ao separar seus postulados dos axiomas. A matemática moderna, no entanto, não faz distinção entre os dois conceitos (MOL, 2013, p. 48).

Como afirma Bicudo (2009), os cinco postulados nos quais se baseia a Geometria Euclidiana, na íntegra, traduzidos do grego são:

- **1º Postulado** *Fique postulado traçar uma reta a partir de todo ponto até todo ponto.*

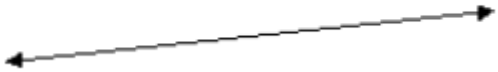
Figura 1.1: Reta definida por dois pontos



FONTE: Produzida pela autora

- **2º Postulado** *Também prolongar uma reta limitada, continuamente, sobre uma reta.*

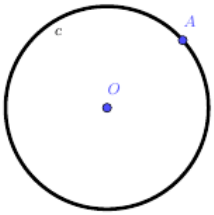
Figura 1.2: Segmento prolongado sobre reta



FONTE: Produzida pela autora

- **3º Postulado** *E, com todo centro e distância, descrever um círculo.*

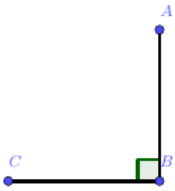
Figura 1.3: Círculo de centro e raio quaisquer



FONTE: Produzida pela autora

- **4º Postulado** *E serem iguais entre si todos os ângulos retos.*

Figura 1.4: Ângulos Retos



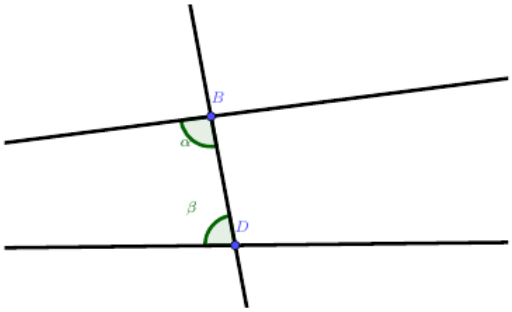
FONTE: Produzida pela autora

Na verdade, os quatro primeiros postulados não possuem alta complexidade para entendimento. Talvez, as dificuldades apresentadas pelos leitores sejam referentes ao termo *reta limitada* do **2º Postulado** e ao termo *distância* (quando trata do raio do círculo) no **3º Postulado**.

- **5º Postulado** *E, caso uma reta, caindo sobre duas retas, faça os*

ângulos interiores e do mesmo lado menores do que dois retos, sendo prolongadas as duas retas, ilimitadamente, encontrarem-se no lado qual estão os menores do que dois retos.

Figura 1.5: Postulado das Paralelas



FONTE: Produzida pela autora

O **5º Postulado** também conhecido como o **Postulado das Paralelas**, durante anos, foi muito criticado por diversos matemáticos. Eles discordavam que ele seria um Postulado e acreditavam que ele poderia ser provado utilizando os postulados anteriores. É importante ressaltar que a negação do 5º Postulado geraria a descoberta de novas geometrias, como a Geometria Hiperbólica, entre outras.

Esses postulados, juntamente com as definições e os axiomas, serviram de base para as demonstrações dos teoremas e construção das figuras contidas no livro *Os Elementos*.

Os *Elementos* não pode ser considerado apenas um compêndio de Geometria, pois contém toda a Matemática conhecida daquela época, por volta de 300 a.C.. Com certeza, representa uma das obras mais importantes da Matemática, mesmo não possuindo aplicações nem exercícios e a exposição das demonstrações sendo feita de forma direta. Foi utilizado pelas Escolas e Universidades até o final do século XIX e início do século XX. Segundo Barbosa "a geometria ensinada na escola secundária é, frequentemente, cópia quase literal de 8 ou 9 dos 13 volumes que o constituem"(2012, p. 71). Tornou-se o livro mais traduzido para outras línguas, ao lado da Bíblia, como afirma Barbosa,

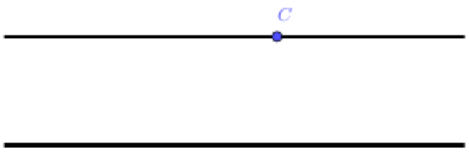
> Ao lado da bíblia, é sem dúvida o livro mais reproduzido e estudado de todos os que já foram escritos na história do mundo ocidental. Mais de 1000 edições dele já foram produzidas desde a invenção da imprensa e, antes disto, cópias manuscritas dominavam todo o ensino da matemática (2012, p. 71).

Quando as primeiras traduções do livro *Os Elementos* de Euclides foram feitas por volta de 1482, em plena Renascença, muitos interessados começaram um minucioso estudo sobre os teoremas e resultados nele contidos, com ênfase no Postulado das Paralelas e se ele era ou não um axioma independente dos outros, conforme Mol (2013). Vários estudos foram feitos por muitos matemáticos ao longo dos séculos, tentando demonstrar o Postulado das Paralelas utilizando os outros postulados, o que o faria deixar de ser um postulado, mas eles não tiveram êxito.

Segundo Avila (1992), existem várias formulações para o Postulado das Paralelas. Uma das mais simples e muito encontrada nos livros didáticos é a de John Playfair, enunciada abaixo:

Postulado de Playfair - *Por um ponto fora de uma reta não se pode traçar mais que uma reta paralela à reta dada.*

Figura 1.6: Retas Paralelas



FONTE: Produzida pela autora

A culminância no desenvolvimento da Geometria, como aponta Bicudo (2009), se deu no final do século XIX, no ano de 1897, com a obra *Fundamentos da Geometria*, na qual o matemático alemão David Hilbert apresentou um sistema axiomático para a Geometria Euclidiana. De acordo com Mol (2013), Hilbert propôs uma construção partindo de três elementos

- o ponto, a reta e o plano - e de relações entre esses elementos. Essas relações foram feitas através de 21 axiomas, divididos em cinco grupos:

- Axiomas de Conexão
- Axiomas de Ordem
- Axiomas de Congruência
- Axiomas de Continuidade
- Axioma das Paralelas

Com o trabalho de Hilbert, foi dada uma precisão lógica à Geometria Euclidiana, provando não haver falhas na geometria proposta por Euclides. Hoje, no ensino da Geometria, é utilizado esse método axiomático, como no livro de João Lucas Marques Barbosa, *Geometria Euclidiana Plana* (BARBOSA, 2012), no qual o método axiomático de A. V. Pogorelov leva o estudante, de forma precisa e rápida, aos teoremas mais importantes da Geometria Euclidiana.

1.2.3 Sequência didática

O ensino da Geometria sempre foi considerado um trabalho difícil em sala de aula. Muitas pessoas não tiveram a oportunidade de inserir no seu currículo educacional os conhecimentos geométricos devido a diversos fatores, como os livros didáticos, que antigamente traziam os conteúdos de Geometria nos últimos capítulos, o extenso currículo escolar para ser cumprido e a falta de motivação e preparação por parte de muitos professores. Algumas dessas situações perduram até hoje em muitas escolas. Assim, analisando as etapas do processo ensino-aprendizagem, precisamos utilizar atividades que favoreçam esse processo.

Sobre os modelos das aulas de matemática os PCNs relatam:

> Tradicionalmente, a prática mais frequente no ensino da Matemática tem sido aquela que o professor apresenta o conteúdo

> oralmente, partindo de definições, exemplos, demonstração de propriedades, seguidos de exercícios de aprendizagem, fixação e aplicação, e pressupõe que o aluno aprenda pela reprodução (BRASIL, 1998, p. 37).

Mas os PCNs também ressaltam que essa prática não tem sido eficaz, a reprodução correta não representa a apreensão do conteúdo e sua utilização em outros contextos.

Com esse mesmo pensamento, a BNCC ressalta que

> Os processos matemáticos de resolução de problemas, de investigação, de desenvolvimento de projetos e da modelagem podem ser citados como formas privilegiadas da atividade matemática, motivo pelo qual são, ao mesmo tempo, objeto e estratégia para a aprendizagem ao longo de todo o Ensino Fundamental (BRASIL, 2018, p. 266).

A BNCC também traz o seguinte direcionamento a respeito da Geometria no Ensino Fundamental: que as ideias matemáticas fundamentais associadas a essa temática são, principalmente, **construção, representação e interdependência** (BRASIL, 2018, p. 271, grifo nosso).

Com os direcionamentos dos PCNs e da BNCC, podemos ver que o planejamento do professor deve ser um processo de reflexão para uma abordagem adequada dos conteúdos em cada turma de alunos, observando seus conhecimentos prévios e suas necessidades, a fim de atingir o objetivo - a aprendizagem. Zabala usa o termo *Sequências Didáticas* "como sendo um conjunto de atividades ordenadas, estruturadas e articuladas para a realização de certos objetivos educacionais, que têm um princípio e um fim conhecidos tanto pelos professores como pelos alunos" (1998, p. 18).

Como afirma Cabral (2017, p. 33), é justamente o Planejamento, a Aplicação e a Avaliação que formam a tríade sugerida por Zabala (1998), na qual o professor identifica a dimensão de ensinar e aprender Matemática.

Schneuwly define Sequência Didática como:

> A unidade de trabalho escolar, constituída por um conjunto de atividades que apresentam um número limitado e preciso de objetivos e que são organizadas no quadro de um projeto de apropriação de dimensões constitutivas de um gênero de texto, com o objetivo de estruturar as atividades particulares em uma atividade englobante, de tal forma que essas atividades tenham um sentido para os aprendizes (SCHNEUWLY, 1991 apud MACHADO, 2000, p. 7).

Assim, para Dolz, "a elaboração da Sequência Didática deve ser precedida de uma espécie de estudo de gênero a ser ensinado" (2004 apud CABRAL, 2017, p. 34). Tomaremos então a Sequência Didática como um conjunto de atividades articuladas, executadas por etapas, que visam uma aprendizagem mais significativa.

1.2.4 Metodologia - material e métodos

Nesta seção, apresentaremos a Sequência Didática que foi construída com o intuito de auxiliar os alunos do Reforço Escolar. O tema foi escolhido pela necessidade de revisão dos conteúdos de Geometria no 2º Semestre Letivo da escola onde foi realizada a pesquisa.

Para montagem da Oficina, levamos em consideração as palavras de Dolz, acima, a respeito da elaboração da sequência didática. Primeiramente foi realizado um Pré-Teste com as duas turmas pesquisadas. Após os resultados do Pré-Teste, foi feita a montagem da Oficina para os alunos do Reforço Escolar, com atividades que envolvessem a construção, medição e análise de Perímetro e Área das Figuras Planas, utilizando material de baixo custo e/ou recicláveis que pudessem servir como objeto manipulável para os alunos e, buscando com essas atividades, fortalecer o processo ensino-aprendizagem e a investigação e resolução de problemas, como ressalta a citação da BNCC vista na seção anterior.

A Sequência Didática foi desenvolvida numa escola pública municipal na cidade de Bonito - PE, com duas turmas do 9º ano, num total de 66

(sessenta e seis) alunos. Nessa escola, os alunos que se encontram com baixo rendimento escolar são encaminhados para o Reforço Escolar. Dessas duas turmas, foram encaminhados 25 (vinte e cinco) alunos. Essas aulas aconteceram duas vezes por semana (terça-feira e quinta-feira) com duração de 1 (uma) hora de aula cada dia. A oficina foi realizada apenas para os alunos que participaram do Reforço Escolar, nos dias 17, 19, 24 e 26 de Setembro e 01, 03, 08 e 10 de Outubro de 2019.

Apresentaremos ainda a Aplicação da Sequência Didática, os desafios surgidos durante as Oficinas e o encaminhamento dado buscando uma aprendizagem efetiva.

1.2.4.1 Montagem da sequência didática

- **TEMA:** Perímetro e Área das Figuras Planas.
- **PÚBLICO ALVO:** Alunos do 9º ano do Ensino Fundamental.
- **DURAÇÃO:** 12 (doze) horas/aulas
- **DISCIPLINA:** Matemática - unidade temática: GEOMETRIA.
- **OBJETIVO GERAL:** Apresentar uma situação didática em forma de Oficinas, com medições de perímetro e área, além da utilização de fórmulas para comprovação das medições.
- **OBJETIVOS ESPECÍFICOS:**

    1. Identificar o nível dos alunos sobre o assunto de Perímetro e Área das Figuras Planas através de um Pré-Teste (Anexo 1).
    2. Vivenciar as atividades da Oficina:
        - Construção das figuras planas com cartolina guache (colorida), papelão ou E.V.A. para medição do perímetro e da área dessas figuras;
        - Medição das dimensões (largura, comprimento, lados e diâmetro) das figuras planas construídas e preenchimento da Tabela 1;

- Medição do perímetro (contorno) das figuras planas construídas utilizando barbante e régua, na qual os alunos irão fazer o contorno da figura com o barbante e depois medir o comprimento do barbante utilizado. Esses dados serão preenchidos na Tabela 2;
- Analisar o perímetro encontrado pelas medições da Tabela 2, com o cálculo feito no caderno do Perímetro das mesmas figuras com as dimensões da Tabela 1;
- Calcular a razão entre o comprimento da circunferência e o diâmetro do círculo, buscando que os alunos percebam que essa razão se aproxima do valor de $3,14$ (π);
- Construir, no Geoplano tradicional, figuras planas com área específica e perímetro determinado;
- Construir, no Geoplano Circular, um círculo com o objetivo de identificar seus elementos e calcular seu perímetro.

3. Identificar o nível dos alunos após a aplicação das atividades da Oficina através de um Pós-Teste.
4. Comparar os resultados obtidos no Pós-Teste dos alunos que participaram da Oficina e alunos que não participaram.

- **DESENVOLVIMENTO:**

1º Momento: Aplicação do Pré-Teste com todos os alunos das duas turmas pesquisadas.

2º Momento: Início da Oficina com os alunos do Reforço Escolar, a partir de uma explanação sobre os conteúdos de Perímetro e Área de Figuras Planas. Após a explanação, os alunos deverão construir, com cartolina guache, papelão ou E.V.A., as figuras planas pedidas, observando as características de cada figura. Nesse momento, os alunos deverão anotar as dimensões de cada figura na Tabela 1.

3º Momento: Medição do contorno das figuras com barbante e régua e anotação na Tabela 2.

Tabela 1.1: Medidas das Figuras Planas

Figuras	*Largura*	*Comprimento*
QUADRADO 1		
QUADRADO 2		
RETÂNGULO 1		
RETÂNGULO 2		
PARALELOGRAMO 1		
PARALELOGRAMO 2		
TRAPÉZIO 1		
TRAPÉZIO 2		
TRIÂNGULO 1	Lados:	
TRIÂNGULO 2	Lados:	
CÍRCULO 1	Diâmetro:	
CÍRCULO 2	Diâmetro:	

Fonte: Produzido pela autora

4º Momento: Cálculo do perímetro das figuras construídas com as informações da Tabela 1 e comparação com as medidas do perímetro da Tabela 2. Nesse momento, os alunos também deverão calcular a razão entre o comprimento da circunferência e o diâmetro do círculo, com o objetivo de observarem a aproximação do número $3,14$ (π).

5º Momento: Construção de figuras planas no Geoplano Tradicional com perímetro e área determinados. No Geoplano Circular, construir um círculo, identificar seus elementos (raio, diâmetro e cordas) e calcular o comprimento da circunferência construída.

6º Momento: Aplicação do Pós-Teste (Anexo 2) com os alunos que participarão da pesquisa.

- **RECURSOS:**
  - Cartolinas guaches, papelão e E.V.A., régua, tesoura, compasso, par de esquadros e barbante.
  - Tabelas 1 e 2.
  - Geoplano Tradicional e Geoplano Circular.

Tabela 1.2: Perímetro das Figuras Planas

Figuras	***Perímetro***
QUADRADO 1	
QUADRADO 2	
RETÂNGULO 1	
RETÂNGULO 2	
PARALELOGRAMO 1	
PARALELOGRAMO 2	
TRAPÉZIO 1	
TRAPÉZIO 2	
TRIÂNGULO 1	
TRIÂNGULO 2	
CÍRCULO 1	
CÍRCULO 2	

Fonte: Produzido pela autora

- **AVALIAÇÃO:** A avaliação será de forma contínua, durante todo o processo de execução da Oficina, observando a participação dos alunos em cada atividade proposta. A condensação da avaliação será feita comparando os resultados do Pré-Teste com os resultados do Pós-Teste.

1.2.4.2 Aplicação da sequência didática

1º Momento: Total de 2 (duas) horas/aulas - Aplicação do Pré-Teste (Anexo 1), contendo questões do eixo Geometria aplicadas nas avaliações anteriores do SAEPE. O Pré-Teste foi aplicado com duas turmas do 9º ano da Escola pesquisada, ou seja, os alunos que participaram do Reforço Escolar e os demais alunos das turmas.

APLICAÇÃO DA OFICINA

A aplicação da Oficina foi feita apenas para os alunos do Reforço Escolar durante as aulas de reforço. Durante esse período de aplicação da Oficina, as duas turmas pesquisadas, com os alunos do Reforço Escolar e

os demais, tiveram revisão do Eixo de Geometria pelo professor vigente da disciplina em seu horário normal de aula.

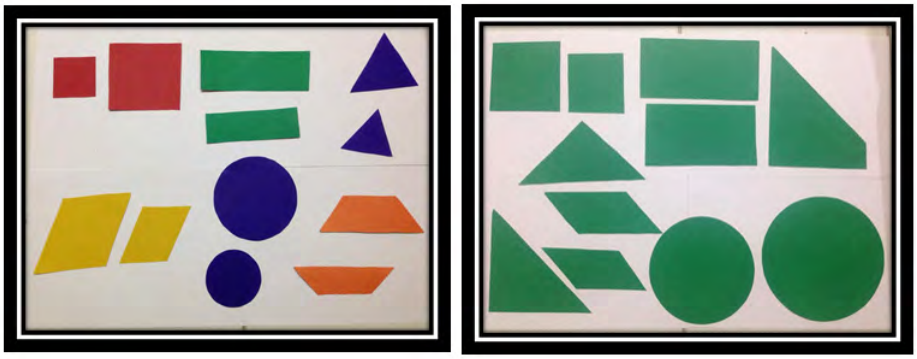
2º Momento: Total de 2 (duas) horas/aulas - Inicialmente fizemos uma introdução sobre os conceitos de Perímetro e Área das Figuras Planas, identificando as características das figuras, conteúdos esses que são revisados no 9º ano do Ensino Fundamental. Com uso de cartolina guache colorida, régua, compasso, lápis e tesoura, os alunos construíram: dois quadrados, dois retângulos, dois paralelogramos, dois trapézios, dois triângulos e dois círculos, com dimensões diferentes.
As construções foram feitas utilizando a sala da Biblioteca da Escola, por ser um espaço maior que as salas de aula, com mesas que comportam até 4 (quatro) alunos. Após construídas as figuras, os alunos anotaram suas dimensões na Tabela 1.

Figura 1.7: Construção das Figuras Planas

Fonte: Produzido pela autora

3º Momento: Total de 2 (duas) horas/aulas - Deveríamos ter passado para a medição do contorno (Perímetro) das figuras construídas, mas, quando fomos organizar as figuras construídas por cada aluno, observamos

Figura 1.8: Figuras construídas pelos alunos



Fonte: Produzido pela autora

que os pretendidos paralelogramos não estavam bem construídos, pois os lados opostos não eram paralelos. Tendo em vista os problemas das figuras, fez-se necessário trabalhar construção de paralelas e construção de ângulos retos. Conversamos com a turma do Reforço e vimos que eles não sabiam trabalhar com o par de esquadros, na verdade, eles nem o conheciam por esse nome, achavam apenas que eram réguas, só que num formato diferente. Dessa forma, reorganizamos a atividade para ensinar como construir perpendiculares (ângulo reto) com uso do par de esquadros e como construir as paralelas (lados paralelos do paralelogramo e do trapézio).

Essa parte da sequência didática não estava prevista, pois acreditávamos que os alunos dominavam o uso de instrumentos como a régua, compasso, esquadros e transferidor. Fizemos uma explanação oral, seguida de exemplos, sobre o uso do par de esquadros para a construção de perpendiculares (ângulos retos) e retas paralelas. Os alunos fizeram então, a nova construção das figuras que não estavam com as medidas angulares corretas.

Esse momento foi realizado na própria sala de aula e não na Biblioteca, como fizemos no 2º Momento, pois precisávamos do quadro branco para fazer as construções junto com os alunos.

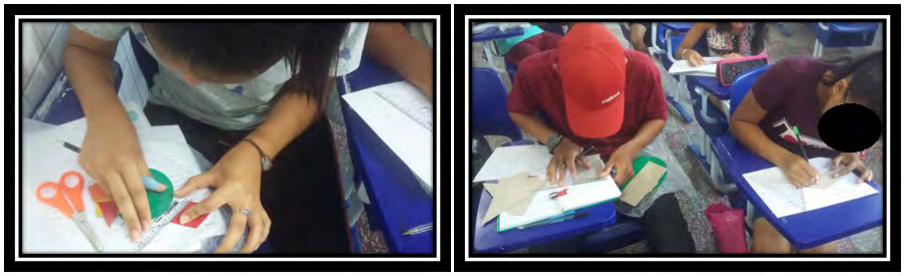
Figura 1.9: Construção de Perpendiculares e Paralelas com par de esquadros

Fonte: Produzido pela autora

4º Momento: Total de 2 (duas) horas/aulas - Começamos fazendo uma explanação de como os alunos deveriam fazer a medição do contorno das figuras, utilizando o barbante e a régua. Eles deveriam contornar a figura construída com o barbante e depois medir, com a régua, o comprimento que fora utilizado. Os alunos fizeram a medição do contorno e perímetro das figuras construídas com certa dificuldade. Devido à espessura da cartolina guache (sugerimos utilizar papelão, papel panamá ou E.V.A. com espessura mínima de 3 milímetros), fazer o contorno com o barbante torna-se um pouco mais trabalhoso. Após a medição dos contornos e preenchimento da Tabela 2, os alunos calcularam o Perímetro dessas figuras com as dimensões anotadas na Tabela 1. Momento esse de muitas discussões, porque as construções não ficaram perfeitas, logo, houve pequenas divergências entre os valores obtidos no cálculo do perímetro e as medições do contorno anotadas na Tabela 2. Como desafio, colocamos o cálculo da razão entre o comprimento da circunferência e o diâmetro da mesma.

Alguns alunos puderam observar que os valores dessa razão estavam próximos de $3,14$ e que esse valor é o que utilizamos como aproximação para π (pi).

Figura 1.10: Medição do Contorno das figuras construídas



Fonte: Produzido pela autora

5º Momento: Total de 2 (duas) horas/aulas - As atividades com Geoplano foram divididas em duas etapas: a primeira, com o Geoplano Tradicional (figuras poligonais); a segunda, com o Geoplano Circular (círculo).

Na primeira etapa, os alunos construíram figuras planas no Geoplano. Primeiro, fizemos uma explanação oral sobre o Geoplano, o que significa a unidade de área utilizada no mesmo e como os alunos deveriam contar as unidades de área.

No geoplano tradicional, foi solicitado aos alunos que construíssem figuras planas, com as seguintes características:

1 - Construir uma figura com perímetro de 10 unidades;
2 - Construir uma figura com 8 unidades de área;
3 - Construir um triângulo isósceles;
4 - Construir um triângulo com 10 unidades de área;
5 - Construir um retângulo com 14 unidades de área;
6 - Construir um quadrado com 25 unidades de área.

Figura 1.11: Medição do Contorno das figuras construídas

Fonte: Produzido pela autora

Na segunda etapa, utilizamos o Geoplano Circular. Foi solicitado aos alunos as seguintes ações:

1 - Construir uma circunferência de raio qualquer;

2 - Marcar o raio da circunferência com um lápis de cor e identificá-lo como segmento de reta;

3 - Desenhar duas cordas nessa circunferência, diferenciando-as por cores e identificando-as como segmento de reta;

4 - Marcar o diâmetro, identificá-lo como segmento de reta. Nessa etapa, o objetivo era que os alunos observassem que o diâmetro é a maior corda da circunferência;

5 - Calcular o comprimento dessa circunferência usando a equação $C = 2\pi r$.

Figura 1.12: Atividades com Geoplano Tradicional

Fonte: Produzido pela autora

6º Momento: Total de 2 (duas) horas/aulas - Finalizamos a Sequência Didática, aplicando o Pós-Teste. A aplicação foi feita com as duas turmas pesquisadas, ou seja, com os alunos que participaram da Oficina durante o Reforço Escolar e os demais alunos das turmas.

1.3 Considerações finais

Nessa seção, faremos uma Análise do Pré-Teste, evidenciando em quais questões e seus respectivos temas e/ou conteúdos os alunos obtiveram menor e maior índice de acertos. Faremos também uma comparação entre os alunos que participaram do Reforço Escolar e os demais.

Da mesma forma, em seguida, faremos uma Análise do Pós-Teste, evidenciando também as questões com menor e maior índice de acertos e, com isso, realizaremos uma comparação do antes e depois da Oficina aplicada. Uma análise mais detalhada desses resultados pode ser encontrada na dissertação *Uma proposta didática para o Ensino de Perímetro e Área no Ensino Fundamental II* (ARAUJO, 2020).

Figura 1.13: Atividades com Geoplano Circular

Fonte: Produzido pela autora

1.3.1 Análise pré-teste

A Aplicação do Pré-Teste (Anexo 1) foi dada com 66 (sessenta e seis) alunos que compõem as duas turmas avaliadas. O resultado consta na tabela 3 a seguir.

Observando os dados coletados no Pré-Teste, podemos verificar que as questões 2 e 3 foram as que os alunos tiveram maior percentual de acertos com 84,80% e 98,50%, vemos também que essas questões foram organizadas utilizando Malha Quadriculada. Entretanto a questão 4 também envolve Malha Quadriculada, mas, como trata de comprimento de circunferência, o resultado não foi o esperado em comparação às questões anteriores. Já as questões 5 e 7, que envolvem cálculo do Comprimento da Circunferência, foram as que tiveram um percentual mais baixo de acerto, de 4,50% e

Tabela 1.3: Resultados do Pré-Teste

Questão	*Quantidade de Acertos*	*Percentuais de Acertos (%)*	*Temas das questões*
01	20	30,30	Corda e diâmetro de circunferência
02	56	84,80	Perímetro de região em malha quadriculada
03	65	98,50	Área de região na malha quadriculada
04	31	46,90	Área de região na malha quadriculada, com circunferência
05	03	4,50	Perímetro de região, envolvendo circunferência
06	16	24,24	Área de anel circular
07	02	3,00	Comprimento de circunferência
08	08	12,10	Comprimento de circunferência
09	37	56,10	Área de retângulo
10	29	43,90	Composição e decomposição de figura, cálculo de perímetro

Fonte: Produzido pela autora

3,00%, respectivamente.

Separando os resultados do Pré-Teste entre os alunos que participavam do Reforço Escolar e os demais alunos participantes da turma, obtivemos o seguinte gráfico:

Figura 1.14: Resultados do Pré-Teste

Fonte: Produzido pela autora

Podemos ver que os alunos que foram encaminhados para o Reforço Escolar estavam com percentual de acertos abaixo dos demais alunos que compõem as turmas pesquisadas, demonstrando que também nos conteúdos de Perímetro e Área das Figuras Planas eles possuíam dificuldades.

1.3.2 Análise pós-teste

O Pós-Teste (Anexo 2) em sua elaboração constava de 10 (dez) questões, envolvendo apenas os temas em que os alunos tiveram dificuldade no Pré-Teste, pois vimos que eles dominavam os conteúdos de Perímetro e Área de Figuras Planas com malha quadriculada e Área de Retângulo e Região Poligonal, mas, quando levamos o Pós-Teste para apreciação do professor vigente de Matemática das turmas pesquisadas, ele salientou que algumas questões utilizavam cálculos com números irracionais e as turmas não possuíam domínio desses conteúdos. Achamos sensato retirar essas questões com o objetivo de que o Pós-Teste avaliasse os conteúdos trabalhados nas revisões do professor em sala de aula e na sequência didática aplicada no Reforço Escolar.

No dia da aplicação do Pós-Teste tivemos um total de 08 (oito) alunos faltosos: 02 (dois) alunos do Reforço Escolar e 06 (seis) alunos dos demais que compõem as turmas pesquisadas.

Os dados do Pós-Teste foram coletados e condensados, como mostra a tabela 4 a seguir, evidenciando o percentual de acerto por questão.

Tabela 1.4: Resultados do Pós-Teste

Questão	***Quantidade de Acertos***	***Percentuais de Acertos (%)***	***Temas das questões***
01	31	53,45	Comprimento de circunferência
02	50	86,20	Raio de circunferência
03	40	68,96	Corda, raio e diâmetro de circunferência
04	52	89,65	Comprimento de circunferência
05	56	96,55	Corda, raio e diâmetro de circunferência
06	20	34,48	Perímetro de uma região, envolvendo circunferência
07	13	22,41	Área de circunferência

Fonte: Produzido pela autora

Podemos observar esses resultados para uma melhor comparação no gráfico a seguir:

Figura 1.15: Comparação dos Resultados do Pós-Teste

Fonte: Produzido pela autora

Comparando os resultados dos alunos que participaram da Sequência Didática, que tiveram em média 72,05% de acerto, com os resultados dos demais alunos que participaram apenas das revisões feitas pelo professor vigente de Matemática, que tiveram em média 59,59% de acerto, podemos ver que os alunos que participaram da Sequência Didática tiveram um melhor resultado, com cerca de 20% acima do percentual dos demais alunos, ressaltando que os alunos que fazem o Reforço Escolar estavam com baixo rendimento escolar.

1.3.3 Conclusão

A busca por novas ações pedagógicas visando facilitar o processo ensino-aprendizagem tem sido o anseio de muitos professores de Matemática. As diferenças entre os níveis de conhecimento de alunos de uma mesma turma pode ser também um fator que traz dificuldade ao processo.

O desenvolvimento da Sequência Didática proposta neste trabalho, realizada com alunos do Reforço Escolar (baixo rendimento escolar), demonstrou que ações pedagógicas que envolvam construção e manipulação

de figuras planas podem contribuir para uma aprendizagem significativa, reiterando o que Kamii e Declarck ressaltam sobre o conhecimento matemático, "conhecimento físico é aquele que existe na realidade externa que as pessoas veem e é diferente do conhecimento matemático: este consiste nas relações que o indivíduo constrói em sua mente"(apud LORENZATO, 2006). A oficina de construção de figuras planas e medição de contornos trouxe aos alunos habilidades e competências para estabelecer relações entre as fórmulas matemáticas e o significado dos objetos matemáticos (figuras). Baseando-se nessa argumentação, os alunos puderam resolver problemas sem utilização de fórmulas. Com as atividades com os Geoplanos, os alunos puderam verificar relações entre perímetro e área de figuras planas e os elementos de uma circunferência. Podemos observar também a segurança dos alunos ao fazerem as atividades durante a Oficina, demonstrando a apropriação dos significados de cada objeto matemático (figuras) e suas características.

Quanto à comparação entre o resultado do Pré-Teste e do Pós-Teste dos alunos do Reforço Escolar (baixo rendimento escolar), podemos verificar um desenvolvimento qualitativo e quantitativo muito expressivo, ficando com um percentual de acertos 20% superior ao resultado dos demais alunos no Pós-Teste.

Dessa forma, respeitar a individualidade de cada aluno passa a ser uma necessidade no processo ensino-aprendizagem, no qual as dificuldades que cada aluno possui em Matemática podem ser vistas como um norteador para a prática educativa do professor.

Os resultados desse trabalho nos trouxe encorajamento para inserir novas sequências didáticas com construção e manipulação de objetos nas aulas de Matemática, bem como, pensando no futuro, organizar um Laboratório de atividades de Geometria para serem vivenciadas na Escola pesquisada em todas as séries/anos do Ensino Fundamental II. Esperamos também que ele possa auxiliar professores do Ensino Fundamental na escolha de Sequências Didáticas para o ensino de Perímetro e Área de Figuras Planas.

1.4 Referências bibliográficas

A HISTÓRIA da geometria euclidiana do antigo Egito às salas de aula. **GLOBO**, 2011. Disponível em: <http://redeglobo.globo.com/globociencia/noticia /2011/12/historia-da-geometria-euclidiana-do-antigo-egito-salas-de-aula.html>. Acesso em 05 de nov. de 2019.

ARAUJO, D. **Uma proposta didática para o Ensino de Perímetro e Área no Ensino Fundamental II**. 2020. Dissertação (Mestrado) - Universidade Federal Rural de Pernambuco, Programa de Mestrado Profissional em Matemática (PROFMAT), Recife, PE.

ÁVILA, G. Legendre e o Postulado das Paralelas. **Revista do Professor de Matemática**, São Paulo, no. 22, p. 16-28, 1992.

BARBOSA, J. L. M. **Geometria euclidiana plana**. Rio de Janeiro: Sociedade Brasileira de Matemática, 2012.

BICUDO, I. et al. **Os elementos.** São Paulo: Unesp, 2009.

BOYER, C. B. **História da matemática.** Tradução de Elza F. Gomide. São Paulo: Blucher, 1974.

BRASIL. **Parâmetros Curriculares Nacionais: Matemática.** Brasília: MEC, 1998.

BRASIL. **Base Nacional Comum Curricular.** Brasília: Ministério de Educação, 2018. Disponível em: <http://basenacionalcomum.mec.gov.br/wpcontent/uploads/2018/12/BNCC_19dez2018_site.pdf>. Acesso em: 08 fev. de 2019.

CABRAL, N. F.. **Sequências didáticas: estrutura e elaboração**. Belém: SBEM/SBEM-PA, 2017.

DOLZ, J. et al. **Sequências didáticas para o oral e a escrita**: apresentação de um procedimento. Gêneros orais e escritos na escola. Campinas: Mercado de Letras, 2004.

INEP. **Programa Internacional de Avaliação de Estudantes (PISA)**. 2019. Disponível em: <http://portal.inep.gov.br/pisa>. Acesso em 07 de dez. de 2019.

KAMII, C.; DECLARCK, G. **Reinventando a aritmética: implicações**

da teoria de Piaget. Campinas: Papirus, 1986.

LORENZATO, S. **Para aprender matemática,** Campinas: Autores Associados, 2006.

MACHADO, A. R. Uma experiência de assessoria docente e de elaboração de material didático para o ensino de produção de textos na universidade. **DELTA: Documentação e Estudos em Linguística Teórica e Aplicada**, São Paulo vol. 16, no. 1, SciELO Brasil, 2000.

MIORIM, M. Â. **O ensino de matemática: evolução e Modernização.** 1995. Tese (doutorado) - Universidade Estadual de Campinas, Faculdade de Educação, Campinas, SP.

MOL, R. S. **Introdução à História da Matemática.** Belo Horizonte: Editora CAED-UFMG, 2013.

MORENO, A. C.; OLIVEIRA, E. Brasil cai em ranking mundial de educação em matemática e ciências; e fica estagnado em leitura. **G1**, 2019. Disponível em: <https://glo.bo/2SoXcO8>. Acesso em 07 de dez. de 2019.

ROQUE, T.; DE CARVALHO, J. B.. **Tópicos de história da matemática.** Rio de Janeiro: Sociedade Brasileira de Matemática, 2012.

SCHNEUWLY, B. Diversification et progression en DFLM: l'apport des typologies. **Etudes de linguistique appliquée**, Paris, no. 83, p. 131-141, 1991.

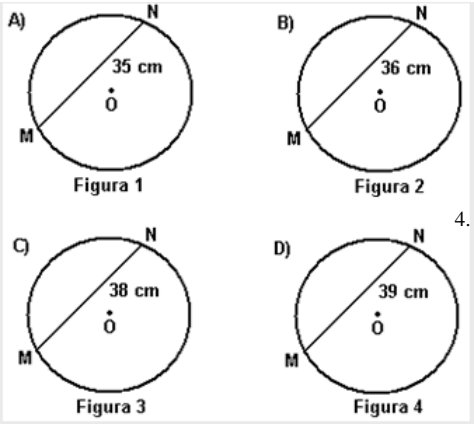
TANEBAUM, A. S. **Sistemas Operacionais Modernos**. ed. 3. Hoboken: Pearlson Prentice Hall, 2010.

ZABALA, A., R. **A prática Educativa: como ensinar**. Tradução de Ernani F. da F. Porto Alegre: Artmed, 1998.

1.4.1 Anexo 1 pré-teste

Dados de Identificação	
Disciplina:	Matemática
Professor:	
Aluno(a):	

1. (Oficina de Itens/2010) Nas figuras abaixo, estão desenhadas quatro circunferências, todas com o raio medindo 18 cm. A figura que indica a medida correta da corda $\overline{MN}$ é:



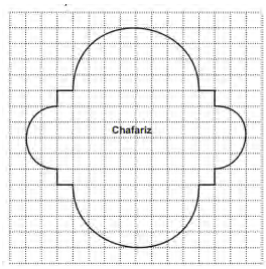
2. (Oficina de Itens/2010) Ana desenhou o modelo de seu bordado na malha quadriculada abaixo. Cada quadradinho dessa malha tem 1 cm de lado.

Quanto mede o contorno da figura desenhada por Ana?
a) ( ) $9cm$
b) ( ) $11cm$
c) ( ) $15cm$
d) ( ) $16cm$

3. (Oficina de Itens/2010) Veja a figura cinza desenhada na malha quadriculada abaixo. A medida da área de cada quadradinho da malha é igual a $1cm^2$.

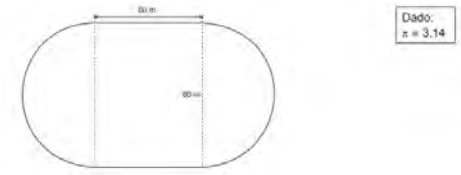
Qual é a medida da área dessa figura cinza?
a)( ) $19cm^2$
b)( ) $20cm^2$
c)( ) $28cm^2$
d)( ) $49cm^2$

4. (SAEPE/2016) Na praça principal de uma cidade tem um chafariz cujo formato está representado na malha quadriculada abaixo, em que o lado de cada quadradinho equivale a 2 metros. Em uma reforma, os azulejos que revestem o fundo do tanque desse chafariz foram trocados por novos.



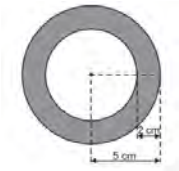
Quantos metros quadrados de azulejos, no mínimo, foram utilizados para cobrir todo o fundo desse chafariz?
a) ( ) $20(\pi+3)$
b) ( ) $20(4\pi+3)$
c) ( ) $24(\pi+10)$
d) ( ) $80(\pi+3)$
e) ( ) $80(4\pi+3)$

5. (SAEPE/2016) Em um shopping foi inaugurada uma pista de corrida cujo formato é a justaposição de duas semicircunferências e um retângulo com as medidas indicadas no desenho abaixo. Para proteção, existe uma mureta em todo o contorno dessa pista.



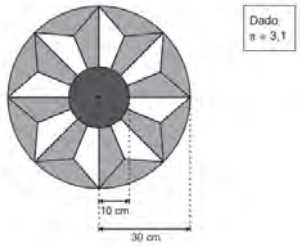
Qual é a extensão dessa mureta de proteção?
a) ( ) $251,20m$
b) ( ) $371,20m$
c) ( ) $622,40m$
d) ( ) $4800m$
e) ( ) $5144m$

6. (SAEPE/2016) O desenho abaixo é formado por dois círculos concêntricos.



Qual é a medida da área da parte colorida de cinza?
a) ( ) $34\pi cm^2$
b) ( ) $25\pi cm^2$
c) ( ) $21\pi cm^2$
d) ( ) $16\pi cm^2$
e) ( ) $13\pi cm^2$

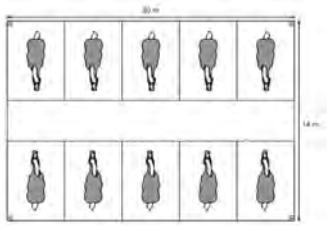
7. (SAEPE/2016) Uma artesã construiu uma mandala em formato circular e contornou o maior círculo com fita. Os raios dos círculos da mandala encontram-se representados no desenho abaixo.



Qual foi a quantidade mínima, aproximada, de fita utilizada pela artesã para confeccionar essa mandala?
a) ( ) $60cm$
b) ( ) $93cm$
c) ( ) $124cm$
d) ( ) $186cm$
e) ( ) $248cm$

8. (SAEPE/2016) Lucas é atleta e, como treinamento, dá diariamente 6 voltas completas em uma pista circular de raio 50 m. A distância aproximada, em metros, percorrida diariamente por Lucas nessa pista é: (Use: $\pi \cong 3,14$)
a) ( ) 15700
b) ( ) 7850
c) ( ) 1884
d) ( ) 314
e) ( ) 300

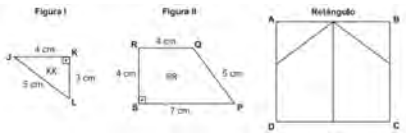
9. Observe, no desenho abaixo, o esquema de um estábulo que foi construído para acomodar dez cavalos.



Qual é a medida da área ocupada por esse estábulo?
a) ( ) $960m^2$
b) ( ) $280m^2$

c) ( ) $140m^2$
d) ( ) $68m^2$
e) ( ) $34m^2$

10. Marcos usou dois triângulos e dois trapézios idênticos aos das figuras I e II para construir o retângulo *ABCD*, conforme o desenho abaixo.



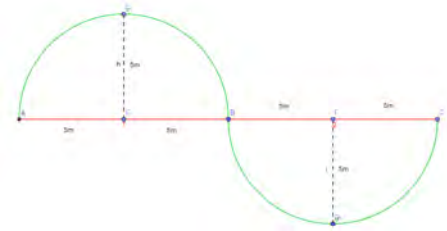
Qual é a medida do perímetro do retângulo *ABCD* construído por Marcos?
a) ( ) $30cm$
b) ( ) $32cm$
c) ( ) $44cm$
d) ( ) $47cm$
e) ( ) $56cm$

"A Geometria faz com que possamos adquirir o hábito de raciocinar, e esse hábito pode ser empregado, então, na pesquisa da verdade e ajudar-nos na vida"
(Jacques Bernoulli)

1.4.2 Anexo 2 pós-teste

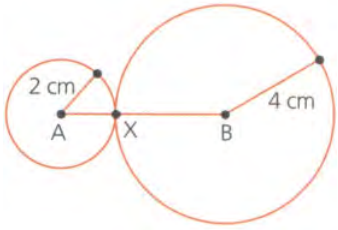
Dados de Identificação	
Disciplina:	Matemática
Professor:	
Aluno(a):	

1. (PROJETO TELÁRIS, 9º ano - Adaptada) Maria deseja ir do ponto A a C, quanto ela percorreria a mais pegando o caminho verde ao invés do caminho vermelho? Use $\pi \cong 3,1$



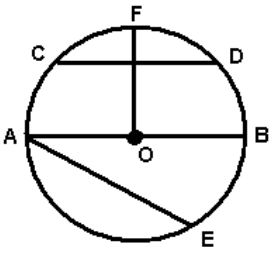
a) ( ) $3,1m$
b) ( ) $13,1m$
c) ( ) $11m$
d) ( ) $10m$

2. (TICs na Matemática) Na figura, as circunferências de centro A e B tocam-se no ponto X.



A distância *AB* é:
a) ( ) maior que 6 cm
b) ( ) 6 cm
c) ( ) 5 cm
d) ( ) menor que 5 cm

3. (TICs na Matemática) Na circunferência abaixo, de centro O, os segmentos $\overline{CD}$, $\overline{OF}$ e $\overline{AB}$ são, nessa ordem:

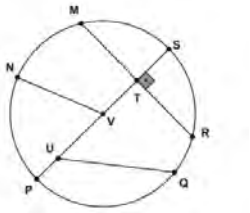


a) ( ) corda, raio e diâmetro
b) ( ) diâmetro, raio e corda
c) ( ) raio, corda e diâmetro
d) ( ) corda, diâmetro e raio

4. (TICs na Matemática) Uma pessoa pretende colocar meio fio em torno de uma praça circular de raio 20m. Sabendo que o contorno da praça pode ser calculado pela seguinte expressão: $C = 2$, onde R é o raio e considere $\pi \cong 3$.

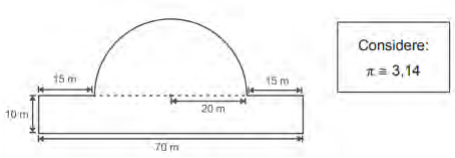
A medida do contorno da praça é:
a) ( ) $50m$
b) ( ) $100m$
c) ( ) $40m$
d) ( ) $120m$

5. (SAEPE - Pacto pela Educação - Adaptada) Sendo V o centro da circunferência, observe os segmentos destacados abaixo:



Qual desses segmentos corresponde ao diâmetro dessa circunferência?
a) ( ) $\overline{VN}$
b) ( ) $\overline{TS}$
c) ( ) $\overline{RM}$
d) ( ) $\overline{QU}$
e) ( ) $\overline{PS}$

6. (SAEPE - Pacto pela Educação) Letícia costuma caminhar em volta de uma praça formada por uma região retangular e um semicírculo. O contorno dessa praça está representado no desenho abaixo.



Qual é a distância aproximada que Letícia percorre ao dar uma volta completa ao redor dessa praça?
a) ( ) $748m$
b) ( ) $245,6m$
c) ( ) $182,8m$
d) ( ) $160m$
e) ( ) $151,4m$

7. (SAEPE - Pacto pela Educação - Adaptada) Na casa de Luana, havia um jardim de formato circular com 12 m de diâmetro. Para cortar custos, a área desse jardim foi reduzida à quarta parte, mantendo o mesmo formato circular. Qual é a medida do *novo diâmetro* do jardim após essa redução?
(Considere: $\pi \cong 3$)
a)()6 m
b)()9 m
c)()12 m
d)()24 m
e)()48 m

Desejo uma boa atividade a todos!

Capítulo 2

Função ϕ de Euler e o princípio da inclusão e exclusão

Eldaline Rocha da Silva [1]
Rodrigo Genuino Clemente [2]

Resumo: O presente trabalho tem como propósito fazer um estudo sobre a função ϕ de Euler, que foi desenvolvida pelo matemático e físico suíço Leonhard Euler para apresentar uma generalização do Pequeno Teorema de Fermat (HEFEZ, 2011) e que mais tarde se mostrou uma importante ferramenta no desenvolvimento da Teoria dos Números. Veremos conceitos, propriedades, teoremas, demonstrações e alguns resultados importantes. Além disso, forneceremos alguns exemplos que ajudam a compreender as ideias utilizadas nas demonstrações e traremos alguns problemas não resolvidos envolvendo esta função. Para este estudo, é necessário apenas a compreensão de conteúdos vistos na educação básica, isto inclui as propriedades dos inteiros positivos relacionados com a primalidade, a divisibilidade e as operações elementares. Também apresentaremos a função de Euler interligada ao Princípio da Inclusão e Exclusão, conteúdo abordado no ensino médio.

Palavras-chave: Função Totiente de Euler; teoria dos números.

[1]UFRPE - Universidade Federal Rural de Pernambuco, eldaline_rocha@hotmail.com
[2]UFRPE - Universidade Federal Rural de Pernambuco, rodrigo.clemente@ufrpe.br

2.1 Introdução

Neste trabalho, veremos conceitos, propriedades, teoremas e alguns resultados importantes da Função ϕ de Euler, também chamada por função Totiente, usada por Leonhard Euler para provar o Pequeno Teorema de Fermat. Esta função associa a cada inteiro positivo n a quantidade de inteiros positivos menores do que n que são coprimos com n e é denotada por $\phi(n)$.

Uma outra aplicação da função ϕ é na descoberta da ordem do grupo multiplicativo de inteiros módulo n. Temos que ϕ é a cardinalidade do grupo de unidades do anel $\mathbb{Z}/n\mathbb{Z}$. Essa função também possui uma aplicação moderna em criptografia e desempenhou um papel fundamental na definição do sistema de criptografia do método RSA criado em 1977 por R. Rivest, A. Shamire e L. Adleman.

Para a compreensão deste artigo, é necessário ter o conhecimento de alguns temas referentes ao ensino básico, como, por exemplo, números primos, divisores de um número natural e operações elementares (adição, subtração, multiplicação e divisão) que são abordados desde o inicio do ensino fundamental.

Algumas definições e exemplos que serão apresentados são de fácil entendimento, possibilitando assim que o professor possa trabalhar conteúdos de nível superior com alunos da educação básica. Além disso, apresentaremos a função de Euler interligando-a com o Princípio da Inclusão e Exclusão, que é um tema visto no Ensino Médio quando se estuda Teoria dos conjuntos.

Este estudo tem como base a dissertação *Funções elementares e teoria dos números* (SILVA, 2019), que trata de algumas Funções elementares. Algumas demonstrações, mais detalhes e outros exemplos podem ser encontrados nesse trabalho. Esse material também é indicado para aprofundar-se no tema de Funções elementares e teoria dos números.

2.2 Função totiente de Euler

A função Totiente, também chamada de Função ϕ de Euler, é, na teoria dos números, definida para um número inteiro positivo n como sendo igual à quantidade de números inteiros positivos que são relativamente primos com n não excedendo n, que denotaremos por $\phi(n)$.

Foi o matemático suíço Leonhard Euler (1707-1783) que a definiu. Ele foi um dos maiores matemáticos de todos os tempos. Nascido na Suíça, era filho de um pastor protestante que esperava que ele seguisse os passos do pai. Euler possuía facilidade para o aprendizado de línguas e uma enorme habilidade para efetuar contas mentalmente.

Aos 14 anos, já ingressava na Universidade da Basileia, mas foi aos 20 anos que ganhou reconhecimento internacional, quando recebeu uma menção honrosa da Academia de Ciências de Paris. Assumiu a função de físico na nova Academia de São Petersburgo, na Rússia, em 1727, começando assim sua vida profissional. Em 1733, Euler já assumia a cátedra de matemática nesta mesma academia.

Euler produziu resultados matemáticos ao longo de sua vida. Mesmo quando a doença o assolou e ele ficou totalmente cego em 1771, isto não diminuiu a sua produtividade científica. Ele escreveu sobre vários temas como números complexos, teoria das funções, cálculo diferencial e integral, música, teoria dos números, teoria das partições e mecânica, tornando-se, assim, um dos maiores matemáticos de todos os tempos (HEFEZ, 2016).

No entanto, Euler não escolheu nenhum símbolo específico para representar esta função na época. A notação ϕ foi introduzida por Gauss no livro *Disquisitiones Arithmeticae*, publicado pela primeira vez em 1801, mas o uso do parênteses em torno do argumento não foi utilizado, sendo usada a seguinte forma: ϕn.

Foi o matemático James Joseph Sylvester que escolheu o nome Totiente, pois ele tinha o costume de inventar palavras novas para as coisas com as quais tratava. Este matemático fez contribuições nas áreas da teoria matricial, teoria dos invariantes, análise combinatória e teoria dos números.

A seguir, faremos um estudo sobre a função Totiente. Iniciaremos

apresentando a sua definição, para, em seguida, trazermos algumas de suas propriedades e exemplos. Além disso, no decorrer do trabalho, apresentaremos um estudo combinatorial desta função e a relacionaremos com o principio da inclusão e exclusão.

Definição 1. *Seja n um número natural. Definimos a função* $\phi : \mathbb{N} \to \mathbb{N}$ *dada por* $\phi(n) = |\{k \in \mathbb{N} : 1 \leq k \leq n \text{ e } mdc(k,n) = 1\}|$*, na qual* $|A|$ *indica o números de elementos de um conjunto A.*

Abaixo temos o gráfico de $\phi(n)$ para $1 \leq n \leq 1000$. Observe-se que $\phi(1) = 1$, pois o único natural menor ou igual a 1 é ele mesmo e ainda temos $\text{mdc}(1,1) = 1$. Para $n \geq 2$, temos $n = \text{mdc}(n,n) \neq 1$, de onde podemos concluir que $\phi(n) < n$.

Para encontrarmos o valor de $\phi(8)$, observemos o conjunto dos inteiros positivos que são relativamente primos com 8 não excedendo 8.
$\{x \in \mathbb{N} : 1 \leq x \leq 8 \text{ e } \text{mdc}(x,8) = 1\} = \{1,3,5,7\}$. O conjunto possui 4 elementos, assim, concluímos que $\phi(8) = 4$. Agora encontraremos o valor de $\phi(15)$.
Temos $\{x \in \mathbb{N} : 1 \leq x \leq 15 \text{ e } \text{mdc}(x,15) = 1\} = \{1,2,4,7,8,11,13,14\}$. Note que o conjunto possui 8 elementos, portanto $\phi(15) = 8$.

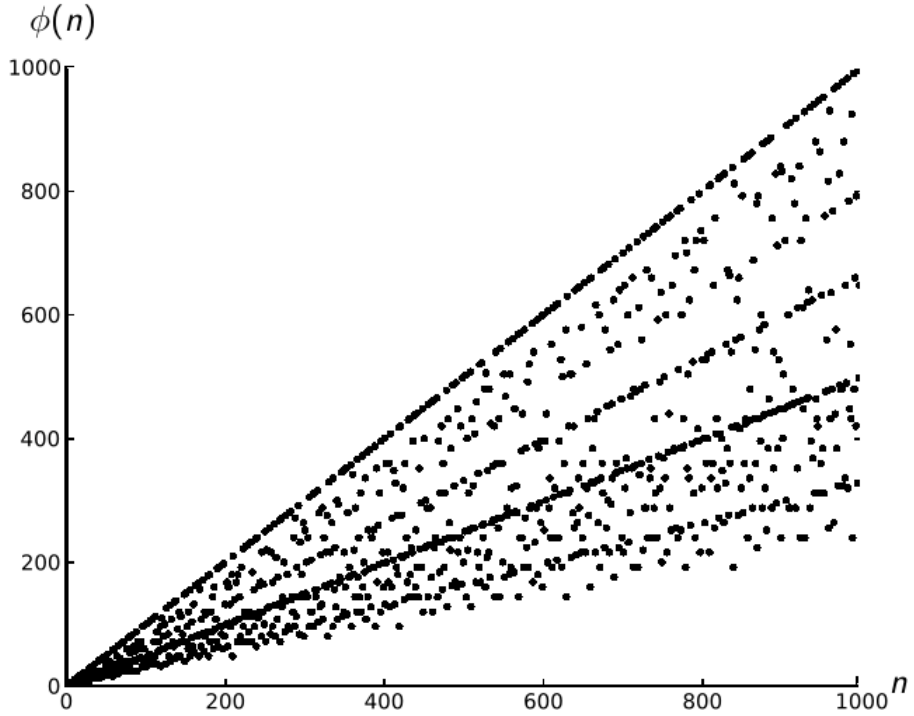
A seguir, temos duas proposições importantes e suas demonstrações.

Proposição 1. *Temos* $\phi(2) = 1$ *e* $\phi(n) \geq 2$*, para todo número natural* $n \geq 3$.

Demonstração. Temos que o único número relativamente primo com 2 e menor que 2 é o 1, logo $\phi(2) = 1$. Para $n \geq 3$ temos $n - 1 \geq 2$, como dois números consecutivos são primos entre si, segue que, para $n \geq 3$, n e $n-1$ são relativamente primos. E como $\text{mdc}(n,1) = 1$, temos 1 e $(n-1)$ coprimos com n. Logo, $\phi(n) \geq 2$ para todo número natural $n \geq 3$, como queríamos. □

Proposição 2. *Seja n um número natural, então* $\phi(n) = n - 1$*, se, e somente se, n é primo.*

Figura 2.1: Gráfico de $\phi(n)$



Fonte: Cruise (2012), editada pelo autor.

Demonstração. Suponha que $\phi(n) = n-1$, então para todo $m < n$ temos $\text{mdc}(n,m) = 1$. Logo, n não pode ser composto por um produto de fatores primos menores que n, ou seja, n é primo. Suponha que n seja primo, então todos os números naturais menores que n são relativamente primos com n, os números naturais menores que n são $1,2,3,...,n-1$, portanto $\phi(n) = n-1$, como queríamos. □

Sabemos que existem alguns tipos de números primos especiais, como, por exemplo, os *primos gêmeos*. Os primos da forma p e $p+2$ são chamados de gêmeos, denominação que foi usada pela primeira vez em 1916 pelo matemático alemão Paul Stäckel (1862 – 1919). Pela proposição anterior, é fácil mostrar que para esses primos teremos $\phi(p+2) = \phi(p)+2$. Considerando $n = p+2$ primo, temos $\phi(p+2) = (p+2)-1 = p+1 = (p-1)+2 = \phi(p)+2$.

Podemos calcular o valor de $\phi(n)$ para um natural n qualquer a partir do fato de que a função ϕ de Euler é multiplicativa, ou seja, $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$ para m e n inteiros positivos com $\text{mdc}(m,n) = 1$.

Veremos agora uma sequência de teoremas e exemplos, a fim de que consigamos calcular o valor de $\phi(n)$ para algum n relativamente grande.

Teorema 1. *Dados m e n inteiros positivos com $mdc(m,n) = 1$, então*

$$\phi(m \cdot n) = \phi(m) \cdot \phi(n).$$

Para ilustrar o método do Teorema 1, sejam $m = 6$ e $n = 5$. Mostraremos que $\phi(5 \cdot 6) = \phi(5) \cdot \phi(6)$. Observemos a tabela abaixo contendo os números de 1 a $5 \cdot 6 = 30$

1	2	3	4	5
6	7	8	9	10
11	12	13	14	15
16	17	18	19	20
21	22	23	24	25
26	27	28	29	30

Para encontrar os inteiros que são primos com 5, devemos observar a coluna k somente se $\text{mdc}(5,k) = 1$, ou seja, observar as colunas dos $\phi(5) = 4$ elementos que são primos com 5, então, consideraremos $k = \{1,2,3,4\}$. Na primeira linha, temos 4 elementos que são primos com 5, logo são 4 colunas para encontrarmos os elementos primos com 6. Como $\text{mdc}(5,6) = 1$, os elementos de cada coluna deixam restos diferentes quando divididos por 6, pois formam um sistema completo de resíduos módulo 6. Suponha que não se forme um sistema completo de resíduos, então pegue dois elementos quaisquer desta coluna, obedecendo a seguinte equação $(6-x) \cdot 5 + k \equiv (6-y) \cdot 5 + k \mod 6 \iff (6-x) \cdot 5 \equiv (6-y) \cdot 5 \mod 6 \iff (6-x) \equiv (6-y) \mod 6 \iff x \equiv y \mod 6$, contradição. Além disso, sabemos que $\text{mdc}(6,x) = \text{mdc}(6,r)$ onde r é o resto da divisão de x por 6, assim, em cada coluna, teremos os elementos perpassando por todos os restos de 6 (Por exemplo, na coluna

$k = 1$ teremos {1,6,11,16,21,26} que correspondem respectivamente aos restos {1,0,5,4,3,2} na divisão por 6). Logo, cada uma dessas colunas tem $\phi(6) = 2$ elementos primos com 6. Na coluna 1, temos $\{1, 11\}$; na coluna 2, {7, 17}; na coluna 3, {13, 23}; e, na coluna 4, {19, 25}. Concluímos, portanto, que $8 = \phi(5 \cdot 6) = \phi(5) \cdot \phi(6) = 4 \cdot 2$.

