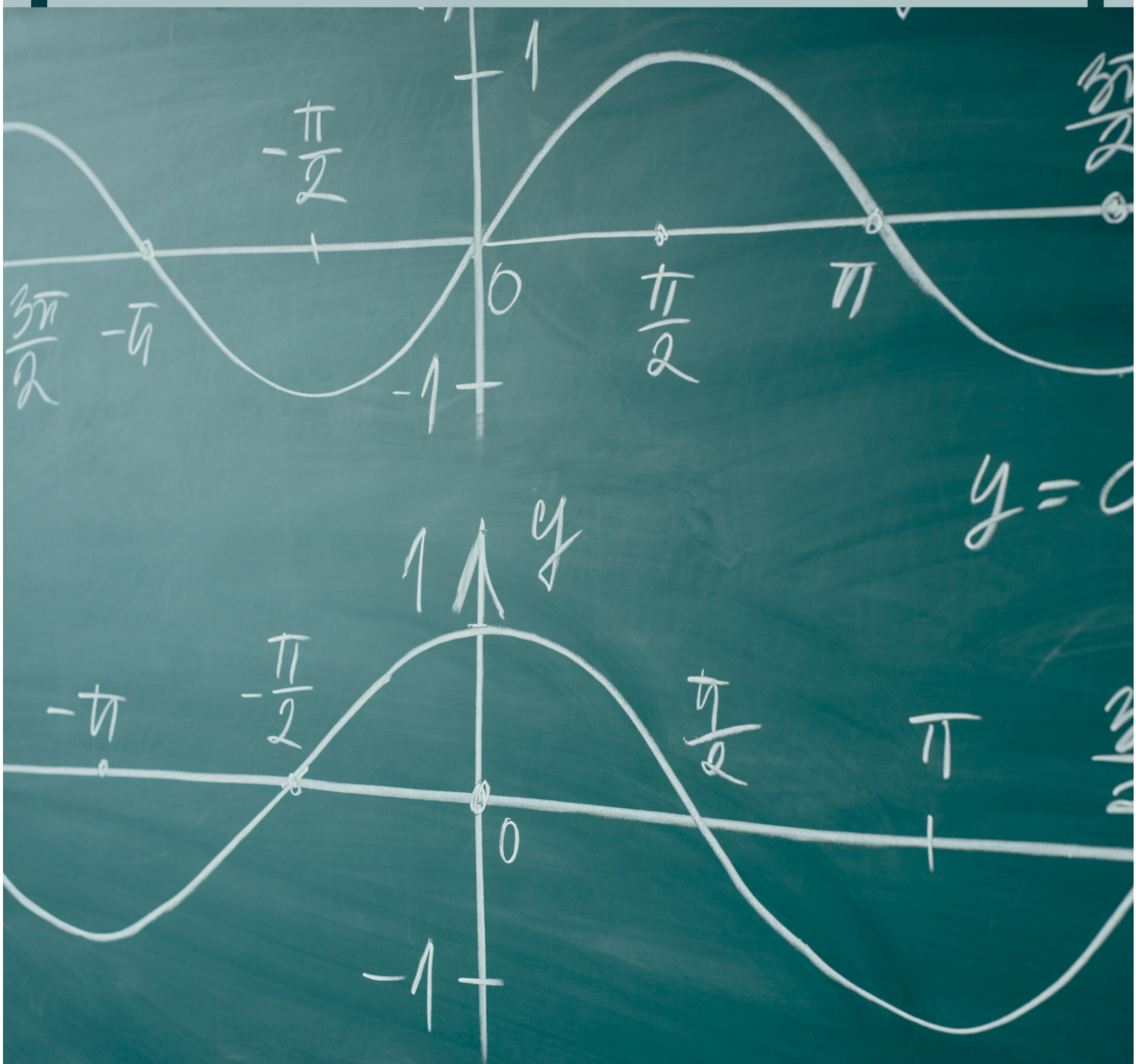


COLETÂNEA DE TRABALHOS DO PROFMAT/UFERSA VOLTADO AOS ESTUDOS DE FUNÇÕES E SUAS APLICAÇÕES AO ENSINO MÉDIO



Antônio Ronaldo Gomes Garcia
Antônia Jocivânia Pinheiro
Franceliza Monteiro da Silva Dantas
Maria Joseane Felipe Guedes Macedo

Paulo Cesar Linhares da Silva
Kleber Soares Câmara
Walter Martins Rodrigues



EDITORA CONHECIMENTO LIVRE

Antônio Ronaldo Gomes Garcia
Antônia Jocivânia Pinheiro
Franceliza Monteiro da Silva Dantas
Maria Joseane Felipe Guedes Macedo
Paulo Cesar Linhares da Silva
Kleber Soares Câmara
Walter Martins Rodrigues

Coletânea de trabalhos do PROFMAT/UFERSA voltado aos estudos de funções e suas aplicações ao ensino médio

1ª ed.

Piracanjuba-GO
Editora Conhecimento Livre
Piracanjuba-GO

1ª ed.

Dados Internacionais de Catalogação na Publicação (CIP)

Garcia, Antônio Ronaldo Gomes
G216C Coletânea de trabalhos do PROFMAT/UFERSA voltado aos estudos de funções e suas aplicações ao ensino médio

/ Antônio Ronaldo Gomes Garcia. Antônia Jocivânia Pinheiro. Franceliza Monteiro da Silva Dantas. Maria Joseane Felipe Guedes Macedo. Paulo Cesar Linhares da Silva. Kleber Soares Câmara. Walter Martins Rodrigues. — Piracanjuba-GO
Editora Conhecimento Livre, 2021

133 f.: il

DOI: 10.37423/2021.edcl386

ISBN: 978-65-5367-100-3

Modo de acesso: World Wide Web

Incluir Bibliografia

1. ensino-médio 2. tipos-de-funções 3. aplicações-das-funções-no-ensino-médio I. Garcia, Antônio Ronaldo Gomes II. Pinheiro, Antônia Jocivânia III. Dantas, Franceliza Monteiro da Silva IV. Macedo, Maria Joseane Felipe Guedes V. Silva, Paulo Cesar Linhares da VI. Câmara, Kleber Soares VII. Rodrigues, Walter Martins VII. Título

CDU: 370

<https://doi.org/10.37423/2021.edcl386>

O conteúdo dos artigos e sua correção ortográfica são de responsabilidade exclusiva dos seus respectivos autores.

EDITORA CONHECIMENTO LIVRE

Corpo Editorial

Dr. João Luís Ribeiro Ulhôa

Dra. Eyde Cristianne Saraiva-Bonatto

MSc. Frederico Celestino Barbosa

MSc. Carlos Eduardo de Oliveira Gontijo

MSc. Plínio Ferreira Pires

Editora Conhecimento Livre

Piracanjuba-GO

2022

CAPÍTULO 1	5
APRESENTAÇÕES GERAIS	
Walter Martins Rodrigues	
Franceliza Monteiro da Silva Dantas	
Maria Joseane Felipe Guedes Macêdo	
Antônia Jocivânia Pinheiro	
Kleber Soares Câmara	
DOI 10.37423/220405655	
CAPÍTULO 2	14
APRENDER FUNÇÕES COM APOIO NO SOFTWARE EXCEL: USO DAS NOVAS	
TECNOLOGIAS NO PROCESSO ENSINO-APRENDIZAGEM DE MATEMÁTICA NA EDUCAÇÃO	
BÁSICA	
Franco Cleidson Fonseca Oliveira	
Walter Martins Rodrigues	
DOI 10.37423/220305543	
CAPÍTULO 3	35
ESTUDO DE FUNÇÕES GERADORAS E SUAS APLICAÇÕES EM PROBLEMAS DE ANÁLISE	
COMBINATÓRIA	
Laudelino Gomes Ferreira	
Antonio Ronaldo Gomes Garcia	
DOI 10.37423/220305541	
CAPÍTULO 4	55
FUNÇÕES LINEARES NO ESTUDO DO SISTEMA DE CORES RGB	
Lucas Oliveira Ferreira	
Walter Martins Rodrigues	
DOI 10.37423/220305623	
CAPÍTULO 5	82
FUNÇÕES AFINS E CRIPTOGRAFIA	
Maria Joseane Felipe Guedes Macêdo	
Willa da Silva Medeiros	
DOI 10.37423/220305624	
CAPÍTULO 6	98
FUNÇÕES QUADRÁTICAS E CRIPTOGRAFIA	
Maria Joseane Felipe Guedes Macêdo	
Willa da Silva Medeiros	
DOI 10.37423/220305625	

CAPÍTULO 7 120

FUNÇÕES TRIGONOMÉTRICAS: UMA PROPOSTA DE ENSINO BASEADA NO CONTEXTO HISTÓRICO, NO USO DE RECURSOS TECNOLÓGICOS E NA RESOLUÇÃO DE SITUAÇÕES PROBLEMAS

John Nathan Pereira de Carvalho

Luiza Helena Felix de Andrade

DOI 10.37423/220305622

Capítulo 1



10.37423/220405655

APRESENTAÇÕES GERAIS

Walter Martins Rodrigues

*Universidade Federal Rural do Semi-Árido -
UFERSA*

Franceliza Monteiro da Silva Dantas

*Universidade Federal Rural do Semi-Árido -
UFERSA*

Maria Joseane Felipe Guedes Macêdo

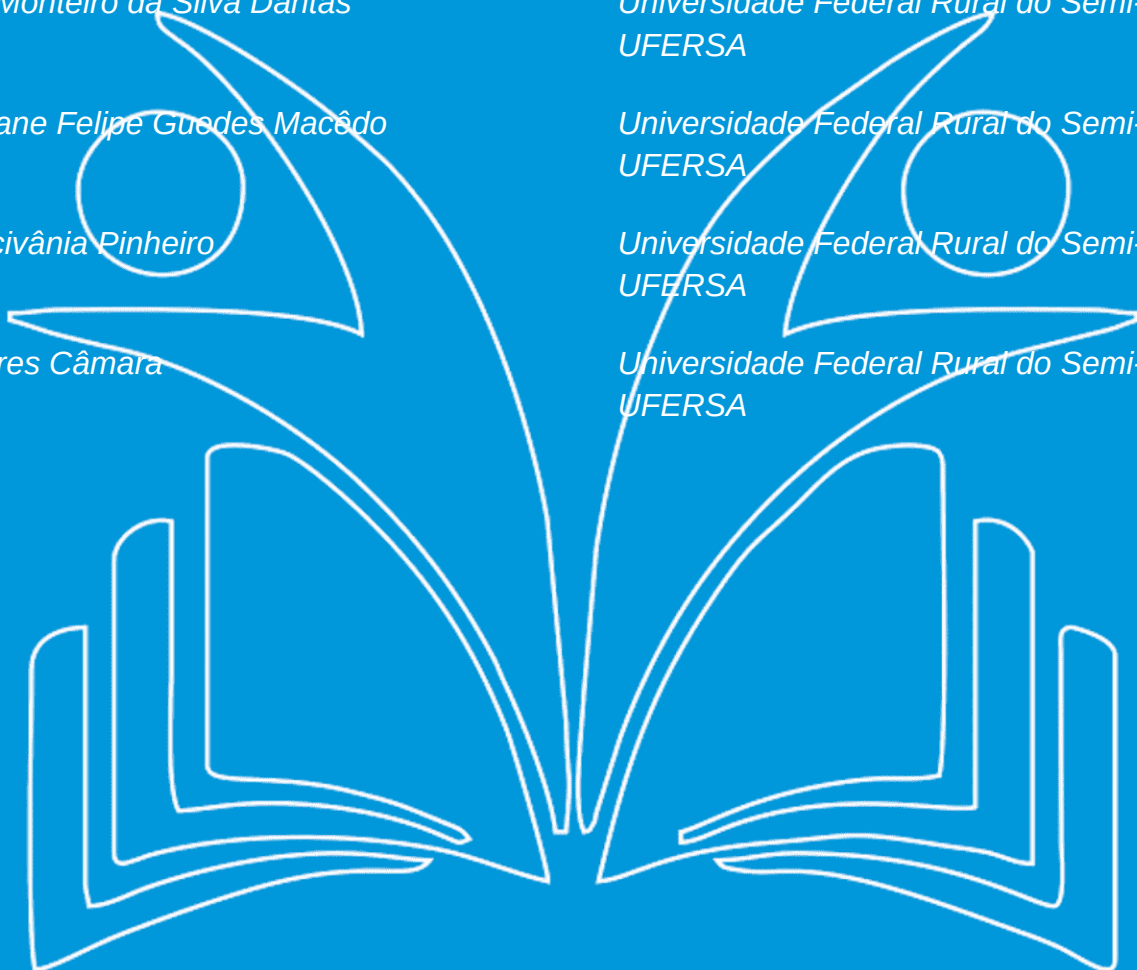
*Universidade Federal Rural do Semi-Árido -
UFERSA*

Antônia Jocivânia Pinheiro

*Universidade Federal Rural do Semi-Árido -
UFERSA*

Kleber Soares Câmara

*Universidade Federal Rural do Semi-Árido -
UFERSA*



EQUIPE ORGANIZADORA DA COLETÂNEA DE TRABALHOS DO PROFMAT/UFERSA VOLTADO AOS ESTUDOS DE FUNÇÕES E SUAS APLICAÇÕES AO ENSINO MÉDIO

Este trabalho foi proposto pelo Colegiado do Mestrado Profissional em Matemática (PROFMAT/UFERSA), que nomeou uma comissão responsável pela seleção dos trabalhos e pela organização deste livro. A seleção dos trabalhos ocorreu por intermédio de um edital interno na Universidade Federal Rural do Semi-Árido (UFERSA). A seguir apresentamos os colaboradores que possibilitaram a realização deste trabalho.



Membro da comissão organizadora desta coletânea. A Prof. Dra. Antônia J. Pinheiro é Licenciada e Mestre em Matemática pela Universidade Federal do Ceará (2010). Doutora em Ciência da Computação pela Universidade Federal do Rio Grande do Norte. É professora da UFERSA. Atua como membro permanente do quadro docente do PROFMAT/UFERSA.



Membro da comissão organizadora desta coletânea. O Prof. Dr. Antonio R. G. Garcia cursou Licenciatura em Ciências com Habilitação em Matemática na UERN. Possui dedicação exclusiva na UFERSA Campus de Mossoró-RN. É doutor em Ciências na área de Matemática pelo IME-USP, onde também cursou o mestrado. Atualmente é membro permanente do quadro docente do PROFMAT/UFERSA, atua na linha de pesquisa de Análise Matemática estudando as Equações Diferenciais Parciais Soluções Generalizadas, com ênfase em Álgebra das Funções Generalizadas de Colombeau.



Membro da comissão organizadora desta coletânea. O Prof. Dr. Kleber S. Câmara possui graduação em Licenciatura Plena em Matemática pela Universidade do Estado do Rio Grande do Norte (2010) e Mestrado em Matemática pela Universidade Federal da Paraíba (2012), tendo Análise como área de concentração. É membro permanente do quadro docente do PROFMAT/UFERSA.



Membro da comissão organizadora desta coletânea. A Profa. Dra. Franceliza M. S. Dantas cursou o doutorado em Estudos da Linguagem pelo Programa de Pós-Graduação em Linguística Aplicada (PPGEL/UFRN). Mestre em Ensino de Ciências Naturais e Matemática pela UFRN/PPGECNM e Graduada em Letras com Habilitação em Língua Portuguesa e respectivas Literaturas, pela UERN. Faz parte do quadro Técnico Administrativo da UFERSA, na função de Secretária Executiva. Toda a atuação e produção são desenvolvidas dentro da Linguística, Linguística Aplicada, Educação e Língua Portuguesa.



Membro da comissão organizadora e autora de dois capítulos nesta coletânea. A Profa. Dra. M. Joseane F. G. Macêdo é efetiva da UFERSA desde 2009. Possui Doutorado em Matemática (2017), na área de Otimização, pela UFPR em regime de cotutela com a Universidade do Minho (PT). Sua pesquisa é voltada para Matemática Aplicada, com ênfase em Otimização. Possui bacharelado em Meteorologia (2001) e mestrado em Meteorologia (2004) pela UFCG, Bacharelado em Matemática (2007) e mestrado em Matemática (2009), na área de Equações Diferenciais, pela UFCG. Atua como membro permanente do PROFMAT/UFERSA.



Membro da comissão organizadora e autor de dois capítulos nesta coletânea. Possui graduação em Licenciatura em Matemática pela USP, onde também cursou o mestrado e doutorado em Matemática, na área de Representação de álgebras. Atualmente é professor Titular da UFERSA. Trabalha com pesquisa voltada para modelagem matemática aplicada a irrigação, realiza pesquisas em Matemática, com ênfase no estudo de álgebras e participa de um grupo de pesquisa voltado ao estudos das álgebras de Colombeau, desde 2013. Atualmente é coordenador do Mestrado Profissional em Matemática (PROFMAT/UFERSA).



Autora de um capítulo desta coletânea. A Profa. Dra. Luiza H. F. Andrade possui graduação em Licenciatura em Matemática pela Universidade Estadual do Ceará (2002), mestrado em Matemática pela UFC (2007) e doutorado em Engenharia de Teleinformática pela UFC (2018). Atualmente é adjunto II da UFERSA e membro permanente do quadro de docentes do PROFMAT/UFERSA. Tem experiência na área formação de professores de matemática e de Geometria Riemanniana, atuando principalmente em Geometria da Informação.



Autor de um capítulo desta coletânea. Ms. Lucas Oliveira Ferreira cursou a graduação em Matemática pela Universidade Estadual do Ceará - FAFIDAM/UECE, mestrado profissional em Matemática pela UFERSA. Desde 2009 é professor da rede estadual de ensino do Ceará. Em 2019, passou a atuar como formador regional de matemática da SEDUC/CE. A partir de 2020, tornou-se professor tutor nos cursos de licenciatura do Núcleo de Educação a Distância (NEAD) da UFERSA e também professor do programa Obmep na Escola (ONE).

Membro da comissão organizadora desta coletânea. O Prof. Dr. Paulo C. L. da Silva é doutor em Engenharia Elétrica/Computação, com área de concentração em Telecomunicações pela UFRN. Mestre em Ciências da Computação, com área de Concentração em Fundamentos da Computação, pela UFC (2009). Bacharel em Matemática pela UFC (2003). Atualmente é Professor Adjunto I UFERSA, lecionando nesta universidade desde 15 de janeiro de 2010.

Laudelino Ferreira Gomes é autor de um capítulo desta coletânea de artigos. Possui graduação em Licenciatura Plena em Matemática pela Universidade do Estado do Rio Grande do Norte (2001). Cursou o mestrado profissional em Matemática na UFERSA. Atualmente é professor assistente II da

Universidade do Estado do Rio Grande do Norte atuando no Departamento de Matemática e Estatística.



Autor de dois capítulos desta obra. Ms. Willa S. Medeiros é graduado em Licenciatura em matemática pela Universidade do Estado do Rio Grande do Norte - UERN. cursou mestrado profissional em Matemática pela UFERSA. Professor efetivo da Rede Estadual de Ensino do Estado da Paraíba



Autor de um capítulo desta coletânea. John N. P. Carvalho é graduado em Licenciatura em matemática pela Universidade do Estado do Rio Grande do Norte – UERN. cursou o mestrado profissional em Matemática na UFERSA sob orientação da Prof. Dra Luiza Helena Felix de Andrade.

APRESENTAÇÃO DA ESTRUTURA DA COLETÂNEA DE TRABALHOS DO PROFMAT/UFERSA VOLTADO AOS ESTUDOS DE FUNÇÕES E SUAS APLICAÇÕES AO ENSINO MÉDIO

Este livro é estruturado na escolha de trabalhos essenciais desenvolvidos por pesquisadores e colaboradores do projeto de divulgação de ações práticas de ensino provenientes do Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) da UFERSA.

Trata-se de um trabalho completamente voltado ao aspecto de aplicação em sala de aula. A comissão responsável pela organização da coletânea de trabalhos foi definida pelo colegiado do Mestrado Profissional em Matemática da UFERSA, e formalizada pela emissão da Portaria UFERSA/PROPPG Nº 50 / 2021 de 29 de julho do ano de 2021, formada pelo Prof. Dr. Antônio Ronaldo Gomes Garcia, Profa. Dra. Antônia Jocivania Pinheiro, Profa. Dra. Maria Joseane Felipe Guedes Macêdo, Profa. Dra. Franceliza Monteiro da Silva Dantas, Prof. Dr. Paulo César Linhares da Silva, Prof. Dr. Walter Martins Rodrigues e Prof. Dr. Kleber Soares Câmara.

A comissão contempla professores experientes, com grandes contribuições na formação de professores, profissionais que também são pesquisadores que contribuem no desenvolvimento da Educação, e da Matemática brasileira.

Inicialmente a comissão optou por trabalhar dentro do tema que aborda os mais variados trabalhos tocantes ao ensino e aprendizado de funções e suas aplicações, que podem ser explorados pelos professores do ensino médio, como forma de dinamizar o trabalho pedagógico. São trabalhos que permitem levar a prática de sala de aula as principais vertentes de aprendizagem ativa e das novas metodologias da educação matemática.

Nessa coletânea de trabalhos provindos de dissertações do PROFMAT/UFERSA, temos a oportunidade de levar aos leitores, em particular aos professores da rede pública os seguintes conteúdos.

Dois capítulos tratando de estudos que relacionam o tema criptografia com funções quadráticas e com funções afins. Ambos desenvolvidos durante o trabalho de dissertação de mestrado de Willa da Silva Medeiros, sob a orientação da Profa. Dra. M. Joseane F. G. Macêdo. Funções é um dos temas mais importantes na matemática e infelizmente muitas vezes é estudado e ensinado sem um contexto de aplicação. Neste sentido, é proposto uma abordagem bem contextualizada com a finalidade de motivar os estudantes e professores, cujo objetivo principal é apresentar um método de criptografia bastante intuitivo envolvendo as funções quadráticas e afins.

Um capítulo sobre a exploração de funções lineares no trabalho de modelagem do sistema de cores RGB. Trata-se de um trabalho associado aos estudos realizados por Lucas Oliveira Ferreira durante o trabalho de mestrado, que foi orientado pelo Prof. Dr. Walter Martins Rodrigues. Neste sentido aborda-se aplicação de funções lineares, associado ao sistema de cores RGB e o uso das tecnologias da informação, especificamente o site webcalc e calculadora para a resolução de problemas para o ensino aprendizagem desse relevante tópico matemático. O principal objetivo é propiciar aos professores de matemática do ensino médio um método de apresentar o conteúdo de forma que a aprendizagem seja motivadora e significativa, mostrando uma importante aplicação de sistemas lineares.

Outro capítulo associado a um trabalho de orientação do Prof. Dr. Walter Martins, é o capítulo sobre uso de planilhas eletrônicas como suporte no ensino e aprendizagem dos conceitos gerais de funções. Esse capítulo, proveniente do trabalho de dissertação de mestrado de Franco Cleidson Fonseca Oliveira, propõe o uso do suporte computacional, a partir de softwares bem difundidos e de fácil acesso, no ensino e aprendizagem de funções, elaboração de gráficos e manejo de dados.

No tocante ao estudo de funções, é bem sabido que o tema funções trigonométrica geralmente é muito desafiador para o estudante, bem como para o professor trazer elementos de motivação para seu estudo no ensino médio. A Profa. Dra. Luiza Helena Felix de Andrade orientou o trabalho de dissertação de mestrado de John Nathan Pereira de Carvalho, que dá uma contribuição no ensino e aprendizagem de funções trigonométricas a partir de uso de recursos tecnológicos e de resolução de problemas.

O conceito de funções é muito rico e possui inúmeras aplicações na compreensão de fenômenos naturais, em particular no tratamento estatístico de informações. Neste sentido, essa coletânea traz uma contribuição associada ao trabalho de mestrado de Laudelino Pereira Gomes, realizado sob orientação do Prof. Dr. Antonio Ronaldo Gomes Garcia. Trata-se de um capítulo que tem como foco um estudo sobre Funções Geradoras, em que elementos sobre problemas de contagem modelados por recorrências lineares de primeira e segunda ordens, são estudados.

Os autores e comissão organizadora esperam que este trabalho possa contribuir de maneira significativa com o trabalho dos professores do ensino básico, motivando-os a buscar mais aplicações ao conteúdo abordado em sala de aula. Em especial, nas aulas de matemática.

Para o leitor que desconhece o programa de Mestrado profissional em Matemática, dedicamos alguns parágrafos afim de apresentar um pouco desse importante programa de pós-graduação.

O Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) foi o primeiro projeto nacional de mestrado profissional do Brasil. Surgiu a partir de uma colaboração entre a Sociedade Brasileira de Matemática (SBM) e o Instituto de Matemática Pura e Aplicada (IMPA). É um programa de mestrado semipresencial na área de Matemática que viabiliza a qualificação do professor de Matemática, em consonância com atividades de ensino. O PROFMAT foi recomendado pelo Conselho Técnico-Científico da Educação Superior – CTC-ES da CAPES, em sua reunião realizada nos dias 25 a 29 de outubro de 2010 iniciando com o conceito 3 e atualmente, em uma nova avaliação, é um programa de mestrado referendado com o mais alto conceito que um programa de mestrado pode ter, tendo avaliação Capes de conceito 5 em todas as avaliações nos últimos dez anos. O PROFMAT é coordenado atualmente pela SBM e oferecido em Instituições Associadas de Ensino Superior por todos os estados da federação e Distrito Federal.

O público alvo do PROFMAT consiste, prioritariamente, dos professores do Ensino Básico que se encontram efetivamente em sala de aula no ensino de matemática, porém é aberto a qualquer portador de diploma de ensino superior. Aos professores das instituições públicas de Ensino Básico estão previstas bolsas de mestrado da CAPES, nos mesmos moldes das bolsas de mestrado de demanda social. Um ponto fundamental é que os professores que recebem bolsa CAPES assumem como contrapartida o compromisso de continuar em exercício na rede pública por um período de cinco anos após a conclusão do mestrado.

O PROFMAT é formado por uma rede de Instituições de Ensino Superior, envolvendo as principais instituições de ensino superior brasileiras. A UFERSA faz parte desde sua primeira turma em 2011, quando o Programa de Pós-Graduação em Matemática Stricto Sensu em nível de mestrado na modalidade profissional do Departamento de Ciências Naturais, Matemática e Estatística – DCME da Universidade Federal Rural do Semi-Árido – PROFMAT/UFERSA foi aprovado pelo Conselho de Ensino e Pesquisa – CONSEPE e referendado pelo Conselho Superior Universitário – CONSUNI – RESOLUÇÃO CONSUNI/UFERSA Nº 001/2011, de 14 de março de 2011, para ter início no período 2011.1.

O PROFMAT da UFERSA dispõe de um quadro de professores efetivos, todos com o título de doutor. A cada ano ingressa, em média 20 mestrandos no programa. Nos últimos dois exames de qualificação a UFERSA teve 100% de aprovação dos qualificantes.

A admissão de discentes e a distribuição de bolsas de estudos se dão por meio de um Exame Nacional de Acesso, versando sobre um programa de conteúdo matemático do Ensino Básico, previamente definido e divulgado através de Edital. O Exame Nacional de Acesso consiste num único exame,

realizado pelo menos uma vez por ano, ao mesmo tempo, nas Instituições Associadas. O número de vagas é decidido antecipadamente a cada ano de acordo com cada instituição associada e estabelecido em editais.

A estrutura do PROFMAT, é montada visando que os formandos deste Programa de Mestrado saiam com uma sólida formação de matemática básica, o que garante uma melhor atuação profissional, melhorando assim a qualidade do ensino de matemática nas escolas básicas.

Capítulo 2



10.37423/220305543

APRENDER FUNÇÕES COM APOIO NO SOFTWARE EXCEL: USO DAS NOVAS TECNOLOGIAS NO PROCESSO ENSINO-APRENDIZAGEM DE MATEMÁTICA NA EDUCAÇÃO BÁSICA

Franco Cleidson Fonseca Oliveira

*Universidade Federal Rural do Semi-Árido -
UFERSA*

Walter Martins Rodrigues

*Universidade Federal Rural do Semi-Árido -
UFERSA*



1. INTRODUÇÃO

A matemática, em sua história, traz a contribuição de diversos povos primitivos, uma vez que foi inventada e vem sendo desenvolvida pelo homem em função de necessidades sociais. Assim, segundo (BOYER, 1996) durante o Paleolítico inferior (3.000.000 de anos) o homem viveu da caça e da coleta, necessitando das noções de mais–menos, maior–menor e formas para a fabricação de armas.

Ainda de acordo com (BOYER,1996), no período Paleolítico Superior, que foi caracterizado por instrumentos mais elaborados para a caça e coleta, entre os quais estavam: armadilhas, redes, cestos, arcos, flechas, roupas de peles, canoas, o homem utilizava materiais como: paus, pedras, ossos, peles, cipós e fibras e, nesse período, sentiam a necessidade de registros: números e figuras, isto é, para fazer um cesto necessitava da contagem e noções intuitivas de paralelismo e perpendicularismo. Foi nessa época que surgiu a geometria e a pictografia.

Precisando cada vez mais de conhecimentos que pudessem melhorar a vida do homem, o período chamado Neolítico surgiu com o domínio do homem sobre a natureza por meio da domesticação de plantas e animais. Foi então que surgiu a agricultura e a pecuária, cerca de 6.000 anos a.C. A evolução social do homem Neolítico fez com que novos conhecimentos fossem incorporados por tentativa e erro: conhecimentos sobre terra e fertilidade, semestres, técnicas de plantio e colheita, datação do plantio, seleção, contagem dos rebanhos, elaboração de calendários agrícolas, o armazenamento de grãos e o cozimento que criaram a necessidade da cerâmica. Assim, cada vez mais avançava o conhecimento matemático por meio da prática cotidiana do homem pré-histórico.

E a evolução da vida em comunidade não parava de crescer: as choupanas transformaram-se em casas e as aldeias em cidades, fazendo surgir o período histórico. Com essa nova forma de organização social, surgiu: o Estado, as classes sociais, a propriedade, a escrita (fonética), por causa do aumento da produção que gerou o excedente, havendo a necessidade de armazenamento de produtos em grande escala e de sua contabilização. Desenvolvia-se cada vez mais a matemática. Surgia, então, uma ciência.

1. O ENSINO E A APRENDIZAGEM DE MATEMÁTICA

Ensinar e aprender: duas palavras que estão intrinsecamente relacionadas e que necessitam ser assimiladas pelos atores envolvidos nesse processo. Em relação à Matemática não poderia ser diferente: as necessidades cotidianas fazem com que os alunos desenvolvam capacidades de natureza prática para lidar com a atividade matemática, o que lhes permite reconhecer problemas, buscar e

selecionar informações, tomar decisões. Quando essa capacidade é potencializada pela escola, a aprendizagem se efetiva com resultados mais positivos. Conceitos ligados à: proporcionalidade, igualdade, composição, decomposição, inclusão podem ser demonstrados pelos alunos mesmo antes de terem acesso aos princípios e teoremas matemáticos. De acordo com as diretrizes curriculares nacionais da educação básica (BRASIL, 2013) deve haver uma relação dos conteúdos **matemáticos** com situações de práticas de aprendizagem, essa relação deve ser feita através da interdisciplinaridade, aplicando os conceitos **matemáticos** nas outras disciplinas.

No contexto histórico atual as crianças participam ativamente de situações sociais que contribuem para o processo de sua aprendizagem matemática. Estão imersas em experiências que as remetem a relações de quantidade, noção de espaço e manipulação de dinheiro. Estão inseridas em situações que envolvem números nos mais diversos contextos e são convidadas a buscar soluções para os variados problemas cotidianos, possibilitando-as comunicar-se matematicamente.

2. AS NOVAS TECNOLOGIAS E SUA UTILIDADE EDUCACIONAL

Nos tempos atuais, o uso da tecnologia no ensino-aprendizagem no ambiente escolar vem crescendo constantemente, aprimorando o conteúdo passado pelo professor, como sendo de um melhor entendimento, conseguindo ter uma melhor atenção do aluno de uma forma positiva. A internet é uma das ferramentas que mais está sendo usada, tendo os mais jovens como usuários principais, sendo exigidas pesquisas em sites, obrigando o professor a se atualizar e acompanhar as novas formas de ensino que vem sendo modernizadas pela velocidade das tecnologias, que sempre prendem a atenção do educando, por conhecerem as novidades das tecnologias. Isso faz com que eles se sintam mais interessados, por adquirirem intimidade com cada novidade que a internet traz. De forma geral, sabe-se que transformar em realidade o ensino tecnológico é uma tarefa árdua que exige do profissional de educação, pesquisa, conhecimento como abertura para as mudanças, como vemos em (LOPES e BISOGNIN, 2017).

A tecnologia está sendo muito valorizada no ambiente escolar, sendo forte influência na construção de informações que estão fortalecendo o ensino e a aprendizagem, tendo o professor como mediador, produzindo ideias com o auxílio da tecnologia e, na área de Matemática, fazendo uso do Excel para desenvolver melhor as competências dos alunos.

O educador encontra-se a cada dia de aula sentindo que está interagindo cada vez mais com a tecnologia, considerando a tecnologia como uma necessidade nos tempos de hoje, com a interação com a TV, o vídeo o celular, o data show e outros vários meios de utensílios modernos.

3. AULAS DE MATEMÁTICA OU AULAS DE INFORMÁTICA?

Muitas vezes o professor que utiliza ferramentas tecnológicas em suas aulas é questionado pelos alunos sobre qual a necessidade de recorrer à informática para ministrar aulas de Matemática, já que os cálculos precisam ser registrados nas avaliações, pois, se assim não for, existe a desconfiança de que houve “cola” e poderá vir, como consequência. De acordo com (DANTE, 2002) explorar o contexto e gerar aplicações são facilitadores que pode ser uma boa ferramenta para inserção do computador como ferramenta efetiva no ensino e aprendizagem de matemática.

Este fato ocorre por causa de alguns mitos que envolveram a Matemática por muito tempo. “Matemática só sabe quem vai para a ponta do lápis”; “Calculadora nas aulas de Matemática? Em hipótese nenhuma”; “Cálculo mental? Nem pensar”. “Para saber Matemática tem que ser muito bom de cálculo e é no lápis e caderno”.

Essas e outras expressões foram muito utilizadas em escolas que mantinham um currículo engessado por conteúdos abstratos que não tinham mediação com o cotidiano dos alunos. Dessa forma, não havia realmente motivação para identificar o Laboratório de Informática como um espaço privilegiado onde os alunos poderiam pesquisar e usar ferramentas tecnológicas para compreenderem melhor a relação que existe entre os conceitos matemáticos e a resolução de problemas do dia a dia.

É importante deixar claro para os alunos que a Informática é mais uma ferramenta que colabora para que a Matemática saia do mundo da abstração e seja aplicada em situações cotidianas.

4. ESTRATÉGIAS DE ENSINO COM O EXCEL

Conceitos foram estabelecidos, considerações foram expostas, explorou-se a história e a cronologia da Matemática e do desenvolvimento das tecnologias. Até mesmo foi abordada a questão da junção de Matemática com a Informática, para que se alcance uma aprendizagem significativa. Assim, além de desenvolver considerações acerca do que fora exposto, é preciso também apresentar sugestões que tragam algum benefício para a realização de aulas que apontem como principal meta a aquisição de conhecimentos que se firmem e subsidiem ações vindouras. Dessa forma, cabe agora sugerir algumas estratégias de Ensino de Matemática utilizando o programa Microsoft Excel, inclusive é uma

boa oportunidade para explorar a modelagem matemática como estratégia de ensino, nesse sentido sugerimos a leitura de (BIEMBEGUT, 2003).

Então, serão elencadas algumas atividades e passos a serem seguidos na utilização do Excel em aulas de Matemática.

a) Atividade I – Função

Para esboçarmos um gráfico da função do primeiro grau, podemos dar valores para o x e substituímos na fórmula. Dessa forma, dada a função $f(x) = 4x - 4$ esboce o seu gráfico no Excel. Neste caso basta seguir os seguintes passos:

- 1- Atribua valores para x que serão substituídos na fórmula. O resultado de cada função será o valor de y .
- 2- Substituindo na função temos:

	A	B
1	Função:	$f(x) = 4X-4$
2		
3	Valores de x	Valores de y
4	0	=4*A4-4
5	1	
6	2	
7	3	
8	4	

Figura 1: Atividade I. Fonte: Arquivo pessoal do autor.

- 3- Utilizaremos a alça de preenchimento para replicar a fórmula para as demais células.

	A	B
1	Função:	$f(x) = 4X-4$
2		
3	Valores de x	Valores de y
4	0	-4
5	1	
6	2	
7	3	
8	4	

Figura 2: Atividade I. Fonte: Arquivo pessoal do autor.

- 4- Por fim, encontramos os valores de x e y respectivamente de acordo com a função apresentada.

	A	B
1	Função:	$f(x) = 4x - 4$
2		
3	Valores de x	Valores de y
4	0	-4
5	1	0
6	2	4
7	3	8
8	4	12

Figura 3: Atividade I. Fonte: Arquivo pessoal do autor.

Agora que conhecemos os valores de x e y , basta selecionar todo o conjunto e acessar: Inserir, Gráficos e Dispersão e selecionar o gráfico Dispersão com Linhas Suaves conforme mostrado a seguir.

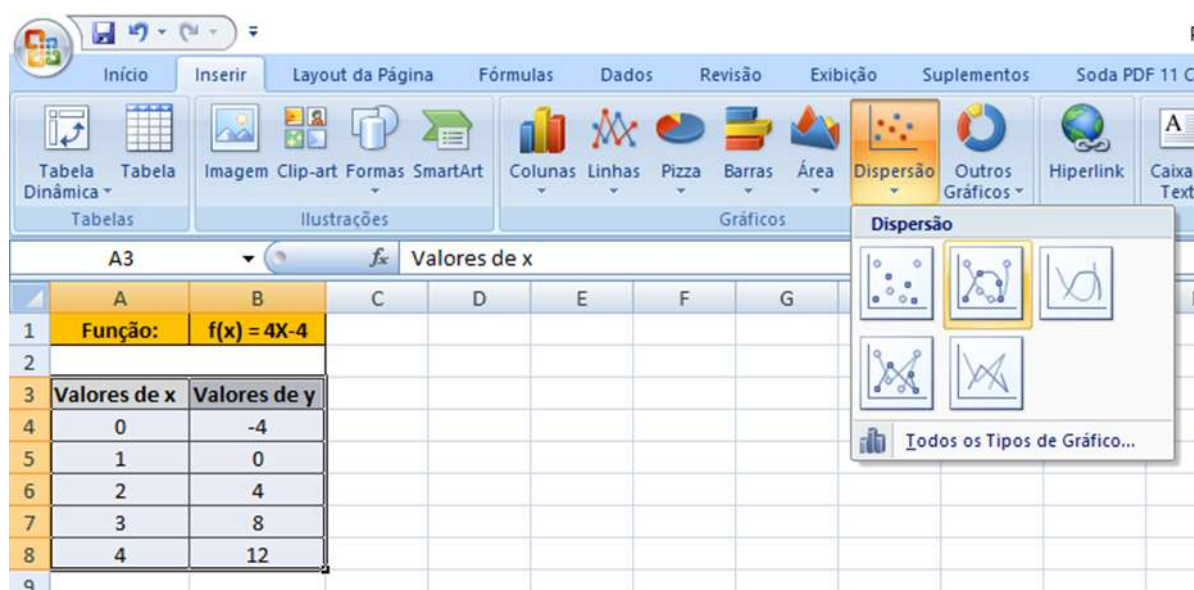


Figura 4: Atividade I. Fonte: Arquivo pessoal do autor.

Automaticamente o gráfico será esboçado. Note que a reta está crescente já que o coeficiente a da função exemplificada é positivo.

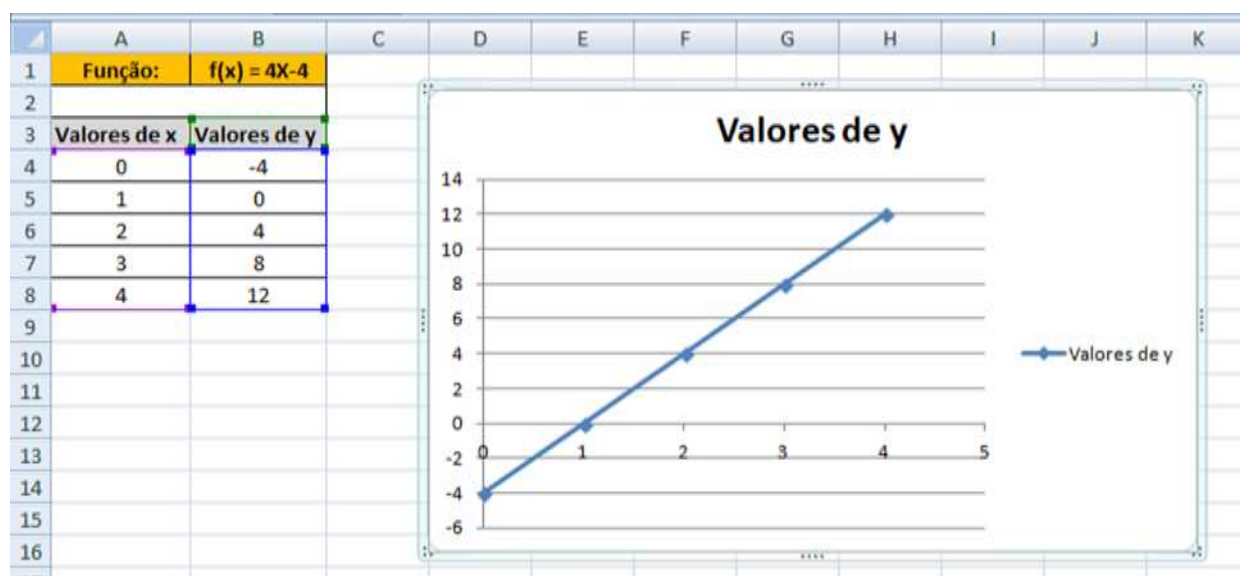


Figura 5: Atividade I. Fonte: Arquivo pessoal do autor.

b) Atividade II – Função do 2º grau

As funções do segundo grau, também conhecidas como Funções Quadráticas e são apresentadas da na forma $f(x) = ax^2 + bx + c$, onde a, b, c são números reais e a deve ser diferente de zero.

O gráfico da função do segundo grau é sempre representado por uma parábola. Logo, quando o a for positivo a parábola será esboçada com concavidade voltada para cima, porém quando o a for negativo, esta será esboçada com concavidade voltada para baixo.

Exemplo Prático: Dada a função, $f(x) = x^2 + 3x + 2$, esboce seu gráfico.

Neste caso basta seguir os seguintes passos:

- 1- Separamos os valores de a, b e c em cada célula.
- 2- Atribui-se valores para x .

	A	B	C	D	E
1	Função:	$f(x) = x^2 + 3x + 2$		x	y
2				-5	
3	a	1		-4	
4	b	3		-3	
5	c	2		-2	
6				-1	
7				0	
8				1	
9				2	
10				3	
11				4	
12				5	

Figura 6: Atividade II. Fonte: Arquivo pessoal do autor.

3- Substituem-se os valores na função $f(x) = ax^2 + bx + c$ com base em cada valor de x atribuído.

	A	B	C	D	E
1	Função:	$f(x) = x^2 + 3x + 2$		x	y
2				-5	=B3*D2^2+B4*D2+B5
3	a	1		-4	
4	b	3		-3	
5	c	2		-2	
6				-1	
7				0	
8				1	
9				2	
10				3	
11				4	
12				5	

Figura 7: Atividade II. Fonte: Arquivo pessoal do autor.

4- Tecle Enter e confira o resultado.

	A	B	C	D	E
1	Função:	$f(x) = x^2 + 3x + 2$		x	y
2				-5	12
3	a	1		-4	
4	b	3		-3	
5	c	2		-2	
6				-1	
7				0	
8				1	
9				2	
10				3	
11				4	
12				5	

Figura 8: Atividade II. Fonte: Arquivo pessoal do autor.

Para utilizamos a alça de preenchimento automático neste caso, basta travarmos as células que contém os valores de a , b e c .

	A	B	C	D	E
1	Função:	$f(x) = x^2 + 3x + 2$		x	y
2				-5	=B\$3*D2^2+B\$4*D2+B\$5
3	a	1		-4	
4	b	3		-3	
5	c	2		-2	
6				-1	
7				0	
8				1	
9				2	
10				3	
11				4	
12				5	

Figura 9: Atividade II. Fonte: Arquivo pessoal do autor.

Depois, basta copiar a fórmula para as demais células e conferir os valores atribuídos para y de acordo com cada valor de x.

	A	B	C	D	E
1	Função:	$f(x) = x^2 + 3x + 2$		x	y
2				-5	12
3	a	1		-4	
4	b	3		-3	
5	c	2		-2	
6				-1	
7				0	
8				1	
9				2	
10				3	
11				4	
12				5	

Figura 10: Atividade II. Fonte: Arquivo pessoal do autor.

	A	B	C	D	E
1	Função:	$f(x) = x^2 + 3x + 2$		x	y
2				-5	12
3	a	1		-4	6
4	b	3		-3	2
5	c	2		-2	0
6				-1	0
7				0	2
8				1	6
9				2	12
10				3	20
11				4	30
12				5	42

Figura 11: Atividade II. Fonte: Arquivo pessoal do autor.

Por fim, para a criação do gráfico, basta selecionar a tabela contendo os valores de x e y e acessar: Inserir, Gráficos e Dispersão e selecionar o gráfico Dispersão com Linhas Suaves conforme mostrado abaixo.

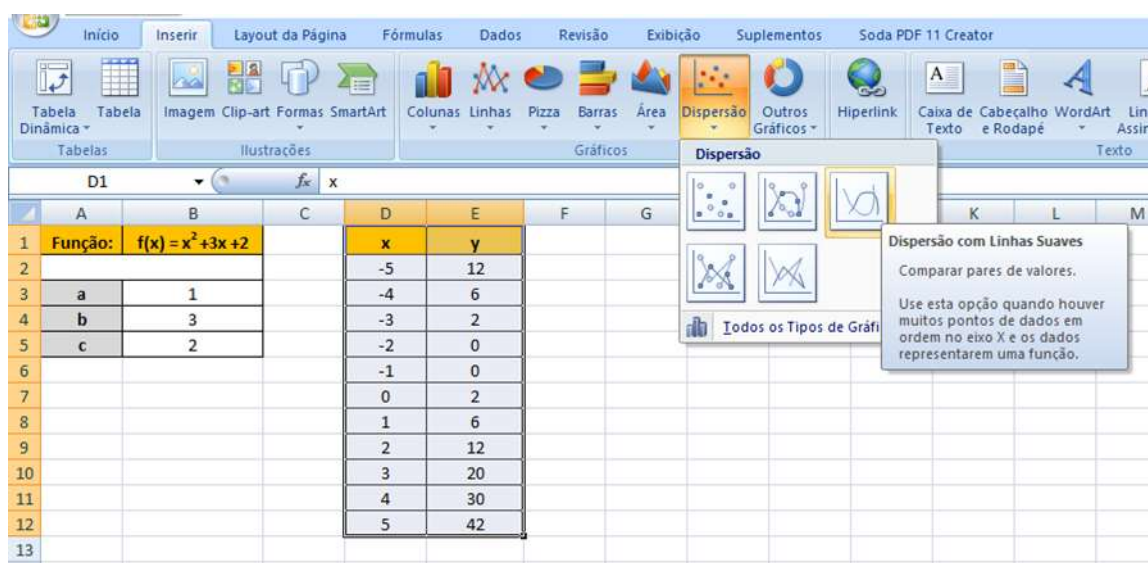


Figura 12: Atividade II. Fonte: Arquivo pessoal do autor.

Deste modo, o gráfico será esboçado automaticamente.

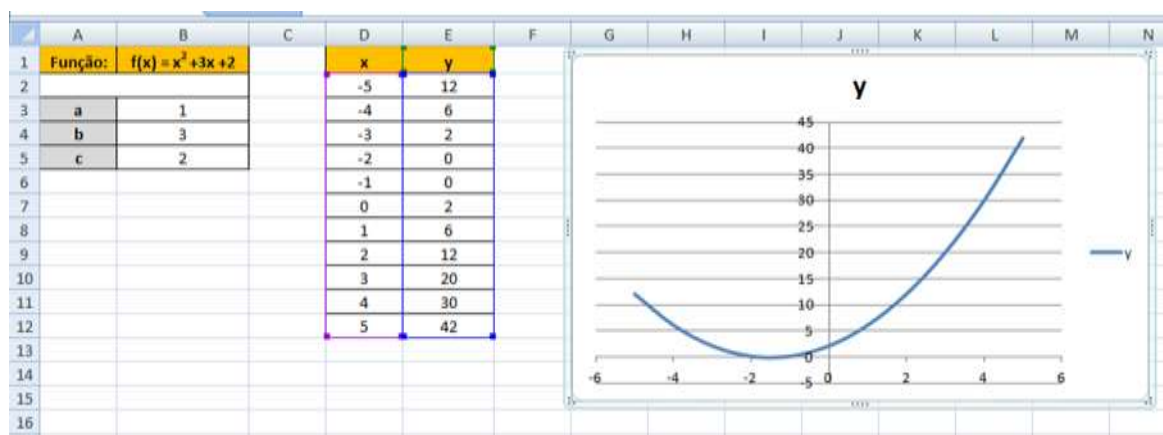


Figura 13: Atividade II. Fonte: Arquivo pessoal do autor.

Com base nos conhecimentos aqui adquiridos, foi possível aprender como criar gráficos das funções de primeiro e segundo grau no Excel. Além disso, nota-se a facilidade em esboçar gráficos com precisão bem como a flexibilidade em alterar os dados e obter uma instantânea atualização no gráfico.

c) Atividade III – Divisão de Polinômios

Em álgebra, a divisão polinomial é um algoritmo para dividir um polinômio por outro polinômio de menor ou igual grau. Dada a função $f(x) = x^2 - 2x + 3$ e $g(x) = x - 3$, esboce o gráfico de $h(x) = \frac{f(x)}{g(x)}$.

Nesse caso basta seguir os seguintes passos:

1 - Separamos os valores de A, B e C de cada função em células.

	A	B	C
1	Função:	$f(x) = x^2 - 2x + 3$	$g(x) = x - 3$
2			
3	a	1	0
4	b	-2	1
5	c	-3	-3
6			

Figura 14: Atividade III. Fonte: Arquivo pessoal do autor.

2 - Fazemos uma tabela com valores para x (veja que os valores de x devem ser diferentes de 3, pois $g(x)$ é denominador em $h(x)$), e colocamos uma coluna para cada função.

	A	B	C	D	E	F	G	H
1	Função:	$f(x) = x^2 - 2x - 3$	$g(x) = x - 3$		X	f(x)	g(x)	h(x)
2					-4			
3	a	1	0		-3			
4	b	-2	1		-2			
5	c	-3	-3		-1			
6					0			
7					1			
8					2			
9					4			
10					5			
11					6			

Figura 15 – Atividade III. Fonte: Arquivo pessoal do autor.

3 – Calculamos os valores das funções para cada valor de x .

	A	B	C	D	E	F	G	H
1	Função:	$f(x) = x^2 - 2x - 3$	$g(x) = x - 3$		X	f(x)	g(x)	h(x)
2					-4	21	-7	-3
3	a	1	0		-3	12	-6	-2
4	b	-2	1		-2	5	-5	-1
5	c	-3	-3		-1	0	-4	0
6					0	-3	-3	1
7					1	-4	-2	2
8					2	-3	-1	3
9					4	5	1	5
10					5	12	2	6
11					6	21	3	7

Figura 16: Atividade III. Fonte: Arquivo pessoal do autor.

4 - Para a criação do gráfico, basta selecionar a tabela contendo os valores de x e das funções e acessar: Inserir, Gráficos e Dispersão e selecionar o gráfico Dispersão.

Figura 17: Atividade III. Fonte: Arquivo pessoal do autor.

5 – Agora, clicamos no gráfico que representa $h(x)$ com o botão direito do mouse e selecionamos a opção: **Formatar Linha de Tendência**.

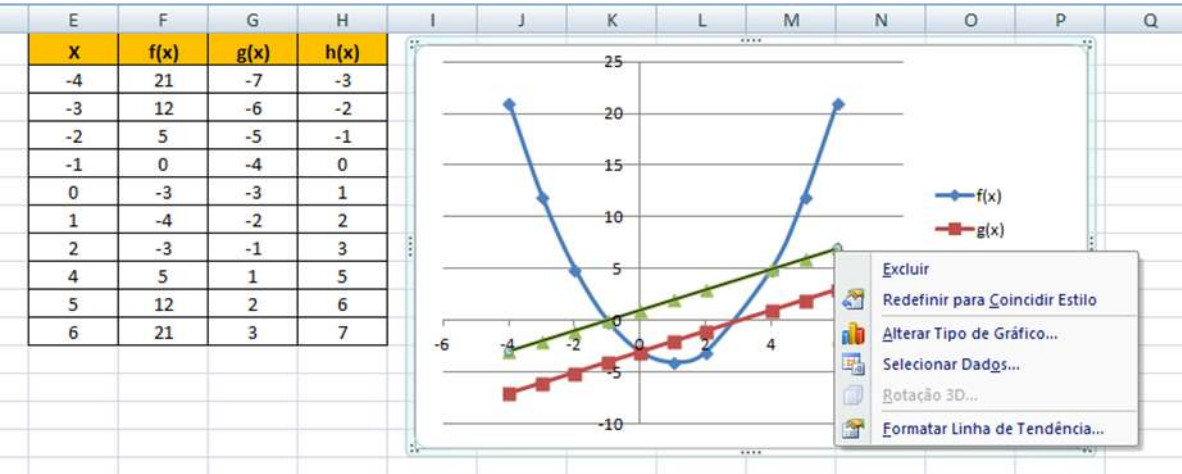


Figura 18: Atividade III. Fonte: Arquivo pessoal do autor

6 – No quadro que abrir, selecionamos a opção: **Exibir Equação no Gráfico**. Logo a equação que representa $h(x)$ aparecerá em sua forma simplificada ao lado do respectivo gráfico.

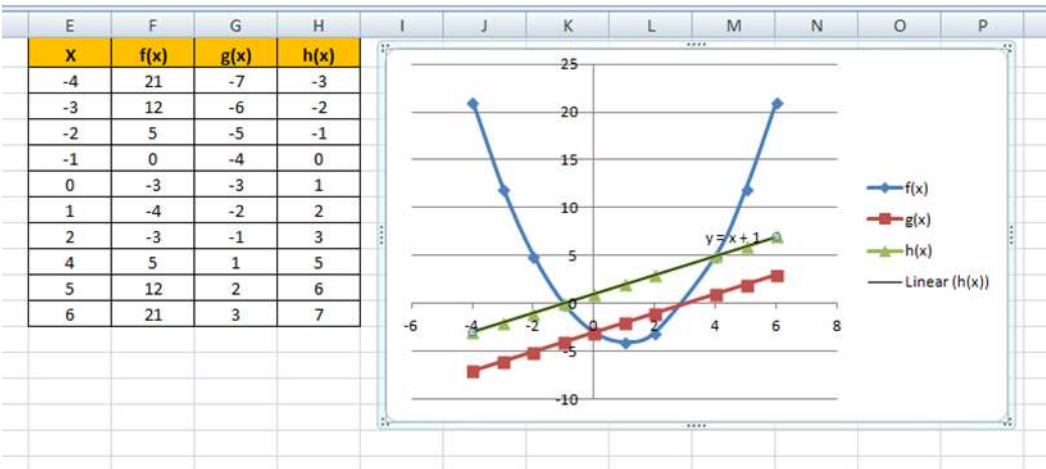


Figura 19: Atividade III. Fonte: Arquivo Pessoal do autor.

d) Atividade IV – Estatística

CONT.NÚM

A função **CONT.NÚM** basicamente conta a quantidade de números existentes em um conjunto de células selecionado. Logo, se desejamos saber a quantidade de números existente na listagem, basta inserir a função CONT.NÚM e selecionar o intervalo de células desejado. Ao término da função basta teclar Enter e conferir o resultado.

	A	B	C	D	E	F	G	H
1	Segunda	Terça	Quarta	Quinta	Sexta			
2	7	11	18	21	26			
3								
4	=CONT.NÚM(A1:G2)							
5	CONT.NÚM(valor1; [valor2]; ...)							

Figura 20: Atividade IV. Fonte: Arquivo pessoal do autor.

	A	B	C	D	E	F	G	H
1	Segunda	Terça	Quarta	Quinta	Sexta			
2	7	11	18	21	26			
3								
4	5							
5								
6								

Figura 21: Atividade IV. Fonte: Arquivo pessoal do autor.

CONT.VALORES

Se quisermos contar todos os dados da planilha exceto os campos vazios, podemos utilizar a função CONT.VALOR que contará todas as células dentro de um intervalo estipulado. Observe um exemplo na figura a seguir.

	A	B	C	D	E
1	Segunda	Terça	Quarta	Quinta	Sexta
2	7	11	18	21	26
3					
4					
5	=CONT.VALORES(A1:E3)				
6	CONT.VALORES(valor1; [valor2]; ...)				

Figura 22: Atividade IV. Fonte: Arquivo pessoal do autor.

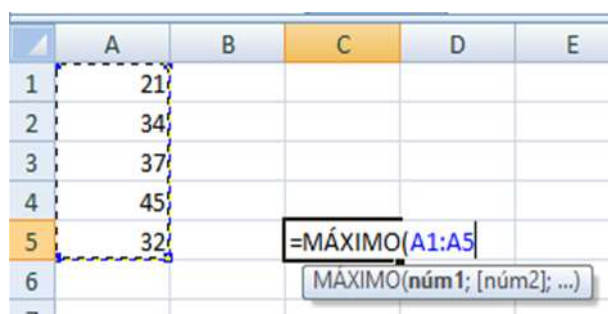
	A	B	C	D	E
1	Segunda	Terça	Quarta	Quinta	Sexta
2	7	11	18	21	26
3					
4					
5	10				
6					

Figura 23: Atividade IV. Fonte: Arquivo pessoal do autor.

Observação: na necessidade de contar somente as células em branco, basta utilizar a função CONT.VAZIO com o mesmo princípio das funções: CONT.NÚM e CONT.VALORES.

MÁXIMO E MÍNIMO

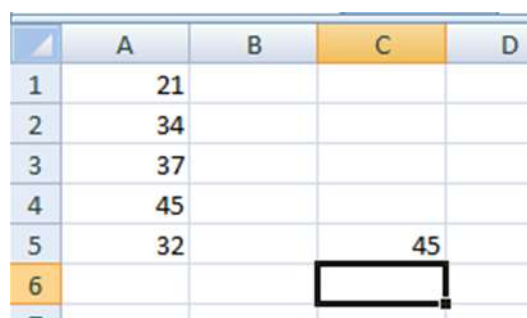
Estas duas funções como os próprios nomes se referem, trazem os valores máximo e mínimo em um intervalo de dados. Neste caso, se quisermos, por exemplo, saber o valor máximo em um intervalo de células, basta aplicar a função conforme mostrado abaixo e conferir o resultado. O mesmo procedimento serve para a função MÍNIMO.



The screenshot shows an Excel spreadsheet with columns A through E and rows 1 through 7. Column A contains the values 21, 34, 37, 45, and 32 in rows 1 to 5 respectively. A dashed blue selection box highlights the range A1:A5. In cell C5, the formula bar shows the formula `=MÁXIMO(A1:A5)`. A tooltip below the formula bar displays the syntax: `MÁXIMO(núm1; [núm2]; ...)`.

	A	B	C	D	E
1	21				
2	34				
3	37				
4	45				
5	32				
6					
7					

Figura 24: Atividade IV. Fonte: Arquivo pessoal do autor.



The screenshot shows the same Excel spreadsheet as Figure 24, but now the result of the formula is visible. The value 45 is displayed in cell C5. Cell C6 is currently selected and is empty.

	A	B	C	D
1	21			
2	34			
3	37			
4	45			
5	32		45	
6				
7				

Figura 25: Atividade IV. Fonte: Arquivo pessoal do autor.

CONT. SE

Esta função faz a contagem de elementos de acordo com um critério pré-estabelecido. **Sintaxe:** `CONT.SE (células; critério)`. Onde, **células** representa o intervalo de células selecionado e **critério** representa o critério que desejamos estabelecer para a contagem.

No exemplo a seguir temos uma sequência numérica aleatória. Porém, desejamos obter a quantidade de valores que estão abaixo de 20. Deste modo, basta utilizar a função conforme mostrado na Figura 26.

	A	B	C	D	E	F
1	21	22				
2	34	23				
3	37	20				
4	45	13				
5	32	14				
6						
7						

=CONT.SE(A1:B5;"<20"
CONT.SE(intervalo; critérios)

Figura 26: Atividade IV. Fonte: Arquivo pessoal do autor.

	A	B	C	D	E	F
1	21	22				
2	34	23				
3	37	20				
4	45	13				
5	32	14				
6						
7						

2

Figura 27: Atividade IV. Fonte: Arquivo pessoal do autor.

MAIOR E MENOR

Estas duas funções são semelhantes às funções MÁXIMO e MÍNIMO. Porém neste caso é possível escolher a ordem de maior ou menor valor que se deseja (exemplo: segundo maior valor, terceiro menor valor e assim por diante).

Sintaxe: Maior ou Menor (matriz; k).Onde, matriz é um intervalo de células desejado e k é a posição do valor que desejamos encontrar.

No exemplo, exibido na figura a seguir, desejamos obter o segundo menor número da lista. Deste modo, aplicaremos a função MENOR.

	A	B	C	D	E
1	21	22			
2	34	23			
3	37	20			
4	45	13			
5	32	14			
6					
7					

=MENOR(A1:B5;2
MENOR(matriz; k)

Figura 28: Atividade IV. Fonte: Arquivo pessoal do autor.

	A	B	C	D
1	21	22		
2	34	23		
3	37	20		
4	45	13		
5	32	14		14
6				

Figura 29: Atividade IV. Fonte: Arquivo pessoal do autor.

MÉDIA

Esta função traz a média de um intervalo de dados. Ou seja, realiza-se a soma entre eles e posteriormente divide-se o total da soma pela quantidade de valores somados. A seguir temos um exemplo simples onde é utilizada esta função.

	A	B	C	D	E
1	Jogo	Gols Marcados			
2	I	5			
3	II	4			
4	III	1			
5	IV	3			
6	V	4			
7					
8					

Média de Gols
=MÉDIA(B2:B6)
MÉDIA(núm1; [núm2]; ...)

Figura 30: Atividade IV. Fonte: Arquivo pessoal do autor.

	A	B	C	D
1	Jogo	Gols Marcados		
2	I	5		
3	II	4		
4	III	1		
5	IV	3		
6	V	4		
7				

Média de Gols
3,4

Figura 31: Atividade IV. Fonte: Arquivo pessoal do autor.

MED

Sabemos que em estatística o termo Mediana representa o valor central em uma amostra de dados ordenados. Deste modo, para calculá-la, basta utilizar a função MED conforme mostrado abaixo:

	A	B	C	D
1	5	6	7	
2	4	6	8	
3	6	7	9	
4				
5	Mediana	=MED(A1:C3)		
6		MED(núm1; [núm2]; ...)		

Figura 32: Atividade IV. Fonte: Arquivo pessoal do autor.

	A	B	C	D
1	5	6	7	
2	4	6	8	
3	6	7	9	
4				
5	Mediana	6		
6				
7				

Figura 33: Atividade IV. Fonte: Arquivo pessoal do autor.

MODOS

Moda refere-se ao valor que é repetido com maior frequência dentro de uma amostra. Deste modo, utiliza-se a função MODOS para encontrar a moda de uma sequência

A figura a seguir apresenta um exemplo que ilustra o uso da função MODOS.

	A	B	C	D
1	5	6	7	
2	4	6	8	
3	6	7	9	
4				
5	Moda	=MODOS(A1:C3)		
6		MODOS(núm1; [núm2]; ...)		
7				

Figura 34: Atividade IV. Fonte: Arquivo pessoal do autor.

	A	B	C
1	5	6	7
2	4	6	8
3	6	7	9
4			
5	Moda	6	
6			

Figura 35: Atividade IV. Fonte: Arquivo pessoal do autor.

DESVPAD

O desvio padrão tem o objetivo de demonstrar o grau de oscilação de uma amostra perante a sua própria média. O cálculo para encontrar o desvio padrão de uma amostra envolve diversas etapas, porém no Excel pode ser simplificado somente com a função DESVPAD.

A figura a seguir apresenta um exemplo de aplicação da função de desvio padrão no Excel.

	A	B	C	D	E
1	5	6	7		
2	4	6	8		
3	6	7	9		
4					
5	Desvio Padrão	=DESVPAD(A1:C3)			
6		DEVPAD(núm1; [núm2]; ...)			
7					

Figura 49: Atividade IV. Fonte: Arquivo pessoal do autor.

	A	B	C
1	5	6	7
2	4	6	8
3	6	7	9
4			
5	Desvio Padrão		1,51

Figura 50: Atividade IV. Fonte: Arquivo pessoal do autor.

6. CONSIDERAÇÕES FINAIS

Dado que o ensino de Matemática na Educação Básica tem se constituído, ao longo dos tempos, um grande desafio para professores e alunos, devido à cultura de que essa disciplina é “um bicho de 7

cabeças”, que Matemática é muito difícil, abstrata etc. Essas questões são repassadas como verdades e os alunos chegam pré-determinados a não aprenderem os conteúdos tão necessários para sua formação cidadã e profissional.

Conclui-se então que é importante que seja possível aos alunos compreenderem esses exercícios como elementos de aprendizagem, por meio da formulação e aquisição de conceitos, de modo que todas as propostas aqui se enquadrem como sugestões de uso do Excel em aulas de Matemática. É possível usar o Excel em qualquer série do ensino básico, e é em decorrência dessa possibilidade que se sugere que não só estas, mas outras atividades sejam utilizadas, de forma que proporcione a aquisição dos conhecimentos obedecendo a série que se pretende elencar atividades desse tipo.

A aprendizagem ocorrerá de maneira significativa se houver relação com as expectativas dos alunos, e por isso é que se pretende com essas sugestões contribuir com a prática pedagógica que se interesse pela realização da aprendizagem dos alunos mediante sua formação.

7. REFERÊNCIAS BIBLIOGRÁFICAS

BOYER, C. B.; História da Matemática, segunda edição, p. 50-56. Editora Edgard Blucher, 1996.

BRASIL. MEC/SEF. Diretrizes Curriculares Nacionais da Educação Básica. Brasília/DF: MEC/SEF, 2013.

BIEMBENGUT, M. S., HEIN, N.; Modelagem Matemática no Ensino. 3ª Ed. São Paulo: Contexto, 2003, 127p

D'AMBROSIO, U. Etnomatemática: arte ou técnica de explicar ou conhecer. 4. Ed. São Paulo: Ática, 1998.

DANTE, L. R. Matemática Contexto & Aplicações. Ensino Médio e Preparação para a Educação Superior. 2ª Edição. São Paulo: Ed. Ática, 2002.

FREIRE, Paulo. A Educação na Cidade. 5. Ed. são Paulo: Cortez, 2001 a.

LOPES, E. J. S., BISOGNIN, C.; O uso do excel como ferramenta no ensino de funções afins. Curso de Especialização em Matemática, Mídias Digitais e Didática para educação básica, 2017.

VASCONCELOS, Celso dos Santos. Avaliação da Aprendizagem: Práticas de

Mudança – Por uma Práxis Transformadora. São Paulo: Libertad, 1998. (Coleção Cadernos Pedagógicos do Libertad, v. 6).

WERNECK, Hamilton. O Profissional do Século XXI. Rio de Janeiro, Record, 2003.

Capítulo 3



10.37423/220305541

ESTUDO DE FUNÇÕES GERADORAS E SUAS APLICAÇÕES EM PROBLEMAS DE ANÁLISE COMBINATÓRIA

Laudelino Gomes Ferreira

Universidade Estadual do Rio Grande do Norte - UERN

Antonio Ronaldo Gomes Garcia

Universidade Federal Rural do Semi-Árido - UFERSA



1 INTRODUÇÃO:

Neste trabalho faremos uma introdução ao estudo das funções geradoras. Esta técnica surgiu no século XV II nos trabalhos de Abraham De Moivre. Os matemáticos Leonhard Euler, Laplace e N. Bernoulli usaram para resolver problemas na teoria de partições, estudo de probabilidade e permutações caóticas respectivamente. O Princípio Fundamental da Contagem é uma ferramenta poderosa na resolução de problemas de análise combinatória, mas, torna-se praticamente impossível aplica-lo a problemas com restrições . Por isso, o principal objetivo desta artigo é apresentar soluções via funções geradoras ordinárias. Mais especificamente, nos concentraremos nos problemas de contagem do número de elementos de um conjunto nos quais a ordem não importe e que a repetição seja permitida.

Este artigo tem como base a dissertação Funções Geradoras: Problemas e Aplicações (FERREIRA, 2018). A dissertação também tratava de problemas de contagem modelados por recorrências lineares de primeira e segunda ordens, onde as funções geradoras foram usadas para resolver tais recorrências.

2- FUNÇÕES GERADORAS ORDINÁRIAS:

Nesta seção definiremos as funções geradoras ordinárias. Esta é a principal ferramenta para a resolução de problemas de contagem em que a ordem dos elementos não é relevante, ou seja, problemas de combinações simples e combinações completas.

Definição 1: Seja $(a_n)_{n \geq 0}$ uma sequência de números reais. A série geradora é dada pela expressão

$$\sum_{n=0}^{\infty} a_n x^n = G(x)$$

$G(x)$ é dita função geradora ordinária e os coeficientes da função geradora nos fornece a solução de um problema de contagem.

Exemplo 1. Seja n um número inteiro positivo. Considere $a_r = \binom{n}{r}$ a quantidade de combinação de n elementos em r posições, onde $0 \leq r \leq n$. Qual a função geradora da sequência $a_0, a_1, \dots, a_n$?

A função geradora ordinária para essa sequência é a seguinte

$$F(x) = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n \quad (1)$$

Que do Teorema Binomial sabemos que é o desenvolvimento de $(1+x)^n$. Também é equivalente ao problema de encontrar o número de maneiras de retirarmos r objetos de um conjunto de n objetos distintos.

O coeficiente $a_0 = \binom{n}{0}$ que está associado a x^0 significa que não foi retirado nenhum objeto. O coeficiente $a_1 = \binom{n}{1}$ que está associado a x significa que foi retirado um objeto e continuando com este raciocínio. O coeficiente $a_n = \binom{n}{n}$ está associado a x^n significa que foram retirados n objetos.

Exemplo 2. Neste exemplo encontraremos a função geradora ordinária $G(x)$ para sequência de Lucas $F_{n+2} = F_n + F_{n+1}$, com $F_1 = 1$ e $F_2 = 3$. Os primeiros termos da sequência de Lucas são : 1; 3; 4; 7; 11; 18; ... Temos, então que a função geradora ordinária para essa sequência é

$$G(x) = x + 3x^2 + 4x^3 + 7x^4 + 11x^5 + 18x^6 + \cdots \quad (2)$$

3-UM POUCO DE CÁLCULO DIFERENCIAL E INTEGRAL

Note que as funções geradoras (1) e (2) são séries de potências. Na perspectiva da análise combinatória estamos interessados apenas no cálculo dos coeficientes destas funções. Por isso, trabalharemos com as séries formais, ou seja, estudaremos as séries sem nos preocupar com as questões de convergência (sobre séries formais veja (NIVEN, 1969)).

Logo, a conhecida fórmula de série geométrica é dada por

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots, \text{ para } |x| < 1, \quad (3)$$

substituindo x por x^2 em (3), obtemos:

$$\frac{1}{1-x^2} = 1 + x^2 + x^4 + x^6 + \cdots, \text{ para } |x| < 1. \quad (4)$$

e, se substituirmos x por x^3 em (3), obtemos:

$$\frac{1}{1-x^3} = 1 + x^3 + x^6 + x^9 + \dots, \text{ para } |x| < 1. \quad (5)$$

4-DETERMINAÇÃO DOS COEFICIENTES

Nesta seção, discutiremos as principais formas de calcularmos os coeficientes de uma função geradora. Note que, da **Definição 1**, temos que uma função geradora ordinária é uma função polinomial de grau n . Do cálculo diferencial e integral temos que funções polinomiais são deriváveis e integráveis.