Uma demonstração do Teorema 1 pode ser encontrada em Silva (2019). Observe que esse Teorema não implica que os números relativamente primos com $m \cdot n$ sejam obtidos como produto dos números relativamente primos com m e os relativamente primos com n. Usemos o exemplo anterior para ilustrar $\phi(30) = \phi(5) \cdot \phi(6)$. Note que os números relativamente primos com 6 são $\{1,5\}$ e os números relativamente primos com 5 são $\{1,2,3,4\}$, enquanto que os números relativamente primos com 30 são $\{1,7,11,13,17,19,23,29\}$. Veja que há números no último conjunto que não são produtos de dois números dos outros dois conjuntos.

corolário 1. *Se m_1, m_2,...,m_r são primos entre si, dois a dois, então*

$$\phi(m_1 \cdot m_2 \cdot ... \cdot m_r) = \phi(m_1) \cdot \phi(m_2) \cdots \phi(m_r).$$

Demonstração. Demonstraremos esse corolário por indução sobre o número r de fatores. Para $r = 1$ temos $\phi(m_1) = \phi(m_1)$. Suponha que seja válido para $r = k$,

$$\phi(m_1 \cdot m_2 \cdot ... \cdot m_k) = \phi(m_1) \cdot \phi(m_2) \cdots \phi(m_k).$$

Mostraremos que é válida para $r = k + 1$. Considere m_1, m_2,...,m_k, m_{k+1} primos entre si, dois a dois. Considere $a = m_1 \cdot m_2 \cdot ... \cdot m_k$. Observe que a e m_{k+1} são primos entre si, pois $\text{mdc}(a, m_{k+1}) = mdc(m_1 \cdot m_2 \cdot ... \cdot m_k, m_{k+1}) = 1$. Como a e m_{k+1} são primos entre si, pelo Teorema 1 temos

$$\begin{aligned}
\phi(m_1 \cdot m_2 \cdot ... \cdot m_k \cdot m_{k+1}) &= \phi(a \cdot m_{k+1}) \\
&= \phi(a) \cdot \phi(m_{k+1}) \\
&= \phi(m_1 \cdot m_2 \cdot ... \cdot m_k) \cdot \phi(m_{k+1}) \\
&= \phi(m_1) \cdot \phi(m_2) \cdot ... \cdot \phi(m_k) \cdot \phi(m_{k+1})
\end{aligned}$$

Assim mostramos que a fórmula é válida para $r = k+1$, logo, por indução finita, é válida para todo número natural r. □

A partir do corolário anterior podemos afirmar que se $p_1^{\alpha_1}$, $p_2^{\alpha_2}$,...,$p_r^{\alpha_r}$ são primos entre si, dois a dois, então $\phi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}) = \phi(p_1^{\alpha_1}) \cdot \phi(p_2^{\alpha_2}) \cdot \ldots \cdot \phi(p_r^{\alpha_r})$. Demonstremos agora a fórmula para calcular $\phi(p^{\alpha})$ para cada inteiro positivo α e cada primo p.

Teorema 2. *Seja p um primo e α um inteiro positivo. Então*

$$\phi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} = p^{\alpha-1} \cdot (p-1) = p^{\alpha} \cdot \left(1 - \frac{1}{p}\right).$$

Demonstração. Sabemos que $\phi(p^{\alpha})$ é a quantidade de inteiros positivos não superior a p^{α} e relativamente primos com p^{α}. Os únicos números positivos menores e que são relativamente primos com p^{α} são aqueles que não possuem o fator p. Observe que os números que possuem o fator p são os seguintes múltiplos:

$$p, 2p, 3p, \cdots, kp,$$

onde $kp = p^{\alpha}$. Logo $k = p^{\alpha-1}$. Portanto, existem $p^{\alpha-1}$ inteiros não primos com p^{α}. Portanto, $\phi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$. □

Vamos calcular $\phi(8)$ usando o teorema demonstrado anteriormente. Temos $\phi(8) = \phi(2^3) = 2^3 - 2^2 = 8 - 4 = 4$.

Observe ainda que, pelo Corolário 1 e Teorema 2, temos:

Teorema 3. *Seja $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot \ldots \cdot {p_k}^{r_k}$ a decomposição de n em fatores primos. Então $\phi(n) = {p_1}^{r_1-1} \cdot {p_2}^{r_2-1} \cdot \ldots \cdot {p_k}^{r_k-1} \cdot (p_1-1) \cdot (p_2-1) \cdot \ldots \cdot (p_k-1)$.*

A partir deste último teorema, podemos calcular facilmente o valor de $\phi(n)$ para algum n relativamente grande. Vamos fazer um exemplo. Decompondo o número 12600 em fatores primos obtemos $12600 = 2^3 \cdot 3^2 \cdot$

$5^2 \cdot 7$. Utilizando o Teorema 3, temos

$$\begin{aligned}\phi(12600) &= \phi(2^3 \cdot 3^2 \cdot 5^2 \cdot 7) \\ &= \phi(2^3) \cdot \phi(3^2) \cdot \phi(5^2) \cdot \phi(7) \\ &= 2^2(2-1) \cdot 3^1(3-1) \cdot 5^1(5-1) \cdot 7^0(7^1-1) \\ &= 4 \cdot 3 \cdot 2 \cdot 5 \cdot 4 \cdot 1 \cdot 6 \\ &= 2880\end{aligned}$$

Portanto, o número 12600 possui 2880 inteiros positivos menores que ele mesmo e que são relativamente primos com ele.

corolário 2. *Para todo número natural $n > 2$, $\phi(n)$ é par.*

Demonstração. Se a decomposição de n contém um fator primo $p \geq 3$, considere p^k a maior potência de p nesta decomposição. Podemos escrever n como o seguinte produto de fatores primos entre si $n = p^k \cdot a$. Pelos Teoremas 1 e 2, segue-se que $\phi(n) = \phi(p^k) \cdot \phi(a) = p^{k-1}(p-1) \cdot \phi(a)$. Como p é um primo maior que 3, $(p-1)$ é par, logo, $\phi(n)$ é par. Agora, se na decomposição não existir um fator primo $p \geq 3$, podemos escrever n da seguinte forma $n = 2^r$ e, como $n > 2$, temos $r > 1$, assim como $\phi(n) = \phi(2^r) = 2^{r-1}.(2-1)$. Como $r > 1$, assim $\phi(n)$ é par. □

Observemos agora os resultados abaixo para chegarmos numa nova conclusão acerca dessa função.

$$\begin{aligned}\phi(2^2) &= \phi(4) = 2 \\ \phi(2^3) &= \phi(8) = 4 \\ \phi(2^2 \cdot 2^3) &= \phi(32) = 16\end{aligned}$$

Note que $\phi(4) \cdot \phi(8) = 2 \cdot 4 < 16 = \phi(32)$. Concluímos que $\phi(2^2) \cdot \phi(2^3) < \phi(2^{2+3})$.

Ainda podemos mostrar que, para quaisquer r, s números naturais e p um número primo, teremos $\phi(p^r) \cdot \phi(p^s) < \phi(p^{r+s})$.

Teorema 4. *Se m e n são números naturais que não são primos entre si, então $\phi(m \cdot n) \neq \phi(m) \cdot \phi(n)$.*

Esse teorema e todos os resultados anteriores são obtidos a partir das propriedades multiplicativas da função ϕ de Euler. Sabemos que um número natural pode ser decomposto em um produto de fatores primos de modo único, mas pode ser escrito como a soma de dois outros números naturais de várias maneiras diferentes, por isso não se espera que ϕ tenha propriedades aditivas. Observe o seguinte exemplo para nos certificarmos:

Sabemos que $\phi(7) = 6$. Podemos decompor o número 7 das seguintes maneiras:

$$7 = 1+6, \text{ temos } \phi(7) \neq \phi(1)+\phi(6) = 1+2 = 3$$
$$7 = 2+5, \text{ temos } \phi(7) \neq \phi(2)+\phi(5) = 1+4 = 5$$
$$7 = 3+4, \text{ temos } \phi(7) \neq \phi(3)+\phi(4) = 2+2 = 4$$

Perceba que nenhumas das respostas é igual ao valor de $\phi(7)$. Além disso, note que os resultados são menores que $\phi(7)$, o que motiva a proposição seguinte:

Proposição 3. *Seja p um primo, para qualquer decomposição aditiva $p = m+n$, m e n naturais, tem-se $\phi(m)+\phi(n) < \phi(p)$.*

A partir do fato de que a função ϕ é multiplicativa e do Teorema 2, temos, a seguir, um importante resultado:

Teorema 5. *Seja $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdot \ldots \cdot {p_k}^{r_k}$ a decomposição de n em fatores primos.*

$$\phi(n) = n\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right).$$

A demonstração deste Teorema pode ser encontrada em Silva (2019). Vamos conferir dois exemplos para uma melhor compreensão. Primeiro, calculemos $\phi(15)$ de outra forma. Inicialmente encontraremos os primos presentes na fatoração de $n = 15$. Temos que $15 = 3 \cdot 5$, então:

$$\begin{aligned}\phi(15) &= 15\prod_{i=1}^{2}\left(1-\frac{1}{p_i}\right)\\ &= 15\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)\\ &= 15\left(\frac{2}{3}\right)\cdot\left(\frac{4}{5}\right)\\ &= 8\end{aligned}$$

Então $\phi(15) = 8$, assim como foi encontrado anteriormente, quando verificamos a quantidade de elementos do conjunto $\{x \in \mathbb{N}: 1 \leq x \leq 15 \text{ e } \text{mdc}(x,15) = 1\}$.

Vamos refazer outro exemplo, calculando $\phi(n)$ para $n = 12600$ de outra forma.

Vimos que a fatoração é $12600 = 2^3 \cdot 3^2 \cdot 5^2 \cdot 7$, então consideraremos os primos 2,3,5 e 7.

$$\begin{aligned}\phi(12600) &= 12600\prod_{i=1}^{4}\left(1-\frac{1}{p_i}\right)\\ &= 12600\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{3}\right)\cdot\left(1-\frac{1}{5}\right)\cdot\left(1-\frac{1}{7}\right)\\ &= 12600\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)\left(\frac{6}{7}\right)\\ &= 2880\end{aligned}$$

Logo, confirmamos que existem 2880 números inteiros menores que 12600 e primos com ele. Fica evidente a dificuldade que teríamos para determinar todos os elementos do conjunto $\{x \in \mathbb{N}: 1 \leq x \leq n \text{ e } \text{mdc}(x,n) = 1\}$ quando n for relativamente grande. Mas, através da fórmula encontrada no Teorema 5, se torna rápido o cálculo de $\phi(n)$.

Em 1907, o matemático Robert Carmichael propôs um enigma que ainda permanece sem solução. Basicamente, Carmichael conjecturou que, para todo inteiro positivo n, há pelo menos um outro inteiro $m \neq n$ tal que $\phi(m) = \phi(n)$. Essa conjectura foi declarada em 1907, mas, como um

teorema no entanto, sua prova foi falha e em 1922 Carmichael retirou sua reivindicação e declarou a conjectura como um problema em aberto.

Tomemos, como exemplo, $\phi(m) = 4$ quando m assume um dos seguintes valores: 5,8,10 e 12. Assim, se tomarmos qualquer um desses valores como m, então qualquer um dos outros três valores pode ser usado como m, para o qual $\phi(m) = \phi(n)$.

A conjectura nos diz que, em cada caso, há mais de um valor de n com o mesmo valor de $\phi(n)$. Observa-se alguns valores na tabela a seguir:

k	Números n tais que $\phi(n) = k$	Número de soluções
1	1,2	2
2	3,4,5	3
3	5,8,10,12	4
4	7, 9, 14, 18	4
6	7, 9, 14, 18	4
8	15,16,20,24,30	5
10	11, 22	2
12	13, 21, 26, 28, 36, 42	6
16	17, 32, 34, 40, 48, 60	6

A conjectura ainda não foi mostrada como verdadeira para os inteiros pares positivos, mas podemos verificar facilmente que é verdadeira para números ímpares. Considera-se r um inteiro ímpar positivo e relembremos o fato de que $\phi(2) = 1$.

$$\phi(2r) = \phi(2)\phi(r) = \phi(r).$$

Existem alguns limites inferiores muito altos para esta conjectura. Carmichael mostrou que qualquer contra-exemplo para a conjectura deve ser pelo menos 10^{37}. Victor Klee estendeu esse resultado para 10^{400}, e um limite inferior de $10^{10^{10}}$ foi determinado por Kevin Ford em 1998.

Mais um problema não resolvido é o problema de Lehmer: existe algum número n composto tal que $\phi(n)$ divida $n-1$. Observe que para qualquer primo o problema é fácil de se resolver. Considere p um número primo, teremos $\phi(p) = p-1$ e, assim, $\phi(p)$ divide $p-1$. D. H. Lehmer

conjecturou, em 1932, que não há número composto com tal propriedade. Para esse e outros problemas não resolvidos em teoria dos números, o leitor pode consultar Guy (2013).

2.3 Estudo combinatorial de $\phi(n)$

Estudaremos, nessa seção, um teorema desenvolvido por Gauss que envolve a função ϕ de Euler. Segundo Hefez (2016), Carl Friederich Gauss (1777-1855) é um dos maiores matemáticos de todos os tempos. Nasceu na Alemanha, filho de uma família modesta, aprendeu a ler sozinho e possuía enorme habilidade para realizar cálculos mentais. Em 1799, ele demonstra o Teorema Fundamental da Álgebra, que havia sido enunciado por vários matemáticos, mas nenhuma prova correta tinha sido apresentada até então. Gauss foi um dos primeiros a tratar os números complexos dando-lhes a representação geométrica como pontos do plano cartesiano. Gauss foi também um dos criadores das geometrias não-euclidianas, da geometria diferencial, das funções de variáveis complexas, da topologia e da teoria algébrica dos números. Deu contribuições à matemática aplicada, física, astronomia e teoria das probabilidades. "Gauss teve o poder de mudar os rumos da matemática a partir dos seus trabalhos revolucionários, apresentados como extremo rigor e grande concisão e elegância. Por isso, foi considerado, pelos seus contemporâneos e pelas gerações que se sucederam, um príncipe da rainha das ciências"(HEFEZ, 2016).

Teorema 6. *(ANDREWS, 1994, Teorema 6.1)(Gauss) Considere a soma dos valores da função $\phi(n)$ para todos os d divisores de n. Então*

$$\sum_{d|n} \phi(d) = n.$$

Demonstração. Seja S_n o conjunto $\{1,2,3,..,n\}$. Temos claramente que a cardinalidade de S_n é $|S_n| = n$. Para cada d que divide n, denotamos por $T_d(n)$ o conjunto de inteiros positivos não excedendo n, cujo maior divisor comum com n é d. Daí, para cada n, os conjuntos $T_d(n)$ não têm elementos

comuns. Além disso, para qualquer $m \in S_n$, vemos que $m \in T_d(n)$ onde $d = \text{mdc}(m,n)$. Consequentemente, $n = |(S_n)| = \sum_{d|n} |T_d(n)|$.

Agora, mostraremos que $T_d(n)$ tem $\phi\left(\frac{n}{d}\right)$ elementos. Primeiro, note-se que todos os elementos de $T_d(n)$ são múltiplos de d e são menores ou iguais a n. Observe-se que os únicos números da forma ad em $T_d(n)$ são aqueles para os quais $\text{mdc}(a, \frac{n}{d}) = 1$, havendo $\phi\left(\frac{n}{d}\right)$ elementos. De fato, os elementos de $T_d(n)$ são encontrados entre os números $d, 2d, \cdots, \left(\frac{n}{d}\right)d$. Agora, se $\text{mdc}\left(a, \frac{n}{d}\right) = e$, então $\text{mdc}(ad,n) = ed$ e $ed = d$ se, e somente se, $e = 1$. Assim:

$$n = |(S_n)| = \sum_{d|n} |T_d(n)| = \sum_{d|n} \phi\left(\frac{n}{d}\right).$$

Por fim, note-se que:

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

Temos que d assume os valores dos vários divisores de n e o mesmo acontece com o divisor complementar $\frac{n}{d}$. Assim, provamos nosso teorema.

Ilustremos a ideia apresentada na demonstração do Teorema 6 com exemplos. Considere $n = 6$, então d pode assumir os valores $1, 2, 3$ e 6. Teremos $T_1(6) = \{1,5\}$, $T_2(6) = \{2,4\}$, $T_3(6) = \{3\}$ e $T_6(6) = \{6\}$.

Neste exemplo, consideremos $n = 45$. Os divisores de n são: $d = 1, 3, 5, 9, 15, 45$. Separemos os números de 1 a 45 em conjuntos $T_d(n)$, cujo maior divisor comum deste número com n é d. Assim teremos:

$T_{45}(45) = \{45\}$

$T_{15}(45) = \{15, 30\}$

$T_9(45) = \{9, 18, 27, 36\}$

$T_5(45) = \{5, 10, 20, 25, 35, 40\}$

$T_3(45) = \{3, 6, 12, 21, 24, 33, 39, 42\}$

$T_1(45) = \{1, 2, 4, 7, 8, 11, 13, 14, 16, 17, 19, 22, 23, 26, 28, 29, 31, 32, 34, 37, 38, 41, 43, 44\}$

Observe que esses conjuntos são disjuntos e a união deles é o conjunto $\{1,2,3,\cdots,45\}$. Nota-se também a seguir que a quantidade de elementos em cada $T_d(45)$ é igual a $\phi(\frac{45}{d})$:

Conjuntos $T_d(n)$	Números de elementos em $T_d(n)$
$T_1(45)$	$24 = \phi(45) = \phi(\frac{45}{1})$
$T_3(45)$	$8 = \phi(15) = \phi(\frac{45}{3})$
$T_5(45)$	$6 = \phi(9) = \phi(\frac{45}{5})$
$T_9(45)$	$4 = \phi(5) = \phi(\frac{45}{9})$
$T_{15}(45)$	$2 = \phi(3) = \phi(\frac{45}{15})$
$T_{45}(45)$	$1 = \phi(1) = \phi(\frac{45}{45})$

Veja que, se d é divisor de 45, então $\frac{45}{d}$ também é. Confirmamos que $\sum_{d|n}\phi\left(\frac{n}{d}\right) = \sum_{d|n}\phi(d)$ e, além disso, temos $\sum_{d|45}\phi(d) = 45$.

2.4 Função ϕ de Euler e o princípio de inclusão e exclusão

Uma ferramenta muito importante que nos permite encontrar a resolução de vários modelos de problemas matemáticos envolvendo a contagem de elementos é o Princípio da Inclusão e Exclusão. Esse princípio nos permite calcular a quantidade de elementos que pertencem à união de conjuntos quaisquer, não necessariamente disjuntos, e será utilizado para sistematizar a fórmula da função ϕ de Euler, provada no Teorema 5.

2.4.1 Cardinalidade da união de dois conjuntos

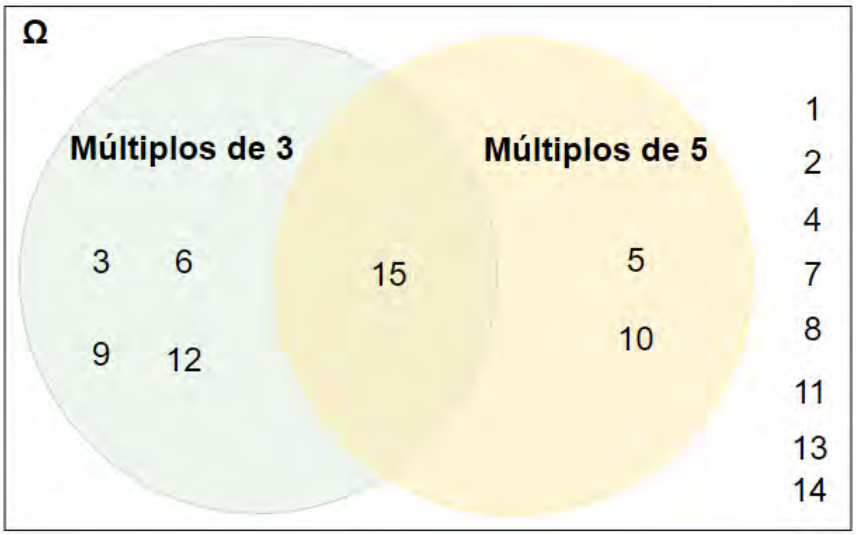
Simbolizemos por Ω o conjunto universo e $\{0\}$ o conjunto vazio. Para esta seção, utilizamos o capítulo 4 de Santos, Mello e Murari (2007), como base do nosso estudo.

Teorema 7. *Sejam A e B conjuntos finitos, então* $|A \cup B| = |A| + |B| - |A \cap B|$.

Essa é a fórmula do Princípio da Inclusão e Exclusão para dois conjuntos não disjuntos. Essa regra também tem êxito para conjuntos disjuntos, uma vez que a interseção entre conjuntos disjuntos é o conjunto vazio, então $A \cap B = \{0\}$ e $|A \cup B| = |A| + |B|$. Veremos no próximo exemplo que é possível obter $\phi(n)$, n um número natural, com facilidade e de maneira precisa pela utilização do Princípio de Inclusão e Exclusão.

Como exemplo, vamos calcular $\phi(n)$ para $n = 15$. Inicialmente devemos encontrar os p_i primos presentes na decomposição em fatores primos de n, onde $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdots {p_i}^{r_i}$.
Defina o conjunto $A_{p_i} = \{$números naturais menores que n e divisíveis por $p_i\}$, em seguida, devemos determinar a quantidade de elementos pertencentes a cada conjunto A_{p_i}. Para encontrarmos a quantidade de números menores ou igual a 15 e coprimos com respeito a ele, devemos encontrar a cardinalidade do complementar da união dos A_{p_i}. Observemos a figura abaixo:

Figura 2.1: Quantidade de elementos para $\phi(15)$



Fonte: Elaborada pelo autor.

Temos $n = 15 = 3 \cdot 5$, então $A_3 = \{$Múltiplos de 3$\} = \{3,6,9,12,15\}$
$A_5 = \{$Múltiplos de 5$\} = \{5,10,15\}$.
Além disso, é necessário determinar a cardinalidade da interseção destes

conjuntos: $A_3 \cap A_5 = \{\text{Múltiplos de } 15\} = \{15\}$. Observa-se que a cardinalidade de cada conjunto pode ser dada por:

$$|A_3| = \frac{15}{3} = 5$$
$$|A_5| = \frac{15}{5} = 3$$
$$|A_3 \cap A_5| = \frac{15}{5 \cdot 3} = 1$$

Tendo encontrado esses valores, podemos calcular $\phi(15)$:

$$\phi(15) = |\Omega| - |A_3 \cup A_5|$$

A partir do Teorema 7, obtemos:

$$\begin{aligned}\phi(15) &= |\Omega| - (|A_3| + |A_5| - |A_3 \cap A_5|) \\ &= 15 - (5 + 3 - 1) = 8\end{aligned}$$

2.4.2 Cardinalidade da união de três conjuntos

Para aplicarmos o Princípio da Inclusão e Exclusão a três conjuntos, devemos identificar as interseções dois a dois e a interseção entre os três conjuntos. Observa-se a seguir a fórmula que nos fornece a quantidade de elementos da união de três conjuntos:

Teorema 8. *Sejam A, B e C conjuntos finitos, então* $|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

Vamos calcular a quantidade de números menores ou igual a 30 e coprimos com respeito a ele. Temos $n = 30 = 2 \cdot 3 \cdot 5$, a decomposição de n em fatores primos, então os p_i fatores primos de n, são $3, 2, 5$. Para calcularmos $\phi(n)$ para $n = 30$ por meio do Princípio da Inclusão e Exclusão, além de determinar a quantidade de elementos que pertencem a cada conjunto A_{p_i}, devemos encontrar a cardinalidade das interseções.

Observemos os conjuntos a seguir:

$$A_2 = \{2,4,6,8,10,12,14,16,18,20,22,24,26,28,30\}$$
$$A_3 = \{3,6,9,12,15,18,21,24,27,30\}$$
$$A_5 = \{5,10,15,20,25,30\}$$
$$A_2 \cap A_3 = \{6,12,18,24,30\}$$
$$A_2 \cap A_5 = \{10,20,30\}$$
$$A_3 \cap A_5 = \{15,30\}$$
$$A_2 \cap A_3 \cap A_5 = \{30\}$$

Podemos contar os elementos de cada conjunto citado, ou encontrar a cardinalidade de cada conjunto, da seguinte maneira:

$$|A_2| = \frac{30}{2} = 15$$
$$|A_3| = \frac{30}{3} = 10$$
$$|A_5| = \frac{30}{5} = 6$$
$$|A_2 \cap A_3| = \frac{30}{2 \cdot 3} = \frac{30}{6} = 5$$
$$|A_2 \cap A_5| = \frac{30}{2 \cdot 5} = \frac{30}{10} = 3$$
$$|A_3 \cap A_5| = \frac{30}{5 \cdot 3} = \frac{30}{15} = 2$$
$$|A_2 \cap A_3 \cap A_5| = \frac{30}{2 \cdot 3 \cdot 5} = \frac{30}{30} = 1$$

Os números menores ou igual a 30 e coprimos com respeito a ele são aqueles que não estão contidos nos conjuntos A_{p_i}. Portanto devemos encontrar a cardinalidade do complementar da união dos A_{p_i}. Logo:

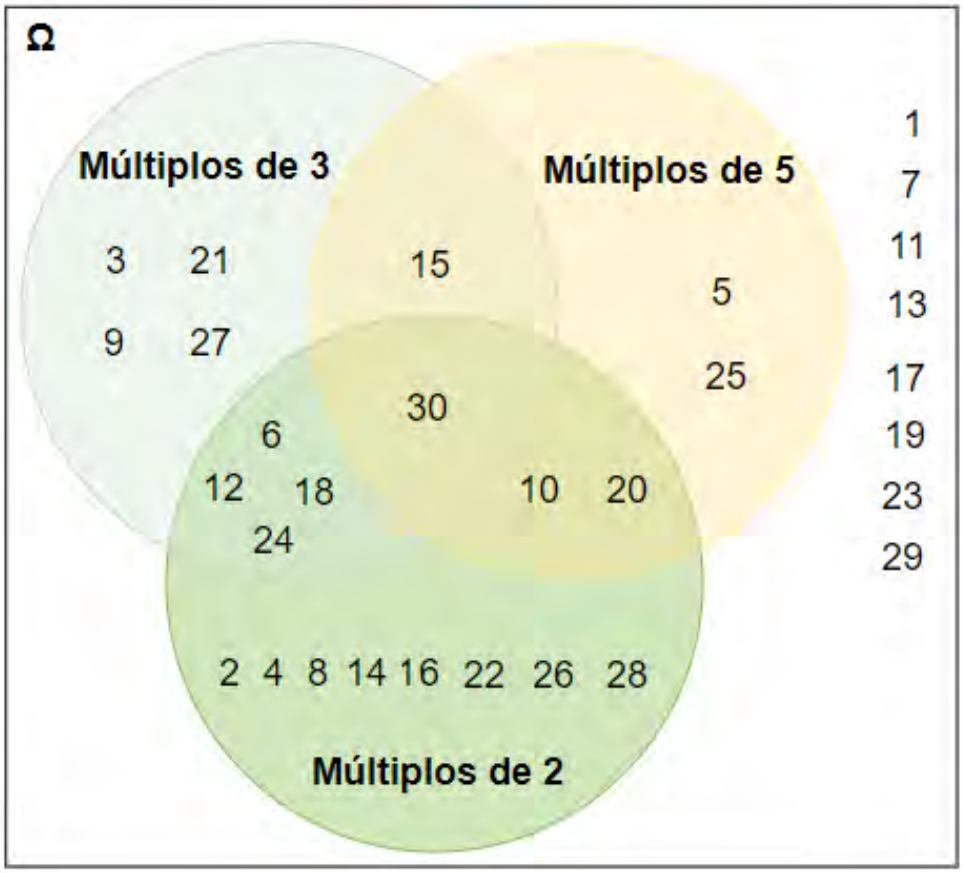
$$\phi(30) = |\Omega| - |A_2 \cup A_3 \cup A_5|$$

Onde $\Omega = \{1,2,3,\cdots,30\}$. Pelo Princípio da Inclusão e Exclusão temos

$$\begin{aligned}\phi(30) &= |\Omega| - (|A_2| + |A_3| + |A_5| - |A_2 \cap A_3| - |A_2 \cap A_5| - |A_3 \cap A_5| + |A_2 \cap A_3 \cap A_5|) \\ &= 30 - (15 + 10 + 6 - 5 - 3 - 2 + 1) = 8\end{aligned}$$

Podemos conferir nosso resultado observando a figura a seguir:

Figura 2.2: Quantidade de elementos para $\phi(30)$



Fonte: Autoria própria.

2.4.3 Princípio da inclusão e exclusão

Vimos que para definirmos a cardinalidade da união de apenas dois conjuntos se utiliza o Teorema 7 e para três conjunto o Teorema 8. A generalização para n conjuntos finitos se dá através do seguinte teorema:

Teorema 9. *(SANTOS; MELLO; MURARI, 2007, Teorema 4.1)(Princípio da Inclusão e Exclusão) Se $A_1, A_2, A_3, \cdots, A_k$ são conjuntos finitos, então:*

$$\begin{aligned}\left|\bigcup_{i=1}^{k} A_i\right| &= \sum_{1\leq i<k} |A_i| - \sum_{1\leq i<j\leq k} |A_i \cap A_j| \\ &+ \sum_{1\leq i<j<p\leq k} |A_i \cap A_j \cap A_p| - \sum_{1\leq i<j<p<q\leq k} |A_i \cap A_j \cap A_p \cap A_q| \\ &+ \cdots + (-1)^{(k-1)} |A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_k|.\end{aligned}$$

Para a demonstração deste teorema consultar Santos, Mello e Murari (2007, seção 4.2).

Usemos o Princípio da Inclusão e Exclusão para demostrar o Teorema 5, isto é, para cada $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdots {p_k}^{r_k}$, temos:

$$\phi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

Demonstração. De fato, considere $n = {p_1}^{r_1} \cdot {p_2}^{r_2} \cdots {p_k}^{r_k}$ e defina os seguintes conjuntos:

$$\begin{aligned} A &= \{1, 2, 3, .., n\} \\ A_1 &= \{x \in A | \quad x \quad \text{é múltiplo de} \quad p_1\} \subset A \\ A_2 &= \{x \in A | \quad x \quad \text{é múltiplo de} \quad p_2\} \subset A \\ A_3 &= \{x \in A | \quad x \quad \text{é múltiplo de} \quad p_3\} \subset A \\ &\vdots \\ A_k &= \{x \in A | \quad x \quad \text{é múltiplo de} \quad p_k\} \subset A \end{aligned}$$

Como os números contidos nesses conjuntos possuem fatores primos

de n em sua fatoração, então nenhum desses é relativamente primo com n. Portanto, temos que retirar esses números do conjunto A para encontrarmos o valor de $\phi(n)$. Logo:

$$\phi(n) = |A| - |A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_k|$$

Pelo Princípio da Inclusão e Exclusão, temos:

$$\begin{aligned}\phi(n) = |A| - \Bigg| &\sum_{1\le i<k} |A_i| - \sum_{1\le i<j\le k} |A_i \cap A_j| + \sum_{1\le i<j<p\le k} |A_i \cap A_j \cap A_p| \\ &- \sum_{1\le i<j<p<q\le k} |A_i \cap A_j \cap A_p \cap A_q| + \cdots + (-1)^{(k-1)} |A_1 \cap A_2 \cap \cdots \cap A_k| \Bigg| \\ = |A| &- \sum_{1\le i<k} |A_i| - \sum_{1\le i<j\le k} |A_i \cap A_j| + \sum_{1\le i<j<p\le k} |A_i \cap A_j \cap A_p| \\ &- \sum_{1\le i<j<p<q\le k} |A_i \cap A_j \cap A_p \cap A_q| + \cdots + (-1)^{(k-1)} |A_1 \cap A_2 \cap \cdots \cap A_k|\end{aligned} \tag{2.1}$$

Sabemos que $|A| = n$ e $|A_i| = \left(\frac{n}{p_i}\right)$ para qualquer $1 \le i \le k$. Assim, para r interseções destes conjuntos, teremos:

$| \text{ A }_1 \cap A_2 \cap \cdots \cap A_r|$
$= |\{m \in N : m \le n; \quad p_{i_1} \text{ divide } m, p_{i_2} \text{ divide } m, \ldots, p_{i_r} \text{ divide } m\}$
$= \frac{n}{p_{i_1} \cdot p_{i_2} \cdots p_{i_r}}$.

Desta forma:

$$\begin{aligned}
\sum_{1\leq i<k} |A_i| &= \sum_{1\leq i<k} \left(\frac{n}{p_i}\right) \\
\sum_{1\leq i<j\leq k} |A_i \cap A_j| &= \sum_{1\leq i<j\leq k} \left(\frac{n}{p_i p_j}\right) \\
\sum_{1\leq i<j<p\leq k} |A_i \cap A_j \cap A_p| &= \sum_{1\leq i<j<p\leq k} \left(\frac{n}{p_i p_j p_p}\right) \\
\sum_{1\leq i<j<p<q\leq k} |A_i \cap A_j \cap A_p \cap A_q| &= \sum_{1\leq i<j<p<q\leq k} \left(\frac{n}{p_i p_j p_p p_q}\right) \\
&\vdots \\
|A_1 \cap A_2 \cap A_3 \cap \cdots \cap A_k| &= \left(\frac{n}{p_1 p_2 \cdots p_k}\right).
\end{aligned}$$

Voltando para (2.1):

$$\begin{aligned}
\phi(n) &= |A| - \sum_{1\leq i<k} |A_i| - \sum_{1\leq i<j\leq k} |A_i \cap A_j| + \sum_{1\leq i<j<p\leq k} |A_i \cap A_j \cap A_p| \\
&\quad - \sum_{1\leq i<j<p<q\leq k} |A_i \cap A_j \cap A_p \cap A_q| + \cdots + (-1)^{(k-1)} |A_1 \cap A_2 \cap \cdots \cap A_k| \\
&= n - \left|\sum_{1\leq i<k} \left(\frac{n}{p_i}\right)\right| + \left|\sum_{1\leq i<j\leq k} \left(\frac{n}{p_i p_j}\right)\right| + \left|\sum_{1\leq i<j<p\leq k} \left(\frac{n}{p_i p_j p_p}\right)\right| \\
&\quad + \cdots + (-1)^{(k)} \left|\left(\frac{n}{p_1 p_2 \cdots p_k}\right)\right| \\
&= n\left[1 - \left|\sum_{1\leq i<k} \left(\frac{1}{p_i}\right)\right| + \left|\sum_{1\leq i<j\leq k} \left(\frac{1}{p_i p_j}\right)\right| + \left|\sum_{1\leq i<j<p\leq k} \left(\frac{1}{p_i p_j p_p}\right)\right| \right. \\
&\quad \left. + \cdots + (-1)^{(k)} \left|\left(\frac{1}{p_1 p_2 \cdots p_k}\right)\right|\right] \\
&= n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right),
\end{aligned}$$

o que conclui a demonstração. □

2.5 Considerações finais

Buscamos neste artigo criar um material rico sobre a função $\phi(n)$ de Euler. Apresentamos algumas definições e exemplos que são de fácil entendimento, possibilitando assim a compreensão dos alunos do ensino médio. Desta forma, espera-se que o trabalho contribua para despertar o interesse do professor em trabalhar conteúdos de nível superior com alunos da educação básica. O estudo da função de Euler pelo Princípio da Inclusão e Exclusão, que é proposto neste trabalho, é uma possibilidade de apresentação do conteúdo para alunos a partir do primeiro ano do ensino médio.

Os alunos se deparam com teoria de números em séries do ensino básico e acabam sentindo dificuldades em desenvolver e aprimorar as habilidades que compõem o raciocínio lógico. Da perspectiva do professor, esse recebe a oportunidade de criar um ambiente na sala de aula em que a comunicação seja benéfica, propiciando momentos de interação entre alunos e professor, trocas de experiências e discussões.

Neste trabalho, buscamos oferecer uma abordagem combinatória para a teoria elementar de números, envolvendo, por exemplo, a função ϕ de Euler e o Princípio de Inclusão e Exclusão. Esses temas compartilham uma certa interseção do conhecimento comum e cada um genuinamente enriquece o outro. Desta forma, ao estudar a teoria dos números a partir de uma perspectiva combinatória, alunos e professores se beneficiam da consequente simplicidade das provas de muitos teoremas, sendo poupados de repetição e adquirindo novos insights.

2.6 Referências bibliográficas

ANDREWS, G. E. **Number Theory**. Chelmsford: Courier Corporation, 1994.

CRUISE, B. Euler's totient function. **Khan Academy**, 2012. Disponível em: <www.khanacademy.org/computing/computer-science/cryptography/modern-crypt/v/euler-s-totient-function-phi-function>. Acesso em: 23 jun. 2021.

GUY, R. **Unsolved problems in number theory**. Berlin: Springer Science Business Media, 2013. v. 1.

HEFEZ, A. **Aritmética - Coleção PROFMAT**. Vol 2. Rio de Janeiro: SBM, 2016.

SANTOS, J. P. de O.; MELLO, M. P.; MURARI, I. T. C. **Introdução análise combinatória.** Rio de Janeiro: Ed. Ciência Moderna, 2007.

SILVA, E. R. **Funções elementares e teoria dos números**. 2019. Dissertação (Mestrado em Matemática) - Departamento de Matemática, Universidade Federal Rural de Pernambuco, Recife, PE. Disponível em: <dm.ufrpe.br/sites/www.dm.ufrpe.br/files/eldaline_tcc.pdf>.

Capítulo 3

Considerações sobre matemática financeira e educação financeira no ensino médio: Uma breve análise de documentos oficiais e de livros didáticos.

Me. Elizeu Odilon Bezerra Filho[1]
Dr. Elisângela Bastos de Mélo Espíndola [2]

Resumo: Neste artigo, apresentamos diferenças entre os conceitos de Educação Financeira (EF) e Matemática Financeira (MF). Além disso, expomos algumas considerações sobre as orientações para o ensino de MF e EF presentes nos documentos oficiais, enfatizando a BNCC, que é o documento mais atual e que já está norteando o funcionamento da educação no país. Analisando esses documentos, verificamos que na Base Nacional Comum Curricular (BNCC) a temática EF passa a ter mais destaque no currículo escolar, podendo ser trabalhada não apenas dentro

[1]Universidade Federal Rural de Pernambuco, eli.odilon@gmail.com
[2]Universidade Federal Rural de Pernambuco, ebmespindola@gmail.com

da área de conhecimento da matemática e suas tecnologias. Também apresentaremos um panorama acerca das propostas dos livros didáticos (LD) do Ensino Médio, aprovados no PNLD 2018 para o ensino desses temas. Nessa análise, buscamos verificar como o assunto MF é introduzido nos LD, quais os conteúdos presentes nos capítulos que tratam de MF e como os conteúdos se relacionam com a EF.
Palavras-chave: Matemática Financeira; Educação Financeira; BNCC; Livros Didáticos.

3.1 Introdução

O artigo 1º no 2º parágrafo da Lei de Diretrizes e Bases da Educação Brasileira (BRASIL, 1996) declara que: "A educação escolar deve vincular-se ao mundo do trabalho e a prática social". Nesse sentido, para o aluno, é essencial a combinação entre o aprendizado teórico e sua respectiva aplicação prática, de modo que o mesmo se torne capaz de resolver problemas cotidianos, de tratar informações de forma crítica e de usar esse aprendizado como suporte à tomada de decisões.

Deste modo, a matemática apresenta-se como um componente da educação escolar que exerce um papel muito importante na construção e no acesso à cidadania, já que se aplica às várias ciências e a inúmeras situações da vida cotidiana. Nesse contexto, entendemos a importância atribuída nos últimos anos ao ensino de Matemática Financeira (MF) em articulação com a Educação Financeira (EF); pois não são raras as situações rotineiras que precisamos usar conhecimentos dessas áreas para nos orientarmos na tomada de decisões na nossa vida. "Uma das temáticas que mais parece aproximar a vida do aluno aos seus conhecimentos escolares são os temas relacionados às finanças, uma vez que, muito ou pouco, as pessoas estão diariamente, lidando com situações que envolvem compra e venda" (PESSOA, 2016, p.5).

Nos últimos anos, o tema EF vem ganhando muito impulso e relevância e não é para menos; todos nós estamos envolvidos com problemas ligados ao mundo econômico e financeiro. O aumento progressivo da complexidade dos mercados financeiros e produtos financeiros, as mudanças demográficas,

econômicas e políticas, fez com que a EF ganhasse mais espaço e relevância, passando a ser mais discutida dentro de uma sociedade cada vez mais consumista.

Desta forma, torna-se importante que desde cedo a temática da EF seja trabalhada nas escolas de modo a contribuir com o processo de desenvolvimento do estudante como cidadão consciente, para que ele seja capaz de fazer planejamento e ter responsabilidade quanto ao consumo, para que tenha habilidade de escolha perante diferentes alternativas de crédito ou de investimentos e para que seja capaz de compreender decisões tomadas pelo governo e que afetam a economia de uma sociedade.

3.2 Educação financeira e matemática financeira

A MF consiste em uma série de conceitos matemáticos aplicados à análise de dados financeiros. É um conhecimento técnico de fórmulas matemáticas para se calcular valor de juros, saber o valor presente de uma dívida etc. Como veremos, a EF passou a ser uma necessidade para a formação do cidadão no mundo atual. De acordo com Pessoa (2016, p. 1), a EF tem por propósito:

> Ajudar as pessoas a administrarem seu dinheiro e o que ele envolve, poupança, finanças, cartões de crédito, investimentos, compras, vendas, dentre outros, para que o consumo ocorra de forma consciente. Quanto mais a sociedade se complexifica, mais necessário é o domínio do conhecimento financeiro das pessoas que compõem a sociedade.

A EF não se trata de ensinar técnicas e fórmulas de MF, muito embora esse processo seja importante e necessário. Educar financeiramente é uma

ação muito mais ampla, que segundo Muniz e Jurkiewicz (2010, p. 2-3), inclui:

> Aprender matemática para compreender as situações financeiras; entender o comportamento do dinheiro no tempo; organizar conscientemente suas finanças (futuras) pessoais; discutir matematicamente o uso consciente do crédito; entender temas de economia como PIB, inflação e seus diferentes índices, IOF, IR dentre outros; aprender, interligar e utilizar matemática financeira nas questões geoeconômicas já abordadas, porém não interligadas, nas aulas de Geografia; compreender os principais sistemas de financiamentos (PRICE e SAC), utilizando inclusive os recursos tecnológicos amplamente disponíveis, como planilhas eletrônicas e calculadoras científicas; refletir e analisar matematicamente o aumento da expectativa de vida do brasileiro e seus impactos na economia nacional, incluindo sua própria aposentadoria, seguros em geral e previdência complementar; discutir e analisar quantitativa e qualitativamente os impactos de problemas geopolíticos e sociais nas economias de uma região, levando-se em consideração a viabilidade das ferramentas matemáticas estudadas, dentre outros. Essas questões certamente devem fazer parte da educação financeira dos alunos que comporão a população economicamente ativa de um país.

Desta forma, introduzir e ensinar aos estudantes questões ligadas a EF acaba por ser imprescindível, pois oferece a eles oportunidades de reflexão, permitindo que os mesmos avaliem decisões no âmbito financeiro, que se tornarão cada vez mais presentes em suas vidas à medida que vão se deparando com a idade adulta.

A inclusão e o destaque dado ao tema EF, fortalece por consequência a própria MF, já que o aprendizado de ambas são interligados. Enquanto a EF pode servir como elemento motivador para o aprendizado dos conteúdos de MF; o conhecimento e domínio destes conteúdos são essenciais no processo de EF de cada indivíduo. Por exemplo, investir dinheiro e financiar bens de consumo são situações comuns no cotidiano de muitas pessoas e um cidadão que tenha boa EF tende a fazer escolhas melhores. O conhecimento de conteúdos ligados a MF são muito úteis no processo de análise de alternativas de investimentos ou financiamentos. Se, por um lado, a EF faz com que o cidadão que deseje financiar um imóvel procure se informar acerca das taxas de juros, do prazo de financiamento etc; a MF vai ser a ferramenta que ele vai usar para fazer os cálculos e comparações das taxas a fim de obter as melhores condições para seu financiamento.

Em suma, entendemos que a MF é uma área que aplica conhecimentos matemáticos à análise de questões ligadas a dinheiro ao longo do tempo, enquanto a EF está ligada à formação de comportamentos do indivíduo em relação às finanças. Embora sejam temáticas com estreita relação, elas não são equivalentes. Por exemplo, é comum nos depararmos com situações em que pessoas com pouco conhecimento de matemática financeira (conhecimento técnico) não tenham dívidas, em alguns casos chegam até a ter reserva financeira para emergência e um patrimônio legal. Também encontramos pessoas com muito conhecimento técnico totalmente endividadas, sem reserva financeira para emergência, vivendo um padrão de vida fora da sua realidade financeira.

3.3 Considerações sobre a matemática financeira e a educação financeira em orientações curriculares

Dada a importância das orientações curriculares, expomos algumas de suas considerações sobre o tema MF e EF, sobretudo relacionadas ao

Ensino Médio. Para isso, consultamos: os Parâmetros Curriculares Nacionais/PCN+ Ensino Médio – Ciências da Natureza, Matemática e suas Tecnologias (BRASIL, 2002); as Orientações Curriculares para o Ensino Médio (BRASIL, 2006); os Parâmetros para a Educação Básica do Estado de Pernambuco (PERNAMBUCO, 2012) e a Base Nacional Comum Curricular (BNCC) (BRASIL, 2018).

3.3.1 PCN + ensino médio

Os PCN + Ensino Médio são orientações educacionais complementares aos Parâmetros Curriculares Nacionais dessa etapa da Educação Básica. Esse documento sistematiza os conteúdos de Matemática em três eixos ou temas estruturadores (Álgebra: Números e Funções; Geometria e Medidas; e Análise de Dados) a serem desenvolvidos durante os três anos do Ensino Médio de maneira concomitante. A MF é brevemente abordada no PCN + Ensino Médio, sendo citada sua aplicação dentro do tema ou eixo estruturador Álgebra: Números e Funções. Destacando-se que na vivência cotidiana esse se apresenta com “enorme importância enquanto linguagem, como na variedade de gráficos presentes diariamente nos noticiários e jornais, e também enquanto instrumento de cálculos de natureza financeira e prática, em geral” (BRASIL, 2000, p. 120). Nesse documento, a ideia de articular a MF com a EF não foi suscitada, visto que, na época dos PCN+, a EF não era sistematicamente discutida.

3.3.2 Orientações curriculares para o ensino médio

Nas Orientações Curriculares para o Ensino Médio, o tema MF aparece quando se aborda o item questões de conteúdo. “Dentre as aplicações da Matemática, tem-se o interessante tópico de Matemática Financeira como um assunto a ser tratado quando do estudo da função exponencial - juros e correção monetária fazem uso desse modelo"(BRASIL, 2006, p. 75).

Nesse documento, ainda verificamos que, no bloco Números e Operações, é dito que deve-se proporcionar aos alunos uma diversidade de

situações, de forma a capacitá-los a resolver problemas do quotidiano, tais como: “operar com números inteiros e decimais finitos; operar com frações, em especial com porcentagens; [...] ler faturas de contas de consumo de água, luz e telefone [...]” (BRASIL, 2006, p. 70).

Também é colocado que o trabalho com esse bloco de conteúdos deve tornar o aluno, ao final do Ensino Médio, capaz de decidir sobre: “as vantagens/desvantagens de uma compra à vista ou a prazo; avaliar o custo de um produto em função da quantidade [...]; calcular impostos e contribuições previdenciárias; avaliar modalidades de juros bancários” (BRASIL, 2006, p. 71). Essas indicações da OCN, embora não apresentem explicitamente o termo "Educação Financeira", apontam, através dessas sugestões, para o tratamento do tema.

3.3.3 Parâmetros curriculares para a educação básica no estado de Pernambuco

Nos Parâmetros Curriculares para a Educação Básica no Estado de Pernambuco (PCEBPE) encontram-se considerações a respeito do ensino de conteúdos relacionados ao estudo de MF desde os anos iniciais do Ensino Fundamental até o Ensino Médio. Embora o termo MF não apareça nesse documento, vários dos seus conteúdos são indicados no bloco Números e Operações. Por exemplo, orienta-se que:

> O trabalho com porcentagens deve ser continuado e aprofundado no Ensino Médio, principalmente por sua grande utilidade nas práticas sociais dos alunos. Eles devem ser capazes de solucionar problemas envolvendo situações de reajustes ou descontos, de cálculos de taxas percentuais e – muito importante para alunos que, muitas vezes, estão inseridos no mercado de trabalho – as ideias de juros simples e compostos. (PERNAMBUCO, 2012, p. 137).

Ainda sobre os conteúdos de MF no Ensino Médio, no bloco Números e Operações, encontram-se duas expectativas de aprendizagem, distribuídas no 10º, 11º e 12º ano, respectivamente relacionadas ao 1º, 2º e 3º ano:

> **10º Ano** - Resolver e elaborar problemas envolvendo porcentagem, incluindo as ideias de juros simples e compostos e a determinação de taxa percentual, relacionando representação percentual e decimal (por exemplo, entender que multiplicar por 1,20 corresponde a um aumento de 20% ; multiplicar por 2,40 equivale a um aumento de 140%; multiplicar por 0,70 corresponde a um desconto de 30% etc.) (PERNAMBUCO, 2012, p. 138).
>
> **11º e 12º anos** - Resolver problemas envolvendo porcentagem, incluindo cálculo de acréscimos e decréscimos, determinação de taxa percentual e porcentagem de porcentagem. (PERNAMBUCO, 2012, p. 139).

Em particular, observamos que, no que concerne à MF, esse documento apresenta diferenças quanto às Orientações Curriculares para o Ensino Médio (OCEM); por exemplo, não é mencionada a possibilidade de se trabalhar os conceitos de juros em articulação com o de funções. Embora se façam referências às práticas sociais dos alunos, Pernambuco (2012) não apresenta sugestões de como abordar a EF.

3.3.4 Base nacional comum curricular

A BNCC reconhece a EF como um dos temas transversais que deverão ser abordados nos currículos de Estados e Municípios. De acordo com a BNCC:

> Cabe aos sistemas e redes de ensino, assim como às escolas, em suas respectivas esferas de autonomia e competência, incorporar aos currículos e às propostas pedagógicas a abordagem de temas contemporâneos que afetam a vida humana em escala local, regional e global, preferencialmente de forma transversal e integradora (BRASIL, 2018, p. 19).

A BNCC incluiu a EF entre os temas transversais que deverão constar nos currículos de todo o Brasil. Sendo assim, a partir desse documento, esse tema passa a fazer parte de um leque de temáticas que devem ser incorporados às propostas pedagógicas de estados e municípios, a exemplo do que ocorre com: Educação das Relações Étnico-raciais, Ensino de História e Cultura Afro-brasileira, Educação Ambiental, entre outros. Essas temáticas são contempladas em habilidades dos componentes curriculares, cabendo aos sistemas de ensino e escolas, de acordo com suas especificidades, tratá-las de forma contextualizada (BRASIL, 2018).

A BNCC propõe para o ensino da Matemática cinco unidades de conhecimentos correlacionadas da própria área, que orientam a formulação de habilidades a serem desenvolvidas ao longo dessa etapa. São elas: Números, Álgebra, Geometria, Grandezas e Medidas e Probabilidade e Estatística. Na unidade temática "Números", um dos aspectos a ser considerado é:

> O estudo de conceitos básicos de economia e finanças, visando à educação financeira dos alunos. Assim, podem ser discutidos assuntos como taxas de juros, inflação, aplicações financeiras (rentabilidade e liquidez de um investimento) e impostos. Essa unidade temática favorece um estudo interdisciplinar envolvendo as dimensões culturais, sociais, políticas e psicológicas, além da econômica, sobre as questões do consumo, trabalho e dinheiro. É possível, por exemplo, desenvolver um projeto com a História, visando ao estudo do dinheiro e sua função na

> sociedade, da relação entre dinheiro e tempo, dos impostos em sociedades diversas, do consumo em diferentes momentos históricos, incluindo estratégias atuais de marketing. Essas questões, além de promover o desenvolvimento de competências pessoais e sociais dos alunos, podem se constituir em excelentes contextos para as aplicações dos conceitos da Matemática Financeira e também proporcionar contextos para ampliar e aprofundar esses conceitos (BRASIL, 2018, p. 269).

Observamos que dentre os documentos já mencionados (PCN+, OCN, PEBPE) é dado pouco destaque à articulação entre MF e EF. Essa articulação passa a ser mais presente na BNCC, devido à EF ter se tornado um tema transversal a ser estudado nas escolas. Isso se reflete na indicação de várias habilidades referentes a esses temas. Das 21 habilidades esperadas nas unidades de conhecimento Números e Álgebra, 7 estão ligadas à MF e EF. A saber:

(EM13MAT104) Interpretar taxas e índices de natureza socioeconômica (índice de desenvolvimento humano, taxas de inflação, entre outros), investigando os processos de cálculo desses números, para analisar criticamente a realidade e produzir argumentos.

(EM13MAT203) Aplicar conceitos matemáticos no planejamento, na execução e na análise de ações envolvendo a utilização de aplicativos e a criação de planilhas (para o controle de orçamento familiar, simuladores de cálculos de juros simples e compostos, entre outros), para tomar decisões.

(EM13MAT404) Analisar funções definidas por uma ou mais sentenças (tabela do Imposto de Renda, contas de luz, água, gás etc.), em suas representações algébrica e gráfica, identificando domínios de validade, imagem, crescimento e decrescimento, e convertendo essas representações de uma para outra, com ou sem apoio de tecnologias digitais.

(EM13MAT503) Investigar pontos de máximo ou de mínimo de funções quadráticas em contextos envolvendo superfícies, Matemática Financeira ou Cinemática, entre outros, com apoio de tecnologias digitais.

(EM13MAT303) Interpretar e comparar situações que envolvam juros simples com as que envolvem juros compostos, por meio de representações gráficas ou análise de planilhas, destacando o crescimento linear ou exponencial de cada caso.

(EM13MAT304) Resolver e elaborar problemas com funções exponenciais nos quais seja necessário compreender e interpretar a variação das grandezas envolvidas, em contextos como o da Matemática Financeira, entre outros.

(EM13MAT305) Resolver e elaborar problemas com funções logarítmicas nos quais seja necessário compreender e interpretar a variação das grandezas envolvidas, em contextos como os de abalos sísmicos, pH, radioatividade, Matemática Financeira, entre outros.

Observamos que as três primeiras habilidades citadas indicam justamente a possibilidade de trabalhar os conteúdos da MF em um contexto que se possa explorar a temática da EF. O uso do estudo de funções no contexto da EF também é destacado nessas habilidades. Repare que as habilidades sugerem o trabalho com temas como inflação, orçamento familiar, contas de água e luz, tabela de imposto de renda, entre outros. Temas que são presentes no cotidiano e que reforçam nosso entendimento de como a matemática é muito útil para se relacionar com muitas situações rotineiras. Além disso, faz parte das expectativas na formação do cidadão que ele adquira conhecimentos básicos de economia, política e finanças. Segundo Filho (2019, p. 66):

> A EF não deve estar restrita ao aconselhamento financeiro de como o cidadão deve consumir, poupar ou financiar. A EF vai mais além disso, deve tratar também questões sociais e reflexivas, ligadas a política e economia do país. A EF aliada à MF são ferramentas que em conjunto, podem ser muito úteis para relacionar questões em torno do salário-mínimo, da cesta básica e da inflação, temas esse ligados direta ou indiretamente a questões socioeconômicas.

Já as quatro últimas habilidades citadas se referem à articulação da MF com o ensino de funções. Vale salientar que as habilidades mencionadas são referentes ao ensino médio. Analisando o texto da BNCC que trata do ensino fundamental, encontramos outras habilidades que sugerem esta articulação entre MF e EF. Como, por exemplo: "**(EF07MA02)** Resolver e elaborar problemas que envolvam porcentagens, como os que lidam com acréscimos e decréscimos simples, utilizando estratégias pessoais, cálculo mental e calculadora, no contexto de educação financeira, entre outros"

3.4 Matemática financeira e educação financeira nos livros didáticos (PNLD 2018)

Neste tópico, faremos um breve levantamento de como a MF e EF são abordadas nos livros didáticos (LD) de Matemática do Ensino Médio presentes no Programa Nacional do Livro Didático - 2018. Levamos em conta que esse recurso tem um papel relevante no processo de ensino e de aprendizagem escolar, pois é um dos mais utilizados pelo professor na sala de aula. De modo geral, de acordo com o Guia Nacional do Livro Didático (PNLD) (BRASIL, 2018), as propostas de ensino para o tema MF no Ensino Médio:

> São trabalhadas, com frequência, questões que envolvem porcentagens, acréscimos e descontos, juros simples e compostos, entre outros. Usualmente, para modelizar tais problemas reais, recorre-se às funções afim e exponencial, o que se constitui em uma aplicação prática relevante desses dois tipos de função. De modo geral, tem havido evolução positiva no tratamento desses e de outros temas da denominada Matemática Financeira, superando-se abordagens com ênfase na aplicação direta de fórmulas (BRASIL, 2018, p. 27).

Compreende-se, no entanto, que "são necessários mais esforços para que a abordagem da Matemática Financeira vá um pouco além das noções mais básicas desse campo, e sejam estudados temas como equivalência de taxas, fator de atualização e amortização" (BRASIL, 2018, p. 27). Essas aplicações da Matemática podem favorecer reflexões sobre questões sociais e econômicas relevantes e atuais, que colaboram com a formação crítica dos alunos no que concerne a sua educação financeira.

3.4.1 Organização dos capítulos sobre matemática financeira nos LD

No Quadro 1 podemos visualizar que o capítulo destinado à MF é abordado, sobretudo, no final do EM. Ou seja, cinco das oito coleções o apresentam no livro do terceiro ano, enquanto duas coleções o abordam no segundo ano. A exceção ocorre na coleção do LD5* que traz o tema logo no início do primeiro ano. Vale ainda ressaltar que esta coleção foi a única que não destinou um capítulo exclusivo a esse tema. O assunto é tratado no capítulo 2 do LD5 do 1º ano, juntamente com temas básicos de álgebra.

Quanto aos conteúdos abordados dentro do capítulo Matemática Financeira (Quadro 1), verifica-se que Juros Simples e Compostos são tratados em todas as coleções. Questões que envolvem Porcentagens, Acréscimos e Descontos Sucessivos, também estão presentes na maioria das coleções. A relação entre Juros Simples com Função Afim e a relação entre Juros Compostos com a Função Exponencial é enfatizada nos LD1, LD2, LD6 e LD7 e merece destaque, já que constitui uma aplicação prática e relevante desses dois tipos de função. Como vimos, o próprio guia do PNLD elogia e recomenda essa abordagem, pois vai além das tradicionais aplicações de fórmulas.

Outro assunto que merece destaque nos LD são os sistemas de amortizações, presente como tópico em apenas três das oito coleções (LD1, LD3 e LD6). Os sistemas de amortizações como o PRICE e o SAC são mais utilizados no mercado de empréstimos e financiamentos, do que os próprios regimes de juros simples (quase não é utilizado nos dias atuais) e

Tabela 3.1: Organização dos capítulos de matemática financeira nos LD

LD	Coleções e autores	Ano	Cap	Tópicos
01	Matemática Interação e Tecnologia (BALESTRI, 2016).	2º	8	Matemática Financeira, Acréscimos e descontos sucessivos, juros simples e compostos, juros e funções, amortizações.
02	Contexto & aplicações (DANTE, 2016)	3º	1	História do dinheiro; Matemática Financeira: Porcentagem, Fator de Atualização, Juros Simples e Compostos, juros e funções, Equivalência de taxas.
03	Quadrante Matemática (CHAVANTE; PRESTES, 2016)	2º	7	Matemática financeira: porcentagem, acréscimos e descontos sucessivos; empréstimos: juros simples, juros compostos; sistemas de amortização: Price, amortização constante (SAC).
04	Conexões com a Matemática (LEONARDO, 2016)	3º	1	Matemática financeira: taxa percentual, aumentos e descontos sucessivos, lucro e prejuízo, montante, juro simples, juro composto.
05	Matemática Paiva (PAIVA, 2015) *	1º	2	Matemática financeira: porcentagem, juros simples, juro composto, montante.
06	Contato Matemática (GARCIA; SOUZA, 2016)	3º	1	Matemática financeira: porcentagem, taxa, acréscimos e descontos sucessivos; juros simples e compostos; juros e funções, amortização.
07	Matemática Ciência e Aplicações (IEZZI et al., 2017)	3º	6	Matemática financeira: aumento e descontos, variação percentual, juros simples e compostos e juros compostos com taxa de juros variável; juros e funções.
08	Matemática Para Compreender o Mundo (SMOLE; DINIZ, 2016)	3º	1	Matemática financeira: linguagem, porcentagem, juros simples e compostos.