Teorema 1. Sendo $F(x)$ e $G(x)$ as funções geradoras das sequências $(a_r)_r$ e $(b_r)_r$, respectivamente, e $A, B \in \mathbb{R}$, temos:

- (i) $AF(x) + BG(x)$ é a função geradora para a sequência $(Aa_r + Bb_r)_r$;
- (ii) $F(x) \cdot G(x) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n (a_k b_{n-k}) \right) x^n$;
- (iii) A função geradora para $(a_0 + a_1 + \dots + a_r)_r$ é igual $(1 + x + x^2 + \dots)F(x)$.
- (iv) A função geradora para $(ra_r)_r$ é igual a $xF'(x)$, onde $F'(x)$ é a derivada de f com relação a x ;
- (v) $\int F(x)dx = \sum_{n=0}^{\infty} \frac{a_n}{n+1} x^{n+1}$, $n \neq -1$.

Demonstração: Sejam $F(x)$ dada pela série:

$$\sum_{n=0}^{\infty} a_n x^n$$

e $G(x)$ dada pela série

$$\sum_{n=0}^{\infty} b_n x^n$$

Funções geradoras para sequencias (a_n) e (b_n) respectivamente (i)

$$\begin{aligned}
 Af(x) + Bg(x) &= A(a_0 + a_1x + a_2x^2 + \dots) + B(b_0 + b_1x + b_2x^2 + \dots) \\
 &= (Aa_0 + Bb_0) + (Aa_1 + Bb_1)x + (Aa_2 + Bb_2)x^2 + \dots \\
 &= \sum_{k=0}^{\infty} (Aa_k + Bb_k)x^k.
 \end{aligned}$$

Portanto, $AF(x) + BG(x)$ é uma sequência geradora para determinada pela soma: $Aa_r + Bb_r$. Note que (ii)

$$\begin{aligned}
 F(x)G(x) &= (a_0b_0) + (a_0b_1 + a_1b_0)x + \dots + (a_0b_n + a_1b_{n-1} + \dots + a_nb_0)x^n + \dots \\
 &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^n (a_kb_{n-k}) \right) x^n.
 \end{aligned}$$

Tomando $b_r = 1$, segue de (ii) que:

$$\begin{aligned}
 F(x)G(x) &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^n (a_k \cdot 1) \right) x^n \\
 &= \sum_{n=0}^{\infty} \left(\sum_{k=0}^n (a_k) \right) x^n
 \end{aligned}$$

Portanto, fica demonstrado o resultado.

(iv) Considerando a derivada termo a termo, segue

$$(iv) \text{ Sendo } F'(x) = \sum_{r=1}^{\infty} ra_r x^{r-1}, \text{ segue que}$$

$$xF'(x) = \sum_{r=1}^{\infty} ra_r x^r$$

Dado que (v) é imediato, temos que são validos todos os resultados apontados no Teorema 1.

□

Agora vamos apresentar o segundo teorema do assunto, que traz mais uma ferramenta para o estudo de determinação de coeficientes da funções geradoras. O Teorema a seguir, que é de fato uma

generalização do Teorema Binomial, é muito útil na determinação de coeficientes de funções geradoras.

Teorema 2 (Teorema Binomial Generalizado). *Seja u um número real qualquer. Assim, temos*

$$(1+x)^u = \binom{u}{0} + \binom{u}{1}x + \binom{u}{2}x^2 + \cdots + \binom{u}{k}x^k + \cdots = \sum_{k=0}^{\infty} \binom{u}{k}x^k$$

onde

$$\binom{u}{k} = \begin{cases} \frac{u(u-1)(u-2)\cdots(u-k+1)}{k!}, & \text{se } k > 0 \\ 1, & \text{se } k = 0 \end{cases}$$

Demonstração. Veja (STEWART, 2014). □

Exemplo 3: Usaremos o Teorema 2 sobre a sequência cuja função geradora é dada por:

$$G(x) = \frac{1}{(1-x)^4}.$$

Note que $G(x) = \frac{1}{(1-x)^4} = (1-x)^{-4}$. Aplicando o Teorema 2, temos

$$(1-x)^{-4} = 1 + (-4) \cdot (-x) + \frac{(-4)(-4-1)}{2}(-x)^2 + \cdots,$$

ou seja,

$$(1-x)^{-4} = 1 + 4x + 10x^2 + 20x^3 + 35x^4 + 56x^5 + 84x^6 + 120x^7 + \cdots.$$

Portanto, $G(x)$ é a função geradora da sequência: $(a_r) = (1, 4, 10, 20, 35, 56, 84, 120, \dots)$.

O próximo resultado é um teorema que também permite facilitar muito o trabalho na determinação de coeficientes de funções geradoras.

Teorema 3. (i) seja a_r o coeficiente de x^r na função geradora ordinária

$$G(x) = (1 + x + x^2 + x^3 + \dots)^n,$$

$$\text{então } a_r = \binom{r+n-1}{r};$$

$$(ii) (1 - x^m)^n = 1 - \binom{n}{1}x^m + \binom{n}{2}x^{2m} - \dots + (-1)^n x^{nm}$$

$$(iii) (1 + x + x^2 + x^3 + \dots + x^{m-1})^n = (1 - x^m)^n (1 + x + x^2 + \dots)^n.$$

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1-x}, \text{ ou seja,}$$

Demonstração: Da equação (3) temos que

Aplicando o Teorema 2, e substituindo x por $-x$ e n por $-n$, temos

$$(1 - x)^{-n} = \sum_{r=0}^{\infty} \binom{-n}{r} (-x)^r = \sum_{r=0}^{\infty} \binom{-n}{r} (-1)^r x^r, \quad (6)$$

Sendo que

$$\begin{aligned} \binom{-n}{r} &= \frac{(-n)(-n-1)(-n-2)\dots(-n-r+1)}{r!} \\ &= (-1)^r \frac{(n)(n+1)(n+2)\dots(n+r-1)}{r!} \\ &= (-1)^r \frac{(n+r-1)\dots(n+1)n(n-1)!}{r!(n-1)!} \\ &= (-1)^r \binom{n+r-1}{r} \end{aligned}$$

Substituindo em (6), obtemos

$$G(x) = (1 + x + x^2 + x^3 + \dots)^n = \sum_{r=0}^{\infty} \binom{n+r-1}{r} x^r$$

Portanto, $a_r = \binom{n+r-1}{r}$.

(ii) No desenvolvimento binomial de $(1 + t)^n$ temos:

$$(1+t)^n = \binom{n}{0} + \binom{n}{1}t + \binom{n}{2}t^2 + \binom{n}{3}t^3 + \dots + \binom{n}{n}t^n$$

Faça $t = (-x^m)$,

$$(1-x^m)^n = \binom{n}{0} + \binom{n}{1}(-x^m) + \binom{n}{2}(-x^m)^2 + \binom{n}{3}(-x^m)^3 + \dots + \binom{n}{n}(-x^m)^n$$

$$(1-x^m)^n = 1 - \binom{n}{1}x^m + \binom{n}{2}x^{2m} - \binom{n}{3}x^{3m} + \dots + (-1)^n x^{mn}$$

Portanto, segue a validade do item (ii).

Para demonstrarmos (iii), note que

$$1 + x + x^2 + x^3 + \dots + x^{m-1} = (1-x^m)(1+x+x^2+x^3+\dots)$$

Elevando ambos os membros à n -ésima potência, segue

$$(1+x+x^2+x^3+\dots+x^{m-1})^n = (1-x^m)^n(1+x+x^2+x^3+\dots)^n$$

Portanto, o resultado (iii) do teorema é válido



Exemplo 4: Vamos determinar o coeficiente de x^{27} no desenvolvimento de

$$(x^3 + x^4 + x^5 + \dots)^6.$$

Inicialmente, note que

$$(x^3 + x^4 + x^5 + \dots)^6 = x^{18} \cdot (1 + x + x^2 + \dots)^6$$

ou seja,

$$(x^3 + x^4 + x^5 + \dots)^6 = x^{18} \cdot (1 + x + x^2 + \dots)^6$$

Usando a equação (3), tem-se que

$$(x^3 + x^4 + x^5 + \dots)^6 = x^{18} \cdot (1-x)^{-6}$$

Como queremos o coeficiente de x^{27} , temos que o fator $(1-x)^{-6}$ deve contribuir com o fator x^9 . É importante notar que não há condições para aplicar o Teorema 2, pois seria necessário muitos cálculos para chegarmos no coeficiente de x^9 . Podemos usar o item (i) do Teorema 3 e obtermos o coeficiente de forma mais rápida

$$\begin{aligned} a_r &= \binom{r+n-1}{r} \\ &= \binom{9+6-1}{9} \\ &= \binom{14}{9} \Rightarrow a_9 = 2002. \end{aligned}$$

Portanto, o coeficiente de x^{27} é exatamente 2002.

5-APLICAÇÕES

Nesta seção apresentamos a resolução de alguns problemas de contagem que possuem alguma restrição em seu enunciado. São problemas resolvidos com aplicação direta das funções geradoras.

Problema 1: (a) Considere o problema de determinar a função geradora para a sequência (a_k) onde a_k é o número de soluções inteiras de $x_1 + x_2 + x_3 = k$, onde x_1, x_2 e x_3 são inteiros com $x_1 > 1, 0 \leq x_2 < 4$ e $1 < x_3 < 6$?

(b) Utilize sua resposta do item (a) para determinar o coeficiente a_6 .

Solução: Seja $F_1(x) = x^2 + x^3 + x^4 + \dots$ a função geradora que associa x^2 a x_1 , associa x^3 a x_2 e associa x^n a x_n . Para a condição $0 \leq x_2 < 4$ temos a representação finita $F_2(x) = 1 + x + x^2 + x^3$, para a condição $1 < x_3 < 6$ temos a representação $F_3(x) = x^2 + x^3 + x^4 + x^5$ como função geradora. Logo fazendo o produto das três funções obtemos:

$$\begin{aligned} F_1(x)F_2(x)F_3(x) &= (x^2 + x^3 + x^4 + \dots) \cdot (1 + x + x^2 + x^3) \cdot (x^2 + x^3 + x^4 + x^5) \\ &= x^2(1 + x + x^2 + \dots) \cdot (1 + x + x^2 + x^3) \cdot x^2(1 + x + x^2 + x^3) \\ &= x^4(1 + x + x^2 + \dots) \cdot (1 + x + x^2 + x^3)^2. \end{aligned}$$

Segue que a função geradora que resolve o problema é dada por:

$$F(x) = \frac{x^4(1+x+x^2+x^3)^2}{1-x}$$

Observe que $(1-x)^{-3}$ contribui com x^2 . Assim basta determinarmos o coeficiente de x^2 no termo, ou seja:

$$a_6 = \binom{3+2-1}{2} = 6 \Rightarrow a_6 = 6.$$

Problema 2: Encontrar o número de maneiras de se obter um total de 15 pontos ao se jogar, simultaneamente, quatro dados diferentes.

Solução: Seja $F(x) = x + x^2 + x^3 + x^4 + x^5 + x^6$ a função geradora para os possíveis resultados do lançamento de um dado. A possibilidade de dar 1 no lançamento de um dado está associado a x , para o resultado 2 estar associado a x^2 . Logo, tem-se

$$\begin{aligned} G(x) &= (x + x^2 + x^3 + x^4 + x^5 + x^6)^4 \\ &= [x(1 + x + x^2 + x^3 + x^4 + x^5)]^4 \\ &= x^4 \cdot (1 + x + x^2 + x^3 + x^4 + x^5)^4 \\ &= x^4 \cdot \frac{(1 - x^6)^4}{(1 - x)^4} \\ &= x^4 \cdot (1 - x^6)^4 \cdot (1 - x)^{-4} \\ &= x^4 \cdot (1 - 4x^6 + 6x^{12} - 4x^{18} + x^{24}) \cdot (1 - x)^{-4}, \end{aligned}$$

ou seja,

$$G(x) = (x^4 - 4x^{10} + 6x^{16} - 4x^{22} + x^{28}) \cdot (1 - x)^{-4}. \quad (7)$$

Em (7) o fator $(1-x)^{-4}$ contribui com x^5 e x^{11} , assim aplicando o item (i) do Teorema 3, obtemos

- $a_5 = \binom{4+5-1}{5} = \binom{8}{5} = 56;$
- $a_{11} = \binom{4+11-1}{11} = \binom{14}{11} = 364.$

Portanto, existe um total de $364 - 4.56 = 140$ maneiras de se obter um total de 15 pontos no lançamento simultâneo de quatro dados.

Problema 3: De quantas formas diferentes se pode selar uma encomenda com o valor total de n Euros sabendo que se tem à disposição selos de 1 Euro e selos de 2 Euros? Depois de obter a expressão para o caso geral, indique o valor para o caso particular de 8 Euros.

Solução: Considere S_n o número de formas de se selar uma encomenda com n euros. Com 1 pode-se selar apenas uma encomenda, logo $S_1 = 1$. Com 2 Euros podemos selar uma encomenda de 2 Euros, ou duas encomendas de um euro, ou seja $S_2 = 2$. Seguindo o raciocínio, com 3 Euros podemos selar três encomendas de um Euro, ou uma encomenda de um Euro e outra de 2 Euros. Ou seja, $S_3 = 2$.

Podemos resolver o problema usando a técnica das funções geradoras para determinarmos uma fórmula para esse problema. Assim, sejam

$$E_1(x) = 1 + x + x^2 + x^3 + \dots \text{ e } E_2(x) = 1 + x^2 + x^4 + x^6 + \dots$$

as funções geradoras para os selos de 1 e 2 Euros, respectivamente. Logo, tem-se a equação

$$E_1(x) \cdot E_2(x) = (1 + x + x^2 + x^3 + \dots) \cdot (1 + x^2 + x^4 + x^6 + \dots), \quad (8)$$

Fazendo uso das equações (3), (4) e (8), obtemos

$$\begin{aligned} E_1(x) \cdot E_2(x) &= \frac{1}{1-x} \cdot \frac{1}{1-x^2} \\ &= \frac{1}{(1-x)} \cdot \frac{1}{(1-x)(1+x)} \end{aligned}$$

ou seja, uma relação que pode ser expressa por:

$$E_1(x) \cdot E_2(x) = \frac{1}{(1+x)(1-x)^2}. \quad (9)$$

Escrevendo as frações parciais associadas a (9), temos

$$\frac{1}{(1+x)(1-x)^2} = \frac{A}{(1+x)} + \frac{B}{(1-x)} + \frac{C}{(1-x)^2}$$

Resolvendo o sistema, obtemos os valores de A, B e C

$$A = \frac{1}{4}, B = \frac{1}{4} \text{ e } C = \frac{1}{2}$$

Portanto,

$$\frac{1}{(1+x)(1-x)^2} = \frac{1}{4} \frac{1}{(1+x)} + \frac{1}{4} \frac{1}{(1-x)} + \frac{1}{2} \frac{1}{(1-x)^2}.$$

Substituindo na equação (9), temos

$$E_1(x) \cdot E_2(x) = \frac{1}{4} \frac{1}{(1+x)} + \frac{1}{4} \frac{1}{(1-x)} + \frac{1}{2} \frac{1}{(1-x)^2}. \quad (10)$$

Observe que a identidade descrita a seguir

$$\frac{1}{1+x} = \sum_{k=0}^{\infty} (-1)^k x^k.$$

Permite que identiquemos o coeficiente de x^n sendo $(-1)^n$, enquanto na identidade dada por

$$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k$$

fica claro que o coeficiente de x^n sendo 1.

Para o termo $(1-x)^{-2}$ aplicamos o item (i) do Teorema 3, o obtemos

$$a_k = \binom{k+2-1}{k} = \binom{k+1}{k} \Rightarrow a_k = k+1$$

Agora, observe que na expressão

$$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1)x^k$$

o coeficiente de x^n é exatamente $n+1$. Substituindo todos os coeficientes na equação (10), obtemos

$$\begin{aligned} E_1(x) \cdot E_2(x) &= \frac{1}{4} \frac{1}{(1+x)} + \frac{1}{4} \frac{1}{(1-x)} + \frac{1}{2} \frac{1}{(1-x)^2} \\ &= \sum_{n=0}^{+\infty} \left[\frac{1}{4} (-1)^n + \frac{1}{4} \cdot 1 + \frac{1}{2} \cdot (n+1) \right] x^n \\ &= \sum_{n=0}^{+\infty} \left[\frac{(-1)^n + 1 + 2(n+1)}{4} \right] x^n \\ &= \sum_{n=0}^{+\infty} \left[\frac{(-1)^n + 2n + 3}{4} \right] x^n \end{aligned}$$

Assim, podemos obter a representação para S_n , dada por

$$S_n = \frac{(-1)^n + 2n + 3}{4}$$

Portanto, temos uma expressão que nos dá a quantidade de formas diferentes que se pode selar uma encomenda com n Euros. Em particular para $n = 8$ Euros, temos $S_8 = \frac{(-1)^8 + 2 \cdot 8 + 3}{4} = 5$ maneiras distintas de selar.

Problema 4: Numa competição, cada um dos quatro juízes deve atribuir notas de 1 a 6 para cada participante. Para ser finalista, um participante deve ter no mínimo 22 pontos. Encontrar o número de maneiras que os juízes têm para atribuir notas de modo que um participante seja finalista.

Solução: Considere $J_1(x), J_2(x), J_3(x)$ e $J_4(x)$ as funções geradoras para as notas que juízes devem atribuir. Cada função geradora é da forma

$$J_i(x) = x + x^2 + x^3 + x^4 + x^5 + x^6,$$

onde $1 \leq i \leq 4$ identifica a nota de cada juiz.

Seja $G(x)$ a função que modela o problema. Logo, tem-se

$$\begin{aligned} G(x) &= J_1(x) \cdot J_2(x) \cdot J_3(x) \cdot J_4(x) \\ &= (x + x^2 + x^3 + x^4 + x^5 + x^6)^4 \\ &= [x \cdot (1 + x + x^2 + x^3 + x^4 + x^5)]^4 \\ &= x^4 \cdot (1 + x + x^2 + x^3 + x^4 + x^5)^4 \\ &= x^4 \cdot \left(\frac{1 - x^6}{1 - x} \right)^4, \end{aligned}$$

Ou seja a função é dada por

$$G(x) = x^4 \cdot (1 - x^6)^4 \cdot (1 - x)^{-4}. \quad (11)$$

Observe que o desenvolvimento do termo central de (11)

$$(1 - x^6)^4 = x^{24} - 4x^{18} + 6x^{12} - 4x^6 + 1$$

Ao substituirmos essa forma expandida na equação (11), temos

$$G(x) = (x^{28} - 4x^{22} + 6x^{16} - 4x^{10} + x^4) \cdot (1 - x)^{-4}. \quad (12)$$

Como os quatro juízes atribuem sempre notas de 1 a 6, temos que um participante poderá ter no máximo 24, e como para ser finalista deve ter no mínimo 22 pontos temos três casos para analisar: o número de maneiras que os juízes tem para atribuir notas de modo que o participante tenha 22, 23 ou 24 pontos. Vamos analisar cada possibilidade:

1º. Caso: Quantidade de maneiras de um candidato obter 22 pontos. Nessa situação o fator $(1 - x)^{-4}$ contribui nos termos x^6, x^{12} e x^{18} . Agora, precisamos determinar os coeficientes para estes termos, para isso usaremos o item (i) do Teorema 3. Temos

$$a_6 = \binom{4+6-1}{6} = \binom{9}{6} = 84;$$

$$a_{12} = \binom{4+12-1}{12} = \binom{15}{12} = 455;$$

$$a_{18} = \binom{4+18-1}{18} = \binom{21}{18} = 1330.$$

Logo, há exatamente 10 maneiras para o candidato obter 22 pontos, pois:

$$-4 + 6 \cdot 84 - 4 \cdot 455 + 1330 = 10$$

2º. Caso: Quantidade de maneiras de um candidato obter 23 pontos. Para que um participante obtenha 23 o fator $(1-x)^{-4}$ contribui com os termos x , x^7 , x^{13} e x^{19} . Assim, os coeficientes são exatamente:

$$\bullet a_1 = \binom{4+1-1}{1} = \binom{4}{1} = 4;$$

$$\bullet a_7 = \binom{4+7-1}{7} = \binom{10}{7} = 120;$$

$$\bullet a_{13} = \binom{4+13-1}{13} = \binom{16}{13} = 560;$$

$$\bullet a_{19} = \binom{4+19-1}{19} = \binom{22}{19} = 1540.$$

Logo, há exatamente 4 maneiras para o candidato obter 23 pontos, pois:

$$-4 \cdot 4 + 6 \cdot 120 - 4 \cdot 560 + 1540 = 4$$

3º. Caso: Quantidade de maneiras de um candidato obter 24 pontos. Para que um participante obtenha 24 o fator $(1-x)^{-4}$ contribui com os termos x^2 , x^8 , x^{14} e x^{20} . Assim temos:

$$\bullet a_2 = \binom{4+2-1}{2} = \binom{5}{2} = 10;$$

$$\bullet a_8 = \binom{4+8-1}{8} = \binom{11}{8} = 165;$$

$$\bullet a_{14} = \binom{4+14-1}{14} = \binom{17}{14} = 680;$$

$$\bullet a_{20} = \binom{4+20-1}{20} = \binom{23}{20} = 1771.$$

Logo, como era de se esperar, há exatamente 1 maneiras para o candidato obter 24 pontos, pois:

$$-4 \cdot 10 + 6 \cdot 165 - 4 \cdot 680 + 1771 = 1$$

Portanto, há um total de $15 = 10 + 4 + 1$ maneiras dos quatro juizes distribuirem notas .

Problema 5: Trata-se de uma questão que já fez parte do exame de ingresso no ITA-2021. Pretende-se distribuir 48 balas em 4 tigelas designadas pelas letras A, B, C e D . De quantas maneiras pode-se fazer essa distribuição de forma que todas as tigela contenham ao menos 3 balas e a tigela B contenha a mesma quantidade que a tigela D . As alternativas apresentadas foram:

- (a) 190
- (b) 361
- (c) 722
- (d) 1083
- (e) 1444

Solução: Seja B_n a sequência que conta o número de maneiras de distribuir as n balas em quatro tigelas. Sejam x_1, x_2, x_3 e x_4 as quantidades de balas nas tigelas A, B, C e D , respectivamente. Logo,

$$x_1 + x_2 + x_3 + x_4 = 48 \tag{13}$$

Como em cada tigela deve conter pelos menos três balas, tem-se $x_i \geq 3$ para $0 \leq i \leq 4$ e não esquecendo a restrição de que a tigela B contenha a mesma quantidade balas que a tigela D . Note que $x_i - 3 \geq 0$ para $0 \leq i \leq 4$. Logo tomando $y_i = x_i - 3$ temos que $x_i = y_i + 3$ para $0 \leq i \leq 4$, substituindo em (13), temos:

$$x_1 + x_2 + x_3 + x_4 = 48$$

$$(y_1 + 3) + (y_2 + 3) + (y_3 + 3) + (y_2 + 3) = 48$$

ou seja,

$$y_1 + 2y_2 + y_3 = 36 \quad (14)$$

Note que a série de potências cujos expoentes são os possíveis valores de y_1 e y_3 é $1 + x + x^2 + x^3 + \dots$, por outro lado $2y_2$ é par, temos a seguinte série: $1 + x^2 + x^4 + \dots$, logo a função geradora ordinária é dada por

$$G(x) = (1 + x + x^2 + x^3 + \dots) \cdot (1 + x^2 + x^4 + \dots) \cdot (1 + x + x^2 + x^3 + \dots)$$

$$G(x) = (1 + x + x^2 + x^3 + \dots)^2 \cdot (1 + x^2 + x^4 + \dots)$$

$$G(x) = \left(\frac{1}{1-x} \right)^2 \cdot \frac{1}{1-x^2}$$

ou seja,

$$G(x) = \frac{1}{(1+x)(1-x)^3} \quad (15)$$

Decompondo a expressão de $G(x)$ em frações parciais

$$G(x) = \frac{1}{8} \cdot \frac{1}{1+x} + \frac{1}{8} \cdot \frac{1}{1-x} + \frac{1}{4} \cdot \frac{1}{(1-x)^2} + \frac{1}{2} \cdot \frac{1}{(1-x)^3} \quad (16)$$

Assim podemos obter os coeficientes

$$\frac{1}{1+x} = \sum_{k=0}^{\infty} (-1)^k x^k$$

ou seja, o coeficiente de x^n é exatamente $(-1)^n$. Enquanto a expressão

$$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k,$$

nos aponta que o coeficiente de x^n é exatamente 1. Agora aplicando o item (i) do Teorema 3, para os termos $(1-x)^{-2}$ e $(1-x)^{-3}$ obtemos

$$a_k = \binom{k+2-1}{k} = \binom{k+1}{k} \Rightarrow a_k = k+1,$$

Portanto o coeficiente é $n+1$.

$$\frac{1}{(1-x)^3} = \sum_{r=0}^{\infty} \binom{3+r-1}{r} x^r$$

ou seja:

$$a_r = \frac{(r+1)(r+2)}{2}$$

assim o coeficiente é

$$\frac{(n+1)(n+2)}{2}.$$

Agora, substituindo na equação (16), obtemos

$$B_n = \frac{1}{8} \cdot (-1)^n + \frac{1}{8} \cdot 1 + \frac{1}{4} \cdot (n+1) + \frac{1}{2} \cdot \frac{(n+1)(n+1)}{2}$$

Portanto, de forma mais reduzida temos

$$B_n = \frac{2n^2 + 8n + 7 + (-1)^n}{8}$$

Tomando $n = 36$, obtemos

$$B_{36} = \frac{2 \cdot 36^2 + 8 \cdot 36 + 7 + (-1)^{36}}{8} \Rightarrow B_{36} = 361,$$

Portanto, há 361 maneiras de distribuir 48 balas em quatro tigelas com as restrições impostas.

6-CONSIDERAÇÕES FINAIS

Uma função geradora é uma série formal que organiza uma sequência numérica. Neste trabalho aplicamos tais funções em problemas de análise combinatória nos quais a ordem não importa, ou seja, as combinações completas (ou combinações com repetições). Portanto, as funções geradoras se mostram muito eficientes na resolução de problemas de contagem com restrições. Isso se dá, principalmente, por trabalhar com a teoria algébrica das séries formais. Essas séries nos permitem a adição, multiplicação e a decomposição em frações parciais de funções.

7. REFERÊNCIAS

- BACHX, A. de C., POPPE, L. M. B. , TAVARES, R. Prelúdio à análise combinatória, Companhia Editora Nacional, São Paulo, SP, 1975.
- CARVALHO, P. C. P., MORGADO, A. de O. Matemática Discreta, Sociedade Brasileira de Matemática, Rio de Janeiro, RJ, 2015.
- COSTA, J. F., GOUVEIA, P. Matemática Discreta: A Caixa de Ferramentas, IST Universidade de Lisboa, Lisboa, Portugal 2015.
- FERREIRA, L. G. Funções Geradoras : Problemas e Aplicações. Mossoró / RN. 75 páginas. Dissertação (Mestrado em Matemática). Universidade Federal Rural do Semi-Árido. 2018.
- GROSS, J. L . Combinatorial methods with computer applications, Chapman and Hall/CRC, 2016.
- LANDO, S. K. Lectures on generating functions, American Mathematical Soc.,2003.
- LIMA, E. L. Análise Real, Sociedade Brasileira de Matemática, Rio de Janeiro, RJ, 2004.
- LIMA, P. C. de. Fundamentos de Análise I, CAED-UFMG, Belo Horizonte , MG, 2013.
- MACIEL, A. B., LIMA, O. A. Introdução à Análise Real,EDUEP, Campina Grande, PB, 2005.
- MORGADO, A. C. de O., CARVALHO, J. B. P., CARVALHO P. C. FERNANDEZ, P. Análise combinatória e probabilidade, Sociedade Brasileira de Matemática, Rio de Janeiro, RJ, 2006.
- NIVEN, I. M. Formal Power Series. Amer. Math. Monthly 76, 1969, p. 871-889.
- SANTOS, J.P.O. , MELLO, M. P. , MURARUI, I. T. C. Introdução à Análise Combinatória, Editora Ciência Moderna, Rio de Janeiro / RJ, 2007.
- STEWART, J. Cálculo: volume II,CENGAGE Learning, São Paulo, SP, 2014.

Capítulo 4



10.37423/220305623

FUNÇÕES LINEARES NO ESTUDO DO SISTEMA DE CORES RGB

Lucas Oliveira Ferreira

*Universidade Federal Rural do Semi-Árido -
UFERSA*

Walter Martins Rodrigues

*Universidade Federal Rural do Semi-Árido -
UFERSA*



1. INTRODUÇÃO

Segundo o PCN Parâmetros Curriculares Nacionais (1999) quanto mais se implementa o processo de globalização, mais a Educação deve se preocupar com o desenvolvimento das capacidades de comunicação, de resolver problemas, de tomar decisões, de criar, de aperfeiçoar conhecimentos e valores, e trabalhar cooperativamente.

O PCN preocupa ainda com a relação entre Matemática e tecnologia, ressaltando que embora seja comum, quando há referência às tecnologias ligadas à Matemática, tomar por base a informática e o uso de calculadoras, estes instrumentos, não obstante sua importância, de maneira alguma constituem o centro da questão.

Destacamos ainda, o estudo dos sistemas lineares no ensino superior, onde surgem fortemente em conteúdo de Álgebra Linear e no Cálculo Numérico, e onde vemos também sua aplicação em diversas áreas como Engenharia, Economia, Física e Biologia.

Nestes contextos, este trabalho busca associar sistemas de equações lineares ao uso de tecnologias, explorando o sistema de cores RGB e o uso de calculadora para solução dos sistemas propostos. O trabalho foi implementado em forma de uma oficina aplicada na Escola Estadual de Educação Profissional Professor Walquer Cavalcante Maia, no Ceará, com alunos do 2º ano do ensino médio mostrando a relação entre as cores do sistema RGB e os sistemas de equação lineares.

2. DESENVOLVIMENTO

Neste capítulo temos como objetivo apresentar os conceitos básicos de matrizes e sua associação aos sistemas lineares, bem como falar sobre a solução de um sistema linear. Abordaremos ainda os espaços vetoriais, as características de seus elementos e quais são as condições necessárias para obtê-los. Sabemos que as matrizes são ferramentas fundamentais no desenvolvimento da álgebra linear, são aplicadas na resolução de sistemas de equações lineares e também representam transformações lineares entre espaços vetoriais.

O termo matriz já havia sido usado antes por James Joseph Sylvester (1814 - 1897) em 1850. Neste trabalho Cayley notou que a multiplicação de matrizes, como ele definiu, simplificava o estudo dos sistemas de equações lineares. Também notou que o produto entre matrizes não apresentava propriedades importantes, como a comutatividade e a lei do corte, e que uma matriz não nula não é

necessariamente invertível. Quanto as matrizes Cayley introduziu-as para simplificar a notação de uma transformação linear. Assim, ao invés de escrever

$$\begin{cases} x' = ax + by \\ y' = cx + dy \end{cases}$$

Escrevia

$$(x', y') = \begin{bmatrix} a & b \\ c & d \end{bmatrix} (x, y).$$

2.1 SISTEMA DE EQUAÇÕES LINEARES

Segundo lezzi (2016) a observação de duas transformações lineares sucessivas deu-lhe a ideia de produto de matrizes. Em um outro artigo, três anos depois, Cayley introduziu a adição de matrizes e o produto de matrizes por escalar.

Ao desenvolver a teoria das matrizes, o objetivo de Cayley era formar uma estrutura algébrica, nos séculos XX e XXI apareceriam inúmeras aplicações para matrizes. Se a ideia de matriz precede a de determinante, historicamente ocorreu o contrário, pois os determinantes já eram usados pelos Babilônios na solução de sistemas de equações.

Desde a antiguidade, muitos problemas de diversas áreas do conhecimento eram modelados matematicamente por sistemas de equações lineares, tema este que abordaremos a seguir. De acordo com Filho (2013) solução simultânea de um conjunto de equações é um problema fundamental na descrição matemática de alguns fenômenos, que ocorre com frequência. Explicando numa linguagem matemática, esses fenômenos são expostos por um conjunto com m equações em que se aspira encontrar a solução de n incógnitas.

Filho (2013) afirma que era comum os chineses usarem barras de bambu para escrever seus coeficientes e representarem os sistemas lineares sobre os quadrados de um tabuleiro. Surge daí o método de resolução por eliminação que, por meio de operações elementares, anulam-se coeficientes. Exemplos assim são encontrados no Chiu Chang Suan-Shu.

O Chiu Chang Suan-Shu ou Nove Capítulos sobre a Arte Matemática (ou simplesmente Nove Capítulos), composto por volta de 250 a.C., e possivelmente o mais influente livro de matemática chinês, contém 246 problemas sobre assuntos matemáticos diversos como propriedades dos triângulos retângulos,

agricultura, impostos, solução de equações (BOYER, 2010). Esse estudo evoluiu, com a colaboração de diversos matemáticos, como Gabriel Cramer ao resolver um sistema de equações num caso específico. Esse trabalho obteve um aprofundamento com Jacobi (FILHO; SILVA, 2003).

Carl Friedrich Gauss (1777 – 1855) criou um método sistemático e eficaz para resolver sistemas lineares, a eliminação Gaussiana, que consiste em aplicar operações elementares sobre as linhas da matriz aumentada do sistema, sem alterar o conjunto solução. De fato, o sistema linear que corresponde com a forma escalonada por linhas, possuirá as mesmas soluções do sistema inicialmente utilizado (FAGUNDES, 2013).

De acordo com Fagundes (2013), uma versão desse método já havia aparecido no livro chinês Nove Capítulos, todavia só foi reconhecido quando Gauss calculou a órbita do asteroide Ceres; popularizou-se mais tarde pelo alemão Wilhelm Jordan no Handbuch der Vermessungskunde, livro publicado em 1888.

Definição: Um sistema linear com m equações e n incógnitas, é um conjunto de equações do tipo

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m \end{cases}$$

Onde cada a_{ij} e b_i , com $1 \leq i \leq m$ e $1 \leq j \leq n$, $m, n \in \mathbb{N}$, são elementos de um corpo $\mathbb{K}$. Dentre os sistemas de equações lineares, ocupam uma posição de destaque, como veremos adiante, os sistemas lineares homogêneos, que são sistemas onde todos b_i 's são nulos, isto é,

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = 0 \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = 0 \end{cases}$$

O conjunto solução destes sistemas possuem algumas particularidades que não são compartilhadas pelos sistemas mais gerais. Por exemplo, o vetor nulo $(0,0,0,\dots,0)$ pertence ao conjunto Sh de soluções do sistema. Organizando os valores $(a_{i1}, a_{i2}, \dots, a_{in}, b_i)$ em uma matriz temos

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \vdots & \vdots & & \vdots & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{bmatrix}$$

Que é chamada matriz ampliada do sistema. Se o sistema é homogêneo temos

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{bmatrix}$$

Hefez e Fernandez (2016, p. 10), traz uma informação relevante sobre a aplicação das matrizes na solução de sistemas lineares na China antiga.

As matrizes surgiram por volta do ano 200 a.C. com os chineses, motivados pelo interesse em calcular soluções de sistemas com mais de quatro equações lineares. De fato, no capítulo 8 do texto intitulado *Jiuzhang Suanshu*, de autor desconhecido, que significa “Nove capítulos sobre a Arte matemática”, fica claro que o procedimento para a resolução de sistemas lineares usado pelos chineses é semelhante ao método de escalonamento. Cabe observar que os chineses só consideravam sistemas lineares com o mesmo número de equações e incógnitas, não contando em seus escritos o motivo desses sistemas produzirem sempre uma única solução e como o algoritmo chinês funcionava.

Falaremos a seguir no conjunto solução do sistema de equações lineares.

2.2 SOLUÇÃO DE UM SISTEMA LINEAR

Para resolver um sistema de equações lineares nos moldes acima é necessário determinarmos o conjunto

$$S = \{(c_1, c_2, \dots, c_n) \in \mathbb{R}^n; a_{i1}c_1 + a_{i2}c_2 + \dots + a_{in}c_n = b_i, 1 \leq i \leq m\}.$$

Esse subconjunto do $\mathbb{R}^n$ é chamado de conjunto solução do sistema. Estamos interessados nessa seção em estabelecer as condições para que possamos determinar as soluções de um sistema, a priori, notaremos que podemos definir um sistema como impossível, ou possível e determinado, ou possível e indeterminado. Um sistema linear é dito impossível, quando não tem solução, possível e determinado, quando tem solução única e possível e indeterminado quando tem mais de uma solução.