Fonte: Brasil (2017).

compostos. Sendo assim, julgamos que deveria ser tópico presente em todas as coleções. Outras habilidades no âmbito da MF que julgamos importante por suas utilidades práticas são deixadas de lado pela maioria das coleções; a saber, por exemplo, determinar taxas de juros equivalentes, determinar

taxas acumuladas e fazer simulações em planilhas eletrônicas. Em suma, entendemos que a maior parte dos LD analisados apresentam lacunas na tentativa de estabelecer uma conexão dos conteúdos tratados com a realidade do mercado financeiro.

De modo geral, consideramos que se o aluno consegue compreender a relevância dos tópicos tratados em MF (nos LD ou por meio de outros recursos) como ferramenta para subsidiar decisões importantes no seu dia-a-dia, ele pode demonstrar mais interesse em estudá-los. Fazendo-se, assim, importante que seu contato inicial com o estudo do tema ocorra de modo a fazê-lo perceber a utilidade do que será estudado. Dessa forma, apresentamos a seguir como os LD introduzem o tema MF, visto que essa parte dos LD é aquela em que se percebe uma ênfase dos autores sobre o uso da MF nas práticas cotidianas, como forma de chamar a atenção para a importância do tema, buscando uma aproximação com temáticas da EF.

3.4.2 Introdução do tema

Sobre como os LD introduzem o capítulo de MF, pode ser observado no Quadro 2 a seguir que isso ocorre de maneira bem diversa. Podemos ver que os LD2 e LD6 iniciam o capítulo abordando a origem do dinheiro. Tal abordagem possibilita a articulação entre as áreas de Matemática e História, como é sugerido na BNCC. Essa articulação proposta na BNCC da Matemática com a disciplina de História se faz muito relevante. De acordo com Lopes e Ferreira (2013, p. 1) essa articulação é importante, pois os alunos, "ao conhecerem a história dos conteúdos estudados, percebem a matemática como parte de uma herança cultural, interligada a outras áreas de conhecimentos e a diversas atividades humanas".

Outras introduções que chamam a atenção são a do LD1 e a do LD4. O primeiro trata a questão da responsabilidade financeira, do consumo e da poupança, trazendo alertas ao cuidado com juros e superpromoções. Compreendemos que o texto é útil para se trabalhar a EF, já que remete à formação de comportamentos do indivíduo em relação às finanças. Essa abordagem é relevante, pois pode favorecer o desenvolvimento da criticidade do

Tabela 3.2: Introdução do Capítulo de Matemática Financeira nos LD

Coleção e Autor	Tipo de introdução do Capítulo
LD1 - Matemática Interação e Tecnologia (BALESTRI, 2016).	Diz ser uma responsabilidade financeira, do consumo e da poupança, alertando sobre o cuidado com os juros e superpromoções.
LD2 - Contexto & Aplicações (DANTE, 2016)	Conta uma história do dinheiro e sua relação com a matemática.
LD3 - Quadrante Matemática (CHAVANTE; PRESTES, 2016)	Define o que é Matemática Financeira. Introduzida no estudo de porcentagem com um exemplo revisando o cálculo de porcentagens.
LD4 - Conexões com a Matemática (LEONARDO, 2016)	Apresenta como os impostos são cobrados no Brasil, trabalhando a questão das porcentagens.
LD5 - Matemática Paiva (PAIVA, 2015)	Não possui um capítulo específico para o tema. O assunto aparece na metade do segundo capítulo junto com temas básicos de álgebra.
LD6 - Contato Matemática (GARCIA; SOUZA, 2016)	Apresenta um breve resumo da origem do dinheiro, da época do escambo até os dia atuais.
LD7-Matemática Ciência e Aplicações (IEZZI et al., 2017)	Exemplifica cinco situações-problemas estudadas na matemática financeira. Ex: pagamento de conta telefônica envolvendo multa e juros; financiamento de um automóvel e taxas de juros.
LD8 - Matemática Para Compreender o Mundo (SMOLE; DINIZ, 2016)	Apresenta uma situação-problema envolvendo juros simples e compostos.

Fonte: Autoria própria.

aluno como cidadão, tornando-o capaz de utilizar os seus conhecimentos para decidir sobre opções individuais e coletivas.

Já o LD4 traz como introdução os impostos no Brasil. Esse é um tema que lida diretamente com o bolso do cidadão e com o bem-estar da sociedade. Sendo assim, bem abordado em sala de aula, tende a atrair a atenção dos alunos motivando-os e tornando-os mais conscientes e esclarecidos. Haja vista que o cidadão por muitas vezes, em sua maioria, não tem a noção da quantidade de tributos que paga, mas tem apenas a ideia de que paga muito e que não tem o retorno devido com as suas contribuições. O LD4 traz os principais impostos a que estamos sujeitos (IR, ICMS, IPVA, IPTU etc.) e a porcentagem que cada um gera ao total arrecadado pelo governo.

Também é abordado, na introdução do LD4, o percentual de imposto que pagamos em alguns produtos, além de um infográfico com a evolução dos tributos no nosso país. O conteúdo apresentado enriquece o aluno com

conhecimentos de extrema utilidade, visando sua formação como cidadão crítico. Os dados e informações presentes podem ser usados para elaborar problemas e realizar cálculos de porcentagens, que é um dos objetivos da MF proposto nesse LD (LEONARDO, 2016).

Essa introdução abordada no LD4 é seguramente muito útil no processo de EF. A abordagem trazida na introdução desse capítulo indica como a EF está bastante relacionada com alguns conteúdos matemáticos permitindo que o aluno conheça o sistema tributário do país, o valor da moeda, a importância dos impostos e o modo como são utilizados pelas esferas governamentais. Pode-se, assim, usar a Matemática para subsidiar todas esses assuntos.

Como dito no Quadro 2, o LD7 exemplifica cinco situações problemas estudadas na MF. O manual do professor desse LD destaca a relevância da MF para a formação da cidadania dos estudantes, pois oferece a oportunidade de trabalhar assuntos ligados à EF:

> A importância de poupar, e consumir conscientemente; a importância de pesquisar e comparar preços e condições na hora da compra; os processos que envolvem aumentos e descontos e a variação percentual; a necessidade de estar atento a juros abusivos, cobrados muitas vezes em operações com cartão de crédito; o uso do limite do cheque especial, etc. (IEZZI et al. 2017, p. 294).

De um modo geral, verificamos que, no estudo da MF, alguns dos LD das coleções do PNLD - 2018 buscam, ainda que de forma tímida, a familiarização do leitor com questões ligadas ao processo de EF. Além disso, os LD poderiam explorar mais temas que apresentam uma maior ligação com a realidade do mercado financeiro, como o caso das amortizações, por exemplo. É importante ressaltar que os LD analisados foram aprovados

antes da BNCC entrar em vigor no país, sendo assim, espera-se que os novos LD explorem cada vez mais a temática da EF.

3.5 Considerações finais

Entendemos que a EF é uma ferramenta muito útil para potencializar o ensino da matemática e consequentemente contribuir na formação de cidadãos críticos, cientes de suas responsabilidades sociais. Nos documentos oficiais analisados, verificamos que antes da BNCC a temática EF era pouco explorada e as próprias indicações para o trabalho com MF não apresentavam ligação significativa com a EF. Já a BNCC traz a EF como tema transversal e indica, em algumas habilidades esperadas para o ensino de matemática, sua articulação com a MF. Além disso, na elaboração deste artigo, tivemos a oportunidade de conhecer trabalhos acadêmicos sobre o tema, a maioria trabalhos recentes, indicando que a EF é um tema que vem ganhando espaço nas discussões voltadas para o campo educacional.

Quanto aos LD do Ensino Médio analisados, percebemos que, em sua maioria, eles seguem um roteiro padrão de conteúdos, iniciando os capítulos com uma revisão envolvendo cálculos com porcentagens, tratando, em seguida, de aumentos e descontos percentuais sucessivos, e, na sequência, os conceitos de capital, montante, juros e taxa de juros para introduzir os regimes de juros simples e compostos. Temas complementares como amortizações e equivalências de taxas e que apresentam uma maior conexão com a realidade do mercado financeiro e, por conseguinte, com a realidade que os estudantes devem se deparar na sua vida adulta são deixados de lado na maioria das coleções deste PNLD. Ainda sobre os LD, constatamos que alguns já começam a familiarizar o leitor com questões ligadas ao processo de EF, com questões relevantes, como, por exemplo: impostos no país, consumismo e responsabilidade financeira. Entretanto, vale destacar que os LD do EM consultados, não passaram pelo crivo de avaliação da BNCC, pois na época de elaboração desses livros a mesma ainda não estava em vigor no país. A BNCC passa a dar uma ênfase maior à EF, tratando-a como

tema transversal no currículo escolar. Tivemos a oportunidade de ter acesso às coleções de livros de matemática do Ensino Fundamental aprovadas no PNLD 2020. No pouco contato que tivemos com essas coleções, pudemos constatar que, de fato, a EF é uma temática muito explorada. Algumas coleções trazem a EF em seções recorrentes dentro dos capítulos. Isso indica que os novos LD de matemática para o ensino médio devam seguir com essa tendência que é um dos parâmetros exigidos pela BNCC.

3.6 Referências bibliográficas

BALESTRI, R. **Matemática: interação e tecnologia. v.2.** São Paulo: Leya, 2016.

BRASIL. **Base Nacional Comum Curricular.** Brasília: Ministério de Educação, 2018. Disponível em: <http://basenacionalcomum.mec.gov.br/wpcontent/uploads/2018/12/BNCC_19dez2018_site.pdf>. Acesso em: 08 fev. de 2019.

BRASIL. **Guia de Livros Didáticos do Programa Nacional do Livro Didático (PNLD 2018). Brasília: 2017.** Disponível em: <http://www.fnde.gov.br/pnld-2018>. Acesso em: 20 jan. 2019.

BRASIL. **Instituto Nacional de Estudos e Pesquisas Educacionais. Sistema de Avaliação da Educação Básica (Saeb): evidências da edição 2017.** Brasília: INEP, 2018.

BRASIL. **Lei de Diretrizes e Bases da Educação Nacional.** Lei número 9.394, 20 de dezembro de 1996.

BRASIL, Ministério da Educação. Secretaria de Educação Média e Tecnológica (Semtec). **Parâmetros Curriculares Nacionais para o Ensino Médio,** Brasília: 1999. Disponível: <http://portal.mec.gov.br/seb/arquivos/pdf/ciencian.pdf>. Acesso em: 26 jul. 2019.

BRASIL. **Orientações Curriculares para o Ensino Médio. Ciências da Natureza, Matemática e suas Tecnologias.** Brasília: Ministério de Educação, 2006. BRASIL. **Parâmetros Curriculares Nacionais:**

Matemática: 3o e 4o ciclos do ensino fundamental. Brasília: MEC, 1998.

BRASIL. PCN + Ensino Médio. **Orientações Educacionais Complementares aos Parâmetros Curriculares Nacionais. Ciências da Natureza, Matemática e suas Tecnologias.**Brasília: Ministério de Educação, 2002.

CHAVANTE, E.; PRESTES, D. **Quadrante Matemática.** v.2. São Paulo: SM, 2016.

DANTE, L.R. **Matemática: contexto aplicações. v.3.** São Paulo: Ática, 2017.

FILHO, E. **Educação Matemática Crítica: Uma sequência didática para o ensino de matemática e educação financeira a partir do tema Inflação.** 2019, 117f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional). Universidade Federal Rural de Pernambuco, Recife, 2019. GARCIA, J; SOUZA, J. **Contato matemática.** v.3. São Paulo: FTD, 2016.

IEZZI, G.etal. **Matemática: Ciência e aplicações.v.3.** São Paulo: Saraiva, 2017.

LEONARDO, F.M. **Conexões com a matemática. v.3.** São Paulo: Moderna, 2016.

LOPES, L.S.; FERREIRA A.L.A. **Um olhar sobre a história nas aulas de matemática.** Abakós, Belo Horizonte, v. 2, n. 1, p. 75–88, nov. 2013.

MUNIZ, I. Jr.; JURKIEWICZ,S. **Educação Financeira: uma nova concepção para o ensino médio.** In: COLÓQUIO DE HISTÓRIA E TECNOLOGIA NO ENSINO DA MATEMÁTICA, V., 2010, Recife. Anais...: Recife: SBEM, 2010. p. 1-12.Disponível em:<http://www.lematec.net.br/CDS/HTEM10/pdfs/C21.pdf.> Acesso em:15 mar.2019.

PAIVA, M. **Matemática Paiva. Ensino Médio. v.1.** São Paulo: Moderna, 2015.

PERNAMBUCO. **Parâmetros para a Educação Básica do Estado de Pernambuco.** Matemática. Recife: Secretaria de Educação, 2012.

PESSOA, C.A.S. Educação financeira na perspectiva da educação matemática crítica em livros didáticos de matemática dos anos iniciais do ensino fundamental. In: ENCONTRO NACIONAL DE EDUCAÇÃO

MATEMÁTICA, XII.,2016, São Paulo. Anais...São Paulo: SBEM, 2016. p. 1- 12.Disponível:
<http://www.sbem.com.br/enem2016/ anais/pdf/$5176_2681_ID.pdf$. > *Acesso*
em : 20*deabri*.2019.*SMOLE*, *K.S.*; *DINIZ*, *M.I.Matemtica* : *EnsinoMdio.v.*3.
SoPaulo : *Saraiva*, 2016.

Capítulo 4

Códigos corretores de erros no ensino médio: um estudo sobre o código de Hamming

Me. Everton Henrique Cardoso de Lira[1]
Dra. Márcia Pragana Dantas[2]

Resumo: Os Códigos Corretores de Erros são um tema de bastante utilidade em diversas aplicações tecnológicas nas engenharias, por exemplo, e em pesquisas na área da matemática aplicada. Embora o tema seja amplamente abordado em pesquisas matemáticas acadêmicas, o mesmo ainda é pouco explorado em nível da Educação Básica, mais precisamente, no Ensino Médio. Por esse motivo, no presente trabalho, nos propomos a contribuir com a inserção desse importante assunto na esfera do Ensino Básico. Dessa forma, realizamos uma apresentação do Código de Hamming elementar e acessível para professores do Ensino Médio, partindo de sua formulação original, proposta pelo autor em 1950, e, em seguida, apresentando esse código do ponto de vista matricial, tendo em vista o seu ensino

[1]Universidade Federal de Pernambuco/Secretaria de Educação de Pernambuco, everton.ufpe@hotmail.com
[2]Universidade Federal Rural de Pernambuco, marcia.dantas@ufrpe.br

em nível básico. Por fim, indicamos outra leitura sobre o tema, na qual apresentamos uma sequência didática para o ensino dos Códigos Corretores de Erros no Ensino Médio.

Palavras-chave: Códigos Corretores de Erros; Código de Hamming; Ensino Médio.

4.1 Introdução

A Teoria dos Códigos Corretores de Erros é, grosso modo, o ramo da matemática que estuda os problemas relacionados com o processo de transmissão e recepção de informações digitais, bem como o papel do erro nesse processo. De acordo com Hefez (2018), um Código Corretor de Erros consiste em um procedimento para a transmissão de informações, no qual a introdução sistemática de informação redundante a uma informação prévia que se deseja transmitir é realizada, de forma que a informação redundante seja utilizada posteriormente na detecção e correção dos possíveis erros ocorridos durante a transmissão.

Tais códigos são um dos grandes responsáveis pelo bom funcionamento de tecnologias que fazem parte do nosso cotidiano como, por exemplo, televisores, smartphones, computadores, música digital, internet, dentre outros. Mais ainda, suas aplicações podem ser vistas nas mais diversas áreas da ciência, tais como Engenharia Elétrica (GUIMARÃES, 2003); Biologia (ROCHA, 2010; FARIA, 2011); Computação Quântica (AGUIAR, 2010) e Criptografia (BOLLAUF, 2015). A importância dos Códigos Corretores de Erros pode ser vista também através da atenção que tem sido dada a sua divulgação para um público mais amplo do que a comunidade acadêmica. Consideremos, por exemplo, as obras de divulgação matemática de Milies (2008), Stewart (2013) e Ellenberg (2015, p. 301-325), que trazem o tema de forma mais intuitiva e informal, ou Shine (2009), Sá e Rocha (2012) e Rousseau e Aubin (2015), que apresentam abordagens um pouco mais técnicas, porém elementares.

No que diz respeito às pesquisas acadêmicas advindas do PROFMAT,

o assunto já foi abordado por: Miranda (2013), no qual se destaca o foco dado ao problema do "empacotamento de esferas"; Carvalho (2014), como campo da matemática no qual os conceitos de Matrizes, Determinantes e Polinômios são aplicados; Alves (2015), como contexto para o estudo de Aritmética e Matrizes no Ensino Médio; Nicoletti (2015), em que o autor destaca a relação entre o assunto e a Álgebra Linear, assim como a importância de se introduzir ideias básicas do mesmo no Ensino Médio; Pinz (2013) e Machado (2016), nos quais o tema é abordado através do conceito de dígitos verificadores, utilizados em códigos de barra, no CPF, em cartões de crédito, dentre outros; Dias (2017), no qual o autor apresenta uma aplicação dos Códigos Corretores de Erros realizada pela NASA em 1971 na Missão Mariner; Rodrigues (2017), em que os diagramas de Venn são inteligentemente utilizados para introduzir o assunto no Ensino Básico; e, finalmente, Schroeder (2017), no qual truques de mágica são realizados através da utilização de alguns Códigos Corretores de Erros.

Isso nos sugere o surgimento de uma tendência de introdução e adaptação deste assunto para a sua futura abordagem no Ensino Médio, uma vez que, o mesmo consiste em um rico tema para a contextualização de assuntos como Matrizes, Determinantes, Polinômios, Aritmética Binária, dentre outros assuntos relevantes para este nível de ensino. Decorre daí que, entendemos ser relevante para os professores de matemática do Ensino Básico, a devida compreensão do que são estes códigos, para que em sua atuação nas salas de aula, os mesmos sejam capazes de abordá-los de forma clara e adequada para este nível de ensino. Além disso, entendemos que propostas como esta possuem potencial para serem geradoras de outras propostas na mesma direção, o que no futuro, pode consolidar os Códigos Corretores de Erros como um tema de ensino e estudo na Educação Básica, o que dentre outras coisas, representaria uma renovação e modernização nos conteúdos abordados nos currículos de matemática da Educação Básica.

Tendo em vista que os estudos sobre os Códigos Corretores de Erros têm abordado o tema através de variados enfoques e de perspectivas diversas, neste trabalho optamos por dar um enfoque ao assunto de forma que dele possam advir contribuições relevantes para o ensino da matemática a nível

básico. Assim, nossa escolha recaiu sobre o *Código de Hamming*, desenvolvido em 1950 pelo matemático e engenheiro americano Richard Wesley Hamming (1915 - 1998). Um dos motivos para tal escolha deveu-se ao fato desse código apresentar papel de destaque no desenvolvimento inicial dos primeiros Códigos Corretores de Erros, conforme aponta Abrantes (2003), bem como pelas possibilidades de abordagem do assunto, que acreditamos possíveis de serem realizadas no Ensino Médio.

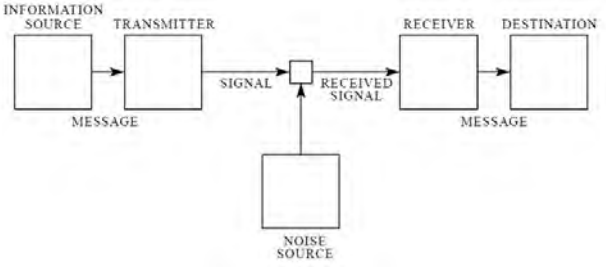
4.2 Teoria da informação e códigos corretores de erros

Os Códigos Corretores de Erros estão intimamente relacionados com a chamada Teoria da Informação, a qual foi inicialmente desenvolvida pelo matemático americano Claude Elwood Shannon (1916 - 2001), em seu clássico trabalho *A Mathematical Theory of Communication* (SHANNON, 1948). Nesse trabalho, Shannon estudou o problema fundamental da comunicação, que segundo ele "é o de reproduzir em um ponto exatamente ou aproximadamente uma mensagem selecionada em outro ponto" (SHANNON, 1948, p. 1, tradução nossa). Para isso, ele definiu inicialmente uma *unidade de medida de informação*, que chamou de *bit* (abreviação de *binary digit*) e um *sistema de comunicação*, o qual é formado basicamente por cinco componentes, a saber: *uma fonte de informação*, que produz a mensagem a ser transmitida; *um transmissor*, que atua sobre a mensagem produzindo um sinal passível de ser transmitido; *um canal*, que consiste basicamente no meio utilizado para transmitir o sinal do transmissor até o receptor; *um receptor*, que decodifica o sinal recebido na mensagem enviada pelo transmissor; e *um destino*, que é a pessoa ou equipamento que recebe a mensagem enviada[3]

Tais conceitos foram amplamente utilizados e aproveitados para o estabelecimento da Teoria dos Códigos Corretores de Erros por dois motivos.

[3]Para maiores detalhes sobre os componentes de um sistema de informação, ver Shannon (1948, p. 2) e Gleick (2013, p. 231).

Figura 4.1: Sistema de informação



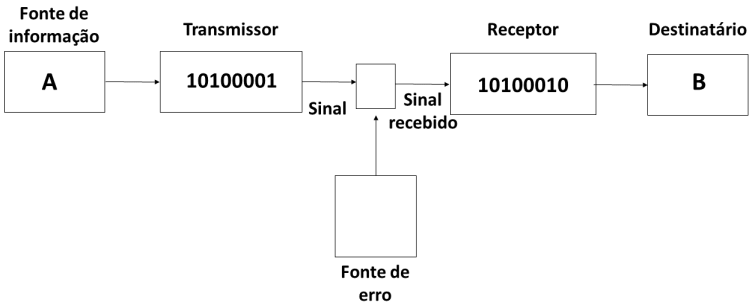
Fonte: Shannon (1948, p. 2).

O primeiro foi o fato de o bit ser adotado como a unidade de medida para a informação, possibilitando, assim, o tratamento científico da informação, o que já ocorria há séculos com outras grandezas, como, por exemplo, as físicas. O segundo foi a sistematização do processo de comunicação, o que, dentre outras coisas, possibilitou uma ampla compreensão de como o erro interfere nesse processo, como também levou Shannon a mostrar que "existe um limite fundamental de quanta informação um canal de comunicação pode transportar" (STEWART, 2013, p. 327). A partir dessa constatação, os cientistas da área buscaram desenvolver métodos e códigos eficientes para a transmissão de informações em suas mais diversas formas, sem, contudo, se preocuparem com a quantidade máxima de informação que um canal poderia transportar, visto que este problema já estava resolvido.

Sobre o papel do erro no processo de comunicação, o diagrama da Figura 4.1 nos mostra que, entre a transmissão e a recepção de uma dada mensagem, pode ocorrer um ruído, ou seja, uma interferência que eventualmente modifica o sentido da mensagem original, causando, assim, um erro de comunicação. Foi precisamente a identificação da presença do ruído interferindo na transmissão de mensagens que levou Shannon e seus companheiros à busca de uma solução para este problema. Essa busca também contribuiu no desenvolvimento dos Códigos Corretores de Erros, cuja função é, como o nome já sugere, impedir, por meio da correção de erros, que a mensagem original tenha seu sentido distorcido após o seu envio.

Por exemplo, a ação do erro na transmissão de um símbolo do código ASCII[4] pode ser representada pelo diagrama de Shannon abaixo. Neste caso, a letra A é codificada pelo símbolo 10100001 e a letra B por 10100010. O erro aqui ocorreu porque os últimos dois dígitos do símbolo enviado foram permutados, o que resultou na transmissão da letra A e da recepção da letra B:

Figura 4.2: Exemplo de erro



Fonte: Ilustração do autor.

4.2.1 O código de Hamming

Um dos pioneiros na pesquisa e no desenvolvimento dos Códigos Corretores de Erros foi o matemático americano Richard Hamming, o qual, em abril de 1950, publicou no *The Bell System Technical Journal* o artigo *Error Detecting and Error Correcting Codes* (HAMMING, 1950). Nesse artigo, conceitos fundamentais para a Teoria dos Códigos Corretores de Erros, como *métrica, redundância, equivalência de códigos e códigos sistemáticos*, por exemplo, foram primeiramente enunciados e abordados. Hamming também explica que a motivação para o estudo foi a necessidade de se resolver o problema que inevitavelmente surge no processamento de uma dada tarefa por uma máquina como um computador, a saber, os eventuais erros que ocorrem na realização da tarefa. Sobre o erro presente em um cálculo realizado por um computador, ele afirmou:

[4]Do inglês: *American Standard Code for Information Interchange*

> uma única falha geralmente significa o fracasso completo, no sentido de que se ela é detectada nenhum cálculo pode ser realizado até a falha ser localizada e corrigida, enquanto que se ela escapa da detecção então ela invalida todas as operações posteriores da máquina (HAMMING, 1950, p. 147, tradução nossa).

Dessa forma, o operador ou usuário de tal máquina se vê diante de um impasse. Se um erro ocorrer e for detectado, então a máquina não funciona até o erro detectado ser corrigido, tarefa que, na época, não era realizada em pouco tempo e sem pouco trabalho. Por outro lado, se um erro ocorrer e não for detectado, os cálculos realizados não serão úteis, pois foram afetados pelo erro, que comprometerá o resultado final de todo o trabalho realizado.

Foi justamente neste novo e pouco explorado contexto que Hamming se encontrava em 1947, enquanto trabalhava com os computadores dos laboratórios Bell. Nessa época, a utilização dos computadores da empresa era bastante restrita e disputada por seus pesquisadores, de forma que Hamming só tinha acesso aos mesmos nos finais de semana. Foi nessas pesquisas de "final de semana" quando ele percebeu que as máquinas por ele utilizadas eram capazes de detectar os erros em sua programação, entretanto isso não o ajudava em nada, pois as máquinas não possuíam a capacidade de corrigir tais erros.

Em entrevista dada em 1977, ele explica a situação em que se encontrava na época, e que, em grande parte, foi um dos motivos que o levaram a trabalhar no desenvolvimento dos Códigos Corretores de Erros:

> Em dois finais de semanas consecutivos eu fui e descobri que todas minhas coisas tinham sido descarregadas e nada tinha sido feito. Eu estava realmente aborrecido e irritado porque queria estas respostas e tinha perdido dois finais de semana. E então eu me disse "Maldição, se as máquinas podem detectar um erro, porque não podemos localizar a posição do erro e corrigi-lo"(MILLIES, 2009, p. 2).

Ao lermos o artigo de Hamming, fica claro que era com o objetivo de compreender e fazer bom uso da correção de erros que ele passou a estudar o problema da sua detecção e posterior correção, uma vez que o problema da simples detecção de erros já estava resolvido na época, como ele mesmo afirma: "parece desejável examinar o próximo passo além da detecção do erro, nomeadamente correção do erro" (HAMMING, 1950, p. 148, tradução nossa). Para desenvolver sua teoria, Hamming elabora alguns conceitos que o ajudarão nessa tarefa. A essência de tais conceitos está presente nas Definições 1, 2 e 3, a seguir:

Definição 1. *Sejam A um conjunto finito não vazio, o qual será chamado de alfabeto, e $|A|$ o seu número de elementos. Um código corretor de erros C é um subconjunto próprio qualquer de A^n, para algum n natural. Um elemento $c \in C$ é chamado um símbolo do código.*

Da definição acima decorre que, dado um conjunto finito não vazio A qualquer, podemos, a partir dele, definir quantos Códigos Corretores de Erros desejarmos, sendo tal construção limitada apenas por nossa criatividade e disposição. Por exemplo, se escolhermos como alfabeto o conjunto $A = \{0,1,2,3,4,5,6,7,8,9\}$, temos que $|A| = 10$ e o seu número de identidade é um símbolo do conjunto $C \subset A^9$, em que C é um Código Corretor de Erros. Agora, se o conjunto A escolhido for o nosso alfabeto, então o conjunto $C \subset A^{46}$, formado por todas as palavras do nosso idioma, também é um Código Corretor de Erros.[5] Por fim, os códigos de barras dos produtos que compramos, o registro de livros ISBN e o número do nosso CPF, são todos exemplos de Códigos Corretores de Erros cujo alfabeto também é $A = \{0,1,2,3,4,5,6,7,8,9\}$ e cujos símbolos estão no conjunto A^{13}, para os dois primeiros, e A^{11}, para o último.

Uma pergunta que pode surgir após esses exemplos é: Como corrigir os erros nesses códigos? Essa pergunta não possui uma única resposta. Nos casos dos números de identidade e das palavras do nosso idioma, por exemplo, a repetição de um símbolo ao transmiti-lo consiste num

[5]Nesse exemplo, consideramos que a maior palavra na língua portuguesa é Pneumoultramicroscopicossilicovulcanoconiótico, a qual, como pode ser visto, possui 46 letras.

procedimento que permite a correção de erros, porém a repetição nem sempre é o procedimento mais eficaz possível. Já para os códigos de barra, o ISBN e o CPF, existem procedimentos matemáticos um pouco mais sofisticados para a detecção e correção dos eventuais erros. Para os interessados em como esses procedimentos funcionam, ver Sá e Rocha (2012).

Sendo assim, surge aqui a necessidade de se buscar procedimentos mais eficazes para a detecção e correção de erros, tarefa essa que nem sempre é simples, principalmente quando trabalhamos com alfabetos com muitos símbolos, como os exemplos acima. Para resolver e evitar este tipo de problema, Hamming escolheu trabalhar com códigos cujos símbolos fossem compostos por sequências numéricas contendo apenas 0's e 1's em seus dígitos. Alguns desses dígitos serão utilizados para transmitir a informação desejada e outros serão utilizados para a detecção e correção dos eventuais erros. Essa escolha nos leva para a próxima Definição:

Definição 2. *Sejam C um Código Corretor de Erros e n, m e k números naturais com $n > m$. Dizemos que C é sistemático quando cada símbolo de C tem exatamente n dígitos binários, dos quais m são associados com a informação, enquanto os $k = n - m$ dígitos restantes são utilizados para a detecção e correção de erros.*

Ao se escolher trabalhar com códigos sistemáticos, nos vemos diante da seguinte pergunta: Dados dois códigos sistemáticos C e C', como decidir qual dos dois é o mais eficiente? Entendendo mais eficiente por aquele que transmite a maior quantidade de informação m, dado um valor para o comprimento dos símbolos n, ou, equivalentemente, transmite uma determinada quantidade m de informação com o menor valor possível de n. Para responder essa pergunta, Hamming propôs a seguinte definição:

Definição 3. *Sejam C um código e n e m naturais. A redundância R do código C é a razão entre o número de dígitos binários utilizados e o número mínimo necessário para transmitir a mesma informação, ou seja, $R = \frac{n}{m}$. Note que a redundância é um número maior ou igual a 1.*

A partir de agora vamos trabalhar com códigos considerando a menor redundância possível, pois essa escolha é exatamente a que Hamming faz em seu artigo. Vale destacar que sempre é possível obtermos tais códigos, que chamaremos de *códigos de redundância mínima*, uma vez que, como será visto posteriormente, m e n estão bem definidos. Além disso, salvo menção contrária, sempre usaremos $A = \{0, 1\}$.

Na primeira parte de seu artigo, Hamming apresenta a construção de códigos de redundância mínima em três casos específicos, a saber:

(1) Códigos *detectores* de um único erro;

(2) Códigos *corretores* de um único erro;

(3) Códigos *corretores* de um único erro, além de *detectores* de erros duplos.

Nas próximas subseções, detalharemos os casos (1) e (2). O caso (3) não será considerado, pois o mesmo consiste simplesmente na aplicação do algoritmo apresentado no caso (1) em um código elaborado conforme o algoritmo apresentado no caso (2). Dessa forma, no caso (3), corrigimos um erro e detectamos dois, um pelo algoritmo em (1) e um pelo algoritmo em (2). Em suma, sempre que falarmos nos códigos dos casos (1) e (2), teremos em mente as seguintes definições:

Definição 4. *Um código C é dito detector de um único erro quando, na transmissão de um dado símbolo $c \in C$, um único erro ocorrido em apenas uma de suas posições pode ser detectado.*

Definição 5. *Um código C é dito corretor de um único erro quando, na transmissão de um dado símbolo $c \in C$, um único erro ocorrido em apenas uma de suas posições pode ser detectado e corrigido pela troca de 0 por 1 ou vice versa.*

4.2.2 Códigos detectores de um único erro

Para o caso mais simples, ou seja, os códigos detectores de um único erro, Hamming propõe o seguinte algoritmo, chamado de *verificação de*

paridade, para a codificação de um símbolo composto de uma lista com n 0's e 1's:

Algoritmo 1. *Nas primeiras $n-1$ posições, nós colocamos $n-1$ dígitos de informação. Na n-ésima posição, nós colocamos outro 0 ou 1, de modo que as n posições completas tenham um número par de 1's.*

Note que o algoritmo acima é claramente um código detector de um único erro, uma vez que um único erro na transmissão deve levar a um número ímpar de 1's nos símbolos do código, o que nos permitirá concluir imediatamente que, de fato, a transmissão foi afetada pelo erro. Esse código é denotado por $C(n,n-1)$ ou $C(n,m)$, em que n é a quantidade de posições dos símbolos do código e m é a quantidade de posições que contém a informação. É possível observar abaixo um exemplo de como este algoritmo de codificação/decodificação funciona para o caso do código $C(8,7)$.

Exemplo 1. *Considerando a Tabela 4.1 a seguir, note que, com respeito aos 7 dígitos de informação, as duas primeiras linhas da tabela contêm um número ímpar de 1's. Portanto, antes de transmitir os símbolos 1000110 e 0010110 presentes nessas linhas, devemos adicionar, na 8ª posição, o dígito 1, para que a quantidade de 1's seja par, resultando nos símbolos codificados 10001101 e 00101101. Por outro lado, os símbolos nas duas últimas linhas contêm um número par de 1's nas 7 posições de informação. Assim, antes de transmitir os símbolos 0111010 e 1010011 presentes nestas linhas, devemos adicionar, na 8ª posição, o dígito 0, para que a quantidade de 1's seja par, resultando nos símbolos codificados 01110100 e 10100110. Dessa forma, se na transmissão o receptor receber um símbolo com um número ímpar de 1's, ele pode concluir que ocorreu um erro na transmissão.*

Cabe notar aqui que, como $R = \frac{n}{m} = \frac{n}{n-1} = 1 + \frac{1}{n-1}$, poderíamos supor que, para obtermos uma redundância cada vez menor, deveríamos tornar o valor de n cada vez maior. Porém o que ocorre ao se aumentar o valor de n é o indesejável aumento na probabilidade de ocorrência de erros na transmissão dos símbolos. Em suas palavras, Hamming explica: "se

Tabela 4.1: Funcionamento do código $C(8,7)$, detector de um único erro.

Dígitos de informação							**Dígito de verificação**
1	0	0	0	1	1	0	1
0	0	1	0	1	1	0	1
0	1	1	1	0	1	0	0
1	0	1	0	0	1	1	0

Fonte: Elaborada pelo autor.

$p \ll 1$ é a probabilidade de algum erro, então para n tão grande como $\frac{1}{p}$, a probabilidade de um símbolo correto é aproximadamente $\frac{1}{e} = 0,3679\ldots$, enquanto um erro duplo tem probabilidade $\frac{1}{2e} = 0,1839\ldots$." (ibid, p. 150). Como os erros duplos não são detectados por esse código, ocorre que existe uma probabilidade de aproximadamente $18,4\%$ de surgirem erros duplos passando pelo sistema, ou seja, quase um em cada cinco símbolos sendo transmitidos com erros e, pior ainda, não detectados.

Antes de passar para o próximo tipo de código, vale ressaltar que o código do exemplo acima é, de acordo com a Definição 1, um subconjunto de A^8, em que A, como já dissemos, é o conjunto $\{0,1\}$. Além disso, a redundância desse código é $R = \frac{n}{m} = \frac{8}{7} \approx 1,14$, o que, em termos práticos, significa que a transmissão dos $2^7 = 128$ símbolos desse código após sua codificação é equivalente à transmissão de $128 \times \frac{8}{7} \approx 146$ símbolos do mesmo código se eles não fossem codificados. Por esse motivo, trabalhamos com códigos com redundância mínima, pois eles possibilitam uma maior economia de dados na transmissão de uma dada informação.

4.2.3 Códigos corretores de um único erro

No caso dos códigos corretores de um único erro, Hamming desenvolve dois algoritmos. Um será utilizado para a *codificação* e outro será utilizado para a *detecção, correção* e *decodificação* de um erro em uma sequência binária de n posições, das quais m são escolhidas para conter a informação e as outras k restantes, em que k é tal que $k = n - m$, são escolhidas para a *verificação de paridade*. A relação entre n, m e k é dada pela Tabela 4.2,

que apenas utilizaremos aqui, deixando a sua construção para a subseção 2.4 (Proposição 1). No próximo exemplo, adaptado de Hefez (2008, p. 2), mostraremos como a Tabela 4.2 é utilizada na codificação de comandos para a movimentação de um robô que se move em 4 direções sobre um tabuleiro.

Tabela 4.2: Relação entre n, m e k.

n	m	k correspondente
1	0	1
2	0	2
3	1	2
4	1	3
5	2	3
6	3	3
7	4	3
8	4	4
9	5	4
10	6	4
11	7	4
12	8	4
13	9	4
14	10	4
15	11	4
16	11	5
	Etc.	

Fonte: Hamming (1950, p. 151).

Exemplo 2. *Considere um robô que se move sobre um tabuleiro quadriculado de modo que, ao darmos um dos comandos (Leste, Oeste, Norte ou Sul), o robô se desloca do centro de uma casa para o centro da casa contígua indicada pelo comando.*
Se definirmos estes comandos por: Leste $\longmapsto 00$*, Oeste* $\longmapsto 01$*, Norte* $\longmapsto 10$ *e Sul* $\longmapsto 11$*, a Tabela 4.2 mostra que* 2 *dígitos de informação* ($m = 2$)*, exigem* 3 *dígitos de verificação* ($k = 3$)*, logo, os símbolos codificados terão* 5 *posições* ($n = 5$)*.*

Segue daí que uma codificação para estes comandos é a dada por: $00 \longmapsto 00\mathbf{0}0\mathbf{0}$, $01 \longmapsto 10\mathbf{0}1\mathbf{1}$, $10 \longmapsto 11\mathbf{1}0\mathbf{0}$ e $11 \longmapsto 01\mathbf{1}1\mathbf{1}$. Em que os dígitos destacados em negrito (informação) são os comandos originais do robô pré-codificação, e os outros dígitos que aparecem sem negrito (redundância) estão todos em posições que são potências de 2. Essa não é a única forma de codificar os comandos do robô, mas, como veremos à seguir (Algoritmo 2), é uma que permite a detecção e correção de um único erro. De fato, a ocorrência de um único erro antes da codificação, como, por exemplo, o envio de 00 ao invés de 01, faria com que o robô se movimentasse na direção oposta à que queríamos que ele fosse, porém, após a codificação, a ocorrência de um único erro não gera tal situação e, mais ainda, é passível de ser corrigida, como veremos a seguir.

Num primeiro momento, o leitor pode pensar que a escolha dessa codificação particular foi feita de forma arbitrária, mas, ao contrário do que pode parecer, a mesma foi realizada seguindo um algoritmo definido em Hamming (1950), o qual exemplificaremos a seguir e generalizaremos no Algoritmo 2.

Em seu algoritmo de codificação, Hamming afirma que as posições de verificação devem estar localizadas em potências de 2, ou seja, as posições de verificação serão a 1ª, 2ª e 4ª, como vimos no Exemplo 2. Por questões de melhor entendimento, chamaremos essas posições de v_1, v_2 e v_4 e destacaremos, em negrito, os símbolos $00, 01, 10, 11$, de sorte que tais símbolos, ao serem codificados, serão escritos como: $v_1v_2\mathbf{0}v_4\mathbf{0}$, $v_1v_2\mathbf{0}v_4\mathbf{1}$, $v_1v_2\mathbf{1}v_4\mathbf{0}$ e $v_1v_2\mathbf{1}v_4\mathbf{1}$. Para determinar v_1, v_2 e v_4, seguiremos o seguinte algoritmo:

- Para a codificação do símbolo $\mathbf{00}$ em $v_1v_2\mathbf{0}v_4\mathbf{0}$, v_1 será escolhido de forma que a soma $v_1 + \mathbf{0} + \mathbf{0}$ seja par; v_2, de forma que a soma $v_2 + \mathbf{0}$ seja par; e v_4, de forma que a soma $v_4 + \mathbf{0}$ seja par. Logo, teremos $v_1 = 0, v_2 = 0$ e $v_4 = 0$ e o símbolo codificado será $00\mathbf{0}0\mathbf{0}$.

- Para a codificação do símbolo $\mathbf{01}$ em $v_1v_2\mathbf{0}v_4\mathbf{1}$, v_1 será escolhido de forma que a soma $v_1 + \mathbf{0} + \mathbf{1}$ seja par; v_2, de forma que a soma $v_2 + \mathbf{0}$ seja par; e v_4, de forma que a soma $v_4 + \mathbf{1}$ seja par. Logo, teremos $v_1 = 1, v_2 = 0$ e $v_4 = 1$ e o símbolo codificado será $10\mathbf{0}1\mathbf{1}$.

- Para a codificação do símbolo **10** em $v_1v_2\mathbf{1}v_4\mathbf{0}$, v_1 será escolhido de forma que a soma $v_1+\mathbf{1}+\mathbf{0}$ seja par; v_2, de forma que a soma $v_2+\mathbf{1}$ seja par; e v_4, de forma que a soma $v_4+\mathbf{0}$ seja par. Logo, teremos $v_1=1, v_2=1$ e $v_4=0$ e o símbolo codificado será 11**10**0.

- Para a codificação do símbolo **11** em $v_1v_2\mathbf{1}v_4\mathbf{1}$, v_1 será escolhido de forma que a soma $v_1+\mathbf{1}+\mathbf{1}$ seja par; v_2, de forma que a soma $v_2+\mathbf{1}$ seja par; e v_4, de forma que a soma $v_4+\mathbf{1}$ seja par. Logo, teremos $v_1=0, v_2=1$ e $v_4=1$ e o símbolo codificado será 01**11**1.

Assim, obtemos os símbolos codificados do Exemplo 2. Vejamos, agora, o caso geral para um símbolo $v_1v_2d_3v_4d_5d_6d_7v_8\cdots$ codificado a partir do símbolo $d_3d_5d_6d_7\cdots$.

Algoritmo 2. ***(Codificação)*** *Para determinar v_1, some os valores dos dígitos nas posições $1,3,5,7,\cdots$ de forma que a soma seja par, ou seja, "escolha" um dígito e "pule" um dígito a partir da 1ª posição. Para determinar v_2 some os valores dos dígitos nas posições $2,3,6,7,10,11,\ldots$ de forma que a soma seja par, ou seja, "escolha" dois dígitos e "pule" dois dígitos a partir da 2ª posição. Para determinar v_4 some os valores dos dígitos nas posições $4,5,6,7,12,13,14,15,\cdots$ de forma que a soma seja par, ou seja, "escolha" quatro dígitos e "pule" quatro dígitos a partir da 4ª posição. Este algoritmo continua até que sejam percorridas todas as posições nas potências de 2 do símbolo, sempre "escolhendo" e "pulando" dígitos nas potências de dois.*

Suponha agora, que, ao enviarmos o comando para o robô se movimentar para o norte, tenha ocorrido um erro e, ao invés de ser transmitido o símbolo 11100, tenha sido transmitido o símbolo 11000, com um erro na terceira posição. Como verificar e corrigir esse erro? Hamming nos responde com mais um algoritmo.

Algoritmo 3. ***(Decodificação e correção)*** *Vamos imaginar por um momento, que recebemos um símbolo de código, com ou sem um erro. Vamos aplicar as k verificações de paridade em ordem, e, para cada vez que a*

verificação de paridade especificar o valor observado em sua verificação de posição, escreveremos um 0, enquanto que, para cada vez que os valores especificado e observado diferirem, escreveremos um 1. Quando escrevermos, da direita para a esquerda, em uma linha, esta sequência de k 0's e 1's [...] ela poderá ser considerada como um número binário e será chamada de um número de verificação. Vamos exigir que esse número de verificação dê a posição de um único erro, com o valor zero significando nenhum erro no símbolo (HAMMING, 1950, p. 150, tradução nossa).

Vamos agora aplicar o Algoritmo 3 no símbolo 11000 e constatar que de fato o erro está na 3ª posição. Com efeito, para esse símbolo temos $v_1 = 1, v_2 = 1$ e $v_4 = 0$, de maneira que:

- A primeira verificação de paridade é realizada nas posições $1, 3$ e 5, logo, para que $v_1 + 0 + 0$ seja par, v_1 tem que ser igual a zero, o que não confere com o valor de v_1. Assim, essa verificação contribui com um 1 na sequência do número de verificação.

- A segunda verificação de paridade é realizada nas posições 2 e 3, de sorte que, para que $v_2 + 0$ seja par, v_2 tem que ser igual a zero, o que não confere com o valor de v_2. Assim, essa verificação também contribui com um 1 na sequência do número de verificação.

- A terceira e última verificação de paridade é realizada nas posições 4 e 5, de maneira que, para que $v_4 + 0$ seja par, v_4 tem que ser igual a zero, o que confere com o valor de v_4. Assim, essa verificação contribui com um 0 na sequência do número de verificação.

Escrevendo essa sequência como indicado no Algoritmo 3, obtemos a sequência 011, que pode ser identificada com o número 011 na base 2, que é igual a 3 na base 10. Dessa maneira, o erro se encontra na 3ª posição, como já era de se esperar. Na próxima subseção, explicaremos com detalhes por que esse algoritmo funciona e por que a sequência obtida representa, de fato, a posição onde se encontra o erro. Consideremos, agora, um exemplo em que o robô do Exemplo 2 é atualizado para se movimentar em mais quatro direções:

Exemplo 3. *Suponha que o robô do Exemplo 2 foi aprimorado, de forma que também seja possível movimentá-lo nas direções: Nordeste, Noroeste, Sudeste e Sudoeste. Se redefinirmos os comandos por: Leste* $\longmapsto 000$*, Oeste* $\longmapsto 010$*, Norte* $\longmapsto 100$*, Sul* $\longmapsto 110$*, Nordeste* $\longmapsto 001$*, Noroeste* $\longmapsto 011$*, Sudeste* $\longmapsto 101$ *e Sudoeste* $\longmapsto 111$*, o Algoritmo 2 e a Tabela 4.2 (3 dígitos de informação* $m = 3$*, requerem 3 dígitos de verificação* $k = 3$*) nos fornecerão a seguinte codificação:* $000 \longmapsto 00\boldsymbol{0}0\boldsymbol{0}$*,* $010 \longmapsto 10\boldsymbol{0}1\boldsymbol{1}\boldsymbol{0}$*,* $100 \longmapsto 11\boldsymbol{1}0\boldsymbol{0}\boldsymbol{0}$*,* $110 \longmapsto 01\boldsymbol{1}1\boldsymbol{1}\boldsymbol{0}$*,* $001 \longmapsto 01\boldsymbol{0}1\boldsymbol{0}\boldsymbol{1}$*,* $011 \longmapsto 11\boldsymbol{0}0\boldsymbol{1}\boldsymbol{1}$*,* $101 \longmapsto 10\boldsymbol{1}1\boldsymbol{0}\boldsymbol{1}$ *e* $111 \longmapsto 00\boldsymbol{1}0\boldsymbol{1}\boldsymbol{1}$*, em que os dígitos destacados em negrito correspondem aos símbolos antes da codificação.*

A forma de realizar a codificação desses símbolos é a mesma realizada no Exemplo 2, portanto não a repetiremos aqui. Entretanto, vamos apresentar uma forma mais direta para a verificação e correção do erro, ou seja, de aplicação do Algoritmo 3. Suponha que, ao darmos o comando para o robô se movimentar na direção nordeste, o símbolo 010001 tenha sido transmitido em vez do símbolo 010101, ou seja, ocorreu um erro na 4ª posição. Para detectar e corrigir esse erro, considere a Tabela 4.3 abaixo.

Tabela 4.3: Correção de um erro

v_1	v_2	d_3	v_4	d_5	d_6	Número de Verificação
0	1	0	0	0	1	
0		0		0		0
	1	0			1	0
			0	0	1	1

Fonte: Elaborada pelo autor.

Na primeira linha da tabela, rotulamos os dígitos que aparecerão nas colunas de 1 a 6 por v_1, v_2, d_3, v_4, d_5 e d_6, em que v_1, v_2 e v_4 são os dígitos de verificação e d_3, d_5 e d_6 são os dígitos de informação (os escritos em negrito no Exemplo 3). Na segunda linha da tabela, temos o símbolo que foi recebido na transmissão, a saber, 010001. Agora, note que os três zeros que aparecem na 3ª linha das seis primeiras colunas da tabela são os

valores de v_1, d_3 e d_5 e que a soma de d_3 com d_5 é par e, como $v_1 = 0$, essa verificação contribui com um 0 para o número de verificação (3ª linha e 7ª coluna). Prosseguindo a verificação, temos que a soma dos valores de d_3 e d_6, presentes na 4ª linha, é ímpar e, como $v_2 = 1$, essa verificação contribui com um 0 para o número de verificação. Finalmente, somando os valores de d_5 e d_6 na última linha, obtemos resultado ímpar e, como $v_4 = 0$, essa verificação contribui com um 1 para o número de verificação. Escrevendo o número de verificação em sua forma binária, obtemos 100, que em escrita decimal é igual a 4, ou seja, o erro se encontra na 4ª posição, como era de se esperar.

Vejamos agora um exemplo no qual consideraremos o caso do envio de um símbolo sem erro e verificaremos que o Algoritmo 3 retorna, de fato, uma sequência contendo apenas zeros como indicação da não ocorrência de erro.

Exemplo 4. *Seja* $x = 01001110$ *um símbolo pertencente a um código que transmite símbolos contendo um byte de informação, ou seja,* $m = 8$*. Para codificá-lo, consultamos a Tabela 4.2 e notamos que, para este valor de* m*, devemos escolher* $k = 4$ *e* $n = 12$*, logo, o símbolo* x*, ao ser codificado, terá 12 posições. Após utilizarmos o Procedimento 2, obtemos o símbolo* $x' = 100110011110$*, a codificação de* x*. Suponha que tal símbolo tenha sido transmitido corretamente, assim, ao utilizarmos o Procedimento 3 e calcularmos o número de verificação desse símbolo, devemos obter a sequência* 0000*, a qual indicará que não houve erro na transmissão. De fato, considerando a Tabela 4.4 abaixo, é fácil verificar que os valores dos dígitos na última coluna da mesma são realmente todos iguais a zero.*

Com esses exemplos, encerramos a apresentação do código de Hamming em sua formulação original. A seguir, mostraremos por que esses procedimentos de codificação e correção funcionam, para finalmente, na subseção 2.5, apresentar a formulação matricial desse código.

Tabela 4.4: Verificação da não ocorrência de erro

v_1	v_2	d_3	v_4	d_5	d_6	d_7	v_8	d_9	d_{10}	d_{11}	d_{12}	Número de Verificação
1	0	0	1	1	0	0	1	1	1	1	0	
1		0		1		0		1		1		0
	0	0			0	0			1	1		0
			1	1	0	0					0	0
							1	1	1	1	0	0

Fonte: Elaborada pelo autor.

4.2.4 Justificativa dos algoritmos e construção da tabela 2

A pergunta natural que surge nesse momento é: Por que estes algoritmos de codificação, decodificação e correção funcionam? A resposta para essa pergunta pode ser encontrada na relação existente entre os números escritos nas bases 2 e 10. Para entender melhor essa afirmação, consideremos o teorema a seguir e o seu corolário mais adiante, cujas demonstrações podem ser encontradas em Hefez (2014, p. 68; 73), respectivamente.

Teorema 1. *Sejam dados os números inteiros a e b, com $a > 0$ e $b > 1$. Existem números inteiros $n \geqslant 0$ e $0 \leqslant r_0, r_1, \ldots, r_n < b$, com $r_n \neq 0$, univocamente determinados, tais que $a = r_0 + r_1 b + r_2 b^2 + \cdots + r_n b^n$.*

Note que esse teorema garante que podemos escrever um número a dado, na base $b > 1$ que preferirmos. Em particular, quando $b = 10$, dizemos que o número a está escrito na base 10 ou em sua expansão decimal e escrevemos $(a)_{10}$, enquanto que, quando $b = 2$, dizemos que o número a está escrito na base 2 ou em sua expansão binária e escrevemos $(a)_2$. O corolário a seguir nos permite relacionar um número em sua representação na base 10 com a sua respectiva representação na base 2 e vice-versa. Tal relação, embora não tenha sido explicitada, está no cerne dos algoritmos de codificação, decodificação e detecção de erro desenvolvidos por Hamming.

corolário 1. *Todo número natural a escreve-se de modo único como soma de potências distintas de 2, a saber, $a = r_n \times 2^n + r_{n-1} \times 2^{n-1} + \ldots r_1 \times$*

$2^1 + r_0 \times 2^0$, *com* $r_i \in \{0,1\}$.

Exemplo 5. *Segundo o corolário anterior, o número* $(739)_{10}$ *é escrito, utilizando-se apenas potências de 2, como* $1\times 2^9 + 0\times 2^8 + 1\times 2^7 + 1\times 2^6 + 1\times 2^5 + 0\times 2^4 + 0\times 2^3 + 0\times 2^2 + 1\times 2^1 + 1\times 2^0$. *Ou, de forma mais sucinta,* $(739)_{10} = (1011100011)_2$.

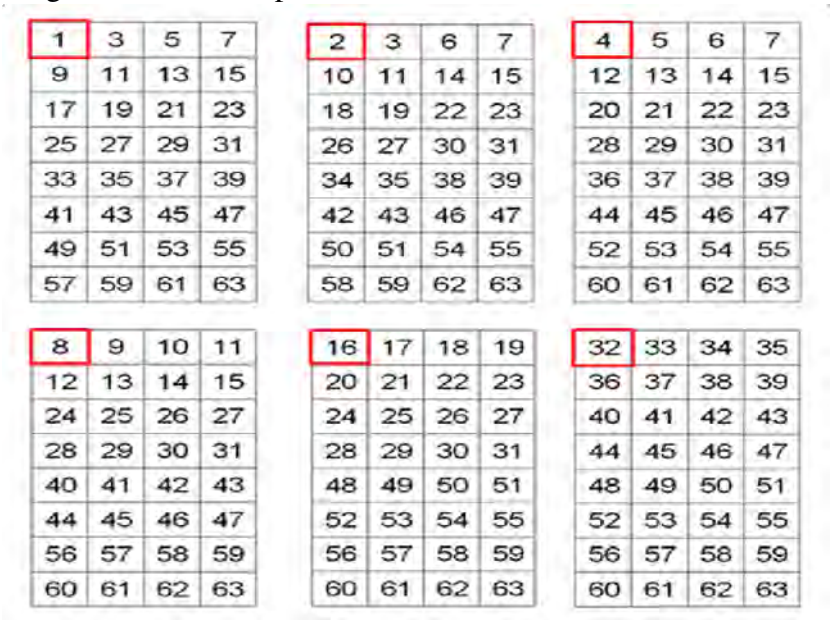
O exemplo a seguir é bastante esclarecedor para a compreensão do Algoritmo 3:

Exemplo 6. *Os cartões da Figura 4.3 abaixo podem ser utilizados para representar qualquer número natural entre 1 e 63 como a soma de potências de dois. Note ainda que a obtenção do número 39, por exemplo, é feita escolhendo os cartões que começam com* $1 = 2^0, 2 = 2^1, 4 = 2^2$ *e* $32 = 2^5$, *respectivamente, ou seja,* $39 = 1\times 2^5 + 0\times 2^4 + 0\times 2^3 + 1\times 2^2 + 1\times 2^1 + 1\times 2^0$ *ou, se preferirmos,* $(39)_{10} = (100111)_2$. *Esses cartões são também os únicos nos quais figura o número* 39.

Perceba, porém, que o que fizemos no Exemplo 6 é exatamente o que Hamming faz no Algoritmo 3. De fato, no Algoritmo 2 (para codificar um símbolo) Hamming escolhe somar os dígitos nas posições $1,3,5,7,9,11,13,15\ldots$ na obtenção de v_1; somar os dígitos nas posições $2,3,6,7,10,11,14,15\ldots$ na obtenção de v_2; somar os dígitos nas posições $4,5,6,7,12,13,14,15\ldots$ na obtenção de v_4; e assim por diante. Esses números que aparecem aqui são exatamente os que figuram nos 1º, 2º e 3º cartões da Figura 4.3, respectivamente. Desta forma, ao obter $v_1, v_2, v_4, \ldots$ por esse algoritmo, Hamming "prepara o caminho" para a utilização do Algoritmo 3.

Com efeito, de acordo com o Algoritmo 3, se o valor obtido na primeira verificação coincidir com o valor de v_1, escrevemos um 0, caso contrário, escrevemos um 1. Semelhantemente, procedemos para $v_2, v_4, \ldots$ até percorrermos todas as posições de verificação do símbolo. Desta forma, ao obtermos a sequência de k $0's$ e $1's$ ao final do cálculo envolvendo todas as posições de verificação, ela, de fato, representará um número escrito na base 2, pois escrever um 0 ou um 1 em cada etapa implica em escolher

Figura 4.3: Cartões para obter um número natural entre 1 e 63



1	3	5	7
9	11	13	15
17	19	21	23
25	27	29	31
33	35	37	39
41	43	45	47
49	51	53	55
57	59	61	63

2	3	6	7
10	11	14	15
18	19	22	23
26	27	30	31
34	35	38	39
42	43	46	47
50	51	54	55
58	59	62	63

4	5	6	7
12	13	14	15
20	21	22	23
28	29	30	31
36	37	38	39
44	45	46	47
52	53	54	55
60	61	62	63

8	9	10	11
12	13	14	15
24	25	26	27
28	29	30	31
40	41	42	43
44	45	46	47
56	57	58	59
60	61	62	63

16	17	18	19
20	21	22	23
24	25	26	27
28	29	30	31
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63

32	33	34	35
36	37	38	39
40	41	42	43
44	45	46	47
48	49	50	51
52	53	54	55
56	57	58	59
60	61	62	63

Fonte:https://www.ticsnamatematica.com/2014/11/entenda-como-construir-cartoes-jogo-adivinhe-idade.html

ou não um dos cartões da Figura 4.3, e tal escolha significa, tão somente, escrever um número natural como a soma de potências de dois.

Para encerrar esta subseção, vamos mostrar como os valores de n, m e k presentes na Tabela 4.2 foram obtidos. Para isso, considere a seguinte proposição que relaciona o número de verificação com os valores de n, m e k:

Proposição 1. *Sejam $C \in A^n$, um código corretor de erros, e n, m e k naturais, tais que m é o número de posições de informação, k é o número de posições de verificação dos símbolos do código e $n = m + k$, vale a seguinte relação entre n e m: $\frac{2^n}{n+1} \geqslant 2^m$.*

Demonstração. De fato, note que o número de verificação deve descrever $m + k + 1$ possibilidades diferentes, a saber, $n = m + k$ posições que dizem respeito a um erro em qualquer posição no símbolo, mais uma possibilidade no caso da não existência de erro. Isso implica na necessidade de ser

$2^k \geqslant m+k+1$, uma vez que 2^k é o número de sequências com k posições contendo apenas $0's$ e $1's$. Utilizando o fato de que $n = m+k$, obtemos $2^{n-m} \geqslant n+1 \Rightarrow \frac{2^n}{2^m} \geqslant n+1 \Rightarrow \frac{2^n}{n+1} \geqslant 2^m$, o que prova o resultado. □

Com essa proposição, concluímos que atribuindo valores para n, ou seja, escolhendo a quantidade de posições que os símbolos de C possuirão, a inequação acima nos fornece o maior valor possível para m, ou seja, a maior quantidade de posições de informação que os símbolos de C possuirão. Por outro lado, feita a escolha de m, a mesma inequação nos fornece o menor valor para n, ou seja, os símbolos com menor tamanho para o código C contendo uma certa quantidade de informação. Dessa forma, a inequação acima nos permite escrever o código que carregue a maior quantidade de informação possível com a maior economia possível.

Note que, se no lugar de considerarmos a inequação $2^k \geqslant m+k+1$, como fizemos anteriormente, nós considerarmos apenas a igualdade $2^k = m+k+1$, ou seja, se o número de verificação nos der exatamente $m+k+1$ posições diferentes, e sabendo que $n = m+k$, segue que $m = 2^k-k-1$ e $n = 2^k-1$. Logo, ao representarmos um código de Hamming na forma $C(n,m)$, o mesmo será descrito por $C(2^k-1, 2^k-k-1)$ e é justamente para essa família de códigos que daremos uma abordagem matricial na próxima subseção. Códigos que satisfazem essa condição são ditos *perfeitos*. Para demonstrações de que o código de Hamming é perfeito, ver Hefez (2008, p. 100) e Shine (2009, p. 301).

4.2.5 O código $C(7,4)$ e a família de códigos $C(2^k-1, 2^k-k-1)$

Agora que estudamos o código de Hamming em sua formulação original, daremos mais um passo em nosso estudo apresentando uma formulação mais recente do mesmo, utilizando ferramentas advindas da Teoria das Matrizes. Isso nos permitiu construir uma sequência didática, na qual alguns conceitos estudados no Ensino Médio, como por exemplo, a multiplicação de matrizes e a transposta de uma matriz, foram abordados. Para os

interessados na sequência didática, ver Lira (2018a) e Lira (2018b).

Isso posto, seguiremos de perto as ideias desenvolvidas em Rousseau e Aubin (2015), fazendo as devidas modificações e alterações para tornar o texto mais acessível, pensando em sua aplicação na Educação Básica. Dessa forma, trazemos uma teoria geral para os códigos $C(2^k-1, 2^k-k-1)$, paralelamente a uma visão particular sobre o código $C(7,4)$, onde os dígitos de informação são $m=4$ e os de verificação são $k=3$. Esse código codifica todas as sequências binárias contendo 4 elementos, ou seja, $16=2^4$ símbolos, que vão de 0000 até 1111. Nosso objetivo aqui é mostrar como funcionam a codificação, a decodificação e a correção de um único erro desses símbolos de uma forma diferente, porém equivalente a apresentada por Hamming (1950). A diferença aqui é que, em vez de colocarmos os dígitos de verificação nas potências de 2, nós os colocaremos em posições diferentes dessas, a saber, nas últimas posições do símbolo, porém com a mesma verificação de paridade utilizada na subseção 2.4.

Para deixarmos nossa exposição alinhada com a encontrada nos trabalhos atuais, consideraremos com mais detalhes o papel do conjunto $\mathbb{Z}_2$ na construção desses códigos. Para isso, vamos construí-lo a partir da ideia de congruência módulo 2. Considere a seguinte definição:

Definição 6. *Sejam a, b e m inteiros com $m>1$. Dizemos que a e b são congruentes módulo m e denotamos $a \equiv b \ (mod\ m)$, quando a e b deixam o mesmo resto na divisão euclidiana por m.*

Neste trabalho, estamos interessados apenas no caso em que $m=2$. Como o resto na divisão euclidiana de um número por 2 só pode ser ou 0 ou 1, podemos classificar todos os números inteiros em dois grupos (ou conjuntos): os números que deixam resto 0, que estão reunidos no conjunto denotado por $\overline{0} = \{a \in \mathbb{Z};\ a \equiv 0\ (mod\ 2)\}$ e os números que deixam resto 1, que estão reunidos no conjunto denotado por $\overline{1} = \{a \in \mathbb{Z};\ a \equiv 1\ (mod\ 2)\}$. Note que $\overline{0} = \{\cdots, -4, -2, 0, 2, 4, \cdots\}$ e $\overline{1} = \{\cdots, -3, -1, 1, 3, \cdots\}$. Usualmente o conjunto $\mathbb{Z}_2$ é representado como $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$, porém, por simplicidade, denotá-lo-emos por $\mathbb{Z}_2 = \{0, 1\}$, tendo sempre em mente que a soma de dois elementos de $\overline{1}$ resulta em um elemento de $\overline{0}$, pois a soma

de dois números que deixam resto 1 na divisão por 2 (ímpares) resultará em um número que deixa resto 0 na divisão por 2 (par). Assim, podemos concluir que em $\mathbb{Z}_2$ vale a relação $1+1=0$.

Isso posto, consideremos o símbolo $x = 0101$ e vejamos como o codificar e o decodificar, além de corrigir um único erro em uma de suas posições. Descrevendo os dígitos dos símbolos codificados da esquerda pra direita, os quatro primeiros serão os dígitos de informação, d_1, d_2, d_3 e d_4, e os três últimos, os de verificação, v_5, v_6 e v_7. O cálculo dos dígitos de verificação, e consequentemente sua codificação, é realizado através das igualdades: $v_5 = d_1 + d_2 + d_4, v_6 = d_1 + d_3 + d_4$ e $v_7 = d_2 + d_3 + d_4$, cuja disposição explicaremos mais adiante. Dessa forma, o símbolo codificado tem a representação $d_1d_2d_3d_4v_5v_6v_7$, na qual v_5, v_6 e v_7 são como postos acima. Assim, para o símbolo $x = 0101$, temos $d_1 = 0, d_2 = 1, d_3 = 0, d_4 = 1, v_5 = d_1 + d_2 + d_4, v_6 = d_1 + d_3 + d_4$ e $v_7 = d_2 + d_3 + d_4$. Logo, ao codificá-lo, obtemos o símbolo $x' = 0101010$.

Note que, na codificação dada pelo Algoritmo 2, o símbolo codificado tem a representação $v_1v_2d_3v_4d_5d_6d_7$, onde v_1 é escolhido de forma que a soma $v_1 + d_3 + d_5 + d_7$ seja par; v_2, de forma que a soma $v_2 + d_3 + d_6 + d_7$ seja par; e v_4, de forma que a soma $v_4 + d_5 + d_6 + d_7$ seja par, o que é o mesmo que:

$$\begin{aligned} v_1 &= d_3 + d_5 + d_7 \\ v_2 &= d_3 + d_6 + d_7 \\ v_4 &= d_5 + d_6 + d_7. \end{aligned} \tag{4.1}$$

Daí segue que a codificação, agora escrita como $d_1d_2d_3d_4v_5v_6v_7$, é equivalente à codificação da subseção 2.4, escrita como $v_1v_2d_3v_4d_5d_6d_7$, na qual a relação entre as duas codificações, quanto aos dígitos de verificação, é dada pela Tabela 4.5. Note também que, nessa forma de codificação, a relação com a codificação da subseção 2.4 é a seguinte: v_5 faz o papel de v_1; v_6 faz o papel de v_2; v_7 faz o papel de v_4; e d_1, d_2, d_3 e d_4 fazem o papel de d_3, d_5, d_6 e d_7, respectivamente. Dessa forma, para codificar um símbolo do código $C(7,4)$, utilizamos o seguinte algoritmo:

Algoritmo 4. *Para codificar um símbolo $d_1d_2d_3d_4v_5v_6v$ do código $C(7,4)$, utilize o Algoritmo 2 com a equivalência da Tabela 4.5.*

Tabela 4.5: Equivalência entre os dígitos v_5, v_6 e v_7 e v_1, v_2 e v_4

Codificação na subseção 2.4	v_1	v_2	d_3	v_4	d_5	d_6	d_7
Codificação equivalente	v_5	v_6	d_1	v_7	d_2	d_3	d_4

Fonte: Elaborada pelo autor

Vale destacar aqui que uma forma prática para codificar qualquer símbolo do código $C(7,4)$ é através da soma das colunas da Tabela 4.6 abaixo. Assim, se, por exemplo, considerarmos o símbolo $y = 0111$, temos $d_1 = 0, d_2 = 1, d_3 = 1$ e $d_4 = 1$, de modo que, ao substituirmos esses valores na Tabela 4.6 e somarmos suas respectivas colunas, obteremos o símbolo codificado $y' = 0111001$.

Tabela 4.6: Esquema para a codificação de um símbolo de $C(7,4)$

d_1	d_2	d_3	d_4	v_5	v_6	v_7
$1 \cdot d_1$	$0 \cdot d_1$	$0 \cdot d_1$	$0 \cdot d_1$	$1 \cdot d_1$	$1 \cdot d_1$	$0 \cdot d_1$
$0 \cdot d_2$	$1 \cdot d_2$	$0 \cdot d_2$	$0 \cdot d_2$	$1 \cdot d_2$	$0 \cdot d_2$	$1 \cdot d_2$
$0 \cdot d_3$	$0 \cdot d_3$	$1 \cdot d_3$	$0 \cdot d_3$	$0 \cdot d_3$	$1 \cdot d_3$	$1 \cdot d_3$
$0 \cdot d_4$	$0 \cdot d_4$	$0 \cdot d_4$	$1 \cdot d_4$	$1 \cdot d_4$	$1 \cdot d_4$	$1 \cdot d_4$

Fonte: Elaborada pelo autor

Agora que já sabemos codificar um símbolo de $C(7,4)$, a pergunta que surge é: Como decodificar e corrigir um erro de um símbolo desse código? Para responder a essa pergunta, precisamos detectar se existe um erro, sua posição e corrigi-lo, trocando 0 por 1 ou vice-versa. Isso é feito de acordo com o seguinte algoritmo, apresentado em Rousseau e Aubin (2015):

Algoritmo 5. *Para detectar um possível erro, calculamos os dígitos de verificação do símbolo recebido, os quais denotaremos por w_5, w_6 e w_7, e depois os comparamos com os respectivos valores, nas posições de verificação, do símbolo recebido. Uma das possibilidades a seguir pode ocorrer:*

1. $v_5 = w_5, v_6 = w_6$ *e* $v_7 = w_7$*, nesse caso, o símbolo foi enviado sem erro;*

2. $v_5 \neq w_5$ *e* $v_6 \neq w_6$*, nesse caso, o erro está na primeira posição;*

3. $v_5 \neq w_5$ *e* $v_7 \neq w_7$*, nesse caso, o erro está na segunda posição;*

4. $v_6 \neq w_6$ *e* $v_7 \neq w_7$*, nesse caso, o erro está na terceira posição;*

5. $v_5 \neq w_5$*,* $v_6 \neq w_6$ *e* $v_7 \neq w_7$*, nesse caso, o erro está na quarta posição;*

6. $v_5 \neq w_5$*, nesse caso, o erro está na quinta posição;*

7. $v_6 \neq w_6$*, nesse caso, o erro está na sexta posição;*

8. $v_7 \neq w_7$*, nesse caso, o erro está na sétima posição.*

Antes de mostrarmos esse algoritmo em ação, entendemos que cabe aqui uma breve explicação, caso a caso, do porquê do seu funcionamento.

1. No caso 1, não temos muito o que explicar, pois todos as verificações de paridade coincidem, logo, o simbolo enviado foi recebido sem erro.

2. No caso 2, ao notarmos que $v_5 \neq w_5$ e $v_6 \neq w_6$, concluímos que $v_7 = w_7$ e, como $v_7 = d_2 + d_3 + d_4$, o erro não pode estar em d_2, d_3 ou d_4, logo, só pode estar em d_1, pois é a discrepância de valores nesse dígito que faz com que $v_5 \neq w_5$ e $v_6 \neq w_6$.

3. No caso 3, ao notarmos que $v_5 \neq w_5$ e $v_7 \neq w_7$, concluímos que $v_6 = w_6$ e, como $v_6 = d_1 + d_3 + d_4$, o erro não pode estar em d_1, d_3 ou d_4, logo, só pode estar em d_2, pois é a discrepância de valores nesse dígito que faz com que $v_5 \neq w_5$ e $v_7 \neq w_7$.

4. No caso 4, ao notarmos que $v_6 \neq w_6$ e $v_7 \neq w_7$, concluímos que $v_5 = w_5$ e, uma vez que $v_5 = d_1 + d_2 + d_4$, o erro não pode estar em d_1, d_2 ou d_4, logo só pode estar em d_3, pois é a discrepância de valores nesse dígito que faz com que $v_6 \neq w_6$ e $v_7 \neq w_7$.

5. No caso 5, ao notarmos que $v_5 \neq w_5$, $v_6 \neq w_6$ e $v_7 \neq w_7$, concluímos que o erro só pode estar em um dígito que é comum a v_5, v_6 e v_7, o qual, como pode ser visto facilmente, é d_4, pois é a discrepância de valores nesse dígito que faz com que $v_5 \neq w_5, v_6 \neq w_6$ e $v_7 \neq w_7$.

6. Nos casos 6, 7 e 8, ao notarmos que $v_5 \neq w_5, v_6 \neq w_6$ e $v_7 \neq w_7$, respectivamente, tendo em vista as observações anteriores, só podemos concluir que o erro ocorreu na posição v_5, v_6 ou v_7, respectivamente.

Vejamos em um exemplo como esse procedimento funciona na correção de um único erro de um símbolo.

Exemplo 7. *Suponha que o símbolo* $x' = 0101010$ *tenha sido transmitido com um erro na quinta posição, ou seja, o símbolo recebido foi* $x'' = 0101110$.
Aplicando o Algoritmo 5 ao símbolo recebido, temos que $w_5 = d_1 + d_2 + d_4 = 0+1+1 = 0, w_6 = d_1 + d_3 + d_4 = 0+0+1 = 1$ *e* $w_7 = d_2 + d_3 + d_4 = 1+0+1 = 0$. *Comparando com* $v_5 = 1, v_6 = 1$ *e* $v_7 = 0$ *fica fácil ver que* $v_5 \neq w_5$, *logo, o erro está na quinta posição, como já era de se esperar. Para corrigir o erro, basta modificar o símbolo da quinta posição, trocando o 1 por 0 e, para decodificar o símbolo, basta tomar as 4 primeiras posições.*

Com os Algoritmos 4 e 5, podemos codificar, decodificar e corrigir um único erro de qualquer um dos 16 símbolos do código $C(7,4)$. Entretanto, existe uma maneira mais prática de se codificar, decodificar e corrigir um único erro nesse código, mais ainda, tal maneira é facilmente generalizada para a família de códigos $C(2^k - 1, 2^k - k - 1)$.

Considerando a Tabela 4.6 acima, observamos que os coeficientes de $d_1, \cdots, v_7$ presentes em suas entradas são os mesmos da matriz:

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

a qual é chamada de *matriz geradora* do código $C(7,4)$, visto que qualquer símbolo X desse código é codificado no símbolo X' através da sua multiplicação com a matriz geradora, ou seja, $X' = XG_3$. O índice 3 designa o número de dígitos de verificação do código que, como já vimos anteriormente, nesse caso são 3.

Exemplo 8. *Para codificar o símbolo $x = 0101$ novamente, basta realizar a multiplicação em $\mathbb{Z}_2$ das matrizes*

$$X = \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}$$

e

$$G_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

obtendo a matriz:

$$XG_3 = X' = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

a qual representa o símbolo codificado $x' = 0101010$. Note que obtemos o mesmo símbolo codificado anteriormente.

Para o caso geral da matriz geradora de um código $C(2^k - 1, 2^k - k - 1)$, nós temos a seguinte definição:

Definição 7. *A matriz geradora, denotada G_k, é uma matriz de dimensão $(2^k - k - 1) \times (2^k - 1)$ com coeficientes em $\mathbb{Z}_2$, tal que todos os elementos codificados do código C sejam obtidos através da sua multiplicação pela matriz geradora.*

Outra matriz que possui destaque no código de Hamming é a chamada *matriz de controle* ou *matriz de paridade* H_k. Para o código $C(7,4)$, temos que:

$$H_3 = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

e para o caso geral, temos que a matriz de paridade de um código $C(2^k - 1, 2^k - k - 1)$ é definida como segue:[6]

Definição 8. *A matriz de paridade, denotada por H_k, é uma matriz de dimensão $k \times (2^k - 1)$ com coeficientes em $\mathbb{Z}_2$, tal que $G_k H_k^t = \mathbf{0}$, na qual H_k^t denota a matriz transposta de H_k e $\mathbf{0}$, a matriz nula.*

Note que as matrizes G_3 e H_3 do código $C(7,4)$ podem ser escritas como $G_3 = [I_4 \ \ A]$ e $H_3 = [B \ \ I_3]$, em que A e B são matrizes satisfazendo $A^t = B$, e I_3 e I_4 denotam as matrizes identidade de dimensão 3 e 4, respectivamente. Além disso, quando as matrizes G_3 e H_3 estão escritas nessa forma, dizemos que as mesmas estão em sua *forma padrão*. A generalização desse fato é o conteúdo do próximo teorema, o qual nos permitirá obter G_k em sua forma padrão, sempre que definirmos H_k também em sua forma padrão e vice versa. A demonstração desse teorema não será inserida aqui, pois se utiliza de conceitos que fogem do escopo deste trabalho, porém ela pode ser encontrada em Meneghesso (2012, p. 19-20).

Teorema 2. *Sejam $G_k = [I_{2^k-k-1} \ \ A]$ e $H_k = [B \ \ I_k]$. H_k será a matriz de verificação de paridade associada à matriz geradora G_k se, e somente se, $A^t = B$. Além disso, o código binário correspondente $C(2^k - 1, 2^k - k - 1)$ será corretor de um único erro se, e somente se, as colunas de H_k forem não nulas e distintas.*

Em vista do Teorema 2, uma pergunta que pode surgir é: As matrizes G_k e H_k são as únicas que definem um código da forma $C(2^k - 1, 2^k - k - 1)$? A

[6] O leitor com conhecimentos de Álgebra Linear deve ter percebido que as linhas da matriz geradora formam uma base para um espaço vetorial que é isomorfo a $\mathbb{Z}_2^{2^k-k-1}$. Mais ainda, nota-se também que as colunas da transposta da matriz de paridade formam uma base para o complemento ortogonal do espaço vetorial gerado pelas linhas da matriz geradora.

resposta para essa pergunta é negativa, além disso, a seguinte definição nos dá as condições para a criação de outras matrizes geradoras e de paridade, chamadas de *matrizes equivalentes*.

Definição 9. *Duas matrizes G_k e G'_k geram o mesmo código C, ou seja, são equivalentes, se uma pode ser obtida da outra através de uma sequência finita de operações do tipo:*

L1 Permutação de duas linhas;

L2 Adição de uma linha a outra;

C1 Permutação de duas colunas.

Exemplo 9. *É fácil ver que a matriz geradora do código de Hamming definido na subseção 2.4, através do Algoritmo 2 é igual a:*

$$G_3 = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

A qual, por sua vez é equivalente à matriz geradora do código de Hamming que definimos nesta seção à partir da Tabela 4.6:

$$G'_3 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Pois podemos obter uma da outra através de aplicações sucessivas das operações acima definidas. Faça Isso!

Para o caso geral, temos a seguinte proposição, cuja demonstração segue da simples aplicação das operações $(L1), (L2)$ e $(C1)$. Para uma demonstração dessa proposição para o caso em que os coeficientes das

matrizes são elementos de um corpo K qualquer, ver Hefez (2008, p. 92-93).

Proposição 2. *Dado um código C com matriz geradora G_k, existe um código equivalente C' com matriz geradora G'_k na forma padrão.*

Isto posto, temos definida uma matriz geradora G_k. A codificação de um símbolo u qualquer do código $C(2^k-1, 2^k-k-1)$ se dá simplesmente pela multiplicação de u por G_k, obtendo-se o símbolo codificado $v = uG_k$, ou seja, a codificação é simplesmente uma multiplicação de matrizes com coeficientes em $\mathbb{Z}_2$. Para a decodificação e correção há dois casos: i) o símbolo foi transmitido sem erro; e ii) o símbolo foi transmitido com um único erro.

Para o primeiro caso, se o símbolo codificado v foi transmitido sem erro, então o mesmo é anulado pela matriz de paridade. Com efeito, $vH_k^t = (uG_k)H_k^t = u(G_kH_k^t) = u\mathbf{0} = \mathbf{0}$, assim, sempre que o produto vH_k^t for igual à matriz nula, podemos concluir que o símbolo foi transmitido sem erro.

Para o segundo caso, sejam v um símbolo do código $C(2^k-1,2^k-k-1)$ (sem erro) e $v^{(i)} \in Z_2^{2^k-1}$ o símbolo obtido pela adição, em $\mathbb{Z}_2$, de 1 ao i-ésimo digito de v. Logo, $v^{(i)}$ é um símbolo codificado transmitido com um erro no i-ésimo dígito. Assim podemos escrever $v^{(i)} = v + (0 \cdots 0 \underbrace{1}_{i-simo} dgito\ 0 \cdots 0)$, a partir do que, temos:

$$v^{(i)}H_k^t = \underbrace{vH_k^t}_{0} + \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix} H_k^t$$

$$= \begin{pmatrix} 0 & \cdots & 0 & 1 & 0 & \cdots & 0 \end{pmatrix} H_k^t.$$

Note que $v^{(i)}H_k^t$ é a i-ésima linha de H_k^t, logo, a i-ésima coluna de H_k. Dessa forma, um erro ocorrido na i-ésima posição da mensagem transmitida equivale a i-ésima coluna de H_k. Para corrigir o erro, portanto, temos que modificar o dígito do símbolo recebido na posição que é equivalente a i-ésima coluna da matriz de paridade. A seguir, ilustramos como esse

procedimento funciona na correção de um símbolo do código $C(7,4)$, o qual é o código para $k=3$ no código $C(2^k-1, 2^k-k-1)$:

Exemplo 10. *Consideremos novamente o símbolo $x = 0101$, que como pôde ser visto no Exemplo 8, ao ser codificado, se torna $x' = 0101010$. Assim, como fizemos no Exemplo 7, introduziremos um erro na quinta posição, obtendo $x'' = 0101110$. Para corrigir esse erro, multiplicaremos o símbolo x'' pela transposta da matriz de paridade para este código H_3^t, obtendo:*

$$X''H_3^t = \begin{pmatrix} 0 & 1 & 0 & 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix},$$

a quinta linha de H_3^t e, consequentemente, a quinta coluna de H_3, logo, o erro se encontra na quinta posição do símbolo x'', como já esperávamos.

Antes de irmos para o próximo exemplo, note que no código $C(15,11)$, os símbolos são escritos na forma $d_1d_2d_3\cdots d_{11}v_{12}v_{13}v_{14}v_{15}$, e que, estendendo o Algoritmo 4 para esse caso, podemos definir:

$$\begin{aligned} v_{12} &= d_1+d_2+d_4+d_5+d_7+d_9+d_{11} \\ v_{13} &= d_1+d_3+d_4+d_6+d_7+d_{10}+d_{11} \\ v_{14} &= d_2+d_3+d_4+d_8+d_9+d_{10}+d_{11} \\ v_{15} &= d_5+d_6+d_7+d_8+d_9+d_{10}+d_{11} \end{aligned} \tag{4.2}$$

Essa maneira de definir v_{12}, v_{13}, v_{14} e v_{15} é equivalente à definição de v_1, v_2, v_4 e v_8 dada pelo Algoritmo 2 na subseção 2.4, e a relação entre os dígitos lá e aqui pode ser vista na Tabela 4.7 abaixo. Desta forma, para construir a matriz geradora $G_4 = [I_4 \ \ A]$, basta tomar $A = [v_{12}v_{13}v_{14}v_{15}]$, na qual cada uma das quatro colunas de A é formada pelos coeficientes dos

dígitos $d_i, i = 1 \cdots 11$, que definem v_{12}, v_{13}, v_{14} e v_{15}.

Tabela 4.7: Equivalência entre os dígitos v_{12}, v_{13}, v_{14} e v_{15} e v_1, v_2, v_4 e v_8

Subseção 2.4	v_1	v_2	d_3	v_4	d_5	d_6	d_7	v_8	d_9	d_{10}	d_{11}	d_{12}	d_{13}	d_{14}	d_{15}
Aqui	v_{12}	v_{13}	d_1	v_{14}	d_2	d_3	d_4	v_{15}	d_5	d_6	d_7	d_8	d_9	d_{10}	d_{11}

Fonte: Elaborada pelo autor

Com esse exemplo, encerramos as considerações sobre o Código de Hamming e concluímos esta seção. Para mais exemplos e outras considerações sobre esse código, como, por exemplo, sua interpretação geométrica, ver Lira (2018a).

4.3 Considerações finais

O código de Hamming definitivamente representou um marco para a Teoria dos Códigos Corretores de Erros. Os desenvolvimentos que se seguiram, em certa medida, só foram possíveis graças ao trabalho desse pioneiro. Sendo assim, a abordagem de seu código na Educação Básica é mais do que merecida, bem como representa uma excelente forma de introduzir o assunto para as novas gerações de futuros engenheiros, matemáticos e pesquisadores das mais diversas áreas da ciência.

Na dissertação que gerou este trabalho, Lira (2018a), nós desenvolvemos uma sequência didática para o ensino do código de Hamming em suas duas formulações, tal como foram apresentadas anteriormente. Devido a natureza deste trabalho, optamos por não a apresentar aqui, porém deixarmos a sugestão de leitura, e, porque não, de aplicação da mesma nas escolas, para o leitor disposto a tal.

4.4 Referências bibliográficas

ABRANTES, S. A. **Notas históricas da codificação para controle de erros**. São Paulo, 09 de jul. de 2021. Disponível em: https://docplayer.com.br/amp17613484-Notas-historicas-da-codificacao-para-controlo-de-erros.html. Acesso em 09 de jul. de 2021.

AGUIAR, J.; VIEIRA, S.; CAVALCANTE, R. Códigos quânticos corretores de erros. In: V Congresso Norte-Nordeste de Pesquisa e Inovação, 2010, Maceió. **Anais**... Maceió: IFAC, 2011.

ALVES, B. C. **Uma proposta de oficina sobre códigos para a contextualização do estudo de aritmética e matrizes no ensino médio**. 2015. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Universidade Federal de Goiás, Goiânia.

BOULLAF, F. **Códigos, reticulados e aplicações em criptografia**. 2015. Dissertação (Mestrado) – Instituto de Matemática, Estatística e Computação Científica, Universidade Estadual de Campinas, Campinas.

CARVALHO, S. **Matrizes, determinantes e polinômios: aplicações em códigos em corretores de erros, como estratégias motivacional para o ensino de matemática**. 2014. Dissertação (Mestrado) - Programa de Pós-Graduação e Mestrado Profissional em Matemática em Rede Nacional PROFMAT, Universidade Federal de Rondônia-UNIR, Porto Velho.

DIAS, J. **O código da mariner 9**. 2017. Dissertação (Mestrado) - Programa de Pós-Graduação e Mestrado Profissional em Matemática em Rede Nacional PROFMAT, Universidade Federal de São João del-Rei, São João del-Rei.

Ellenberg, J. **O poder do pensamento matemático**: a ciência de como não estar errado. 1 ed. Rio de Janeiro: Zahar, 2015.

FARIA, L. **Existências de códigos corretores de erros e protocolos de comunicação em sequências de DNA**. 2011. Doutorado em engenharia elétrica, Universidade Estadual de Campinas, Campinas.

GLEICK, J. **A informação**: Uma história, uma teoria, uma enxurrada. São Paulo: Companhia das Letras, 2013.

GUIMARÃES, W. Códigos corretores de erros para gravação magnética.

2003. Dissertação (Mestrado) - Programa de Pós-Graduação em Engenharia Elétrica, Universidade Federal de Pernambuco, Recife.

HAMMING, R. Error detecting and error correcting codes. **Bell System Technical Journal**, Nova York, v. 29, n. 2, p. 147–160, 1950.

HEFEZ, A. **Aritmética**. Rio de Janeiro: SBM, 2014.

HEFEZ, A.; VILLELA, M. Códigos Corretores de Erros. Rio de Janeiro: IMPA, 2008.

LIRA, E. **Códigos corretores de erros no ensino médio**: Um estudo sobre o Código de Hamming. 2018. Dissertação (Mestrado) – Universidade Federal Rural de Pernambuco, Mestrado Profissional em Matemática, Recife.

LIRA, E.; DANTAS, M. **Uma sequência didática para o ensino de códigos corretores de erros no ensino médio**. In: III Encontro de Educação Matemática do Vale do São Francisco, 2018, Petrolina.

MACHADO, D. **Uma abordagem de dígitos verificadores e códigos corretores no ensino fundamental**. 2016. Dissertação (Mestrado) - Mestrado Profissional em Matemática em Rede Nacional, Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Paulo.

MENEGHESSO, C. **Códigos corretores de erros**. 2012. Dissertação (Graduação - Trabalho de Conclusão de Curso). Departamento de Matemática, Centro de Ciências Exatas e Tecnologia, Universidade Federal de São Carlos, São Carlos.

MILIES, C. A matemática dos códigos de barras – Detectando erros. **RPM**, Rio de Janeiro, v. 68, 2008.

MILIES, C. Breve introdução à Teoria dos Códigos Corretores de Erros. In: Sociedade Brasileira de Matemática, Colóquio de Matemática da Região Centro-Oeste, 2009, Campo Grande. **Anais**... Campo Grande: Departamento de Matemática Universidade Federal do Mato Grosso do Sul, 2009.

MIRANDA, D. **Códigos corretores de erros e empacotamentos de discos**. 2013. Trabalho de Conclusão (Mestrado Profissional) - Departamento de Matemática da Universidade Federal Rural de Pernambuco, Recife.

NICOLETTI, E. **Aplicações de álgebra linear aos códigos corretos de erros e ao ensino médio**. 2015. Dissertação (Mestrado) - Universidade Estadual Paulista, Instituto de Geociências e Ciências Exatas, Rio Claro.

PINZ, C. **Dígitos verificadores e detecção de erros**. 2013. Dissertação (Mestrado Profissional em Matemática em Rede Nacional) - Instituição de Matemática, Estatística e Física, Universidade Federal do Rio Grande, Rio Grande.

ROCHA, A.. textbfModelo de sistema de comunicações digital para o mecanismo de importação de proteínas mitocondriais através de códigos corretores de erros. 2010. Tese (doutorado) - Universidade Estadual de Campinas, Faculdade de Engenharia Elétrica e de Computação, Campinas.

RODRIGUES, N. **Códigos Corretores de Erros**. 2017. Dissertação (mestrado profissional) - Universidade Federal de Santa Catarina, Centro de Ciências Físicas e Matemáticas, Programa de Pós-Graduação em Matemática, Florianópolis.

ROUSSEAU, C.; AUBIN, Y. **Matemática e atualidade**. Volume 1. Rio de Janeiro: SBM, 2015. SCHROEDER, E. **Códigos binários e truques de mágica**. 2017. Dissertação (Mestrado) - Universidade Estadual do Mato Grosso do Sul, Curso de Mestrado Profissional de Matemática em Rede Nacional, Dourados.

SHANNON, C. A mathematical theory of communication.**Bell System Technical Journal**, Nova York, v. 27, p. 379-423. 1948.

SHINE, C. **21 Aulas de Matemática Olímpica**. Rio de Janeiro: SBM, 2009.

STEWART, I. **17 Equações que mudaram o mundo**. Rio de Janeiro: Zahar, 2013.

SÁ, C; ROCHA, J. **Treze Viagens pelo Mundo da Matemática**. 2 ed. Rio de Janeiro: SBM, 2012.

Capítulo 5

O estudo de polinômios com relatos de história da matemática

Ma. Francisca Alves de Souza[1]
Dra. Bárbara Costa da Silva[2]

Resumo: Os polinômios são de suma relevância para a matemática e, quando associados a funções, modelam vários fenômenos do nosso dia a dia. Esse assunto é abordado, pela primeira vez, no 8º ano do ensino fundamental, porém os alunos chegam ao ensino médio e superior com várias dificuldades na aprendizagem desse assunto, principalmente no que tange produtos notáveis. Essas dificuldades ocorrem por inúmeros motivos, sendo um dos principais a aversão que os alunos têm pelas aulas de matemática. Por essa razão, este capítulo tem como objetivo tornar o conteúdo atrativo devido ao *design* da abordagem utilizada na digitação e da sua junção com a história da matemática, tornando-a uma ferramenta de auxílio do processo de ensino-aprendizagem, assim como revela uma matemática mais dinâmica já que mostra o desenvolvimento dessa ciência no decorrer do tempo.

Palavras-chave: **Polinômios; História da Matemática; Ensino-Aprendizagem.**

[1]IFCE-Instituto Federal de Educação, Ciência e Técnologia do Ceará, alves-souza@ifce.edu.br

[2]UFRPE, Universidade Federal Rural de Pernambuco, barbara.costasilva@ufrpe.br

5.1 Origem da álgebra

Era uma vez...

Vou contar-lhe uma pequena história. Você está preparado para ouvir? Sente-se e vamos dar um passeio em um mundo cheio de aventuras e feitos. Sabe que mundo é esse? Não? Pense bem. É o nosso. Então comecemos.

Fonte: Imagem de OpenClipart-Vectors por Pixabay

A civilização egípcia desenvolveu-se ao longo de uns quatro mil anos e deixou-nos marcas maravilhosas. As mais conhecidas são, claro, as pirâmides de Gisé e a Esfinge. Vamos abordar um pouco a herança matemática desses ilustres antepassados. A nossa fonte principal é um papiro contendo problemas de matemática, escrito por volta de 1650 a.C. Esse documento contém 85 enunciados copiados em escrita hierática (escrita hieroglífica simplificada usada para escrever textos com um pincel em tiras de papiro), cujo autor foi Ahmes. Ele ficou conhecido pelo nome do historiador escocês que o comprou no século XIX, Alexander Henry Rhind.

O papiro de Rhind é uma fonte primária rica sobre a matemática egípcia antiga. Ele descreve os métodos de multiplicação e divisão, o uso que se fazia das frações unitárias, emprega a regra da falsa posição, apresenta uma solução para o problema da determinação da área de um círculo e muitas outras aplicações da matemática a situações práticas.[4]

[4]Texto com base no livro: *10 livros, 10 regiões, 10 jogos para aprender e divertir-se* (SANTOS et al, 2008).

Vejamos um exemplo:

Problema 24: O valor de "aha" se "aha" e um sétimo de "aha" é 19.

Para solucionar o problema, os egípcios utilizavam uma técnica denominada MÉTODO FALSA POSIÇÃO. Esse método consistia em escolher um valor arbitrário para "aha" e, a partir desse valor, eles faziam os cálculos e comparavam com o resultado, mas provavelmente não era o resultado esperado. Por isso, eles utilizavam um fator de correção para obter o valor correto de "aha", ou seja, o valor que satisfaz a expressão. Seguindo o método egípcio, vamos resolver o problema e encontrar o valor de "aha".

Solução:

Seja "aha"$= 7$. Logo, um sétimo de "aha" é 1 e consequentemente "aha" e um sétimo de "aha" é $7+1=8\neq 19$.

Então, o fator de correção é um número que multiplicado por 8 é igual a 19, ou seja, $\frac{19}{8}$.

Portanto, o valor de "aha" é $\frac{19}{8}\cdot 7=\frac{133}{8}$

■

Esse problema transcrito para a linguagem matemática moderna seria:

Problema 24: Determine o valor que somado a sua sétima parte é igual a 19.

Solução:

Seja x o valor procurado, ou seja, o "aha" citado anteriormente.

Escrevendo o enunciado na linguagem matemática atual, temos: $x+\frac{1}{7}x=19$.

Logo,

$$x+\frac{1}{7}x=19 \quad\Leftrightarrow\quad 7\cdot\left(x+\frac{1}{7}x\right)=7\cdot 19\Leftrightarrow 7x+1x \tag{5.1}$$

$$=133 \tag{5.2}$$

$$\Leftrightarrow 8x=133\Leftrightarrow x=\frac{133}{8}$$

■

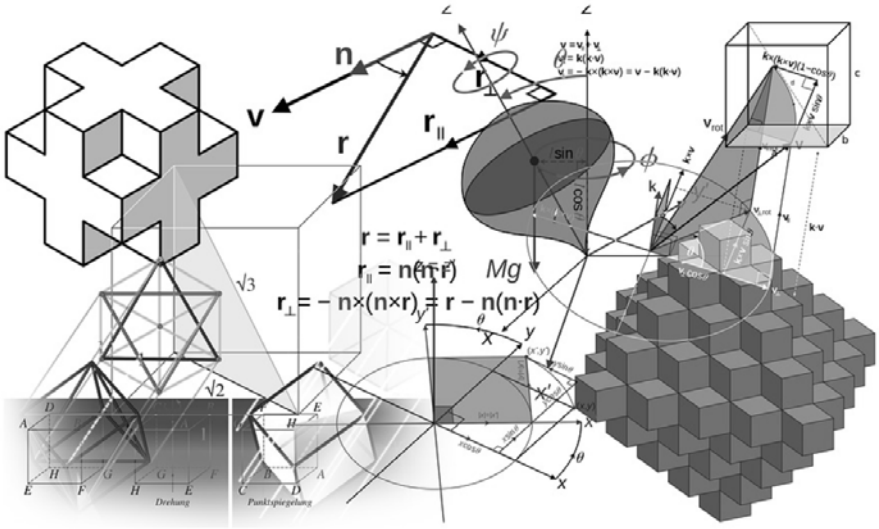
Observemos que o problema se resume em encontrar a raiz de uma equação algébrica $x + \frac{1}{7}x = 19$, ou seja, o valor x para que o polinômio $P(x) = x + \frac{1}{7}x$ tenha como valor numérico 19 ($P(x) = 19$).

O papiro de Ahmes ou Rhind, como é mais conhecido, é o documento que marca a origem da álgebra, em especial o surgimento dos polinômios na nossa história, já que os polinômios fazem parte da álgebra.

Agora, que tal aprendermos um pouco mais de álgebra, ou melhor, da álgebra dos polinômios? Mas o que é um polinômio? Essa resposta teremos em breve.

5.2 O cálculo algébrico

Mais uma história? Sim! Que ótimo. Continuemos.



Fonte: Imagem de Gerd Altmann por Pixabay

Simon Stevis (1548-1620) nasceu em Bruges, foi comerciante em Antuérpia, viajou pela Dinamarca e para fora da Europa, e, aos 35 anos,

ingressou na Universidade de Leyden, onde estudou matemática, grego e engenharia.

Apesar de ter entrado com idade fora do padrão (por motivos familiares), continuou como professor durante alguns anos, tornando-se amigo de um aluno aplicado, o príncipe Maurício de Nassau. Mais tarde, este o tornou diretor do departamento do exército holandês, responsável pela construção de armamentos e de navios. Stevis foi um engenheiro genial e, como tal, supervisionou a construção de estradas, de vias navegáveis e de outras obras públicas, além de realizar incursões na óptica, na qual deixou algumas obras, e na hidrostática, com experiências que comprovaram que a pressão exercida no fundo de um recipiente por um líquido, depende, principalmente, da sua altura (ANDRADE, 2015).

Suas principais contribuições foram na estática e na matemática. Na matemática, Simon foi o primeiro a estudar, de forma metódica e minuciosa, o sistema de frações decimais e suas aplicações, os números inteiros e os números irracionais, estudo esse que facilitou o CÁLCULO ALGÉBRICO, cuja definição, de expressão algébrica, segundo (SERRASQUEIRO, 1906) [5] é: a reunião dos processos empregados para efetuar as operações algébricas, ou seja, os processos usados para transformar uma expressão algébrica em outra equivalente. Stevis fez um estudo unificado das equações quadráticas e apresentou métodos para obtenção de soluções aproximadas de equações algébricas de qualquer grau, em outras palavras, ele estudou equações polinomiais de grau n (ANDRADE, 2015). Agora, vamos estudar essas expressões algébricas? Ótimo, eu sabia que você ia querer continuar.

5.2.1 Expressão algébrica

Definição: É toda expressão que tem apenas letras, ou apenas números, ou números e letras.

[5] Tratado de Álgebra Elementar: Livro Primeiro, Capítulo I, Noções preliminares §2º Expressões algébricas, 1906. pg 11

Exemplos: (1) mn (2) $3m+2n$ (3) 5

5.2.2 Classificação das expressões algébricas

As expressões algébricas podem ser classificadas da seguinte forma:irracional, racional, racional inteira e racional fracionária.

Vejamos abaixo cada uma delas.
Expressão Algébrica Irracional: É toda expressão algébrica que apresenta letras no radicando.

Exemplos: (1) $\sqrt{x}+y$ (2) $2\sqrt{a}-\frac{b}{3}$

Expressão Algébrica Racional: É toda expressão algébrica que não apresenta letras no radicando.

Exemplos: (1) $\frac{\sqrt{3}+2a}{3b}$ (2) $2x^2-5x+1$

Expressão Algébrica Racional Inteira: É toda expressão algébrica racional que não apresenta letras no denominador.

Exemplos: (1) $\frac{\sqrt{3}+2a}{3}$ (2) $2x^2-5x+1$

Expressão Algébrica Racional Fracionária: É toda expressão algébrica racional que apresenta letras no denominador.

Exemplos: (1) $\frac{\sqrt{3}+2a}{3b}$ (2) $\frac{2x+y}{x-y}$

5.2.3 Valor numérico de uma expressão algébrica

Vamos entender o que significa o *valor numérico* de uma expressão algébrica por intermédio de um exemplo.

Exemplo: Em uma gráfica, cada xerox custa $ 0,20. Que expressão algébrica relaciona o valor a ser pago e a quantidade de cópias? Se João xerocar 30 páginas, quanto ele deve pagar?

Solução:

Cada cópia custa $ 0,20 e o valor a ser pago depende da quantidade de cópias. Então, podemos pensar da seguinte forma:

Número da linha	Quantidade de cópias	Valor a ser pago
(1ª linha)	1	$1 \cdot 0,20 = 0,20$
(2ª linha)	2	$2 \cdot 0,20 = 0,40$
(3ª linha)	3	$3 \cdot 0,20 = 0,60$
(4ª linha)	x	$x \cdot 0,20 = 0,20x$

Observe que na 4ª linha foi colocado a letra x para indicar a quantidade de cópias, pois essa quantidade é variável. Ou seja, a letra ocupa o lugar de um número.

Sejam x a quantidade de cópias e $V(x)$ o valor a ser pago, então a expressão algébrica procurada é $V(x) = 0,20x$.

Como João vai xerocar 30 páginas, então o valor a ser pago é $30 \cdot (\$\ 0,20) = \$\ 6,00$. Veja que, para determinar o valor a ser pago, é só substituirmos o x na expressão $V(x) = 0,20x$ por 30. Logo, 6 é o valor numérico da expressão algébrica encontrada.

Em outras palavras, para encontrar o valor numérico de uma expressão algébrica basta substituir as variáveis por números.

Definição: Dado o número a e a expressão $P(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_2 \cdot x^2 + a_1 \cdot x + a_0$, chamamos de valor numérico de $P(x)$ em a o valor obtido quando substituímos o x por a na expressão $P(x)$, ou seja, $P(a)$.

Exemplo: Calcule o valor numérico da expressão $Q(x) = \dfrac{3x^2 - 5x}{x+3}$ para $x = 4$.

Solução:

Substituindo x pelo seu valor, que é 4, na expressão $Q(x) = \dfrac{3x^2 - 5x}{x+3}$, obtemos:

$$Q(4) = \frac{3 \cdot 4^2 - 5 \cdot 4}{4+3} = \frac{3 \cdot 16 - 20}{7} = \frac{48 - 20}{7} = \frac{28}{7} = 4$$

■

5.3 Monômios

Você gostou das histórias anteriores? Eu sabia que você ia gostar. Então, que tal mais uma? Formidável, então vamos a história.

Fonte: Imagem de Clker-Free-Vector-Images por Pixabay

Nicolo Fontana nasceu em 1501 na cidade italiana de Bréscia. Em 1512, a Bréscia foi invadida pelas tropas francesas e o jovem Nicolo foi gravemente ferido por golpes de espadas de um soldado. Por esse motivo, ficou com uma profunda cicatriz na boca, o que lhe ocasionou um defeito na fala. Por isso recebeu o apelido de Tartaglia, que quer dizer gago. Segundo a história, ele foi deixado para morrer, mas sua mãe o encontrou e, por não ter remédios para tratar seus ferimentos, ela procedeu da mesma forma que gatos e cachorros fazem para cuidar dos seus filhotes. Porém, foi esse cuidado que salvou a vida do seu filho.

Tartaglia não frequentou a escola devido a suas posses serem escassas, por isso estudou sozinho em casa, nos livros que conseguia encontrar. Sem dinheiro para comprar papel, tinta e pena, escrevia com carvão sobre paredes. Alguns historiadores dizem que as lápides também serviam como cadernos. Dono de uma memória extraordinária, Nicolo aprendeu a ler e escrever por conta própria e rapidamente obteve conhecimento de latim, grego e matemática, tornando-se professor de matemática em Veneza, Verona, Bréscia e Vicenza. Tartaglia publicou diversas obras, sendo a mais conhecida um tratado sobre aritmética, no qual ele abordou operações numéricas e regras comerciais. Foi o primeiro a realizar cálculos de artilharia e participou de vários debates.

Porém, o que o colocou no anais da matemática foi sua rivalidade com Girolamo Cardano (1501 - 1576) sobre o método de resolução das equações cúbicas. Vamos entende melhor essa história.

Antonio Maria Del Fiore, tendo obtido o método de resolver equações cúbicas algebricamente de Del Ferro, desafiou Tartaglia para ver se ele era capaz de encontrar soluções para as tais equações, mas ele não sabia que Tartaglia já havia descoberto a solução geral de equações do tipo $x^3 + px^2 = q$. A disputa ocorreu em 1535 e cada participante deveria apresentar 30 questões para o outro resolver. Tartaglia apresentou várias questões distintas colocando Fiore em uma situação desconfortável, pois o mesmo não tinha conhecimento do que se gabava. Já era de se espera o resultado, ou seja, Fiore mostrou-se incapaz de solucionar os problemas propostos.

Esse episódio despertou a curiosidade de Cardano, o qual não sabia solucionar as equações polinomiais de grau 3, então ele entrou em contato com Tartaglia e solicitou o método de resolução para publicar no livro que ele estava escrevendo. Tartaglia se recusou, pois ele mesmo queria publicar, então Cardano prometeu manter o método em segredo e em seguida quebrou a promessa: mesmo dando os créditos a seu inventor.

Tartaglia ficou muito chateado e escreveu um livro publicando sua descoberta e, de certo modo, insultando Cardano. [6]

Definição: Monômios são expressões algébricas racionais inteiras representadas por um único produto.

Exemplo (1):

$$\begin{array}{ccc} 5x^3y^2 & \longrightarrow & 5 \text{ (Coeficiente)} \\ \downarrow & & \downarrow \\ x^3y^2 \text{ (Parte literal)} & \longrightarrow & \text{monômio} \end{array}$$

Exemplo (2):

$$\begin{array}{ccc} -\frac{2}{7}ab^3m & \longrightarrow & -\frac{2}{7} \text{ (Coeficiente)} \\ \downarrow & & \downarrow \\ ab^3m \text{ (Parte literal)} & \longrightarrow & \text{monômio} \end{array}$$

Exemplo (3):

$$\begin{array}{ccc} \sqrt{2}\,x & \longrightarrow & \sqrt{2} \text{ (Coeficiente)} \\ \downarrow & & \downarrow \\ x \text{ (Parte literal)} & \longrightarrow & \text{monômio} \end{array}$$

Observação: Quando o expoente da parte literal for igual a zero

[6] Dica: visite a página https://pt.wikipedia.org/wiki/Tartaglia e leia mais sobre essa história.

denominamos monômio constante

5.3.1 Grau de um monômio

Definição: O grau (gr) de um monômio cujo coeficiente não é nulo é indicado pela soma dos expoentes da parte literal.

Exemplos: (1) O grau do monômio $4x^2y^2$ é 4 (2) O grau do monômio -7 é 0

5.3.2 Monômios semelhantes

Definição: São aqueles que possuem a mesma parte literal ou não possuem parte literal.

Exemplos: (1) $4x$ e $-7x$ (2) 8 e -3 (3) $7z^2y$ e $9z^2y$

5.3.3 Operações com monômios

Adição e Subtração: É obtida somando-se algebricamente os coeficientes e conservando-se a parte literal dos monômios semelhantes.

Exemplos: (1) $24x^2 + 12x^2 = 36x^2$ (2) $-10x + 6x = -4x$

Multiplicação: É obtida multiplicando os coeficientes e depois as partes literais.

Exemplo: $(5a^2b).(-3a) = -15a^3b$

Divisão: É obtida dividindo os coeficientes e depois as partes literais.

Exemplo: $(12a^4b^3) \div (2ab^2) = 6a^3b$

Nem sempre é possível efetuar a divisão. Vejamos o exemplo seguinte:

Exemplo: $(30a^2b^3) \div (7a^3) = \dfrac{30b^3}{7a} = \dfrac{30}{7}a^{-1}b^3$

A parte literal é $a^{-1}b^3$, mas o expoente da variável a é negativo.

Logo, $\dfrac{30b^3}{7a}$ não é um monômio.

Potenciação: É obtida elevando o coeficiente e a parte literal à potência indicada.

Exemplo: $(-5ab^2)^3 = (-5)^3.(a)^3.(b^2)^3 = -125a^3b^6$

Radiciação: É obtida extraindo a raiz n-ésima do coeficiente e dividindo o expoente de cada variável por n.

Exemplos: (1) $\sqrt{25y^2} = \sqrt{25} \cdot y^{\frac{2}{2}} = 5y$ (2) $\sqrt[5]{32x^{10}y^5} = \sqrt[5]{32} \cdot x^{\frac{10}{5}} \cdot y^{\frac{5}{5}} = 2x^2y$

Observe o índice do radical e os expoentes da parte literal em cada exemplo e veja que os expoentes são múltiplos do índice, por isso é possível efetuar a radiciação. Mas nem sempre isso é possível. Vejamos:

Exemplo:

(1) $\sqrt{3y^3} = \sqrt{3}.y^{\frac{3}{2}} = \sqrt{3}y^{1,5}$, veja que $1,5 \notin \mathbb{N}$ e, por esse motivo, $\sqrt{3y^3}$ não é um monômio.

5.4 Polinômios

Definição: É toda expressão algébrica racional inteira.

Monômio: expressões algébricas racionais inteiras representadas por um único produto (polinômio que possui um único termo);

Binômio: polinômio formado pela soma de dois monômios, ou seja, que possui dois termos;

Trinômio: polinômio formado pela soma de três monômios, ou seja, que possui três termos;
Polinômio nulo: polinômio formado por monômios nulos.

Os polinômios com mais de três termos não recebem denominação particular (BIANCHINI, 2006).

Exemplos:

(1) -5 (4) $2x^2 - 3x$

(2) x (5) $x^2 - 2xy + y^2$

(3) $a^5 - 3$ (6) $5x^2 - 3x + 2x^3 - 4$

5.4.1 Grau de um polinômio

Definição: É igual ao grau do monômio não nulo de maior grau que compõe o polinômio.

Observação: Não se define grau para o polinômio nulo

Exemplos:

Polinômio	Grau do Polinômio
(1) $P(x,y) = 2x^2y - 5x^2y^3 + 4xy$	$gr(P(x,y)) = 5$
(2) $Q(a,b) = 5a^3b + 2a^2b^3 - 4a^3b^4 - 2ab^3$	$gr(Q(a,b)) = 7$
(3) $R(x) = 5$	$gr(R(x)) = 0$

5.4.2 Polinômio com uma variável

Definição: Um polinômio na variável real x é uma expressão dada por:

$$P(x) = a_n \cdot x^n + a_{n-1} \cdot x^{n-1} + \ldots + a_2 \cdot x^2 + a_1 \cdot x + a_0$$

em que:

- $a_n, a_{n-1}, \ldots, a_2, a_1, a_0 \in \mathbb{R}$ e são chamados de coeficientes do polinômio;

- a_0 é coeficiente independente ou termo independente;
- $n \in \mathbb{N}$;
- o grau do polinômio é o número n, onde $a_n \neq 0$.

Exemplos:

(1) $P(x) = 5x^2 - 4x + 2$ é um polinômio completo de grau 2.

(2) $P(x) = x^3 - 2x^2 + x + 1$ é um polinômio completo de grau 3.

(3) $P(x) = x^2 - 4$ é um polinômio incompleto de grau 2.

Reescrevendo, temos $P(x) = x^2 + 0x - 4$, por esse motivo, dizemos que é incompleto.

(4) $P(x) = 2x^4 - 3x^2 + 2$ é um polinômio incompleto de grau 4.

Reescrevendo, temos $P(x) = 2x^4 + 0x^3 - 3x^2 + 0x + 2$.

(5) $P(x) = 2x + 3x^{-2} + 4x^{-1}$ não é um polinômio, pois o expoente de x é negativo.

(6) $P(x) = 3x^2 - 5\sqrt{x} + 2$ não é um polinômio, pois o expoente de x é fracionário.

5.5 Operações com polinômios

Vamos entender como efetuar as operações com polinômios por meio de exemplos.

5.5.1 Adição e subtração

Exemplos:
(1) $(4x^2 - 7x + 2) + (3x^2 + 2x + 3) = ?$

Solução:

$$\begin{aligned}(4x^2-7x+2)+(3x^2+2x+3) &= 4x^2+3x^2-7x+2x+2+3\\ &= (4+3)x^2+(-7+2)x+(2+3)\\ &= 7x^2-5x+5\end{aligned}$$

■

(2) $(4x^3-7x+2)-(3x^2+2x+3)=?$

Solução:

$$\begin{aligned}(4x^3-7x+2)-(0x^3+3x^2+2x+3) &= 4x^3-7x+2-0x^3-3x^2-2x-3\\ &= 4x^3-0x^3-3x^2-7x-2x+2-3\\ &= (4-0)x^3-3x^2+(-7-2)x+(2-3)\\ &= 4x^3-3x^2-9x-1\end{aligned}$$

■

Com base nos exemplos acima, vemos que, para efetuarmos a soma ou subtração de polinômios, devemos associá-los aos monômios semelhantes. Ou seja:

Definição: Dados dois polinômios $P(x)=a_nx^n+a_{n-1}x^{n-1}+\ldots+a_2x^2+a_1x+a_0$ e $Q(x)=b_nx^n+b_{n-1}x^{n-1}+\ldots+b_2x^2+b_1x+b_0$, denominamos soma e diferença de P com Q os polinômios: $P(x)+Q(x)=(a_n+b_n)x^n+(a_{n-1}+b_{n-1})x^{n-1}+\ldots+(a_2+b_2)x^2+(a_1+b_1)x+(a_0+b_0)$ e $P(x)-Q(x)=(a_n-b_n)x^n+(a_{n-1}-b_{n-1})x^{n-1}+\ldots+(a_2-b_2)x^2+(a_1-b_1)x+(a_0-b_0)$, respectivamente (IEZZI, 2013b).

5.5.2 Multiplicação e divisão

Exemplo:

Multiplicação de polinômio por polinômio:

(2) $(7x^2-2x+1).(x-2)=?$

Solução:

$$\begin{aligned}(7x^2-2x+1).(x-2) = \\ 7x^2\cdot x+7x^2\cdot(-2)+(-2x)\cdot x+\ (-2x)\cdot(-2)+1\cdot x+1\cdot(-2) = \\ 7x^3\cdot -14x^2-2x^2+4x+x-2 = \\ 7x^3-16x^2+5x-2\end{aligned}$$

■

Como vimos acima, para efetuar a multiplicação de polinômios usamos a propriedade distributiva, ou seja, basta multiplicar cada termo de um dos polinômios por cada termo do outro polinômio.

Definição: Dados dois polinômios $P(x) = a_m x^m + a_{m-1}x^{m-1} + \ldots + a_2x^2 + a_1x + a_0$ e $Q(x) = b_n x^n + b_{n-1}x^{n-1} + \ldots + b_2x^2 + b_1x + b_0$, denominamos produto de $P \cdot Q$ o polinômio $P(x)\cdot Q(x) = a_m b_n x^{m+n} + \ldots + (a_2b_0 + a_1b_1 + a_0b_2)x^2 + (a_0b_1 + a_1b_0)x + a_0b_0$.

Divisão de polinômio por monômio:
(3) $(18x^3 - 12x^2 + 3x) \div (3x) = ?$

Solução:

$$\begin{aligned}(18x^3-12x^2+3x)\div(3x) = \\ \frac{18x^3-12x^2+3x}{3x} = \\ \frac{18x^3}{3x}-\frac{12x^2}{3x}+\frac{3x}{3x} = \\ 6x^2-4x+1\end{aligned}$$

■

Divisão de polinômio por polinômio:

Para efetuarmos a divisão, podemos utilizar o algoritmo da divisão (algoritmo de Euclides ou método da chave) ou o método de Descartes,

porém vamos focar somente no algoritmo da divisão, já que ele funciona de forma mais geral. Existe também o dispositivo prático de Briot-Ruffini, mas ele só deve ser utilizado para dividir polinômio por binômio.

Para facilitar o entendimento do algoritmo, resolveremos o exemplo abaixo detalhando cada passo da solução:

(4) $(-1+8x^3) \div (2x-1) = ?$

Solução:

(1) O dividendo $-1+8x^3$ é um polinômio incompleto e está na ordem crescente de expoente. Logo, vamos colocá-lo na ordem decrescente de expoentes e completá-lo com zeros, ou seja: $8x^3+0x^2+0x-1$.

(2) O divisor $2x-1$ já está na ordem decrescente de expoentes.

(3) Agora, dividimos o termo de maior grau do dividendo pelo termo de maior grau do divisor. Logo: $\frac{8x^3}{2x} = 4x^2$.

(4) Em seguida, multiplicamos o resultado encontrado no item (3) pelo divisor, ou seja: $4x^2 \cdot (2x-1) = 8x^3 - 4x^2$.

(5) Agora façamos a diferença entre o dividendo e o resultado obtido no cálculo anterior (item 4). A primeira diferença é $8x^3+0x^2+0x-1-(8x^3-4x^2) = 4x^2+0x-1$.

(6) Assim, temos a nova divisão $(4x^2+0x-1) \div (2x-1)$ e seguimos o mesmo procedimento até que o grau da última diferença seja menor que o grau do divisor ou que a última diferença seja igual a zero, e, nesse caso, o dividendo é divisível pelo divisor.

Vejamos o algoritmo a seguir:

$$\begin{array}{rl} 8x^3+0x^2+0x-1 & \big|\underline{2x-1} \\ \underline{-8x^3+4x^2} & 4x^2+2x+1 \\ 4x^2+0x-1 & \\ \underline{-4x^2+2x} & \\ 2x-1 & \\ \underline{-2x+1} & \\ 0 & \end{array}$$

■

(5) $(12x^4-17x^3-3x^2-11x-3)\div(3x^2-2x-3)=?$

Solução:

$$\begin{array}{rl} 12x^4-17x^3-3x^2-11x-3 & \big|\underline{3x^2-2x-3} \\ \underline{-12x^4+8x^3+12x^2} & 4x^2-3x+1 \\ -9x^3+9x^2-11x-3 & \\ \underline{9x^3-6x^2-9x} & \\ 3x^2-20x-3 & \\ \underline{-3x^2+2x+3} & \\ -18x & \end{array}$$

■

Definição: Dados dois polinômios P (dividendo) e $D\neq 0$ (divisor), dividir P por D com resto é determinar dois outros polinômios Q (quociente) e R (resto), de modo que se verifiquem as seguintes condições:

(I) $P=Q\cdot D+R$

(II) $gr(R)<gr(D)$ ou $R=0$

Observação: Se $R=0$ dizemos que P é divisível por D

5.6 Produtos notáveis

O que significa produto notável? Os cálculos algébricos obedecem a alguns padrões de resolução, dentro os quais podemos citar determinadas multiplicações. Para efetuar essas multiplicações, utilizamos constantemente a propriedade distributiva, mas algumas dessas multiplicações aparecem frequentemente e, por esse motivo, denominamos produtos notáveis.