Para afirmarmos sobre a solução de um sistema usaremos um teorema visto no ensino médio, que é conhecido como teorema do posto ou teorema de Rouché-Campelli, em homenagem aos matemáticos Eugène Rouché (França, 1832 – 1919) e Alfredo Campelli (Itália, 1855 – 1910). Antes de enunciarmos o teorema de Rouché-Campelli ou teorema do posto, daremos a definição do que é o posto de uma matriz.

Definição: Sejam A uma matriz $m \times n$ e B a matriz escalonada equivalente a matriz A . O posto da matriz A , é o número de linhas não nulas da matriz B .

Teorema de Rouché-Campelli: Consideremos um sistema linear com m equações e n incógnitas $AX=B$. Sejam p_{AB} o posto da matriz ampliada do sistema e p_A o posto da matriz A , dos coeficientes do sistema. Então

- (1) O sistema é possível se, e somente se, $p_{AB}=p_A$.
- (2) O sistema é possível e determinado se, e somente se, $p_{AB}=p_A=n$.
- (3) O sistema é possível e indeterminado se $p_{AB}=p_A<n$. Neste caso, $n-p_A$ é o número de incógnitas livres do sistema, isto é, incógnitas que podem assumir qualquer valor real.

Observação, caso $p_{AB}>p_A$, o sistema é obviamente impossível. Aplicando o teorema do posto a sistemas homogêneos, obtemos o seguinte corolário

Corolário: Seja dado um sistema linear do tipo $AX=0$, com m equações e n incógnitas, então (1) Se A tem posto igual a n , então o sistema possui apenas a solução nula. Em particular, isto ocorre quando $m=n$ e A é invertível.

(2) Se A tem posto menor que n , então o sistema possui infinitas soluções. Em particular, isto sempre ocorre quando $m<n$.

Daremos agora um exemplo da aplicação do teorema de Roché-Campelli.

Exemplo:

$$\begin{cases} x + 2y - 2z + 3w = 2 \\ 2x + 4y - 3z + 4w = 5 \\ 5x + 10y - 8z + 11w = 12 \end{cases}$$

Resolvamos o sistema

Segue que a matriz ampliada do sistema é dada por

$$\begin{bmatrix} 1 & 2 & -2 & 3 & 2 \\ 2 & 4 & -3 & 4 & 5 \\ 5 & 10 & -8 & 11 & 12 \end{bmatrix} \xrightarrow{L_2 \rightarrow L_2 - 2L_1, L_3 \rightarrow L_3 - 5L_1} \begin{bmatrix} 1 & 2 & -2 & 3 & 2 \\ 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 2 & -4 & 2 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 2 & -2 & 3 & 2 \\ 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 2 & -4 & 2 \end{bmatrix} \xrightarrow{L_1 \rightarrow L_1 + 2L_2, L_3 \rightarrow L_3 - 2L_2} \begin{bmatrix} 1 & 2 & 0 & -1 & 4 \\ 0 & 0 & 1 & -2 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}$$

Como $p_{AB}=p_A=2<4=n$, onde n é o número de incógnitas do sistema então, pelo teorema de Rouché-Campelli podemos afirmar que o sistema é possível e indeterminado e possui duas variáveis livres, digamos y e w . Assim, sejam $a, b \in \mathbb{R}$, tais que $y=a$ e $w=b$, temos que $z=1+2b$ e $x=4-2a+b$. Portanto a solução do sistema é o conjunto

$$S = \{(4 - 2a + b, a, 1 + 2b, b); a, b \in \mathbb{R}\}.$$

O número de variáveis livres de um sistema é sempre determinado por $n-p_A$, no exemplo anterior, escolhemos as variáveis y e w , mas poderíamos ter escolhido x e z .

2.3 ESPAÇOS VETORIAIS

Exploraremos agora conjuntos que atendem propriedades especiais, a esses conjuntos, chamamos de espaços vetoriais. A primeira definição abstrata de espaços vetoriais foi dada por Giuseppe Peano (Itália, 1858 – 1932) em seu livro *Calcolo Geometrico*, de 1888.

Para Peano (1888, capítulo IX),

os elementos desses conjuntos devem satisfazer as leis comutativa e associativa da adição, enquanto a multiplicação por um escalar pertencente a um corpo $\mathbb{K}$ deve satisfazer as duas leis distributivas da adição em relação ao produto, uma lei associativa e a lei que $1v=v$ para toda quantidade v pertencente ao conjunto.

Definição: Um espaço vetorial V sobre um corpo $\mathbb{K}$ é um conjunto cujos elementos, chamados de vetores, podem ser somados e multiplicados por escalares de modo que todas as propriedades abaixo aconteçam

A1 A adição é associativa: $(u+v)+w=u+(v+w)$.

A2 A adição é comutativa: $u+v=v+u$.

A3 A adição possui elemento neutro: $\exists 0 \in V$, tal que $v+0=0+v, \forall v \in V$.

A4 A adição possui um elemento simétrico: $\forall v \in V, \exists -v \in V$ tal que

$$v + (-v) = 0.$$

E além disso, existe uma operação chamada de multiplicação por escalar, que associa a um elemento $a \in \mathbb{K}$ e um elemento $v \in V$, um elemento $av \in V$, tal que

M1 $a(u+v) = au + av$, para todos $a \in \mathbb{K}$ e $u, v \in V$.

M2 $(a_1 + a_2)v = a_1v + a_2v$, para todos $a_1, a_2 \in \mathbb{K}$ e $v \in V$.

M3 $(a_1 a_2)v = a_1(a_2v)$ para todos $a_1, a_2 \in \mathbb{K}$ e $v \in V$.

M4 $1v = v, \forall v \in V$.

Tais propriedades, se satisfeitas, servem para caracterizar certos conjuntos que, apesar de terem natureza diferente dos vetores no espaço, comportam-se como eles. Um exemplo clássico de espaço vetorial é o conjunto solução de um sistema homogêneo, seja os vetores $u = (c_1, c_2, \dots, c_n)$ e $v = (c_1', c_2', \dots, c_n')$ soluções do sistema, e se $a \in \mathbb{R}$, então os vetores

$$u + v = (c_1 + c_1', c_2 + c_2', \dots, c_n + c_n') \text{ e } au = (ac_1, ac_2, \dots, ac_n)$$

também são soluções do sistema pois, A1 e A2 da definição são satisfeitas para todos os vetores do $\mathbb{R}^n$ e em particular para os de S_h . Por outro lado, $(0, 0, \dots, 0) \in S_h$ e se $(c_1, c_2, \dots, c_n) \in S_h$, então

$$-1(c_1, c_2, \dots, c_n) = (-c_1, -c_2, \dots, -c_n) \in S_h,$$

O que mostra que a adição em S_h possui também as propriedades A3 e A4. Além disso as propriedades M1 - M4 são facilmente verificadas para S_h . Disso resulta que o espaço S_h das soluções do sistema é um espaço vetorial sobre o corpo $\mathbb{R}$.

2.4 SUBESPAÇOS VETORIAIS

Em algumas situações é necessário detectarmos dentro de espaços vetoriais, subconjuntos W que sejam eles próprios espaços vetoriais.

Definição: Sejam V um espaço vetorial e W um subconjunto não vazio de V . Dizemos que W um subespaço vetorial de V , se W , com as operações de adição em V e da multiplicação de vetores de V por escalares de um corpo, é um espaço vetorial, isto é, se:

1) Para quaisquer $u, v \in W$ implica que $u+v \in W$.

2) Para quaisquer $a \in \mathbb{K}$ e $u \in W$, implica $au \in W$.

As condições acima, nos garantem que sempre que somarmos ou multiplicarmos por um escalar vetores de W , não obteremos vetores fora de W , isto implica que W é ele próprio um espaço vetorial, segue da condição 2 que $0 \in W$, basta tomarmos $a=0$. Podemos afirmar também que todo espaço vetorial admite pelos menos dois subespaços, que são, o conjunto formado apenas pelo vetor nulo e próprio espaço vetorial, tais subespaços são chamados de triviais. Se tomarmos $V = \mathbb{R}^3$, temos com exemplos de subespaços vetoriais, todas as retas e planos que passarem pela origem.

Definição: Seja V um espaço vetorial e sejam $v_1, v_2, \dots, v_r$ vetores de V . Dizemos que $v \in V$ é uma combinação linear de $v_1, v_2, \dots, v_r$, se existirem números reais $a_1, a_2, \dots, a_r$ tais que

$$v = a_1 v_1 + a_2 v_2 + \dots + a_r v_r.$$

Por exemplo, o vetor $(2, -3, 4) \in \mathbb{R}^3$ é combinação linear dos vetores $v_1 = (1, -1, 1)$ e $v_2 = (0, -1, 2)$, pois $(2, -3, 4) = 2v_1 + v_2$.

Já o vetor $(2, 2, 3)$ não é uma combinação linear de v_1 e v_2 , pois não existem números reais a_1 e a_2 tais que $(2, 2, 3) = a_1(1, -1, 1) + a_2(0, -1, 2)$, esta equação é equivalente ao sistema de equação

$$\begin{cases} a_1 = 2 \\ -a_1 - a_2 = 2 \\ a_1 + 2a_2 = 3 \end{cases}$$

Que é um sistema impossível.

Definição: Dizemos que um conjunto $v_1, v_2, \dots, v_r$ é um conjunto gerador de um espaço vetorial V se todo vetor v de V for escrito como combinação linear de $v_1, v_2, \dots, v_r$, isto é, para todo $v \in V$ tem-se que

$$v = a_1 v_1 + a_2 v_2 + \dots + a_r v_r$$

2.5 DEPENDÊNCIA E INDEPENDÊNCIA LINEAR

Sejam $v_1, v_2, v_3, \dots, v_n, n \in \mathbb{N}$, vetores de um espaço vetorial V , dizemos que $v_1, v_2, v_3, \dots, v_n$ são linearmente independentes ou LI, se a equação

$$a_1 v_1 + a_2 v_2 + a_3 v_3 \dots + a_n v_n = 0$$

é satisfeita somente quando $a_1=a_2=a_3=\dots=a_n=0$. Do contrário, isto é, caso exista algum $a_i \neq 0$, dizemos que $v_1, v_2, v_3, \dots, v_n$ são linearmente dependentes ou LD.

Como exemplo, vamos verificar se os vetores $v_1=(1,-3,4)$, $v_2=(3,2,1)$ e $v_3=(1,-1,2)$ são LI ou LD.

A equação $a_1v_1 + a_2v_2 + a_3v_3 = 0$, é dada por

$$a_1(1, -3, 4) + a_2(3, 2, 1) + a_3(1, -1, 2) = (0, 0, 0)$$

Que é equivalente ao sistema linear homogêneo

$$\begin{cases} a_1 + 3a_2 + a_3 = 0 \\ -3a_1 + 2a_2 - a_3 = 0 \\ 4a_1 + a_2 + 2a_3 = 0 \end{cases}$$

resolvendo o sistema, achamos que a_3 é livre, $a_1 = -\frac{5}{11}a_3$ e $a_2 = -\frac{2}{11}a_3$.

2.6 BASE DE UM ESPAÇO VETORIAL

Quando falamos em base de um espaço vetorial, estamos interessados dentro do espaço vetorial achar um conjunto finito de vetores, tais que qualquer outro vetor do espaço seja uma combinação linear deles e tais vetores sejam ainda linearmente independentes.

Definição: Dizemos que β é uma base de um espaço vetorial V se:

- 1) β é linearmente independente;
- 2) β gera V .

O número de elementos de uma base de um espaço vetorial não nulo V é chamado de dimensão de V , isto é, a dimensão de V nos diz quantos vetores são necessários para que consigamos determinar todos os outros vetores do espaço vetorial. No exemplo anterior, podemos afirmar que a dimensão do $\mathbb{R}^3$ é 3, e isto implica que qualquer conjunto com 4 vetores em $\mathbb{R}^3$ é necessariamente L.D.

Teorema: Se a dimensão de um espaço vetorial V é n , um conjunto com n vetores gera V se, e somente se, é LI.

Teorema: Seja V um espaço vetorial de dimensão finita n , então:

- 1) Todo conjunto X de geradores de V contém uma base.

- 2) Todo conjunto LI $\{v_1, v_2, \dots, v_r\} \subset V$ está contido numa base.
- 3) Todo subespaço vetorial W de V tem dimensão finita, a qual é menor do que, ou igual a n .
- 4) Se a dimensão do subespaço $W \subset V$ é igual a n , então $W=V$.

2.7 MATRIZ MUDANÇA DE BASE

Um problema comum no estudo de espaços vetoriais de dimensão finita é conhecer as relações de um vetor em diferentes bases. A noção de mudança de base é análoga a mudar os eixos coordenados de $\mathbb{R}^2$ ou $\mathbb{R}^3$. Dado um espaço vetorial qualquer V de dimensão finita e duas bases α e β de V , podemos obter uma relação entre as matrizes $[v]\alpha$ e $[v]\beta$, usando o operador identidade em V .

A matriz $[IV]_{\beta}^{\alpha}$ é chamada de matriz mudança de base de α para β , com ela podemos obter as coordenadas de um vetor $v \in V$ em relação a base β , sabendo suas coordenadas na base α .

Exemplo: Considerando a base canônica α do $\mathbb{R}^2$ e um base $\beta=\{(1,1),(2,3)\}$, temos que

$$[I_{\mathbb{R}^2}]_{\beta}^{\alpha} = \begin{bmatrix} a_1 & b_1 \\ a_2 & b_2 \end{bmatrix}$$

onde, a_1, a_2, b_1 e b_2 são as coordenadas dos vetores da base α , na base β , que são obtidas resolvendo o sistema de equações abaixo

$$\begin{cases} (1, 0) = a_1(1, 1) + a_2(2, 3) \\ (0, 1) = b_1(1, 1) + b_2(2, 3) \end{cases}$$

Então

$$\begin{cases} a_1 + 2a_2 = 1 \\ a_1 + 3a_2 = 0 \end{cases}$$

e

$$\begin{cases} b_1 + 2b_2 = 0 \\ b_1 + 3b_2 = 1 \end{cases}$$

onde obtemos como solução $a_1=3, a_2=-1$ e $b_1=-2, b_2=1$, logo

$$[I_{\mathbb{R}^2}]_{\beta}^{\alpha} = \begin{bmatrix} 3 & -2 \\ -1 & 1 \end{bmatrix}$$

É a matriz mudança de base.

Teorema: Sejam α e β duas bases de um espaço vetorial V de dimensão finita, então a matriz $[IV]_{\beta}^{\alpha}$ é invertível e sua inversa é a matriz $[IV]_{\alpha}^{\beta}$, isto é,

$$([I_V]_{\beta}^{\alpha})^{-1} = [I_V]_{\alpha}^{\beta}$$

2.8 CORES

O registro mais antigo que temos conhecimento sobre cores, deve-se ao filósofo grego Aristóteles que concluiu que as cores eram uma propriedade dos objetos, assim como peso, material, textura, eles tinham cores, e conjecturou que que eram em número de seis, o vermelho, o verde, azul, amarelo, preto e branco. Durante os anos seguintes, vários cientistas importantes estudaram as cores com destaque para Leonardo da Vinci, Isaac Newton, Le Blon e Goethe.

A medida em que a humanidade foi avançando científica e tecnologicamente as obras de arte e pinturas tornaram-se mais complexas, assim a diversidade de cores usadas para tais representações eram bem maiores, dessa forma, foi preciso um estudo mais aprofundado de como obtê-las. As cores são percepções visuais provocadas por um feixe de fótons sobre células específicas da nossa retina, chamadas de cones é também por isso que enxergamos os objetos, eles recebem luz proveniente de uma fonte luminosa, ao contrário da ideia que normalmente temos de que ele tem a própria luz, e é visível por si.

A fonte de luz que o ilumina, por sua vez, possui diversas cores que a compõe, de forma que os raios contêm todas as cores imagináveis. Em nossa retina, existem três tipos cones para captarem as cores vermelho, verde e azul, adiante, no presente trabalho, entenderemos a justificativa pela qual captando somente estas três cores, conseguimos enxergar todas as demais cores imagináveis.

No espectro da luz branca, que emana do sol, existem 7 cores, tal fato foi provado em um trabalho publicado por Isaac Newton em 1672 no qual apresentava suas ideias sobre a natureza das cores. A interpretação sobre a dispersão da luz e a natureza das cores, dada por Isaac Newton, é aceita até hoje, segundo ele **“as cores de todos os corpos são devidas simplesmente ao fato de que eles refletem a luz de uma certa cor em maior quantidade do que as outras”**. No experimento de Newton

ele utilizou um prisma retangular de base triangular para refratar a luz branca, com isso ele conseguiu 7 cores: **vermelho**, **laranja**, **amarelo**, **verde**, **azul**, anil (ou **índigo**) e **violeta**, mostrando assim que a luz branca do sol é formada pela junção dessas cores. Segundo Marco Aurélio, o fenômeno de refração ocorre em razão da dependência da velocidade da onda com a sua frequência, quando a luz se propaga e muda de um meio para outro de desigual densidade, as ondas de diferentes frequências tomam diversos ângulos na refração, assim sendo, surgem as cores que compõe a luz branca.



Figura 1: Experimento de Newton. Fonte: Maurício (2018).

Isso justifica a razão de não enxergarmos no escuro, por exemplo, se entrarmos em um quarto completamente escuro (sem luz) não enxergaremos nenhum objeto contido neste quarto, pois os objetos não refletiriam luz e, portanto, nossos olhos não poderão captá-la.

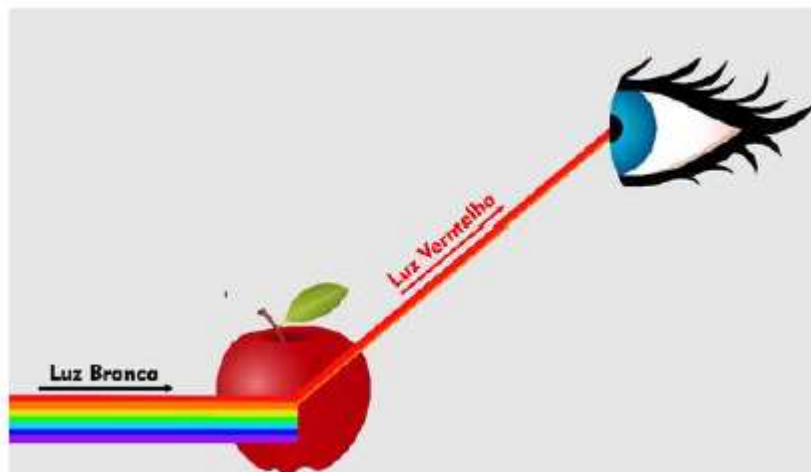


Figura 2: Visão de um objeto vermelho. Fonte: Gt-mre (2018).

2.9 O SISTEMA DE CORES RGB

Assim é natural uma representação tridimensional do espaço de cor, cuja base de cores primárias seria constituída por três cores nas faixas vermelha, verde e azul do espectro visível, e isto resultou no primeiro modelo padrão básico o CIE-RGB.

O trabalho desenvolvido por Thomas Young (1773-1829), revelou o princípio da teoria básica das cores luz. Ele descobriu que, projetando luz através de filtros vermelho, verde e azul, no sentido de produzir círculos sobrepostos, diversos efeitos eram obtidos:

- Onde os círculos coincidiam, a luz branca era produzida;
- Onde qualquer duas das cores coincidiam eram produzidas novas cores: vermelho + azul = magenta; vermelho + verde = amarelo e azul + verde = ciano.
- Com a variação da quantidade relativa (proporção) de vermelho, verde e azul na área de sobreposição era possível produzir uma enorme gama de cores.
- Qualquer uma das três cores não podia ser produzida pela mistura de qualquer uma delas. Por isso, Thomas as chamou de cores primárias.

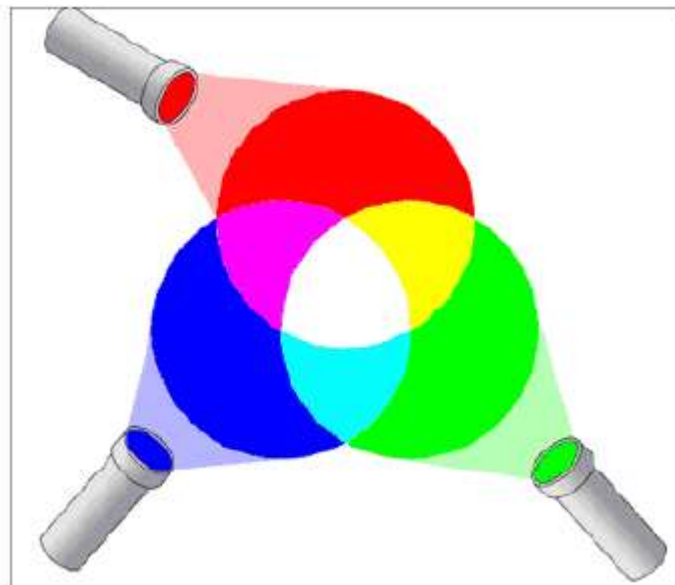


Figura 3: Ilustração do experimento de Thomas Young. Fonte: Maurício (2018).

O sistema de cores luminosas RGB (também designado por cor-luz) é usado nos objetos que emitem luz como, por exemplo, os monitores de computador e televisão, as câmeras digitais, o *scanner*, celulares, tablets entre outros eletrônicos. RGB é a sigla do sistema de cores aditivas formado pelas iniciais das cores em inglês *Red*, *Green* e *Blue*, que significa em português, respectivamente, Vermelho, Verde e Azul.

As cores nesse sistema são obtidas através das misturas das três cores primárias, em quantidades determinadas. Cada uma das cores obtidas está enquadrada numa escala que varia de 0 a 255. As cores vermelha, verde e azul são representadas respectivamente pelos vetores $(255,0,0)$, $(0,255,0)$ e $(0,0,255)$ do $\mathbb{R}^3$. Quando a mistura das três cores está no valor mínimo $(0,0,0)$, o resultado é a cor preta. Quanto está no máximo $(255,255,255)$, resulta na cor branca, isto implica que a mistura das três cores resulta no branco e que a ausência das três, resulta no preto. A escolha do valor 255 se dar pelo fato de que a menor unidade de configuração que pode ser transmitida ou armazenada é 1bit, que assume dois valores: 0 e 1.

Em imagens capturadas em câmera digital (2D), por exemplo, os programas computacionais fazem uma associação: cada unidade de imagem com um valor inteiro não negativo que corresponde a 1byte = 8bits. Assim, para cada bit, tem-se 0 ou 1 (2 possibilidades). Como são 8 bits, então tem-se: $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^8 = 256$, que é o número de valores distintos que pode ser associado a um pixel.

Nestes termos, 0 indica a ausência total de intensidade luminosa (cor preta) e 255 indica a luminosidade máxima (cor branca). Os valores entre 0 e 255 representam escalas de cinza. E assim se formam as imagens digitais em preto e branco, com tons de cinza.

Para imagens coloridas, cada pixel pode ter uma cor, que é a combinação de três cores primitivas: vermelho (*red*), verde (*green*) e azul (*blue*). Cada cor possui 256 tonalidades, com variações da mais clara à mais escura: o zero (0) indica a ausência de cor e o 255 indica a presença máxima da cor na combinação, representada por ternas (R,G,B), indicando, sempre nesta ordem, a intensidade de cada cor no ponto de imagem considerado.

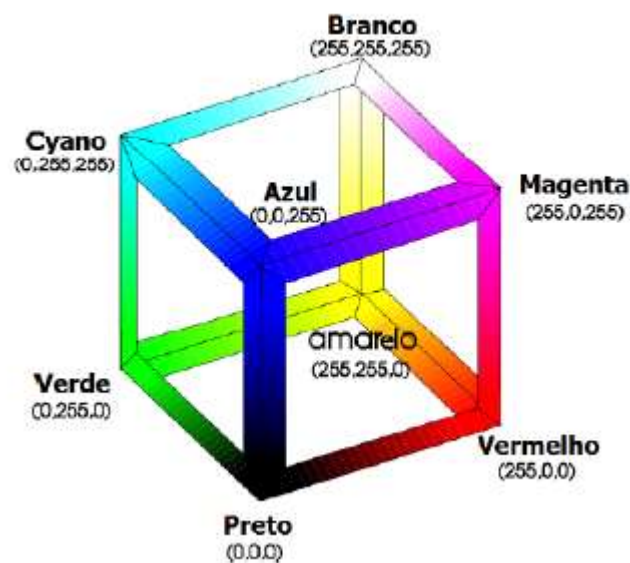


Figura 4: Cubo representando o sistema RGB no espaço tridimensional. Fonte: Teoria básica das cores: O espaço RGB; Sebem, Elódio.

A variação entre valores mínimos corresponde a tons escuros e entre os valores máximos, os tons são mais intensos, mais claros. Se normalizarmos esses vetores obtemos um cubo de aresta 1, onde os vetores $(1,0,0)$, $(0,1,0)$ e $(0,0,1)$ representam as cores vermelho, verde e azul, respectivamente.

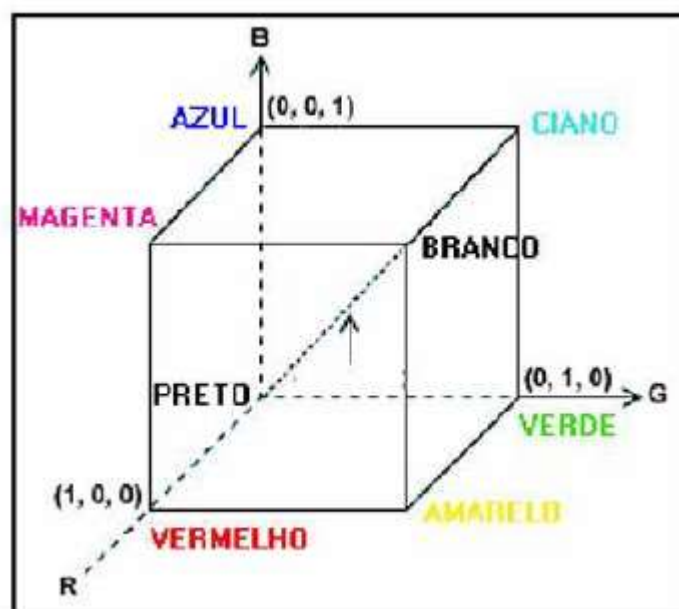


Figura 5: Cubo representando o sistema RGB normalizado no espaço tridimensional. Fonte: Maurício (2018).

Deste modo, podemos imaginar cada cor como pontos dentro deste cubo definidos por vetores que partem da origem. A partir do exposto acima, podemos definir que o espaço de cores RGB como

espaço gerado pelos vetores linearmente independentes $(255,0,0)$, $(0,255,0)$ e $(0,0,255)$. Caso a soma de dois ou mais vetores ou o produto de um vetor por um escalar, resultar em um vetor cujas coordenadas são maiores do que 255, devemos escrever como coordenadas desse vetor os restos de sua divisão por 255, por exemplo, se somarmos os vetores $(255,91,83)$ róseo claro, e $(161,163,147)$ cinza, obteremos o vetor $(416,254,230)$ como a primeira coordenada foi maior que 255, então devemos substituí-la pelo resto da divisão dela por 255, obtendo assim o vetor $(206,254,230)$.

Conforme definido acima, o espaço RGB é um subespaço vetorial do $\mathbb{R}^3$, isto implica que sempre que somarmos ou multiplicarmos por um escalar quaisquer que sejam os vetores (cores) desse espaço, obteremos sempre vetores dentro do cubo de arestas medindo 255, conforme representado na Figura 5. Como o espaço RGB é gerado pelos vetores $(255,0,0)$, $(0,255,0)$ e $(0,0,255)$ que compõe a base do espaço dos espaços, podemos afirmar que ele é espaço vetorial de dimensão 3, isso quer dizer que necessitamos apenas de 3 cores, chamadas de primárias, para obtermos todas as demais cores.

Um exemplo usual de espaços de cores são as impressoras, que representam suas cores no sistema CMYK que usam 3 cores distintas (Ciano, Amarelo e Magenta) para gerarem as demais cores, e por um fator de custo a cor preta e a cor branca não valem a pena serem obtidas como combinações lineares das cores da base, por isso as impressoras tem um cartucho exclusivo para cor preta (K). Em particular o espaço de cores CMYK é um sistema de cores subtrativas semelhante ao RGB, onde o C representa cor ciano, o M a cor magenta, o Y é a cor amarela (*yellow*) e o K representa cor preta.

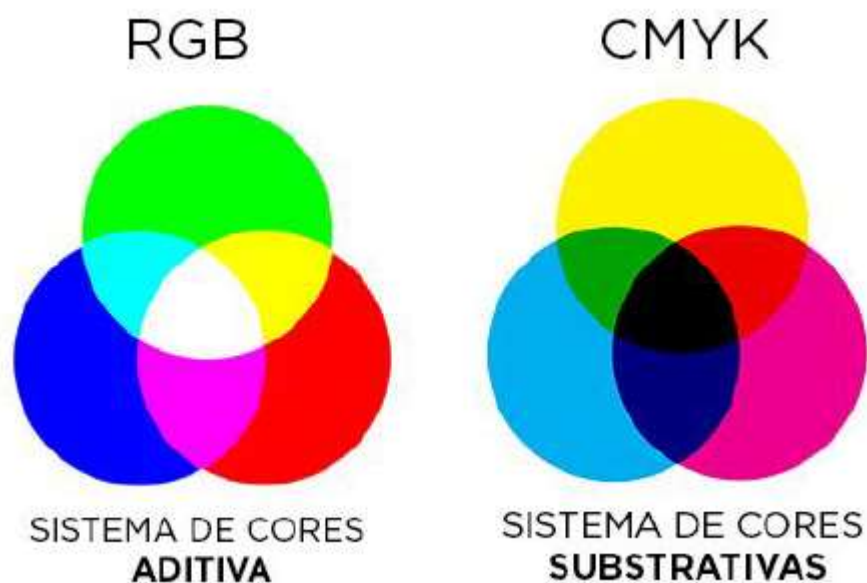


Figura 6: Representação luminosa dos sistemas RGB e CMYK. Fonte: Modelos de cor; Rogers e Adms – seção 5.5, cap. 7.

Note que no sistema CYMK para obter a cor preta, seria necessário misturar as três cores, neste caso gerando um custo maior para os demais cartuchos. Um computador para efetuar uma impressão necessita fazer uma transformação linear que leva as cores (vetores) do sistema RGB para as cores do sistema CMYK, pois a tela do computador está configurada no sistema RGB enquanto a impressora opera no sistema CMYK.

A imagem dos monitores de computadores e televisões por exemplo, são constituídas de pixels, e a resolução de uma imagem é a quantidade de informação que a imagem contém por unidade de comprimento. O pixel, é a unidade elementar de brilho e cor que constitui uma imagem digital. A qualidade, e a definição de uma imagem, depende da informação de cada pixel.

Para representar a cor de cada pixel os monitores fazem um processo similar ao descrito acima, por exemplo, se um pixel deve possuir a cor laranja, que é representada pelo vetor $(255, 165, 0)$, ele deve receber 100% da luminosidade vermelha, 64,7% da luminosidade verde e 0% da azul, a figura abaixo ilustra como é o processo para a formação da cor de um pixel.

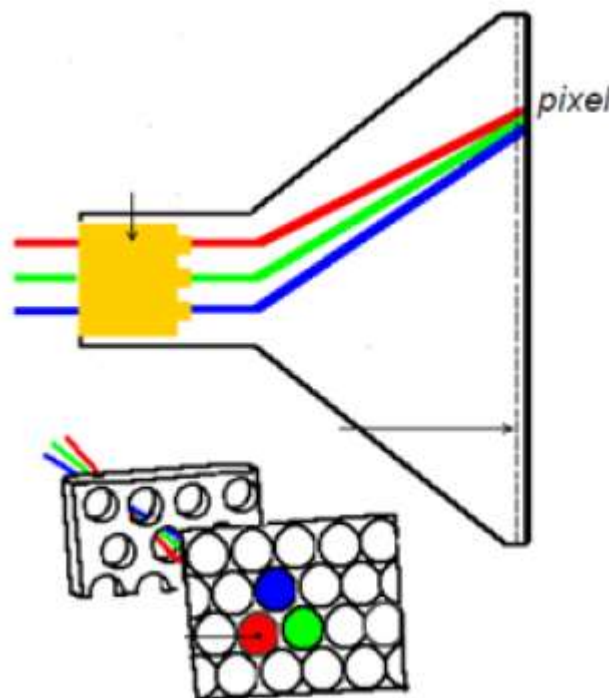


Figura 2: Representação de um pixel em um monitor. Fonte: Dafaqidiz (2018).

3. DIRETRIZES SOBRE O ENSINO DE SISTEMAS DE EQUAÇÃO

Associando o sistema de cores RGB com um aplicativo oferecido pelo site http://webcalc.com.br/Utilitarios/form/rgb_hex temos uma valiosa ferramenta para trabalhar o ensino de sistemas de equações lineares de forma a propiciar para os alunos uma aprendizagem significativa associado ao conceito do uso do computador e da tecnologia no ambiente de ensino pois, o computador traz uma infinidade de possibilidades que contribuem no processo de aprendizagem devido as imensas possibilidades de aplicação na disciplina (TOLEDO e TOLEDO, 2009).

Neste sentido, o uso de softwares parece poder auxiliar a prática docente, e criar um ambiente favorável à construção de conceitos matemáticos que possibilitem a superação das dificuldades e tornem a aprendizagem mais estimuladora. O computador, pelas suas potencialidades a nível de cálculo, visualização, modelação e geração de micromundos, é o instrumento mais poderoso de que atualmente dispõem os educadores matemáticos para proporcionar este tipo de experiências aos seus alunos (PONTES, 1986).

O principal objetivo do presente trabalho é explorar a resolução de sistemas de equações lineares utilizando as cores no sistema RGB de forma a propiciar uma aprendizagem significativa aos alunos, segundo Marcos Antonio Moreira (Aprendizagem Significativa, 2012, p.13), “aprendizagem significativa é aquela que ideias expressas simbolicamente interagem de maneira substantiva e não arbitrária com aquilo que o aprendiz já sabe.”

As Orientações Curriculares para o Ensino Médio: Ciências da Natureza, Matemática e suas Tecnologias (BRASIL, 2006) servem de norte aos professores do Ensino Médio. Conforme observado nesse documento, ao final do Ensino Médio espera -se que os alunos saibam usar a Matemática para resolver problemas práticos do cotidiano; para modelar fenômenos em outras áreas do conhecimento; compreendam que a Matemática é uma ciência com características próprias, que se organiza via teoremas e demonstrações; percebam a Matemática como um conhecimento social e historicamente construído; saibam apreciar a importância da Matemática no desenvolvimento científico e tecnológico (BRASIL, 2006, p. 69).

Destacando que esta divisão não significa que os conteúdos desses blocos devam ser trabalhados de forma estanque, mas, ao contrário, deve-se buscar constantemente a articulação entre eles. (BRASIL, 2006, p. 70).

Especificamente sobre Sistemas Lineares, as Orientações Curriculares sinalizam que além de trabalhar a técnica de resolução de sistemas lineares, é recomendável colocar a álgebra sob o olhar da geometria. A resolução de um sistema linear 2×2 , de duas equações e duas variáveis pode ser associada ao estudo da posição relativa de duas retas no plano. Com operações elementares simples, pode-se determinar a existência ou não de soluções desse sistema, o que significa geometricamente os casos de interseção/coincidência de retas ou paralelismo de retas. A resolução de sistemas 2×3 ou 3×3 também deve ser feita via operações elementares (o processo de escalonamento), com discussão das diferentes situações (sistemas com uma única solução, com infinitas soluções e sem solução). Quanto à resolução de sistemas de equação 3×3 , através da regra de Cramer sugere-se que a mesma deve ser abandonada, pois é um procedimento custoso (no geral, apresentado sem demonstração, e, portanto, de pouco significado para o aluno), que só permite resolver os sistemas quadrados com solução única. (BRASIL, 2006, p. 77-78).

Desta forma pretendemos trabalhar através de uma oficina a resolução de sistemas lineares usando o método do escalonamento, bem como trabalhar a soma de vetores e o algoritmo de divisão nos inteiros.