5.6.1 Quadrado da soma de dois termos

Definição: O quadrado da soma de dois termos é igual ao quadrado do primeiro termo mais duas vezes o produto do primeiro termo pelo segundo termo mais o quadrado do segundo termo.

Exemplo: (1) Desenvolva $(x+3)^2$.

Solução:

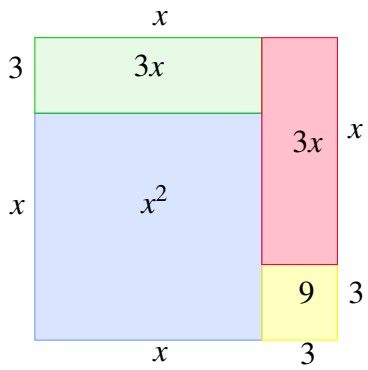
$$\begin{aligned}(x+3)^2 &= (x+3)\cdot(x+3) \\ &= x\cdot x + x\cdot 3 + 3\cdot x + 3\cdot 3 \\ &= x^2 + 3x + 3x + 9 \\ &= x^2 + 6x + 9\end{aligned}$$

(5.3)

(5.4)

■

Geometricamente, essa expressão representa a área $A(x)$ de um quadrado de lado igual a $x+3$. Vejamos a figura abaixo:



Ou seja, $A(x) = (x+3)^2 = x^2+3x+3x+9 = x^2+6x+9$.
Generalizando, temos:

$$(a+b)^2 = a^2+2\cdot a\cdot b+b^2$$

5.6.2 Quadrado da diferença de dois termos

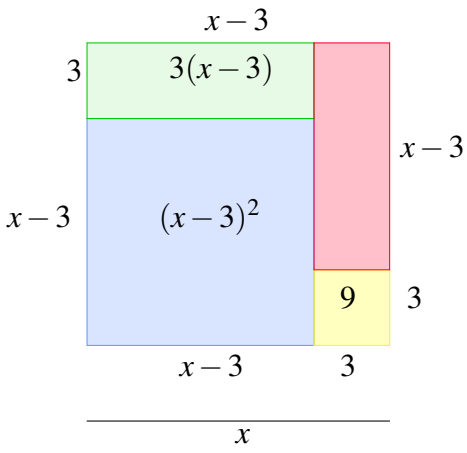
Definição: O quadrado da diferença de dois termos é igual ao quadrado do primeiro termo menos duas vezes o produto do primeiro termo pelo segundo termo mais o quadrado do segundo termo.

Exemplo:
(1) Desenvolva $(x-3)^2$.
Solução:

$$\begin{aligned}(x-3)^2 &= (x-3)\cdot(x-3)\\ &= x\cdot x+x\cdot(-3)+(-3)\cdot x+(-3)\cdot(-3)\\ &= x^2-3x-3x+9\\ &= x^2-6x+9\end{aligned}$$

■

Geometricamente, essa expressão representa a área $B(x)$ de um quadrado de lado igual a $x-3$. Vejamos a figura abaixo:



Ou seja,

$B(x) = (x-3)^2 = x^2 - 3(x-3) - 3(x-3) - 9 = x^2 - 3x + 9 - 3x + 9 - 9 = x^2 - 6x + 9$.

Generalizando, temos:

$$(a-b)^2 = a^2 - 2 \cdot a \cdot b + b^2$$

5.6.3 Produto da soma pela diferença de dois termos

Definição: O produto da soma pela diferença de dois termos é igual ao quadrado do primeiro termo menos o quadrado do segundo termo.

Exemplos:

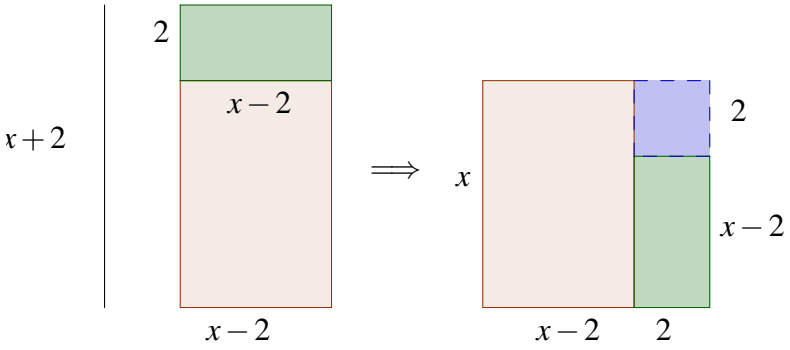
(1) $(x+2).(x-2) = ?$

Solução:

$$\begin{aligned}(x+2).(x-2) &= x\cdot x+x\cdot(-2)+2\cdot x+2\cdot(-2)\\ &= x^2-2x+2x-2^2\\ &= x^2-4\end{aligned}$$

■

Geometricamente, essa expressão representa a área $C(x)$ de um retângulo de lados $x+2$ e $x-2$. Vejamos a figura abaixo:



Logo, a área desse retângulo é $C(x) = \overline{(x+2)\,x(x-2)} = x^2-4$.

Generalizando, temos:

$$(a+b)\cdot(a-b) = a^2-b^2$$

(2) $(5m+2n).(5m-2n) = 25m^2-4n^2$

Solução:

$$\begin{aligned}(5m+2n).(5m-2n) &= (5m)^2-(2n)^2\\ &= 25m^2-4n^2\end{aligned}$$

■

5.6.4 Cubo da soma e da diferença de dois termos

Exemplos:
(1) Desenvolva $(x+5)^3$.
Solução:

$$\begin{aligned}(x+5)^3 &= (x+5)^2 \cdot (x+5)\\ &= (x^2+10x+25)\cdot(x+5)\\ &= x^2\cdot x + x^2\cdot 5 + 10x\cdot x + 10x\cdot 5 + 25\cdot x + 25\cdot 5\\ &= x^3+5x^2+10x^2+50x+25x+125\\ &= x^3+15x^2+75x+125\end{aligned}$$

■

Generalizando, temos:

$$(a+b)^3 = a^3+3\cdot a^2\cdot b+3\cdot a\cdot b^2+b^3$$

(2) Desenvolva $(x-y)^3$.
Solução:

$$\begin{aligned}(x-y)^3 &= x^3+3\cdot x^2\cdot(-y)+3\cdot x\cdot(-y)^2+(-y)^3\\ &= x^3-3x^2y+3xy^2-y^3\end{aligned}$$

■

Até o momento, vimos como desenvolver expressões com expoentes 2 e 3. Agora vamos nos apropriar de conhecimentos que facilitarão o desenvolvimento de expressões com expoente maior ou igual a 2.

5.6.5 Fatorial

Exemplo: João está organizando o armário e possui 4 livros de matemática. De quantas maneiras distintas João pode dispor esses livros?

Solução:

João tem 4 livros, então vamos numerá-los com $1, 2, 3$ e 4. Logo, temos as seguintes sequências:

(1, 2, 3, 4)	(1, 2, 4, 3)	(1, 3, 2, 4)	(1, 3, 4, 2)	(1, 4, 2, 3)	(1, 4, 3, 2)
(2, 1, 3, 4)	(2, 1, 4, 3)	(2, 3, 1, 4)	(2, 3, 4, 1)	(2, 4, 1, 3)	(2, 4, 3, 1)
(3, 1, 2, 4)	(3, 1, 4, 2)	(3, 2, 1, 4)	(3, 2, 4, 1)	(3, 4, 2, 1)	(3, 4, 1, 2)
(4, 1, 2, 3)	(4, 1, 3, 2)	(4, 2, 1, 3)	(4, 2, 3, 1)	(4, 3, 1, 2)	(4, 3, 2, 1)

Portanto, temos 24 sequências. Ou seja, 24 maneiras distintas para João dispor os livros.

Outro modo de solucionar a questão é pensar dessa forma:

- Primeira posição: ele pode escolher qualquer um dos 4 livros;
- Segunda posição: ele só pode escolher qualquer um dos 3 livros restantes;
- Terceira posição: ele só pode escolher qualquer um dos 2 livros restantes;
- Quarta posição: ele só tem 1 único livro.

Logo, a quantidade de maneiras distintas em que ele pode dispor os livros é dada pelo produto $4 \cdot 3 \cdot 2 \cdot 1 = 24$.

■

Em problemas de contagem, aparecem frequentemente multiplicações de números naturais na ordem decrescente e, por isso, os matemáticos criaram um símbolo para representá-las. Esse símbolo, !, recebe o nome de fatorial. O símbolo de fatorial foi introduzido pela primeira vez em 1808 pelo professor universitário Christian Kramp, cujo objetivo era eliminar as dificuldades encontradas na escrita. Em 1811, Legendre representou o

fatorial usando a letra grega gama (Γ) e Gauss utilizou a letra grega pi (Π). Atualmente usamos o símbolo de Kramp, então o cálculo anterior seria escrito como: $4 \cdot 3 \cdot 2 \cdot 1 = 4!$

Definição: Seja $n \in \mathbb{N}$. Denominamos fatorial de n e indicamos por $n!$ a relação:

$n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$ para $n \geq 2$;
$1! = 1$;
$0! = 1$.

Exemplos:

(1) $3! = 3 \cdot 2 \cdot 1 = 6$

(2) $4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24$

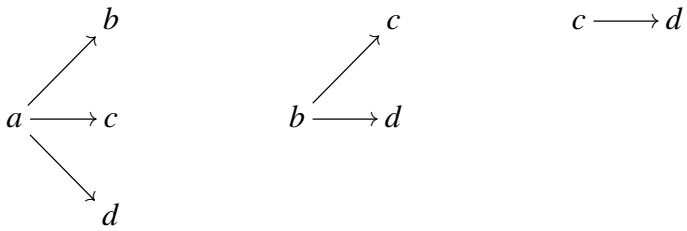
(3) $\dfrac{10!}{8!} = \dfrac{10 \cdot 9 \cdot 8!}{8!} = 10 \cdot 9 = 90$

5.6.6 Combinação

Definição: Seja A um conjunto com n elementos. Chamamos de combinações (C) dos n elementos, tomados p a p, e denotamos por $C_{n,p}$ os subconjuntos de A constituídos de p elementos.

Exemplo: Considere o conjunto $E = \{a, b, c, d\}$. Determine a quantidade de subconjuntos do conjunto E com dois elementos.

Solução: Para determinar a quantidade de subconjuntos de E com dois elementos, é preciso apenas fazer as combinações dos 4 elementos de E, tomados 2 a 2, e depois contar quantas combinações fizemos. Lembre-se que $\{a, b\} = \{b, a\}$, então:



Logo, os subconjuntos de E com dois elementos são:

$$\{a,b\};\{a,c\};\{a,d\};\{b,c\};\{b,d\};\{c,d\}$$

Portanto, temos 6 subconjuntos.

Observe que o conjunto E só possui 4 elementos, então é bastante simples exprimir os subconjuntos pedidos. Mas se o conjunto dado possuísse 10, 15 ou 1000 elementos, como exprimir os subconjuntos com dois elementos ou todos os subconjuntos? Seria muito trabalhoso e exaustivo. Então, para otimizar o tempo e facilitar o cálculo, usamos a fórmula abaixo (IEZZI, 2013a):

Fórmula para o cálculo do número de combinações

$$C_{n,p} = \left(\begin{array}{c} n \\ p \end{array} \right) = \frac{n!}{p! \cdot (n-p)!},\ n \in \mathbb{N} \geq p$$

Exemplos:

(1) $C_{3,2} = \dfrac{3!}{2!.(3-2)!} = \dfrac{6}{2} = 3$

(2) $C_{5,2} = \dfrac{5!}{2!.(5-2)!} = \dfrac{5.4.3!}{2!.3!} = \dfrac{20}{2} = 10$

5.6.7 Binômio de Newton

> Não sei o que o mundo pode pensar de mim, mas eu mesmo me considero tão somente um menino que, brincando na areia

> da praia, se diverte ao encontrar um seixo arredondado ou uma concha mais bonita que as comuns, enquanto o grande oceano da verdade jaz indecifrável ante meus olhos. (ISAAC NEWTON) (PALARO, 2006)

Na epígrafe acima, Newton deixa claro que desconhece uma grande quantidade de coisas, mas o pouco que ele afirma ter conhecimento foi suficiente para descobrir e desenvolver estudos em matemática e física. Creio que nesse momento você deve estar querendo saber um pouco mais sobre Newton, é verdade? Eu sabia. Então, vamos à história.

Fonte: Imagem de Prawny por Pixabay

Isaac Newton nasceu em 25 de dezembro de 1642, na aldeia de Woolsthorpe. Newton se dedicava a projetar miniaturas mecânicas até que, um dia, encontrou um livro de astrologia que mudou sua atenção para a matemática. Esse novo interesse o levou a ler vários livros, sendo o primeiro deles os *Elementos de Euclides* e depois *La géométrie* de Descartes,

a *Clavis* de Oughtred, a *Arithmetica infinitorum* de Wallis, entre outros trabalhos.

Pouco depois, Newton descobriu o teorema do binômio generalizado e inventou o método do fluxões, o qual hoje chamamos de cálculo diferencial. No período de março a junho de 1666, a Universidade de Cambridge foi fechada devido a uma epidemia de peste e Newton teve que retornar a sua cidade natal. Esse período foi bem inspirador para Newton, pois, além do cálculo, ele se dedicou a várias partes da física, testou suas primeiras experiências em óptica e também formulou os princípios básicos da teoria da gravitação. Alguns historiadores, porém, dizem que essas descobertas só ocorreram após o seu retorno à universidade.

Newton retornou a Cambridge em 1667, desenvolveu suas pesquisas no campo da óptica por dois anos, ocupou a cátedra lucasiana em 1669 e publicou um artigo com suas descobertas em óptica. Contudo, surgiram várias críticas sobre seu trabalho, deixando-o muito chateado e, por esse motivo, Newton demorou para publicar suas descobertas posteriores, fato que o levou a uma disputa com Leibniz sobre a primazia da criação do cálculo.

Em 1675, comunicou a *Royal Society* sua teoria corpuscular, lecionou álgebra e teoria das equações de 1673 à 1683, publicou o tratado *Philosophiae Naturalis Principia Mathematica* (material compostos em três livros) e, em 1692, Newton adoeceu e teve como consequência da doença um distúrbio mental. Desse ano em diante, seus esforços se voltaram para a química, alquimia e teologia. No ano de 1696, foi indicado inspetor da Casa da Moeda, sendo promovido a diretor em 1699. Em 1703, foi eleito presidente da *Royal Society*, cargo que ocupou até a sua morte em 1727.

Newton é considerado um dos maiores gênios de todos os tempos e suas realizações foram expressas neste poema de Alexandre Pope: “A natureza e as leis da natureza jaziam ocultas na noite; Deus disse: Faça-se Newton, e a luz se fez”.

Todos nós temos habilidades que, às vezes, estão escondidas e não deixamos que floresçam. Ainda assim, acredito que cada um de nós é capaz de gostar e de aprender os mistérios da matemática, mas isso só depende do

nosso querer e do nosso esforço. Como diz o capitão planeta: O poder é de vocês.

[Teorema Binomial] O desenvolvimento de $(x+a)^n$ para $n \in \mathbb{N}$ e $x, a \in \mathbb{R}$ é dado por:[7]

$$(x+a)^n = \binom{n}{0} \cdot x^n + \binom{n}{1} \cdot x^{n-1} \cdot a^1 + \binom{n}{2} \cdot x^{n-2} \cdot a^2 + \ldots + \binom{n}{n} \cdot a^n$$

Exemplo: Desenvolva $(x+y)^4$.
Solução:

$$(x+y)^4 = \binom{4}{0} \cdot x^4 \cdot y^0 + \binom{4}{1} \cdot x^3 \cdot y^1 + \binom{4}{2} \cdot x^2 \cdot y^2 + \binom{4}{3} \cdot x^1 \cdot y^3 + \binom{4}{4} \cdot x^0 \cdot y^4$$

$$(x+y)^4 = 1 \cdot x^4 \cdot 1 + 4 \cdot x^3 \cdot y^1 + 6 \cdot x^2 \cdot y^2 + 4 \cdot x^1 \cdot y^3 + 1 \cdot x^0 \cdot y^4$$

$$(x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$

■

Para determinar o valor de cada coeficiente binomial, podemos utilizar a fórmula para combinações vista anteriormente ou utilizar o triângulo de Pascal, o qual veremos adiante e facilitará bastante o cálculo.

[7] Dica: visite a página https://www.colegioweb.com.br/binomio-de-newton/propriedades-do-triangulo-de-pascal.html para saber mais

5.6.8 Triângulo aritmético

O triângulo aritmético, também chamado de triângulo de Tartaglia-Pascal, é uma tabela de formato triangular (não limitada) de números naturais, fácil de construir e que permite obter, de modo imediato, os coeficientes do desenvolvimento de $(a+b)^n$. Esse triângulo foi descoberto pelo matemático chinês Yang Hui e suas propriedades aritméticas foram estudadas pelo matemático francês Blaise Pascal, razão pela qual o triângulo leva o seu nome. Pascal e Fermat foram os criadores da Análise Combinatória e da Teoria de Probabilidades (MORGADO, 2013).

Você já conheceu um pouco da história de Tartaglia. Agora vamos conhecer a história de Pascal? Sim? Ótimo, eu sabia que você ia gostar. Então, continuemos com nossa viajem ao passado.

Fonte: Imagem de James Sutherland por Pixabay

Blaise Pascal nasceu em 19 de julho de 1623, em Clermont-Ferrand, na França. A mãe de pascal, Antoniette Bejon, faleceu quando ele tinha apenas 3 anos de idade. Étienne Pascal, pai de Blaise, encarregou-se pessoalmente

da educação do garoto por meio de um método um pouco diferente dos adotados na época, cujo objetivo era o estudo da razão. Esse método consistia na aplicação de exercícios diversos abordando as disciplinas geografia, história e filosofia. Já as aulas de matemática só deveriam ser ministradas quando o jovem Pascal estivesse com o intelecto preparado para aprender essa ciência, ou seja, maduro, de acordo com seu pai.

O jovem Pascal ouvia conversas sobre matemática e sua curiosidade foi se acentuando. Sem professor ou mesmo livros, ele começou a desenvolver seus estudos. Depois de autorizado a estudar matemática, juntou-se aos sábios do círculo de Mersenne e, a partir daí, teve contato com conhecimentos que proporcionaram o desenvolvimento dos seus trabalhos. Aos 17 anos, descobriu e publicou vários teoremas em geometria projetiva, essenciais para o desenvolvimento tecnológico da aviação. Criou uma máquina de calcular para ajudar seu pai e existe, hoje, uma linguagem de programação denominada pascal, em sua homenagem, pois ele achava que no futuro as máquinas poderiam pensar.

Blaise dedicou-se ao estudo da aritmética e desenvolveu os cálculos de probabilidade, o triângulo de pascal e o tratado sobre as potências numéricas, além de contribuir com a física no campo da hidrostática. Devido a seus esforços excessivos, ficou gravemente doente e, em 1648, se tornou adepto do misticismo de *Port-Royal*. Pascal faleceu em Paris no dia 19 de junho de 1662. Sofreu bastante, mas suportou toda dor com grande resignação. Suas palavras finais foram: “Que Deus jamais me abandone” (RUIZ, 2010).

Definição: O triângulo de Pascal é uma tabela na qual podemos dispor ordenadamente os coeficientes binomiais.

Vejamos abaixo:

$$
\begin{array}{ccccccccccccccccccccc}
 & & & & & & & & \binom{0}{0} & & & & & & & & & & \\
 & & & & & & & \binom{1}{0} & & & & \binom{1}{1} & & & & & & & \\
 & & & & & & \binom{2}{0} & & & & \binom{2}{1} & & & & \binom{2}{2} & & & & \\
 & & & & & \binom{3}{0} & & & & \binom{3}{1} & & & & \binom{3}{2} & & & & \binom{3}{3} & \\
 & & & & \binom{4}{0} & & & & \binom{4}{1} & & & & \binom{4}{2} & & & & \binom{4}{3} & & & \binom{4}{4} \\
\ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots
\end{array}
$$

Isto é:

A linha 1 contém o coeficiente do desenvolvimento de $(x+a)^0$

A linha 2 contém os coeficientes do desenvolvimento de $(x+a)^1$

A linha 3 contém os coeficientes do desenvolvimento de $(x+a)^2$

.....

Também podemos escrever o triângulo de Pascal substituindo cada coeficiente binomial pelo seu valor, isto é:

$$
\begin{array}{ccccccccccccccccccccc}
 & & & & & & & & 1 & & & & & & & & & & \\
 & & & & & & & 1 & & & & 1 & & & & & & & \\
 & & & & & & 1 & & & & 2 & & & & 1 & & & & \\
 & & & & & 1 & & & & 3 & & & & 3 & & & & 1 & \\
 & & & & 1 & & & & 4 & & & & 6 & & & & 4 & & & 1 \\
 & & & 1 & & & & 5 & & & & 10 & & & & 10 & & & & 5 & & & 1 \\
 & & 1 & & & & 6 & & & & 15 & & & & 20 & & & & 15 & & & & 6 & & & & 1 \\
 & 1 & & & & 7 & & & & 21 & & & & 35 & & & & 35 & & & & 21 & & & & 7 & & & & 1 \\
\ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots & & \ldots
\end{array}
$$

Para construir o triângulo de Pascal não é necessário calcular os coeficientes binomiais, basta usarmos algumas de suas propriedades. Vejamos:

(1) Em cada linha do triângulo, o primeiro e o último número são iguais a 1.

(2) A partir da terceira linha, cada número (exceto o primeiro e o último) é a soma dos números da linha anterior, imediatamente acima dele.

(3) Na mesma linha, dois números equidistantes dos extremos são iguais.

Exemplo: Desenvolva $(2a-b)^5$. Solução:

Observando a forma como é desenvolvido o binômio de Newton e a 6ª linha do triângulo de Pascal, temos:

$$(2a-b)^5 = 32a^5 - 80a^4b + 80a^3b^2 - 40a^2b^3 + 10ab^4 - b^5$$

■

5.6.9 Fatoração

Definição: Fatorar é o termo usado na álgebra para designar a decomposição que se faz de cada um dos elementos que integram um produto. O objetivo da fatoração é a simplificação das fórmulas matemáticas em que ocorre a multiplicação, especialmente das chamadas equações.

As fatorações mais conhecidas são:

1. Fator comum em evidência

   Nessa forma de fatoração, determinamos o elemento comum aos termos que formam o polinômio e escrevemos o polinômio como o produto $m \cdot n$, em que m é o elemento comum e n é o resultado da divisão dos termos do polinômio pelo elemento comum.

   Exemplo: $a^3 - 5a^2 = a^2(a-5)$

2. Agrupamento

Agrupamos os termos semelhantes de forma que seja possível utilizar a fatoração por evidência mais de uma vez.

Exemplo: $5x - xy + 15 - 3y = (x+3).(5-y)$

Solução:

$5x - xy + 15 - 3y = 5x + 15 - xy - 3y = 5(x+3) - y(x+3) = (x+3).(5-y)$

■

3. Diferença entre dois quadrados

   Extraímos a raiz quadrada dos elementos e os resultados obtidos formarão um produto entre binômios, na forma produto da soma e da diferença.

   Exemplo: $a^4 - 9 = (a^2 - 3) \cdot (a^2 + 3)$

   Solução:

   Extraindo as raízes, temos: $\sqrt{a^4} = a^2$ e $\sqrt{9} = 3$

   Logo, $(a^2 - 3) \cdot (a^2 + 3) = a^4 + 3a^2 - 3a^2 + 9 = a^4 - 9$

   ■

4. Trinômio quadrado perfeito

   Basta determinar o produto notável responsável pela formação do trinômio.

   Exemplo: $x^2 + 4x + 4 = (x+2)^2$

   Solução:

   Extraindo as raízes, temos: $\sqrt{x^2} = x$ e $\sqrt{4} = 2$

   Fazendo o produto $2 \cdot x \cdot 2 = 4x$. Logo: $(x+2)^2 = x^2 + 4x + 4$

   ■

Exemplo: Determine as raízes do polinômio $P(x) = 4x^4 - 9x^2 + 16x^3 - 36x$.

Solução:

Determinar as raízes de um polinômio é encontrar valores para x tais que o valor numérico de $P(x)$ é igual a 0, ou seja $P(x) = 0$. Logo:

$$4x^4 - 9x^2 + 16x^3 - 36x = 0$$

Observe que há um elemento comum em todos os termos desse polinômio, o x. Colocando x em evidência, temos:

$$4x^4 - 9x^2 + 16x^3 - 36x = 0 \Longleftrightarrow x(4x^3 - 9x + 16x^2 - 36) = 0$$

Usando a fatoração por agrupamento, temos:

$$\begin{aligned} x(4x^3 - 9x + 16x^2 - 36) = \\ x(4x^3 + 16x^2 - 9x - 36) = \\ x\left[4x^2(x+4) - 9(x+4)\right] = 0 \\ x\left[(x+4)(4x^2 - 9)\right] = \\ x(x+4)(4x^2 - 9) = 0 \end{aligned}$$

Veja que $4x^2 - 9 = (2x-3)(2x+3)$, então:

$$x(x+4)(4x^2 - 9) = x(x+4)(2x-3)(2x+3) = 0$$

Logo:

$x = 0, x+4 = 0 \Rightarrow x = -4, 2x-3 = 0 \Rightarrow x = \dfrac{3}{2}$ ou $2x+3 = 0 \Rightarrow x = -\dfrac{3}{2}$

Portanto, as raízes reais do polinômio $P(x)$ são $0, -4, \dfrac{3}{2}$ e $-\dfrac{3}{2}$.

■

5.7 Referências bibliográficas

ANDRADE, C. H. V. d. **História Ilustrada da Medicina da Idade Média ao Século do Início da Razão: a medicina no seu contexto sociocultural história.** 1. ed. São Paulo: Editora Baraúna, 2015.

BIANCHINI, E. **Matemática, 8o ano. 6. ed.** São Paulo: Moderna, 2006.

IEZZI, G. **Fundamentos de Matemática Elementar, 5: combinatória, probabilidade.** 8. ed. São Paulo: Atual, 2013a.

IEZZI, G. **Fundamentos de Matemática Elementar, 6: complexos, polinômios, equações**. 8. ed. São Paulo: Atual, 2013b.

MORGADO A C E CARVALHO, P. C. P. **Coleção PROFMAT: matemática discreta**. Rio de janeiro: SBM, 2013.

PALARO, L. A. **Concepção de Educação Matemática de Henri Lebesgue**. 584 p. Tese (Doutorado em Educação Matemática) — PUC/SP, São Paulo,2006.

RUIZ, R. L. **Blaise pascal: o homem e a ciência.** Revista Ética e Filosofia Política, v. 1, n. 12, 2010.

SANTOS, C. et al. **10 livros, 10 regiões, 10 jogos para aprender e divertir-se**. Santo Tirso: Norprint, 2008.

SERRASQUEIRO, J. A. **Tratado de Álgebra Elementar**. 9. ed. Coimbra: Livraria Central de J. Diogo Pires, 1906.

Capítulo 6

Sobre algoritmos de ordenação e sua abordagem no ensino médio

Me. Ilso Francisco dos Santos[1]
Dr. Marcelo Pedro dos Santos[2]

Resumo: O presente artigo se baseia no trabalho *Algoritmos de Ordenação: uma abordagem didática para o ensino médio* (SANTOS, 2020). A proposta do trabalho se concentra numa abordagem didática de três algoritmos de ordenação tomando como base competências e habilidades propostas na Base Nacional Curricular Comum (BNCC). Os algoritmos de ordenação estudados foram o *Bubble Sort*, *Selection Sort* e o *Quick Sort*. Inicialmente foi realizada uma análise de competências e habilidades presentes não somente na BNCC, o documento mais recente, mas também nos Parâmetros Curriculares Nacionais de Matemática: 5ª a 8ª séries, do Ensino Médio, Complemento para o Ensino Médio e dos Parâmetros Curriculares do Estado de Pernambuco. Os conteúdos didáticos necessários para a compreensão do trabalho são: Somatórios e Funções Afim, Quadrática e Logarítmica, necessárias para avaliarmos os desempenhos assintóticos dos algoritmos. Alguns

[1]Professor da rede pública Estadual e Municipal de Ensino em Pernambuco, ilsofrancisco@gmail.com.

[2]Professor do Departamento de Matemática - Universidade Federal Rural de Pernambuco, marcelo.pedrosantos@ufrpe.br.

exemplos dos algoritmos servirão para o entendimento do funcionamento, bem como a forma como sua complexidade é analisada e propostas de atividades são colocadas no intuito de mostrar a viabilidade da abordagem do tema no Ensino Médio.

Palavras-chave: Parâmetros Curriculares; Competências; Algoritmos de Ordenação; Complexidade.

6.1 Introdução

De acordo com as Diretrizes Curriculares Nacionais da Educação Básica, a escola, no desempenho de suas funções, deve construir e utilizar métodos, estratégias e recursos de ensino que melhor atendam às características cognitivas e culturais dos alunos. O tema Algoritmos de Ordenação propicia uma abordagem diversificada da Matemática em um contexto que auxilia no desenvolvimento cognitivo e cultural dos estudantes. O presente trabalho se propõe a analisar, à luz da BNCC, o funcionamento e a complexidade dos algoritmos de ordenação *Bubble Sort*, *Selection Sort* e *Quick Sort*, comparando seus desempenhos por meio de funções matemáticas, tanto algebricamente quanto graficamente.

Apresentaremos exemplos dos algoritmos de ordenação e atividades afins com o propósito de trazer subsídios educacionais para uma abordagem didática do tema no Ensino Médio. Apesar da análise dos Parâmetros Curriculares se estenderem ao Ensino Fundamental, optou-se por direcionar o trabalho com o tema para o Ensino Médio. A justificativa de tal direcionamento deve-se ao fato de se supor que os estudantes já possuam um repertório matemático capaz de compreender os conceitos e procedimentos abordados no estudo dos algoritmos já citados. O tema dos algoritmos está intrinsecamente relacionado à computação, no entanto não faremos tal abordagem neste trabalho e nos resumiremos ao viés matemático do tema, recorrendo de forma superficial aos conteúdos de Somatórios e Funções Afim, Quadrática e Logarítmica.

Tendo como fundamento que o Ensino Médio é uma etapa de aprofun-

damento de conceitos e procedimentos trabalhados com os estudantes no Ensino Fundamental, consideramos plausível uma análise dos Parâmetros Curriculares nessa etapa do Ensino. Não se pretende aprofundar a matemática utilizada para obter a Função que representa a complexidade de cada algoritmo e nem a análise assintótica de cada função. A proposta é apenas mostrar, de forma inteligível, como se pode chegar aos resultados e a maneira que tais resultados são utilizados na análise dos algoritmos. Para tanto, traremos exemplos de cada algoritmo de ordenação, com suas respectivas funções representativas e complexidades correlatas. No que diz respeito a análise assintótica, utilizada para representar a complexidade de cada algoritmo, nos limitaremos a apresentar qual a representação da mesma sem que haja preocupação de como se chegou a tal representação, pois tais demonstrações fogem do escopo do trabalho.

Por fim, deve-se atentar para o fato de que o estudo do tema não se encerra nessa simples abordagem, restando um vasto campo a ser investigado por outros pesquisadores com focos diversos dos que foram aqui destacados.

6.2 Fundamentos teóricos e metodológicos

6.2.1 Análise dos parâmetros curriculares

Inicialmente buscou-se mostrar uma possível evolução curricular nos documentos oficiais, ou melhor, nos Parâmetros Curriculares Nacionais e também do Estado de Pernambuco, na busca de competências e habilidades que tivessem relação com o tema. Os Parâmetros Curriculares Nacionais de Matemática 5ª a 8ª séries (PCN - 5ª a 8ª) já trazem uma problematização ao declararem:

> Situação - problema é o ponto de partida da atividade matemática e não a definição. No processo de ensino e aprendizagem, conceitos, ideias e métodos matemáticos devem ser abordados mediante a exploração de problemas, ou seja, de situações em

> que os alunos precisem desenvolver algum tipo de estratégia para resolvê-las (BRASIL, 1998, p. 40).

Segundo o mesmo documento, é por meio da exploração de situações-problemas que o estudante reconhecerá diferentes funções da álgebra, bem como exercitará a indução e a dedução em Matemática. Apesar dos PCN - 5ª a 8ª séries já sugerirem o quão importante é uso da tecnologia, do computador e de softwares no processo de ensino - aprendizagem, ainda não se faz menção ao tema algoritmos. Nos *Parâmetros Curriculares Nacionais de Matemática*, afirma-se que: "muitos conteúdos importantes são descartados por serem julgados, sem uma análise adequada, que não são de interesse para os alunos porque não fazem parte de sua realidade ou não têm uma aplicação prática imediata" (BRASIL, 1998). Encontramos também nesse documento uma referência aos conteúdos procedimentais e a capacidade do saber fazer. É evidente que o trabalho com algoritmos se enquadra em tal espécie de conteúdo, visto que se trata de um procedimento ou conjunto deles.

Na etapa do Ensino Médio, deve-se propor ao estudante uma ampliação dos conhecimentos adquiridos no Ensino Fundamental, bem como uma elevação no nível de abstração de conceitos e procedimentos matemáticos. De acordo com os Parâmetros Curriculares Nacionais para o Ensino Médio (PCNEM), essa etapa "[$\cdots$] deve ser mais do que memorizar resultados dessa ciência e que a aquisição do conhecimento matemático deve estar vinculada ao domínio de um saber fazer Matemática e de um saber pensar matemático"(BRASIL, 2000). Também há de se garantir, nessa etapa do ensino, que o estudante seja capaz de lidar com o conceito de funções em situações diversas, ajustando seus conhecimentos na busca de soluções de problemas, na construção de modelos para interpretação e investigação em Matemática. Também é preciso garantir que ele aprofunde conhecimentos sobre números e álgebra, de forma conectada com outros conteúdos. Nos PCNEM, algumas competências de base foram elencadas em duplas, as de representação e comunicação, bem como as de investigação e compreensão. A relação de tais competências com o tema Algoritmos de Ordenação é

bastante clara, pois a análise destes proporciona a representação e a comunicação por meio de esquemas, linguagem natural e fluxogramas, assim como instiga a investigação e a compreensão quando se busca assimilar o procedimento utilizado por cada algoritmo e a função que descreve o número de comparações necessárias para ordenar a lista (vetor), como será visto adiante. Também se averiguou, na versão complementar para o Ensino Médio, os PCNEM$_+$, um enfoque na contextualização dos conteúdos matemáticos e na interdisciplinaridade, retomando as competências elencadas nos PCNEM, dentre as quais podemos destacar:

> Traduzir uma situação dada em determinada linguagem para outra; por exemplo, transformar situações dadas em linguagem discursiva em esquemas, tabelas, gráficos, desenhos, fórmulas ou equações matemáticas e vice-versa, assim como transformar as linguagens mais específicas umas nas outras, como tabelas em gráficos ou equações (BRASIL, 2002, p. 115).

A competência citada anteriormente está inserida nas de representação e comunicação, que possuem ampla relação com a proposta didática em tela, pois o trabalho com Algoritmos de ordenação favorece toda essa gama de representações e formas de comunicar o conhecimento matemático a partir da situação-problema. Os PCNEM$_+$ também propõem o ensino por meio de temas estruturadores para que se alcancem as competências e habilidades desejadas. Nesse caso, o tema Algoritmos de Ordenação poderia servir como estruturador, pois favorece a articulação lógica entre diferentes ideias e conceitos matemáticos.

Já os Parâmetros Curriculares da Educação Básica do Estado de Pernambuco também trazem tópicos semelhantes aos apresentados anteriormente nos documentos já citados, como a resolução de problemas e a modelagem matemática, mas difere na nomenclatura dada às competências e habilidades. Nesse documento, usa-se a expressão Expectativas de Aprendizagem:

> As expectativas de aprendizagem explicitam aquele mínimo que o estudante deve aprender para desenvolver as competências básicas na disciplina. Em outras palavras, elas descrevem

> o "piso" de aprendizagens, e não o "teto". Dependendo das condições de cada sala de aula, elas podem ser ampliadas e/ou aprofundadas (PERNAMBUCO, 2012, p. 13).

O documento destaca, dentre outras coisas, o trabalho com situações-problemas, os problemas abertos em detrimento dos fechados e a modelagem matemática. Algumas expectativas de aprendizagem que possuem relação com o estudo de Algoritmos de Ordenação perpassam por todo os ensino médio como "reconhecer função como modelo matemático para o estudo das variações entre grandezas do mundo natural ou social" (PERNAMBUCO, 2012, p. 21).

A BNCC, último e mais recente documento analisado, traz competências e habilidades relacionadas com o trabalho sobre Algoritmos de Ordenação, tanto na parte destinada para Ensino Fundamental, quanto para o Ensino Médio. Como o aprofundamento e ampliação dos conceitos devem ser consolidados no Ensino Médio, esse documento propõem o desenvolvimento de competências e habilidades de forma análoga aos PCNEM. De acordo com a BNCC: "Competência é definida como a mobilização de conhecimentos (conceitos e procedimentos), habilidades (práticas cognitivas e socioemocionais), atitudes e valores para resolver demandas complexas da vida [$\cdots$]" (BRASIL, 2018). Na seção do Ensino Fundamental, são explicitadas competências gerais da Educação Básica e competências específicas de cada área do conhecimento, dentre as quais são indicadas as habilidades requeridas. Os conteúdos, por outro lado, são separados em unidades temáticas do 1º ao 9º ano, como vem a seguir, para a disciplina de Matemática: Números, Álgebra, Geometria, Grandezas e Medidas, Probabilidade e Estatística. Consta neste documento que "A linguagem algorítmica tem pontos em comum com a linguagem algébrica, sobretudo em relação ao conceito de variável" (BRASIL, 2018, p. 271). Quanto às habilidades diretamente relacionadas ao tema, destacamos:

> -Representar por meio de um fluxograma os passos utilizados para resolver um grupo de problemas.

> -Descrever, por escrito e por meio de um fluxograma, um algoritmo para a construção de um triângulo qualquer, conhecidas as medidas dos três lados.
>
> -Descrever, por escrito e por meio de um fluxograma, um algoritmo para a construção de um polígono regular (como quadrado e triângulo equilátero), conhecida a medida de seu lado.
>
> -Identificar a regularidade de uma sequência numérica ou figural não recursiva e construir um algoritmo por meio de um fluxograma que permita indicar os números ou as figuras seguintes (BRASIL, 2018).

Percebe-se um uso pretensioso de fluxogramas em várias habilidades mas não há, ainda, relação com o pensamento computacional que "envolve as capacidades de compreender, analisar, definir, modelar, resolver, comparar e automatizar problemas e suas soluções, de forma metódica e sistemática, por meio do desenvolvimento de algoritmos" (BRASIL, 2018, p. 474).

A estruturação das competências e habilidades para o Ensino Médio se fez, na BNCC, de forma distinta do Ensino Fundamental. No Ensino Médio, as competências específicas não estão diretamente relacionadas à unidades temáticas, configurando uma liberdade de associação de acordo com a situação-problema, tema estruturador ou itinerários formativos que sejam escolhidos. Porém, merecem destaque algumas habilidades que possuem forte relação com o tema Algoritmos de Ordenação. São elas:

> -Investigar e registrar, por meio de um fluxograma, quando possível, um algoritmo que resolve um problema.

> -Utilizar conceitos iniciais de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática (BRASIL, 2018, p. 538-539).

Observa-se que no Ensino Médio já se busca uma relação mais estreita com o pensamento computacional ao se referir à linguagem de programação e implementação de algoritmos, fato não antes visto na parte do Ensino Fundamental.

Por fim, pudemos constatar que são notáveis as competências e habilidades constantes nos Parâmetros Curriculares analisados que podem ser desenvolvidas por meio da abordagem didática do tema proposto neste trabalho. E, como a BNCC é o documento mais recente, faz-se necessário mais estudos e propostas tangíveis ao processo de ensino-aprendizagem na educação básica.

6.2.2 Algoritmos de ordenação e complexidade

Um Algoritmo de Ordenação tem como procedimento ordenar os n elementos de uma lista finita, a qual passaremos a chamar de vetor, em ordem crescente ou decrescente.

Os primeiros contatos que os estudantes têm com o significado de algoritmo se dá com o estudo de procedimentos matemáticos, mas sabemos ser tal definição mais abrangente. Segundo Ribeiro, algoritmo é "um conjunto de regras e operações bem definidas e ordenadas, destinadas à solução de um problema ou de uma classe de problemas, em um número finito de etapas" (2018, p. 32). Já para Cormen et al., "um algoritmo é qualquer procedimento computacional bem definido que toma algum valor ou um conjunto de valores como **entrada** e produz algum valor ou conjunto de valores como **saída**" (2002). Este último acrescenta que problemas de ordenação são comuns e que a ordenação é uma operação fundamental na ciência da computação.

Uma ordenação por **comparação simples** realiza ou não a troca dos elementos dos vetores dois a dois após compará-los como é caso dos algo-

ritmos ***Bubble Sort*** e ***Selection Sort***. Já há os algoritmos que utilizam uma ordenação por comparação mais complexa chamada de **método eficiente** como ocorre com o ***Quick Sort***. Este último possui uma técnica chamada **divisão e conquista** que consiste em dividir um problema a ser resolvido em problemas menores, que podem ser divididos em partes ainda menores. A partir disso, encontram-se as soluções dos problemas menores e combina-se as soluções dos problemas menores em uma solução global, que resolve o problema inicial.

Para realizar-se a comparação da eficiência dos Algoritmos de Ordenação utilizamos a **notação assintótica** ou notação **O-grande**, representada pelo símbolo O. que se refere a um limite assintótico superior. Vale salientar que, ao analisar assintoticamente os Algoritmos de Ordenação, considera-se o termo de maior crescimento da lei de formação da função representante do desempenho do Algoritmo de Ordenação. Entretanto, não faz parte do escopo deste trabalho um aprofundamento, tanto no que diz respeito à representação da notação assintótica acima citada, quanto do motivo da escolha do termo de maior crescimento que nos referimos anteriormente.

> Quando observamos tamanhos de entrada grandes o suficiente para tornar relevante apenas a ordem de crescimento do tempo de execução, estamos estudando a **eficiência assintótica** dos algoritmos. Ou seja, estamos preocupados com a maneira como o tempo de execução de um algoritmo aumenta com o tamanho da entrada no *limite*, à medida que o tamanho da entrada aumenta indefinidamente. Em geral, um algoritmo que é assintoticamente mais eficiente será a melhor escolha para todas as entradas, exceto as muito pequenas (CORMEN et al., 2002, p. 51).

Para que se tenha mais clareza desse conceito segue uma definição da notação **O-grande** e um simples exemplo, pois tal notação será utilizada mais adiante.

Para uma dada função $g(n)$, denotamos por $O(g(n))$ o conjunto de funções $O(g(n)) = \{f(n)$: *existem constantes* c e n_o *tais que* $0 \leq f(n) \leq c \cdot g(n)$ *para todo* $n \geq n_o\}$.

Exemplo 1. *Considere as funções* $f(n) = n^2 + 5n + 1$ *e* $g(n) = n^2$.
Tem-se, para $n \geq 1$, $n^2 + 5n + 1 \leq n^2 + 5n^2 + n^2 = 7 \cdot n^2 \Longrightarrow f(n) \leq 7 \cdot g(n)$.
Portanto:

$$f(n) \in O(g(n)).$$

Segundo Cormen et al., "para indicar que uma função $f(n)$ é membro de $O(g(n))$, escrevemos $f(n) = O(g(n))$" (2002, p. 35).

No caso do vetor já estar ordenado configura-se o **melhor caso** da ordenação e, se estiver em ordem contrária, teremos o **pior caso da ordenação**. Existe ainda o **caso médio** da ordenação que considera o tempo médio para se percorrer $n/2$ elementos do vetor até obter o elemento procurado na ordenação. Contudo, o caso médio difere dependendo do tipo de algoritmo, sendo objeto de um estudo mais aprofundado que não é o foco deste trabalho.

Apesar do conceito de Fluxogramas estar associado ao estudo de algoritmos, merecendo um destaque nas competências e habilidades em matemática na BNCC, não faremos tal abordagem neste documento e sugerimos uma leitura do capítulo 3 de Santos (2020).

6.2.2.1 *Bubble Sort*

O Algoritmo de Ordenação ***Bubble Sort*** é considerado um dos mais simples. É também conhecido como Ordenação por Flutuação, daí o nome ***Bubble***, cuja tradução para o Português é **Bolha**. Seu procedimento se dá da seguinte maneira: para uma ordenação crescente, iniciando-se com o primeiro elemento, compara-se cada elemento do vetor com o posterior, caso este seja maior, muda-se de posição com o anterior, caso não o seja, a troca de posição não é feita e passa-se para o próximo par de comparação até que não haja mais comparações e o vetor fique ordenado. Para uma ordenação decrescente, compara-se o elemento com o posterior, caso este

seja maior, não se muda sua posição atual. Segue-se para o próximo par de comparação e assim sucessivamente até que o vetor esteja ordenado. Além da simplicidade, outra vantagem desse Algoritmo de Ordenação é a estabilidade, mas a lentidão o deixa em desvantagem com relação a outros Algoritmos de Ordenação. É indicando para pequenos vetores e contraindicado para vetores com um número grande de elementos.

Tomemos, como exemplo, o vetor $A = (5,4,3,2,1)$, que possui o número de elementos $n = 5$. O objetivo é colocá-lo em ordem crescente com a estratégia de comparação do *Bubble Sort*. O vetor A caracteriza o pior caso do *Bubble Sort*.

Os procedimentos se dão da seguinte maneira:
Passo I. 5 compara com 4 e troca de posição, pois 5 > 4;
Passo II. 5 compara com 3 e troca de posição, pois 5 > 3;
Passo III. 5 compara com 2 e troca de posição, pois 5 > 2;
Passo IV. 5 compara com 1 e troca de posição, pois 5 > 1.
Agora, ocorre o mesmo com o 4.
Passo V. 4 compara com 3 e troca de posição, pois 4 > 3;
Passo VI. 4 compara com 2 e troca de posição, pois 4 > 2;
Passo VII. 4 compara com 1 e troca de posição, pois 4 > 1.
Passo VIII. 3 compara com 2, como 3 < 2, troca de posição com este.
Passo IX. 3 compara com 1 e também troca de posição com ele.
Passo X. 2 compara com 1 e troca de posição.

Outra forma de representar o procedimento está descrito na tabela a seguir:

Tabela 6.1: Exemplo do *Bubble Sort* com 5 elementos, $n = 5$, representando o pior caso.

VETOR	**Nº de comparações**
5-4-3-2-1	4 comparações (5 e 4, 5 e 3, 5 e 2, 5 e 1).
4-3-2-1-5	3 comparações (4 e 3, 4 e 2, 4 e 1).
3-2-1-4-5	2 comparações (3 e 2, 3 e 1).
2-1-3-4-5	1 comparação (2 e 1).
1-2-3-4-5	$(n-1)$ iterações: vetor ordenado.

Fonte: Adaptado de Oliveira (2004).

Seja, por exemplo, C_n a quantidade de comparações quando se retira o elemento a de um vetor de n elementos. Portanto, tem-se $C_n = n-1$ comparações. Com esta ideia, pode-se escrever

$$\sum_{i=1}^{n} C_i = (n-1) + (n-2) + \cdots + 1 = \frac{n(n-1)}{2} = \frac{n^2}{2} - \frac{n}{2}, \qquad (6.1)$$

comparações no pior caso. Sua eficiência (complexidade) é, assintoticamente, representada por $O(n^2)$. No melhor caso do *Bubble Sort*, quando o vetor já se encontra ordenado, teremos apenas $(n-1)$ iterações e sua eficiência é representada por $O(n)$. No pior caso e no caso médio, temos uma complexidade representada por uma função quadrática e, no melhor caso, por uma função linear.

6.2.2.2 *Selection Sort*

O termo ***Selection Sort***, de origem inglesa, significa **Ordenação por seleção**. Utiliza o método ou paradigma da comparação por seleção ou seleção direta. Nela, a ideia é ordenar a lista selecionando, em cada iteração, os menores itens e ordenando-os da esquerda para direita, no caso de ordem crescente. Quando o menor elemento da lista é localizado na 1ª posição, ocorre nova iteração para localizar o segundo menor elemento da lista na 2ª posição e assim sucessivamente, até que a lista esteja em ordem crescente.

Algumas vantagens desse algoritmo são: fácil implementação e uso de pouca memória. Entre as desvantagens destaca-se, principalmente, seu desempenho, que é ruim em todos os casos: melhor, médio e pior, sendo indicado apenas para pequenas listas. Além disso, ele não é um algoritmo estável.

Como exemplo, consideremos o vetor $B = (5,3,1,2,4)$, com $n = 5$ elementos, o qual será ordenado de acordo com os seguintes procedimentos do *Selection Sort*.

Passo I. 5 compara com 3, 3 é menor e troca de posição com 5, assim 3 vai para a 1ª posição;
Passo II. 3 compara com 1, 1 é menor e troca de posição com 3, ou seja, 1 fica na 1ª posição e 3 na 3ª posição;
Passo III. 1 compara com 2, 1 é menor e continua sem trocar;
Passo IV. 1 compara com 4; 1 é menor e continua sem trocar.
O 1 é o menor elemento e ocupa a 1ª posição, após isso temos os seguintes passos:
Passo V. 5 compara com 3, 3 é menor e muda de posição com 5;
Passo VI. 3 compara com 2, 2 é menor e muda de posição com 3;
Passo VII. 2 compara com 4, 2 é menor e não muda de posição.
O 2 irá para a 2º posição no lugar do 3, e o 3 irá para a 4ª posição.
Seguem-se os passos:
Passo VIII. 5 compara com 3, 3 é menor e muda de posição com 5;
Passo IX. 3 compara com 4, 3 é menor e não muda de posição.
O 3 irá para a 3ª posição no lugar do 5, que está na posição inicial do 1, e o 5 vai para a 4ª posição, onde estava o 3. Realizada a troca, teremos a última comparação.
Passo X. 5 compara com 4, 4 é menor e muda de posição com 5. O 4 vai para a 4ª posição e o 5 para a 5ª posição.

A representação dos procedimentos realizados resume-se na tabela abaixo.

Utilizando o mesmo raciocínio da equação (6.1), para um vetor de n

Tabela 6.2: Exemplo do *Selection Sort* com 5 elementos, $n = 5$, representando o caso médio.

VETOR	**Nº de comparações**
5-3-1-2-4	4 comparações (5 e 3, 3 e 1, 1 e 2, 1 e 4)
1-5-3-2-4	3 comparações (5 e 3, 3 e 2, 2 e 4)
1-2-5-3-4	2 comparações (5 e 3, 3 e 4)
1-2-3-5-4	1 comparação (5 e 4)
1-2-3-4-5	$(n-1)$ iterações: vetor ordenado

Fonte: Adaptado de Oliveira (2004).

elementos, temos o total de Comparações C_n dado por:

$$\sum_{i=1}^{n} C_i = (n-1) + (n-2) + ... + 1 = \frac{n(n-1)}{2} = \frac{n^2}{2} - \frac{n}{2}. \qquad (6.2)$$

Sua eficiência é representada assintoticamente por $O(n^2)$ em qualquer caso e, por isso, é considerado de péssimo desempenho em comparação com outros algoritmos.

6.2.2.3 *Quick Sort*

Será visto nesta seção um Algoritmo de Ordenação chamado ***Quick Sort***. Ele utiliza uma estratégia de ordenação por comparação bastante diferente das duas abordadas anteriormente. Ela é conhecida por divisão e conquista. Nesse tipo de Algoritmo de Ordenação, o vetor é dividido em duas partes, a partir de um elemento denominado pivô, sendo colocados, antes do pivô, os elementos menores ou iguais ao mesmo e, depois dele, os elementos maiores. O processo se repete em cada uma das partes sucessivamente até que se obtenha partes com apenas um elemento. Para finalizar, acontece o que se chama de conquista: os resultados são combinados e obtém-se a ordenação requerida. É um algoritmo bastante

popular, considerado rápido e eficiente. Utiliza técnicas de recursão sendo considerado complexo e não estável. A escolha do pivô, bem como a forma de particionamento, são situações que não serão levadas em conta neste estudo, interessando apenas a análise e comparação com os demais algoritmos acima. No esquema a seguir, apresenta-se um exemplo de como seria a ordenação utilizando a estratégia de divisão e conquista do ***Quick Sort***.

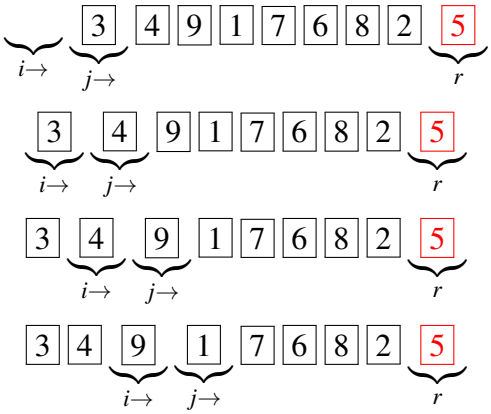
Dado o vetor $Q = (5,3,4,9,1,7,6,8,2)$, sendo $n = 9$. Uma das possíveis ordenações utilizando o ***Quick Sort*** seria:

5	3	4	9	1	7	6	8	2

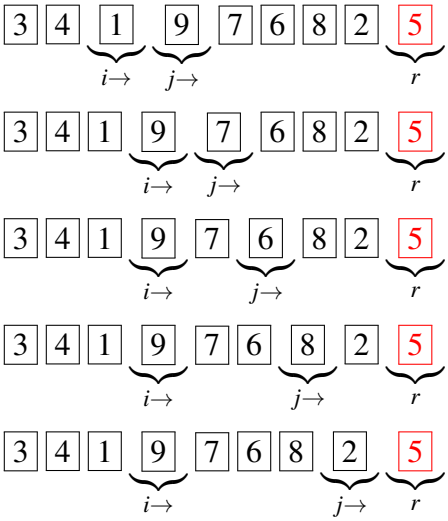
Considere 5 o pivô escolhido.

Considere r a última posição dos elementos que formam o vetor e $p \neq r$ qualquer outra posição que um elemento ocupa no vetor. Após a escolha do pivô, este fica na posição r e, para que os valores menores que o pivô fiquem antes dele e os valores maiores que ele fiquem depois, as comparações ocorrem da seguinte maneira: são criadas duas variáveis i e j representando as posições dos valores. Essas variáveis serão usadas para percorrer o vetor de entrada de modo que cada posição i seja percorrida da esquerda para direita, para localizar elementos com valores menores que o pivô, e cada posição j seja também percorrida da esquerda para a direita, até localizar elementos maiores que o pivô. Inicia-se com $i = j - 1$. Ao mesmo tempo em que j percorre o vetor, na busca dos valores maiores que o pivô, i vai, logo após, localizando os valores menores que o pivô. À medida que forem localizando, respectivamente, valores maiores e menores, eles passam para a posição imediatamente posterior até que j localize um valor menor que o pivô e i localize um valor maior que o pivô. Nesse caso, o valor de posição j troca de lugar com o valor de posição i. O procedimento continua até que todos os valores menores que o pivô estejam numa posição $p \leq i$ e os valores maiores que o pivô estejam numa posição $i < p \leq j$. Feito isso, o pivô ocupará a posição $i + 1$.

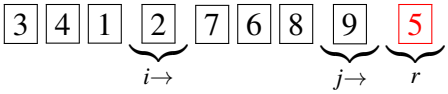
Com relação ao vetor Q teremos:



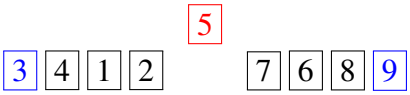
Aqui, o valor 1 muda de posição com o valor 9 e continuamos com o vetor no seguinte formato:



Observe que ocorreu, simultaneamente, de j localizar um valor menor que o pivô 5 e i localizar um valor maior que o pivô 5. Daí, o valor 2 muda de posição com o valor 9, ficando o vetor com nova configuração.

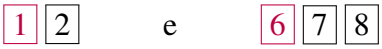


Temos que j está na posição $r-1$ e já encerrou o percurso pelo vetor, de modo que o valor na posição i também não sofrerá mais nenhuma troca com algum valor de posição j. Assim, o pivô 5 de posição r ocupará a posição $i+1$ e ficaremos com dois subvetores: o primeiro antes do pivô, com elementos menores que 5 e o segundo, depois do pivô, com elementos maiores que 5.



Escolhemos agora, nos subvetores, os pivôs 3 e 9, respectivamente, ocorrendo o mesmo procedimento nos subvetores quando o pivô foi 5. A configuração nos dois subvetores fica:

Agora escolhemos nos subvetores 1 2 e 7 6 8 os pivôs 1 e 6, respectivamente. Novamente a estratégia de divisão é efetuada e os subvetores ficam com a seguinte ordem:



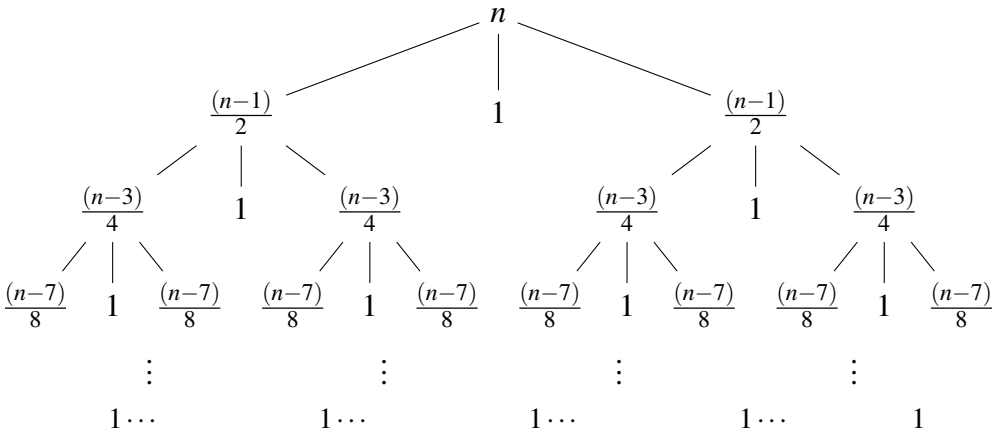
Apesar de o vetor já estar ordenado, os subvetores sofrem subdivisões até que se obtenha o último subvetor com tamanho unitário. Desse modo, no subvetor não unitário, 7 8, escolhemos o pivô 7. Executando novamente o procedimento de divisão do *Quick Sort*, fica o vetor ordenado da seguinte maneira:

Observe que a escolha do pivô é aleatória, mas o pivô ideal seria aquele que dividisse o vetor ou subvetor em tamanhos aproximadamente iguais, ou seja, um pivô que represente um valor mediano do vetor ou subvetor. Contudo, isso não ocorre na prática, e a escolha aleatória dos pivôs acarretam

nas situações de melhor caso, pior caso ou caso médio. No melhor caso, o particionamento produz segmentos(subvetores) de tamanhos iguais; já o pior caso ocorre quando o pivô é o maior (ou menor) elemento do vetor ou subvetor. O caso médio ocorre quando o particionamento é desbalanceado, como, por exemplo, numa partição em que todos os subproblemas estejam na proporção 1 para 8 em cada nível.

A seguir, faz-se uma abordagem matemática na análise da complexidade, para o melhor caso do *Quick Sort*, que se mostre clara e acessível para o Ensino Médio e auxilie os professores na obtenção da complexidade de tal algoritmo. A comparação por árvore de distribuição binária foi a escolha que se julgou mais viável para se conjecturar a função que representa o desempenho do ***Quick Sort***.

Figura 6.1: Árvore de distribuição binária do *Quick Sort*, no melhor caso, para um vetor de n elementos.



Fonte: Adaptado de Silva (2013).

Na tabela a seguir, apresenta-se uma compilação do que está representado na árvore anterior, com o intuito de facilitar a obtenção da função que representa o desempenho desse Algoritmo de Ordenação.

Por questões didáticas, não detalharemos o procedimento matemático que traduz a análise assintótica do *Quick Sort*, apenas mostraremos os

Tabela 6.3: Resumo da distribuição binária do *Quick Sort* representada na Figura (6.1).

Níveis(altura)	**Nº de subproblemas**	Tamanho do subproblema
0	1	n
1	2	$(n-1)/2$
2	4	$(n-3)/4$
3	8	$(n-7)/8$
$\vdots$	$\vdots$	$\vdots$
j	2^j	$\frac{[n-(2^j-1)]}{2^j}$

Fonte: Adaptado de Silva (2013).

resultados obtidos e deixaremos a análise dos detalhes em Santos (2020, p. 60).

Sabendo-se o valor de $\lfloor j \rfloor$, é possível calcular o trabalho total, indicado por $T(j)$, bastando somar o trabalho por nível ao longo dos níveis, isto é:

$$T(j) = \sum_{i=1}^{\lfloor j \rfloor}(n-2^i+1) = \sum_{i=1}^{\left\lfloor \log_2 \frac{(n+1)}{2} \right\rfloor}(n-2^i+1) = \underbrace{\sum_{i=1}^{\left\lfloor \log_2 \frac{(n+1)}{2} \right\rfloor} n}_{I} - \underbrace{\sum_{i=1}^{\left\lfloor \log_2 \frac{(n+1)}{2} \right\rfloor} 2^i}_{II} + \underbrace{\sum_{i=1}^{\left\lfloor \log_2 \frac{(n+1)}{2} \right\rfloor} 1}_{III}. \tag{6.3}$$

Em cada parcela anterior, a que possui maior ordem de crescimento é (I), ficando a complexidade do trabalho total $T(j)$ realizado pelo Algoritmo *Quick Sort*, para o melhor caso, representada assintoticamente por $O(n \cdot \log_2 n)$ ou $O(n \cdot \log n)$.

6.2.2.4 Comparação gráfica das complexidades dos algoritmos de ordenação

Observou-se, nas seções antecedentes, algumas leis algébricas de funções representando o total de comparações, bem como as complexidades dos Algoritmos de Ordenação analisados. Faremos uma comparação de tais desempenhos inicialmente numa tabela e posteriormente por gráfico. A visualização gráfica expressa bem o comportamento assintótico das funções que os representam. Vale salientar que a utilização de linguagens variadas, para expressar os resultados matemáticos obtidos ao se analisar os algoritmos, é bastante relevante para que se desenvolvam as competências requeridas na BNCC.

Tabela 6.4: Tabela de comparação do desempenho assintótico dos Algoritmos de Ordenação

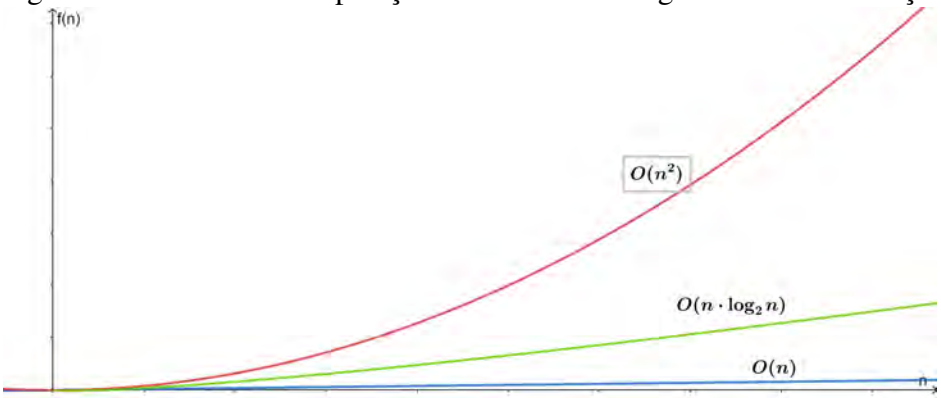
Nº de elementos	***Bubble Sort*:** $O(n)$	***Selection Sort*:** $O(n^2)$	***Quick Sort*:** $O(n \cdot \log_2 n)$
2	2	4	2
4	4	16	8
16	16	256	64
256	256	65.536	2048
1.024	1.024	1.048.576	10.240

Fonte: Elaborada pelo autor.

É notório na tabela anterior que, no melhor caso, o *Bubble Sort* é sempre mais eficiente que os outros dois Algoritmos de Ordenação, mas o *Quick Sort* se mostra mais eficiente que um algoritmo de complexidade Quadrática.

A complexidade $O(n \cdot \log n)$, chamada de linearítmica, possui uma taxa de crescimento maior que uma complexidade linear $O(n)$ e menor que qualquer complexidade polinomial, como é o caso de $O(n^2)$. Sabe-se que a análise assintótica *Big-O* compara as funções no limite superior, ou seja, quando a quantidade n de elementos do vetor é suficientemente grande.

Figura 6.2: Gráfico de comparação assintótica dos Algoritmos de Ordenação



Fonte: Elaborada pelo autor.

Um algoritmo é dito mais eficiente que outro quando sua complexidade possui assintoticamente uma taxa de crescimento menor, portanto, conclui-se que $O(n) < O(n \cdot \log n) < O(n^2)$.
O caso médio do *Quick Sort* se aproxima do melhor caso, tendo sua complexidade $O(n \cdot \log n)$ também e, apesar do seu desempenho no pior caso ser $O(n^2)$, na média, sua performance é excelente, o que o faz ser tão popular.

6.2.3 Sequência didática

O objetivo da sequência didática foi propor as atividades de modo a abordar os conteúdos matemáticos concernentes aos Algoritmos de Ordenação e desenvolver, gradualmente, os conceitos ligados ao tema, bem como as competências e habilidades em matemáticas da BNCC.

No capítulo 4 de Santos (2020), propomos uma sequência didática com oito aulas, mas fizemos um recorte apenas para ilustrar a forma como se propõe a abordagem do tema no Ensino Médio. Escolhemos a aula 5 a seguir:

5ª aula: Ordenando com os Algoritmos *Bubble Sort*, *Selection Sort*

e *Quick Sort*. *Procedimentos A turma será dividida em equipes que receberão a Ficha 3 (ver modelo sugerido) e cinco fichas ou cartas de baralho numeradas. As fichas deverão ser ordenadas de três formas diferentes, utilizando as estratégias do *Bubble Sort*, *Selection Sort* e *Quick Sort* respectivamente, registrando todo o procedimento. O professor pede para cada equipe socializar suas respostas e comparar com as estratégias que foram criadas pelos estudantes em outra aula. Os estudantes ainda não estarão instigados a desenvolver a modelagem e escrever algebricamente a função que representa a complexidade. Se limitarão a executar o procedimento de cada algoritmo.

Ficha 3

1) Cada equipe está recebendo cinco cartas com valores diferentes. Como por exemplo: 4 -2 0 8 5. Estas cartas deverão ser ordenadas utilizando os Algoritmos de Ordenação a seguir e registrar todo o processo em um material a parte.

Ordenando com o *Bubble Sort*: Se o objetivo é ordenar os valores em forma crescente, então, a posição atual é comparada com a próxima posição e, se a posição atual for maior que a posição posterior, é realizada a troca dos valores nessa posição. Caso contrário, não é realizada a troca, apenas passa-se para o próximo par de comparações.

Ordenando com o *Selection Sort*: A ordenação por seleção ou *Selection Sort* consiste em selecionar, por comparação, o menor item e colocar na primeira posição, selecionar o segundo menor item e colocar na segunda posição, segue estes passos até que reste um único elemento.

Ordenando com o *Quick Sort*: O vetor é dividido em duas partes a partir de um elemento denominado pivô, antes do pivô são colocados os elementos menores ou iguais ao mesmo e depois dele os elementos maiores. O processo se repete em cada uma das partes (subvetores) sucessivamente até que se obtenha partes com apenas um elemento. Para finalizar, os resultados são combinados e obtém-se o resultado esperado.

As competências e habilidades relacionadas a essa aula (atividade) são:

6.2.3.1 Competência específica 3 da BNCC

Utilizar estratégias, conceitos, definições e procedimentos matemáticos para interpretar, construir modelos e resolver problemas em diversos contextos, analisando a plausibilidade dos resultados e a adequação das soluções propostas, de modo a construir argumentos consistentes.

6.2.3.2 Habilidade 15

Investigar e registrar, por meio de um fluxograma, quando possível, um algoritmo que resolve um problema.

6.2.3.3 Competência específica 4 da BNCC

Compreender e utilizar com flexibilidade e precisão diferentes registros de representação matemáticos (algébrico, geométrico, estatístico, computacional, etc.) na busca de solução e comunicação de resultados de problemas.

6.2.3.4 Habilidade 05

Utilizar conceitos iniciais de uma linguagem de programação na implementação de algoritmos escritos em linguagem corrente e/ou matemática. Além desse tipo de atividade apresentado na 5ª aula da referida sequência, outras podem ser propostas com o tema envolvendo jogos e brincadeiras, modelagem matemática e representação gráfica. Como foi apresentado na Seção 6.2, o tema Algoritmos de Ordenação propicia o desenvolvimento de competências e habilidades relacionadas a diversos conteúdos matemáticos.

6.3 Considerações finais

O estudo em tela mostrou que é possível uma abordagem didática dos Algoritmos de Ordenação no Ensino Médio sem a presença de estruturas de programação computacional, e que essa abordagem favorece o desenvolvimento de competências e habilidades que constam na BNCC. São vários os conteúdos matemáticos relacionados com o tema como Números, Álgebra e Geometria. Apesar de termos suprimidos o conteúdo matemático mais denso nesse artigo, o tema engloba o estudo e aprofundamento de séries aritméticas e geométricas, função afim, função quadrática e função logarítmica.

A notação assintótica **O - grande** não se enquadra no Ensino Médio, mas pode ser apresentada complementarmente na abordagem do tema como um ganho na aprendizagem. O tema aqui proposto é recorrente nos cursos de graduação em computação, mas como consta na BNCC, que é um documento recente, sua inclusão no Ensino Médio se faz necessária e se mostra viável. Daí, é importante que o tema possa ser mais pesquisado e

aprofundado pelo meio acadêmico e que mais subsídios como sequências didáticas possam não apenas serem construídas, mas também possam ser aplicadas e seus impactos educacionais avaliados.

6.4 Referências bibliográficas

BRASIL. **Parâmetros Curriculares Nacionais de Matemática**. Brasília: MEC, 1998. 148 p.

BRASIL. **Parâmetros Curriculares Nacionais do Ensino Médio (PCNEM).** Brasília: MEC, 2000. 148 p.

BRASIL. **PCN+ Ensino médio: Orientações educacionais complementares aos Parâmetros Curriculares Nacionais-Ciências da Natureza, Matemática e suas Tecnologias.** Brasília: MEC, 2002. 142 p.

BRASIL, M. d. E. **Base Nacional Curricular Comum.** Brasil: MEC, 2018.

CORMEN, T. H. et al. **Algoritmos: Teoria e Prática, tradução da segunda edição, [americana].** São Paulo: Editora Campus, 2002.

OLIVEIRA, P. R. de. **Algoritmos e Programação de Computadores.** 2004. Disponível em: <https://slideplayer.com.br/slide/364011/>.

PERNAMBUCO, C. **Parâmetros para a Educação Básica do Estado de Pernambuco.** Recife-PE: Governo de Pernambuco, 2012.

RIBEIRO, M. R. da C. **Grafos, Algoritmos e Programação.** 152 p. Dissertação (Mestrado) — UFRPE, Recife-PE, 2018.

SANTOS, I. F. dos. **Algoritmos de Ordenação: uma abordagem didática para o ensino médio.** 78 p. Dissertação (Mestrado) — UFRPE, Recife-PE, 2020.

SILVA, A. P. C. da. **Classificação de dados por troca QuickSort.** 2013. Disponível em: <https://slideplayer.com.br/slide/364011/>.

Capítulo 7

Teoria dos números no ensino básico: uma proposta de texto didático

Me. Josemar Claudino Barbosa[1]
Dra. Barbara Costa da Silva[2]

Resumo: A Teoria dos Números é uma área da matemática de extrema importância, por suas aplicações e por trazer muitas técnicas para resolução de problemas. Este artigo aborda os temas mais clássicos da Teoria dos Números e que também pertence ao currículo do ensino fundamental, tais como divisibilidade, números primos, mdc e mmc. Além disso, também abordamos temas como equações diofantinas e congruência modular, apresentamos a resolução de alguns exemplos, frutos da aplicação dessa teoria, bem como a demonstração das proposições e teoremas expostos, sem abrir mão do rigor matemático.

Palavras-chave: Teoria dos Número; Congruências; Teorema de Euler.

[1]IFPE-Instituto Federal de Pernambuco, josemar.barbosa@pesqueira.ifpe.edu.br
[2]UFRPE-Universidade Federal Rural de Pernambuco, barbara.costasilva@ufrpe.br

7.1 Fundamentos teóricos e metodológicos

7.1.1 Divisibilidade

A Teoria dos Números é o ramo da matemática pura que estuda propriedades dos números inteiros, bem como a larga classe de problemas que surge no seu estudo. O termo aritmética (*arithmetiké*) vem do idioma grego e literalmente significa ciência dos números, sendo também usado para se referir à Teoria dos Números.

Um conceito muito importante no estudo da Teoria dos Números é chamado de divisibilidade. Mas, do que trata tal conceito? Vejamos a seguir.

Definição 1. *Sejam a e b inteiros com* $a \neq 0$*. Dizemos q*

43 errors36 warnings ue a é um divisor de b ou que b é um múltiplo de a, se existir um inteiro c tal que $b = a \cdot c$ *(indicamos* $a|b$*). Caso contrário, expressamos* $a \nmid b$*.*

Exemplo 1. $8|24$*, pois* $24 = 3.8$*.*

É fácil ver que $1|a$ para todo a inteiro, $a|a$ e $a|0$ para todo $a \neq 0$, $a \in \mathbb{Z}$. De fato, temos que $a = 1 \cdot a$, para todo $a \in \mathbb{Z}$ e que $0 = a \cdot 0$, para todo inteiro a, $a \neq 0$.

As propriedades a seguir serão de fundamental importância, pois se revelarão bastante úteis na resolução de vários exercícios. A princípio, tente verificar por meio de alguns números a veracidade de cada afirmação abaixo.

1. Sejam a, b e c inteiros, $a \neq 0$, $b \neq 0$. Se $a|b$ e $b|c$, então $a|c$.

2. Sejam a, b, c, e d inteiros, $a \neq 0$, $c \neq 0$. Se $a|b$ e $c|d$, então $ac|bd$.

3. Sejam a, b, m e n inteiros, com $a \neq 0$ e $n \neq 0$. Se $an|am$, então $n|m$.

4. Sejam a, b e c inteiros, com $a \neq 0$. Se $a|(b+c)$, então $a|b$ se, e somente se, $a|c$.

5. Sejam a, b e c inteiros, com $a \neq 0$. Se $a|(b-c)$, então $a|b$ se, e somente se, $a|c$.

6. Sejam a, b e c inteiros, com $a \neq 0$. Se $a|b$ e $a|c$, então $a|(bx \pm cy)$ para quaisquer x, y inteiros.

7. Dados a, b com $a \neq 0$. Temos que se $a|b$, então $b \geq a$.

Vejamos agora as demonstrações de cada propriedade.

Demonstrações:

1. Ora, se $a|b$, então podemos escrever $b = am$, para algum $m \in \mathbb{Z}$. Por outro lado, como $b|c$, então podemos escrever $c = bn$, para algum $n \in \mathbb{Z}$. Portanto, teremos que $c = bn = a(mn)$, o que mostra que $a|c$.

2. Ora, se $a|b$ então podemos escrever $b = am$ para algum $m \in \mathbb{Z}$. Por outro lado, se $c|d$ então $d = cn$, para algum $n \in \mathbb{Z}$. Daí, temos que $b \cdot d = (ac)(mn)$, o que mostra que $ac|bd$.

3. De fato, como $an|am$, temos que existe k inteiro tal que $am = (an)k$. Ora, como $a \neq 0$, podemos dividir ambos os membros por a, o que vai resultar $m = nk$, o que mostra que $n|m$.

4. Como $a|(b+c)$, existe $k \in \mathbb{Z}$ tal que $b+c = ak$. Mais ainda, como $a|b$, temos que existe $r \in \mathbb{Z}$ tal que $b = ar$. A partir das duas igualdades, concluímos que

$$ar + c = ak,$$

Logo, temos que

$$c = ak - ar = a(k-r),$$

o que implica que $a|c$. Ficará como exercício para o leitor a demonstração da outra implicação.

5. A demonstração dessa propriedade também fica a cargo do leitor, pois tem uma demonstração análoga à propriedade anterior.

6. De fato, como $a|b$ e $a|c$, então existem inteiros m e n tais que $b = am$ e $c = an$. Daí, temos que
$bx \pm cy = (am)x \pm (an)y = a(mx) \pm a(ny) = a(mx \pm ny)$, para todo $x, y \in \mathbb{Z}$,

   portanto, concluí-se que $a|(bx \pm cy)$.

7. Essa última demonstração utiliza ideias análogas às anteriores, ficando, portanto, como exercício para o leitor.

Exemplo 2. *Prove que o número* $N = 5^{45362} - 7$ *não é divisível por* 5.

Solução 1. *Suponhamos que esse número fosse divisível por* 5. *Pela propriedade* 5 *acima, temos que se* $5|5^{45362} - 7$, *então* $5|7$, *o que não é verdade, mostrando assim que* $5 \not| 5^{45362} - 7$.

Exemplo 3. *Se a e b são dois números naturais e* $2a + b$ *é divisível por* 13, *mostre que* $93a + b$ *também é múltiplo de* 13.

Solução 2. *De fato, temos que* $93a + b = 91a + (2a + b)$. *Ora, como* $13|91a$, *pois* $91a = 13 \cdot (7a)$ *e, por hipótese,* $13|2a + b$, *concluímos que* $13|93a + b$.

Definição 2. *Chamamos de conjunto dos divisores naturais de um natural n dado, e indicamos por* $D(n)$, *os naturais de quem n é múltiplo.*

Exemplo 4. *Sendo* $n = 20$, *temos* $D(20) = \{1, 2, 4, 5, 10, 20\}$.

Se $D(n)$ tem exatamente dois elementos, isto é, $D(n) = \{1, n\}$, dizemos que n é um número primo. O número 7 possui apenas dois divisores, 1 e 7, portanto é um número primo.

7.1.2 Divisão Euclidiana

O algoritmo da divisão, apesar de sua simplicidade, é uma das ferramentas mais poderosas no estudo da Teoria dos Números. Apresentado pelo matemático Euclides, é bastante útil na resolução de muitos problemas. Vimos no tópico anterior que um número inteiro b é divisível por outro $a \neq 0$, se existir um inteiro c, tal que $b = a \cdot c$. Mas, quando b não é divisível por a, isto é,a ,/é o algoritmo da divisão que possibilitará as devidas representações desse processo. Vamos, então, ao enunciado desse importante resultado.

Teorema 1 (Algoritmo da divisão)**.** *Dados dois inteiros b e a, com* $a \neq 0$*, existem dois únicos inteiros q e r, tais que:*

$$b = a \cdot q + r, \ \ com \ \ 0 \leq r < |a|,$$

Nesse caso, o número b é chamado de dividendo, a é chamado de divisor, q é chamado de quociente e r é chamado de resto da divisão.

Exemplo 5. *Note que* $13 = 5 \cdot 2 + 3$ *e isso significa dizer que, ao dividirmos* 13 *por* 5*, o quociente é* 2 *e o resto dessa divisão é* 3*.*

Exemplo 6. *Vejamos também que* $4 = 5 \cdot 0 + 4$*, ou seja, na divisão de* 4 *por* 5*, o quociente é* 0 *e o resto é* 4*.*

Exemplo 7. *Ao dividirmos* -19 *por* 5*, obteremos* $q = -4$ *e* $r = 1$*.*

Demonstração. Considere o número inteiro a, com $a \neq 0$. Podemos escrever o conjunto dos números inteiros da seguinte forma:

$$\mathbb{Z} = ... \cup \big[-2a, -a\big) \cup \big[-a, 0\big) \cup \big[0, a\big) \cup \big[a, 2a\big) \cup \big[2a, 3a\big) \cup ... \cup \big[qa, (q+1)a\big) \cup ...$$

Os subconjuntos descritos acima são disjuntos, ou seja, sendo b um inteiro qualquer, temos que b pertence a apenas um desses subconjuntos, sendo portanto único. Mais ainda, podemos escrever:

$$qa \leq b < (q+1)a = qa + a \Rightarrow 0 \leq \underbrace{b - qa}_{r} < a$$

Desta forma, r é únicamente determinado e

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

□

Uma das importantes consequências do algoritmo da divisão é saber que, ao dividirmos um inteiro b por um inteiro a, $a \neq 0$, o resto r dessa divisão pertence ao conjunto $\{0, 1, 2, 3, ..., a-1\}$. Estudando o caso em que $a = 2$, temos que o resto r da divisão de b por a será 0 ou 1. Se $r = 0$, temos que $b = 2 \cdot q$, com q inteiro e, nesse caso, dizemos que b é um número par. Se $r = 1$, escrevemos $b = 2 \cdot q + 1$, com q inteiro e, nesse caso, dizemos que b é um número ímpar. Tal análise permite-nos generalizar e dizer que todo inteiro b pode ser expresso na forma $2 \cdot q$ ou $2 \cdot q + 1$, com $q \in \mathbb{Z}$. Analogamente, no caso em que $a = 3$, temos que b será da forma $3 \cdot q$, $3 \cdot q + 1$ ou $3 \cdot q + 2$, com q inteiro.

A seguir, estudaremos um importante resultado conhecido como lema dos restos.

Lema 1 (Lema dos restos)**.** *A soma e o produto de quaisquer dois números inteiros deixa o mesmo resto que a soma e o produto dos seus restos, respectivamente, na divisão por um inteiro a, $a \neq 0$.*

Demonstração. Sejam n_1 e $n_2 \in \mathbb{Z}$. Ao fazermos a divisão com resto desses dois números por a, teremos:

$$n_1 = aq_1 + r_1 \text{ e } n_2 = aq_2 + r_2$$

em que $0 \leq r_1, r_2 < a$. Daí, teremos:

$$\begin{aligned} n_1 n_2 &= (aq_1 + r_1)(aq_2 + r_2) \\ &= a^2 q_1 q_2 + aq_1 r_2 + aq_2 r_1 + r_1 r_2 \\ &= a(aq_1 q_2 + q_1 r_2 + q_2 r_1) + r_1 r_2 \\ &= aq + r_1 r_2 \end{aligned} \tag{7.1}$$

onde consideraremos $q \in \mathbb{Z}$ e $q = aq_1q_2 + q_1r_2 + q_2r_1$. Mais ainda, ao dividirmos r_1r_2 por a, teremos:

$$r_1 r_2 = ap + r, \quad p \in \mathbb{Z}, \quad 0 \leq r < a \tag{7.2}$$

Daí, de (7.1) e (7.2), concluí-se que

$$n_1 n_2 = aq + ap + r = a(p+q) + r,\ 0 \leq r < a$$

□

A demonstração para a soma é muito simples e tem procedimento análogo ao anterior, ficando, portanto, como exercício.

Exemplo 8. *Qual é o resto da divisão de* 3^{250} *por* 4*?*

Solução 3. *Note que, ao dividirmos* $3^2 = 9$ *por* 4*, o resto será* 1*. Como* $3^{250} = (3^2)^{125}$*, temos, pelo lema dos restos, que o resto da divisão de* 3^{250} *por* 4 *será igual ao produto* $\underbrace{1 \cdot 1 \cdot 1 \cdot 1 \cdots 1}_{125\, fatores} = 1$.

Exemplo 9. *Qual é o resto da divisão de* $3^{100} + 5^{45}$ *por* 2*?*

Solução 4. *Inicialmente, note que o resto da divisão de* 3 *por* 2*, é* 1*. Portanto, pelo lema do resto, temos que o resto da divisão de* 3^{100} *por* 2 *será igual a* $1^{100} = 1$*. Por outro lado, o resto da divisão de* 5 *por* 2 *também é igual a* 1*; sendo assim, o resto da divisão de* 5^{45} *por* 2 *será igual a* $1^{45} = 1$ *e, consequentemente, o resto da divisão de* 3^{100} + 5^{45} *por* 2 *será* $1 + 1 = 2$*. É claro que, cfomo o divisor é* 2*, o resto será, portanto, igual a* 0*!*

7.1.3 Números primos

Agora, vamos estudar um tema que há bastante tempo tem sido objeto de estudo de vários matemáticos: os números primos.

Definição 3. ***Número primo***. *Um número inteiro $p > 1$ é dito primo se possui apenas dois divisores positivos:* 1 *e p. São exemplos de números primos, os números* 5*,* 17*,* 19*,* 71*, etc. Quando um número inteiro positivo não é primo, ele é chamado de número composto.*

A aplicabilidade dos números primos no nosso cotidiano é vasta. Por exemplo, podemos citar o método de criptografia (conjunto de regras que visa codificar informações) RSA, um sistema criado pelos matemáticos Ron Rivest, Adi Shamir e Leonard Adleman na década de 70, que permite a segurança do uso de cartões de crédito, criando números primos de até 100 dígitos. Hoje em dia, já são usados números primos com 600 dígitos, objetivando uma maior segurança.

Teorema 2 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que 1 ou é primo ou pode ser escrito de forma única, como produto de números primos.*

Demonstração. Seja n um número inteiro tal que $n > 1$. Mais ainda, seja p_1 o menor entre os divisores de n diferentes de 1. Temos assim que p_1 é primo ou composto. Suponhamos que p_1 seja composto. Daí, existirá um inteiro d, $1 < d < p_1$, de forma que $d|p_1$. Ora, como $d|p_1$ e $p_1|n$, concluímos, pela propriedade 1 estudada na discussão sobre divisibilidade, que $d|n$. No entanto, essa conclusão vai contradizer a escolha de p_1. Logo, p_1 é primo. Mas, como $p_1|n$, existe $m_1 \in \mathbb{N}$, tal que $n = p_1 \cdot m_1$. Daí:

- Se $m_1 = 1$, temos $n = p_1$, portanto, n é primo.
- Se $m_1 > 1$, então podemos fazer o mesmo procedimento que fizemos para o valor de n, ou seja, teremos $m_1 = p_2 \cdot m_2$, com p_2 primo e, consequentemente, podemos escrever $n = p_1 \cdot p_2 \cdot m_2$, com $1 \leq m_2 < m_1$ e p_1, p_2 primos.
- Se tivermos $m_2 = 1$, teremos $n = p_1 \cdot p_2$ e, assim, terminaríamos a prova.
- Se $m_2 > 1$, de maneira análoga, podemos decompor m_2 assim como fizemos com m_1.

Dando continuidade a esse procedimento, obtemos números primos $p_1, p_2, p_3, ..., p_i$ e uma sequência de números naturais $m_1 > m_2 > m_3 > ... > m_i \geq 1$, de forma que, sempre que $m_i > 1$, podemos continuar a decomposição de n. Ora, como entre 1 e n existe uma quantidade finita de números naturais, haverá, na decomposição de n, um último passo, no qual teremos $m_j = 1$ e, portanto:

$$n = p_1 \cdot p_2 \cdot p_3 \cdots p_j, \text{ com } p_1, p_2, p_3, ..., p_j \text{ primos.}$$

□

Exemplo 10. *Notemos que* $18 = 3 \cdot 3 \cdot 2 = 3^2 \cdot 2$, $40 = 2 \cdot 2 \cdot 2 \cdot 5 = 2^3 \cdot 5$ *e* $800 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \cdot 7 = 2^4 \cdot 3 \cdot 5^2 \cdot 7$

Uma importante consequência do Teorema Fundamental da Aritmética está no fato de descobrirmos a quantidade de divisores positivos de um número natural n. Representando por $d(n)$ o número de divisores positivos de n, e sendo $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, onde $p_1, p_2, \cdots, p_k$ são primos e $\alpha_1, \alpha_2, ..., \alpha_k \in \mathbb{N}$, então:

$$D(n) = (\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdots (\alpha_k + 1)$$

De fato, todos os divisores de n serão da forma $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$, com $r_1 \in \{0, 1, ..., \alpha_1\}$, que é um conjunto que possui, obviamente, $\alpha_1 + 1$ elementos. Por outro lado, temos que $r_2 \in \{0, 1, ..., \alpha_2\}$, que por sua vez, possui $\alpha_2 + 1$ elementos e assim por diante. Portanto, é fácil ver, pelo Princípio Multiplicativo, que o número de divisores positivos, $d(n)$, do natural n será dado pela expressão vista anteriormente.

Exemplo 11. *Encontrar o número de divisores positivos do número* 80.

Solução 5. *Temos que* $80 = 2^4 \cdot 5$. *Daí, é fácil ver que* $D(80) = (4+1) \cdot (1+1) = 5 \cdot 2 = 10$.

Teorema 3. *O conjunto dos números primos é infinito.*

Demonstração. Suponhamos que exista um primo p_n tal que p_n seja o maior número primo. Seja $n \in \mathbb{N}$ tal que $n = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$, onde $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$. Logo, como $n > 1$, pelo Teorema Fundamental da Aritmética, existe pelo menos algum primo p, tal que $p|n$. No entanto, como $p_1, p_2, p_3, p_4, ..., p_n$ são, por hipótese, os únicos primos, concluímos que $p|p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdots p_n$. Daí, pela propriedade 4 estudada na discussão sobre divisibilidade, temos que $p|1$, o que é absurdo, pois o único inteiro positivo divisor de 1 é ele mesmo. Portanto, qualquer que seja o primo p_n, existirá sempre um outro primo p_m tal que $p_m > p_n$, a partir do que concluímos que a quantidade de primos é infinita. □

Dando prosseguimento, veremos uma proposição que servirá para estudarmos um importante procedimento, conhecido como Crivo de Eratóstenes, procedimento esse utilizado para descobrir se um número positivo inteiro é primo.

Proposição 1. *Seja n um número natural maior que 1. Se n é um número composto, temos então que o menor divisor, diferente de* 1*, de n é* $\leq \sqrt{n}$*, isto é, se os divisores de n, diferentes de* 1*, forem maiores que* $\sqrt{n}$*, então n é primo.*

Demonstração. Com efeito, seja p o menor divisor de n, diferente de 1. Temos então que $n = pq$, com $q \geq p$. Se multiplicarmos cada membro da desigualdade por p, o resultado será:

$$n = pq \geq p^2,$$

daí, segue que $\sqrt{n} \geq p$. □

O crivo de Eratóstenes - Trata-se de um algoritmo criado pelo matemático grego Eratóstenes (285 - 194 a.C) cujo objetivo é encontrar, até determinado número n inteiro positivo dado, quais são os números primos menores ou iguais a ele. De acordo com esse algoritmo, inicialmente lista-se numa tabela todos os inteiros positivos ordenadamente, a partir de 2, até o n, isto é,

$$2, 3, 4, , 5, 6, 7, 8, 9, ..., n$$

Após isso, marca-se com um X o primeiro número primo da tabela, no caso o 2 e em seguida circula-se todos os múltiplos de 2 da tabela por serem todos eles compostos. O primeiro número que não foi circulado, após o 2, foi o 3, que é próximo número primo da tabela. Daí, o procedimento prossegue , ou seja, marca-se com um X o número 3 e circula-se todos os múltiplos de 3 da tabela. O processo será repetido até que o primeiro número não circulado na tabela seja maior que $\sqrt{n}$, devido à **Proposição 1**. A partir daí, todos os números restantes são os primos menores ou iguais a n.

Um dos problemas mais famosos relacionados aos números primos e que ainda não foi provado, sendo portanto ainda uma conjectura, é chamado de Conjectura de Goldbach. Em 1742, o matemático Christian Goldbach enviou uma carta para outro matemático, cujo nome era Leonhard Euler. Nessa carta, Goldbach afirmava que todo número natural par, maior ou igual a 4, podia ser expresso como a soma de dois números primos. Vejamos alguns exemplos:

$$4 = 2+2,\ 22 = 19+3,\ 70 = 59+11.$$

Outro importante matemático, Pierre de Fermat $(1601-1665)$, fascinado pela beleza dos números primos, tentou criar uma fórmula através da qual pudéssemos encontrar qualquer número primo. Tal busca levou Fermat a conjecturar que são primos todos os números F_n, da forma:

$$F_n = 2^{2^n}+1,$$

sendo n um inteiro não-negativo.

Fermat conseguiu verificar a veracidade de tal conjectura para os seguintes casos:

$n = 0 \Rightarrow F_o = 2^{2^0}+1 = 3$
$n = 1 \Rightarrow F_1 = 2^{2^1}+1 = 5$
$n = 2 \Rightarrow F_2 = 2^{2^2}+1 = 17$
$n = 3 \Rightarrow F_3 = 2^{2^3}+1 = 257$
$n = 4 \Rightarrow F_4 = 2^{2^4}+1 = 65537$

O números acima são chamados de Primos de Fermat. O problema é que a partir de $n \geq 5$, Fermat conjecturou que todos os próximos números seriam primos. Porém, outro grande matemático citado anteriormente, Leonhard Euler $(1707-1783)$, mostrou que, para o caso $n = 5$, o número obtido é composto. De fato,

$$F_5 = 2^{2^5} + 1 = 4294967297 = 641.6700417,$$

que é, consequentemente, um número composto.

7.1.4 Máximo divisor comum - MDC

Considere todos os divisores positivos dos números 36 e 42:

$$D(36) = \{1,2,3,4,6,9,12,18,36\} \text{ e } D(42) = \{1,2,3,6,7,14,21,42\}$$

Note que o maior número que é divisor de 36 e 42, ao mesmo tempo, é 6. Dizemos que 6 é o máximo divisor comum de 36 e 42 e escrevemos $(32,42) = 6$.

Definição 4. *Sejam $a,b \in \mathbb{Z}$ com pelo menos um deles diferente de zero. O máximo divisor comum de a e b (MDC) é um inteiro positivo d tal que d é o maior dentre os divisores positivos comuns de a e b. Escrevemos $(a,b) = d$. Se $(a,b) = 1$, dizemos que a e b são primos entre si.*

É fácil ver que, sendo $a \in \mathbb{Z}$, temos que $(a,0) = |a|$,$(a,1) = 1$ e que $(a,a) = |a|$. As proposições a seguir são de grande importância na teoria dos números, em especial para o cálculo do MDC de números inteiros.

Proposição 2. *Sejam a e b dois inteiros, com pelo menos um deles diferente de zero. As seguintes afirmações são válidas:*

(i) Se a é múltiplo de b, então $(a,b) = |b|, b \neq 0$.

(ii) Se $a = bq + c$, com $c \neq 0$, então o conjunto dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e c e temos, em particular, que $(a,b) = (b,c)$.

Demonstração. Inicialmente, demonstraremos (i). De fato, se um inteiro pertence ao conjunto dos divisores comuns dos números a e b, então, em particular, ele também é divisor de b. Mas, como b|a, segue que todo divisor de b também é divisor de a. Daí, o conjunto dos divisores comuns de a e b é, portanto, igual ao conjunto dos divisores de b. No entanto, como o maior inteiro que divide b é ele mesmo, concluímos que (a,b) = b.

Para provarmos (ii), utilizaremos a propriedade 4 estudada no tópico de Divisibilidade. Baseados nela, temos que todo divisor comum de a e b também é divisor de c e, portanto, divisor de b e c. Por outro lado, todo divisor comum de b e c também é divisor de a e, assim, também é um divisor de a. Logo, os divisores comuns dos inteiros a e b também são os mesmos que os divisores comuns dos inteiros b e c o que resulta que $(a,b) = (b,c)$.

□

Exemplo 12. *Sejam* $a = 15$ *e* $b = 5$. *De* (i), *temos que* $(15,5) = 5$

Exemplo 13. *Sendo* $a = 28$ *e* $b = 8$, *temos* $28 = 3 \cdot 8 + 4$. *Logo, por* (ii), *concluímos que* $(28,8) = (8,4) = 4$.

Teorema 4 (Algoritmo de Euclides)**.** *Dados dois inteiros positivos a e b, considere as divisões sucessivas, para obtermos:*

$$\begin{array}{rcrcrcl}
a &=& bq &+& r, & & 0<r<b \\
b &=& rq_1 &+& r_1, & & 0<r_1<r \\
r &=& r_1q_2 &+& r_2, & & 0<r_2<r_1 \\
r_1 &=& r_2q_3 &+& r_3, & & 0<r_3<r_2 \\
\vdots & \vdots & \vdots & \vdots & \vdots & & \vdots \\
r_k &=& r_{k+1}q_{k+2} &+& r_{k+2}, & & 0<r_{k+2}<r_{k+1} \\
r_{k+1} &=& r_{k+2}q_{k+3} & & & &
\end{array}$$

até algum r_{k+2} *dividir* r_{k+1}. *Assim, temos que* $(a,b) = r_{k+2}$, *que é o último resto não-nulo das divisões sucessivas anteriores.*

Demonstração. É fácil ver que processo de divisões sucessivas descritos acima é finito. De fato, pelo algoritmo da divisão, temos que $b > r_0 > r_1 >$

$r_2 > ...$, e, se essa sequência de restos não fosse finita, em algum momento teríamos um resto negativo, o que é absurdo. Mais ainda, analisando as igualdades de cima para baixo, como também utilizando a **Proposição 2**, concluímos que:

$$(a,b) = (b,r_0) = (r_0,r_1) = \cdots = (r_{k+1},r_{k+2}) = r_{k+2}$$

□

Exemplo 14. *Calcular* $(1320,35)$.

Solução 6. *Baseados no algoritmo de Euclides, tal cálculo será realizado da seguinte forma:*

1320	35	35	25	25	10	10	5
25	37	10	1	5	2	0	2

Ou seja,

$$\begin{aligned} 1320 &= 35 \cdot 37 + 25 \\ 35 &= 25 \cdot 1 + 10 \\ 25 &= 10 \cdot 2 + 5 \\ 10 &= 5 \cdot 2 \end{aligned}$$

A partir dos resultados acima, temos que $(1320,35) = (35,25) = (25,10) = (10,5) = (5,0) = 5$. *Daí,* $(1320,35) = 5$. *Esse método é chamado de divisões sucessivas. Uma forma de representarmos as divisões sucessivas é usando uma grade conforme ilustrada abaixo para o cálculo de* $(1320,35)$. *Utilizando esse mecanismo,* $(1320,35)$ *será o último resto, no caso, igual a* 5.

Exemplo 15. *Vejamos outro exemplo. Calculemos* $(60,42)$. *Utilizando o método descrito acima, temos:*

	37	1	2	2
1320	35	25	10	5
25	10	5	0	

	1	2	3
60	42	18	6
18	6	0	

Portanto, $(60,42) = 6$. *Note que, a partir desses dados, podemos escrever:*

$$18 = 60 - 42 \cdot 1 \tag{7.1}$$
$$6 = 42 - 18 \cdot 2 \tag{7.2}$$

Substituindo (7.1) *em* $(7,2)$*, teremos:*

$$\begin{aligned} 6 &= 42 - (60 - 42 \cdot 1) \cdot 2 \\ 6 &= 42 - 60 \cdot 2 + 42 \cdot 2 \\ 6 &= 42 \cdot 3 - 60 \cdot 2 \\ 6 &= 60 \cdot (-2) + 42 \cdot 3. \end{aligned}$$

Nesse último exemplo, o fato $(60,42) = 60 \cdot (-2) + 42 \cdot 3$ será generalizado a seguir.

Teorema 5 (Teorema de Bachet-Bézout)**.** *Seja* $d = (a,b)$*. Então, existem inteiros* x *e* y *de forma que:*

$$d = ax + by.$$

Demonstração. Com efeito, considere o conjunto $C = \{ax + by, \text{com } x,y \in \mathbb{Z}\}$ e $n = ax_0 + by_0$ o menor elemento de C. Suponhamos, por absurdo, que $n \nmid a$. Pelo algoritmo da divisão, temos que $a = nq + r$, com $0 < r < n$. Daí, $r = a - nq$.

Substituindo o valor de n nessa última equação, teremos $r = a - (ax_0 + by_0)q = a - ax_0q - by_0q = a(1 - x_0q) + b(-y_0q)$, ou seja, $r \in C$. Mas, como $r < n$, esse fato contraria a hipótese de n ser o menor elemento de C. Portanto, $n|a$. De forma análoga, podemos provar que $n|b$. Sendo assim, n é divisor comum de a e b. Agora, resta-nos mostrar que $n = d$. De fato, como $d|a$ e $d|b$, podemos escrever $a = dq_1$ e $b = dq_2$. Como $n = ax_0 + by_0$, temos então, $n = (dq_1)x_0 + (dq_2)y_0$, mais ainda, $n = d(q_1x_0 + q_2y_0)$, e daí concluímos que $d|n$. Como $d = (a,b)$, segue que $d = n$. □

Uma consequência importante desse Teorema é a proposição abaixo.

Proposição 3. *Dados a,b inteiros com pelo menos um deles diferente de zero, se existirem inteiros r,s tais que $1 = ra + sb$, então $(a,b) = 1$.*

Demonstração. De fato, sendo $d = (a,b)$, temos que $d|ra$ e $d|sb$, portanto $d|(ra + sb)$. Daí, temos que $d|1$. Logo, $d = 1$. □

Uma outra proposição importante é a que veremos a seguir.

Proposição 4. *Dados a, b e c inteiros não nulos, então $(a,b,c) = \big((a,b),c\big)$.*

Demonstração. Com efeito, sejam $(a,b) = d$, $(a,b,c) = d_1$, $\big((a,b),c\big) = d_2$. Daí, temos que $d_2|c$ e $d_2|d$. Mas, como $d|a$ e $d|b$, concluímos que d_2 divide a,b e c. Portanto, $d_2 \leq d_1$. No entanto, como d_1 divide a,b e c, temos que, em particular, $d_1|a$ e $d_1|b$, logo $d_1|d$. Daí, segue que d_1 divide d e c, donde seque que $d_1|d_2$ e, portanto, $d_1 \leq d_2$. Enfim, $d_1 = d_2$, como queríamos mostrar. □

Exemplo 16. *Calcular* $(24,18,12)$.

Solução 7. *Deixaremos a solução a cargo do leitor.*

Proposição 5. *Sejam $b_1,b_2,b_3,...,b_n$ inteiros com pelo menos um diferente de zero, temos que $(b_1,b_2,b_3,...,b_n)$ será o produto de todas as potências p^s, tal que p pertence ao conjunto de todos os primos que dividem simultaneamente $b_1,b_2,b_3,...,b_n$, e s é o menor expoente de p de forma que p^s divide, ao mesmo tempo, $b_1,b_2,b_3,...,b_n$.*

Exemplo 17. *Calcular* $(24, 18, 12)$.

Solução 8. *Notemos que* $24 = 2^3 \cdot 3$, $18 = 2 \cdot 3^2$ *e* $6 = 2 \cdot 3$. *Note que os primos* 2 *e* 3 *dividem simultaneamente* 24, 18 *e* 6. *Mais ainda, o menor expoente de tanto do* 2 *quanto do* 3, *é* 1. *Portanto,* $(24, 18, 6) = 2^1 \cdot 3^1 = 6$.

Proposição 6. *Sejam a e b inteiros não nulos. Se* $a|bc$ *e* $(a,b) = 1$, *então* $a|c$.

Demonstração. De fato, pela Proposição 5, podemos escrever $ra + sb = 1$, com r, s inteiros. Multiplicando cada membro dessa igualdade por c, teremos:

$$a(rc) + s(bc) = c$$

Como $a|a(rc)$ e $a|s(bc)$, segue, pela propriedade 4 da divisibilidade, que $a|c$.

□

7.1.5 Menor múltiplo comum - MMC

Suponhamos que, no alto de uma torre de uma emissora de televisão, duas luzes piscam com frequências diferentes. A primeira pisca 15 vezes por minuto e a segunda pisca 10 vezes por minuto. Se num certo instante as luzes piscam simultaneamente, após quantos segundos elas voltarão a piscar simultaneamente? Para resolvermos esse problema de uma maneira muito prática, estudaremos o conceito de MMC (menor múltiplo comum).

Definição 5. *Sejam a e b inteiros não nulos. Chamamos de menor múltiplo comum de a e b, e indicamos por* $[a,b]$, *o inteiro positivo m tal que m é o menor número que é divisível por a e b ao mesmo tempo.*

Exemplo 18. $M(24) = \{24, 48, 72, 96, 120, 144, ...\}$ *e*
$M(30) = \{30, 60, 90, 120, 150, ...\}$.

Notemos que 120 é o menor número da lista que é divisível ao mesmo tempo por 24 e 30, ou seja, é o menor número inteiro positivo que é múltiplo ao mesmo tempo de 24 e 30. Portanto, $[24,30] = 120$.

Um método bastante prático para o cálculo do mmc de dois inteiros dados será visto a seguir, utilizando a decomposição em fatores primos, assim como foi feito para o MDC. Para utilizar esse método, considere $b_1, b_2, b_3, ..., b_n$ inteiros não nulos. Decompondo em fatores primos cada número desse, temos que $[b_2, b_3, ..., b_n]$ será o produto de todos os fatores primos, comuns e não-comuns a eles, cada um elevado ao maior expoente que aparece "acompanhando" cada um dos fatores primos. É claro que se algum b_i, $i \in \{1,2,3,...,n\}$ é negativo, basta decompor $|b_i|$.

Exemplo 19. *Calcular* $[18,24,30]$. *Temos que* $18 = 2 \cdot 3^2$, $24 = 2^3 \cdot 3$ *e* $30 = 2 \cdot 3 \cdot 5$. *Daí,* $[18,24,30] = 2^3 \cdot 3^2 \cdot 5 = 360$.

Esse resultado também poderia ser obtido através do método que consiste em colocar os três números um ao lado do outro, separados por vírgulas e com uma barra vertical a sua direita, assim realizando as divisões sucessivas. Abaixo de cada número, colocamos o quociente da divisão de cada um deles pelo menor primo que divide pelo menos um deles. Se algum deles não for divisível por esse primo, ele é repetido na linha seguinte. O procedimento termina quando todos os quocientes forem iguais a 1. O MMC será o resultado do produto dos fatores primos.

18,	24,	30	2
9,	12,	15	2
9,	6,	15	2
9	3,	15	3
3,	1,	5	3
1,	1,	5	5
1,	1,	1	

Agora, vejamos uma situação bastante interessante. Já vimos anteriormente que $[24,30] = 120$. É trivial encontrarmos que $(24,30) = 6$. Efetuando $[24,30] \cdot (24,30)$, teremos:

$$[24,30] \cdot (24,30) = 120 \cdot 6 = 24 \cdot 30$$

Será que isso sempre será verdade? Veremos mais adiante um teorema importante que generaliza esse fato. Mas, antes, estudaremos dois lemas que fundamentarão a prova desse teorema.

Lema 2. *Sejam a e b inteiros não nulos e $(a,b) = d$. Sendo $a = dm_1$ e $b = dm_2$, então $(m_1, m_2) = 1$.*

Demonstração. Suponhamos que $(m_1, m_2) = k$, tal que $k > 1$. Sendo assim, teremos:

- $m_1 = k \cdot n_1 \Rightarrow a = d \cdot kn_1 \Rightarrow d \cdot k | a$
- $m_2 = k \cdot n_2 \Rightarrow b = d \cdot kn_2 \Rightarrow d \cdot k | b$

Daí, concluímos que $d \cdot k$ é um divisor comum de a e b. Logo, como por hipótese $k > 1$, teremos $d \cdot k > d$, o que é absurdo, pois d é o maior divisor comum de a e b. Portanto, $(m_1, m_2) = 1$.

□

Lema 3. *Sejam a e b inteiros não nulos e $[a,b] = m$. Sendo $m = ak_1$ e $m = bk_2$, então $(k_1, k_2) = 1$.*

Demonstração. Suponhamos que $(k_1, k_2) = l$, tal que $l > 1$. Sendo assim, teremos:

- $k_1 = l \cdot r_1 \Rightarrow m = a \cdot l \cdot r_1$
- $k_2 = l \cdot r_2 \Rightarrow m = b \cdot l \cdot r_2$

Das duas igualdades acima, concluímos que

$$a \cdot l \cdot r_1 = b \cdot l \cdot r_2 \Rightarrow a \cdot r_1 = b \cdot r_2$$

Se $m_1 = a \cdot r_1 = b \cdot r_2$, temos $m_1 < m$. Como m_1 é um múltiplo comum de a e b e menor que m, chegamos a um absurdo, pois $[a,b] = m$. Portanto, $(k_1, k_2) = 1$. □

Agora, vejamos o seguinte teorema:

Teorema 6. *Sejam a e b inteiros não nulos. Então* $(a,b)\cdot[a,b] = a\cdot b$.

Demonstração. Seja $(a,b) = d$. Então:

- $a = d\cdot h_1$
- $b = d\cdot h_2$

Daí, pelo **Lema 2**, temos que $(h_1,h_2) = 1$. Sejam também $[a,b] = m$. Temos que:

- $m = a\cdot\alpha_1$ e
- $m = b\cdot\alpha_2$

Sendo assim, pelo **Lema 3**, temos $(\alpha_1,\alpha_2) = 1$. Podemos escrever, então:

- $m = a\cdot\alpha_1 = d\cdot h_1\cdot\alpha_1$
- $m = b\cdot\alpha_2 = d\cdot h_2\cdot\alpha_2$

Daí, temos que $d\cdot h_1\cdot\alpha_1 = d\cdot h_2\cdot\alpha_2 \Rightarrow h_1\cdot\alpha_1 = h_2\cdot\alpha_2$. Portanto, $h_1|h_2\cdot\alpha_2$. Mas, como $(h_1,h_2) = 1$, só nos resta concluir que $h_1|\alpha_2$. Analogamente, temos $h_2|h_1\cdot\alpha_1$. No entanto, como já foi visto antes, $(h_1,h_2) = 1$. Concluímos que $h_2|\alpha_1$. Utilizando a mesma argumentação, chegaremos a conclusão que $\alpha_2|h_1$ e que $\alpha_1|h_2$ e, consequentemente:

- $h_1 = \alpha_2$; e que
- $h_2 = \alpha_1$

Por fim, teremos:

$$a\cdot b = d\cdot h_1\cdot d\cdot h_2 = d^2\cdot\alpha_1\cdot\alpha_2 = d^2\frac{m}{a}\cdot\frac{m}{b} = \frac{d^2\cdot m^2}{a\cdot b} \Rightarrow a^2\cdot b^2 = d^2\cdot m^2$$

Ou seja, $ab = dm$, como queríamos demonstrar. □

Observação: uma importante consequência desse fato é que, sendo a e b inteiros não nulos e primos entre si, ou seja, $(a,b) = 1$, teremos: q

$$(a,b) \cdot [a,b] = a \cdot b \Rightarrow [a,b] = a \cdot b$$

.

7.1.6 Equações diofantinas

Suponhamos a seguinte situação: Pedro deseja comprar selos de 5 reais e de 3 reais e, para isso, quer gastar exatamente 50 reais. De quantas maneiras ele pode fazer essa compra?

Para resolvermos o problema acima, chamemos de x e y a quantidade de selos de 5 reais e 3 reais, respectivamente. Então, chegaremos a seguinte equação:

$$5x + 3y = 50 \,,$$

na qual devemos encontrar x e y inteiros positivos.

A equação encontrada é um exemplo do que chamamos de equação diofantina e será objeto de estudo nessa aula. O nome diofantina é uma homenagem ao matemático grego Diofanto (214 - 299) considerado por muitos como o "pai da Álgebra". Sua obra *Arithmetica*, que foi escrita por volta de 250 d.C, já traz referências a esses tipos de equações e como resolvê-las.

Definição 6 (Equação Diofantina)**.** *Chamamos de Equação Diofantina, toda equação da forma:*

$$ax + by = c, \;\; com \;\; a,b,c \in \mathbb{Z} \;\; e \; a,b \neq 0$$

Na equação $5x + 3y = 50$, temos $a = 5$, $b = 3$ e $c = 50$. Vejamos mais exemplos de equações diofantinas:

- $3x + y = 100$
- $4x + 6y = 9$

Proposição 7. *A equação diofantina*

$$ax+by=c, \ \ com \ \ a,b,c\in\mathbb{Z} \ \ e \ a,b\neq 0$$

possui solução se, e somente se, $(a,b)=d|c$. *Mais ainda, se o par* (x_0,y_0) *é uma solução dessa equação, temos que o conjunto dessa equação será formada por todos os pares de inteiros* (x,y) *da forma:*

$$x=x_0+t\frac{b}{d} \quad e \quad y=y_0-t\frac{a}{d}, \quad emque \quad t\in\mathbb{Z}$$

Demonstração. Suponhamos, por hipótese, que o par (x_0,y_0) seja uma solução da equação. Logo, teremos $ax_0+by_0=c$. Mas, como $d|a$ e $d|b$, temos que $d|c$, pela propriedade 6 estudada na seção de divisibilidade.

Da mesma forma, se $d|c$, existe $q\in\mathbb{Z}$ de forma que $c=qd$. No entanto, pelo Teorema de Bézout, existem dois inteiros x_0 e y_0 tais que $ax_0+by_0=d$. Daí, multiplicando os dois membros dessa última igualdade por q, teremos:

$$aqx_0+bqy_0=dq=c$$

Portanto, o par (x_1,y_1), com $x_1=x_0q$ e $y_1=y_0q$ é solução da equação difantina inicial.

Agora, considerando a solução (x_0,y_0) e seja o par (x,y) uma outra solução da equação difantina. Sendo assim, $ax_0+by_0=ax+by$. Então:

$$a(x-x_0)=b(y_0-y)$$

e, dividindo essa última igualdade por d, teremos:

$$\frac{a}{d}(x-x_0)=\frac{b}{d}(y_0-y)$$

mas, como $(\frac{a}{d},\frac{b}{d})=1$, pelo lema 2 concluímos que $\frac{a}{d}|(y_0-y)$ e $(\frac{b}{d}|(x-x_0)$. Portanto, existe $t\in\mathbb{Z}$ tal que:

$$x-x_0=t\frac{b}{d}\Rightarrow x=x_0+t\frac{b}{d} \quad e \quad y_0-y=t\frac{a}{d}\Rightarrow y=y_0-t\frac{a}{d}$$

□

Em termos de solução de uma equação diofantina, só existem duas possibilidades: ou ela não possui soluções ou possui infinitas soluções.

Exemplo 20. *Resolver a equação* $15x + 10y = 20$.

Solução 9. *Inicialmente, observemos que* $(15, 10) = 5$ *e que* $5|20$. *Logo, é garantido que essa equação possui solução. Vamos encontrar uma particular e, assim, encontrar a solução geral. Utilizando o algoritmo de Euclides para calcular* $(15, 10)$, *encontraremos as seguintes igualdades:*

$$\begin{aligned} 15 &= 10 \cdot 1 + 5, \\ 10 &= 5 \cdot 2 + 0. \end{aligned}$$

Daí, temos que $5 = 15 \cdot 1 - 10 \cdot 1$. *Multiplicando essa igualdade por* 4, *teremos,* $20 = 15 \cdot 4 + 10 \cdot (-4)$. *Portanto,* $x_0 = 4$ *e* $y_0 = -4$ *são soluções particulares dessa equação e a solução geral dessa equação será:*

$$x = 4 + t\frac{10}{5} = 4 + 2t \quad e \quad y = -4 - \frac{15}{5}t = -4 - 3t$$

Para $t = 2$, *por exemplo, teremos* $x = 4 + 2 \cdot 2 = 8$ *e* $y = -4 - 3 \cdot 2 = -10$. *De fato,* $15 \cdot 8 + 10 \cdot (-10) = 120 - 100 = 20$.

Exemplo 21. *Resolver a equação* $5x + 3y = 50$.

Solução 10. *Pelo algoritmo de Euclides, temos:*

$$\begin{aligned} 5 &= 3 \cdot 1 + 2, \\ 3 &= 2 \cdot 1 + 1, \\ 2 &= 1 \cdot 1 + 1. \end{aligned} \tag{7.3}$$

Da primeira e segunda igualdade, temos

$$1 = 3 - 2 \cdot 1 \;\; e \;\; 2 = 5 - 3 \cdot 1$$

Usando essas duas últimas, vamos obter:

$$\begin{aligned} 1 &= 3-2\cdot 1 \\ &= 3-(5-3\cdot 1)\cdot 1 \\ &= 5\cdot(-1)+3\cdot(2) \end{aligned} \tag{7.4}$$

mas, multiplicando por 50 essa última igualdade, teremos

$$5\cdot(-50)+3\cdot(100)=50$$

e daí, temos $x_0=-50$ *e* $y_0=100$*, soluções particulares dessa equação, donde concluímos que a solução geral será, para* $t\in\mathbb{Z}$*:*

$$x=-50+3t \quad e \quad y=100-5t$$

.

Essa equação desse último exemplo é referente ao problema exposto no início desse tópico. Pela natureza do problema, as soluções devem ser naturais. Deixaremos a cargo do leitor encontrá-las.

7.1.7 Congruências

O estudo da aritmética modular introduz o conceito de congruências, linguagem que foi desenvolvida por Karl Friedrich Gauss no início do século XIX e faz parte da Teoria dos Números.

Definição 7 (**Aritmética Modular**)**.** *A aritmética modular é um sistema em que as operações entre números inteiros são feitas em módulo, um outro inteiro n, positivo e diferente de zero. Para isso, definimos que um inteiro a é congruente a outro inteiro b módulo m,* $m\in\mathbb{Z}$*,* $m>1$*, se a divisão de a e b por m deixam o mesmo resto. Indica-se* $a\equiv b\ (mod\ m)$*. Por exemplo,* $9\equiv 5\ (mod\ 4)$*, pois ambos deixam restos* 1 *na divisão por* 4*. Temos também que* $15\equiv 2\ (mod\ 13)$*.*

Proposição 8. *$a \equiv b \ (mod\ n) \Leftrightarrow a - b$ é divisível por m.*

Demonstração. De fato, se a e b deixam o mesmo resto na divisão por m, temos

$$a = mq_1 + r_1 \quad e \quad b = mq_2 + r_2, \ com \ \ 0 \leq r_1 < m \ \ e \ \ 0 \leq r_2 < m$$

mas como, por hipótese, $r_1 = r_2$, temos $a - b = mq_1 + r_1 - (mq_2 + r_2) = m(q_1 - q_2)$, donde concluímos que $m|(a-b)$.

Vamos provar agora a outra implicação. Com efeito, temos $a - b = mq_1 + r_1 - (mq_2 + r_2) = m(q_1 - q_2) + (r_1 - r_2)$. Mas, como $m|(a-b)$ e $m|m(q_1 - q_2)$, concluímos que $m|(r_1 - r_2)$. No entanto, notemos que $-m < r_1 - r_2 < m$. Porém, como $r_1 - r_2$ é um múltiplo de m e, entre $-m$ e m, o único múltiplo de m é 0, concluímos que $r_1 - r_2 = 0$, o que resulta $r_1 = r_2$.