3.1 CORES E SISTEMAS DE EQUAÇÕES LINEARES

Na Seção 2.3, abordamos a seguinte situação: é possível que existam outras cores tais que as demais cores no sistema RGB sejam expressas pela combinação entre elas?

Sabemos da álgebra linear que a resposta é sim, pois como o espaço RGB é um espaço vetorial de dimensão três então, basta tomarmos três cores (vetores) linearmente independentes e conseguiremos uma nova base.

Porém a resposta para problema anterior nos fornece um método de trabalhar sistemas de equações lineares associado as cores no sistema RGB com alunos do ensino médio, como sugere o exemplo a seguir.

Exemplo: Com as cores Ciano (0,255,255), azul escuro (0,0,139) e laranja (255,165,0) é possível obtermos a cor róseo intenso (255,20,147)?

Inicialmente devemos notar que a solução desse problema consiste em resolver o sistema

$$x(0, 255, 255) + y(0, 0, 139) + z(255, 165, 0) = (255, 20, 147)$$

Então

$$\begin{cases} 0x + 0y + 255z = 255 \\ 255x + 0y + 165z = 20 \\ 255x + 139y + 0z = 147 \end{cases}$$

Que na forma matricial é

$$\begin{bmatrix} 0 & 0 & 255 \\ 255 & 0 & 165 \\ 255 & 139 & 0 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 255 \\ 20 \\ 147 \end{bmatrix}$$

A matriz ampliada do sistema é

$$\begin{bmatrix} 0 & 0 & 255 & 255 \\ 255 & 0 & 165 & 20 \\ 255 & 139 & 0 & 147 \end{bmatrix}$$

escalonando a matriz,

$$\begin{bmatrix} 0 & 0 & 255 & 255 \\ 255 & 0 & 165 & 20 \\ 255 & 139 & 0 & 147 \end{bmatrix} \xrightarrow{L_2 \rightarrow L_1} \begin{bmatrix} 255 & 0 & 165 & 20 \\ 0 & 0 & 255 & 255 \\ 255 & 139 & 0 & 147 \end{bmatrix}$$

$$\begin{bmatrix} 255 & 0 & 165 & 20 \\ 0 & 0 & 255 & 255 \\ 255 & 139 & 0 & 147 \end{bmatrix} \xrightarrow{L_1 \rightarrow \frac{L_1}{255}} \begin{bmatrix} 1 & 0 & \frac{11}{17} & \frac{4}{51} \\ 0 & 0 & 255 & 255 \\ 255 & 139 & 0 & 147 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & \frac{11}{17} & \frac{4}{51} \\ 0 & 0 & 255 & 255 \\ 255 & 139 & 0 & 147 \end{bmatrix} \xrightarrow{L_3 \rightarrow L_3 - 255 \cdot L_1} \begin{bmatrix} 1 & 0 & \frac{11}{17} & \frac{4}{51} \\ 0 & 0 & 255 & 255 \\ 0 & 139 & -165 & 12 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & \frac{11}{17} & \frac{4}{51} \\ 0 & 0 & 255 & 255 \\ 0 & 139 & -165 & 127 \end{bmatrix} \xrightarrow{L_2 \rightarrow L_3} \begin{bmatrix} 1 & 0 & \frac{11}{17} & \frac{4}{51} \\ 0 & 139 & -165 & 127 \\ 0 & 0 & 255 & 255 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & \frac{11}{17} & \frac{4}{51} \\ 0 & 139 & -165 & 127 \\ 0 & 0 & 255 & 255 \end{bmatrix} \xrightarrow{L_2 \rightarrow \frac{L_2}{139}} \begin{bmatrix} 1 & 0 & \frac{11}{17} & \frac{4}{51} \\ 0 & 1 & \frac{-165}{139} & \frac{127}{139} \\ 0 & 0 & 255 & 255 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & \frac{11}{17} & \frac{4}{51} \\ 0 & 1 & \frac{-165}{139} & \frac{127}{139} \\ 0 & 0 & 255 & 255 \end{bmatrix} \xrightarrow{L_3 \rightarrow \frac{L_3}{255}} \begin{bmatrix} 1 & 0 & \frac{11}{17} & \frac{4}{51} \\ 0 & 1 & \frac{-165}{139} & \frac{127}{139} \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 0 & \frac{11}{17} & \frac{4}{51} \\ 0 & 1 & \frac{-165}{139} & \frac{127}{139} \\ 0 & 0 & 1 & 1 \end{bmatrix} \xrightarrow[L_1 \rightarrow \frac{-11}{17} L_3]{L_2 \rightarrow \frac{165}{139} L_3} \begin{bmatrix} 1 & 0 & 0 & \frac{-29}{51} \\ 0 & 1 & 0 & \frac{292}{139} \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

Portanto, segue que

$$x = \frac{-29}{51} \cong 0,56863$$

$$y = \frac{292}{139} \cong 2,10072$$

$$z = 1$$

isto implica, que o vetor que representa a cor róseo intenso (255,20,147) na base $\beta = \{(0,255,255), (0,0,139), (255,165,0)\}$ é $(\frac{-29}{51}, \frac{292}{139}, 1)$.

O valor negativo da solução, acontece pelo fato de termos trocado a base, dessa forma o vetor solução sai do tetraedro formado pelos vetores (0,255,255), (0,0,139) e (255,165,0). Se fizermos a mudança para base RGB, obteremos como matriz mudança de a matriz

$$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & \frac{11}{17} \\ 1 & \frac{139}{255} & 0 \end{bmatrix}$$

Pois

$$(0, 255, 255) = 0 \cdot (255, 0, 0) + 1 \cdot (0, 255, 0) + 1 \cdot (0, 0, 255)$$

$$(0, 0, 139) = 0 \cdot (255, 0, 0) + 0 \cdot (0, 255, 0) + \frac{139}{255} \cdot (0, 0, 255)$$

$$(255, 165, 0) = 1 \cdot (255, 0, 0) + \frac{11}{17} \cdot (0, 255, 0) + 0 \cdot (0, 0, 255)$$

Se multiplicarmos o vetor $(\frac{-29}{51}, \frac{292}{139}, 1)$ pela matriz mudança de base, obteremos o vetor na base RGB.

Devemos notar que o sistema foi possível e determinado pelo fato das cores (vetores) Ciano $(0, 255, 255)$, azul escuro $(0, 0, 139)$ e laranja $(255, 165, 0)$ serem linearmente independentes.

Devemos notar que caso escolhamos três vetores linearmente dependentes não será possível. Se tentarmos achar a cor róseo intenso, usando os vetores $(255, 165, 0)$ laranja, $(51, 33, 0)$ marrom e $(147, 253, 77)$ verde claro, teremos que resolver o sistema

$$x(255, 165, 0) + y(51, 33, 0) + z(147, 253, 77) = (255, 20, 147)$$

$$\begin{cases} 255x + 165y + 0z = 255 \\ 51x + 33y + 0z = 20 \\ 147x + 253y + 77z = 147 \end{cases}$$

que na forma matricial é

$$\begin{bmatrix} 255 & 165 & 0 \\ 51 & 33 & 0 \\ 147 & 253 & 77 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 255 \\ 20 \\ 147 \end{bmatrix}$$

e

$$\begin{bmatrix} 255 & 165 & 0 & 255 \\ 51 & 33 & 0 & 20 \\ 147 & 253 & 77 & 147 \end{bmatrix}$$

é a matriz ampliada do sistema. Escalonando a matriz, obtemos

$$\begin{bmatrix} 255 & 165 & 0 & 255 \\ 51 & 33 & 0 & 20 \\ 147 & 253 & 77 & 147 \end{bmatrix} \xrightarrow{L_1} \frac{L_1}{255} \begin{bmatrix} 1 & \frac{11}{17} & 0 & 1 \\ 51 & 33 & 0 & 20 \\ 147 & 253 & 77 & 147 \end{bmatrix}$$

$$\begin{bmatrix} 1 & \frac{11}{17} & 0 & 1 \\ 51 & 33 & 0 & 20 \\ 147 & 253 & 77 & 147 \end{bmatrix} \xrightarrow{L_2} L_2 - 51L_1 \begin{bmatrix} 1 & \frac{11}{17} & 0 & 1 \\ 0 & 0 & 0 & -31 \\ 147 & 253 & 77 & 147 \end{bmatrix}$$

pela segunda linha, podemos afirmar que o sistema é impossível, isso acontece pelo fato dos vetores laranja (255,165,0) e marrom (51,33,0) são linearmente dependentes pois, $(255,165,0)=5 \cdot (51,33,0)$.

Outro questionamento pertinente é: quais cores podemos formar se misturarmos somente duas cores ao invés de três? Por exemplo o laranja (255,165,0) e o verde claro (147,253,77)?

Como os vetores são linearmente independentes, pois

$$a(255, 165, 0) + b(147, 153, 77) = (0, 0, 0)$$

$$\begin{cases} 255a + 147b = 0 \\ 165a + 153b = 0 \\ 0a + 77b = 0 \end{cases}$$

da equação 3 temos que $b=0$, o que implica que $a=0$ portanto, os vetores são LI.

Dessa forma esses dois vetores determinam um semiplano no espaço RGB, e todas os vetores que partirem da origem e tiverem pontos finais pertencentes a esse semiplano, podem ser formados por uma combinação linear dos dois, qualquer vetor que não pertencer a esse semiplano não pode ser combinação linear dos vetores dados, isto implica que, caso o vetor pertença ao semiplano, o sistema de equações terá solução única e, caso o vetor não pertença ao semiplano o sistema de equações lineares não possuirá solução.

No caso de selecionarmos 4 vetores, teremos no mínimo um vetor supérfluo, isto é, um vetor que é combinação linear dos demais, pois o espaço é de dimensão 3 então, necessariamente umas das linhas da matriz ampliada do sistema será nula quando escalonada, se os demais vetores forem LI então o

sistema será possível e determinado, no caso de 2 vetores serem linearmente independentes, recaímos no caso do parágrafo anterior.

Com base nesses exemplos, decidimos montamos uma oficina de 4 aulas para trabalhar a solução de sistemas de equações lineares associadas ao sistema de cores RGB, bem como incentivar o uso do computador e da calculadora pelos alunos.

4. CONSIDERAÇÕES FINAIS

Parte em que se apresenta as conclusões correspondentes aos objetivos e hipóteses propostos. Após a análise e discussões dos resultados, são apresentadas as conclusões e as descobertas do texto, evidenciando com clareza e objetividade as deduções extraídas dos resultados obtidos ou apontadas ao longo da discussão do assunto. Neste momento são relacionadas às diversas ideias desenvolvidas ao longo do trabalho, num processo de síntese dos principais resultados, com os comentários do autor e as contribuições trazidas pela pesquisa.

Cabe, ainda, lembrar que a conclusão é um fechamento do trabalho estudado, respondendo às hipóteses enunciadas e aos objetivos do estudo, apresentados na Introdução, onde não se permite que nesta seção sejam incluídos dados novos, que já não tenham sido apresentados anteriormente.

REFERÊNCIAS

- BOLDRINI, José Luiz. Álgebra linear. 3ª edição. São Paulo: editora HABRA, 1980.
- CALLIOLI, C.A.; DOMINGUES, H. H; COSTA, R. F. C. Álgebra Linear e aplicações. 6º. ed. São Paulo: ATUAL, 1990.
- DAFAQISDIZ. Modelo RGB. 2018. Disponível em: <https://sites.google.com/site/dafaqisdiz/Modelo-rgb>. Acesso em: 05 abr. 2018.
- E. L. Lima: Álgebra Linear. 8ª edição. IMPA, Rio de Janeiro 2012.
- E. L. Lima: Geometria Analítica e Álgebra Linear. 2ª edição. Coleção Matemática Universitária, IMPA. 2010.
- GONZALEZ, R.C; WOODS, R.E. Processamento digital de imagem.
- GT-MRE. Disco de Newton. 2018. Disponível em:]
<http://gt-mre.ufsc.br/moodle/course/view.php?id=22&ion=5>. Acesso em: 05 abr. 2018.
- H. P Bueno. Álgebra Linear, um segundo curso. Coleção Textos Universitários, SBM, 2006.
- HEFEZ, Abramo; FERNANDEZ, Cecília. Introdução a Álgebra Linear. Coleção PROFMAT, SBM. 2016.
- IEZZI, G.; DOLCE, O.; DEGENSZAJN, D. PÉRIGO, R.; ALMEIDA, N. Matemática Ciência e aplicação. 9. ed. São Paulo: Saraiva, 2016.
- MAURÍCIO, Joana. Espaço de Cores RGB! Disponível em:
<http://theworldofcolorjo.blogspot.com/2012/01/espaco-de-cores-rgb.html>. Acesso em: 05 abr. 2018.
- PONTES, J. O computador — Um Instrumento da Educação. Lisboa: Texto Editora, 1986.
- SANTOS, Marco Aurélio da Silva. "A Dispersão da Luz Branca"; Brasil Escola. Disponível em <<https://brasilecola.uol.com.br/fisica/a-dispersao-luz-branca.htm>>. Acesso em 12 de julho de 2018.
- SZELISK, R. Computer Vision. Seção 2.3.2. Springer, 2011.
- TOLEDO, Marília Barros de Almeida; TOLEDO, Mauro de Almeida. Teoria e prática da matemática: como dois e dois. Volume único. São Paulo: FTD, 2009.

Capítulo 5



10.37423/220305624

FUNÇÕES AFINS E CRIPTOGRAFIA

Maria Joseane Felipe Guedes Macêdo

*Universidade Federal Rural do Semi-Árido -
UFERSA*

Willa da Silva Medeiros

*Universidade Federal Rural do Semi-Árido -
UFERSA*



1. INTRODUÇÃO

O presente capítulo está inserido na perspectiva de contextualizar e de inter-relacionar a matemática com outras ciências, afim de enriquecer e motivar o seu estudo. A ciência a qual iremos relacionar com a matemática é a criptografia. Uma área da computação muito antiga e que tem sua origem bem parecida com a da matemática. Hoje em dia a matemática é essencial para a criptografia, constituindo sua base conceitual de segurança. A palavra criptografia provém do grego *kriptos*, que significa secreto, oculto, e *graphein*, que significa escrever. Assim, entendemos criptografia como a ciência que estuda os meios, os métodos, para tornar o conteúdo de uma mensagem incompreensível para todos aqueles que não têm permissão de lê-la, de modo que somente o destinatário legítimo possa obter a mensagem verdadeira.

É natural do ser humano a preocupação em impor sigilo a determinadas informações que ele considera importante e que, por algum motivo de privacidade e segurança pessoal, não podem ser conhecidas por pessoas não autorizadas. Essa preocupação acompanha o homem desde os tempos mais remotos, sendo ela a responsável pelo desenvolvimento de habilidades extraordinárias para manter a segurança das informações trocadas via mensagens.

A troca de mensagens representou um grande avanço no desenvolvimento da comunicação, possibilitando o tráfego dessas informações por vias de diferentes naturezas. No entanto, durante um intercâmbio de mensagens, onde o conteúdo das mesmas não poderia ser compartilhado por pessoas não autorizadas, o emissor e o receptor (quem envia e recebe a mensagem, respectivamente) tinham ciência do perigo caso tal mensagem chegasse a mãos erradas. Assim, entra em cena a questão da segurança e privacidade dessas mensagens: como enviar uma informação sigilosa com segurança de modo que, se por ventura ela caia em mãos erradas, seu conteúdo não possa ser compreendido?

Tal pergunta, e o problema central que a acompanha, foram responsáveis por fazer com que o homem desenvolvesse técnicas de proteção e ocultação do significado real de uma mensagem antes da mesma ser *enviada* para outra pessoa. Dessa maneira, o envio e, principalmente, o trajeto dessa mensagem se tornam mais seguros e com maior probabilidade de não ser violados. Surgem então os códigos secretos, os procedimentos, e os algoritmos para proteger as comunicações.

Com a evolução das comunicações e o desenvolvimento da linguagem, os códigos tiveram que ser aperfeiçoados, se não substituídos, para poder atender à crescente demanda por segurança no envio de mensagens. A evolução dos códigos primitivos se dar com o surgimento das *cifras* que, segundo

Singh (2004), dominaram a arte dos códigos secretos no primeiro milênio. Porém, estas cifras não conseguiram seguir no topo da segurança das comunicações. Isso porque havia outro ramo de estudo, chamado criptoanálise, que se destinava a desenvolver alternativas para vencer as cifras. Isso fez com que fossem idealizados vários tipos de cifras com o intuito de aperfeiçoar as alterações feitas nas mensagens. Mesmo assim, estas cifras eram baseadas em métodos que possuíam muitas deficiências quanto ao seu modo de mudar o significado de uma mensagem e a maneira de recuperá-la. Essa deficiência foi responsável por fazer com que um novo ramo de escrita secreta surgisse. Daí em diante a escrita secreta toma um novo rumo, mais moderno, onde a matemática desempenha o papel principal, garantindo a segurança dos códigos.

Hoje, conhecemos o estudo da arte dos códigos através da criptografia, uma ciência que se encarrega de desenvolver métodos que possibilitem o máximo de privacidade e segurança no envio de mensagens. A criptografia está relacionada com muitos conceitos básicos de matemática (BUCHMANN, 2002), o que permite estabelecer facilmente relações entre essas duas. Sendo a criptografia um tema de enorme relevância, pois representa uma das aplicações mais importantes da matemática para a sociedade, relacioná-la com conteúdos básicos de matemática tornará as aulas mais interessantes, dinâmicas e conseqüentemente a aprendizagem mais significativa (PEREIRA, 2015). O Capítulo FUNÇÕES QUADRÁTICAS E CRIPTOGRAFIA, presente nessa mesma obra, apresenta um breve histórico sobre o desenvolvimento da criptografia.

Funções é um tópico muito importante na matemática do ensino básico, o seu bom entendimento é indispensável para a compreensão e o desenvolvimento de conteúdos mais avançados na matemática. Dessa maneira, este capítulo tem por objetivo descrever, por meio de um estudo introdutório, como a Função Afim está inserida em conceitos elementares de criptografia e como isso pode ser útil no aprendizado do aluno. Compreenderemos como tais funções podem ser trabalhadas e contextualizadas com base na criptografia. Os exemplos e as descrições dos métodos funcionarão como fonte de inspiração para o desenvolvimento de atividades em sala de aula, contribuindo como subsídios para que o professor possa dar maior aplicabilidade aos conteúdos estudados e, com maior ênfase, tornar o estudo mais significativo, sólido e mais próximo da realidade do aluno. Salientamos que este estudo se fundamenta em obras como, Buchmann (2002), Brandão (2017), Coutinho (2005), França (2014), Jesus (2013), Medeiros (2017). Na seção seguinte desenvolveremos um pouco da teoria relacionada com funções, em particular as funções afins.

2. NOÇÕES BÁSICAS SOBRE FUNÇÕES

Nesta seção apresentaremos alguns conceitos básicos sobre funções. Não nos aprofundaremos neste assunto, uma vez que o objetivo principal deste estudo é apresentar aplicações das funções e não o seu conteúdo teórico. Para o leitor interessado em revisar as noções básicas sobre Função Afim, e outras funções elementares vistas no ensino básico, indicamos as obras Giovanni Júnior et al. (2018), Bianchini (2018), Balestri (2016), Iezzi et al. (2002), Lima et al. (2006a), Dante (2006), Guidorizzi (2018), Flemming e Gonçalves (2012), entre tantos outros livros que contemplam tais tópicos.

De uma maneira informal, costumamos associar a definição de função como sendo uma regra que associa dois conjuntos quaisquer. Mas, será que toda regra que associa dois conjuntos é de fato uma função? Ou, para ser função tal regra precisa obedecer algumas condições especiais?

De acordo com Lima (2013, p. 13),

Uma função $f: A \rightarrow B$ consta de três partes: um conjunto A , chamado o domínio da função (ou o conjunto onde a função é definida), um conjunto B , chamado de contradomínio da função, ou o conjunto onde a função toma valores, e uma regra que permite associar, de modo bem determinado, a cada elemento $x \in A$, um único elemento $f(x) \in B$, chamado o valor que a função assume em x (ou no ponto x).

Assim, uma função nada mais é que uma receita (um algoritmo) que nos ensina como associar cada elemento de A a um único elemento de B . Quanto as notações, uma função f , de A em B , é comumente indicada por $f: A \rightarrow B$ (como já vimos anteriormente), ou $A \xrightarrow{f} B$, ou então $x \rightarrow f(x)$ para indicar que $f(x)$ é o valor associado à x por f . Dizemos que $y = f(x)$ é a imagem de x por f .

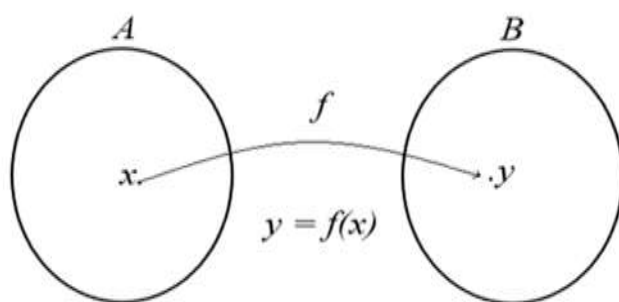


Figura 1: Uma função f de A em B . Fonte: Autoria própria.

Lima (2013) nos ensina ainda duas coisas importantes sobre funções:

1ª) Para todo $x \in A$, deve existir ao menos um $y \in B$, tal que, $y = f(x)$. Ou seja, a regra que ensina como obter $f(x)$ a partir de x deve valer para todos os elementos x do domínio de f ;

2ª) Um elemento $x \in A$ só pode ter uma imagem $y = f(x) \in B$. Isto significa que se existir $x \in A$, tal que, $f(x) = y$ e $f(x) = y'$, então $y = y'$.

Exemplo 1: Fazendo $A = \mathbb{R}$ e $B = \mathbb{Z}$, podemos definir uma função $f: \mathbb{R} \rightarrow \mathbb{Z}$ pondo, para cada $x \in \mathbb{R}$, $f(x) = [x] = \text{parte inteira de } x$. Onde $[x]$ é o maior inteiro que não excede x .

Definição 1: Uma função $f: \mathbb{R} \rightarrow \mathbb{R}$ dada por, $f(x) = ax + b$, onde a e b são números reais é chamada de Função Afim.

Note que, quando $a = 0$, temos a função constante $f(x) = b$ que é um caso particular de Função Afim. Outros exemplos de Funções Afins são: $f(x) = ax$, (no caso em que temos $b = 0$ e $a \neq 0$), conhecida também como função linear, $f(x) = x + b$ (Função Translação), $f(x) = 2x + 1$, neste caso temos $a = 2$ e $b = 1$, etc. Outros conceitos relacionados à teoria das Funções Afins, como gráfico, taxa de variação e teorema de caracterização, por exemplo, não serão tratados aqui.

Definição 2: Dizemos que duas funções f e g são iguais se elas possuírem o mesmo domínio, o mesmo contradomínio e a mesma lei de associação. Ou seja, dadas as funções $f: A \rightarrow B$ e $g: C \rightarrow D$, $f = g \Leftrightarrow A = C, B = D$ e $f(x) = g(x)$ para todo $x \in A$.

Definição 3: Seja dada uma função $f: A \rightarrow B$, f é chamada de injetiva se dados x_1 e x_2 em A , com $x_1 \neq x_2$, tivermos $f(x_1) \neq f(x_2)$ em B . Ou seja, uma função é injetiva quando elementos distintos no domínio possuem imagens distintas no contradomínio.

Exemplo 2: Toda função afim $f: \mathbb{R} \rightarrow \mathbb{R}$; $f(x) = ax + b$, com $a \neq 0$, é injetiva. Com efeito, dados x_1 e x_2 em $\mathbb{R}$, com $x_1 \neq x_2$, temos:

$$ax_1 \neq ax_2 \Rightarrow ax_1 + b \neq ax_2 + b \Rightarrow f(x_1) \neq f(x_2).$$

Definição 4: Seja $f: A \rightarrow B$ uma função. Dizemos que f é sobrejetiva se para todo elemento $y \in B$ existe ao menos um $x \in A$ tal que $y = f(x)$. Ou seja, todo elemento de B é imagem de algum elemento em A . Dizemos que B é a imagem de f e denotamos por $B = \text{Im}(f)$.

Uma função também será dita sobrejetiva se $f(A) = B$. Para obter algumas propriedades importantes com relação a imagens de subconjuntos de A por f consulte Lima (2013, p. 17-18).

Exemplo 3: A função $f: \mathbb{R} \rightarrow \mathbb{R}$ dada por $f(x) = 2x + 1$ é sobrejetiva. Com efeito, dado um $y \in \mathbb{R}$, existe $x \in \mathbb{R}$, $x = \frac{y-1}{2}$, tal que, $f(x) = f\left(\frac{y-1}{2}\right) = 2 \cdot \frac{y-1}{2} + 1 = (y-1) + 1 = y$.

Definição 5: Uma função $f: A \rightarrow B$ é dita bijetiva se for injetiva e sobrejetiva simultaneamente.

Exemplo 4: A função $f: \mathbb{R} \rightarrow \mathbb{R}$ dada por $f(x) = 2x + 1$ é bijetiva. É também bijetiva a função $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ dada por $f(x) = x^2$. A sobrejetividade dela é provada em Lima (2013).

Exemplo 5: A função $f: \mathbb{R} \rightarrow \mathbb{R}$ dada por $f(x) = |x|$, onde $|x|$ denota o valor absoluto de x , não é injetiva, pois, por exemplo, $f(-1) = |-1| = |1| = f(1)$. Portanto, f não é bijetiva.

Seja dada uma função $f: A \rightarrow B$ e um subconjunto $X \subset A$. Chama-se imagem de X por f o conjunto de todos os elementos $f(x)$, onde $x \in X$. Isto é, $f(X) = \{f(x) \in B; x \in X\}$.

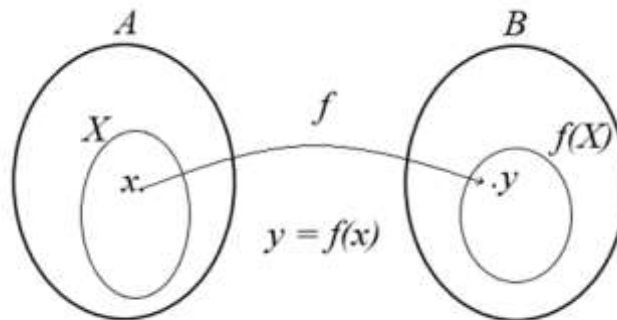


Figura 2: Imagem de um Conjunto por meio de uma Função f . Fonte: Autoria própria

A imagem inversa de um subconjunto $Y \subset B$ será definida como sendo o conjunto de todos os $x \in A$ tais que $f(x) \in Y$. Esse conjunto é indicado na literatura por $f^{-1}(Y)$. Isto é, $f^{-1}(Y) = \{x \in A; f(x) \in Y\}$.

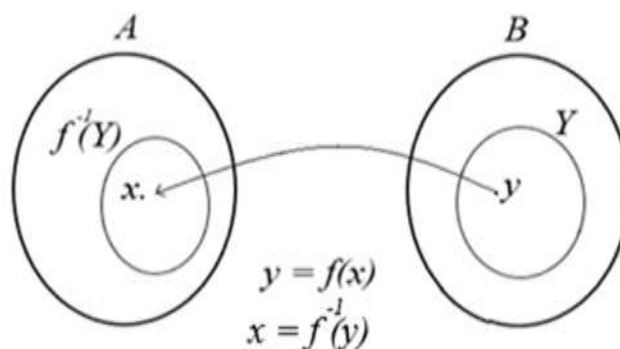


Figura 3: Imagem inversa de um Conjunto por meio de uma Função f . Fonte: Autoria própria.

Para obter algumas propriedades importantes com relação a imagens inversas de subconjuntos $Y \subset B$ por f consulte Lima (2013, p. 19-20).

Outra operação importante entre funções é a operação de composição. Em Dante (2011), o leitor encontrará uma rica fonte de informações sobre funções em nível de ensino básico, onde a função composta é definida da seguinte forma.

Definição 6: Dadas as funções $f:A \rightarrow B$ e $g:B \rightarrow C$, denominamos função composta de g e f a função $g \circ f: A \rightarrow C$, que é definida por $(g \circ f)(x) = g(f(x))$, $x \in A$. (DANTE, 2011, p. 50).

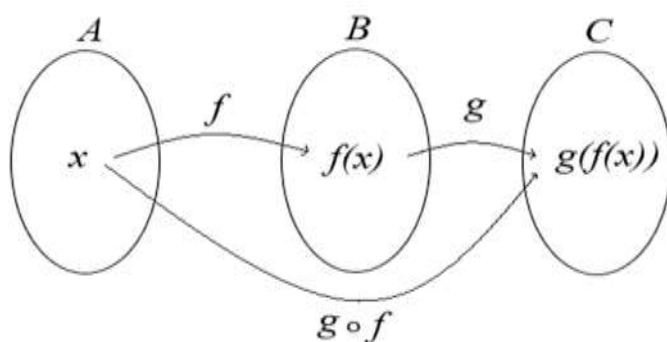


Figura 4: Composição de Funções. Fonte: Autoria própria.

Exemplo 6: Dadas as funções $f: \mathbb{R} \rightarrow \mathbb{R}$, tal que, $f(x) = x^2$ e $g: \mathbb{R}^+ \rightarrow \mathbb{R}$, tal que $g(x) = \sqrt{x}$, teremos $g \circ f: \mathbb{R} \rightarrow \mathbb{R}$ dada por $(g \circ f)(x) = g(f(x)) = \sqrt{x^2} = |x|$.

Finalizaremos estas considerações sobre funções apresentando o importante conceito de função inversa. Para isso, vamos entender o que é função inversa à direita e função inversa à esquerda para uma função $f: A \rightarrow B$.

Definição 7: Uma função $g: B \rightarrow A$ será dita uma *inversa à esquerda* para f se $(g \circ f)(x) = g(f(x)) = x$ para todo $x \in A$. De modo análogo, $g: B \rightarrow A$ será dita uma *inversa à direita* para f se $(f \circ g)(x) = f(g(x)) = y$ para todo $y \in B$. Por fim, se $g: B \rightarrow A$ for uma inversa à direita e à esquerda para $f: A \rightarrow B$, diremos simplesmente que g é uma *inversa* para f .

Exemplo 7: Dadas as funções $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$, tal que $f(x) = x^2$, e $g: \mathbb{R}^+ \rightarrow \mathbb{R}^+$, definida por $g(x) = \sqrt{x}$, teremos: $(g \circ f)(x) = g(f(x)) = \sqrt{x^2} = |x| = x$. Além disso,

$$(f \circ g)(x) = f(g(x)) = (\sqrt{x})^2 = x. \text{ Logo, } g \text{ é uma inversa para } f.$$

Teorema 1: Uma função $f: A \rightarrow B$ admite inversa à esquerda se, e somente se, for injetiva, e inversa à direita se, e somente se, for sobrejetiva.

Teorema 2: Se a função f tem por inversa à direita a função g e por inversa à esquerda a função h , então $g = h$ é a função inversa de f , e f será dita *invertível*.

Os Teoremas 1 e 2 nos ensinam que uma função f admite inversa se, e somente se, é bijetiva, e essa inversa, caso exista, é única. Para indicar a função inversa de $f: A \rightarrow B$ usamos a notação $f^{-1}: B \rightarrow A$. Para uma demonstração destes teoremas, consulte Lima (2013).

O exposto até aqui sobre funções é suficiente para entendermos o papel dela na Criptografia, apresentado na seção a seguir.

3. UM MÉTODO CRIPTOGRÁFICO INTUITIVO UTILIZANDO FUNÇÕES AFINS

O objetivo desta seção é apresentar um exemplo bem didático (e intuitivo) de uma cifra utilizando as Funções Afins. O valor didático desse exemplo reside no fato de que podemos trabalhar várias noções básicas sobre essas funções, tais como: definição (exibir exemplos de Funções Afins), imagem de um elemento do domínio, cálculo da Função Inversa, imagem inversa de um elemento, etc. O professor pode ampliar as aplicações desse exemplo, buscando relacionar outros conceitos.

Inicialmente, iremos utilizar a Tabela 1 de pré-codificação. O método criptográfico que apresentamos possui como espaço de texto comum o alfabeto $\{1, 2, 3, 4, \dots, 26\}$. Ele é uma cifra de blocos com comprimento 1, isto é, codifica letra por letra. Seu espaço de texto cifrado é um subconjunto (finito) de $\mathbb{N}$. Ou seja, cada letra será codificada em um número. Assim, a mensagem codificada passa a ser representada por uma sequência de números separados por um traço.

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Tabela 1: Tabela de Pré-codificação. Fonte: Autoria própria.

A seguir, apresentamos um guia de desenvolvimento e aplicação do método, através de um exemplo numérico. Para tal, iremos codificar a mensagem CRIPTOGRAFIA NO PROFMAT. O Roteiro 1 apresenta o processo de codificação, isto é, transformar a mensagem desejada em um código. O Roteiro 2 apresenta o processo de decodificação, ou seja, como fazer transformar tal código na mensagem inicial.

Roteiro 1 – Processo de codificação do método

Etapa 1 - Nesta etapa iremos escolher, como exemplo, uma mensagem curta para ser codificada por um método criptográfico simples baseado em funções afins. A vantagem desse método é que sua

simplicidade torna possível utilizar exemplos de codificação com mensagens longas sem se preocupar com cálculos extensos. Logo, é uma ótima alternativa para trabalhar em sala de aula com variados tipos de exemplos.

Etapa 2 - Aqui inicia-se o processo de pré-codificação. Usando a Tabela 1, substituímos cada letra da mensagem CRIPTOGRAFIA NO PROFMAT pelo número que lhe é correspondente, separando-os por um traço (-). Logo, a mensagem passará a ser:

3-18-9-16-20-15-7-18-1-6-9-1-14-15-16-18-15-6-13-1-20.

Etapa 3 - Agora iremos utilizar o conhecimento sobre funções afins para desenvolver um processo de codificação criptográfica, isto é, uma função de codificação criptográfica. A função de codificação que iremos utilizar será uma Função Afim. Para obtê-la, começamos escolhendo um par ordenado (a, b) (com a e b inteiros para evitar números fracionários, raízes, etc). Depois, consideraremos a função de codificação criptográfica como sendo $f(x) = ax + b$, onde a variável x , de acordo com a Tabela 1, será um número natural pertencente ao conjunto $\{1, 2, 3, \dots, 26\}$. Sendo assim, tomemos, por exemplo, o par $(2, 1)$ como chave de codificação, isto é, nossa função de codificação será $f(x) = 2x + 1$.

Etapa 4 - Da Etapa 2 temos que a mensagem CRIPTOGRAFIA NO PROFMAT passa a ser representada pela sequência de números (blocos)

3-18-9-16-20-15-7-18-1-6-9-1-14-15-16-18-15-6-13-1-20.

Da Etapa 3, cada um desses blocos será codificado por meio da função $f(x) = 2x + 1$, onde iremos calcular a imagem de cada número que compõe a mensagem. Cada uma dessas imagens será a codificação do número (bloco) correspondente. Devemos respeitar a sequência dos números, e os resultados devem ser separados por traço na mesma ordem. Esta nova sequência é a codificação da mensagem original.

Agora utilizaremos nosso conhecimento sobre cálculo do valor de uma Função Afim num ponto x para codificar cada bloco da mensagem original. Calculando a imagem de cada bloco da mensagem 3-18-9-16-20-15-7-18-1-6-9-1-14-15-16-18-15-6-13-1-20, obtemos:

Bloco (x)	Função de codificação ($f(x) = 2x + 1$)	Bloco codificado ($y = f(x)$)
3	$f(3) = 2 \cdot 3 + 1 = 7$	7
18	$f(18) = 2 \cdot 18 + 1 = 37$	37
9	$f(9) = 2 \cdot 9 + 1 = 19$	19
16	$f(16) = 2 \cdot 16 + 1 = 33$	33
20	$f(20) = 2 \cdot 20 + 1 = 41$	41
15	$f(15) = 2 \cdot 15 + 1 = 31$	31
7	$f(7) = 2 \cdot 7 + 1 = 15$	15
14	$f(14) = 2 \cdot 14 + 1 = 29$	29
6	$f(6) = 2 \cdot 6 + 1 = 13$	13
13	$f(13) = 2 \cdot 13 + 1 = 27$	27
1	$f(1) = 2 \cdot 1 + 1 = 3$	3

Tabela 2: Codificando a Mensagem. Fonte: Autoria própria.

Daí, a mensagem codificada passará a ser:

7-37-19-33-41-31-15-37-3-13-19-3-29-31-33-37-31-13-27-3-41.

Substituímos cada número pela sua imagem por meio da função $f(x) = 2x + 1$.

Portanto, a mensagem CRIPTOGRAFIA NO PROFMAT será substituída por:

7-37-19-33-41-31-15-37-3-13-19-3-29-31-33-37-31-13-27-3-41.

Veja que, nestas condições, a chave utilizada para codificar a mensagem foi o par ordenado (2, 1). Mas, por que fixamos esse par como ordenado? Porque no caso em que $a \neq b$, temos que $(a, b) \neq (b, a)$. Logo, temos duas chaves distintas! Ademais, observe que a mensagem codificada dependerá do par ordenado escolhido. Sem a chave de codificação é difícil desvendar a mensagem original.

Roteiro 2 – Processo de decodificação do método

Codificada a mensagem, nosso proceder agora será desenvolver a função de decodificação criptográfica para o nosso método. Ora, se o bloco x foi substituído por sua imagem $f(x)$, o que devemos fazer para recuperar x ? Como sabemos do estudo sobre funções, x é recuperado quando calculamos a imagem inversa dele. Dessa forma, se $y = f(x)$, então $x = f^{-1}(y)$ (é a imagem de y pela função inversa de f). Portanto, para decodificarmos a mensagem, precisamos saber a função inversa da função de codificação (claro, se ela existir). No caso da função afim, a sua inversa sempre vai existir, pois as funções afins são bijetivas.

Etapla 1 - Bom, temos que a função de codificação criptográfica é $f(x) = 2x + 1$. Então, devemos determinar a função inversa da função $f(x) = 2x + 1$. Isolando x nessa igualdade, temos $x = \frac{f(x)-1}{2} = \frac{y-1}{2}$. Logo, $f^{-1}(y) = \frac{y-1}{2}$. Portanto, a função inversa de f é dada por $f^{-1}(x) = \frac{x-1}{2}$.

Etapla 2 - Como já temos a função de decodificação criptográfica, basta calcular a imagem de cada número na mensagem codificada para obter a mensagem original. Ou seja, calcularemos a imagem de cada número na sequência

7-37-19-33-41-31-15-37-3-13-19-3-29-31-33-37-31-13-27-3-41 por meio da função $f^{-1}(x) = \frac{x-1}{2}$, de acordo com a tabela a seguir.

Bloco (y)	Função de decodificação ($f^{-1}(y) = \frac{y-1}{2}$)	Bloco codificado ($x = f^{-1}(y)$)
7	$f^{-1}(7) = \frac{7-1}{2} = \frac{6}{2} = 3$	3
37	$f^{-1}(37) = \frac{37-1}{2} = \frac{36}{2} = 18$	18
19	$f^{-1}(19) = \frac{19-1}{2} = \frac{18}{2} = 9$	9
33	$f^{-1}(33) = \frac{33-1}{2} = \frac{32}{2} = 16$	16
41	$f^{-1}(41) = \frac{41-1}{2} = \frac{40}{2} = 20$	20
31	$f^{-1}(31) = \frac{31-1}{2} = \frac{30}{2} = 15$	15
15	$f^{-1}(15) = \frac{15-1}{2} = \frac{14}{2} = 7$	7

29	$f^{-1}(29) = \frac{29-1}{2} = \frac{28}{2} = 14$	14
13	$f^{-1}(13) = \frac{13-1}{2} = \frac{12}{2} = 6$	6
27	$f^{-1}(27) = \frac{27-1}{2} = \frac{26}{2} = 13$	13
3	$f^{-1}(3) = \frac{3-1}{2} = \frac{2}{2} = 1$	1

Tabela 3: Decodificando a Mensagem. Fonte: Autoria própria.

Assim, tendo decodificado cada número, fica fácil recuperar a mensagem. Basta substituir os números na mensagem 7-37-19-33-41-31-15-37-3-13-19-3-29-31-33-37-31-13-27-3-41 codificada por seus correspondentes na tabela anterior. A mensagem torna-se então:

3-18-9-16-20-15-7-18-1-6-9-1-14-15-16-18-15-6-13-1-20.

Por meio da tabela de pré-codificação (Tabela 1), podemos observar as letras correspondentes a esses números e obter a mensagem original.

CRIPTOGRAFIA NO PROFMAT.

Agora um detalhe técnico: como a função de decodificação consiste na inversa da função $f(x) = 2x + 1$, temos que a chave de decodificação é $(\frac{1}{2}, -\frac{1}{2})$, pois $f^{-1}(x) = \frac{x-1}{2} = \frac{1}{2}x - \frac{1}{2}$. De modo geral, se codificarmos uma mensagem com chave (a, b) , com $a \neq 0$, temos que a chave de decodificação será $(\frac{1}{a}, -\frac{b}{a})$, pois se $a \neq 0$, a inversa da função $f(x) = ax + b$ é $f^{-1}(x) = \frac{x-b}{a} = \frac{1}{a}x + (-\frac{b}{a})$.

Os Exemplos a seguir trazem mais algumas alternativas para explorar a relação entre criptografia e funções afins por meio do método descrito anteriormente. Juntos, os roteiros desenvolvidos e os exemplos constituem um bom guia para tratar a relação entre funções afins e criptografia em sala de aula, trabalhando os conceitos matemáticos envolvidos por meio da resolução de problemas e codificação criptográfica.

Exemplo 8: Codifique, com base na Tabela 1 e na chave (3, 10), a mensagem: O SEGREDO DO COFRE É SUA DATA DE NASCIMENTO.

Solução: Com base na Tabela 1, a mensagem dada torna-se a seguinte sequência de blocos:

15-19-5-7-18-5-4-15-4-15-3-15-6-18-5-5-19-21-1-4-1-20-1-4-5-14-1-19-3-9-13-5-14-20-15.

Como a chave de codificação é função de codificação $(3, 10)$, segue que a função de codificação criptográfica é dada por $f(x) = 3x + 10$. Assim, calculando a imagem de todos os números que aparecem na sequência anterior, correspondente à mensagem original, teremos:

x	1	3	4	5	6	7	9	13	14	15	18	19	20	21
$f(x)$	13	19	22	25	28	31	37	49	52	55	64	67	70	73

Tabela 4: Codificação da Mensagem do Exemplo 8. Fonte: Autoria própria.

Logo, a mensagem codificada será dada por:

55-67-25-31-64-25-22-55-22-55-19-55-28-64-25-25-67-73-13-22-13-70-13-22-25-52-13-67-19-37-49-25-52-70-55.

Exemplo 9: Vamos supor que um estudante A está utilizando esse método de criptografia com funções afins para mandar mensagens secretas para outro estudante B na sala de aula. Um terceiro estudante, C, está interessado em saber o conteúdo das mensagens trocadas por A e B. No entanto, C não possui a chave de decodificação envolvida no processo, pois ele é um intruso nessa situação. Obstinado a quebrar o código utilizado por A e B, C descobriu, de alguma forma, que por meio da função de codificação utilizada por A, o número 1 passa a ser representado por 52, e o número 5 passa a ser representado por 188. Pergunta-se: com essa nova informação, C tem condições de quebrar o código utilizado pelos estudantes A e B? Suponha que C sabe que o método utilizado por A e B é este baseado em funções afins, e que a pré-codificação é dada na Tabela 1.

Solução: Sim! De fato, como C sabe que A e B estão codificando usando uma função do tipo $f(x) = ax + b$, então ele sabe que basta conhecer os valores de a e b para obter as funções de codificação e decodificação criptográficas. Ora, com a informação que C possui, ele pode concluir que $f(1) = 52$ e $f(5) = 188$. Logo, substituindo essas informações na expressão $f(x) = ax + b$, obtêm-se: $a + b = 52$ e $5a + b = 188$. Portanto, para saber os valores de a e b , C só precisa resolver o sistema a seguir:

$$\begin{cases} a + b = 52 \\ 5a + b = 188. \end{cases}$$

Subtraindo a primeira equação da segunda, temos $4a = 188 - 52 = 136$. O que implica que $a = \frac{136}{4} = 34 \Rightarrow b = 52 - a = 52 - 34 = 18$. Daí, C conclui que $a = 34$ e $b = 18$. Logo, a função utilizada para criptografar as mensagens é $f(x) = 34x + 18$. Com esta função em mãos, o estudante

C pode facilmente decifrar as mensagens trocas por A e B. Claro, supondo que A e B não modifiquem algum elemento na utilização desse método de criptografia.

4. CONSIDERAÇÕES FINAIS

Em nível elementar, a teoria que garante a segurança imposta pela criptografia deriva de conceitos simples de matemática que são aprendidos até o fim do Ensino Médio. Portanto, não é difícil falar de criptografia na escola e, mais ainda, de suas aplicações no nosso cotidiano. Ao fazer isso, levamos o aluno a conhecer essa importante inteligência que nos proporciona a segurança necessária nas nossas transações bancárias, comerciais, compras e trocas de mensagens pela internet, entre outras. Mais fundamental ainda é fazer com que o aluno seja levado a perceber o quão significativa é a matemática para nossa vida. Não é só uma questão de explorar determinados conceitos de matemática em criptografia, e sim educar e situar os estudantes no meio tecnológico e computacional o mais cedo possível.

Desse modo, como mais um auxílio para o professor em sala de aula, desenvolvemos alguns roteiros relacionados à aplicação de métodos criptográficos na codificação de mensagens utilizando a Função Afim. Tais roteiros funcionam como guias para a aplicação de atividades envolvendo criptografia. De modo geral, fica claro que as relações apresentadas e os exemplos dados funcionarão como fonte de inspiração de atividades (essa é a intenção) que serão elaboradas pelo próprio professor (e de acordo com o nível e experiência de cada turma) em sala de aula. Entretanto, é preciso destacar que tais atividades só serão bem confeccionadas e aplicadas se o professor estiver disposto a adentrar e estudar o tema criptografia e matemática na temática proposta por esse trabalho. Só assim ele será capaz de extrair as aplicações do texto e agregá-las a suas aulas. Além de motivá-lo a criar outros exercícios inspirados nos exemplos aqui propostos.

Deste breve estudo sobre matemática e criptografia, fica a certeza de que a criptografia é um tema inovador em sala de aula (apesar de ser uma ciência bem antiga) e que, quando corretamente tratada, fornece ao professor uma ferramenta poderosíssima para melhorar a qualidade do ensino e aprendizagem em matemática, tornando suas aulas mais criativas, atrativas, com mais rendimentos e mais próxima da realidade do aluno. Os benefícios para o aluno são inúmeros. Podemos incluir, entre outras, o desenvolvimento do seu raciocínio lógico-dedutivo e de suas habilidades de resolução de problemas. Sem contar que trabalhar o tema criptografia na educação básica fornece uma ótima

oportunidade para que o aluno possa ser inserido no campo dessas ciências que dominam a tecnologia da computação.

REFERÊNCIAS

- BALESTRI, R. Matemática 1: Interação e Tecnologia. 2ª ed. São Paulo: LEYA, 2016.
- BIANCHINI, E. Matemática Bianchini, 9º ano. 9ª ed. São Paulo: MODERNA, 2018.
- BRANDÃO, M. M. D. Uma Adaptação da Cifra de Hill para Estudo de Matrizes. 91f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT), Universidade Federal de Ouro Preto, Ouro Preto/MG, 2017.
- BUCHMANN, J. A. Introdução à Criptografia. São Paulo: BERKELEY, 2002.
- COUTINHO, S. C. Números Inteiros e Criptografia RSA. 2ª ed. Rio de Janeiro: IMPA, 2005.
- DANTE, L. R. Matemática, 1ª série. 1ª ed. São Paulo: Ática, 2006.
- FLEMMING, D. M.; GONÇALVES, M. B. Cálculo A: funções, limite, derivação e integração. 6ª ed. São Paulo: PEARSON PRENTICE HALL, 2009.
- FRANÇA, W. B. A. A utilização da Criptografia para uma Aprendizagem Contextualizada e Significativa. 63f. Dissertação (Mestrado Profissional em Matemática), Universidade de Brasília - UNB, Brasília, 2014.
- GIOVANNI JÚNIO, J. R.; CASTRUCCI, B. A Conquista da Matemática, 9º ano. 4ª ed. São Paulo: FTD, 2018.
- GUIDORIZZI, H. L. Um Curso de Cálculo, vol. 1. 5ª ed. Rio de Janeiro: LTC, 2018.
- IEZZI, G.; DOLCE, O.; DEGENSZAJN, D.; PÉRIGO, R. Matemática, volume único. 1ª ed. São Paulo: ATUAL, 2002.
- JESUS, A. L. N. de. Criptografia na Educação Básica: utilização da criptografia como elemento motivador para o ensino aprendizagem de matrizes. 82f. Dissertação (Mestrado Profissional em Rede Nacional em Matemática - PROFMAT), Universidade Federal do Vale do São Francisco, Juazeiro/BH, 2013.
- LIMA, E. L.; CARVALHO, P. C. P.; WAGNER, E.; MORGADO, A. C. A Matemática do Ensino Médio, vol. 1. 9ª ed. Rio de Janeiro: SBM, 2006.
- LIMA, E. L.; CARVALHO, P. C. P.; WAGNER, E.; MORGADO, A. C. A Matemática do Ensino Médio, vol. 2. 6ª ed. Rio de Janeiro: SBM, 2006.
- LIMA, E. L. Curso de Análise, vol. 1. 14ª ed. Rio de Janeiro: IMPA, 2013.
- MEDEIROS, W. da S. Números Primos e Criptografia RSA: uma descrição da mais bela relação em teoria dos números. 70f. Monografia (Licenciatura Plena em Matemática), Universidade do Estado do Rio Grande do Norte – UERN. Patu/RN, 2017.
- PEREIRA, N. M. I. Criptografia: uma nova proposta de ensino de matemática no ciclo básico. 76f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT), Universidade Estadual Paulista “Júlio de Mesquita Filho”, Ilha Solteira/SP, 2015.
- SINGH, S. O livro dos códigos. 4ª ed. Rio de Janeiro: Record, 2004.

Capítulo 6



10.37423/220305625

FUNÇÕES QUADRÁTICAS E CRIPTOGRAFIA

Maria Joseane Felipe Guedes Macêdo

*Universidade Federal Rural do Semi-Árido -
UFERSA*

Willa da Silva Medeiros

*Universidade Federal Rural do Semi-Árido -
UFERSA*



1. INTRODUÇÃO

Recentemente o Brasil passou a integrar o grupo de elite em pesquisa matemática mundial. Somos uma potência em matemática, ao lado de outras grandes potências como Estados Unidos, China, França e Alemanha¹. Chega a ser espantoso o fato de que essa potencialidade ainda não se refletiu na educação básica. Ainda não conseguimos alcançar patamares mais elevados e o estado atual em que se encontra o ensino e a aprendizagem em matemática básica é crítico.

O Brasil é um dos países com pior desempenho em matemática na educação básica como mostra as avaliações educacionais já realizadas. O último PISA (PROGRAMA INTERNACIONAL DE AVALIAÇÃO DE ALUNOS), realizado em 2018, mostrou que apesar de um pequeno aumento na média, o Brasil não conseguiu atingir uma melhoria significativa no desempenho dos estudantes em relação às disciplinas de Matemática, Língua Portuguesa e Ciências, ficando entre os 10 países com pior desempenho no ranking mundial².

Se tratando de matemática, e de frente a essa real situação, é de extrema importância e urgência a criação e desenvolvimento de práticas inovadoras de ensino e metodologias que possam proporcionar avanços expressivos no ensino e aprendizagem em matemática na educação básica. Nesse conjunto de metodologias, a prática de desenvolver o ensino de matemática por meio da contextualização e interdisciplinaridade dos conteúdos vem se tornando cada vez mais frequente entre os docentes. O ensino de matemática ao ser relacionado com o cotidiano do aluno e com outras ciências torna-se mais prazeroso, produtivo e significativo, pois o aluno pode ver a importância de um determinado conhecimento, não apenas dentro da própria disciplina, mas em outras áreas do saber, e isso dá mais sentido ao estudo realizado.

Assim, a contextualização e a interdisciplinaridade, como forma de apresentar as aplicações da matemática em outros campos, são ferramentas poderosas que já vêm sendo bastante usadas no ensino, não só de matemática. Brousseau (1996), citado por Pinheiro (2012), entende que a contextualização ocorre quando o aluno é levado a estudar um conteúdo por meio de uma situação-problema, sendo essa situação próxima à realidade do aluno e, mais ainda, que esteja inserida num cenário capaz de atribuir significado e sentido ao objeto de estudo. Desse modo, observamos que dar sentido ao conteúdo ensinado por meio de situações é de extrema importância. Isso se reflete em matemática, como resposta àquelas perguntas que todo professor de matemática já ouviu: isso serve para quê? Onde vou usar isso na minha vida?

A criptografia é a ciência que estuda os métodos para tornar o conteúdo de uma mensagem incompreensível para todos aqueles que não têm permissão de lê-la, de modo que somente o destinatário legítimo possa obter a mensagem verdadeira. Com a evolução da criptografia e o surgimento da criptografia de chave pública, a matemática passou a ser o pilar de sustentação de toda teoria que assegura confiança e segurança aos métodos criptográficos. Portanto, não é difícil falar de criptografia na escola e de suas aplicações no nosso cotidiano. Ao fazer isso, aproximamos o aluno dessa importante ciência que proporciona a segurança necessária nas transações bancárias, comerciais, compras e trocas de mensagens pela internet, etc. Introduzindo o aluno à conteúdos que envolvem o meio tecnológico e computacional, além de fazê-los perceber a importância da matemática em eventos do seu cotidiano.

Neste contexto, a presente pesquisa objetiva investigar a relação entre matemática básica e criptografia, através das funções polinomiais de segundo grau (função quadrática), descrevendo um método bem elementar de criptografia baseado em tal função. Propomos atividades onde a criptografia será chave para a motivação do estudo. Essa relação inesperada entre determinados conteúdos de matemática e criptografia torna-se elemento fundamental de inspiração, motivação e atração nas aulas de matemática. Este estudo fundamenta-se em obras como Buchmann (2002), Brandão (2017), Coutinho (2005), França (2014), Jesus (2013), Medeiros (2017), entre outros. Nas seções seguintes apresentaremos alguns conceitos básicos sobre criptografia e funções quadráticas, essenciais para o bom entendimento do método proposto.

2. UM BREVE HISTÓRICO E ALGUMAS NOÇÕES BÁSICAS SOBRE CRIPTOGRAFIA

Nesta seção, faremos um breve histórico sobre a criptografia e apresentaremos alguns conceitos básicos necessários ao entendimento do método proposto. Além de dar um pequeno embasamento teórico sobre o tema.

2.1 UM POUCO DE HISTÓRIA

Precisar quando os códigos secretos surgiram é algo muito complicado, pois há inúmeros relatos da utilização de códigos em envios de mensagens em épocas remotas e em períodos diferentes da história da humanidade. Acredita-se, e seria o natural supor, com base nos relatos históricos, que os primeiros procedimentos para ocultar a existência de uma mensagem ao ser enviada surgiram com maior evidência no período das grandes guerras ocorridas há milhares de anos. De fato, “durante milhares de anos, reis, rainhas e generais dependeram de comunicações eficientes de modo a

governar seus países e comandar seus exércitos” (SINGH, 2004, p.11). Essa dependência de uma comunicação mais segura provocou o início da era dos códigos secretos. “Foi a ameaça da interceptação pelo inimigo que motivou o desenvolvimento de códigos e cifras, técnicas para mascarar uma mensagem de modo que só o destinatário possa ler seu conteúdo” (SINGH, 2004, p. 11).

No primeiro capítulo de Singh (2004) consta que um dos primeiros relatos relacionados à utilização de escritas secretas se deve ao grande historiador Heródoto, conhecido como o pai da história.

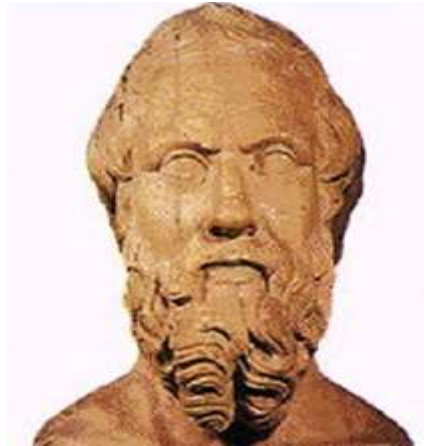


Figura 1: Heródoto. Fonte: <https://images.app.goo.gl/6Dcu5Aq4d4enZZij9>

Nesse contexto, Besselaar (1962) ainda nos situa no ambiente no qual se desenvolveu todo o trabalho de Heródoto. O autor comenta:

Heródoto viveu, globalmente falando, entre os dois grandes conflitos do povo grego no século V, entre as guerras persas e as guerras do Peloponeso, isto é, numa Grécia vitoriosa sobre os bárbaros e cheia de si, numa Grécia dolorosamente dividida por correntes de separatismo e por tentativas de imperialismo, mas numa Grécia ainda não dilacerada, massacrada e humilhada. Neste ambiente viveu e respirou Heródoto, deste ambiente sua obra é a eloquente expressão [...]. (BESSELAAR 1962, p. 7)

Nesse ambiente, Heródoto narra um episódio sobre os conflitos entre a Grécia e a Pérsia ainda no século V a.C. onde se observa a utilização de uma manobra para enviar uma mensagem secretamente. Para entender como tudo se originou, devemos nos ater as palavras de Singh (2004), que nos diz:

A antiga inimizade entre a Grécia e a Pérsia evoluiu para uma crise logo depois que Xerxes começou a construir a cidade de Persépolis, a nova capital do seu reino. Presentes e tributos chegaram de todas as regiões do império e dos estados vizinhos, com a notável exceção de Atenas e Esparta. Determinado a vingar esta insolência, Xerxes começou a mobilizar um exército [...]. Ele passou os cinco anos seguintes montando secretamente a maior força de combate da história. Então, no ano 480 a.C., ele estava pronto para lançar um ataque-surpresa. (SINGH, 2004, p. 20)

Xerxes é o rei, líder dos persas. No entanto, ao elaborar seu ataque ao povo grego, ele não imaginava que seus planos estavam sendo observados por outra pessoa que não era seu aliado. Esta outra pessoa se chamava Demarato³, um grego que mesmo depois de ser expulso da Grécia ainda era fiel ao seu país de origem e estava disposto a tudo para salvar sua terra natal do terrível ataque do exército persa. Havia, entretanto, um problema: como fazer para avisar os gregos sobre o ataque de Xerxes? Segundo Heródoto, citado por Singh (2004):

O perigo de ser descoberto era grande; havia apenas um modo pelo qual a mensagem poderia passar: isso foi feito raspando a cera de um par de tabuletas de madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mesma foi coberta novamente com cera. Deste modo, as tabuletas pareciam estar em branco e não causariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de perceber o segredo, até que, pelo que entendi, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles raspassem a cera encontrariam alguma coisa escrita na madeira. Isso foi feito, revelando a mensagem, então transmitida para os gregos.

Com isso, graças à engenhosidade de Demarato, os gregos tiveram condições de se preparar para o ataque de Xerxes, se armando fortemente para tal fim. Assim, ainda segundo Singh (2004), com a perda do elemento surpresa, o rei Xerxes e todo o seu exército foram surpreendidos e encurralados na baía de Salamina, aos arredores de Atenas, perdendo o confronto humilhantemente para o exército grego. Graças a uma escrita secreta, os gregos foram capazes de se livrar dos persas e vencer a guerra.

O relato feito por Heródoto, citado por Singh (2004), representa um dos primeiros que trata da utilização de um método primitivo para mascarar a existência de uma mensagem. Veja que Demarato se preocupou em esconder a mensagem e não seu conteúdo. Este tipo de estratégia era muito comum e foi a primeira a ser utilizada pelo ser humano para esconder os vestígios de suas comunicações secretas. Quando usamos algum meio para esconder a mensagem em nossas comunicações, estamos praticando a esteganografia. Mais precisamente, temos que “a comunicação secreta, quando é obtida através da ocultação da mensagem, é conhecida como esteganografia, nome derivado das palavras gregas *steganos*, que significa coberto, e *graphein*, que significa escrever” (SINGH, 2004, p. 21). Existem na literatura vários exemplos de esteganografia, um deles é devido ao povo chinês. Segundo Singh (2004), para esconder uma mensagem os chineses a escrevia numa seda fina que era então amassada em formato de bolinha e envolvida numa cera. Para o transporte dessa mensagem, o mensageiro a engolia, escondendo assim sua existência.

Podemos observar que com esses métodos mais rudimentares, embora a mensagem estivesse oculta e isso representasse certa segurança, era necessário algo mais para impor um alto nível de segurança

nos envios de informações privadas. Era preciso que além da anulação visível, fosse desenvolvido algum meio para tornar o conhecimento da informação por parte de terceiros não autorizados, mais difícil. Métodos e alternativas para modificar o texto original de uma mensagem, tornando-o ilegível para aqueles que não fossem seu real destinatário, impulsionaram o desenvolvimento da criptografia.

2.2 ALGUNS CONCEITOS BÁSICOS

Na criptologia⁴, qualquer método que consiste em substituir uma letra do alfabeto original, a qual consta na mensagem, por outra letra ou símbolo é chamado de Cifra. Podemos citar as cifras de substituição (métodos de codificação por substituição) e as cifras de transposição (métodos de codificação por transposição). No entanto, precisamos deixar claro que, estritamente falando, cifra e código não são a mesma coisa, embora em alguns momentos essas ideias se confundam.

O conceito de cifra se refere a qualquer mecanismo de criptografia que se resume a converter cada letra do alfabeto original em outra letra ou um símbolo qualquer. Quando usamos uma cifra para modificar o significado real de uma mensagem, dizemos que a mensagem foi cifrada. Por outro lado, utilizaremos a palavra codificar para denotar o processo de mudar o significado original de uma mensagem por meio de um método de criptografia, seja ele cifra ou não. Então, decodificar será usado para descrever o processo inverso.

Já a palavra decifrar é, precisamente falando, o processo de desfazer uma codificação que foi feita através de uma cifra (SINGH, 2004). Entretanto, há autores como Sautoy (2007) que entende este conceito como sendo o ato de um indivíduo descobrir o texto original de uma mensagem por meio do texto codificado, sendo que para isso ele não utiliza o processo específico de decodificação. Ou seja, decifrar para Sautoy (2007) é quebrar o procedimento de codificação, descobrir a mensagem verdadeira, sem, no entanto, ser o legítimo destinatário daquela mensagem. É com este entendimento que optamos em usar a palavra decifrar com este significado.

Por outro lado, “a palavra código se refere a um tipo especial de comunicação secreta, cujo uso vem declinando ao longo dos séculos” (SINGH, 2004, p. 14). Um código é um método de criptografia mais geral do que as cifras no sentido de que agora palavras ou até mesmo frases inteiras podem ser substituídas por outras palavras, números ou símbolos quaisquer. É como se os códigos fossem uma generalização das cifras. Por exemplo,

[...] os agentes secretos usam nomes em códigos no lugar de seus nomes verdadeiros, de modo a esconder suas identidades. De modo semelhante, a frase “ataque ao amanhecer” pode ser substituída pela palavra código “júpiter” e esta palavra será transmitida ao comandante, no campo de batalha, com o fim de confundir o inimigo. (SINGH, 2004, p. 14)

Ou seja, o envio de mensagens por meio de códigos se caracteriza pela definição dos símbolos ou palavras-códigos que substituirão o conteúdo da mensagem original. Nesse caso, o código age como um simplificador da mensagem em questão, pois um trecho ou até mesmo a própria mensagem inteira, podem ser substituídos por um único símbolo ou uma palavra. Este tipo de característica não é comum às cifras. Cabe, então, uma pergunta: qual a diferença técnica entre código e cifra? “tecnicamente um código é definido como uma substituição de palavras ou frases, enquanto a cifra é definida como uma substituição de letras” (SINGH, 2004, p.47). Porém, haverá ocasiões em que vamos nos referir a um tipo de método criptográfico como sendo código, mesmo ele não sendo, necessariamente, um, segundo a definição anterior. Ficará claro no contexto se estamos tratando de uma cifra ou código. No esquema a seguir apresentamos uma divisão das ramificações da escrita secreta.

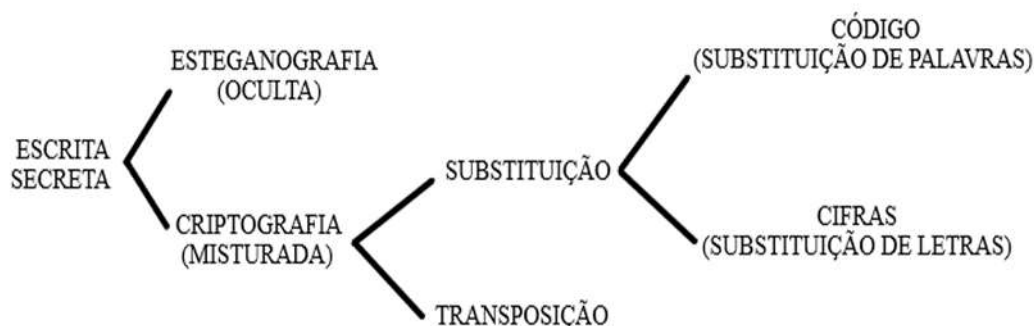


Figura2: Algumas Ramificações da Escrita Secreta. Fonte: Singh (2004).

Dentre inúmeros códigos desenvolvidos ao longo da história da criptografia, destacaremos dois, por se tratarem de sistemas revolucionários que contribuíram fortemente para o desenvolvimento das comunicações e são, até hoje, mundialmente usados: o Código Braille e o Código Morse. O código Braille (ou sistema Braille) foi desenvolvido por Louis Braille (1809 - 1852), um francês que ficou completamente cego ainda criança em decorrência de um acidente sofrido quando manipulava as ferramentas da oficina de seu pai (COSTA, 2009). Uma ligeira versão do sistema criado por Braille foi proposto inicialmente por Charles Barbier de la Serre, um capitão de artilharia que desenvolveu um tipo de código para se comunicar com seus soldados. Daí, poderíamos dizer que o código Braille teve sua essência em um método de esteganografia militar⁵. A ideia do código de Barbier era que os

soldados pudessem ler mensagens no escuro (por isso o código ficou conhecido como escrita no escuro) e, para isso, as mensagens eram transmitidas por meio de pontos em alto relevo que poderiam ser “lidas” com as pontas dos dedos. Já a versão de Braille ainda conserva a disposição de pontos em alto relevo, porém é mais completa e menos complexa, “é constituído por 63 sinais formados por pontos a partir do conjunto matricial :: (123456). Este conjunto de 6 pontos chama-se, por isso, sinal fundamental” (BRASIL, 2006, p.17). Denominamos Célula Braille a qualquer disposição dos pontos do conjunto fundamental, isto é, a qualquer configuração que gere um sinal produzido nesse sistema. A célula vazia é aquela que nenhum ponto se destaca em relação aos demais. Ela também é considerada um símbolo. Logo, o código Braille passa a ser formado por 64 símbolos.

Um dos conceitos mais importantes da criptografia é o de chave. Para entender o que significa uma chave e qual o seu papel nos métodos criptográficos devemos ter bem claro a diferença entre o método geral de criptografia em uso (algoritmo) e o procedimento específico de codificação de uma mensagem por meio desse método. Vamos esclarecer isso através de exemplos: digamos que queremos estabelecer uma comunicação por mensagens e escolhemos uma cifra de César (qualquer translação do alfabeto entre 1 e 25 letras nos fornece uma maneira de definirmos o alfabeto cifrado) como método de codificação. Desse modo, se deslocarmos o alfabeto uma, duas, três ou quatro letras à frente, obtemos cifras de César cujos alfabetos cifrados são, respectivamente, os seguintes:

B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, A

C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, A, B

D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, A, B, C

E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, A, B, C, D

Assim sendo, cada um desses alfabetos cifrados distintos nos dá uma maneira específica de codificar uma mensagem. Portanto, dizemos que cada um desses alfabetos cifrados constitui uma *chave* para a cifra de César, sendo esta cifra o método geral de codificação. Como há 25 maneiras de transladarmos o alfabeto, então a cifra de César possui 25 chaves.

A importância das chaves está ligada a segurança dos métodos criptográficos. O conhecimento do método geral usado para codificar a mensagem pode (ou não) ser do conhecimento do intruso. No entanto, mesmo de posse da cifra em uso, se o mesmo não conhece a chave ou não tem nenhuma condição de obtê-la por qualquer de seus métodos, a mensagem continua em segurança.

De um modo geral, se um inimigo intercepta uma mensagem em código, ele pode suspeitar qual seja o algoritmo, mas espera-se que ele não conheça a chave exata. Por exemplo, ele pode suspeitar de que cada letra no texto original foi substituída por uma letra diferente, de um alfabeto cifrado, mas é improvável que o inimigo saiba qual alfabeto cifrado foi usado. (SINGH, 2004, p. 27)

Mais importante do que se ter um número imenso de chaves, é saber guarda-las bem, isto é, deve-se manter sempre em segredo a chave, sendo de posse restrita do emissor e receptor. A justificativa para isso é óbvia, uma vez que se a chave exata cair nas mãos do inimigo, ele poderá decodificar todas as mensagens que foram codificadas usando aquela chave. Daí a relevância do sigilo da chave, que supera o sigilo do algoritmo utilizado. Ou seja, o conhecimento do algoritmo de criptografia utilizado não é mais importante do que manter em segredo a chave. Segundo Singh (2004, p. 28),

A importância da chave, em oposição ao algoritmo, é um princípio constante da criptografia, como foi definido de modo definitivo em 1883 pelo linguista holandês Auguste Kerckhoff von Nieuwenhof, em seu livro *La Cryptographie Militaire*. Este é o princípio de Kerckhoff: ‘a segurança de um criptossistema não deve depender da manutenção de um criptoalgoritmo em segredo. A segurança depende apenas de se manter em segredo a chave’. (SINGH, 2004, p. 28)

Criptossistemas estão intimamente relacionados ao conceito de *função*, generalizam e conceituam precisamente a ideia de métodos criptográficos. Já criptoalgoritmo é um novo nome usado para se referir a algoritmos de criptografia. É preciso ressaltar que essa preocupação em manter em sigilo a chave de codificação só se faz presente na criptografia de chave privada (que abordaremos a seguir). No entanto, existe outro tipo de criptografia, que atua com duas chaves, onde a chave de codificação pode ser conhecida por qualquer um, mas a chave de decodificação é mantida em segredo.

Vejamos agora as definições de alfabetos e palavras em criptografia. Como já sabemos, para que possamos escrever uma mensagem ou um texto comum precisamos utilizar um alfabeto. No nosso caso, o alfabeto usual utilizado é $\{A, B, C, \dots, Z\}$. No entanto, esse não é o único alfabeto possível e as palavras e os textos assumirão características que dependem, logicamente, do alfabeto utilizado. Por exemplo, já vimos dois exemplos clássicos de alfabetos: o alfabeto Morse e o alfabeto Braille. A definição a seguir baseia-se na dada por Buchmann (2002).

Definição 1: Chama-se *Alfabeto* todo conjunto $\mathcal{A}$ finito e não vazio. Se $\mathcal{A}$ tem n elementos, dizemos que o *Comprimento* de $\mathcal{A}$ é igual a n . Os elementos de $\mathcal{A}$ são chamados de *Letras* ou *Símbolos*.

Exemplo 1: Vejamos alguns tipos de alfabetos.

- a) $\mathcal{A} = \{A, B, C, D, \dots, Z\}$ = Alfabeto usual. Comprimento de $\mathcal{A}$ é igual a 26;
- b) $\mathcal{A} = \{0, 1\}$ = Alfabeto binário. Comprimento de $\mathcal{A}$ é igual a 2;

Se considerarmos, a associação apresentada na Tabela 1, podemos interpretar o alfabeto $\{A, B, C, D, \dots, Z\}$ como sendo o conjunto $\{1, 2, 3, \dots, 26\}$. Isto é muito usado em criptografia, pois permite “calcular com letras”. Em geral, podemos fazer essa associação com qualquer alfabeto $\mathcal{A}$. Ou seja, se $\mathcal{A}$ tem comprimento m , então podemos associar aos símbolos de $\mathcal{A}$ os números $1, 2, 3, \dots, m$, ou de maneira análoga aos números $0, 1, 2, \dots, m - 1$ (BUCHMANN, 2002).