□

As propriedades abaixo serão importantes na resolução de vários exercícios. Sejam a, b, c e m inteiros, $m > 1$ e $n \in \mathbb{N}$, então:

1. $a \equiv a \ (mod\ m)$. (Reflexividade)
2. Se $a \equiv b \ (mod\ m)$, então $b \equiv a \ (mod\ m)$. (Comutatividade)
3. Se $a \equiv b \ (mod\ m)$ e $b \equiv c \ (mod\ m)$, então $a \equiv c \ (mod\ m)$. (Transitividade)
4. Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $a + c \equiv b + d \ (mod\ m)$.
5. Se $a \equiv b \ (mod\ m)$ e $c \equiv d \ (mod\ m)$, então $ac \equiv bd \ (mod\ m)$.
6. Se $a \equiv b \ (mod\ m)$, então $a^n \equiv b^n \ (mod\ m)$, $c \in \mathbb{N}$.
7. $a + c \equiv b + c \ (mod\ m) \Leftrightarrow a \equiv b \ (mod\ m)$.

8. Se $ac \equiv bc \ (mod\ m)$ e $(c,m) = 1$, então $a \equiv b \ (mod\ m)$.

9. Se $a \equiv b \ (mod\ m_i), i = 1,2,...,r$, então $a \equiv b \ (mod\ [m_1, m_2, ..., m_r])$.

Demonstração. Vejamos a demonstração de cada uma dessas propriedades:

1 De fato, $m|(a-a)$ para todo $a \in \mathbb{Z}$.

2 Com efeito, se $m|(a-b)$, então $m|(b-a)$.

3 De fato, se $m|(a-b)$ e $m|(b-c)$, então $m|(a-b)+(b-c)$. Daí, $m|(a-c)$, donde concluímos que $a \equiv c \ (mod\ m)$.

4 De fato, se $m|(a-b)$ e $m|(c-d)$, então $m|(a-b)+(c-d) = (a+c)-(b+d)$, o que mostra que $a+c \equiv b+d \ (mod\ m)$.

5 Basta notar que $ac - bd = a(c-d) + d(a-b)$. Portanto, $m|(ac-bd)$. Daí, $ac \equiv bd \ (mod\ m)$.

6 Com efeito, utilizando a propriedade 5 "n"vezes, temos:

$$\underbrace{a \cdot a \cdot a \cdot a \cdots a}_{n\,fatores} \equiv \underbrace{b \cdot b \cdot b \cdot b \cdots b}_{n\,fatores} \ (mod\ m),$$

o que mostra que $a^n \equiv b^n \ (mod\ m)$.

7 De fato, se $a+c \equiv b+c \ (mod\ m)$, então $m|(a+c)-(b+c) = (a-b)$, o que mostra que $a \equiv b \ (mod\ m)$.
Por outro lado, sendo $a \equiv b \ (mod\ m)$, temos que $c \equiv c \ (mod\ m)$ e, da propriedade 4, temos que $a+c \equiv b+c \ (mod\ m)$, como queríamos demonstrar.

8 Com efeito, se $ac \equiv bc \ (mod\ m)$, então $m|(ac-bc) = c(a-b)$. No entanto, sendo m e c primos entre si, temos que $m|(a-b)$, o que mostra que $a \equiv b \ (mod\ m)$.

9 Com efeito, como $a \equiv b \ (mod\ m_i), i = 1,2,...,r$, então $m_i|(a-b)$, para todo i. Sendo assim, $(a-b)$ é um múltiplo de cada m_i, donde segue que $[m_1, m_2, ..., m_r]|(a-b)$, como queríamos demonstrar.

□

Exemplo 22. *Qual é o resto da divisão de* $50^{20} + 35^{35}$ *por* 3*?*

Solução 11. *Utilizando as propriedades das congruências estudadas, tal cálculo será bastante simples. Para isso, notemos que* $50 \equiv -1 \ (mod\ 3)$. *Portanto,* $50^{20} \equiv (-1)^{20} \equiv 1 \ (mod\ 3)$. *Temos também que* $35 \equiv -1 \ (mod\ 3)$ *e, portanto,* $35^{35} \equiv (-1)^{35} \equiv -1 \ (mod\ 3)$. *Mas, como* $0 \equiv 3 \ (mod\ 3)$, *utilizando a propriedade 4, teremos* $35^{35} + 0 \equiv -1 + 3 \ (mod\ 3)$, *resultando, portanto, a partir daí, que* $35^{35} \equiv 2 \ (mod\ 3)$. *Mais uma vez, utilizando a propriedade 4, temos que* $50^{20} + 35^{35} \equiv 1 + 2 \equiv 0 \ (mod\ 3)$, *mostrando que o resto da divisão de* $50^{20} + 35^{35}$ *por* 3 *é* 0.

Proposição 9. *Sejam* $a, b \in \mathbb{Z}$ *e* $n \in \mathbb{N}$. *Temos que* $(a-b)|(a^n - b^n)$.

Demonstração. De fato, em particular, sendo $m = a - b$, temos $a \equiv b \ (mod\ m)$, pois é claro que $a - b|a - b$. Da propriedade 6, temos $a^n \equiv b^n \ (mod\ m)$, o que prova a proposição. □

Proposição 10. *Sejam* $a, b \in \mathbb{Z}$ *e* $n \in \mathbb{N}$. *Então,* $(a+b)|(a^{2n+1} + b^{2n+1})$.

Demonstração. Com efeito, considerando em particular $m = a + b$, temos $a \equiv -b \ (mod\ m)$. Como, para todo $n \in \mathbb{N}$, temos que $2n+1$ é um número ímpar, é fácil ver que $a^{2n+1} \equiv -b^{2n+1} \ (mod\ m)$, o que prova a proposição. □

Proposição 11. *Sejam* $a, b \in \mathbb{Z}$ *e* $n \in \mathbb{N}$. *Então, temos que* $(a+b)|(a^{2n} - b^{2n})$.

Demonstração. Mais uma vez, considerando $m = a + b$, verificando que $a \equiv -b \ (mod\ m)$ e que, para todo $n \in \mathbb{N}$, o número $2n$ é par, facilmente observa-se que $a^{2n} \equiv b^{2n} \ (mod\ m)$, como queríamos demonstrar. □

Exemplo 23. *Mostrar que, para todo* $n \in \mathbb{N}$, $11|(10^{2n+1} + 1)$.

Solução 12. *De fato, pela propriedade* 6, $11 = (10+1)|(10^{2n+1} + 1^{2n+1}) = 10^{2n+1} + 1$, *como queríamos demonstrar.*

Definição 8. *Um inteiro a é dito inversível módulo m se existir um outro inteiro* a' *tal que*

$$a \cdot a' \equiv 1 (mod\ m)$$

Por exemplo, 2 *e* 4 *são inversíveis módulo* 7*, pois* $2 \cdot 4 = 8 \cdot \equiv 1\ (mod\ 7)$.

Proposição 12. *Se um inteiro a é inversível módulo m, então* $(a,m) = 1$.

Demonstração. De fato, como por hipótese a é inversível módulo m, temos que:

$$a \cdot a' \equiv 1\ (mod\ m) \Rightarrow aa' = mk + 1 \Rightarrow aa' - mk = 1$$

daí, pelo teorema de Bezout, temos que $(a,m) = 1$. □

7.1.8 Teorema de Euler e Fermat

Definição 9. *Seja* $m \in \mathbb{N}^*$. *Seja* $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ *a decomposição de m em fatores. Definimos:*

$$\varphi(m) = p_1^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1} \cdot \ldots \cdot p_n^{\alpha_n - 1}(p_1 - 1)(p_2 - 1) \cdots (p_n - 1).$$

onde

$$\varphi : \mathbb{N}^* \longrightarrow \mathbb{N},$$

é chamada de função phi de Euler .

Exemplo 24. *Calcular* $\varphi(20)$.

Solução 13. *Como* $20 = 2^2 \cdot 5$*, então* $\varphi(2^2 \cdot 5) = 2^{2-1} \cdot 5^{1-1}(2-1)(5-1) = 8$.

Exemplo 25. *Encontrar* $\varphi(36)$.

Solução 14. *Ora,* $\varphi(36) = \varphi(2^2 \cdot 3^2) = 2^{2-1} \cdot 3^{2-1}(2-1)(3-1) = 12$.

Note que se se p é primo, então $\varphi(p) = p-1$. De fato, pela definição vista, $\varphi(p) = p^{1-1} \cdot (p-1) = p-1$. Por exemplo, $\varphi(23) = 23-1 = 22$.

Teorema 7 (Teorema de Euler)**.** *Sejam $m, a \in \mathbb{N}$ com $m > 1$ e $(a,m) = 1$. Então,*

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

A demonstração desse teorema não será realizada nesse artigo, mas sugerimos aos leitores que a pesquisem.

Exemplo 26. *Qual é o resto da divisão de 5^{61} por 33?*

Solução 15. *Ora, como $(5,33) = 1$, e $\varphi(33) = 3^0 \cdot 11^0(3-1)(11-1) = 20$, pelo Teorema de Euler, $5^{20} \equiv 1 \ (mod\ 33)$. Daí, $5^{61} = 5^{60+1} \equiv (5^{20})^3 \cdot 5 \equiv 1 \cdot 5 \equiv 5 \ (mod\ 33)$, o que mostra que o resto dessa divisão é 5.*

Uma consequência desse Teorema será vista a seguir.

Teorema 8 (Teorema de Fermat)**.** *Seja p um número primo e $a \in \mathbb{Z}$ com $(a,p) = 1$. Então:*

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

Demonstração. Como p é primo, $\varphi(p) = p-1$ e, mais ainda, como $p \nmid a$, pelo Teorema de Euler, teremos:

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

Como $a \equiv a \ (mod\ p)$, utilizando as propriedades das congruências, temos:

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

□

Observação: Sendo p primo, $a \in \mathbb{Z}$ com $(a,p) = 1$, concluímos, na demonstração anterior, que

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

Esse resultado é conhecido como **Pequeno Teorema de Fermat**.

Exemplo 27. *Quais são os dois últimos algarismos do número* 3^{121} *?*

Solução 16. *É claro que para descobrirmos esses dois algarismos, precisamos dividir* 3^{121} *por* 100*. Como* $(3,100) = 1$*, uma boa estratégia é utilizarmos o Teorema de Euler. Com um simples cálculo, descobrimos que* $\varphi(100) = 40$ *e, portanto,* $3^{40} \equiv 1 \ (mod \ 100)$*. Daí:*

$$3^{121} = 3^{40 \cdot 3+1} \equiv (3^{40})^3 \cdot 3 \equiv 3 \ (mod \ 100)$$

Porém, fazendo os devidos cálculos, também poderíamos descobrir que o menor inteiro n tal que $3^n \equiv 1 \ (mod \ 100)$ é $n = 20$, ou seja, $3^{20} \equiv 1 \ (mod \ 100)$ (fica a cargo de leitor fazer tal verificação). Dizemos, nesse caso, que 20 é a ordem de 3 com relação a 100. Em notação, $\text{ord}_{100}(3) = 20$. De maneira geral, temos:

Definição 10. *Sejam* $a, m \in \mathbb{N}^*$*, com* $m > 1$ *e* $(a,m) = 1$*. Definimos como a ordem de a com relação a m como sendo o número natural tal que:*

$$ord_m(a) = min\{i \in \mathbb{N}^*; a^i \equiv 1 \ (mod \ m)\}$$

Proposição 13. *Se* $k = ord_m(a)$*, então* $k | \varphi(m)$*.*

Demonstração. De fato, pela divisão euclidiana, podemos escrever:

$$\varphi(m) = kq + r, \text{ com } 0 \leq r < k.$$

daí, supondo, por absurdo, que $r \neq 0$, teremos:

$$1 \equiv a^{\varphi(m)} \equiv a^{kq+r} \equiv (a^k)^q \cdot a^r \equiv a^r \ (mod \ m)$$

mas isso é um absurdo, pois supomos $0 < r < k$ e k é o menor expoente não nulo i tal que $a^i \equiv 1 \ (mod \ m)$. □

Exemplo 28. *Mostre que* $18 | 5^{1000} + 5$.

Solução 17. *Inicialmente, notemos que* $(5,8) = 1$. *Daí, podemos utilizar o Teorema de Euler. Temos então que* $\varphi(18) = \varphi(2) \cdot \varphi(3^2) = 1 \cdot 6 = 6$. *Portanto,* $5^6 \equiv 1 \ (mod\ 18)$. *No entanto, como* $1000 = 6 \cdot 166 + 4$, *segue que* $5^{1000} \equiv (5^{166})^6 \cdot 5^4 \equiv 1 \cdot 625 \equiv 13 \ (mod\ 18)$. *Portanto,* $5^{100} + 5 \equiv 13 + 5 \equiv 0 \ (mod\ 18)$, *como queríamos mostrar.*

Exemplo 29. *Qual é o resto da divisão de* 4^{110} *por* 23*?*

Solução 18. *Note que* $(4,23) = 1$. *Como* 23 *é primo, pelo Pequeno Teorema de Fermat, temos*

$$4^{23-1} = 4^{22} \equiv 1 \ (mod\ 23) \Rightarrow (4^{22})^5 \equiv 1^5 \ (mod\ 23) \Rightarrow 4^{110} \equiv 1 \ (mod\ 23).$$

Portanto, o resto divisão de 4^{110} *por* 23 *é* 1.

7.2 Considerações finais

Este artigo, acreditamos, contribui com o estudo, conhecimento e aprofundamento de tópicos básicos da Teoria dos Números. A linguagem utilizada é bastante acessível, inclusive para alunos do ensino básico. É importante destacar que esse trabalho foi fundamentado na dissertação de Josemar Claudino Barbosa, sob a orientação da Dra. Bárbara Costa da Silva, cujo título é "Teoria dos Números no Ensino Básico: Um estudo de caso no 2º ano do Ensino Médio". Será possível acessá-lo nas referências bibliográficas desse artigo.

7.3 Referências bibliográficas

BARBOSA, Josemar Claudino. .**Teoria dos números no ensino básico: um estudo de caso no 2º ano do ensino médio**.2017. 130f. Dissertação. Mestrado Profissional em Matemática. Universidade Federal Rural de Pernambuco, Recife.

BISPO, Dinguiston dos Santos.**Equações Diofantinas Lineares e suas**

Aplicações.2013.76 f. Monografia (Licenciatrua em Matemática). Universidade Estadual do Sudoeste da Bahia, Vitória da Conquista.

COSTA, Eduardo S..**Equações Diofantinas Lineares e o Professor do Ensino Médio**. 2007. 119f. Dissertação. Mestrado Acadêmico em Educação Matemática. Pontifícia Universidade Católica de São Paulo, São Paulo.

COUTINHO, S.C. **Números Inteiros e Criptografia RSA**. Rio de Janeiro: IMPA, 2014.

DIAS, Cristina Helena Bovo Batista.**Números Primos e Divisibilidade: Estudo de Propriedades**. 2013.49f. Dissertação (Mestrado Profissinal em Matemática). Universidade Estadual Paulista, São Paulo.

FOMIM, Dmitri. **Círculos Matemáticos.** Rio de Janeiro: IMPA, 2012.

FONSECA, Rubens.**Teoria dos Números**. Belém: Universidade Estadual do Pará (UEPA), 2011.

noindent HEFEZ, Abramo. **Elementos de Aritmética**. 2ª ed. Rio de Janeiro: SBM, 2011.

MOREIRA, Carlos Gustavo Tamm de Araújo. **Tópicos de Teoria dos Números.** Rio de Janeiro: SBM, 2012.

MOREIRA, Carlos Gustavo Tamm de Araújo. **Olimpíadas Brasileiras de Matemática - 9ª à 16ª.**1ª ed. Rio de Janeiro: SBM, 2003.

OLIVEIRA, Maycon Costa de.**Aritmética: Criptografia e outras aplicações de Congruências**.2013.74 f. Dissertação (Mestrado Profissional em Matemática). Universidade Federal do Mato Grosso do Sul, Campo Grande.

TAO, Terence.**Como resolver problemas matemáticos - Uma perspectiva pessoal**. Rio de Janeiro: SBM, 2013.

Capítulo 8

Cônicas: Refletindo e aprendendo

Ma. Kaliny Ferreira do Nascimento[1]
Dra. Anete Soares Cavalcanti[2]

Resumo: As cônicas são objetos matemáticos com várias aplicações, como seu uso na Acústica, na Medicina e na Engenharia Civil, dentre outras. Apesar disso, pouco se fala nas salas de aula de Ensino Básico sobre essas utilidades, vinculadas fortemente às suas propriedades de reflexão, estabelecendo para os alunos uma restrição desses objetos ao mundo "abstrato" da Álgebra por meio do estudo de suas equações. Para apresentar aos estudantes uma abordagem mais concreta e significativa das cônicas, este artigo visa propor atividades que busquem introduzir esse conteúdo de maneira simples e divertida. Tais atividades também são úteis para consolidar a ideia do conceito dessas cônicas e da localização de seus elementos, preparando, assim, os alunos para um posterior estudo mais aprofundado e teórico dessas curvas. Este trabalho, composto por cinco atividades, foi aplicado na Escola de Referência em Ensino Médio (EREM) Aníbal Falcão, localizada em Tejipió,

[1]Professora da Secretaria de Educação e Esportes de Pernambuco – SEE, kaliny.ferreira@yahoo.com.br

[2]Professora da Universidade Federal Rural de Pernambuco – UFRPE, anete.soares@ufrpe.br

bairro de Recife-PE. Espera-se que essa pesquisa inspire professores de matemática a aplicarem, nas suas aulas, a proposta apresentada.

Palavras-chave: Cônicas; Reflexão; Lúdico; Ensino de Matemática.

8.1 Introdução

As cônicas têm sido objetos de estudo há muitos séculos. Elas possuem propriedades de reflexão que instigaram a curiosidade de muitos matemáticos desde antes de Cristo até hoje. Muitas são as suas aplicabilidades na sociedade, entretanto elas são pouco exploradas em sala de aula. Além de estimular os alunos, o uso de aulas lúdicas com experimentos práticos é útil para consolidar a ideia do conceito dessas cônicas e da localização de seus elementos.

Nas últimas décadas, a Educação brasileira vem sofrendo uma grande revolução quanto aos seus objetivos fundamentais, procurando se distanciar cada vez mais de uma formação engessada e formulaica, por vezes inalcançável aos alunos, e focando em uma maneira mais simples e contextualizada. Essa nova onda filosófica defende que o raciocínio matemático não deve ser compartimentalizado e desvinculado do contexto social no qual o estudante está inserido. Pode-se verificar essa ideia nos documentos oficiais recentes de Educação, cujo principal é a Base Nacional Comum Curricular (BNCC) do Ensino Médio.

A BNCC do Ensino Médio enfatiza que é necessário haver um ensino de maneira a integrar os campos da Matemática (Aritmética, Álgebra, Geometria, Probabilidade e Estatística, Grandezas e Medidas). Para isso, utilizam-se os pares de ideias. São eles: variação e constância; certeza e incerteza; movimento e posição; e relações e inter-relações (BRASIL, 2018). Estudando as seções cônicas, pode-se utilizar de muitos desses pares de ideias.

Quando, por exemplo, a partir do conceito dessas curvas como Lugar Geométrico (L.G.) chegamos ao formato dessa cônica, estamos utilizando, pelo menos, o par de ideia variação e constância que, segundo a BNCC,

"envolve observar, imaginar, abstrair, discernir e reconhecer características comuns e diferentes ou o que mudou e o que permaneceu invariante, expressar e representar (ou descrever) padrões, generalizando-o" (BNCC, 2018, p. 520). Daí a relevância de se estudar não somente as cônicas, mas também suas propriedades que são muito usadas em várias áreas do conhecimento e revertidas em benefícios para a nossa sociedade.

No ensino público estadual de Pernambuco, o conteúdo GEOMETRIA ANALÍTICA: SECÇÕES CÔNICAS - Parábola; Elipse; Hipérbole - é restrito para o currículo das escolas integrais, pois essas possuem uma carga horária maior em comparação com as regulares. As expectativas de aprendizagem são as seguintes:

> Dominar a aplicação dos conhecimentos de geometria analítica na resolução de problemas. Encontrar as equações das cônicas (parábola, elipse e hipérbole). Resolver sistemas de equações e inequações do segundo grau a duas variáveis, tanto algébrica quanto graficamente (PERNAMBUCO, 2013, p. 23).

Para se atingir esse nível de abstração matemática que essas expectativas de aprendizagem propõem, é necessário que haja antes uma forte compreensão das características do objeto matemático em estudo. Para facilitar esse aprendizado, o professor pode lançar mão de atividades lúdicas que reforcem essas características básicas das cônicas, como os seus formatos, e as propriedades de reflexão que trarão significado e aguçarão a curiosidade dos estudantes nesse processo de aprendizagem.

Este artigo é um recorte da dissertação *Luz, Cônicas, Reflexão: uma sequência didática para o ensino das cônicas* (NASCIMENTO, 2020), cujo objetivo geral é apresentar um conjunto de atividades lúdicas para auxiliar professores durante o processo de ensino-aprendizagem das cônicas para alunos do Ensino Básico. Os objetivos específicos são: compreender a definição dos elementos determinantes das cônicas e indicá-los algébrica e geometricamente; construir modelos geométricos que representem as cônicas e suas propriedades refletoras; e, por fim, associar as proprieda-

des refletoras das cônicas às suas utilizações na sociedade, a fim de dar significado ao estudo desse objeto matemático.

Ressaltamos que apesar dessa pesquisa se tratar de um assunto presente na grade curricular do Ensino Médio e ter sido aplicada nessa etapa escolar, as atividades lúdicas propostas na Seção 8.2 são bastante simples e requerem pouco conhecimento matemático prévio. Muitos experimentos visam exercitar aspectos mais básicos acerca das cônicas, como identificar seus formatos e compreender suas propriedades refletoras, sendo assim, aplicáveis a quaisquer níveis da educação básica.

O artigo possui duas seções, sendo a primeira uma sequência didática para o ensino das cônicas e suas propriedades refletoras aplicadas em uma turma de Ensino Médio. Ela é baseada em atividades lúdicas na qual o aluno constrói conhecimento através de experimentos práticos. Na segunda e última, apresentamos os resultados das nossas observações durante a aplicação das sequências didáticas. É válido ressaltar que a autora também foi a professora que aplicou as atividades supracitadas.

8.2 Fundamentos teóricos e metodológicos

Em uma sala de aula, cada atividade ou tarefa proposta pelo professor com uma determinada finalidade é classificada por Zabala (2015) como unidade elementar do processo de ensino-aprendizagem. Entretanto ele, apesar de reconhecer a importância dessas unidades, defende que elas são insuficientes por si só para realizar uma análise completa acerca do processo de ensino-aprendizagem de um determinado conteúdo. Para ficar mais claro, segue um exemplo.

Em uma abordagem tradicional, a realização de uma lista de exercício acerca de um determinado assunto normalmente é feita após a sua exposição por parte do professor. Por outro lado, em algumas metodologias ativas de ensino, como na sala de aula invertida, ela pode ser proposta inicialmente para os alunos e o seu conteúdo ser trazido para aula por meio de um debate mediado, posteriormente, pelo professor.

No exemplo acima, pode-se observar que a unidade elementar "lista de exercício" pode assumir funções e características diferentes que dependem das unidades elementares que a precedem ou sucedem. Na primeira situação, ela pode ser entendida como um meio de aferir a internalização dos tópicos apresentados na aula expositiva. Enquanto que, na segunda, o professor pode ter desejado usá-la para introduzir o conteúdo, despertando no estudante habilidades como a investigação e o protagonismo.

Assim, é necessário tomar uma outra unidade que permita realizar a análise desse desenvolvimento educativo em torno de um conteúdo, relacionando as unidades elementares entre si e situando-as em relação às diversas variáveis desse processo como, por exemplo, recursos e tempo utilizados. Zabala (2015) apresenta a "sequência de atividades ou sequência didática" como essa unidade de caráter processual.

Sequência didática é um termo comum no mundo docente. Entretanto, para os leitores não familiarizados, o termo pode ser confundido com outros termos pedagógicos. Sendo assim, a definição de sequência didática considerada neste trabalho é:

> Sequência didática é um conjunto de atividades ligadas entre si, planejadas para ensinar um conteúdo, etapa por etapa, organizadas de acordo com os objetivos que o professor quer alcançar para aprendizagem de seus alunos e envolvendo atividades de avaliação que pode levar dias, semanas ou durante o ano. É uma maneira de encaixar os conteúdos a um tema e por sua vez a outro tornando o conhecimento lógico ao trabalho pedagógico desenvolvido (PERETTI; TONIN DA COSTA, 2013, p. 6).

Além de considerar a sequência didática fio condutor do processo de ensino-aprendizagem, pode-se combiná-la à outras ferramentas para potencializar essa construção de conhecimento. Uma dessas ferramentas é a ludicidade.

Segundo Evangelista et al., "a Matemática é uma ciência muito complexa [...] (que) requer atenção especial e disciplina na sua aplicação, o que faz com que muitos alunos apresentem certa dificuldade no momento da sua

aprendizagem e execução" (2013, p. 4), por isso é importantíssimo obter a atenção e o engajamento dos estudantes nessa caminhada. As atividades lúdicas, como jogos ou experimentos práticos, são armas muito poderosas quando se tem esse objetivo.

Conforme Evangelista et al, "para os alunos, aula boa é aquela que consegue prender a atenção deles de forma que o tempo passe sem que eles percebam e proporcione aprendizagem interativa e dinâmica" (2013, p. 5), atribuições facilmente alcançadas quando se envolve a ludicidade.

Dentre os benefícios de se aplicar uma sequência didática lúdica, destaca-se:

> Explanações que são feitas com exemplos que atrai a atenção e a curiosidade dos alunos são absorvidas e interpretadas com mais facilidade. Temas que são desenvolvidos em ambientes diversificados, claros, arejados, que proporcione o bem estar do aluno e que exija dele participação ativa, certamente não serão esquecidos. Os alunos gostam e preferem aulas diferentes, a metodologia rotineira de quadro negro, sala de aula com professor escrevendo e o aluno copiando está ultrapassado e não desperta no aluno nenhum estímulo nem interesse de prestar atenção e aprender o que o professor está ensinando (EVANGELISTA et al., 2013, p. 5).

Diante dessa explanação acerca das vantagens dessas duas ferramentas, parece relevante utilizá-las. Portanto essa pesquisa foi feita atentando para essa rica combinação pedagógica entre o uso da sequência didática e da ludicidade.

Os materiais utilizados são, em sua grande maioria, de fácil acesso e baixo custo como, lanterna, cartolina, barbante, régua, compasso, tachinhas, isopor, entre outros. Além de reutilizar materiais que seriam descartados, promovendo, assim, um impacto positivo no meio ambiente, os experimentos produzidos foram expostos na II Feira de Matemática da EREM

Aníbal Falcão pelos alunos da turma do 3^o ano A de 2019, além de servirem de recurso pedagógico para auxiliar professores no processo de ensino-aprendizagem das cônicas em turmas futuras, pois estão à disposição de outros docentes na escola.

Na maioria das atividades diferenciadas propostas, optou-se por materializar os conceitos trabalhados no livro didático concordando com o que diz Silva et al.: "o material concreto é uma forma de apresentar ao aluno uma maneira mais fácil e palpável de aprender matemática e como ela pode ser usada no nosso cotidiano" (2016, p. 4).

A seguir, apresentaremos a trajetória de aplicação da sequência didática dessa pesquisa.

8.2.1 Sequência didática - aplicação das atividades lúdicas

Nessa seção, apresentaremos a sequência didática desenvolvida com o intuito de tornar mais lúdico o ensino de cônicas e suas propriedades refletoras.

O enfoque dessa sequência didática foi nas definições gerais e na aplicação das propriedades refletoras, não se apegando à rigidez das fórmulas analíticas das cônicas, sendo assim, não demanda dos alunos conhecimentos matemáticos muito sofisticados ou abstratos, podendo, inclusive, ser aplicada em séries anteriores, como, por exemplo, nos anos finais do Ensino Fundamental.

As demonstrações matemáticas das construções utilizadas nessa sequência didática podem ser encontradas em Nascimento (2020).

- **Tema:** As cônicas e suas propriedades refletoras.

- **Público alvo:** alunos a partir do 8º ano do Ensino Fundamental.

- **Duração:** 12 aulas (aproximadamente 4 encontros com duas aulas de 50 minutos cada e 1 encontro de quatro aulas de 50 minutos cada para a visita técnica).
- **Disciplina:** Matemática.
- **Objetivo geral:** Apresentar uma sequência didática utilizando atividades lúdicas no ensino das cônicas e suas propriedades refletoras.
- **Objetivos específicos:**

    1. Reconhecer as características de cada cônica;
    2. Identificar os elementos das cônicas;
    3. Comprovar a definição de cada cônica através de teste de medição;
    4. Identificar as retas tangentes às curvas;
    5. Compreender e aplicar as propriedades refletoras das cônicas;
    6. Motivar os alunos a estudarem matemática.

- **Avaliação:**

    – *Formativa:* observar o engajamento e desempenho dos alunos durante a aula e acompanhar suas produções nas diversas atividades de classe;

    – *Somativa:* Realização de um teste individual e sem consulta composto por 8 questões abertas acerca do assunto estudado, ver Apêndice 8.4.

Nas subseções a seguir, descreveremos cada uma das atividades realizadas como momentos didáticos em sala de aula, explicitando a quantidade de aulas utilizadas, bem como os materiais e procedimentos adotados.

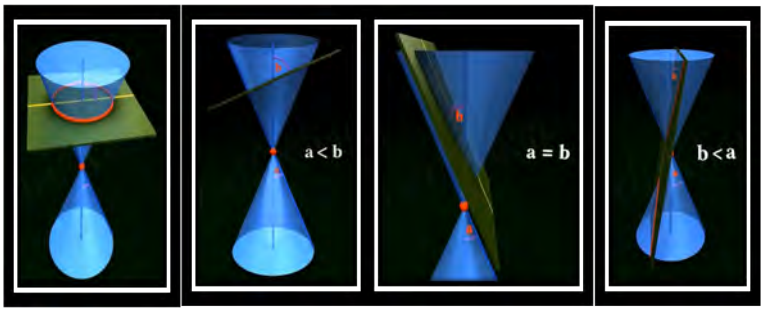
8.2.1.1 Atividade 1: Experimento com lanterna (Duração: 1 aula).

Num primeiro momento, fizemos um experimento com lanterna, a fim de estimular, nos estudantes, a relação do formato de cada curva com suas origens, descobertas por Menaechmus (380 - 320 a.C.), que são as de seções em um cone. Segue a descrição da primeira atividade.

Materiais adotados: notebook, data show e lanterna.

Inicialmente, apresentamos o vídeo *Conic Section 3D Animation* (CREATIVE LEARNING, 2015). Nele, mostramos a relação de cada cônica com o ângulo de inclinação do plano que secciona o cone duplo em relação ao seu eixo, (Ver Figura 8.1). Nesse aspecto, podemos obter quatro tipos de ângulos:

Figura 8.1: Determinação das cônicas através da inclinação de um plano que secciona um cone de duas folhas



Capturas de tela retiradas de Creative Learning (2015).

1. Reto: circunferência;
2. Maior que o da geratriz do cone: elipse;
3. Igual ao da geratriz do cone: parábola;
4. Menor que o da geratriz do cone: hipérbole.

Em um ambiente suficientemente escuro, direcionamos a lanterna para a parede e, à medida que inclinamos a lanterna em relação à parede, a

intersecção dos feixes de luz com a parede desenharam as cônicas. Os feixes de luz que saem da lanterna são emitidos em forma de cone e a parede se comporta como um plano que o secciona.

Figura 8.1: Experimentos com lanterna

Elaborado pela autora.

A cada figura nova que surgia os alunos eram instigados a refletir para responder às seguintes perguntas:

1. Que tipo de ângulo o plano faz com o eixo do cone?

2. Qual é a cônica formada?

Através da variação da inclinação da lanterna[3] pode-se obter uma circunferência, uma elipse, uma parábola ou um ramo de hipérbole.

[3]Em outra perspectiva, pode-se considerar que o plano seccionador do cone (formato com que os feixes se posicionam no espaço), representado pela parede, é quem se move em relação ao eixo desse cone.

8.2.1.2 Atividade 2: Contruções das cônicas com barbante (Duração: 3 aulas).

A segunda atividade diferenciada proposta foi a construção das cônicas pelos alunos.

Materiais utilizados: cartolina, barbante, régua, esquadro, lápis e tachinhas.

(i) **Elipse**

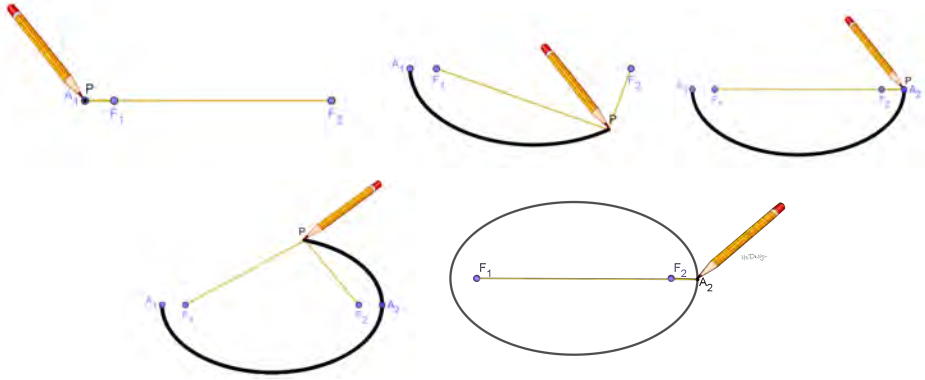
Utilizando um pedaço de barbante e duas tachinhas, pode-se construir uma elipse por meio dos passos (ver Figura 8.2):

- Tome um pedaço de barbante de tamanho $2a$;
- Em seguida, marque dois pontos fixos F_1 e F_2 na cartolina, de modo que a distância entre eles seja menor que $2a$;
- Com o auxílio das tachinhas, fixe as extremidades do barbante em F_1 e F_2;
- Encoste o lápis no barbante e estique-o;
- Faça o lápis deslizar pelo barbante esticado traçando na cartolina essa trajetória.

Pode-se encontrar as animações relativas a essa construção no link: <https://www.geogebra.org/m/dbver82d>.

Após a construção, os alunos marcaram dois pontos quaisquer sobre a elipse e, com o auxílio da régua, verificaram que a soma das distâncias de qualquer um desses pontos aos pontos F_1 e F_2 é constante, concluindo assim que a figura obtida foi uma elipse. Em seguida, identificaram na figura os elementos da elipse.

Figura 8.2: Construção com barbante de uma elipse



Elaborado pela autora.

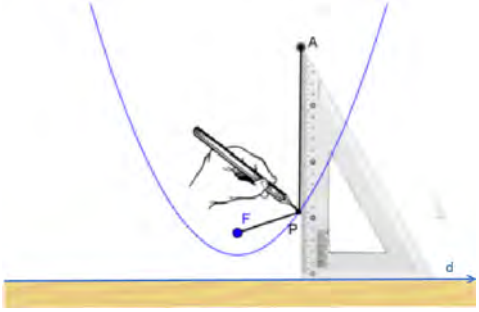
Figura 8.3: Construção da elipse com o auxílio do barbante pelos alunos

Elaborado pela autora.

(ii) **Parábola**

Utilizando um pedaço de barbante, um esquadro, uma régua e uma tachinha, pode-se construir uma parábola através dos passos:

Figura 8.4: Construção com barbante de uma parábola



Moreira (2017, p. 84).

- Tome um pedaço de barbante cujo comprimento seja igual ao maior cateto de um esquadro escaleno (ver Figura 8.4);
- Trace uma reta r qualquer na cartolina e fixe uma régua sobre ela durante o processo de desenho;
- Apoie o lado menor do esquadro sobre a régua fixada e amarre uma das extremidades do barbante na ponta do esquadro que mede 60^o;
- Marque um ponto F na cartolina de modo que a distância entre ele e a reta r seja positiva e menor que o tamanho do cateto maior do esquadro;
- Com o auxílio de uma tachinha, fixe a outra extremidade do barbante no ponto F;
- Desloque o esquadro sobre a régua e, simultaneamente, desenhe a parábola mantendo, com o auxílio de um lápis, o barbante esticado e encostado no esquadro.

Pode-se encontrar as animações relativas a essa construção no link: <https://www.geogebra.org/m/hdpp9dx6>.

Figura 8.5: Construção da parábola com o auxílio do barbante pelos alunos

Elaborado pela autora.

Após a construção, os alunos marcaram dois pontos quaisquer sobre a parábola e, com o auxílio da régua, verificaram que as distâncias entre esses pontos e a reta d (diretriz) e o ponto F (foco) são iguais, concluindo assim que a figura obtida foi uma parábola. Em seguida, identificaram na figura os elementos da parábola.

(iii) **Hipérbole**

Utilizando um pedaço de barbante e uma régua, pode-se construir uma hipérbole por meio dos passos:

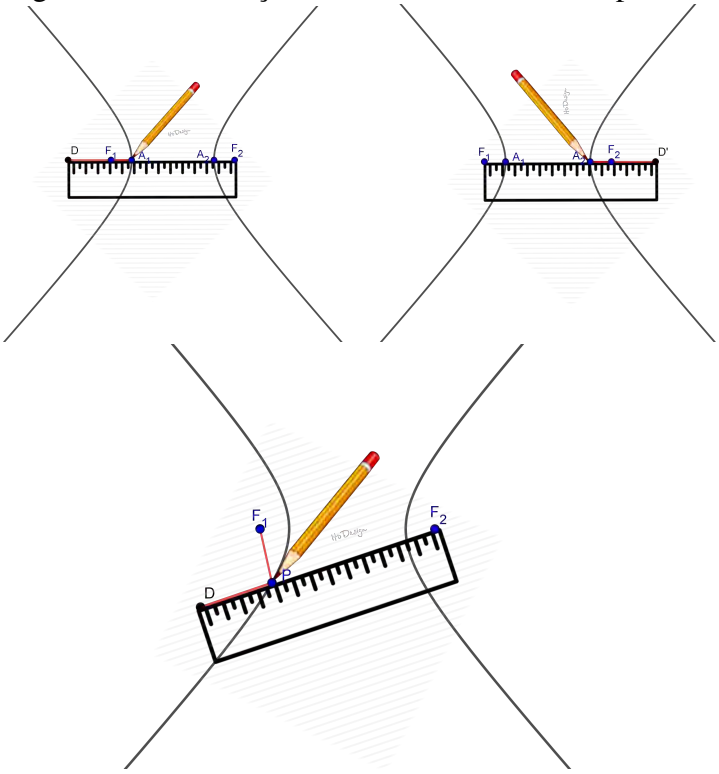
- Marque na cartolina dois pontos, F_1 e F_2;
- Corte um pedaço de barbante de maneira que o seu comprimento não ultrapasse o tamanho da régua;
- Prenda uma das extremidades do barbante na régua;
- Fixe a extremidade livre do barbante no ponto F_1 e coloque a extremidade oposta da régua no outro ponto F_2;

- Mantenha o lápis encostado na régua e o fio esticado e gire a régua em torno do ponto F_2, desenhando esse percurso;

- Depois faça o mesmo, invertendo a posição da régua.

Pode-se encontrar as animações relativas a essa construção no link: <https://www.geogebra.org/m/bbbdabvv>.

Figura 8.6: Construção com barbante de uma hipérbole



Elaborada pela autora.

Figura 8.7: Construção da hipérbole com o auxílio do barbante pelos alunos

Elaborado pela autora.

Após a construção, os alunos marcaram dois pontos quaisquer sobre a hipérbole e, com o auxílio da régua, verificaram que o módulo da diferença das distâncias entre esses pontos e os pontos F_1 e F_2 são sempre constantes, concluindo assim que a figura obtida foi uma hipérbole. Em seguida, identificaram na figura os elementos da hipérbole.

8.2.1.3 Atividade 3: Construção das cônicas usando dobradura (Duração: 2 aulas).

O terceiro experimento realizado utiliza a técnica de dobraduras. O procedimento segue os algoritmos apresentados nas Figuras 8.2, 8.4 e 8.6, mas cada mediatriz (reta tangente) traçada nas figuras anteriormente corresponde aqui a uma dobra de papel. As curvas delimitadas pelas dobras são as cônicas.

Pode-se encontrar as animações relativas a essas construções nos links: <https://www.geogebra.org/m/xtr4mt4m>, <https://www.geogebra.org/m/j2n4e7uy> e <https://www.geogebra.org/m/zezhy52a>.

- Algoritmo de construção de uma elipse por meio de dobraduras.

- PASSO 1 - Construa uma circunferência de centro A, marque um ponto interior, C, e um ponto D sobre ela;

- PASSO 2 - Construa os segmentos $\overline{AD}$ e $\overline{CD}$;

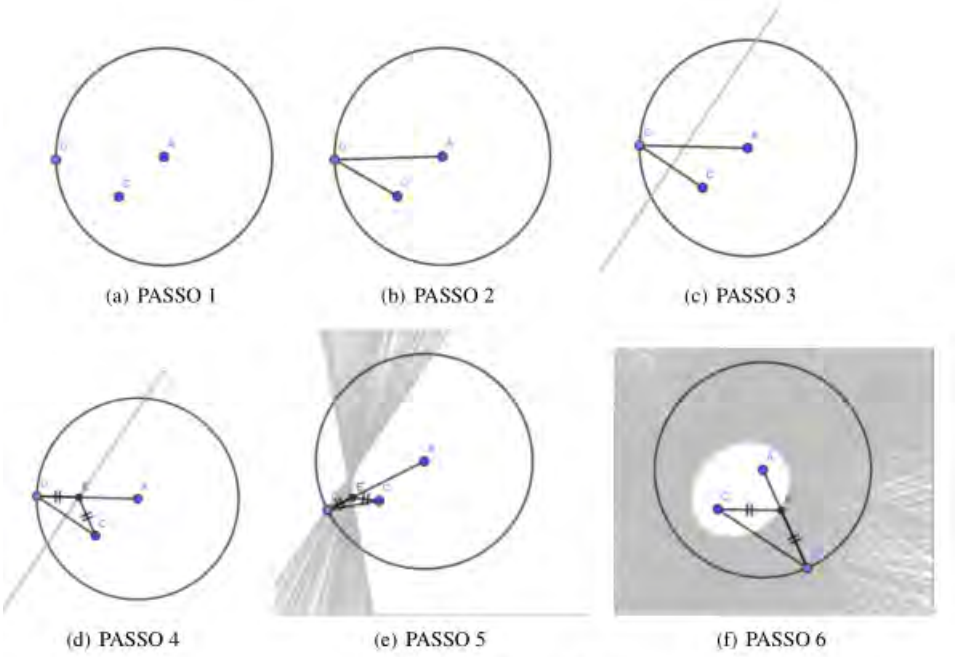
- PASSO 3 - Trace a mediatriz do segmento $\overline{CD}$;

- PASSO 4 - Marque o ponto de interseção E dessa mediatriz com o segmento $\overline{AD}$;

- PASSO 5 - Tome outros pontos sobre a circunferência no lugar de D e repita o processo anterior;

- PASSO 6 - Pela definição de L.G. de uma elipse, o conjunto de pontos "E" é uma elipse, cujos focos são os pontos A e C.

Figura 8.8: Construção da elipse a partir de suas retas tangentes



Fonte: Elaborado pela autora

- Algoritmo de construção de uma parábola através de dobraduras.

- PASSO 1 - Construa uma reta d e marque um ponto A sobre ela e um ponto F fora dela;

- PASSO 2 - Trace o segmento $\overline{AF}$ e a reta r perpendicular a d que passa por A;

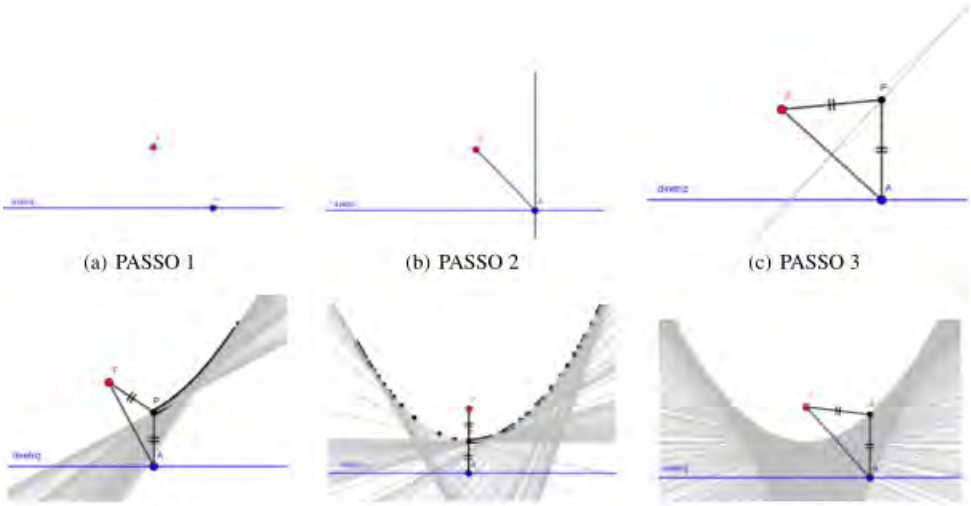
- PASSO 3 - Construa a mediatriz do segmento AF e marque o ponto P de interseção entre ela e a reta r;

- PASSO 4 - Escolha outros pontos na reta d para substituir o A e repita o processo anterior;

- PASSO 5 - Note que o conjunto dos pontos P corresponde à Definição de parábola como L.G.;

- PASSO 6 - Portanto, essa curva é uma parábola cujo foco é o ponto F e diretriz é a reta d.

Figura 8.9: Construção da parábola a partir de suas retas tangentes



(a) PASSO 1 (b) PASSO 2 (c) PASSO 3

(d) PASSO 4 (e) PASSO 5 (f) PASSO 6

Fonte: Elaborado pela autora

- Algoritmo de construção de uma hipérbole através de dobraduras.

- PASSO 1 - Construa uma circunferência de centro F_1 e marque um ponto C sobre ela e um ponto F_2 externo a ela;

- PASSO 2 - Trace o segmento $\overline{CF_2}$ e a sua reta mediatriz;

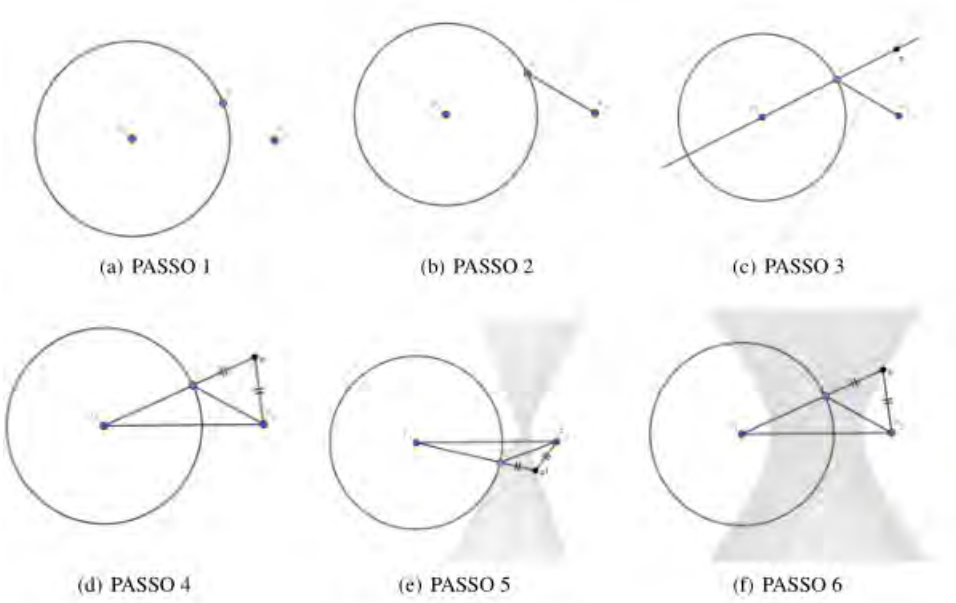
- PASSO 3 - Trace a reta $\overleftrightarrow{F_1C}$ e marque o ponto P de interseção entre ela e a mediatriz do segmento $\overline{CF_2}$;

- PASSO 4 - Trace o segmento $\overline{F_1F_2}$ e note que, como P pertence à mediatriz do segmento $\overline{CF_2}$, então $\overline{PC} \equiv \overline{PF_2}$;

- PASSO 5 - Escolha outros pontos da circunferência para substituir o C e repita o processo anterior;

- PASSO 6 - Note que, segundo a definição de hipérbole como L.G., o conjunto dos pontos P corresponde a uma hipérbole de focos F_1 e F_2.

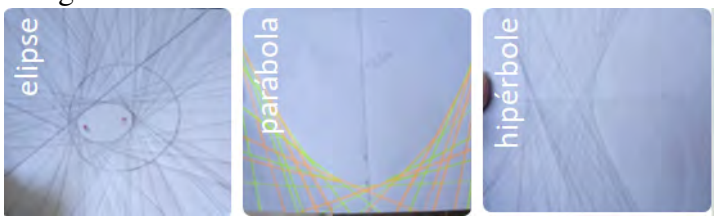
Figura 8.10: Construção da hipérbole a partir de suas retas tangentes



Fonte: Elaborado pela autora

A Figura 8.11 abaixo mostra um exemplo de cada curva produzida em sala de aula pelos estudantes durante o processo de aplicação do terceiro experimento.

Figura 8.11: Cônicas obtidas através de dobraduras



Fonte: Elaborado pela autora.

No processo de construção, o aluno entenderá as características e propriedades de cada cônica, além de desenvolver habilidades de manipulação de

instrumentos geométricos como régua e compasso. A Figura 8.12 abaixo mostra tal experimento sendo realizado.

Figura 8.12: Construção das cônicas através de dobraduras

Elaborado pela autora.

8.2.1.4 Atividade 4: Experimento de reflexão (Duração: 2 aulas).

Nessa quarta atividade, buscamos enfatizar as propriedades óticas (ou refletoras) das cônicas. Elas são utilizadas em tecnologias para beneficiar a sociedade.

Para cada cônicas realizamos uma construção específica que permite aos dissentes a visualização de como funcionam tais propriedades.

(i) **Propriedade refletora da elipse**

A elipse possui uma propriedade refletora aplicada, por exemplo, no aparelho Litotritor usado em tratamentos de cálculos renais. Nessa atividade, propomos a construção de um modelo concreto que mostre a aplicação dessa propriedade em um "bilhar elíptico", considerando a luz como conjunto de partículas em substituição das bolas de bilhar.

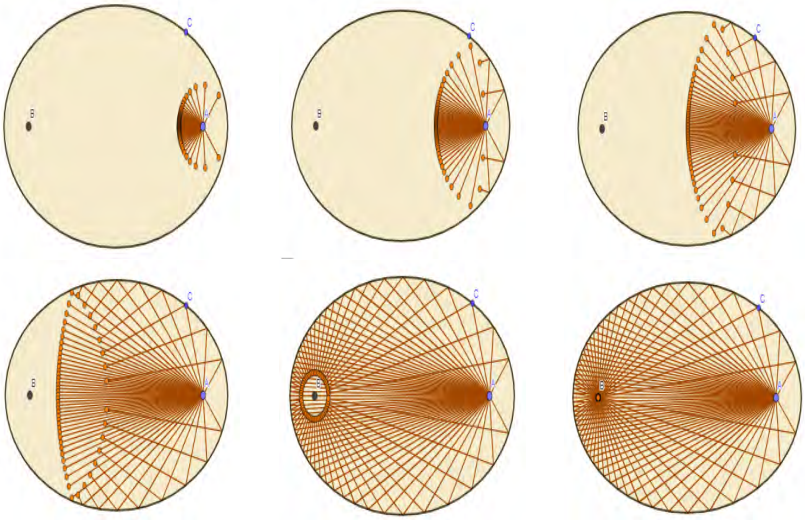
Para simular essa propriedade refletora da elipse, utilizamos folhas de isopor de 10 *mm*, folhas de papel laminado e laser.

Utilizando o molde, desenhamos uma mesma elipse em cinco folhas de isopor. Retiramos a parte interna da elipse e colamos as placas umas sobre as outras. Em seguida, esse bloco foi colado em uma folha inteira de isopor formando uma cavidade com borda elíptica. Nessa base, marcamos os focos e a borda foi toda revestida de papel laminado. O laser foi posicionado horizontalmente em um dos focos de maneira que o feixe de luz refletisse na borda da elipse. Verificamos que, independente da direção para onde se apontava o laser, o feixe de luz refletido sempre passava pelo outro foco. Conforme ilustrado na Figura 8.13.

Figura 8.13: Experimento de reflexão numa superfície refletora elíptica

Elaborado pela autora.

Figura 8.14: Esquema de reflexão dos raios de luz no experimento da Figura 8.13



Bortolossi (2020).

(ii) **Propriedade refletora da parábola**

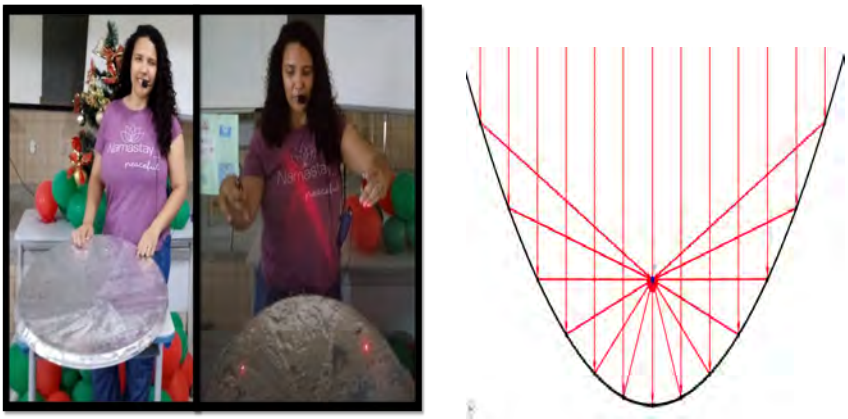
A propriedade refletora da parábola é muito utilizada, dentre outras áreas, em construções como em conchas acústicas, cujo objetivo é direcionar melhor o som para a plateia localizada a sua frente. Essa atividade propõe a construção de um modelo concreto que mostre a aplicação dessa propriedade em uma superfície parabólica, como ocorre em antenas de televisão, por exemplo.

Para simular essa propriedade refletora da parábola, utilizamos uma antena parabólica que seria descartada no lixo, papel alumínio, dois lasers e desodorante aerossol.

Cobrimos a superfície côncava da antena com papel alumínio tomando cuidado de evitar ao máximo formar bolhas. Em um ambiente com pouca luz, direcionamos os lasers à essa superfície da antena de modo que os raios de luz fossem paralelos ao eixo de simetria do paraboloide. Para tornar os raios dos lasers mais nítidos, borrifamos desodorante aerossol no ar ao longo do trajeto da luz.

Após repetir esse procedimento em vários pontos do paraboloide, verificamos que os raios sempre se cruzavam em um determinado ponto (foco das parábolas).

Figura 8.15: Experimento de reflexão numa superfície refletora parabólica



Elaborado pela autora.

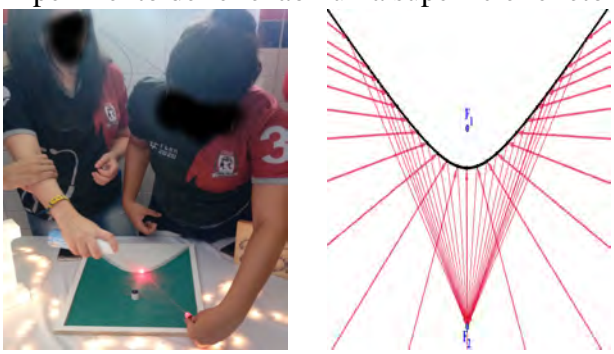
(iii) **Propriedade refletora da hipérbole**

A hipérbole possui uma propriedade refletora que é utilizada, por exemplo, em telescópios refletores como o Hubble. Nessa atividade, propomos a construção de um modelo concreto que mostre a aplicação dessa propriedade em um "bilhar hiperbólico".

Para simular essa propriedade refletora da hipérbole, construímos um modelo de bilhar hiperbólico em MDF no qual uma das bordas possui o formato de um ramo de hipérbole e a caçapa se localiza no ponto focal externo a esse ramo. Na borda da mesa cujo formato é hiperbólico, inserimos uma placa de fórmica para refletir a luz.

Posicionamos um laser horizontalmente sobre a mesa de maneira que a luz refletisse na borda na direção do foco interno à hipérbole. Verificamos que independente da posição de onde o laser emitisse a luz, ela sempre passava pela caçapa (outro foco), conforme ilustrado na Figura 8.16.

Figura 8.16: Experimento de reflexão numa superfície refletora hiperbólica



Elaborado pela autora.

8.2.1.5 Atividade 5: Visita ao museu interativo de ciência de Pernambuco – Espaço Ciência (Duração: 4 aulas).

A última atividade lúdica proposta foi a visita ao Espaço Ciência que possui, em seu acervo de exposições na área de percepção, algumas aplicações das propriedades refletoras das cônicas. Os alunos assistiram a apresentação dos experimentos e os manipularam. Após a visita, eles escreveram relatórios sobre suas observações.

Nessa visita ao Espaço Ciência, os alunos puderam manipular experimentos que exploram as propriedades refletoras das cônicas, especificamente as da parábola, como o fogão solar e o paraboloide de revolução. A seguir, foram descritos superficialmente esses dois experimentos.

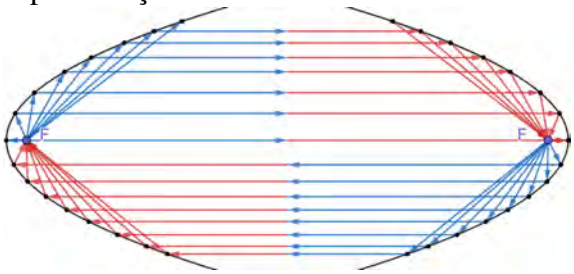
No Paraboloide de Revolução (Orelhão Parabólico), há dois paraboloides com eixos focais paralelos ao solo e com suas superfícies côncavas de frente uma para a outra, a cerca de 20 metros de distância um do outro. Uma pessoa, ao se sentar no local indicado, posiciona sua boca aproximadamente no foco do paraboloide a sua frente. Ao falar, as ondas sonoras colidem no paraboloide e refletem em trajetória retilínea no sentido paralelo ao seu eixo focal em direção ao outro paraboloide. Se não houver obstáculos relevantes nesse trajeto, as ondas sonoras chegam à superfície côncava desse outro paraboloide e reverberam na direção do seu foco onde, se houver uma segunda pessoa, a mensagem inicial será recebida. Veja o esquema da Figura

Figura 8.17: Visita ao Espaço Ciência em Olinda - PE

Elaborado pela autora.

8.18.

Figura 8.18: Representação do funcionamento de um orelhão parabólico



Elaborado pela autora.

Já o fogão solar funciona da seguinte forma: os raios solares incidem paralelamente ao eixo focal de um paraboloide cuja superfície côncava (que recebe os raios solares) é revestida por um material refletor. Ao tocar essa superfície refletora do paraboloide, os raios são refletidos em linha reta na direção do foco onde se localiza convenientemente uma grelha que fica

superaquecida em função da concentração dos raios solares nesse ponto, tornando possível o preparo de alimentos. Para melhor compreensão, veja a Figura 8.19.

Figura 8.19: Representação do funcionamento de um fogão solar parabólico

Garcia, Pappalardo e Beozzo (2013).

Essa atividade estimula o aprendizado tanto de matemática quanto de outras ciências exatas, visto que os alunos visitaram experimentos científicos relativos também à outras ciências, além de exercitar a observação e escrita científicas.

8.3 Considerações finais

A matemática é, sem dúvida, uma ciência abstrata, entretanto, isso não implica que ela seja considerada chata ou incompreensível. Para que essa ciência se aproxime mais da realidade dos alunos, é válido que o professor utilize métodos de ensino divertidos e com aplicações práticas.

É de conhecimento geral as várias dificuldades que um professor de escola pública passa e o quanto ele tem que se desdobrar dentro e fora da sala de aula para atingir o objetivo de fazer com que seus alunos aprendam. Contribuir com o trabalho docente para promover o aprendizado acerca das cônicas foram os principais objetivos dessa pesquisa.