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Tabela1: Tabela de Pré-codificação. Fonte: Autoria própria.

As definições a seguir, baseadas em Buchmann (2002), nos fornecem a noção formal de *Palavra* em criptografia e alguns conceitos relacionados.

Definição 2: Seja $\mathcal{A}$ um alfabeto qualquer. Chamamos de *palavra* (em $\mathcal{A}$) qualquer sequência finita formada por símbolos de $\mathcal{A}$. O espaço entre palavras também está incluso e passará a ser chamado de sequência vazia.

Exemplo 2: Se $\mathcal{A} = \{0, 1\}$, então $m = 1001101011$ é uma palavra em $\mathcal{A}$.

Definição 3: Cada símbolo que compõe uma palavra num alfabeto $\mathcal{A}$ será chamado de componente da palavra. Se uma palavra tem n componentes, diremos que o comprimento dessa palavra é n .

Exemplo 3: Seja $\mathcal{A} = \{A, B, C, D, \dots, Z\}$. A palavra UFERSA tem comprimento 6 em $\mathcal{A}$. Analogamente, a palavra $m = 1001101011$ do alfabeto $\mathcal{A} = \{0, 1\}$ tem comprimento igual a 10.

Definição 4: Seja $\mathcal{A}$ um alfabeto qualquer. O conjunto de todas as palavras que podem ser formadas com os símbolos de $\mathcal{A}$, incluindo a sequência vazia, será denotado por $\mathcal{A}^*$. Da mesma forma, o conjunto de todas as palavras de comprimento fixo n em $\mathcal{A}$ será denotado por $\mathcal{A}^{(n)}$.

Outro conceito importante para o entendimento do nosso estudo são as cifras em blocos. Como o nome sugere, são aquelas que codificam em blocos, isto é, codificam palavras de comprimento fixo n ($n \in \mathbb{N}$). Nas cifras de blocos podemos codificar qualquer sequência finita de letras de mesmo comprimento e do mesmo alfabeto considerado. Passemos à definição formal.

Definição 5: Um método criptográfico (criptossistema) é chamado de *cifra de blocos* (ou *cifras em blocos*) se seu espaço de texto comum e o seu espaço de texto cifrado correspondem ao conjunto

$\mathcal{A}^{(n)}$ das palavras formadas por n símbolos do alfabeto $\mathcal{A}$ (BUCHMANN, 2002). Se uma cifra em blocos codifica palavras de comprimento n , dizemos que essa cifra tem comprimento de bloco igual a n .

Exemplo 4: A cifra de César é uma cifra em blocos. Seu comprimento de bloco é igual a 1 porque ela codifica palavras de comprimento 1 em palavras de comprimento também igual a 1. Outro exemplo, mais geral, de cifras em blocos são as cifras de substituição.

As codificações feitas por métodos de substituição simples podem ser facilmente desfeitas, isto é, a mensagem pode ser decodificada (ou decifrada) se soubermos como ocorreu a substituição, ou seja, qual o alfabeto cifrado. Assim, o conhecimento da chave usada para codificação (o processo específico de codificação) acarreta o conhecimento do processo de decodificação. Afinal, é só reverter o processo. Dizemos nesse caso que a cifra de substituição simples é um método de criptografia de chave privada porque usa apenas uma chave e esta chave, obviamente, deve ser mantida em segredo, sendo de posse restrita do emissor e destinatário legítimos. A área da criptografia que abrange os métodos (algoritmos) criptográficos de chave privada chama-se Criptografia de Chave Privada (ou simétrica).

Existem muitos exemplos de métodos criptográficos de chave privada, alguns mais modernos e sofisticados que desempenham papel importante na segurança computacional. Entre eles podemos destacar: O Data Encryption Standard (DES), criado pela International Business Machines (IBM) no ano de 1977, considerado um dos melhores algoritmos do mundo, tomado como padrão de criptografia nos Estados Unidos, até perder esse posto para seu sucessor Advanced Encryption Standard (AES). “Em outubro de 2000, o secretário de comércio dos Estados Unidos anunciou o novo Padrão Avançado de Codificação Criptográfica (Advanced Encryption Standard) proposto à nação” (BUCHMANN, 2002). O International Data Encryption Algorithm (IDEA) é outro algoritmo de chave privada criado no ano de 1991 por James Massey e Xuejia Lai (FRANÇA, 2014).

Não é difícil perceber qual é a fragilidade dos métodos de criptografia de chave privada. Como a mesma só trabalha com uma chave, para se desenvolver uma troca de mensagens o emissor e o destinatário deveriam intercambiar a chave usada antes de realizar a troca de mensagens. Esse intercâmbio, claro, poderia ser feito pessoalmente, caso os envolvidos se encontrassem para trocar as chaves. Ou então eles poderiam enviar a chave por mensagem através de um veículo de comunicação qualquer. Acontece que em ambos os casos a chave não estaria segura e poderia facilmente cair em mãos inimigas. Esta situação se agrava quando a troca de mensagens acontece entre muitos envolvidos. A segurança e o gerenciamento dessas chaves torna-se um caos.

Imagine esse tipo de criptografia como segurança hoje na internet. Se desejássemos efetuar uma compra em uma loja virtual qualquer, teríamos que esperar a loja mandar uma mensagem informando como deveríamos codificar os nossos dados pessoais para efetuar o pagamento da nossa compra, isto é, a loja mandava a chave de codificação para que pudéssemos codificar, por exemplo, os dados do cartão de crédito, para pagar a compra. Porém, como a comunicação entre loja e comprador estava sendo realizada por meio da internet, a segurança da chave enviada pela loja poderia ser violada por terceiros e, conseqüentemente, os nossos dados pessoais não estariam seguros (SAUTOY, 2007).

Felizmente um novo tipo de criptografia foi proposto em 1976 para acabar com o problema no gerenciamento da chave privada. Esse novo tipo de criptografia trouxe como novidade o fato de funcionar com duas chaves distintas, uma para codificação e outra para decodificação, e o conhecimento da chave de codificação não possibilita decodificar a mensagem. Ou seja, a chave de codificação pode ser pública e só quem poderá decodificar a mensagem é o real destinatário. A chave de codificação é então chamada de chave pública e a chave de decodificação é a chave privada e deve ser mantida em segredo. Sobre o funcionamento deste novo tipo de criptografia, Sautoy (2007, p. 243) acrescenta:

O sistema de criptografia de chave pública é como uma porta com duas chaves diferentes: a chave A tranca a porta, mas uma chave diferente, B, a destranca. Então, não é mais necessário manter qualquer confidencialidade em relação à chave A. Distribuir cópias dela não compromete a segurança. (SAUTOY, 2007, p. 243)

A criptografia de chave pública propõe o desenvolvimento de um método criptográfico que atue com duas chaves distintas. Neste caso, costuma-se dizer que os métodos de criptografia de chave pública atuam baseados numa função (bijetiva) de mão única (FRANÇA, 2014). Isso quer dizer que esses métodos são baseados em processos que, em essência, são fáceis de serem realizados, mas impossíveis de serem revertidos sem o uso da chave privada. Pense, por exemplo, na porta com duas chaves distintas. É fácil fechar a porta com a chave A, mas impossível abri-la com a mesma chave. O primeiro método de criptografia de chave pública desenvolvido foi o RSA. Ele se baseia num problema dessa natureza, que é o problema da fatoração de números inteiros. Para o leitor interessado em saber mais sobre a história e desenvolvimento da criptografia de chave pública e o método RSA sugerimos uma consulta às obras Sautoy (2007) e Singh (2004).

3. FUNÇÕES QUADRÁTICAS E CRIPTOGRAFIA

Se tratando da Teoria das Funções Quadráticas, deixaremos de abordar grande parte dos conceitos habitualmente vistos no ensino básico. A razão para isso é que tais conceitos não são

necessários para o desenvolvimento e entendimento do conteúdo exposto. Trataremos de mencionar aquilo que realmente importa e que assume um papel central na aplicação de criptografia. Temas como gráfico: forma canônica, teorema de caracterização, valores máximos e mínimos, *etc.*, não serão desenvolvidos como de costume. Uma rápida revisão sobre funções foi feita no Capítulo FUNÇÕES AFINS E CRIPTOGRAFIA. Para o leitor interessado em revisar ou aprofundar mais o seu conhecimento sobre funções, indicamos as obras Bianchini (2018), Balestri (2016), Iezzi et al. (2002), Dante (2006), Giovanni Júnior et al. (2018), Guidorizzi (2018), Flemming e Gonçalves (2012), Lima et al. (2006), Lima (2013), entre outros.

Partindo do ponto em que já possuímos algum conhecimento sobre noções básicas de funções, como a sua definição e algumas propriedades, vejamos a definição de uma função polinomial de segundo grau (ou função quadrática).

Definição 5: Função quadrática (ou função polinomial do 2º grau) é uma função $f: \mathbb{R} \rightarrow \mathbb{R}$, tal que, existem números reais a, b e c , sendo $a \neq 0$, de tal sorte que $f(x) = ax^2 + bx + c$.

Observações: Quando $b = c = 0$, temos a função quadrática $f(x) = ax^2$ que é o caso mais simples de tais funções. As quais também podem ser apresentadas por $f(x) = ax^2 + bx$, (no caso em que $c = 0$) e $f(x) = ax^2 + c$, (quando $b = 0$).

Exemplo 5: as funções dadas por $f(x) = 3x^2 + 2x - 1$, $g(x) = 5x^2$ e $h(x) = 2x^2 + 5$ são exemplos de funções quadráticas.

O gráfico de uma função quadrática é representado geometricamente por uma parábola, podendo ter concavidade voltada para cima ou para baixo a depender do sinal do coeficiente a . Nas disciplinas de Cálculo, tomamos ciência de que o que realmente está por trás do sentido da concavidade, neste caso, é o sinal da derivada segunda da função (que para a função quadrática coincide com o sinal do coeficiente a).

3.1. MÉTODO DE CODIFICAÇÃO BASEADO NA FUNÇÃO QUADRÁTICA

Nosso propósito nesta seção é descrever um método bem elementar de criptografia com base na Função Quadrática⁶. Para isto, utilizaremos a Tabela 1 (tabela de pré-codificação) apresentada na Seção 2.2. O método criptográfico que apresentamos, possui espaço de texto comum $\{1, 2, 3, 4, \dots, 26\}$, é uma cifra de blocos com comprimento 1 e seu espaço de texto cifrado é um subconjunto finito de N .

A seguir, apresentamos um guia de desenvolvimento e aplicação do método, através de um exemplo numérico. Neste caso, iremos codificar a mensagem A VIDA É UM SOPRO. O Roteiro 1 apresenta o processo de codificação, enquanto que o Roteiro 2 apresenta o processo de decodificação.

Roteiro 1 – Processo de codificação do método

Etapa 1: Suponhamos que queremos codificar a mensagem A VIDA É UM SOPRO. Usando a Tabela 1, substituímos cada letra pelo número que lhe é correspondente, separando-os por um traço (-). Logo, a mensagem passará a ser:

1-22-9-4-1-5-21-13-19-15-16-18-15.

Etapa 2: Agora, precisamos codificar cada número (bloco) que forma a mensagem. Entra em cena a questão da escolha da função de codificação criptográfica. No caso presente, esta função será a função quadrática, dada por $f(x) = ax^2 + bx + c$ ($a \neq 0$), com domínio restrito ao conjunto $\{1, 2, \dots, 26\}$. Então, começamos escolhendo os coeficientes a, b e c . Em termos de chave de codificação, isto significa escolher uma tripla ordenada (a, b, c) de números reais (que no nosso caso serão escolhidos de modo que os valores da função sejam naturais, para simplificar e evitar exageros nos cálculos). Escolhemos então a chave $(2, 1, 1)$, ou seja, vamos utilizar a função $f(x) = 2x^2 + x + 1$ como função de codificação criptográfica. Vale salientar que o código depende da função quadrática escolhida.

Etapa 3: Escolhida a função de codificação criptográfica $f(x) = 2x^2 + x + 1$, basta calcular a imagem de cada número da sequência que forma a mensagem original, que pela Etapa 1 é

1-22-9-4-1-5-21-13-19-15-16-18-15.

A Tabela 2 a seguir resume os cálculos realizados.

Bloco (x)	Função de codificação ($f(x) = 2x^2 + x + 1$)	Bloco codificado ($y = f(x)$)
1	$f(1) = 2 \cdot 1^2 + 1 + 1 = 4$	4
22	$f(22) = 2 \cdot 22^2 + 22 + 1 = 991$	991
9	$f(9) = 2 \cdot 9^2 + 9 + 1 = 172$	172
4	$f(4) = 2 \cdot 4^2 + 4 + 1 = 37$	37

5	$f(5) = 2 \cdot 5^2 + 5 + 1 = 56$	56
21	$f(21) = 2 \cdot 21^2 + 21 + 1 = 904$	904
13	$f(13) = 2 \cdot 13^2 + 13 + 1 = 352$	352
19	$f(19) = 2 \cdot 19^2 + 19 + 1 = 742$	742
16	$f(16) = 2 \cdot 16^2 + 16 + 1 = 529$	529
18	$f(18) = 2 \cdot 18^2 + 18 + 1 = 667$	667
15	$f(15) = 2 \cdot 15^2 + 15 + 1 = 466$	466

Tabela 2: Codificando a Mensagem. Fonte: Autoria própria.

A mensagem codificada passará a ser a sequência de blocos dada por:

Roteiro 2 – Processo de decodificação do método

Para recuperarmos a mensagem original necessitamos da função de decodificação criptográfica. Ora, já sabemos que essa função é a inversa da função de codificação. Então, temos que calcular a inversa da função $f(x)=2x^2+x+1$. Aqui esbarramos num ponto importante. No entanto, a fim de que uma função tenha inversa é necessário, e suficiente que ela seja bijetiva. É de nosso conhecimento que a função quadrática não é bijetiva em toda a reta, isto é, em $\mathbb{R}$, por não ser injetiva⁷. Porém, é fácil vencer esta dificuldade. Basta considerar a função definida em um dos intervalos $(-\infty, x_v]$ ou $[x_v, +\infty)$, pois neste caso a função será bijetiva. Onde x_v indica a abscissa do vértice da parábola, gráfico da função quadrática em questão. A imagem (que será igual ao contradomínio) da função será $[y_v, +\infty)$ quando $a>0$ ⁸, e $(-\infty, y_v]$ quando $a<0$. Onde y_v indica a ordenada do vértice da parábola, gráfico da função quadrática. Voltando ao caso da função de codificação, o gráfico da mesma

é uma parábola com vértice $\left(-\frac{1}{4}; \frac{7}{8}\right)$. Como só atribuímos valores naturais para x , segue que o domínio de f está contido em $\left[-\frac{1}{4}, +\infty\right)$, logo existe a inversa de f . Portanto, existe a função de decodificação criptográfica. Note que o domínio da inversa de f será um subconjunto de $\left[\frac{7}{8}, +\infty\right)$. Calculemos então a função inversa de f . Essa será nossa Etapa 1 do processo de decodificação.

Etapa 1: Temos que $f(x) = y = 2x^2 + x + 1$ é a função de codificação criptográfica. Queremos calcular x em função de y . Para isso, a igualdade

$$y = 2x^2 + x + 1$$

torna-se a equação do segundo grau $2x^2 + x + 1 - y = 0$ na incógnita x (caso seja necessário, é importante revisar as equações do 2º grau e o método de resolução utilizado a seguir). Calculando as raízes dessa equação em função de y , teremos:

$$x = \frac{-1 \pm \sqrt{1^2 - 4 \cdot 2 \cdot (1 - y)}}{4} = \frac{-1 \pm \sqrt{1 - 8(1 - y)}}{4}$$

$$\Rightarrow x = \frac{-1 + \sqrt{1 - 8(1 - y)}}{4} \text{ ou } x = \frac{-1 - \sqrt{1 - 8(1 - y)}}{4}.$$

Como o domínio de f é $\left[-\frac{1}{4}, +\infty\right)$, segue que $x = \frac{-1 + \sqrt{1 - 8(1 - y)}}{4}$.

Portanto, temos que

$$x = f^{-1}(y) = \frac{-1 + \sqrt{1 - 8(1 - y)}}{4}.$$

A função inversa de f , com domínio $\left[\frac{7}{8}, +\infty\right)$, é:

$$f^{-1}(x) = \frac{-1 + \sqrt{1 - 8(1 - x)}}{4}.$$

Etapa 2: Nessa etapa realizamos o processo de decodificação dos blocos que constituem a mensagem original codificada. Sendo $f^{-1}(x) = \frac{-1 + \sqrt{1 - 8(1 - x)}}{4}$ a função de decodificação, basta aplicá-la aos blocos que forma a mensagem codificada para obter a mensagem original. Não faremos as contas aqui, mas o leitor pode se certificar de que realmente recuperamos todos os blocos codificados calculando a imagem de todos os números na mensagem codificada por meio de f^{-1} . Por exemplo, o primeiro bloco da mensagem codificada é 4. Logo, para decodificar esse bloco, basta substituí-lo na função f^{-1} , obtendo

$$f^{-1}(4) = \frac{-1 + \sqrt{1 - 8(1 - 4)}}{4} = \frac{-1 + \sqrt{1 - 8(-3)}}{4} = \frac{-1 + \sqrt{1 + 24}}{4} = \frac{-1 + 5}{4} = 1.$$

Ou seja, o bloco original correspondente ao bloco 4 é o 1. Repetindo esses cálculos para todos os blocos, recuperamos a mensagem. A tabela a seguir resume o processo de decodificação:

y	4	991	172	37	56	904	352	742	529	667	466
$f^{-1}(y)$	1	22	9	4	5	21	13	19	16	18	15

Tabela 3: Decodificando a Mensagem. Fonte: Autoria própria.

A mensagem decodificada passa a ser a sequência 1-22-9-4-1-5-21-13-19-15-16-18-15 que corresponde à mensagem original A VIDA É UM SOPRO pela Tabela 1, e o processo está encerrado.

Para exercitar o método que aprendemos façamos o exemplo a seguir, o qual pode ser utilizado em sala de aula para exercitar as noções de quadrados perfeitos e raízes quadradas.

Exemplo 6: Neste exemplo, nossa função de codificação criptográfica é $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ dada por $f(x) = x^2$. Note que esta função é quadrática, com mesma lei de formação, porém com domínio e contradomínio restritos ao conjunto dos números reais não negativos. Assim, existe a função de decodificação, pois a função é bijetiva. Neste exemplo, podemos trabalhar não só a ideia de Função Quadrática (no ensino médio), mas também os conceitos de quadrados de números naturais, radiciação e operações inversas (no ensino fundamental). Desse modo, pretendemos criptografar a mensagem A MATEMÁTICA É A RAINHA DAS CIÊNCIAS usando como método elementar as Funções Quadráticas. Em particular, utilizaremos a função $f: \mathbb{R}^+ \rightarrow \mathbb{R}^+$ dada por $f(x) = x^2$. Usando a Tabela 1, a mensagem original será convertida em:

1-13-1-20-5-13-1-20-9-3-1-5-1-18-1-9-14-8-1-4-1-19-3-9-5-14-3-9-1-19.

Agora, para codificar a mensagem precisamos calcular o quadrado dos números que a forma, isto é, calcular a imagem de cada bloco da mensagem pela função $f(x) = x^2$. A tabela a seguir resume esses simples cálculos:

x	1	13	20	5	9	3	18	14	8	4	19
x^2	1	169	400	25	81	9	324	196	64	16	371

Tabela 4: Codificação da Mensagem do Exemplo 6. Fonte: Autoria própria.

A mensagem criptografada será:

1-169-1-400-25-169-1-400-81-9-1-25-1-324-1-81-196-64-1-16-1-371-9-81-25-196-9-81-1-371.

Para recuperarmos a mensagem, necessitamos da função inversa de f . Como sabemos, a operação inversa da potenciação é a radiciação. Logo, a função inversa de $f(x) = x^2$ é $f(x) = \sqrt{x}$ (veja que como $\sqrt{x}$ não está definido para $x < 0$, necessitamos restringir o contradomínio de f à $\mathbb{R}^+$). Precisamos calcular a raiz quadrada de todos os números que formam a mensagem codificada (esta é uma ótima oportunidade para treinar o cálculo de raízes quadradas). Teremos então a seguinte tabela:

y	1	169	400	25	81	9	324	196	64	16	371
$\sqrt{y}$	1	13	20	5	9	3	18	14	8	4	19

Tabela 5: – Decodificação da Mensagem do Exemplo 6. Fonte: Autoria própria.

Substituindo os blocos na mensagem codificada por seus correspondentes, decodificados, obtemos:

1-13-1-20-5-13-1-20-9-3-1-5-1-18-1-9-14-8-1-4-1-19-3-9-5-14-3-9-1-19.

Que representa a mensagem A MATEMÁTICA É A RAINHA DAS CIÊNCIAS. O processo está encerrado!

Na prática em sala de aula, o professor pode explorar mais exemplos como esses com o intuito de revisar e exercitar tópicos já estudados. Note que, estávamos tratando de funções, mas o exemplo nos levou a revisar outras noções igualmente importantes. Assim, com base no que fizemos no exemplo anterior, podemos trabalhar com potências de expoentes mais altos, assim como trabalhar com raízes cúbicas, quartas, quintas, etc., sem contar, claro, que podemos ampliar esses exercícios de criptografia para o caso de outras funções, como as polinomiais de grau n , funções racionais, exponenciais, logarítmicas, etc. Observe, através dos exemplos analisados, que não é necessário falar em função para trabalharmos com exemplos semelhantes em sala de aula no ensino fundamental. O professor pode, e deve quando necessário, adaptar as atividades ao nível e bagagem de conhecimento da turma. Assim, sem mencionar funções, o professor pode, por exemplo, trabalhar fórmulas ou expressões algébricas e desenvolver atividades/exercícios, semelhantes àqueles desenvolvidos com funções, envolvendo criptografia. Desse modo, temos a oportunidade de inserir o assunto criptografia nas séries iniciais do ensino fundamental. É só uma questão de adaptação.

4. CONSIDERAÇÕES FINAIS

Esse capítulo apresentou um método bem intuitivo de criptografia baseado na função quadrática. Para contextualizar o leitor com o tema criptografia, fizemos um breve histórico e apresentamos algumas definições básicas.

Como podemos observar, no contexto do uso da função quadrática na criptografia, o aluno estuda tópicos como radiciação, potenciação, domínio e imagem de função, bijetividade, função inversa, entre outros, de maneira dinâmica e instigadora, contrapondo as aulas tradicionais. Esperamos que tal estudo motive o professor, e sirva de suporte, na busca da contextualização e interdisciplinaridade, refletindo em melhorias para o ensino de matemática, uma vez que foram acrescidos significado e sentido ao objeto de estudo. Ademais, pretende-se ampliar a visão do professor para utilizar tais exercícios de criptografia para o caso de outras funções e aplicações.

REFERÊNCIAS

- BALESTRI, R. Matemática 1: Interação e Tecnologia. 2ª ed. São Paulo: LEYA, 2016.
- BESSELAAR, J. V. D. Heródoto, o pai da história. V. 24, n. 49, 1962. (4 - 26).
- BIANCHINI, E. Matemática Bianchini, 9º ano. 9ª ed. São Paulo: MODERNA, 2018.
- BRANDÃO, M. M. D. Uma Adaptação da Cifra de Hill para Estudo de Matrizes. 91f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT), Universidade Federal de Ouro Preto, Ouro Preto/MG, 2017.
- BROUSSEAU, G. Fondement et Méthodes de la Didactique des Mathématiques. In J. Brun (Ed), Didactique des Mathématiques, p. 45 – 144. Lausanne: Delachaux et Niestlé, 1996. Citado por PINHEIRO, Felipa Margarida Dias Lima. Contextualização do Saber: Formação Inicial dos Professores de 1º e 2º Ciclo do Ensino Básico. 159f. Dissertação (Mestrado em Ciências da Educação), Universidade de Lisboa, Instituto de Educação, Lisboa, 2012.
- BRASIL. Base Nacional Comum Curricular: Ensino Médio. Brasília: MEC/Secretaria de Educação Básica, 2017.
- BUCHMANN, J. A. Introdução à Criptografia. São Paulo: BERKELEY, 2002.
- COSTA, Renata. Como funciona o código Braille? Nova Escola, 2009. Disponível em: <<https://novaescola.org.br/conteudo/397/como-funciona-sistema-braille>>. Acesso em: 19 out. 2019.
- COUTINHO, S. C. Números Inteiros e Criptografia RSA. 2ª ed. Rio de Janeiro: IMPA, 2005.
- COUTINHO, S. C. Criptografia. Programa de Iniciação Científica da OBMEP. 1ª ed. Rio de Janeiro: IMPA/OBMEP, 2009.
- DANTE, L. R. Matemática, 1ª série. 1ª ed. São Paulo: Ática, 2006.
- DANTE, Luiz Roberto. Matemática, volume único. 1ª ed. São Paulo: Ática, 2011.
- FIARRESGA, V. M. C. Criptografia e Matemática, 2010. 161f. Dissertação (Mestrado em Matemática para Professores) – Faculdade de Ciências – Universidade de Lisboa, Lisboa, 2010.
- FLEMMING, D. M.; GONÇALVES, M. B. Cálculo A: funções, limite, derivação e integração. 6ª ed. São Paulo: PEARSON PRENTICE HALL, 2009.
- FRANÇA, W. B. A. A utilização da Criptografia para uma Aprendizagem Contextualizada e Significativa. 63f. Dissertação (Mestrado Profissional em Matemática), Universidade de Brasília - UNB, Brasília, 2014.
- GIOVANNI JÚNIO, J. R.; CASTRUCCI, B. A Conquista da Matemática, 9º ano. 4ª ed. São Paulo: FTD, 2018.
- GUIDORIZZI, H. L. Um Curso de Cálculo, vol. 1. 5ª ed. Rio de Janeiro: LTC, 2018.
- IEZZI, G.; HAZZAN, S. Fundamentos de Matemática Elementar, vol.4. 7ª ed. São Paulo: ATUAL, 1993.

IEZZI, G.; DOLCE, O.; DEGENSZAJN, D.; PÉRIGO, R. Matemática, volume único. 1ª ed. São Paulo: ATUAL, 2002.

JESUS, A. L. N. de. Criptografia na Educação Básica: utilização da criptografia como elemento motivador para o ensino aprendizagem de matrizes. 82f. Dissertação (Mestrado Profissional em Rede Nacional em Matemática - PROFMAT), Universidade Federal do Vale do São Francisco, Juazeiro/BH, 2013.

LIMA, E. L.; CARVALHO, P. C. P.; WAGNER, E.; MORGADO, A. C. A Matemática do Ensino Médio, vol. 1. 9ª ed. Rio de Janeiro: SBM, 2006.

LIMA, E. L.; CARVALHO, P. C. P.; WAGNER, E.; MORGADO, A. C. A Matemática do Ensino Médio, vol. 2. 6ª ed. Rio de Janeiro: SBM, 2006.

LIMA, E. L. Curso de Análise, vol. 1. 14ª ed. Rio de Janeiro: IMPA, 2013.

LOUREIRO, F. O. Tópicos de Criptografia para o Ensino Médio. 43f. Dissertação (Mestrado em Matemática) Universidade Estadual do Norte Fluminense Darcy Ribeiro – UENF. Campos dos Goytacazes/RJ, 2014.

MEDEIROS, W. da S. Números Primos e Criptografia RSA: uma descrição da mais bela relação em teoria dos números. 70f. Monografia (Licenciatura Plena em Matemática), Universidade do Estado do Rio Grande do Norte – UERN. Patu/RN, 2017.

PEREIRA, N. M. I. Criptografia: uma nova proposta de ensino de matemática no ciclo básico. 76f. Dissertação (Mestrado Profissional em Matemática em Rede Nacional - PROFMAT), Universidade Estadual Paulista “Júlio de Mesquita Filho”, Ilha Solteira/SP, 2015.

SAUTOY, M. Du. A música dos números primos: a história de um problema não resolvido na matemática. Rio de Janeiro: ZAHAR, 2007.

SHOKRANIAN, S. Criptografia Para Iniciantes. Brasília: UNB, 2005.

SINGH, S. O livro dos códigos. 4ª ed. Rio de Janeiro: Record, 2004.

TERADA, R. Segurança de Dados: criptografia em redes de computador. São Paulo: EDGARD BLÜCHER LTDA, 2000.

NOTAS

Nota 1

Ver matéria publicada no site do IMPA (INSTITUTO DE MATEMÁTICA PURA E APLICADA) no dia 27 de fevereiro de 2018. Fonte: <<https://impa.br/noticias/tv-escola-destaca-entrada-do-brasil-na-elite-da-matematica/>>. Acesso em: 02 jul. 2020.

Nota 2

Ver matéria do G1 em <<https://g1.globo.com/educacao/noticia/2019/12/03/brasil-cai-em-ranking-mundial-de-educacao-em-matematica-e-ciencias-e-fica-estagnado-em-leitura.ghtml>> e o Relatório Brasil no Pisa 2018 no site do INEP em <<http://portal.inep.gov.br/web/guest/acoes-internacionais/pisa/resultados>>. Acesso em: 02 jul. 2020.

Nota 3

Grego, rei euripôntida de Esparta (Cidade – Estado da Grécia antiga) que viveu entre 515 a.C e 491 a.C. Fonte: <<https://pt.wikipedia.org/wiki/Demarato>>. Acesso em: 28 set. 2019

Nota 4

“É a ciência da escrita secreta em todas as suas formas, cobrindo ambas, a criptografia e a criptoanálise” (SINGH, 2004, p. 424).

Nota 5

Não seria correto afirmar que o código desenvolvido por Barbier era um método criptográfico, pois sua intenção não era modificar o conteúdo da mensagem de modo que só o receptor pudesse entender, e sim desenvolver algum procedimento para esconder a mensagem através de símbolos de modo que os soldados pudessem ler no escuro. Isto está mais próximo de um método de esteganografia. Da mesma forma, não seria aconselhável dizer que os códigos Braille e Morse são métodos criptográficos. Eles não desempenham tal função, mas são meios de transmitir uma mensagem por meio de símbolos. Em suma, vamos chamá-los apenas de códigos.

Nota 6

Rigorosamente falando, e isto se aplica também para o caso já tratado no capítulo sobre Função Afim, não usamos realmente uma Função Quadrática, de acordo com a definição dada. Isso porque o domínio utilizado por nós não é o conjunto dos números reais. O que fazemos é restringir o domínio da função ao conjunto $\{1, 2, 3, \dots, 26\}$ e usar como lei de formação desta função a expressão $f(x)=ax^2+bx+c$. Mas isto não representa nenhum incômodo para a descrição e aplicação do método estudado.

Nota 7

Como o gráfico da função quadrática é uma parábola, dois elementos do domínio, simétricos em relação a abscissa do vértice dessa parábola, terão mesma imagem. Logo, a função é injetiva em $\mathbb{R}$.

Nota 8

Os símbolos x_v e y_v representam, respectivamente, a abscissa e a ordenada do vértice da parábola, gráfico da função quadrática f .

Capítulo 7



10.37423/220305622

FUNÇÕES TRIGONOMÉTRICAS: UMA PROPOSTA DE ENSINO BASEADA NO CONTEXTO HISTÓRICO, NO USO DE RECURSOS TECNOLÓGICOS E NA RESOLUÇÃO DE SITUAÇÕES PROBLEMAS

John Nathan Pereira de Carvalho

*Universidade Federal Rural do Semi-Árido -
UFERSA*

Luiza Helena Felix de Andrade

*Universidade Federal Rural do Semi-Árido -
UFERSA*



1. INTRODUÇÃO

O cenário que nos encontramos hoje tem elevado mais ainda a preocupação com o Ensino de Matemática em nosso país, para muitos pesquisadores em Educação, os baixos índices e a baixa proficiência neste componente curricular tem sido o centro das atenções nos últimos anos. É possível entender essa preocupação quando olhamos para os resultados do Sistema de Avaliação da Educação Básica – SAEB, do Exame Nacional do Ensino Médio – ENEM, para a posição do Brasil no ranking do Programa Internacional de Avaliação dos Estudante – PISA e ainda agravado com o distanciamento social que causou o fechamento dos espaços físicos das Escolas e tendenciou a opção por aulas remotas, que de acordo com UNICEF (2021) o déficit de aprendizagem chega a 70%, principalmente em Matemática e leitura.

Todos esses indicadores mostram que o Ensino de Matemática no Brasil não vai bem e que a pandemia potencializou ainda mais. Diante deste cenário, surge a necessidade de os professores de Matemática buscarem estratégias didáticas pedagógicas para alcançar melhores desempenhos na aprendizagem do componente.

Contudo, resolvemos buscar e trazer para discussão a pesquisa de Carvalho (2020), que propôs uma metodologia mais estratégica para trabalhar o Ensino das funções trigonométricas no Ensino Médio. Esse trabalho foi inspirado em Sousa (2020) e contou com a junção entre três fortes tendências da Educação Matemática: História da Matemática, a Resolução de Problemas e o uso de Recursos Tecnológicos.

Segundo Siqueira (2007), o ensino dos conteúdos matemáticos não pode ser distanciado da sua respectiva história, quando abordado em sala de aula, pois os fatos ajudam o aluno a entender como e quais necessidades contribuíram para aquele resultado. Outras literaturas também foram fortes na construção dessa proposta, como Fossa (2001), que destaca a utilização da História da Matemática como auxílio pedagógico, dizendo que:

A História da Matemática é uma das formas de se contextualizar o ensino da Matemática escolarizada como possibilidades de situar o conhecimento no tempo e no espaço bem como motivar os alunos para um despertar para a aprendizagem da Matemática (FOSSA, 2001, p.16).

Sobre a justificativa da inserção de resolução de problemas nessa proposta, vimos que os alunos precisam enxergar muito além de fórmulas e de exercícios que abordam mesmas regras e métodos prescritos ou memorizados. Para Onuchic e Allevato (2011):

Resolução de problemas desenvolve poder matemático nos alunos, ou seja, capacidade de pensar matematicamente, utilizar diferentes e convenientes estratégias em diferentes problemas, permitindo aumentar a compreensão dos conteúdos e conceitos matemáticos (ONUCHIC; ALLEVATO, 2011, p. 82).

Portanto, após as abordagens anteriores, temos como objetivo apresentar a proposta de Carvalho (2020) e discutir sobre o material de apoio deixado para os professores, material este que foi dividido em quatro partes e conta com uma sequência de trabalho com os estudantes, apoiando-se nas tendências mencionadas.

2. ORIENTAÇÕES AO DOCENTE

Nesta seção, iremos discutir sobre uma proposta didática para o ensino das funções trigonométricas, de acordo com Carvalho (2020). Esse trabalho pode ser acessado no endereço eletrônico <http://repositorio.ufersa.edu.br/handle/prefix/5665>.

No Apêndice D do trabalho citado, há uma proposta de material de apoio para professores utilizarem em suas rotinas pedagógicas sobre as funções trigonométricas. Esse material foi dividido em 4 aulas e aqui iremos comentar um pouco sobre elas, tendo em vista a junção entre as tendências História da Matemática, Recursos Tecnológicos e Resolução de Problemas.

Na Aula 1, para início de abordagem, é feito uma reflexão sobre o estudo das funções trigonométricas usando o movimento de uma roda gigante, associando a variação da altura de uma das cabines com o tempo de movimento, abordando o conceito de periodicidade, da altura máxima e mínima. Em seguida, lança fatos históricos acerca do desenvolvimento da trigonometria, dos povos que deram suas contribuições para o avanço das ciências, como por exemplo na Astronomia, e relata o feito do matemático grego Eratóstenes de Cirene (276-194 a.C.), que calculou o comprimento da terra por volta de 200 a.C.

Na sequência, é dado os primeiros passos na exposição do conteúdo em si, apresentação dos conceitos iniciais, como o de arco de circunferência, classificação e representação. Nessa parte também é feito a apresentação dos conceitos de comprimento e medida de um arco, na qual é abordada uma noção intuitiva utilizando um pedaço de arame, corda ou barbante, ajustando-o sobre a curva e depois esticando e verificando seu valor linear.

É sugerido aos leitores interessados na demonstração do comprimento da circunferência o livro Barbosa (2012). Exemplifica o fato da proporcionalidade entre a medida do raio da circunferência e o

seu comprimento e define as unidades de medida utilizadas, o grau e o radiano. Ao final, resolve alguns exercícios e sugere outros, tendo como fonte Iezzi (2013) e Iezzi et al. (2016).

A Aula 2, com título de Circunferência trigonométrica, inicia com a história das tabelas de cordas construídas pelos gregos Hiparco de Nicéia (180 – 125 a.C.) e Claudio Ptolomeu (85 – 165 a.C.), que mais tarde viriam a, erroneamente, ser chamadas de seno, devido a traduções equivocadas feitas pelos hindus do termo *jya*, segundo Eves (2011). Na verdade, essa corda α era um segmento cujas extremidades eram as extremidades do arco de medida α , contido em uma circunferência de raio 60.

Na continuação, define a circunferência trigonométrica, ou ciclo trigonométrico, os quadrantes, as razões trigonométricas de um arco, bem como sua interpretação geométrica no intervalo de 0 a 2π , e mostra a relação com as medidas algébricas dos segmentos correspondentes. Também é exibido como fazer as reduções desses arcos ao primeiro quadrante usando a simetria. Para essa apresentação, utiliza-se o recurso tecnológico GeoGebra, como pode ser visto na Figura 1.

É conveniente lembrar que o uso correto desse recurso tecnológico, bem como de muitos outros, de acordo com Kenski (2009), no ambiente escolar, provoca modificações nas relações entre professores e alunos e, ainda, proporcionam um maior aprofundamento nos conteúdos estudados, trazendo melhorias para nossa educação. No entanto é sempre bom estimular tais práticas.

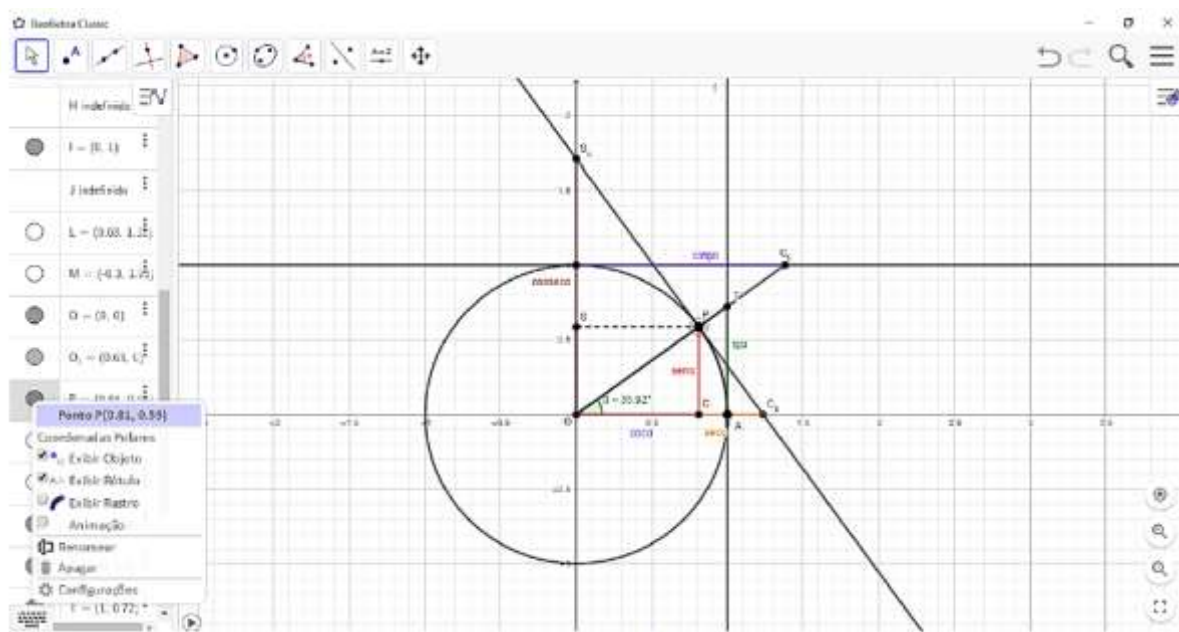


Figura 1: Uso do GeoGebra para definir as razões trigonométricas no 1º Q. Fonte: (CARVALHO, 2020).

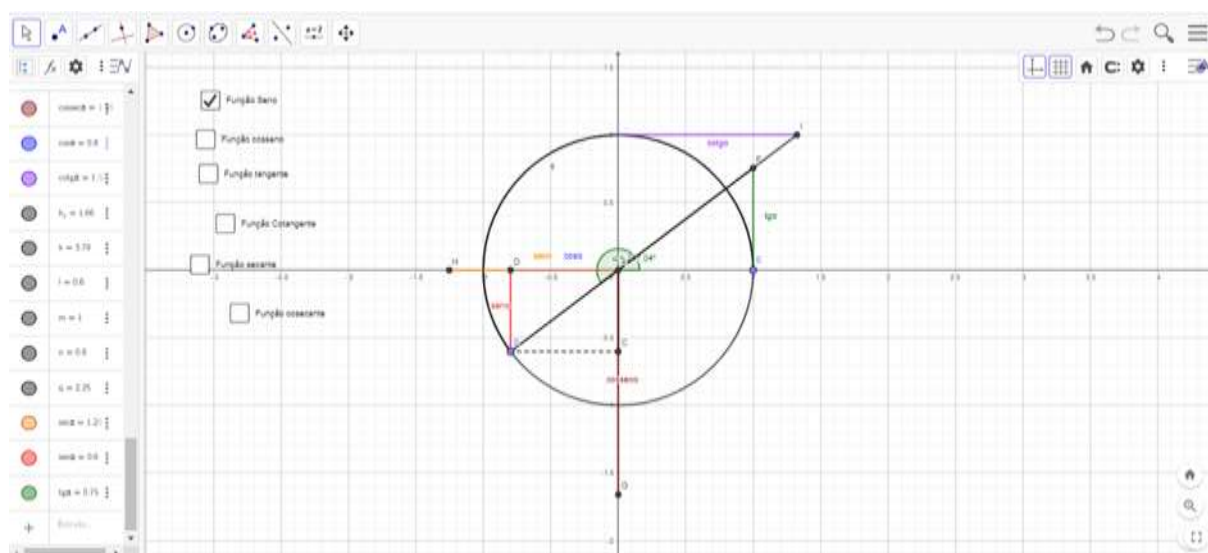


Figura 2: Uso do GeoGebra para definir as razões trigonométricas no 3º Q. Fonte: (CARVALHO, 2020).

No trabalho, é disponibilizado o endereço para a página do GeoGebra para manuseio e para utilização em uma aula prática nos laboratórios de informática das instituições educacionais. Esse material pode ser acessado no endereço eletrônico <https://www.geogebra.org/m/atudtnae>. Ao final dessa parte é resolvido alguns exercícios e propostos outros.

Já na Aula 3, conta-se algumas das contribuições de Leonhard Euler (1707 – 1783) para a trigonometria, principalmente a nova roupagem a partir da conhecida Função Euler, função esta definida no conjunto dos números reais e a sua imagem é o círculo trigonométrico, isto é, a cada número real t , a função E faz corresponder um ponto $E(t)$ do círculo trigonométrico. A partir dessa função E , é calculado o $\sin(x)$ e o $\cos(x)$ em função de uma variável x , $x \in \mathbb{R}$. Esse x é a abscissa dos pontos P do círculo unitário centrado na origem do sistema cartesiano. Através dela também foi possível clarear a interpretação da periodicidade dessas funções.

A partir desse, é possível expandir o estudo das funções para intervalos maiores que a primeira volta, assim como, para arcos negativos. Com esse objetivo, é sugerido um material que está hospedado na plataforma do GeoGebra que vai contribuir para essa visualização, como mostra a Figura 3. Esse material permite enxergar arcos maiores que uma volta, tanto medidos em graus como em radianos, e a simetria de arcos abertos no sentido horário. Para acesso, basta usar o endereço eletrônico <https://www.geogebra.org/m/vykepyjm>.

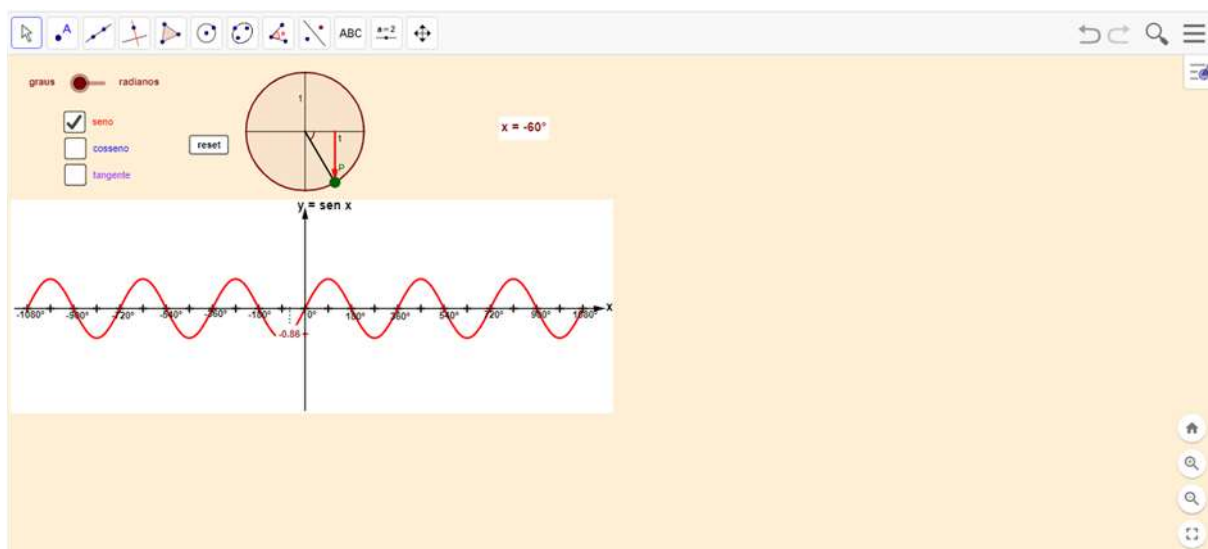


Figura 3: Apresentação de arcos trigonométricos. Fonte: (MARCO A MANETTA, 2019).

Adiante, é definida o que é uma função periódica e as funções seno, cosseno e tangente, também são enunciadas suas características, como por exemplo, domínio, imagem, paridade, intervalos no qual elas são positivas, negativas, crescentes e decrescentes. Aliado a essa exibição, mais uma vez, é utilizado o GeoGebra, permitindo uma visibilidade bem melhor que as imagens contidas nos livros didáticos.

Na Aula 4, é aprofundado o estudo das funções trigonométricas, lançando os casos da forma $f(x) = a + b \cdot \text{sen}(cx + d)$ e $g(x) = a + b \cdot \text{cos}(cx + d)$, com a, b, c e $d \in \mathbb{R}$, com b e $c \neq 0$, funções estas que permitem inúmeras aplicações. A critério do professor, a função $h(x) = a + b \cdot \text{tg}(cx + d)$ também pode ser apresentada, como será mostrado a seguir. Para iniciar, é lançado a aplicação das marés, que são variações periódicas do nível do mar devido principalmente à atração gravitacional da Lua. A função em destaque relaciona a altura da maré em função do tempo, em horas. Tendo em vista uma possibilidade de fixar a atenção dos alunos a alguns detalhes, são feitas as seguintes indagações aos alunos em relação a expressão algébrica:

- 1) Quais as alturas máximas e mínimas da maré?
- 2) Quanto tempo dura um ciclo, isto é, atingir o máximo, o mínimo e voltar a altura inicial?

As perguntas são respondidas ao longo da aula, associando os conceitos as suas respectivas formas de interrogativa, buscando interagir a turma com as participações verbais.

As funções $f(x)$ e $g(x)$ e $h(x)$ citadas anteriormente, tem suas características alteradas de acordo com a variação de seus coeficientes reais a , b , c e d , com $b \neq 0$ e $c \neq 0$. O objetivo da aula é mostrar, usando o

GeoGebra, o que ocorre com a imagem, o período e o gráfico da função e debater sobre algumas aplicações cotidianas desse tema, como a roda gigante, a pressão arterial, o jogo de golfe e resolver alguns itens do ENEM.

Para a exibição da influência da variação dos valores dos coeficientes sobre a representação gráfica e das características da função, mais uma vez, usaremos o GeoGebra. Dessa vez, a ferramenta será manipulada com quatro controles deslizantes, que é uma espécie de controle do valor numérico dos coeficientes, e com as entradas das funções $f(x)$ e $g(x)$ e $h(x)$. As figuras a seguir mostram como são essas apresentações.

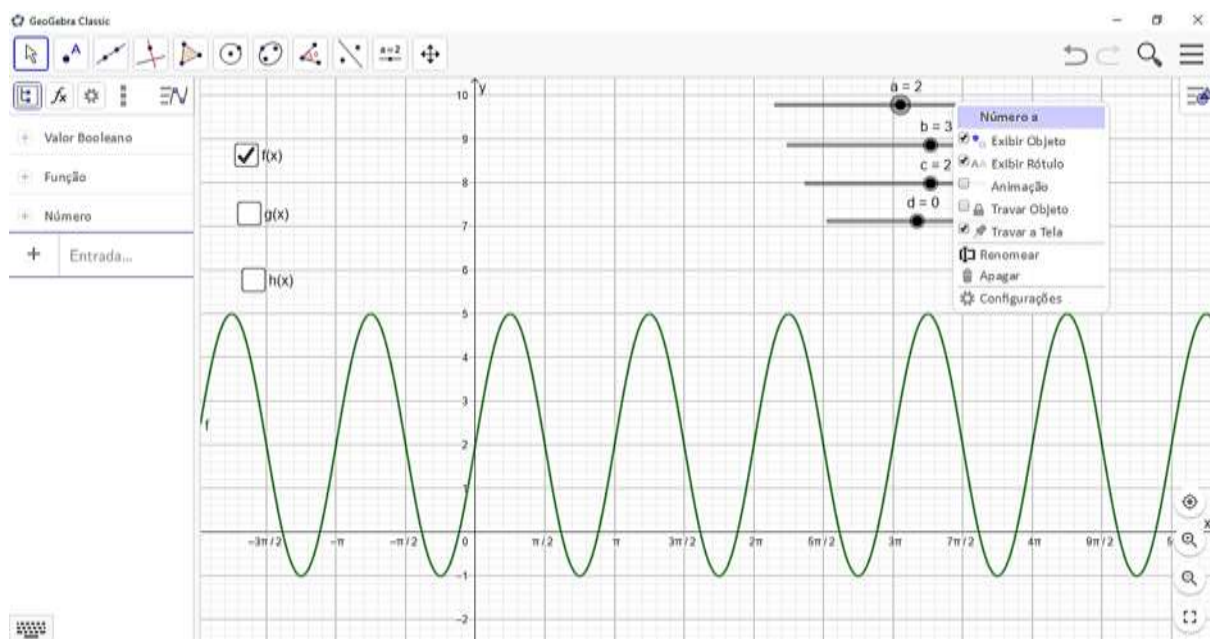


Figura 1: Representação da função $f(x)=2+3\text{sen}(2x)$. Fonte: (CARVALHO, 2020).

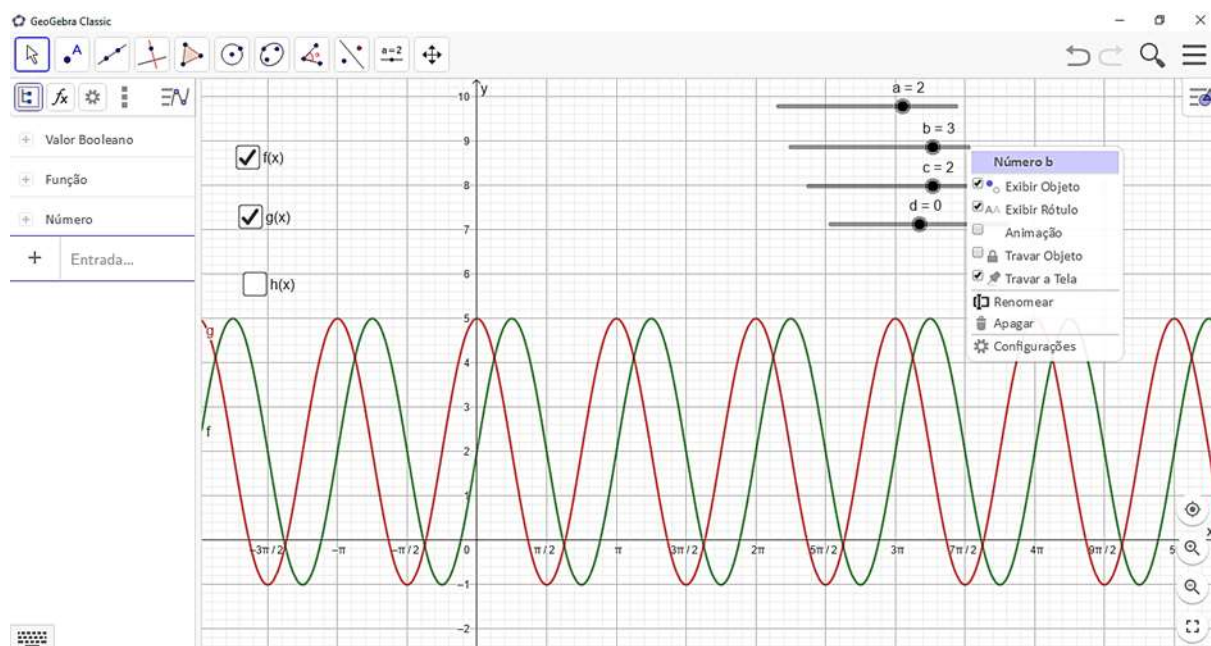


Figura 5: Representação das funções $f(x)=2+3\sin(2x)$ e $g(x)=2+3\cos(2x)$. Fonte: (CARVALHO, 2020).

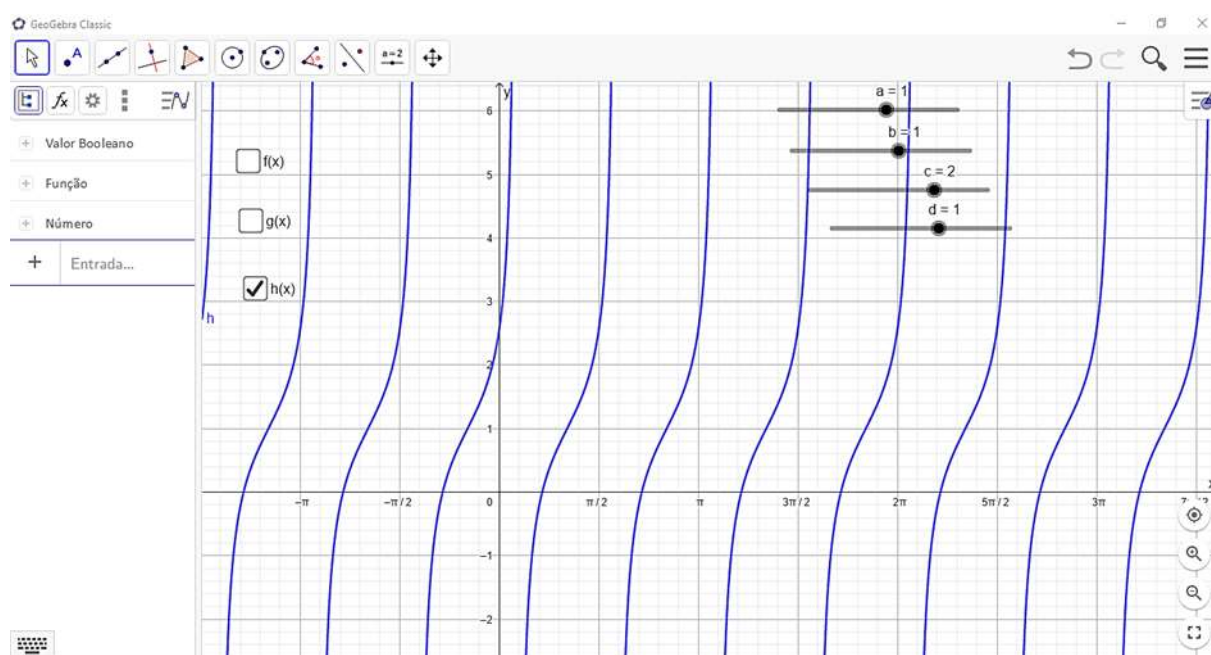


Figura 6: Representação da função $h(x)=1+\tan(2x)$. Fonte: (CARVALHO, 2020).

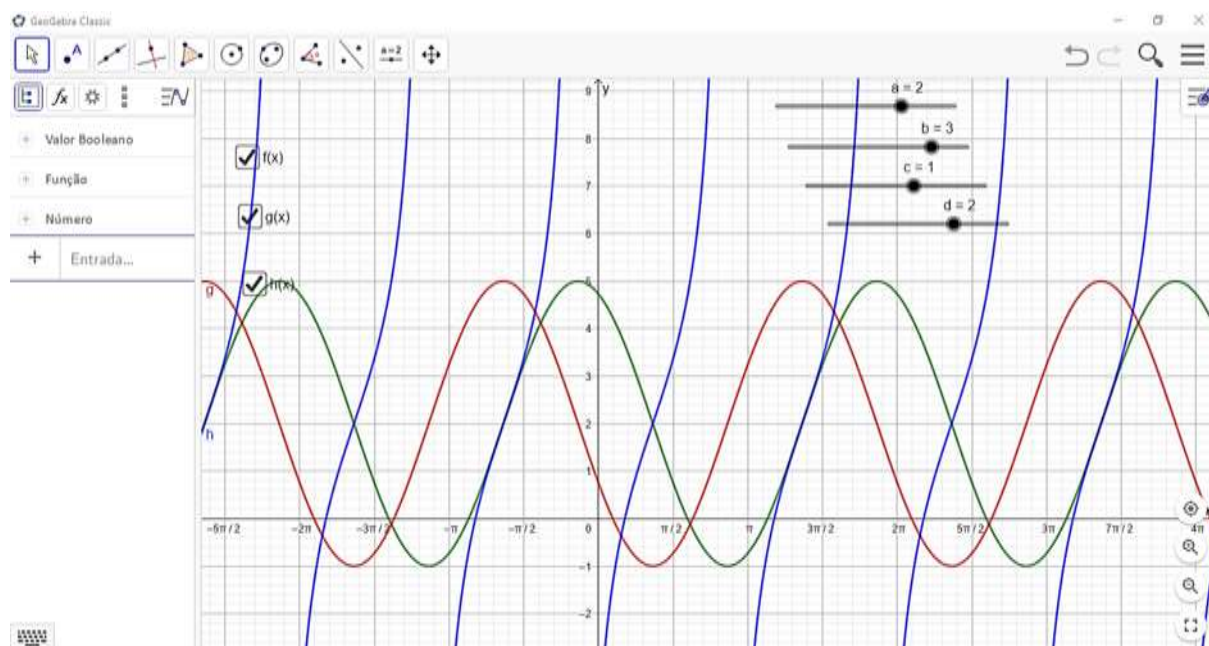


Figura 7: Apresentação das funções f , g e h . Fonte: (CARVALHO, 2020).

Na Figura 4, Figura 5, Figura 6 e Figura 7, mostramos como é o layout dessas ferramentas em questão. Ao manipular esses controles deslizantes, vamos ver a mudança no gráfico e poder proporcionar aos estudantes a construção das suas conclusões a cerca desses parâmetros. Aqui, não há o interesse de abordar o que cada coeficiente altera na função, caso o leitor tenha interesse, basta ler o Capítulo 4 de Carvalho (2020).

É importante que os professores nesse momento da aula motivem os alunos a participar, manipulando esse instrumento. Caso não haja um ambiente propício, sugerimos o uso de um computador com o GeoGebra instalado e um Datashow. Pensando nessa estratégia, objetivamos estreitar o caminho que leva os estudantes a uma aprendizagem significativa. No endereço <https://www.geogebra.org/m/vnbwjszx>, o leitor tem acesso ao material abordado no GeoGebra.

Ainda dentro desta Aula, tem o uso da metodologia PGD, interessados ver Machado e Pinheiro (2009), que consiste em uma estratégia criada para o Ensino de Ciências e Matemática nos cursos de Engenharia, utilizando a resolução de situações problema como aliado no processo da aprendizagem, considerando a construção de uma interpretação através de diálogos e troca de experiências. Essa interação leva o aluno a exercitar suas habilidades e competências para aplicar conhecimentos científicos, experimentais, relacionados à prática do curso (CARVALHO, 2020).

Portanto, essa metodologia foi adaptada e utilizada nas aulas de Matemática com o intuito de atender a uma necessidade que é muito comum entre os estudantes, saber para que estudar/aprender e em

que determinados conteúdos são utilizados. Ainda, foi proposto uma série de aplicações do conteúdo no nosso cotidiano afim de incentivar o desenvolvimento da competência de investigação e compreensão em Matemática na medida em que o estudante deve interpretar a situação proposta, utilizar e elaborar modelos e representações matemáticas para analisar situações, além de compreender o mundo do qual a Matemática é parte integrante, através dos problemas que ela consegue resolver e dos fenômenos que podem ser descritos por meio de seus modelos e representações.

Assim, fomenta-se a formação voltada para o desenvolvimento de habilidades e competências como vem proposto na Base Nacional Comum Curricular-BNCC, e assim ajudando alunos a terem um bom desempenho nas avaliações externas, como o ENEM, que aborda itens contextualizados e isso exige que o estudante esteja familiarizado com tais problemas. Essa proposta é uma alternativa aos métodos de ensino mecanizados que não permitem ao educando se aprofundar na sua capacidade e desenvolvimento de habilidades. Na Figura 8, Figura 9 e Figura 10 exibimos alguns dos itens do Exame Nacional que foram trabalhados.

(ENEM 2010 - 1ª APLICAÇÃO - 2º DIA - CADERNO 5 - AMARELO - Q161 - C5H21)

Um satélite de telecomunicações, t minutos após ter atingido sua órbita, está a r quilômetros de distância do centro da Terra. Quando r assume seus valores máximo e mínimo, diz-se que o satélite atingiu o apogeu e o perigeu, respectivamente. Suponha que, para esse satélite, o valor de r em função de t seja dado por $r(t) = \frac{5865}{1+0.15 \cdot \cos(0.06t)}$.

Um cientista monitora o movimento desse satélite para controlar o seu afastamento do centro da Terra. Para isso, ele precisa calcular a soma dos valores de r , no apogeu e no perigeu, representada por S . O cientista deveria concluir que, periodicamente, S atinge o valor de

- A) 12765 km.
- B) 12000 km.**
- C) 11730 km.
- D) 10965 km.
- E) 5865 km.

Figura 2: Questão ENEM 2010. Fonte: INEP (2021).

(ENEM 2017 – 1ª APLICAÇÃO – 2º DIA – CADERNO 5 – AMARELO – Q179 – C5H19)

Um cientista, em seus estudos para modelar a pressão arterial de uma pessoa, utiliza uma função do tipo $P(t) = A + B\cos(kt)$ em que A , B e k são constantes reais positivas e t representa a variável tempo, medida em segundo. Considere que um batimento cardíaco representa o intervalo de tempo entre duas sucessivas pressões máximas.

Ao analisar um caso específico, o cientista obteve os dados:

Pressão mínima	78
Pressão máxima	120
Número de batimentos cardíacos por minuto	90

Tabela 3 – Pressão mínima, máxima e número de BCM
Fonte: INEP

A função $P(t)$ obtida, por este cientista, ao analisar o caso específico foi

A) $P(t) = 99 + 21\cos(3\pi t)$.

B) $P(t) = 78 + 42\cos(3\pi t)$.

C) $P(t) = 99 + 21\cos(2\pi t)$.

D) $P(t) = 99 + 21\cos(t)$.

E) $P(t) = 78 + 42\cos(t)$.

Figura 9: Questão ENEM 2017. Fonte: INEP (2021).

(ENEM 2019 – 1ª APLICAÇÃO – 2º DIA – CADERNO 5 – AMARELO – Q180 – C5H22)

Um grupo de engenheiros está projetando um motor cujo esquema de deslocamento vertical do pistão dentro da câmara de combustão está representado na figura.

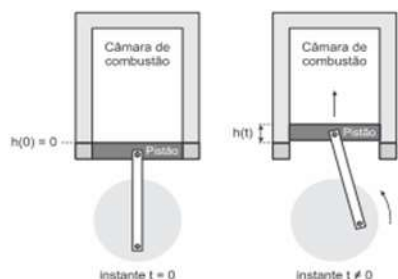


Figura 79 – Esquema do movimento do pistão dentro da câmara de combustão
Fonte: INEP

A função $h(t) = 4 + 4\sin\left(\frac{\beta t}{2} - \frac{\pi}{2}\right)$ definida para $t \geq 0$ descreve como varia a altura h , medida em centímetro, da parte superior do pistão dentro da câmara de combustão, em função do tempo t , medido em segundo. Nas figuras estão indicadas as alturas do pistão em dois instantes distintos. O valor do parâmetro β , que é dado por um número inteiro positivo, está relacionado com a velocidade de deslocamento do pistão. Para que o motor tenha uma boa potência, é necessário e suficiente que, em menos de 4 segundos após o início do funcionamento (instante $t = 0$), a altura da base do pistão alcance por três vezes o valor de 6 cm. Para os cálculos, utilize 3 como aproximação para π . O menor valor inteiro a ser atribuído ao parâmetro β , de forma que o motor a ser construído tenha boa potência, é

- A) 1. B) 2. C) 4. D) 5. E) 8.

Figura 10: Questão do ENEM 2019. Fonte: INEP (2021).

Ao final da Aula 4, vários outros exercícios contextualizados são propostos, como o exemplo ilustrado pela Figura 11 e **Erro! Fonte de referência não encontrada.** Na sequência, também é deixado pelo autor o gabarito de todos os exercícios do material de apoio.

2) (UFPR 2013) O pistão de um motor se movimenta para cima e para baixo dentro de um cilindro, como ilustra a figura.

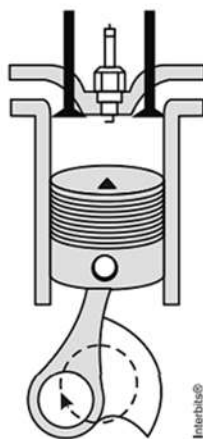


Figura 12 - Ilustração do pistão de um motor

Suponha que em um instante t , em segundos, a altura $h(t)$ do pistão, em centímetros, possa ser descrita pela expressão: $h(t) = 4\text{sen}\left(\frac{2\pi t}{0,05}\right) + 4$.

- Determine a altura máxima e mínima que o pistão atinge.
- Quantos ciclos completos esse pistão realiza, funcionando durante um minuto?

Figura 11: Questão Vestibular UFPR 2013. Fonte: Carvalho (2020).

(UFSM 2015) Cerca de 24,3% da população brasileira é hipertensa, quadro que pode ser agravado pelo consumo excessivo de sal. A variação da pressão sanguínea P (em mmHg) de um certo indivíduo é expressa em função do tempo por $P = 100 - 20 \cos\left(\frac{8\pi}{3}t\right)$, onde t é dado em segundos. Cada período dessa função representa um batimento cardíaco.

Analise as afirmativas:

- A frequência cardíaca desse indivíduo é de 80 batimentos por minuto.
- A pressão em $t = 2$ segundos é de 110 mmHg.
- A amplitude da função $P(t)$ é de 30 mmHg.

Está(ão) correta(s)

- Apenas I.
- Apenas I e II.**
- Apenas III.
- Apenas II e III.
- I, II e III.

Figura 12: Questão UFSM 2015. Fonte: Carvalho (2020).

3. CONSIDERAÇÕES FINAIS

A partir do conhecimento das inúmeras dificuldades que os educadores têm em suas práticas cotidianas, trabalhamos em cima da construção da análise e da discussão de uma proposta de ensino para as funções trigonométricas. Esse objeto de aprendizagem é bastante discutido em trabalhos acadêmicos devido suas complexidades, para ver essa frequência basta pesquisar em grandes repositórios.

Com o exposto, podemos concluir que para diminuirmos esse distanciamento entre o objeto de aprendizagem e a compreensão pelos educandos, temos que nos apropriar das diversas ferramentas a disposição. Aqui, percebe-se que o GeoGebra consegue alcançar um grande pilar do estudo das funções, o acesso a visibilidade do comportamento gráficos, o que em muitas situações são vistos apenas pelas imagens contidas nos livros didáticos, sem manipulação alguma, limitando muitas interpretações. Também há o registro do uso da História da Matemática, que segundo os autores aqui citados, ela consegue causar uma certa atração pelo objeto. Por fim, a resolução de problemas, essa por sua vez, ajuda na compreensão da Matemática em cada parte da nossa vida.

Portanto, esperamos que esse trabalho possa contribuir com os professores de Matemática que buscam instrumentos mais dialogáveis com os educandos na prática pedagógica. Sabemos que o trabalho não é fácil, mas se a cada dia conseguirmos fazer algo pelo Ensino desse componente, daqui a alguns anos alcançaremos os índices e a proficiência desejada.

4. REFERÊNCIAS

- BARBOSA, J. L. M. Geometria Euclidiana Plana. 11 ed. Rio de Janeiro: SBM, 2012. 259 p.
- CARVALHO, J. N. P. De. Funções Trigonométricas e aplicações: uma proposta didática para o ensino médio usando o GeoGebra. - UFERSA, 2020.
- EVES, H. Introdução à História da Matemática. 5a ed. Tradução de Hygino H. Domingues. Campinas-SP: Editora UNICAMP, 2011. 848 p. ISBN: 8526806572.
- IEZZI, G. Fundamentos de Matemática Elementar 3: Trigonometria. 7 ed. São Paulo: Atual, 2013. 303 p.
- _____. Matemática: ciência e aplicações, vol. 2. 9 ed. São Paulo: Saraiva, 2016. 288 p.
- INEP. PISA 2018 revela baixo desempenho escolar em leitura, matemática e ciências no Brasil. 2019. Disponível em: <http://portal.inep.gov.br/artigo/-/asset_publisher/B4AQV9zFY7Bv/content/pisa-2018-revela-baixo-desempenho-escolar-em-leitura-matematica-e-ciencias-no-brasil/21206>. Acesso em: 08/set./20.
- _____. Provas e Gabaritos ENEM. 2021. Disponível em: <<https://www.gov.br/inep/pt-br/areas-de-atuacao/avaliacao-e-exames-educacionais/enem/provas-e-gabaritos>>. Acesso em: 24/mar./22.
- KENSKI, V. M. Educação e tecnologias: o novo ritmo da informação. Campinas: Editora Papirus, 2009. 141 p.
- MACHADO, V.; PINHEIRO, N. A. M. Problema gerador de discussões: uma metodologia para o ensino em Engenharia. Revista Brasileira de Ensino de Ciência e Tecnologia, [s.l.], v. 2, no 1, p. 31–49, 2009.
- MARCO A MANETTA. Materiais Didáticos – GeoGebra. 2019. Disponível em: <<https://www.geogebra.org/materials>>. Acesso em: 07/jan./20.
- ONUCHIC, L. de la R.; ALLEVATO, N. S. G. Pesquisa em Resolução de Problemas: caminhos, avanços e novas perspectivas. Bolema - Mathematics Education Bulletin, Rio Claro, v. 25, no 41, p. 73–98, 2011. ISSN: 0103636X.
- SIQUEIRA, R. A. N. De. Tendências da Educação Matemática na formação de professores. 50 p. - Monografia de Especialização. Departamento de Pesquisa e Pós-Graduação. Universidade Tecnológica Federal do Paraná, 2007.
- SOUSA, G. C. de (org. . Aliança entre História da Matemática e Tecnologias via Investigação Matemática: Reflexões e práticas. 1a ed. São Paulo: Editora Livraria da Física/SBHMat, 2020. 270 p.
- UNICEF. Perdas de aprendizagem com a covid-19 podem custar a esta geração de estudantes quase US\$ 17 trilhões em ganhos durante a vida. Missão Recuperando a Educação. 2021. Disponível em: <<https://www.unicef.org/brazil/comunicados-de-imprensa/perdas-de-aprendizagem-com-covid-19-podem-custar-a-esta-geracao-de-estudantes-ganhos-durante-a-vida>>. Acesso em: 25/mar./22.