Nesse sentido, o propósito deste trabalho foi atingido, visto que foi

apresentada uma aplicação de sequência didática para o ensino das cônicas baseada na ludicidade, que obteve resultados satisfatórios. Nela, os estudantes demonstraram compreender a definição dos elementos determinantes das cônicas e indicá-los algébrica e geometricamente. Além de construírem modelos concretos que representem as cônicas e suas propriedades refletoras, esses modelos foram apresentados na II Feira de Matemática da EREM Aníbal Falcão no ano de 2019.

Registramos, a seguir, as percepções da professora acerca das respostas e indagações durante o processo de aplicação da sequência didática bem como o acompanhamento das construções geométricas nas atividades lúdicas e da receptividade dos alunos, que construíram modelos, realizaram experimentos e visitaram um museu de ciência. No primeiro experimento da lanterna (atividade 8.2.1.1), simulou-se as secções de um plano em um cone. Todos os alunos conseguiram associar as figuras formadas na parede com suas respectivas curvas.

Na atividade 8.2.1.2, foram trabalhadas as definições e os elementos de cada curva. Segundo os alunos, ficou mais fácil compreender a relação da figura com a sua respectiva definição como L.G.

Na atividade 8.2.1.3, os alunos exercitaram tanto as habilidades referentes à área de Geometria como desenvolveram seu lado artístico e produziram várias cônicas usando dobraduras.

A atividade 8.2.1.4 foi a que mais empolgou os alunos, devido à aplicação prática das propriedades refletoras utilizando luzes. Além do interesse dos alunos em estudar matemática, nessa atividade, foi reforçada a identificação dos elementos das cônicas, como focos e eixos. Pensamos na aplicação da atividade 8.2.1.5 para que os alunos desenvolvessem competências como a observação científica e a conversão entre a linguagem visual e a escrita.

Em geral, o resultado da aplicação dessas atividades lúdicas foram alunos mais interessados em assistir e participar das aulas de matemática, além de demonstrarem maior compreensão sobre o assunto quando indagados acerca do formato, dos elementos e das propriedades refletoras das cônicas. Essa sequência didática foi publicada nos Anais do VI CONEDU - Congresso Nacional de Educação (NASCIMENTO, 2018) e apresentada oral e

visualmente nesse evento na modalidade *banner* e recebeu muitos *feedbacks* positivos dos professores, elogiando as atividades lúdicas desenvolvidas em sala de aula e demonstrando interesse em desenvolver essa sequência didática com seus alunos. Portanto, dados os resultados obtidos, esperamos que esse trabalho inspire mais professores de matemática a aplicarem, em suas aulas, a proposta apresentada.

8.4 Referências bibliográficas

BORTOLOSSI, H. Bilhar na Elipse. **GeoGebra**, 2020. Disponível em:<https://www.geogebra.org/m/dkwzwa5m>. Acesso em: 10 mai. 2020.

BRASIL.**Base Nacional Comum Curricular.** Brasília: Ministério de Educação, 2018. Disponível em: <http://basenacionalcomum.mec.gov.br/wpcontent/uploads/2018/12/BNCC_19dez2018_site.pdf>. Acesso em: 08 fev. de 2019.

CREATIVE LEARNING. **Conic Section and 3d Animation**. 2015. 5 min, son., color. Disponível em: <https://youtube/HO2zAU3Eppo>. Acesso em: 08 ago. 2019.

EVANGELISTA, J. et al. Matemática Lúdica Ensino Fundamental e Médio. **Educação em Foco**, Amparo, n. 6, p. 26-36, 2013.

GARCIA, B.; PAPPALARDO, J.; BEOZZO, R. Fogão Solar Parabólico. **UNESP**, 2013. Disponível em: <https://www.sorocaba.unesp.br/Home/Extensao/Engenhocas/esquilotelefonico.pdf>. Acesso em: 12 mai. 2020.

MOREIRA, J. **Construções das cônicas utilizando o desenho geométrico e instrumentos concreto**. 2017. Dissertação (Mestrado) – Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Matemática, Rio de Janeiro.

NASCIMENTO, K. **Luz, Cônicas, Reflexão: uma sequência didática para o ensino das cônicas**. 2020. Dissertação (Mestrado) - Universidade Federal Rural de Pernambuco, Programa de Mestrado Profissional em

Matemática (PROFMAT), Recife.
NASCIMENTO, K. Luz, Cônicas, Reflexão: uma sequência didática para o ensino das cônicas. In VI CONGRESSO NACIONAL DE EDUCAÇÃO – CONEDU, 2018, Fortaleza. **Anais**... Fortaleza: Editora Realize, 2018.
PERETTI, L.; TONIN DA COSTA, G. Sequência Didática na Matemática. **Revista de Educação do IDEAU**, Caxias do Sul, v. 8, n. 17, 2013.
PERNAMBUCO. **Conteúdos de Matemática por Bimestre para o Ensino Médio:** com base no parâmetros curriculares do estado de Pernambuco. Recife: Secretaria de Educação e Esportes de Pernambuco, 2013.
RODRIGUES, B. **Construção da Elipse através do Origami**. 2015. 2 min, son., color. Disponível em: <https://youtube/RNMrDGKYbxw>. Acesso em: 08 ago. 2019.
RODRIGUES, B. **Construção da Hipérbole através do Origami**. 2015. 2 min, son., color. Disponível em: <https://youtube/p8pRw9RIrWY>. Acesso em: 08 ago. 2019.
RODRIGUES, B. **Construção da Parábola através do Origami**. 2015. 2 min, son., color. Disponível em: <https://youtube/GEvgDMBLRDQ>. Acesso em: 08 ago. 2019.
SILVA, F. et al. O uso de material concreto no ensino da matemática. In: VIII FORUM INTERNACIONAL DE PEDAGOGIA, 2016, São Luís. **Anais**... São Luís: UFMA, 2016.
TENANIN, L.; SILVEIRA, C.; URIBE, E. Ensino de cônicas e a arte das dobraduras. **Colloquium Exactarum**, vol. 8, n. Especial, Jul–Dez, 2016.
ZABALA, A. **A prática educativa:** como ensinar. Porto Alegre: Penso Editora, 2015.

TESTE

AS CÔNICAS E SUAS PROPRIEDADES REFLETORAS

ALUNO(A):

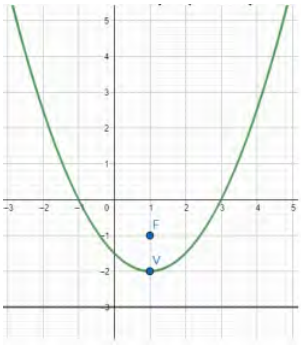
---

1. Que local geométrico é definido como:

   a) O conjunto de todos os pontos em um plano cuja soma das distâncias a dois pontos fixos, denominados focos (F_1 e F_2), é constante e maior que a distância entre os focos?

   b) O conjunto de pontos em um plano cuja distância a um ponto fixo F é sempre igual à distância a uma reta dada?

2. Escreva a equação da parábola representada:



3. Construa uma elipse cuja excentricidade, $\frac{a}{c}$, seja igual a 0.8 e centro C na origem. (Obs.: Deve-se estar indicado os locais dos focos, centro e extremidades dos eixos)

4. Esboce o gráfico de uma hipérbole cujo eixo real mede 8 *cm*, eixo imaginário mede 6 *cm* e centro $C(1,2)$. (Obs.: Deve-se estar indicado os locais dos focos, centro e extremidades dos eixos)

5. Esboce o gráfico de uma parábola cuja concavidade esteja voltada para a esquerda, coordenadas do vértice $V(5,1)$ e de parâmetro 2. (Obs.: Deve-se estar indicado os locais do foco F, vértice V e da reta diretriz d.)

6. A fotografia abaixo reproduz um abajur e a sombra que ele projeta na parede. Que curvas são essas?

7. Uma das aplicações das propriedades refletoras das cônicas é o aparelho iluminador que os dentistas usam em suas consultas. Nele, o dentista necessita que a iluminação seja concentrada em um único ponto, o dente do paciente, e isso é facilmente alcançado quando se tem um espelho de certo formato e a lâmpada fixada em um determinado ponto fixo, interior em relação a curva formada pelo espelho. Quando o dentista movimenta o seu dispositivo, e consegue colocar a iluminação exatamente no dente a ser trabalhado, este se encontra em um ponto estratégico. Veja a foto abaixo:

Acerca da situação descrita, responda:

a) Que formato deverá ter esse espelho para que o seu propósito seja atingido?

b) Em que lugar geométrico relativo à curva essa lâmpada estará?

c) E o dente iluminado?

8. Uma concha acústica é um equipamento cênico,usado em diversos eventos musicais e que está disposto à volta da orquestra e aberto para a plateia. Qual é a vantagem de se construir uma concha acústica com formato parabólico (como no exemplo mostrado na figura abaixo), cujo palco esteja situado no foco dessa curva?

Capítulo 9

A utilização de problemas matemáticos em aberto no ensino médio

Me. Rui de Andrade Lima[1]
Dr. Marcelo Pedro dos Santos[2]

Resumo: Em matemática, um problema em aberto é uma questão não resolvida. A utilização de problemas em aberto incentiva o uso de atividades investigativas fundamentais para a construção do conhecimento, mas está ausente no ambiente escolar, acarretando prejuízos na formação dos estudantes. O ensino por meio da investigação matemática promove o desenvolvimento do raciocínio e a autonomia do estudante, atribuindo novos significados aos objetos de conhecimento e dando a oportunidade de se aprender matemática fazendo matemática. Esse texto é baseado em (LIMA, 2018) e visa apontar a importância da utilização de problemas matemáticos em aberto no Ensino Médio, quebrando a concepção de estudantes desse nível escolar de que todos os problemas matemáticos têm solução. Assim, realizamos uma pesquisa de problemas matemáticos em aberto acessíveis ao

[1]Colégio Damas, professorruilima@gmail.com
[2]Universidade Federal Rural de Pernambuco, marcelo.pedrosantos@ufrpe.br

estudante do Ensino Médio, com desenvolvimento de conteúdos necessários à compreensão dos problemas pesquisados, abrangendo a Teoria dos Números, com vários resultados sobre números primos, a Análise Combinatória, com tópicos sobre quadrados mágicos, e a Geometria. O trabalho apresenta sugestões de atividades que relacionam conteúdos matemáticos do Ensino Médio com problemas em aberto, para professores utilizarem em sala de aula.

Palavras-chave: Problemas em aberto; Investigação matemática; Números Primos; Combinatória; Geometria.

9.1 Introdução

O objetivo deste trabalho é apontar a importância da utilização de problemas matemáticos em aberto no Ensino Médio, quebrando a concepção de alunos do ensino básico de que todos os problemas matemáticos têm solução; desenvolvendo no aluno o poder de duvidar, fundamental na formação do pensamento crítico; promovendo a investigação matemática e aproximando a matemática ensinada nas escolas de Ensino Médio das pesquisas feitas nos centros universitários. Sobre a importância da pesquisa matemática, D'Ambrosio destaca que:

> Assim como no processo de construção da Matemática como disciplina, a essência do processo é a pesquisa, na construção do conhecimento para cada aluno, a essência do processo tem que ser a pesquisa. Dificilmente o aluno de Matemática testemunha a ação do verdadeiro matemático no processo de identificação e solução de problemas. O professor faz questão de preparar todos os problemas a serem apresentados com antecedência; consequentemente, o legítimo ato de pensar matematicamente é escondido do aluno, e o único a conhecer a dinâmica desse processo continua sendo o professor. O professor, com isso, guarda para si a emoção da descoberta de uma solução fascinante, da descoberta de um caminho produtivo, das frustrações inerentes ao problema considerado

> e de como um matemático toma decisões que facilitam a solução do problema proposto. O que o aluno testemunha é uma solução bonita, eficiente, sem obstáculos e sem dúvidas, dando-lhe a impressão de que ele também conseguirá resolver problemas matemáticos com tal elegância. (D'AMBROSIO, 1993, p. 36).

Definição 1. *Um **problema matemático em aberto** é uma questão não resolvida, ou seja, uma questão em que a solução não foi encontrada ou não se provou que a questão não tem solução.*

Os problemas em aberto podem despertar o interesse do aluno pela investigação matemática, pois existem problemas que são fáceis de enunciar, mas cujas soluções ainda não foram encontradas e que despertam um fascínio especial. Um problema desse tipo é a Conjectura de Collatz (1910 - 1990) ou Problema $3n+1$, cujo enunciado é:

Problema 1 (Conjectura de Collatz)**.** *Dado um número natural, n, executando-se os seguintes passos:*

$$\begin{aligned} &\textit{i) Se n for par, o seu sucessor será } \frac{n}{2}; \\ &\textit{ii) Se n for ímpar, o seu sucessor será igual a } 3n+1. \end{aligned}$$

e repetindo-se esse processo, o número 1 é sempre obtido?

Por exemplo, começando com o número 3, obtém-se:

$$3 \to 10 \to 5 \to 16 \to 8 \to 4 \to 2 \to 1$$

A conjectura de Collatz é um problema matemático em aberto com enunciado acessível ao estudante da educação básica e já testado para

milhares de números com uso de supercomputadores sempre atingindo o número 1, mas ela ainda não foi provada matematicamente.

Acredita-se que a solução da conjectura de Collatz abrirá novos caminhos para a matemática e o seu poder em motivar alunos à pesquisa matemática pode ser constatado nas palavras do matemático Derek Jennings

> outra razão é que, por ser fácil de apresentar e entender, tem potencial de atrair jovens para a matemática. Eu mesmo soube de sua existência no Ensino Médio e não resisti ao seu encanto (BBC BRASIL, 2016).

O uso de problemas em aberto no ensino da matemática é fundamental para criar um ambiente interativo entre o aluno e o professor e proporcionar o aprendizado por meio da investigação, permitindo a construção de um conhecimento mais sólido. Assim, é contraditório o professor de matemática não apresentar problemas em aberto aos seus alunos, como destaca Sacristán

> Penso que o mais importante é a dicotomia entre as atividades de ensinar e aprender, introduzida artificialmente por uma prática escolar inadequada. O pesquisador /professor aprende principalmente investigando, mas, no momento em que entra na sala de aula, esquece que o estudante, para aprender, precisa investigar. Assim separa as duas atividades, pois não percebeu que são interligadas, ou por que não se interessa em aprender a utilizar métodos adequados para conectá-las. Outros motivos também se fazem presentes, como a ideia de que a investigação é reservada a um grupo especial de pessoas, assim como a ideia de que a descoberta só é importante quando alguém a faz pela primeira vez conforme os registros acadêmicos. Ocorre também, por parte dos professores, o receio de se depararem, durante a aula, com problemas cuja resposta não conhecem de imediato. Com essa concepção se perde a motivação pedagógica da descoberta e se reduz o ensino à transmissão do produto

> histórico da investigação, perdendo-se o valor da compreensão do processo de produção desse conhecimento (SACRISTÁN, 1998, p. 60).

Apesar do uso de atividades investigativas se mostrar relevante para o aprendizado em matemática, está ausente no cotidiano escolar da educação básica, o que não acontece no ensino superior com os projetos de iniciação científica, que incentivam os estudantes de graduação à pesquisa. Assim, o propósito deste trabalho se concentra na investigação de problemas matemáticos em aberto e na formulação de estratégias para apresentá-los aos alunos do Ensino Médio.

9.2 Fundamentos teóricos e metodológicos

9.2.1 Problemas em aberto de teoria dos números

Os números primos guardam muitos segredos e mistérios que podem estimular o estudante da educação básica a refletir sobre a Teoria dos Números e suas aplicações, estimulando o pensamento crítico e a construção de ideias que fomentem a pesquisa e, consequentemente, estimulem o aluno a aprender matemática, como destaca Abramo Hefez

> Esses números desempenham papel fundamental e a eles estão associados muitos problemas famosos cujas soluções têm resistido aos esforços de várias gerações de matemáticos (HEFEZ, 2016, p.122)

9.2.1.1 Os Números primos

Entre os números naturais, existem números que funcionam como blocos básicos que permitem a construção de todos os números naturais maiores que 1 pela multiplicação, ou seja, existem números primitivos que não podem ser gerados pela multiplicação de outros números, como 2, 3 e 5, e outros números secundários, gerados a partir da multiplicação de números primitivos, como o $6 = 2 \cdot 3$ e o $10 = 2 \cdot 5$.

Definição 2. *Um número natural p maior que 1 é **primo** se possui como divisores apenas 1 e ele próprio, ou seja, 1 e p.*

Por exemplo, 5 é primo.

Definição 3. *Um número natural n maior que 1 que não é primo é dito **composto** e pode ser expresso como produto de dois naturais n_1 e n_2, tais que $1 < n_1, n_2 < n$, ou seja, $n = n_1 n_2$.*

Por exemplo, 12 é composto, pois $12 = 4 \cdot 3$.

9.2.1.1.1 Números primos em progressão aritmética

Nesta seção, abordaremos a distribuição dos números primos e, especificamente, resultados sobre sequência de números primos em progressão aritmética. Para uma análise mais detalhada desse tema, o leitor pode consultar o artigo "Recorrências, progressões aritméticas e teoria ergódica: teoremas de van der Waerden e de Green-Tao", de Peixe e Buescu, indicado nas referências.

Definição 4. *Uma progressão aritmética, denotada por **PA**, é toda sequência numérica em que cada termo, a partir do segundo, é igual ao anterior somado de uma constante r chamada razão da **PA**.*

Por exemplo, a sequência $(2,5,8,11,\ldots)$ é uma **PA** com primeiro termo $a_1 = 2$ e razão $r = 3$.

Um termo qualquer de uma ***PA***, com primeiro termo a_1 e razão r, é dado por $a_1 + (n-1) \cdot r$, para todo n natural. Assim, a sequência formada pelos números da forma $6n + 5 = 11 + (n-1) \cdot 6$ é uma progressão aritmética e nessa progressão é possível encontrar infinitos primos. De fato, esse é um caso particular do teorema a seguir, que foi demonstrado por Dirichlet (1805 - 1859).

Teorema 1 (Dirichlet)**.** *Se a e b são números naturais primos entre si, então a progressão aritmética*

$$a, a+b, a+2b, a+3b, \ldots$$

possui infinitos números primos.

Ao encontrar progressões aritméticas com infinitos termos primos, por exemplo $6n+5$, com n natural, cujos termos são $11, 17, 23, 29, 35, 41, \ldots$, observe-se que, apesar da progressão ter infinitos números primos, nem todos os seus termos são primos, como, por exemplo, $35 = 6 \cdot 5 + 5$. Existe uma busca por progressões aritméticas formadas somente por números primos, a sequência 3, 5 e 7, por exemplo, é uma progressão aritmética formada só por três números primos e as maiores já encontradas contém 26 primos (ANDERSEN, 2017). Em 2016, Takeshi Nakamura encontrou uma dessas progressões aritméticas dada por

$$149836681069944461 + 7725290 \cdot P \cdot n$$

sendo $P = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot 23 = 223092870$ e n inteiro tal que $0 \leq n \leq 25$.

Sobre progressões aritméticas formadas apenas por números primos, destacamos os seguintes resultados:

Teorema 2. *Não existe progressão aritmética formada por três ou mais números primos distintos cujo primeiro termo é 2 ou cuja razão é um número ímpar.*

Demonstração. : O primeiro termo a_1 da ***PA*** não pode ser 2, senão a ***PA***$(2, 2+r, 2+2r, \ldots)$ teria pelo menos dois dos três primeiros termos números primos pares, o que é um absurdo, pois 2 é o único primo par. Então, a_1 é primo ímpar e a razão r da ***PA***$(a_1, a_1+r, a_1+2r, \ldots)$ não pode ser ímpar, senão teria o segundo termo $a_1 + r$ primo par, outro absurdo. □

Teorema 3 (Teorema de Corput)**.** *Existe uma infinidade de progressões aritméticas formadas por três números primos.*

Por exemplo, $(3, 11, 19)$, $(5, 11, 17)$, $(7, 19, 31)$ e $(11, 29, 47)$.

Teorema 4 (Teorema de Green e Tao)**.** *Dado um número natural n qualquer, existem primos $p_1, p_2, \ldots, p_n$ tais que*

$$p_{i+1} - p_i = p_i - p_{i-1},$$

para todo i natural tal que $2 \leq i \leq n-1$.

Em outras palavras, Green e Tao (2008) provaram a existência de progressões aritméticas só formadas por números primos de tamanhos arbitrários. Sobre progressões aritméticas infinitas, o resultado a seguir mostra que não é possível elas possuírem apenas números primos.

Teorema 5. *Não existe uma progressão aritmética com infinitos termos formada apenas por números primos.*

Demonstração. Seja a progressão

$$a, a+b, a+2b, a+3b, \ldots,$$

Suponha, por absurdo, que $a+nb = p$, onde p é primo para todo n natural. Se colocarmos $N = n+kp$, k natural, temos:

$$a+Nb = a+(n+kp)b = a+nb+kpb = p+kpb = p(1+kb)$$

então, $a+Nb$ é divisível por p e, consequentemente, não é primo, o que é um absurdo. □

Sobre progressões aritméticas formadas por números primos, existem as seguintes questões não resolvidas:

Problema 2. *Existem infinitas progressões aritméticas formada por três números primos distintos cujo primeiro termo é 3?*

Em 1939, Van der Corput (1890-1975) provou o **Teorema 3** sobre a existência de infinitas progressões aritméticas de 3 primos, mas não necessariamente iniciadas pelo número 3. Várias progressões aritméticas iniciadas por 3 são conhecidas, mas não se sabe se há uma infinidade delas. Por exemplo, $(3,5,7)$, $(3,11,19)$, $(3,13,23)$, $(3,17,31)$, $(3,23,43)$, $(3,31,49)$, $(3,37,71)$.

Problema 3. *Existem sequências arbitrariamente longas de números primos consecutivos em progressão aritmética?*

Em 1967, Lander e Parkin encontraram a primeira sequência de 6 primos consecutivos em ***PA***, com primeiro termo 121174811 e razão 30. A maior sequência já encontrada possui 10 números primos consecutivos em uma ***PA*** cujo primeiro termo é um número de 93 algarismos e razão 210 (DUBNER et al, 2001).

9.2.2 Problemas em aberto de combinatória

Este assunto é importante para desenvolver no aluno a sua capacidade de raciocínio.

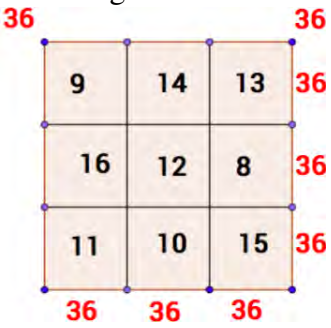
> Embora a Análise Combinatória disponha de técnicas gerais que permitem atacar certos tipos de problemas, é verdade que a solução de um problema combinatório exige quase sempre engenhosidade e a compreensão plena da situação descrita pelo problema. Esse é um dos encantos desta parte da Matemática, em que problemas fáceis de enunciar revelam-se por vezes difíceis, exigindo uma alta dose de criatividade para sua solução. [...] Se a aprendizagem destes conceitos se faz de maneira mecânica, limitando-se a empregá-los em situações padronizadas, sem procurar habituar o aluno com a análise cuidadosa de cada problema, cria-se a impressão de que a Análise Combinatória é somente um jogo de fórmulas complicadas (MORGADO, 1991, p. 3).

9.2.2.1 Quadrados mágicos

Nesta seção, abordaremos os quadrados mágicos que representam uma excelente ferramenta de aprendizagem capaz de desenvolver habilidades em relação à utilização de operações matemáticas.

Definição 5. *Um **quadrado mágico** de ordem n, para todo n natural maior que 2, é uma tabela quadrada de números naturais distintos composta de n linhas e n colunas, tais que a soma de qualquer linha, coluna e diagonal dá sempre o mesmo valor k, chamado constante mágica.*

Figura 9.1: Quadrado mágico de ordem 3 com $k = 36$



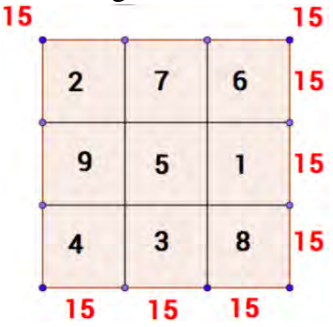
Fonte: Elaborada pelo autor.

Se os n^2 números do quadrado mágico de ordem n estão sequenciados de 1 a n^2, a soma S de todos os números do quadrado mágico de ordem n pode ser encontrada usando a soma dos i primeiros termos de uma progressão aritmética. Então:

$$S = 1+2+\cdots+n^2 = \left(\frac{a_1+a_i}{2}\right)\cdot i = \left(\frac{1+n^2}{2}\right)\cdot n^2,$$

e a constante mágica k, soma de cada linha, coluna ou diagonal, é $k = \frac{S}{n}$, ou seja, $k = \left(\frac{1+n^2}{2}\right)\cdot n$. Por exemplo, num quadrado mágico de ordem 3 numerado de 1 a 9 a constante mágica é $k = \left(\frac{1+3^2}{2}\right)\cdot 3 = 15$.

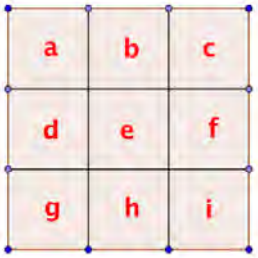
Figura 9.2: Quadrado mágico de ordem 3 com $k = 15$



Fonte: Elaborada pelo autor.

Propriedades dos quadrados mágicos de ordem 3, numerados de 1 a 9: Considerando o seguinte quadrado mágico, temos:

Figura 9.3: Quadrado mágico de ordem 3 genérico



Fonte: Elaborada pelo autor.

1. O termo central é sempre igual a 5;

   Observe que $a+b+c=15$ e $g+h+i=15$. Somando essas duas equações, temos:

   $$a+b+c+g+h+i=15+15$$

   $$(a+i)+(c+g)+(b+h)=30,$$

   mas

   $$a+i=c+g=b+h=15-e,$$

   portanto

   $$15-e+15-e+15-e=30$$

   $$45-3e=30$$

   $$e=5.$$

2. Os cantos são sempre números pares.
   Supondo, por absurdo, que os cantos são os ímpares 1, 3, 7 e 9, devemos colocar nos cantos opostos números que somem 10.

Figura 9.4: Cantos do quadrado mágico de ordem 3

Fonte: Elaborada pelo autor.

Então, teríamos uma linha ou coluna com os números 1 e 3, o que é um absurdo, pois o maior valor que dispomos é 9 e $1+3+9=13$, que é menor que a constante mágica 15. Além disso, os cantos opostos não podem ter paridades distintas, visto que a soma deles seria ímpar e, quando somada ao termo central que é ímpar e igual a 5, seria par, ou seja, a constante mágica seria diferente de 15. Assim, temos a seguinte solução para um quadrado mágico de ordem 3 com números sequenciados de 1 a 9.

Figura 9.5: Quadrado mágico de ordem 3 numerado de 1 a 9

Fonte: Elaborada pelo autor.

Usando os números naturais consecutivos $1,2,\ldots,n^2$ para preencher um quadrado mágico de ordem n, existem precisamente:

- Um único quadrado mágico de ordem 3;
- 880 quadrados mágicos de ordem 4;
- 275.305.224 quadrados mágicos de ordem 5;

Não se sabe o número exato de quadrados mágicos de ordem 6, mas foi estimado que seja da ordem de 10^{19} (STEWART, 2009). O cálculo da quantidade de quadrados mágicos apresenta o seguinte problema não resolvido:

Problema 4. *Qual a quantidade de quadrados mágicos de ordem n diferentes, para todo n natural maior que 5?*

9.2.3 Quadrados mágicos de quadrados perfeitos

Existem quadrados mágicos em que todos os seus números são quadrados de números naturais, ou seja, quadrados perfeitos, e o primeiro deles, de ordem 4, foi encontrado por Leonhard Euler em 1770 (BOYER, 2005).

Figura 9.6: Quadrado mágico de Euler de quadrados perfeitos de ordem 4

68^2	29^2	41^2	37^2
17^2	31^2	79^2	32^2
59^2	28^2	23^2	61^2
11^2	77^2	8^2	49^2

Fonte: Euler's Magic Square (2016).

Problema 5. *Encontrar um quadrado mágico de quadrados perfeitos de ordem 3.*

Esse problema foi proposto pelo matemático Édouard Lucas em 1876 e alguns resultados chegaram perto. Por exemplo, o quadrado encontrado pelo matemático Lee Sallows:

Figura 9.7: Quadrado de quadrados perfeitos de Lee Sallows de ordem 3

127^2	46^2	58^2
2^2	113^2	94^2
74^2	82^2	97^2

Fonte: Boyer (2005).

Observe que esse quadrado tem todas as linhas, colunas e uma diagonal com soma 21.609, mas a diagonal $127^2 + 113^2 + 97^2 = 38.307$, portanto não é mágico. Euler conseguiu encontrar o seguinte quadrado mágico em que apenas dois termos não são quadrados perfeitos:

Figura 9.8: Quadrado mágico de Euler de ordem 3

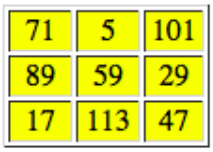
373^2	289^2	565^2
360721	425^2	23^2
205^2	527^2	222121

Fonte: Boyer (2005).

9.2.4 Quadrados mágicos de números primos

O primeiro quadrado mágico de ordem 3 formado apenas por números primos foi encontrado por Sayles em 1913 e possui constante mágica 177 (SHULDHAM, 1914).

Figura 9.9: Quadrado mágico de números primos de Sayles



Fonte: Boyer (c2020).

Considerando a progressão aritmética $(a-4r,\ a-3r,\ a-2r,\ a-r,\ a,\ a+r,\ a+2r,\ a+3r,\ a+4r)$ de 9 termos, com a e r naturais, podemos dispor os seus termos num quadrado mágico de ordem 3 da seguinte forma:

Figura 9.10: Quadrado mágico de ordem 3 de números em PA

Fonte: Elaborada pelo autor.

Em geral, os termos de uma progressão aritmética com n^2 termos podem ser números de um quadrado mágico de ordem n e o **Teorema 4** de Green e Tao, da Subseção 9.2.1.1.1, afirma que existem progressões aritméticas de números primos de tamanhos arbitrários, portanto existem quadrados mágicos de números primos de ordem n, para todo n natural maior que 2. Por exemplo, o quadrado mágico de ordem 3 com números primos em progressão aritmética dada por $210n-11$, com n natural e $1 \leq n \leq 9$.

Figura 9.11: Quadrado mágico de ordem 3 de números primos em PA

Fonte: Elaborada pelo autor.

9.2.4.1 Problemas em aberto de geometria

A Geometria surgiu nas civilizações antigas por meio da experimentação para suprir necessidades cotidianas relacionadas ao plantio, construções e movimento dos astros, sendo usada para cálculo de perímetros, áreas e volumes. Euclides (300 a.C.), em sua obra *Os Elementos*, apresentou a geometria como ciência de natureza lógica e dedutiva, em que cada afirmação deveria ser deduzida de outras mais simples de maneira lógica e sucessiva.

Os problemas geométricos sempre despertaram o interesse das pessoas e os mais marcantes objetivavam construções com uma régua não graduada e um compasso, sendo conhecidos como: "Os três problemas clássicos de Geometria". Eles são:

- a quadratura do círculo: construir um quadrado com área igual ao de um círculo dado;
- a duplicação do cubo: construir um cubo com volume igual ao dobro do volume de um cubo dado;
- a trissecção do ângulo: dividir um ângulo qualquer em três partes com medidas iguais.

A busca pela solução desses problemas promoveu o desenvolvimento da geometria Euclidiana, levando a descobertas, das quais destacamos as

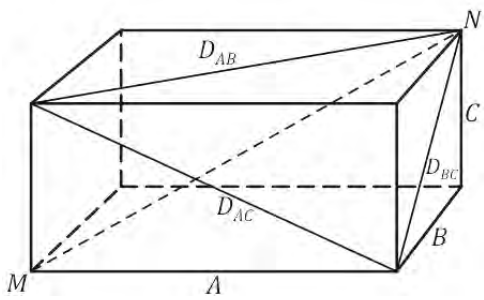
cônicas e curvas cúbicas. Pierre Laurent Wantzel, em 1837, provou a impossibilidade da solução dos três problemas clássicos somente com régua e compasso (BARBOSA; ASSIS NETO, 2011).

Apesar da origem remota, a Geometria Euclidiana não está totalmente pronta e várias questões ainda permanecem sem solução.

9.2.4.2 O Tijolo de Euler

Definição 6. *O **tijolo de Euler** é um paralelepípedo reto-retângulo em que todas as arestas e diagonais das faces têm medidas expressas por números inteiros positivos.*

Figura 9.12: Tijolo de Euler



Fonte: Nascimento (2015).

Encontrar tijolos de Euler é uma aplicação natural de triplas pitagóricas, pois todas as faces do sólido são retângulos e as medidas de suas diagonais são encontradas por meio do teorema de Pitágoras. O menor tijolo de Euler já encontrado tem arestas $A = 240, B = 117$ e $C = 44$, e diagonais das faces $D_{AB} = 267$, $D_{AC} = 244$ e $D_{BC} = 125$, sendo descoberto em 1719, pelo matemático Halcke. Se a diagonal interna do paralelepípedo que não está contida numa das faces também tem como medida um número inteiro, o paralelepípedo diz-se **perfeito**.

Problema 6. *Encontrar um tijolo de Euler perfeito.*

Já foram encontrados alguns paralelepípedos de arestas inteiras com diagonal interna inteira e apenas duas diagonais de suas faces inteiras, sendo considerados paralelepípedos quase perfeitos, por exemplo, o paralelepípedo com arestas $A = 672, B = 153$ e $C = 104$, diagonais das faces $D_{AB} = 3\sqrt{52777}$, $D_{AC} = 680$ e $D_{BC} = 185$ e diagonal interna $D_{ABC} = 697$.

9.2.5 Aplicação em sala de aula

9.2.5.1 Quadrados mágicos e progressões aritméticas

Nesta seção, apresentaremos uma proposta de aplicação das propriedades de progressões aritméticas nos quadrados mágicos.

Tema: Quadrados Mágicos

Objetivos: Estudar propriedades das progressões aritméticas com o uso quadrados mágicos.

Conteúdos Relacionados: Progressão aritmética e matrizes.

Público alvo: Estudantes da segunda série do Ensino Médio.

Metodologia: Aula expositiva apresentando definição e propriedades das progressões aritméticas aplicadas aos quadrados mágicos.

Inicialmente é preciso trabalhar os conteúdos de Progressões Aritméticas e Matrizes, desenvolvendo os seguintes tópicos:

- **Sequência Numérica**: Dado um número natural n, chama-se **sequência numérica finita** toda função dos números naturais menores ou iguais a n nos reais, ou seja, $f : \{1,2,3,4,...,n\} \to \mathbb{R}$ tal que $f(n) = a_n$. Os números $a_1, a_2, ..., a_n$ são chamados de termos da sequência e denota-se a sequência numérica finita por $f = (a_1, a_2, ..., a_n)$, em que as imagens dos números naturais menores

ou iguais a n, pela função $f : \{1,2,3,4,...,n\} \to \mathbb{R}$, aparecem entre parênteses, ordenadamente, da direita para esquerda. Se $f : \mathbb{N} \to \mathbb{R}$, tal que $f(n) = a_n$, a sequência $f = (a_1, a_2, ..., a_n, ...)$ é chamada **numérica infinita**.

- **Progressão Aritmética**: Uma progressão aritmética, denotada por **PA**, é toda sequência numérica em que cada termo, a partir do segundo, é igual ao anterior somado de uma constante r chamada razão da **PA**. Se a sequência numérica que forma a **PA** é finita, a **PA** é finita.

  - **Termo Geral da PA**: Se $(a_1, a_2, \ldots, a_{n-1}, a_n, a_{n+1}, \ldots)$ é uma progressão aritmética de razão r, então o termo de ordem n é dado por $a_n = a_1 + (n-1) \cdot r$, para todo n natural, tal que $n \geq 1$.

  - **Três termos consecutivos de uma PA**: Em toda PA, cada termo, a partir do segundo, é média aritmética entre o antecedente e o consequente.
    Considerando a, b e c, três termos consecutivos de um PA, temos:
    $$b - a = c - b \Rightarrow 2b = a + c \Rightarrow b = \frac{a+c}{2} \blacksquare$$

  - **Termos Equidistantes dos Extremos**: Dois termos de uma sequência finita são **equidistantes dos extremos** quando o número de termos que precede um deles é igual ao número de termos que sucede ao outro. Assim, na sequência:
    $$(\underbrace{a_1, a_2, \ldots, a_i}_{i \text{ termos}}, a_{i+1}, \ldots, a_{n-i}, \underbrace{a_{n-i+1}, \ldots, a_{n-1}, a_n}_{i \text{ termos}})$$
    os termos a_{i+1} e a_{n-i} são equidistantes dos extremos. Observe que dois termos a_k e a_p serão equidistantes dos extremos se $k + p = n + 1$. Por exemplo, a_4 e a_{n-3} são termos equidistantes dos extremos de uma PA de n termos.

Propriedade: Em toda **PA** finita, a soma de dois termos equidistantes dos extremos é igual a soma dos extremos.
Sabemos que os termos a_{i+1} e a_{n-i} são equidistantes dos extremos, aplicando a expressão do termo geral, temos

$$\begin{aligned} a_{i+1} + a_{n-i} &= a_1 + (n-i-1)\cdot r + a_1 + (n-n+i)\cdot r \\ &= a_1 + a_1 + (n-i-1+n-n+i)\cdot r \\ &= a_1 + a_1 + (n-1)\cdot r \\ &= a_1 + a_n. \quad \blacksquare \end{aligned}$$

– **Termo Central de uma PA**: Em toda PA finita, com número ímpar de termos, o termo central é média aritmética dos extremos ou de dois termos equidistantes dos extremos.
Seja uma **PA** com $2n+1$ termos

$$(a_1, a_2, \ldots, a_n, a_{n+1}, a_{n+2}, \ldots, a_{2n}, a_{2n+1})$$

O termo central é a_{n+1}. Note que a_n, a_{n+1} e a_{n+2}

são termos consecutivos da **PA**, portanto

$$a_{n+1} = \frac{a_n + a_{n+2}}{2},$$

como a_n e a_{n+2} são termos equidistantes dos extremos a_1 e a_{2n+1}, temos

$$a_{n+1} = \frac{a_n + a_{n+2}}{2} = \frac{a_1 + a_{2n+1}}{2}.$$

– **Soma dos n primeiros termos de uma PA**: A soma dos n primeiros termos de uma PA é dada por

$$S_n = \left(\frac{a_1 + a_n}{2}\right)\cdot n.$$

Considerando os n primeiros termos de uma PA, podemos escrever

$$\begin{aligned} S_n &= a_1 + a_2 + \cdots + a_{n-1} + a_n. \quad (1) \quad \text{ou} \\ S_n &= a_n + a_{n-1} + \cdots + a_2 + a_1. \quad (2) \end{aligned}$$

Adicionando membro a membro as equações (1) e (2), segue que

$$2 \cdot S_n = (a_1 + a_n) + (a_2 + a_{n-1}) + \cdots + (a_{n-1} + a_2) + (a_n + a_1).$$

O segundo membro da equação acima é composto por parcelas que são somas de termos equidistantes dos extremos, portanto:

$$2 \cdot S_n = (a_1 + a_n) \cdot n \Rightarrow S_n = \left(\frac{a_1 + a_n}{2} \right) \cdot n \ \blacksquare$$

Matriz Quadrada: Uma **matriz quadrada** de ordem n ou $n \times n$ é uma tabela de números dispostos em n linhas e n colunas, onde $a_{i,j}$ representam os elementos que se localizam na linha i e coluna j

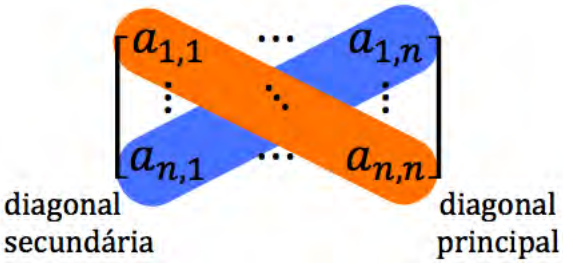
$$A = \begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \cdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{bmatrix}_{n \times n}$$

com $1 \leq i, j \leq n$.

- **Diagonal Principal**: Numa matriz quadrada de ordem n, a **diagonal principal** é formada pelos elementos $a_{i,j}$ tais que $i = j$, ou seja, $a_{1,1}, a_{2,2}, \ldots, a_{n,n}$.

- **Diagonal Secundária**: Numa matriz quadrada de ordem n, a **diagonal secundária** é formada pelos elementos $a_{i,j}$ tais que $i+j=n+1$, ou seja, $a_{1,n}, a_{2,n-1}, \ldots, a_{n,1}$.

Figura 9.13: Diagonais de uma matriz quadrada



Fonte: Elaborada pelo autor.

- **Quadrado Mágico**: Um **quadrado mágico** é uma matriz quadrada de ordem n, com $a_{i,j}$ distintos e $1 \leq i, j \leq n$, onde a soma dos elementos de cada linha, de cada coluna e de cada diagonal é sempre igual a uma constante k, chamada constante mágica.

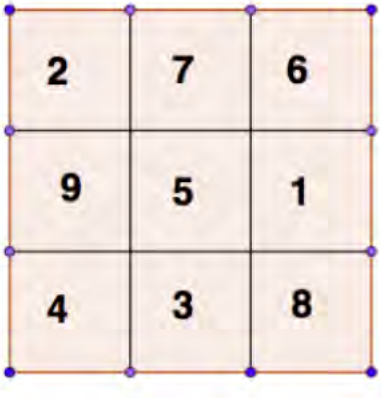
  Após trabalhar os tópicos acima e apresentar a definição de **quadrados mágicos**, mostrar exemplos e propor aos alunos que eles encontrem um quadrado mágico de ordem 3 com números de 1 a 9.

  Na sequência, orientar os alunos para que façam as seguintes transformações em seus quadrados mágicos:

  - **Somar uma constante**: Adicionando uma constante a qualquer a todos os termos do quadrado mágico de ordem 3, numerado de 1 a 9, percebemos que:

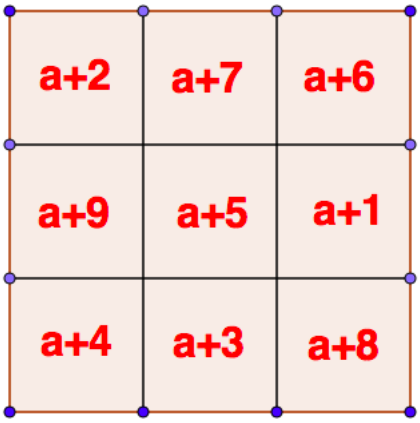
    Qualquer sequência de nove números consecutivos pode ser termos de um quadrado mágico de ordem 3;

Figura 9.14: Quadrado mágico de ordem 3, numerado de 1 a 9



Fonte: Elaborada pelo autor.

Figura 9.15: Quadrado mágico de ordem 3 numerado de a+1 a a+9

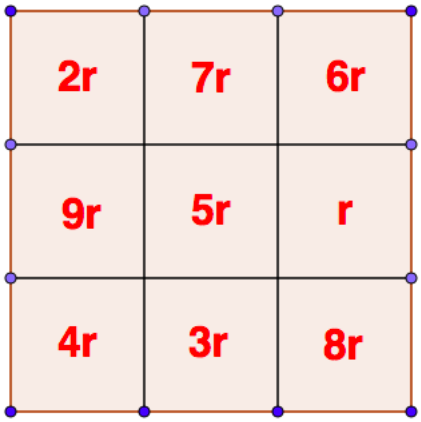


Fonte: Elaborada pelo autor.

– **Multiplicar por uma constante**: Multiplicando por constante s qualquer todos os termos do quadrado mágico de ordem 3, numerado de 1 a 9, percebemos que:

Qualquer sequência de nove múltiplos consecutivos de um número inteiro pode ser termos de um quadrado mágico de ordem 3;

Figura 9.16: Quadrado mágico de ordem 3 numerado de r a $9r$

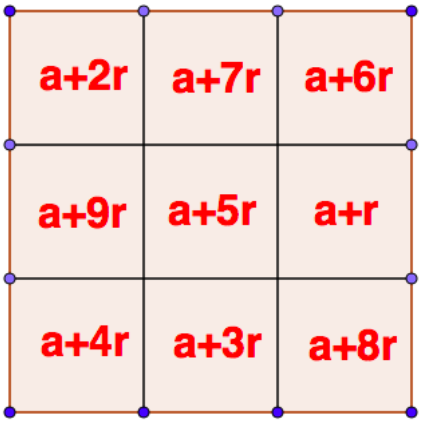


Fonte: Elaborada pelo autor.

– **Multiplicando e somando**: Multiplicando por uma constante r e depois adicionando uma outra constante a a cada um dos termos do quadrado mágico de ordem 3, numerado de 1 a 9, percebemos que:

Qualquer progressão aritmética de nove números pode ser termos de um quadrado mágico de ordem 3 ;

Figura 9.17: Quadrado mágico de ordem 3 numerado de $a+r$ a $a+9r$



Fonte: Elaborada pelo autor.

É possível arranjar termos de progressões aritméticas em quadrados mágicos de ordem maior que 3. Por exemplo, num quadrado mágico de ordem 4, podemos colocar os 16 termos da seguinte progressão aritmética: $(a, a+r, a+2r, \ldots, a+14r, a+15r)$ com a e r naturais, da seguinte forma

Tabela 9.1: Quadrado mágico de ordem 4 com números em *PA*

a	$a+14r$	$a+13r$	$a+3r$	$4a+30r$
$a+11r$	$a+5r$	$a+6r$	$a+8r$	$4a+30r$
$a+7r$	$a+9r$	$a+10r$	$a+4r$	$4a+30r$
$a+12r$	$a+2r$	$a+r$	$a+15r$	$4a+30r$
$4a+30r$	$4a+30r$	$4a+30r$	$4a+30r$	

Fonte: Elaborada pelo autor.

Observe que os 16 termos da progressão aritmética foram arranjados formando um quadrado mágico cuja constante mágica é $4a+30r$.

Existe uma outra relação entre os quadrados mágicos e as progressões aritméticas, como veremos a seguir:

– **A Constante Mágica**: Considerando um quadrado mágico de ordem n, numerado de 1 a n^2,

$$\begin{bmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \cdots & \cdots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{bmatrix}$$

com $1 \leq i, j \leq n$ e $a_{i,j} \in \{1, 2, 3, \ldots, n^2\}$, a soma S de todos os números do quadrado mágico de ordem n pode ser encontrada usando a soma dos i primeiros termos de uma progressão aritmética, então

$$S = 1 + 2 + \ldots + n^2 = \left(\frac{a_1 + a_i}{2}\right) \cdot i = \left(\frac{1 + n^2}{2}\right) \cdot n^2$$

e a constante mágica k, soma de cada linha, coluna ou diagonal, é $k = \frac{S}{n}$, ou seja,

$$k = \left(\frac{1 + n^2}{2}\right) \cdot n.$$

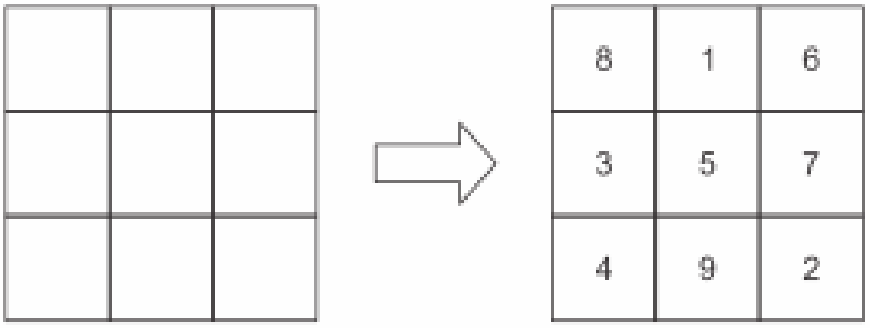
Após trabalhar essas aplicações, o professor pode apresentar aos alunos os problemas em aberto sobre quadrados mágicos da Seção 9.2.2.1, como também propor que procurem quadrados mágicos formados por números primos, o que pode ser feito usando o fato de que progressões aritméticas fornecem números para os quadrados mágicos e o Teorema de Green e Tao, abordado na Subseção 9.2.1.1.1, que garante a existência de progressões aritméticas de números primos de tamanho arbitrário.

Na sequência, sugerimos uma lista de exercícios sobre quadrados mágicos para ser aplicada após trabalhar essa

atividade

Questões Propostas

Questão 1 (Colégio Pedro II - 2017)**.** *O Quadrado Mágico é uma tabela quadrada composta por números inteiros consecutivos a partir do 1, em que a soma de cada coluna, de cada linha e de cada diagonal são iguais. Essa soma é chamada de número mágico.*
Aprenda a encontrar o número mágico de um quadrado 3×3 *como o da figura.*



O quadrado mágico 3×3 *possui 9 posições, portanto deve ser preenchido com os números de 1 até 9 sem repetição.*
O número mágico pode ser encontrado seguindo dois passos.
***Passo 1** – Encontrar a soma total dos números.*

$$1+2+3+4+5+6+7+8+9=45$$

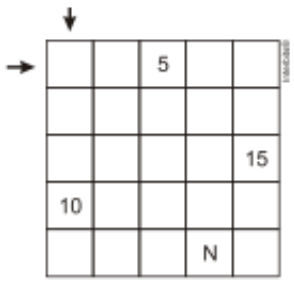
***Passo 2** – Dividir a soma encontrada pelo número de colunas existentes no quadrado. No caso do quadrado mágico* 3×3 *os 9 números estão agrupados em 3 colunas. Logo o número mágico será* $45 : 3 = 15$*. Em condições semelhantes, o número mágico de um quadrado* 4×4 *será*

a) 16.
b) 24.
c) 34.
d) 64.
e) 136.

***Resolução**: Do enunciado, o número mágico de um quadrado* 4×4 *é dado por:*

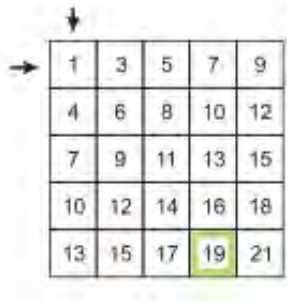
$$\frac{1+2+\cdots+16}{4} = \frac{1}{4} \cdot \left(\frac{1+16}{2}\right) \cdot 16 = 34$$

Questão 2 (UPE - 2012)**.** *O quadrado mágico abaixo foi construído de maneira que os números em cada linha formam uma progressão aritmética de razão x, e, em cada coluna, uma progressão aritmética de razão y, como indicado pelas setas.*



Sendo x e y positivos, qual o valor de N?
a) 14
b) 19
c) 20
d) 23
e) 25

Resolução: Cada linha forma uma progressão aritmética de razão $x = 2$. Cada coluna, uma progressão aritmética de razão $y = 3$. Portanto, temos:



Questão 3 (UFTM - 2012)**.** *O quadrado mágico multiplicativo indicado na figura é composto apenas por números inteiros positivos. Nesse quadrado mágico, o produto dos números de cada linha, de cada coluna e de cada uma das duas diagonais principais dá sempre o mesmo resultado.*

50	2	x
y	10	50
10	z	w

Nas condições dadas, $x+y+z+w$ é igual a
a) 56.
b) 58.
c) 60.
d) 64.
e) 66.

Resolução: Temos que

$100x = 500y = 10zw = 500w = 20z = 50xw \Rightarrow x = 10, y = 2, z = 50$ e $w = 2$

Portanto, $x+y+z = 64$.

Questão 4 (Profmat MA21 - 2015)**.** *Dado $n \in \mathbb{N}$ par, pode existir um quadrado $n \times n$ que é preenchido pelos n^2 primeiros números primos?*

Resolução: A resposta é não, e a razão é uma obstrução de paridade, baseada no fato que 2 é o único primo par. Suponha, por absurdo, que existe um quadrado mágico como estipulado acima. Observe que a linha que contém 2 tem um elemento par e $n-1$ ímpares; como $n-1$ é ímpar, isso quer dizer que a soma dos números na linha é ímpar. Por outro lado, uma linha que não contém 2 tem de ter soma par (estamos somando n números ímpares e n é par!). Mas, então, temos duas linhas com somas distintas, absurdo!

Questão 5 (PUCPR - 2005)**.** *Um quadrado mágico é um arranjo quadrado de números tais que a soma dos números em cada fila (linha ou coluna) e nas duas diagonais é o mesmo. Os nove números $n, n+3, n+6, ..., n+24$, em que n é um número inteiro positivo, podem ser usados para construir um quadrado mágico de três por três.*

A soma dos números de uma fila deste quadrado vale:

a) $3n+6$

b) $3n+36$

c) $3n$

d) $3n+24$

e) $3n+12$

Resolução: Os 9 números $n, n+3, n+6, ..., n+24$ estão em PA cuja soma é S:

$$S = \left(\frac{n+n+24}{2}\right) \cdot 9 = (n+12) \cdot 9$$

e a soma dos elementos de uma fila é

$$\frac{S}{3} = \frac{(n+12) \cdot 9}{3} = 3n+36$$

9.3 Considerações finais

A aplicação de problemas em aberto no Ensino Médio pode motivar os alunos desse nível a aprender matemática, deixando-os surpresos com a possibilidade de entender a afirmação de um problema não resolvido e como problemas com enunciados simples, como a Conjectura de Collatz, não estão resolvidos.

O trabalho mostra que existem vários problemas em aberto cujos enunciados estão no nível da matemática da educação básica, como também afasta dos alunos a mentalidade de que todos os problemas têm respostas conhecidas e que seus professores podem encontrar a resposta a todos os problemas. Apesar de não resolver nenhum dos problemas em aberto, o texto produzido apresenta avanços e soluções parciais para a maioria dos problemas, promovendo um aprofundamento de conteúdos matemáticos da educação básica e acrescentando conteúdos que normalmente não são trabalhados nesse nível escolar.

Em um processo de aprendizagem ativa, o aluno deve ser protagonista de seu aprendizado, em uma relação interativa com o professor, criando uma via de mão dupla em que ambos aprendem e se desenvolvem. É fato que o uso de atividades investigativas proporciona essa aprendizagem ativa, colocando o professor como orientador que ajuda o aluno a ir além do ponto em que conseguiria chegar sozinho. Acreditamos que o uso dos problemas matemáticos em aberto podem promover a investigação, mas durante a elaboração deste material surgiram os seguintes questionamentos:

1. Qual a melhor forma de se propor um problema matemático em aberto a um estudante do Ensino Médio? Mencionar ou não que se trata de um problema em aberto?

2. O conhecimento prévio pelo estudante do Ensino Médio de que um problema matemático está em aberto gera motivação ou desestímulo para tentar respondê-lo?

3. Se um problema matemático em aberto gerar uma motivação num estudante do Ensino Médio para tentar respondê-lo, será apenas por

um curto espaço de tempo e logo ele desistirá após algumas tentativas de resolução?

4. Os problemas matemáticos em aberto motivam apenas alunos do Ensino Médio com alto potencial em matemática ou podem motivar os que têm dificuldade?

5. A motivação gerada por um problema matemático em aberto pode causar dependência e viciação, prejudicando pedagogicamente o estudante do Ensino Médio nos seus estudos regulares?

Assim, pretendemos dar continuidade nesta pesquisa com aplicação desse material para coletar dados que permitam analisar o comportamento dos estudantes do Ensino Médio diante dos problemas em aberto e, consequentemente, elaborar uma proposta curricular de matemática para o Ensino Médio incentivando atividades investigativas por meio de problemas em aberto.

9.4 Referências bibliográficas

ANDERSEN, J. Primes in Arithmetic Progression Records. **Prime Records**, 2017. Disponível em: <http://primerecords.dk/aprecords.htm>. Acesso em: 11 fev. 2018.

BARBOSA, J.; ASSIS NETO, F. Pierre Laurent Wantzel: O Último Capítulo de Dois dos Três. In: IX SEMINÁRIO NACIONAL DE HISTÓRIA DA MATEMÁTICA, 9., 2011, Aracaju. **Anais do IX Seminário Nacional de História da Matemática**. São Paulo: Sbhm, 2011. p. 1 - 9.

BOYER, C. Some notes on the magic squares of problem. **The Mathematical Intelligencer**, [s.l.], v. 27, n. 2, p.52-64, 2005.

BOYER, C. Bimagic squares of primes. **MultiMagic**, c2020. Disponível em: <http://www.multimagie.com/English/BimagicPrimes.htm>. Acesso em: 23 jun. 2021.

BBC BRASIL. **Por que um problema simples é um dos buracos negros da matemática**. 2016. Disponível em:

<http://www.bbc.com/portuguese/geral-36702054>. Acesso em: 10 out. 2016.

D'AMBROSIO, B.. Formação de professores de matemática para o século XXI: o grande desafio. **Pro-posições**, Campinas, v. 4, n. 1, p.35-41, mar. 1993.

DUBNER, H. et al. Ten consecutive primes in arithmetic progression. **Mathematics Of Computation**, [s.l.], v. 71, n. 239, p.1323-1328, 28 nov. 2001.

Disponível em: <http://www.ams.org/journals/mcom/2002-71-239/S0025-5718-01-01374-6/S0025-5718-01-01374-6.pdf>. Acesso em: 17 fev. 2018.

EULER's Magic Square. **Math Garden Blog**, 2016. Disponível em: <http://mathgardenblog.blogspot.com/2016/05/Euler-magic-square.html>. Acesso em: 23 jun. 2021.

GREEN, B.; TAO, T. The primes contain arbitrarily long arithmetic progressions. **Annals Of Mathematics**, [s.l.], v. 167, n. 2, p.481-547, 1 mar. 2008.

HEFEZ, Abramo. **Aritmética**. 2. ed. Rio de Janeiro: SBM, 2016. (Coleção Profmat).

LIMA, R. A. de. **A utilização de problemas matemáticos em aberto no ensino médio**. 2018. Dissertação (Mestrado) — UFRPE, Recife-PE.

MORGADO, A. et al. **Análise Combinatória e Probabilidade**. 8. ed. Rio de Janeiro: SBM, 1991. (Coleção do Professor de Matemática).

NASCIMENTO, S. O Tijolo de Euler. **O baricentro da mente**, 2015. Disponível em: <https://www.obaricentrodamente.com/2015/07/o-tijolo-de-euler.html>. Acesso em: 23 jun. 2021.

PEIXE, T.; BUESCU, J. Recorrências, progressões aritméticas e teoria ergódica: teoremas de van der Waerden e de Green-Tao. **Revista Matemática Universitária**, Rio de Janeiro, v. 48-49, n. 1, p.39-51, 2010. Disponível em: <<http://rmu.sbm.org.br/Conteudo\/n48_n49/n48_n49_Artigo01.pdf>>. Acesso em: 20 fev. 2018.

SACRISTÁN, J. G.; GÓMEZ, A. I. P.. **Compreender e transformar o ensino**. São Paulo: Artmed, 1998.

SHULDHAM, C. Pandiagonal Prime Number Magic Squares.

O Mestrado Profissional em Matemática em Rede Nacional - PROFMAT - é um curso semipresencial de pós-graduação stricto sensu com oferta nacional voltado para o aprimoramento da formação profissional de professores da educação básica.

No âmbito da Universidade Federal Rural de Pernambuco, o PROFMAT comemora 10 anos de existência em 2021 e esta obra, que compreende produções advindas de dissertações apresentadas ao longo de sua história e conta com o apoio da CAPES e da UFRPE, compõe um dos elementos representativos da excelência desse programa como formação continuada de professores de matemática, que reflete, sem dúvida, na elevação da qualidade de ensino de matemática em Pernambuco e em regiões circunvizinhas.

openaccess.blucher.com.br

ISBN 978-65-5550-097-4

Blucher Open Access